Enabling Collaboration in WebSphere Portal Express V6 on i5/OS

Examples using IBM Directory Server, Domino LDAP, and Microsoft Active Directory

Comprehensive step-by-step guide

Tips and common pitfalls explained

Ursula Althoff
Jiong Xin Bai
Theo Edwards
Debbie Landon

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

Notices ............................................................ vii
Trademarks ........................................................... viii

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

### Chapter 1. Planning for collaboration .......................... 1
1.1 Collaborative portlets in WebSphere Portal Express V6. ....... 2
1.2 Scenarios described in this Redpaper ............................ 5
1.3 LDAP servers ..................................................... 5
  1.3.1 Supported LDAP servers ................................ . 6
  1.3.2 Choosing a directory server .............................. 7
  1.3.3 Read/write or read-only access to the directory server. . 7
  1.3.4 LDAP directory entries required for WebSphere Portal Express .... 9
  1.3.5 LDAP and WebSphere Portal terminology ................. 11
1.4 Key technical points for integration ............................ 12
  1.4.1 User authentication ....................................... 13
  1.4.2 Authorization .............................................. 17
  1.4.3 Mail auto-detection ...................................... 20
1.5 Collaborative Services APIs .................................... 22

### Chapter 2. Scenario 1: Using Domino LDAP ..................... 23
2.1 Configuring the Domino environment ............................ 24
  2.1.1 Configuring the Domino LDAP administration server .... 24
  2.1.2 Registering the additional Domino server for Sametime. 25
  2.1.3 Configuring the additional Domino server for Sametime. .... 25
  2.1.4 Registering Domino users .................................. 27
  2.1.5 Preparing the Domino server for LDAP ........................ 27
  2.1.6 Configuring the Sametime server ............................ 32
2.2 Configuring the Domino servers for single sign-on ............... 36
  2.2.1 Creating the SSO key ...................................... 37
  2.2.2 Updating Domino server documents for SSO ................ 39
  2.2.3 Verifying SSO for Domino and Sametime servers .......... 40
2.3 Configuring collaboration in WebSphere Portal Express V6 ....... 42
  2.3.1 Configuring a WebSphere Portal Express V6 profile ....... 43
  2.3.2 Updating the access control list (ACL) of the Domino Directory .... 53
  2.3.3 Verifying WebSphere Portal Express V6 integrated with Domino LDAP .... 54
2.4 Enabling SSO between WebSphere and Domino ................... 56
  2.4.1 Exporting the WebSphere LTPA key ........................ 57
  2.4.2 Importing the LTPA key into Domino ....................... 62
  2.4.3 Verifying SSO between Domino and WebSphere Portal Express .... 65
2.5 Configuring the deployed Lotus collaborative portlets ........... 66
  2.5.1 Accessing Domino mail .................................... 68
  2.5.2 Online awareness ........................................... 69
Chapter 3. Scenario 2: Using IBM Directory Server .............................................. 71
3.1 Preparing the IDS LDAP server ................................................................. 74
   3.1.1 Basic IDS LDAP configuration on i5/OS ........................................... 74
   3.1.2 Starting the IDS Directory Server .................................................. 76
   3.1.3 Stopping the IDS Directory Server .................................................. 77
3.2 Setting up the Domino environment ......................................................... 77
   3.2.1 Configuring the primary Domino server ....................................... 77
   3.2.2 Registering a Domino server ....................................................... 81
   3.2.3 Registering Domino users ......................................................... 85
   3.2.4 Configuring the Sametime server .............................................. 88
3.3 Configuring the WebSphere Portal Express server ...................................... 95
3.4 Configuring SSO between Domino and WebSphere Portal .......................... 105
   3.4.1 LDAP with realm support and SSO .............................................. 105
   3.4.2 Generating and exporting the LTPA key ....................................... 108
   3.4.3 Importing the LTPA key into Domino .......................................... 110
   3.4.4 Enabling multi-server session-based authentication in Domino .......... 113
   3.4.5 Configuring Sametime to use the IDS LDAP settings ....................... 114
   3.4.6 Verifying SSO between Sametime, Domino, and WebSphere Portal .... 117
3.5 Integrating Domino mail and calendar ..................................................... 119
   3.5.1 Steps for Solutions 1 and 2 ....................................................... 122
   3.5.2 Solution 1: Synchronizing user names in Domino Person documents ...... 131
   3.5.3 Solution 2: Using the Domino Directory Assistance database .......... 133
   3.5.4 Verifying mail auto-detection .................................................... 143
   3.5.5 Verifying the Sametime portlets ............................................... 145
3.6 IBM Tivoli Directory Server Web Administration tool ................................ 148
   3.6.1 Enabling the system application server instance .......................... 149
   3.6.2 Configuring the IBM Tivoli Directory Server Web Administration Tool .. 150
   3.6.3 Using the IBM Tivoli Directory Server Web Administration Tool ........ 153
   3.6.4 Setting up templates and realms ............................................. 161
3.7 Using information stored in the System Distribution Directory for LDAP publishing . 166
   3.7.1 Publishing SDD data to the directory server ............................... 168
   3.7.2 Setting up SDD publishing ..................................................... 169
   3.7.3 Example using SDD publishing .............................................. 173
3.8 Managing LDAP entries with LDIF .......................................................... 187
3.9 Adding additional portlets to a WebSphere Portal page ............................ 191

Chapter 4. Scenario 3: Using Microsoft Active Directory .................................... 195
4.1 Typical integration scenarios ................................................................. 196
   4.1.1 Scenario 1 - Integrating Sametime ........................................... 196
   4.1.2 Scenario 2 - Integrating Domino mail, calendar, and Web applications . 196
   4.1.3 Scenario 3 - Integrating Domino Web applications only ................. 197
   4.1.4 Scenario 4 - Integrating Microsoft Exchange mail and calendar ........ 197
4.2 Preparing the Microsoft Active Directory .............................................. 198
   4.2.1 Required information ............................................................. 198
   4.2.2 Installing Microsoft Active Directory ....................................... 199
   4.2.3 Adding users and groups in Microsoft Active Directory .................. 200
   4.2.4 Exporting Microsoft Active Directory user information to an LDIF file . 201
4.3 Setting up the Domino and Sametime environment .................................... 203
   4.3.1 Configuring the Domino server ............................................... 203
   4.3.2 Configuring the Sametime Domino server ................................... 203
4.4 Configuring the WebSphere Portal Express V6 profile ................................ 209
4.5 Enabling SSO between WebSphere and Domino ....................................... 214
   4.5.1 Exporting the WebSphere LTPA key ....................................... 215
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5.2 Importing the LTPA key into Domino</td>
<td>219</td>
</tr>
<tr>
<td>4.5.3 Verifying SSO between Domino and WebSphere Portal Express</td>
<td>223</td>
</tr>
<tr>
<td>4.6 Sametime integration</td>
<td>225</td>
</tr>
<tr>
<td>4.6.1 How people awareness works</td>
<td>225</td>
</tr>
<tr>
<td>4.6.2 Configuring people online awareness for a Mozilla Web browser</td>
<td>228</td>
</tr>
<tr>
<td>4.6.3 Troubleshooting online awareness problems</td>
<td>229</td>
</tr>
<tr>
<td>4.7 Integrating Domino mail, calendar, and applications</td>
<td>230</td>
</tr>
<tr>
<td>4.7.1 Configuring Active Directory Synchronization (ADSync)</td>
<td>230</td>
</tr>
<tr>
<td>4.7.2 Synchronizing users between Domino and Microsoft Active Directory</td>
<td>237</td>
</tr>
<tr>
<td>4.7.3 Name mapping between Domino and Microsoft Active Directory</td>
<td>243</td>
</tr>
<tr>
<td>4.7.4 Services required on Domino for Collaboration portlets</td>
<td>245</td>
</tr>
<tr>
<td>4.7.5 Configuring mail auto-detection in WebSphere Portal Express</td>
<td>246</td>
</tr>
<tr>
<td>4.7.6 Displaying a Domino application in the Lotus Notes View portlet</td>
<td>251</td>
</tr>
<tr>
<td>4.8 Integrating Domino applications only</td>
<td>257</td>
</tr>
<tr>
<td>4.8.1 Configuring Domino</td>
<td>257</td>
</tr>
<tr>
<td>4.8.2 Authorizing users from Microsoft Active Directory to Domino applications</td>
<td>264</td>
</tr>
<tr>
<td>4.9 Integrating Microsoft Exchange mail and calendar</td>
<td>267</td>
</tr>
<tr>
<td>4.9.1 Configuring the credential vault</td>
<td>267</td>
</tr>
<tr>
<td>4.9.2 Configuring the Common PIM portlet for Microsoft Exchange</td>
<td>269</td>
</tr>
<tr>
<td>Appendix A. Using Domino Redirect with the Domino Web Access portlet</td>
<td>273</td>
</tr>
<tr>
<td>Using the Domino Web Access template</td>
<td>274</td>
</tr>
<tr>
<td>Configuring the Domino Web Access Redirect database</td>
<td>275</td>
</tr>
<tr>
<td>Verifying the Domino Web Access Redirect settings</td>
<td>280</td>
</tr>
<tr>
<td>Configuring the Domino Web Access portlet</td>
<td>281</td>
</tr>
</tbody>
</table>

**Related publications**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Redbooks</td>
<td>285</td>
</tr>
<tr>
<td>Other publications</td>
<td>285</td>
</tr>
<tr>
<td>Online resources</td>
<td>285</td>
</tr>
<tr>
<td>How to get Redbooks</td>
<td>286</td>
</tr>
<tr>
<td>Help from IBM</td>
<td>286</td>
</tr>
</tbody>
</table>
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 illustrate 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.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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

- AS/400®
- DB2®
- Domino®
- eServer™
- i5/OS®
- IBM®
- iSeries®
- Lotus Notes®
- Lotus®
- Notes®
- PartnerWorld®
- QuickPlace®
- RDN™
- Redbooks®
- Sametime®
- System i™
- Tivoli®
- WebSphere®
- Workplace™

The following terms are trademarks of other companies:

Novell, the Novell logo, and the N logo are registered trademarks of Novell, Inc. in the United States and other countries.

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

Active Directory, Internet Explorer, Microsoft, Outlook, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

This IBM® Redpaper publication shows you how to integrate collaboration into WebSphere® Portal Express Version 6 running on i5/OS®. Specifically, this paper shows you how to integrate IBM Lotus® Domino® mail and applications, IBM Lotus Sametime®, and Microsoft® Exchange into a WebSphere Portal environment. Three different scenarios are presented. The first scenario focuses on using Domino LDAP as the common directory server between Domino and WebSphere Portal. Scenario two uses IBM Directory Server. The third scenario shows you how to use Microsoft Active Directory® as the common directory server between Domino and WebSphere Portal.

This Redpaper is for system administrators who need to understand how to configure and enable collaboration in a WebSphere Portal Express V6 environment running on i5/OS.

The team that wrote this Redpaper

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

Ursula Althoff works in STG Sales as an IT Specialist for System i™ Technical Sales in Germany. She has worked at IBM for 31 years. Her experience on midrange computers started with S/38 and AS/400®. Her areas of experience include i5/OS, application development, WebSphere Application Server on i5/OS, and WebSphere Development Client for iSeries®. She has developed courses about e-business on System i for IBM Learning Services, written articles, and also co-authored several IBM Redbooks® publications about these topics. You can contact Ursula Althoff by sending e-mail to usalthoff@de.ibm.com.

Jiong Xin Bai is a Senior Product Support Professional in IBM China. She joined IBM in 1999 and worked in the Lotus support organization. In 2006, Jiong Xin joined the WPLC World Wide Support Engineering team, which is focused on technical support for critical situations. Her expertise is focused on Lotus Domino and other Domino-based products, solving complex, cross-platform, cross-product problems. You can contact Jiong Xin by sending e-mail to baijx@cn.ibm.com.
Theo Edwards is a Staff Software Engineer with the IBM Software Group in the United States. He specializes in support and solution deployment strategy for WebSphere Portal and Lotus Collaboration products on the System i platform. His current focus is on WebSphere Portal architectural design and integration. Before joining IBM in 1999, Theo worked as a system specialist and application programmer for a number of industries hosting e-business on the System i platform. Theo has contributed to numerous technical solution papers regarding Domino, Workplace™, and WebSphere Portal. You can contact Theo by sending e-mail to theo_edwards@us.ibm.com.

Debbie Landon is an IBM Certified Senior IT Specialist in the IBM ITSO, Rochester Center. Her current area of expertise is focused on the System i collaboration products, including Domino and related Lotus products such as Sametime and QuickPlace®. Debbie has been with IBM for 23 years working first with the S/36 and then the AS/400, which has since evolved to the IBM System i platform. Before joining the ITSO in November of 2000, Debbie was a member of the PartnerWorld® for Developers iSeries team, supporting IBM Business Partners in the area of Domino for iSeries. You can contact Debbie by sending e-mail to dalandon@us.ibm.com.

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

Marcel Adan
System i Technology Center (iTC) in Rochester, Minnesota

Jody Mueller
Tim Rowe
IBM Rochester Development Lab

CD Choi
IBM Raleigh Development Lab

Walter Scanlan
Global Technology Services - WPLC Support for System i, Rochester, Minnesota

Mark Owusu-Ansah
IBM Software Group - WPLC, Domino Support center in West Chester, Pennsylvania

Thomas Gray
Joanna Pohl-Misczyk
Craig Schmitz
Jenifer Servais
International Technical Support Organization, Rochester Center

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.
Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you
will develop a network of contacts in IBM development labs, and increase your productivity
and marketability.

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

Comments welcome

Your comments are important to us!

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

▸ Use the online Contact us review Redbooks form found at:
  ibm.com/redbooks

▸ Send your comments in an e-mail to:
  redbooks@us.ibm.com

▸ Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400
Chapter 1. Planning for collaboration

Understanding and planning for integrating collaboration into your WebSphere Portal Express server is an important step. Collaboration features in IBM WebSphere Portal Express V6 are provided through a series of portlets, and this chapter begins by describing these portlets. To use these collaborative features, you must install and configure one or more of the supported versions of the following products:

- IBM Lotus Domino
- IBM Lotus Sametime
- IBM Lotus QuickPlace

This Redpaper focuses on the collaboration features provided by Domino and Sametime. Integrating QuickPlace with WebSphere Portal is not covered. For more information about Domino, Sametime, and QuickPlace refer to the Lotus documentation Web site:


Another important step is understanding how the Lightweight Directory Access Protocol (LDAP) directory is used in this environment. This chapter provides information from which LDAP servers are supported, to choosing a directory, to considerations for read/write access verses read-only access, and to which LDAP entries are required to support WebSphere Portal. Finally this chapter provides a discussion of three key technical integration points of user authentication, authorization, and mail auto-detection and provides a brief and concise overview on each of these key integration points.
1.1 Collaborative portlets in WebSphere Portal Express V6

Domino and Extended Products Portlets are installed with WebSphere Portal Express V6 and are deployed automatically. Most of the collaboration portlets are accessible after a WebSphere Portal Express profile is configured. The collaboration portlets can be accessed via the navigation bar (see Figure 1-1). The navigation bar is available at the bottom of every page of your WebSphere Portal Express profile.

![Figure 1-1 WebSphere Portal Express navigation bar](image)

Clicking on the Site Map icon provides you with links for accessing the installed portlets of your WebSphere Portal Express profile as shown in Figure 1-2.

![Figure 1-2 WebSphere Portal Express Site Map](image)
Chapter 1. Planning for collaboration

Following lists the Domino and Extended Products Portlets that are installed by default and a description of how you can access them from your WebSphere Portal Express profile. You can use the Site Map navigation as shown in Figure 1-2 on page 2 to access these portlets.

- Portlets supported by a Sametime server that is configured to work with WebSphere Portal Express:
  - Sametime Contact List portlet
    
    This portlet displays a list of people that the user has added and with whom the user wants to chat online or include in online meetings. The Sametime Contact List portlet appears on the Intranet Jump Start → Collaboration and the Domino Integration → My Work pages.

    Figure 1-3 shows a sample of the Sametime Contact List and People Finder portlet. The Sametime status icon before the user name indicates whether a person is active, away, offline, or does not want to be disturbed. In this example Debra Landon is online as indicated by the green icon.

    ![Figure 1-3 People Finder and Sametime Contact List](image)

    - People Finder portlet
      
      This portlet provides both quick search and advanced search options for locating people and information about people. Once you have found a person, tasks such as adding the person to the Sametime Contact List, online chat, and other functions shown in Figure 1-3 are possible.
The People Finder portlet appears on the **Intranet Jump Start → Home** page, **Intranet Jump Start → Collaboration** page and is also accessible on every page because it is integrated in the People Palette as shown in Figure 1-4.

![People Palette]

*Figure 1-4  People Palette*

- Lotus Web Conferencing portlet
  This portlet allows users to find, attend, and schedule e-meetings as well as view meeting details. The Lotus Web Conferencing portlet appears on the **Domino Integration → My Team** page.

- Who Is Here portlet
  This portlet displays a list of people currently logged into the page or virtual page with whom the user is able to chat. The Who Is Here portlet appears on the **Domino Integration → My Team** page.

**Note:** Because the Who Is Here portlet displays every user’s name, the list can become cumbersome to manage and can degrade performance on a page that has many visitors. Deploy the Who Is Here portlet on your site only if the Sametime Contact List does not fulfill the needs of your users.

- Messaging and Calendar portlets that are referred to as Common PIM (Personal Information Management) portlets or CPP portlets:
  - Common Mail portlet
    Access mail in IBM Lotus Notes®, Microsoft Exchange, IMAP4 clients, or POP3 clients. The Common Mail portlet is shown on the **Intranet Jump Start → Collaboration** and **Messaging → Mail** pages.
  - Common Calendar portlet
    Access the calendar in IBM Lotus Notes or Microsoft Outlook®. The Common Calendar portlet is shown on the **Intranet Jump Start → Collaboration** and **Messaging → Calendar** pages.

- Portlets supported by a Domino server configured to work with WebSphere Portal Express:
  - Domino Web Access (DWA) portlet
    Portlet that can view and work with documents in a Domino mail database that is enabled for Domino Web Access. The Domino Web Access (DWA) portlet is shown on the **Domino Integration → My Work** page.

    In the scenarios covered in this Redpaper, we added the DWA portlet to the **Intranet Jump Start → Collaboration** page. This is described in 3.9, “Adding additional portlets to a WebSphere Portal page” on page 191.
  - Lotus Notes View portlet
    This portlet opens and works with mail, discussion, and teamroom databases. You can configure this portlet to open one or more views of one database or multiple databases. The Lotus Notes View portlet is shown on the **Domino Integration → My Databases** page.
Other collaboration portlets not covered in this Redpaper:

- Lotus Document Viewer portlet
  The Lotus Document Viewer portlet is shown on the Domino Integration → My Databases and Domino Integration → My Team pages.
- Inline QuickPlace portlet
  The Inline Quick Place portlet is shown on the Domino Integration → My Team page.
- My Lotus QuickPlaces portlet
- Domino Document Manager portlet
  The Domino Document Manager portlet is shown on the Documents → Document Manager page.

For a detailed description of each these portlets, refer to the IBM WebSphere Portal product documentation Web site:

### 1.2 Scenarios described in this Redpaper

In this Redpaper we focus on how to enable collaboration features in WebSphere Portal Express V6. Specifically we focus on integrating Domino mail, calendar, and applications as well as Sametime into a WebSphere Portal Express V6 profile.

Because the detailed configuration and steps vary when using different LDAP servers, we selected three typical scenarios to discuss in three separate chapters. Each chapter is a complete solution for enabling collaboration in a WebSphere Portal Express V6 profile:

- Chapter 2, “Scenario 1: Using Domino LDAP” on page 23
- Chapter 3, “Scenario 2: Using IBM Directory Server” on page 71
- Chapter 4, “Scenario 3: Using Microsoft Active Directory” on page 195

### 1.3 LDAP servers

This section describes the fundamental role directory services plays within WebSphere Portal Express V6.

Your directory server is the starting point for your WebSphere Portal server. All user information is stored in the LDAP directory. Everything from authentication, authority, and data access is determined from the information received from the directory server. If the information stored in the directory server is invalid, the function of WebSphere Portal server is compromised. Due to the dependence on the LDAP server, configuring your directory server properly before you configure your first WebSphere Portal server is important.
Note: If you do not configure security as part of the configuration process for WebSphere Portal server, a self-contained directory service based upon WebSphere Portal Member Manager is deployed. This is considered to be the internal directory server. The internal directory server is not designed for use beyond a typical sandbox implementation consisting of a few users.

Because the purpose of this Redpaper is to configure a WebSphere Portal server production environment, we assume that you will use an LDAP server for your directory service provider.

This section covers the following topics:

- 1.3.1, “Supported LDAP servers” on page 6
- 1.3.2, “Choosing a directory server” on page 7
- 1.3.3, “Read/write or read-only access to the directory server” on page 7
- 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9
- 1.3.5, “LDAP and WebSphere Portal terminology” on page 11

Note: Directory servers use the Lightweight Directory Access Protocol (LDAP). In this Redpaper directory server, LDAP server and LDAP directory are synonymous and may be used interchangeably.

1.3.1 Supported LDAP servers

WebSphere Portal Express V6 on i5/OS supports the following LDAP servers:

- IBM Tivoli® Directory Server V6.0
- IBM Tivoli Directory Server V5.2
- IBM Tivoli Directory Server V5.1
- IBM Lotus Domino V7.0.1
- IBM Lotus Domino V6.5.5
- IBM Lotus Domino V6.5.4
- Novell® eDirectory V8.7.3
- Sun™ Java™ System Directory Server V5.2
- Microsoft Active Directory 2003
- Microsoft Active Directory 2000
- Microsoft Active Directory Application Mode (ADAM) 2003

Note: The i5/OS V5R4 Directory Server is equivalent to the IBM Tivoli Directory Server V5.2. The i5/OS V5R3 Directory Server is equivalent to the IBM Tivoli Directory Server V5.1.

When using the Create WebSphere Portal wizard in IBM Web Administration for i5/OS to configure a WebSphere Portal Express server, the Microsoft Active Directory Application Mode (ADAM) 2003 is not supported. For information about using the Create WebSphere Portal wizard to configure a WebSphere Portal Express server, refer to the IBM Redpaper Installing and Configuring WebSphere Portal Express V6 on i5/OS, REDP-4303.
1.3.2 Choosing a directory server

Choosing a directory server is an important decision, and your choice of which directory server is best for you to use with WebSphere Portal Express depends mostly on your existing environment.

If you have an existing LDAP infrastructure that is supported for use with WebSphere Portal Express (see 1.3.1, “Supported LDAP servers” on page 6), your decision might be easy. You can continue to use your existing directory server. When you decide to use your existing directory server environment, it might be necessary to do some additional configuration in your LDAP directory before you configure a WebSphere Portal profile, see 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9.

If you have an existing Domino infrastructure, this Redpaper helps you to configure your Domino server to use the LDAP functionality that is part of Domino. This topic is covered in Chapter 2, “Scenario 1: Using Domino LDAP” on page 23.

If you do not have an LDAP directory in place already, the easiest way to implement an LDAP directory for your WebSphere Portal environment is to configure IBM Directory Server for i5/OS. Because LDAP is part of i5/OS and basic configuration is very easy, you may want to consider using this as your LDAP server. Refer to Chapter 3, “Scenario 2: Using IBM Directory Server” on page 71 for additional information.

1.3.3 Read/write or read-only access to the directory server

Security for the WebSphere Portal environment can be configured with read/write access or read-only access to the LDAP directory information. Before you can run the Create WebSphere Portal wizard provided by the IBM Web Administration for i5/OS, you have to determine whether or not you will allow read-only or read/write access to your directory server.

The following information is a brief explanation of read/write access versus read-only access to help you make this decision.

Read/write access

Read/write access allows the WebSphere Portal server to update and manage user and group information in the LDAP directory. In the background, WebSphere Portal uses the defined WebSphere Portal administrator user for this management.

If you do not have an existing LDAP tree, have little LDAP experience, or want the Create WebSphere Portal wizard (only in the case where you use an IBM Directory Server) to correctly create and configure the objects required for your WebSphere Portal environment, then consider granting read/write access to the directory server. With read/write access and by using IBM Directory Server, the Create WebSphere Portal wizard creates the following entries in the LDAP directory required for the WebSphere Portal environment (see Figure 1-6 on page 9):

- Create a users container.
- Create a groups container.
- Create a WebSphere Portal administrator user in the users container (default is wpsadmin).
- Create four WebSphere Portal administrator group entries in the groups container.
- Add the WebSphere Portal administrator user as a member to all of the WebSphere Portal administrator group entries in the groups container.
If you want to use the WebSphere Portal Express First-time Visitor functionality, where new users can do the self-registration process (see Figure 1-5), which also creates an entry in the LDAP directory for this new user, you have to allow read/write access. The WebSphere Portal administrator user is used in the background to do this registration. This self-registration process works together with the Edit My Profile function for subscriber self-management, where updates to the LDAP directory can be made directly by the WebSphere Portal user.

Figure 1-5   WebSphere Portal First Time Visitor - Self sign up

Permitting users to self-register via the Sign up now link for the First-time Visitor function may not be desired. This feature can be disabled by customizing the WebSphere Portal configuration and thereby causing no harm by granting read/write access to the LDAP directory. With this customization in place, all user registration and maintenance is performed by the LDAP administrator. For information about removing the self-registration and Edit my profile functions, refer to the IBM WebSphere Portal Express Version 6.0 Information Center:
http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp

Tip: For simplicity, we recommend that you allow the WebSphere Portal administrator user via the Create WebSphere Portal wizard, read/write access to the LDAP directory and then customize the WebSphere Portal server to remove the Sign up and Edit my profile links.

Read-only access
Read-only access enables all WebSphere Portal users, including the WebSphere Portal administrator user, to retrieve only user information from the LDAP directory. Read-only access requires that your LDAP directory server have the following entries in place before running the Create WebSphere Portal wizard to create a WebSphere Portal Express profile:

- A users container.
- A groups container.
- A WebSphere Portal administrator user in the users container.
- Four WebSphere Portal administrator group entries in the groups container.
- The WebSphere Portal administrator user has to be a member of all the WebSphere Portal administrator group entries in the groups container.

If you decide to work with read-only access, it is the LDAP administrator’s responsibility to create the objects in the preceding list in your LDAP directory. Refer to 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9 for more information about the required entries for WebSphere Portal implementation.
1.3.4 LDAP directory entries required for WebSphere Portal Express

Figure 1-6 shows the entries of the elements and hierarchy of the LDAP directory that have to exist for the WebSphere Portal environment:

- A users container.
- A groups container.
- The WebSphere Portal administrator user in the users container (by default this is wpsadmin).
- Four WebSphere Portal administrator group entries in the groups container.
- The WebSphere Portal administrator user has to be a member of all the WebSphere Portal administrator group entries.

Figure 1-6  Required elements in the LDAP directory for WebSphere Portal

Figure 1-6 also shows you the default names for these LDAP elements. The Create WebSphere Portal wizard uses these names when it creates these entries in the LDAP directory during the create WebSphere Portal profile process.

Important: The Create WebSphere Portal wizard can create these elements only when read/write access is given. See 1.3.3, “Read/write or read-only access to the directory server” on page 7.

In general you have to have an LDAP directory that has the structure shown in Figure 1-6, but the name of the elements can be different. For implementation you have two choices:

- Create the needed elements in your LDAP directory before configuring a WebSphere Portal profile.
- Let the Create WebSphere Portal wizard create these elements during the WebSphere Portal profile create process.

You should consider the following:

- Container for users and groups

Figure 1-7 on page 10 shows the LDAP Configuration Parameters - Step 10 of 14 panel from the Create WebSphere Portal Express wizard where you define the information for the users and WebSphere Portal administrative group entries.

The wizard can create the users and groups containers and the underlying elements in the LDAP directory only when you do not override the values the wizard shows for Parent DN (cn=users and cn=groups). In other words, only containers with the names users and groups can be created by the wizard.
Enabling Collaboration in WebSphere Portal Express V6 on i5/OS

For Domino LDAP servers, the use of user Parent DN is not required, although it is highly recommended. If you configure your WebSphere Portal server to use a Domino LDAP server, the wizard provides a special value, *ROOT, which you can use for the user Parent DN. This value indicates that users for the WebSphere Portal environment, including the administrator user, are to be located in the root of the Domino LDAP server. This is the only LDAP server type for which this additional support is provided. You are not required to use the *ROOT special value when configuring a Domino server. You can specify locating users for the WebSphere Portal environment in a user parent DN container. You may want to use a user Parent DN and then configure your groups to have a Parent DN of *ROOT. This is a common configuration.

The Object class and the Naming attribute (for both user and group entries) shown in Figure 1-7 can be selected from the list the wizard retrieves from the LDAP server.

Note: If your LDAP server is not an IBM Directory Server, the wizard does not present default values as shown in Figure 1-7 and regardless of your LDAP access level, does not create the containers. The containers must exist in your LDAP directory prior to running the wizard. You can use the Browse button to select an existing Parent DN for the users and groups containers.

For Domino LDAP servers, the use of user Parent DN is not required, although it is highly recommended. If you configure your WebSphere Portal server to use a Domino LDAP server, the wizard provides a special value, *ROOT, which you can use for the user Parent DN. This value indicates that users for the WebSphere Portal environment, including the administrator user, are to be located in the root of the Domino LDAP server. This is the only LDAP server type for which this additional support is provided. You are not required to use the *ROOT special value when configuring a Domino server. You can specify locating users for the WebSphere Portal environment in a user parent DN container. You may want to use a user Parent DN and then configure your groups to have a Parent DN of *ROOT. This is a common configuration.

The Object class and the Naming attribute (for both user and group entries) shown in Figure 1-7 can be selected from the list the wizard retrieves from the LDAP server.

Create WebSphere Portal Express, V6.0
LDAP Configuration Parameters - Step 10 of 14

The Portal server utilizes LDAP to store user information for authentication purposes. Below is where the administrator user and group will reside in your LDAP directory.

Information describing user entries
Parent DN: cn=users,DC=rchsl10,DC=rchland,DC=ibm,DC=com
Object class: inetOrgPerson
Naming attribute: uid

Information describing the administrative group entry
Parent DN: cn=groups,DC=rchsl10,DC=rchland,DC=ibm,DC=com
Object class: groupOfUniqueNames
Naming attribute: cn
Member attribute: uniqueMember

Figure 1-7 Create WebSphere Portal wizard - LDAP configuration parameters

▶ WebSphere Portal administrator user

The wizard automatically creates this user on all LDAP directories except for Windows® Active Directory.

Figure 1-8 on page 11 shows the LDAP Administrative Group and Administrative User - Step 11 of 14 panel from the Create WebSphere Portal wizard where you define the information for WebSphere Portal administrative groups and administrator user.

In the Portal administrator information section you provide the user name for the WebSphere Portal administrator and the password for this administrator. You can also use the Browse buttons to select an existing group and an existing user. In this case, the entries have to exist in the LDAP directory before running the wizard.
The administrator user you define here will also become the WebSphere Application Server administrator.

**Note:** The wizard creates this user even if something other than the default wpsadmin is entered.

- **WebSphere Portal administrative groups**
  
  The wizard automatically creates all four administrative groups on any of the supported LDAP directories (including Microsoft Active Directory). Additionally, the wizard automatically adds the WebSphere Portal administrator user you defined as a member into these four groups.

**Note:** The wizard creates these four administrative groups under the chosen Parent DN container in the LDAP Configuration Parameters - Step 10 of 14 panel (Figure 1-7) even if something other than the default group name is entered.

---

**1.3.5 LDAP and WebSphere Portal terminology**

Following is a brief overview of LDAP terms. Information that is important for WebSphere Portal in an LDAP context is also listed.

- **LDAP server host name:** The fully qualified name of your LDAP server - for example, hostname.domain.com.
- **LDAP port:** The port your LDAP server listens on. The default is 389.
- **Suffix:** A directory contains a collection of objects organized in a tree structure. Entries are organized in a tree-like structure called the Directory Information Tree (DIT). The suffix is the top entry in your LDAP directory information tree. This can also be referred to as the...
base entry or the root. There can be several suffixes in an LDAP directory, each representing the top of a separate directory information tree.

- **Distinguished name (DN):** A DN is a unique name that explicitly identifies a single entry. It is similar to the primary key in a database file. DN is made up of a sequence of relative distinguished names (RDNs). Each RDN™ in a DN corresponds to a branch in the DIT leading from the root of the DIT to the directory entry. A DN is composed of a sequence of RDNs separated by commas, such as uid=althoff,cn=users.

- **User parent DN:** Specifies the user parent DN for the LDAP server. The DN uniquely identifies an entry in the LDAP server and is used to access the LDAP directory for authentication. For example: cn=users,DC=system,DC=subdomain1,DC=subdomain2.

- **Group parent DN:** Specifies the group parent DN for the LDAP server. The DN uniquely identifies an entry in the LDAP server and is used to access the LDAP directory for authentication. For example: cn=groups,DC=system,DC=subdomain1,DC=subdomain2.

- **Object class:** Each entry in a directory belongs to one or more object classes. An object class describes the content and purpose of the object. It also contains a list of attributes, which is described by the schema, such as a telephone number or surname.

For IBM Directory Server, the WebSphere Portal server works with the object class inetOrgPerson for a user and groupOfUniqueNames for a group by default.

- **LDAP administrator:** A user account in your directory server that has read/write authority to the directory server. This could be the administrator of the LDAP directory. Use of this account is required during the configuration of the WebSphere Portal server.

- **Users container:** A container that holds LDAP entries that belongs to the same object class, so these entries have equal attributes. WebSphere Portal works by default with a container called users, where information about users is stored.

- **Groups container:** In the groups container, the administrative users groups used in WebSphere Portal are stored. For every administrator group in the groups container, a minimum of one member (that is, the WebSphere Portal administrator user) is assigned. To grant administrative privileges to other users, add them to the corresponding administrative users group.

- **WebSphere Portal administrator:** The administrator account for WebSphere Portal that is selected or created when the WebSphere Portal server is configured. This account is used for all administration tasks inside the WebSphere Portal server. For example, to configure portlets and to administrate users and user access inside the WebSphere Portal server.

### 1.4 Key technical points for integration

WebSphere Portal is used to integrate several enterprise information systems and present them through the portal user interface. From the users' point of view, they want to log on to the WebSphere Portal home page once and get all information they need from there. The user expects to log on with a single user name and password, no matter how many backend systems WebSphere Portal server must connect to retrieve the required information.

From the system administrators' point of view, they need to integrate the WebSphere Portal server with all the backend systems and products to meet the user's requirements. To provide collaboration services to portal users, you need to integrate Domino and Sametime servers with the WebSphere Portal server.
Domino, Sametime, and WebSphere Portal can generally work with different user registries. They also have different mechanisms for user authentication and authorization. To integrate these different servers, you need to consider these key technical integration points:

- User authentication
- Authorization
- Mail auto-detection

This section describes potential solutions for the previously listed technical integration points. Detailed steps for implementing these solutions depend on the actual configuration you are using and are described throughout this Redpaper.

### 1.4.1 User authentication

The basis of access control is to identify the person or program that is requesting access. This process is called authentication. The most common form of authentication is through the combination of a user identification string (user ID) and a user secret word (password) to establish certainty about the requestor.

#### Forms of authentication

An authentication mechanism defines rules about security information and the format of storing security information. Some standard ways to authenticate a user (for example, user ID and password) are used when a client attempts to access a protected resource on the application server, such as:

- HTTP basic authentication: A Web browser mechanism using a standard logon dialog
- HTTP form-based authentication: A mechanism where the server sends a customized authentication form that is presented to the user

Basic WebSphere Portal authentication stores user IDs and passwords in the WebSphere Portal database. This is the default environment when you configure WebSphere Portal using the basic configuration task or the Create WebSphere Portal configuration wizard specifying not to secure the server using LDAP. In this case, WebSphere global security is not enabled, and WebSphere Portal authentication is not connected to application server security. WebSphere Portal roles and authorization still work. WebSphere Portal uses basic portal-based authentication with the WebSphere Member Manager (WMM) database. User IDs and passwords are stored in the Portal database.

The form-based authentication mechanism permits a site-specific logon through a JavaServer™ Page (JSP™) form. This Redpaper focuses on WebSphere Portal authentication using this form-based authentication mechanism. This authentication mode is configured when you use the Create WebSphere Portal configuration wizard specifying that you want to secure the server using a LDAP user registry. For a list of which LDAP directory servers are supported with WebSphere Portal, see 1.3.1, “Supported LDAP servers” on page 6.

WebSphere Portal has an authentication subsystem that enables it to delegate authentication to the underlying mechanisms of the WebSphere Application Server. Using this native WebSphere Application Server authentication, the user's authentication data provided in the JSP form is posted to a servlet that requests WebSphere Application Server security to validate the user's authentication data.

The authentication mechanism in WebSphere Application Server collaborates closely with a user registry. The user registry is the user and groups account repository that the authentication mechanism consults with when performing authentication. Also, the authentication mechanism is responsible for creating a credential, which is an internal
representation of a successfully authenticated client user. This credential is the Lightweight Third Party Authentication (LTPA cookie), which is discussed in the next section.

For a complete description of the WebSphere Portal authentication options - for example, using an authentication proxy where the system is configured for third-party authentication via an external security manager such as IBM Tivoli Access Manager - refer to the WebSphere Portal Information Center:


Single sign-on and LTPA concepts
After a user logs on to WebSphere Portal, and the authentication mechanism described previously successfully authenticates the client user to the WebSphere Portal, how can all other backend systems know who is accessing them when the user does not provide a user name and password again?

You can configure single sign-on (SSO) between WebSphere Portal, Domino, and Sametime to achieve this.

**Note:** Even if WebSphere Portal is using Domino as the LDAP server, SSO between Domino and WebSphere Portal is required.

The goal of SSO in general is to provide a secure method to authenticate the user once within an environment. The same credentials are then used to authenticate to different applications in the same SSO domain. SSO removes the need for a user to enter authentication information again when switching from one application to another within the WebSphere Portal environment.

This Redpaper provides information about the main concepts that you need to understand to implement WebSphere Portal SSO and targets Domino and WebSphere Portal administrators or IT architects who will integrate WebSphere Portal into an environment using the native SSO capabilities of the products. SSO between WebSphere Portal, Domino, and Sametime is achieved through the use of the Lightweight Third Party Authentication (LTPA) mechanism.

When SSO is properly configured, a LTPA token is generated from the WebSphere Application Server using cryptographic keys after a user is successfully authenticated against the defined user registry of the WebSphere Portal. This encrypted session cookie, called the LTPA cookie, is sent to the client and stored in their Web browser. It contains the distinguished name (DN) of the user as it is stored in the LDAP directory used for authentication. Any additional requests of this successfully authenticated client to the WebSphere Portal and its backend servers such as Domino and Sametime via the collaboration portlets, contains this LTPA cookie.

All servers defined and accessible in the SSO domain use this LTPA cookie to know that the client is already authenticated. They use the same cryptographic keys the WebSphere Application Server used to encrypt for decrypting the LTPA token to determine who the authenticated user is. For this reason, the cryptographic keys the WebSphere Application Server is using must be exported to all servers in the SSO domain such as the Domino and Sametime servers.

The LTPA cookie contains the following information:

- **Cookie name:** Always set to LtpaToken.
- **Domain:** Set to the Internet domain shared by all servers participating in the SSO - for example, rchland.ibm.com.
Chapter 1. Planning for collaboration

- **Cookie expiration**: Set to delete this cookie at the end of the Web browser’s lifetime.
- **Secure**: Set to force the use of SSL. An LTPA configuration setting creates cookies that are sent only through SSL.
- **Cookie value**: Set to the LTPA token. LTPA token is an encrypted string that contains the following information:
  - **User data**: Typically set to the user ID, but can be any user information used to uniquely identify the user.
  - **Expiration time**: This is different from the cookie expiration. This field enforces a time limit that starts from the moment of logon. It is unaffected by Web browser activity or inactivity. The time limit is a configurable LTPA setting that defaults to 30 minutes.
  - **Digital signature**: Used to validate the token.

For more information about the LTPA mechanism, consult the *IBM WebSphere V5.0 Security WebSphere Handbook Series*, SG24-6573 or the WebSphere Version 6 Information Center: [http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp](http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp)

**SSO prerequisites**

Before you configure SSO, you must configure and meet the following prerequisites and conditions:

- Verify that all servers are configured as part of the same Domain Name Service (DNS) domain. For example, if the DNS domain is specified as rchland.ibm.com, then SSO is effective with any Domino server or WebSphere Application Server on a host that is part of the rchland.ibm.com domain - for example, a.rchland.ibm.com and b.rchland.ibm.com.
- Define all users in a single LDAP directory that is used for authentication.
- Enable HTTP cookies in Web browsers because the authentication information generated by the server is transported to the Web browser in a cookie. The cookie is then used to propagate the user's authentication information to other servers. This exempts the user from entering authentication information for every request to a different server.
- Verify that all servers participating in a protection domain have their time, date, and time zone synchronized. If not, LTPA tokens appear as prematurely expired and cause authentication or validation failures. LTPA is time sensitive.
Authentication flow control in WebSphere Portal on first logon

Figure 1-9 shows the authentication flow with WebSphere Portal configured to use WebSphere Application Server security and a LDAP directory for authentication. It shows the detailed flow of control, when a client request for a WebSphere Portal destination is not yet authenticated. This is the case when a user accesses the WebSphere Portal server for the first time.

Following is a brief explanation for each of the steps in Figure 1-9:

1. The client requests access to a WebSphere Portal server for the first time - for example, http://myhost.mycompany.com/wps/portal. The WebSphere Application Server receives a request for this enterprise application (the WebSphere Portal server).

2. The WebSphere Application Server security component requests the authentication credentials from the client. The client is redirected to an authentication form that prompts the user to provide the credentials for authentication - that is, the user ID and password. The URI of the initially requested resource is preserved for the session in another cookie, the Session cookie, while the logon form is served.

3. That Session cookie is returned to the server when the form is submitted by the user and the credentials are posted the to WebSphere Portal's authentication servlet.

4. The servlet makes the required calls to WebSphere Application Server's security functions.

5. WebSphere Application Server security function authenticates the user by checking the provided credentials against the user registry that is defined in the WebSphere Portal server.
6. The WebSphere Application Server security function generates the LTPA token (when authentication is successful - that is, the user is found in the LDAP directory) and uses the URI contained in the Session cookie (redirect URL) to redirect to the originally requested resource via sendRedirect().

7. The result in this case is that the WebSphere Portal home page goes back to the Web browser together with the LTPA cookie and the Session cookie, which are stored in the user's Web browser. The LTPA cookie contains the distinguished name (DN) of the user as it is stored in the LDAP directory used for authentication.

8. At this point, the Web browser has an LTPA token including the DN of the authenticated user, which is sent for all further requests to the WebSphere Portal and its integrated backend servers.

1.4.2 Authorization

By using the SSO and LTPA concepts, the Domino and Sametime servers know who the authenticated user is. At this point, the second question is, what can the user do on the current server?

Sametime allows all authenticated users to use the instant messaging and Web conferencing features. So in addition to configuring SSO for the Sametime server, no further configuration is needed for authorization.

Figure 1-10 shows the flow of SSO between WebSphere Portal and Sametime. To make the flow clear, we show the flow of the process after the authentication (first logon to WebSphere Portal) has occurred.
As an example, we use user `cn=pgn,dc=rchas60,dc=rchland,dc=ibm,dc=com` to explain the steps in Figure 1-10 on page 17:

1. The already authenticated user accesses portlets that use the Sametime functions. The LTPA token including the distinguished name (DN) of the authenticated user, is sent with the request.

2. The Sametime server extracts the user name from the LTPA token.

3. Sametime verifies the user in the LDAP directory. The LDAP directory is defined in the Sametime configuration. In our example, Sametime and WebSphere Portal use the same LDAP server.

4. Sametime returns the requested information back to the portlet.

5. The STLinks applet provides people awareness in all the Domino and Extended Products Portlets, this is downloaded to the Web browser client. Also the result for the accessed Sametime portlet is sent back to the client Web browser.

Domino works with separate access control lists (ACLs) for each database for authorization. For example, each mail file and each application database has its own ACL. To allow an authenticated user to access these databases, you have to define your user in the ACL in different notations, depending on the LDAP server you are using for authentication in your WebSphere Portal. See Table 1-1.

<table>
<thead>
<tr>
<th>LDAP server for WebSphere Portal authentication</th>
<th>User exists in both directories</th>
<th>User name in ACL</th>
<th>Example</th>
<th>Suitable for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino</td>
<td>No</td>
<td>Domino name</td>
<td>JX Bai/ITSO</td>
<td>Mail and applications</td>
</tr>
<tr>
<td>Others</td>
<td>No</td>
<td>LDAP name in Domino format</td>
<td>CN=JX Bai/DC=rchland/DC=IBM/DC=com</td>
<td>Applications only</td>
</tr>
<tr>
<td></td>
<td>Yes (name mapping required)</td>
<td>Domino name and LDAP name</td>
<td>JX Bai/ITSO CN=JX Bai/DC=rchland/DC=IBM/DC=com</td>
<td>Mail and applications</td>
</tr>
</tbody>
</table>

As shown in Table 1-1:

- **Authorization using Domino as LDAP for authentication**
  In this case, authorization is straightforward because all users exist only in the Domino Directory. In the database ACL, you add user names in Domino format and grant an appropriate access level to them. For example, you can add user `JX Bai/ITSO` into the Domino database ACL.

- **Authorization using a non-Domino LDAP for authentication where users only exist in the LDAP and not in Domino**
  In this case, all users exist in the third-party LDAP server, not in the Domino Directory. You can add LDAP user names directly to the Domino database ACL to grant the appropriate access level to them. However, you must convert the LDAP user name into Domino format, that is replace the comma (,) with a slash (/). For example, you can add user `CN=JX Bai/rchland/DC=IBM/DC=com` into the Domino database ACL.

The advantage of this method is there is no need to maintain two sets of user information in the third-party LDAP directory and the Domino Directory. With this solution, you can integrate WebSphere Portal only with Domino applications and not with Domino mail.
Authorization using a non-Domino LDAP for authentication where users exist in the LDAP and in Domino

When you need to integrate Domino mail into WebSphere Portal and you are using a third-party LDAP server for WebSphere Portal authentication, you need to synchronize users between Domino and the LDAP server by implementing name mapping between the Domino Directory and the LDAP directory. Different implementations are possible for this authorization. One solution is to add the LDAP user information in the ACL of the Domino database in the Domino notation in addition to the Domino name.

Figure 1-11 demonstrates the process of authorization in the case of a Domino application integration, where the directory used for WebSphere Portal authentication is a non-Domino LDAP. The example describes the use of the Microsoft Active Directory, but it also works in the same way with an IBM Directory Server (IDS) directory. To make the flow clear, we show the flow of the process after the authentication (first logon to WebSphere Portal) has already occurred.

The user synchronization and name mapping must be configured before the authorization process shown in Figure 1-11 occurs. Following is a brief explanation for each of the steps in Figure 1-11:

1. An already authenticated user accesses a portlet to request access to DB.nsf on a Domino server. The LTPA token including the DN of the authenticated user is sent with the request.

2. Domino extracts the user name from the LTPA token and maps the name to a corresponding Domino user name, which is stored in the Domino Person document.

3. The LTPA cookie is sent with the request, and the Portal Portlet uses it to identify the user.
Domino then verifies the user authority in the DB.nsf ACL. The requested information is then sent back to WebSphere Portal.

3. WebSphere Portal sends the information to the Web browser.

For user synchronization, you can use a Domino utility called ADSync to synchronize users between Domino and Microsoft Active Directory. For name mapping, we added the user's LDAP name in the Domino Person document. Detailed steps are covered in Chapter 4, “Scenario 3: Using Microsoft Active Directory” on page 195.

Note: It is also possible to use Tivoli Directory Integrator to map the names. For more information about IBM Tivoli Directory Integrator, refer to:

1.4.3 Mail auto-detection

For all portlets where mail and calendar information is needed, the corresponding server (Domino or Exchange server) provides the information. The WebSphere Portal server has to know the mail file and mail server name for the accessing user.

The portlets that need mail auto-detection to locate users’ source mail files are:
- Domino Web Access portlet
- Lotus Notes View portlet
- Common Mail portlet
- Common Calendar portlet

The user information requested by the WebSphere Portal server consists of the following attributes for mail auto-detection:
- mailserver
- mailfile
- http-hostname
- http-port

By default, the Domino Directory contains the required attributes for each user. However, you have to configure the LDAP schema settings as described in “Editing the LDAP schema settings” on page 30, and in “Extending the Domino LDAP schema attribute type selection” on page 140.

Another option is to extend the non-Domino LDAP server's schema to add the mailserver and mailfile attributes there. In this case, the values for every user have to be set in the non-Domino LDAP.

In Chapter 3, “Scenario 2: Using IBM Directory Server” on page 71, we provide another option for implementing mail auto-detection and name mapping. This example is described in 3.5.3, “Solution 2: Using the Domino Directory Assistance database” on page 133.

Common PIM portlets rely on settings in the CSEnvironment.properties file to determine which LDAP server to query for the attributes. If you are using Domino LDAP for WebSphere Portal authentication, the Create WebSphere Portal wizard automatically enables the CSEnvironment.properties file with all necessary information. No further manual configuration is required. If you are using an LDAP server other than Domino for WebSphere Portal authentication, you need to configure the CSEnvironment.properties file manually to provide the LDAP server and corresponding binding information. In addition, you have to complete additional steps for name mapping and mail auto-detection.
Figure 1-12 shows the flow for mail auto-detection when WebSphere Portal is using a non-Domino LDAP server.

Following is a brief explanation for each of the steps in Figure 1-12:

1. An already authenticated user accesses a portlet to request access to a mail file. The LTPA token, including the DN of the authenticated user, is sent with the request.
2. The mail portlet (PIM or DWA) checks the CSEnvironment.properties file.
3. The information in the CSEnvironment.properties file determines which LDAP server contains the user's mail information. The mail portlet then makes LDAP queries to get information for the mailfile and mailserver attributes.
4. The LDAP server returns the mail information to the portlet.
5. The WebSphere Portal server requests a specific mail file from Domino.
6. Domino returns the content of the mail file to the WebSphere Portal server.
7. The WebSphere Portal server sends the mail content to the Web browser.

If you provide a Domino LDAP server name in the CSEnvironment.properties file, steps 3 and 4 are executed. If you provide another LDAP server name in the CSEnvironment.properties file, steps 3 and 4 are not executed. In this case, you must extend the LDAP schema to add the mailserver and mailfile attributes for each user.

Note: The LDAP server shown Figure 1-12 is the LDAP server that contains the mailserver and mailfile attributes for each user. WebSphere Portal does not have to use the LDAP server for authentication.
For name mapping, we added the user’s LDAP name in the Domino Person document. Detailed steps are covered in 3.5.2, “Solution 1: Synchronizing user names in Domino Person documents” on page 131.

**Common PIM portlet with Microsoft Exchange mail**
If you are using Microsoft Exchange mail, mail auto-detection is *not* supported by the Common PIM Portlet and Exchange portlets. Each user must manually configure the portlet. See 4.9.2, “Configuring the Common PIM portlet for Microsoft Exchange” on page 269 for details.

**Domino Web Access portlet**
For the Domino Web Access portlet, you can also use the same implementation as for the Common PIM portlets for mail auto-detection. Alternately, you can use the DWA Redirect feature provided by Domino. See “Configuring the Domino Web Access Redirect database” on page 275 for details.

### 1.5 Collaborative Services APIs

The primary goal of the Collaborative Services APIs is to provide the data for the portlets user interface and to enable developers to execute actions on installed Domino and Extended Products Portlets.

Collaborative Services APIs are a set of methods and JavaServer Page tags that enable developers who are writing portlets for WebSphere Portal Express or other application servers to add Lotus collaborative functionality to their portlets.

The Collaborative Services can be used to develop new custom portlets or to add collaborative functionality (for example, menus or person links indicating online status) to existing portlets. The Collaborative Services are Java APIs that provide the building blocks for integrating the functionality of Domino, Sametime, and QuickPlace into the portal and portlets.

Collaborative Services enhance many aspects of the operation of a collaborative portal site, including:

- Authentication and single sign-on
- Directory services
- Other features

The Collaborative Services APIs are used in several collaboration portlets by default. You can modify the operation of the collaborative servers and portlets in various ways by manually editing the Lotus Collaborative Services environment properties file (CSEnvironment.properties) on the WebSphere Portal Express server.

The Collaborative Services program runs in the cs.jar file in the following location on i5/OS:

```
portal_server_root_user/shared/app/
```

For more information about the Collaborative Services APIs, refer to the IBM WebSphere Portal Express Version 6.0 Information Center:

```
http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp
```
Scenario 1: Using Domino LDAP

This chapter provides all the necessary steps for configuring a WebSphere Portal Express environment with collaboration functionality using Domino LDAP for user authentication at the portal site. This chapter provides an example of configuring the following Domino servers and WebSphere Portal profile:

- DOMLD7 - Domino LDAP directory server and administration server
- STLD7 - Sametime server Version 7.5

**Tip:** Sametime configured on a separate dedicated Domino server reflects a best practice in most production environments.

- WPX6LD7 - WebSphere Portal Express V6 profile

**Note:** The LDAP directory services can be provided by any of the other Domino servers in this environment, but we chose to run LDAP on a separate administration Domino server. Make sure the LDAP task is run on only one Domino server. If you run the LDAP task on multiple Domino servers, you run the risk of configuring your environment incorrectly by pointing to the wrong LDAP server.
2.1 Configuring the Domino environment

This section shows you how to configure the Domino environment as well as how to configure Domino to be an LDAP server. The following steps are covered:

- 2.1.1, “Configuring the Domino LDAP administration server” on page 24
- 2.1.2, “Registering the additional Domino server for Sametime” on page 25
- 2.1.3, “Configuring the additional Domino server for Sametime” on page 25
- 2.1.4, “Registering Domino users” on page 27
- 2.1.5, “Preparing the Domino server for LDAP” on page 27
- 2.1.6, “Configuring the Sametime server” on page 32

2.1.1 Configuring the Domino LDAP administration server

Perform the following steps to create the Domino LDAP administration server. In our example, we call this Domino server DOMLD7.

1. From a 5250 emulation session, type the Configure Domino Server (CFGDOMSVR) CL command and press F4 to prompt the command.

2. On the Configure Domino Server display, enter the Domino server name. For our example this is DOMLD7. For the Option parameter, enter *FIRST and press Enter.

3. Enter the remaining Domino server configuration parameters as shown in Table 2-1, and press Enter to configure the Domino server. Following is the completed CFGDOMSVR command:

```
CFGDOMSVR SERVER(DOMLD7) OPTION(*FIRST) DTADIR('/DOMINO/DOMLD7/DATA') ORG(ITSO) ADM(Admin ITSO *N (password) 8 (password)) TIMEZONE(CST) WEB(*HTTP *IIOP) DIRSRV(*LDAP) CNNSRV(*NONE) TCPOPT(*NOENCRYPT DOMLD7.RCHLAND.IBM.COM) SVRHSTNAME(DOMLD7.RCHLAND.IBM.COM) SBS(DOMLD7) TEXT('Domino LDAP Administration server')
```

Table 2-1 CFGDOMSVR parameters for the Domino LDAP administration server, DOMLD7

<table>
<thead>
<tr>
<th>Parameter description</th>
<th>Parameter name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>SERVER</td>
<td>DomLD7</td>
</tr>
<tr>
<td>Option</td>
<td>OPTION</td>
<td>*FIRST</td>
</tr>
<tr>
<td>Data Directory</td>
<td>DTADIR</td>
<td>/Domino/DomLD7/Data</td>
</tr>
<tr>
<td>Organization</td>
<td>ORG</td>
<td>ITSO</td>
</tr>
<tr>
<td>Administrator:</td>
<td>ADM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ Last name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ First name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ Password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ Minimum password length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ Internet password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ Admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ ITSO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ 8 (this is the default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▶ password</td>
<td></td>
</tr>
<tr>
<td>Time zone</td>
<td>TIMEZONE</td>
<td>Enter your time zone. For example, CST.</td>
</tr>
<tr>
<td>Web browsers</td>
<td>WEB</td>
<td>*HTTP *IIOP</td>
</tr>
<tr>
<td>Directory services</td>
<td>DIRSRV</td>
<td>*LDAP</td>
</tr>
<tr>
<td>Connection services</td>
<td>CNNSRV</td>
<td>*NONE</td>
</tr>
<tr>
<td>Advanced services</td>
<td>ADVSRV</td>
<td>*PARTITION</td>
</tr>
</tbody>
</table>
4. When the Domino server has been successfully configured, type the Work with Domino Server (WRKDOMSVR) CL command and press Enter.

5. On the Work with Domino Servers display, enter an option 1 (Start server) next to the Domino LDAP administration server, DOMLD7, and press Enter to start the Domino server.

### 2.1.2 Registering the additional Domino server for Sametime

Any additional Domino servers in a Domino domain must be registered in the Domino Directory on the LDAP and Domino administration server before configuration. This registration process also creates the individual Domino server IDs.

Perform the following steps to register an additional Domino for Sametime:

1. Using the Domino Administration client, register an additional server. In our example we call our Sametime Domino server STLD7. This Sametime server uses Sametime Version 7.5 in our example. Make sure the same certifier ID is used for registering this server.

2. Note the location of the Domino server ID file for this Sametime Domino server because you will need to know this location when configuring the additional server.

### 2.1.3 Configuring the additional Domino server for Sametime

**Note 1:** The Sametime Domino server requires a local replica of the Domino Directory to be a Central directory and not a Configuration directory. Make sure the Domino Directory type parameter is selected as *CENTRAL when configuring the additional server.

**Note 2:** The Lotus Collaborative components use Java APIs to communicate with the Domino servers. These APIs use IIOP to connect and communicate, so you must enable the DIIOP task on the Domino servers.
Perform the following steps to configure the Domino server, STLD7. This Domino server provides users with Sametime support.

1. From a 5250 emulation session, type the Configure Domino Server (CFGDOMSVR) CL command and press F4 to prompt the command.

2. On the Configure Domino Server display, enter the Domino server name. For our example this is STLD7/ITSO. For the Option parameter, type *Add and press Enter.

3. Enter the remaining Domino server configuration parameters as shown in Table 2-2. Following is the completed CFGDOMSVR command.

   CFGDOMSVR SERVER(STLD7/ITSO) OPTION(*ADD) DTADIR('/DOMINO/STLD7/DATA')
   TIMEZONE(CST) NABSVR(DOMLD7 *NONE) ADDSVRID('/domino/domld7/stld7.id')
   WEB(*HTTP *IIOP) DIRSRV(*NONE) CNNSRV(*NONE) TCPOPT(*NOENCRYPT
   STLD7.RCHLAND.IBM.COM) SVRHSTNAME(STLD7.RCHLAND.IBM.COM) SBS(STLD7)
   TEXT('SAMETIME server using Domino LDAP')

Table 2-2 CFGDOMSVR parameters for the Sametime Domino server, STLD7

<table>
<thead>
<tr>
<th>Parameter description</th>
<th>Parameter name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>SERVER</td>
<td>STLD7/ITSO</td>
</tr>
<tr>
<td>Option</td>
<td>OPTION</td>
<td>*ADD</td>
</tr>
<tr>
<td>Data directory</td>
<td>DTADIR</td>
<td>/Domino/STLD7/Data</td>
</tr>
<tr>
<td>Time zone</td>
<td>TIMEZONE</td>
<td>Enter your time zone. For example, CST.</td>
</tr>
<tr>
<td>Get Domino directory from:</td>
<td>NABSVR</td>
<td>DOMLD7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*NONE (this is the default)</td>
</tr>
<tr>
<td>Additional server ID</td>
<td>ADDSVRID</td>
<td>Enter the server ID file location. For example: /Domino/DOMLD7/STLD7.id</td>
</tr>
<tr>
<td>Web browsers</td>
<td>WEB</td>
<td>*HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*IIOP</td>
</tr>
<tr>
<td>Directory services</td>
<td>DIRSRV</td>
<td>*NONE</td>
</tr>
<tr>
<td>Connection service</td>
<td>CNNSRV</td>
<td>*NONE</td>
</tr>
<tr>
<td>Text description</td>
<td>TEXT</td>
<td>Sametime server using Domino LDAP</td>
</tr>
<tr>
<td>TCP/IP port options:</td>
<td>TCPOPT</td>
<td>*NOENCRYPT (this is the default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify Domino server IP address or fully qualified host name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*YES (this is the default)</td>
</tr>
<tr>
<td>Server host name</td>
<td>SVRHSTNAME</td>
<td>stld7.rchland.ibm.com</td>
</tr>
<tr>
<td>Subsystem and object names</td>
<td>SBS</td>
<td>STLD7</td>
</tr>
</tbody>
</table>

4. When the Sametime Domino server has been successfully configured, type the Work with Domino Server (WRKDOMSVR) CL command and press Enter.

5. On the Work with Domino Servers display, enter an option 1 (Start server) next to the Sametime Domino server, STLD7, and press Enter to start the Domino server.
2.1.4 Registering Domino users

You may want to register Domino users that you can use later to test your environment. If you have a Domino Directory containing existing users, you can skip this section.

Register the users on the Domino LDAP administration server, DOMLD7, using the Domino Administrator client.

Note: Remember there is a difference between adding and registering users. Adding users in a Domino Directory creates a Person record in the Domino Directory for that user. Registering a user through the Domino Administrator client creates a Person document in the Domino Directory and also creates a mail file for the person. Only registered users have access to mail on Domino. Refer to the Lotus Domino Administrator Help database for more information about registering users.

2.1.5Preparing the Domino server for LDAP

Unlike other LDAP directory schemas, the default schema for the Domino Directory does not provide a unique ID attribute required for WebSphere Portal Express. You must have a unique identifier for each user in order to use a Domino server as the user repository for WebSphere Portal Express.

Note: Different sets of preparation tasks are required to prepare the Domino server to host the LDAP directory. Additional LDAP elements must be added to the Domino LDAP schema to enable anonymous access for the Domino LDAP directory, or you can bind users to LDAP by modifying settings in the CSEnvironment.properties file. The CSEnvironment.properties file is located in the i5/OS integrated file system directory of <wp_root>/PortalServer/shared/app/config. For example:
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/<profileName>/PortalServer/shared/app/config

It is considered a best practice to make a backup copy of the CSEnvironment.properties file before any changes are made. Refer to “Configuring WebSphere Portal Express to bind to Domino LDAP server” on page 246 for detailed instructions.

To configure LDAP users for anonymous access, you have to include the HTTP-HostName attribute to the Domino LDAP schema. Perform the following steps:

1. On the Domino LDAP server, open the LDAP Schema (schema.nsf) database. Make sure you have Manager access to the Domino LDAP Schema database.
2. In the Domino LDAP Schema database, select the All Schema Documents view.
3. Click New Document → Add Attribute Type.
4. In the LDAP Schema - Attribute Type document, Basic tab (see Figure 2-1 on page 28), enter the field values from Table 2-3. When you are finished entering the values, click Save & Close to save the new attribute as a draft.

Table 2-3 LDAP Schema - Attribute Type document field values

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP name</td>
<td>HTTP-HostName</td>
</tr>
<tr>
<td>OID</td>
<td>2.16.840.1.113678.2.2.2.2461</td>
</tr>
</tbody>
</table>
5. You must approve the draft attribute before it can become operational. Perform the following steps:
   a. Click Draft Documents → Draft Attribute Types on the left navigation pane.
   b. Select the HTTP-HostName draft document and click Approve → Approve Selected Drafts. See Figure 2-2.

6. Verify the HTTP-Hostname document now appears in the All Schema Documents → LDAP Attribute Types view.

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax name</td>
<td>Directory String</td>
</tr>
<tr>
<td>Single valued</td>
<td>Yes</td>
</tr>
<tr>
<td>Collective</td>
<td>No</td>
</tr>
<tr>
<td>No user modification</td>
<td>No</td>
</tr>
</tbody>
</table>

Figure 2-1  Adding the HTTP-Hostname LDAP attribute to the Domino LDAP schema

Figure 2-2  Approving the draft LDAP Schema attribute HTTP-Hostname
Creating a Configuration Settings document

You now need to create a Configuration Settings document that contains the default configuration settings used by all Domino servers. This Configuration document contains most of the LDAP settings used by the Domino servers. Perform the following steps:

1. From the Domino Administrator client, select File → Open Server and open the Domino LDAP server. For our example, this is DOMLD7.

2. Click the Configuration tab and select the Configurations view, then click the Add Configuration button as shown in Figure 2-3.

![Figure 2-3 Adding a Configuration document](image)

3. In Configuration Settings document, Basics tab, check the Yes box for the Use these settings as the default settings for all servers field. This displays an LDAP tab as shown in Figure 2-4.

   **Note:** You do not see the LDAP tab until you select the Use these settings as the default settings for all servers option.

![Figure 2-4 Configuration Settings document, Basics tab](image)
4. Click the **LDAP** tab and page down to the Allow LDAP users write access field, click **Yes** (see Figure 2-5). This enables authenticated LDAP users to add, delete, or modify entries in the Domino Directory this Domain configuration resides in.

Click **Yes** for the Automatically Full Text Index Domino Directory field to create a full text index for the Domino Directory (names.nsf) to improve LDAP search performance. An LDAP search without a full text index is a linear search.

**Note:** To enable authenticated users to add, delete, or modify entries in the Domino Directory, LDAP users must have Editor access with the appropriate roles (usermodifier, usercreator) in the ACL.

Click **Save & Close**.

---

**Editing the LDAP schema settings**

Perform the following steps to edit the Domino LDAP schema settings:

1. From the Domino Administrator client, open the Domino Directory (names.nsf) on the Domino LDAP server. For our example, this is DOMLD7.

2. Click the **Configuration** tab and select the **Configurations** view, then click the **Edit Configuration** button to edit the All Servers document. See Figure 2-6.
3. Click the **LDAP** tab to display the LDAP configuration settings. Click the **Select Attribute Types** button. See Figure 2-7.

![Figure 2-7 Default Configuration Settings document for all servers](image)

4. On the LDAP Attribute Type Selection window, Object Classes field, enter an asterisk (*) and click **Display Attributes**. See Figure 2-8.

![Figure 2-8 Attribute Type Selection for Anonymous LDAP Queries](image)
5. From the Selectable Attribute Types list displayed, select the following attributes and then click the **Add>>** button:

- AltFullName
- dominoCertificate
- givenName
- HTTP-HostName
- Location
- mail
- mailaddress
- MailDomain
- MailFile
- mailserver
- member
- NetAddresses
- publickey
- Sametime
- sn
- uid
- userCertificate

6. Click **OK** to close the LDAP Attribute Type Selection window.

7. Click **Save & Close** on the Configuration Settings document.

8. From the DOMLD7 Domino server console, type the following command to reload the LDAP schema:

   `tell ldap reloadschema`

---

### 2.1.6 Configuring the Sametime server

In this section Sametime is added to the existing Domino server created in 2.1.3, "Configuring the additional Domino server for Sametime" on page 25. We also perform verification to ensure the Sametime server is working correctly.

Note: For more information about installing and configuring Sametime for i5/OS, refer to the *Installing and Managing Sametime 7.5 for i5/OS* document:

[http://www-12.lotus.com/ldd/doc/uafiles.nsf/70817c90542892178525695b0051105c/1a62f6eb0a16c852571ce006f2b91/$FILE/stinstall.pdf](http://www-12.lotus.com/ldd/doc/uafiles.nsf/70817c90542892178525695b0051105c/1a62f6eb0a16c852571ce006f2b91/$FILE/stinstall.pdf)

For the Domino server to start the Sametime services, it is necessary to add the Sametime server to a Domino server. You can do this by using the Add Sametime to Domino (ADDLSTDOM) CL command. To add Sametime to a Domino server, you must stop the Domino server before you add Sametime. You must also make sure that your Domino server is properly configured for adding Sametime.

This section explains how to add Sametime to a Domino server by using the Add Sametime to Domino (ADDLSTDOM) CL command. Your i5/OS user profile must have *ALLOBJ, *JOBCTL, and *IOSYSCFG special authorities in order to add Sametime to a Domino server. It is also important to know that for Sametime on an i5/OS Domino server, the Sametime server administrator defaults to the Domino server administrator. This is specified during the Domino server configuration. To be more specific, during the process of adding the Sametime services to a Domino for i5/OS server, the Domino server administrator is taken from the Domino server document and used as the Sametime server administrator.
Perform the following steps to add Sametime to the Domino server:

1. Stop the Domino server designated for Sametime. In our example, this is STLD7.

2. From a 5250 emulation session, enter the Add Sametime to Domino (ADDLSTDOM) CL command and press F4 to prompt the command.

3. On the Add Sametime to Domino (ADDLSTDOM) display, enter the Domino server name. For our example, this is STLD7. Press F10 to display additional parameter fields.

4. On the Add Sametime to Domino window (Figure 2-9), enter the values from Table 2-4. Leave all other values as default. Press Enter.

**Note:** The Sametime server binds to *localhost* on the ports specified for Event server port and Token server port. You must change these port settings for any additional Sametime server configurations on the same i5/OS partition. These port settings should be unique across all Sametime servers configured on the same i5/OS logical partition.

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino server name</td>
<td>Specify the name of the Domino server to add Sametime</td>
</tr>
<tr>
<td>Directory type</td>
<td>*LDAP</td>
</tr>
<tr>
<td>LDAP server name</td>
<td>Specify the fully qualified host name of LDAP server</td>
</tr>
<tr>
<td>LDAP server port</td>
<td>389</td>
</tr>
</tbody>
</table>

**Table 2-4 Configuration values for adding Sametime to a Domino server**

Add Sametime to Domino (ADDLSTDOM)

Type choices, press Enter.

Domino server name ............ > STLD7

Directory type ............. > *LDAP  *DOMINO, *LDAP
LDAP server:
  Name ................. > DOMLD7.RCHLAND.IBM.COM
  Port .............. 389  1-65535
  HTTP tunneling ......... *NO  *YES, *NO
  Event server port ....... 9092  1-65535
  Token server port ...... 9094  1-65535
  Slide conversion server .. *NONE

Bottom

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
5. Wait for the configuration process to finish; it may take several minutes. When the process has finished, your window will look similar to the one shown in Figure 2-10. Press Enter to end the terminal session.

![Switching to the server identity...](image)

<table>
<thead>
<tr>
<th>Switching to the server identity...</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
</tr>
<tr>
<td>Setting up authentication system...</td>
</tr>
<tr>
<td>30%</td>
</tr>
<tr>
<td>Setup of the authentication system completed.</td>
</tr>
<tr>
<td>55%</td>
</tr>
<tr>
<td>Sametime Server setup completed successfully.</td>
</tr>
<tr>
<td>100%</td>
</tr>
<tr>
<td>Press ENTER to end terminal session.</td>
</tr>
</tbody>
</table>

Figure 2-10 Status window for adding Sametime to a Domino server

6. Start the Sametime server.

**Note:** The Work with Domino Server command (WRKDOMSVR) window status displays the status of the Domino server and not Sametime services. After the Domino server is started, the status changes to STARTED, but it then takes additional time to completely load all services on that Domino server, including the Sametime services.

To verify that all the Sametime services have started, look for a line containing the following text by displaying the Domino server console:

Sametime: All services started successfully.

This indicates that all the Sametime services have started without any errors.

**Verifying the Sametime server**

Now that we have started the Sametime server successfully, we can verify the configuration and settings by logging on to the Sametime server. In this section we verify the Sametime configuration by opening the Sametime server home page and logging on to the Sametime server. Perform the following steps:

1. From a Web browser, open the Sametime home page. Make sure to use the fully qualified host name of the Sametime server.

   http://<fully_qualified_Sametime_Domino_server_host_name>/stcenter.nsf
For our example, we use `stld7.rchland.ibm.com`. See Figure 2-11.

**Note:** Our example uses port 80 for all the HTTP servers in this environment. This is also true for the LDAP server that uses port 389, which is the default port.

*Figure 2-11  Sametime server home page*
2. On the Sametime server home page, click **Log in to IBM Lotus Sametime**. The
Sametime server uses Domino LDAP to authenticate user logons. This verifies that LDAP
authentication is correctly configured by successfully logging on to the Sametime server.
See Figure 2-12.

![Figure 2-12  Logging on to the Sametime server](image)

2.2 Configuring the Domino servers for single sign-on

Beginning with Domino Release 5.0.5, Web users can log on once to a Domino server and
then access any other Domino or WebSphere servers in the same DNS domain that are
enabled for single sign-on (SSO) without having to log on again. In addition, SSO works
across multiple WebSphere application servers and multiple independent Domino domains
as long as they are all in the same Internet domain.

**Note:** See the Lotus Domino 7 Administrator Help database for more information about the
topic of “Enabling single sign-on and basic authentication.”

Selecting the authentication option of “multiserver” authentication in the Domino server
Directory along with the Web SSO configuration document enables session-based
authentication. The Web SSO Configuration document that must be replicated to all Domino
servers participating in the SSO domain is encrypted for participating servers and contains a
shared secret key used by the servers for authenticating user credentials.

Web SSO is made possible by the use of what is called an **LtpaToken**, which is used by the
Web browser. Users’ Web browsers must have cookies enabled, because the authentication
token that is generated by the server is transported to the Web browser in a cookie.
WebSphere Application Server and WebSphere Portal Express support the use of LtpaToken,
and therefore it is possible to achieve SSO between Domino and WebSphere. For more
information see “Single sign-on and LTPA concepts” on page 14.

You can also enable SSO across multiple Domino domains. See the topic of “Setting up the
Web SSO Configuration document for more than one Domino domain” in the Domino 7
Administration Help database.
2.2.1 Creating the SSO key

An SSO-enabled server creates SSO cookies for users, which allows them to log on to the server and then access other participating servers without having to log on again.

**Note:** The Sametime server creates a Web SSO Configuration document automatically. One approach is to replicate the names.nsf file between the Domino and Sametime servers and then modify the existing Web SSO Configuration document created. You access the Web SSO Configuration document from the Domino Directory by clicking the Configuration tab and selecting Web → Web Server Configuration.

Perform following steps to create an SSO key:

1. Using the Domino Administrator client, open the Domino LDAP administration server. For our example, this is the DOMLD7 Domino server.
2. Click the Configuration tab and select the Current Server Document view.
3. Click Create Web → SSO Configuration, as shown in Figure 2-13.

![Figure 2-13 Creating a Web SSO Configuration document](image)
4. In the Web SSO Configuration document, click the **Keys** button and select **Create Domino SSO Key** as shown in Figure 2-14.

![Figure 2-14 Web SSO Configuration document](image)

5. Enter the DNS Domain of the Domino servers that will have access to the LtpaToken. For our example, we used `rchland.ibm.com`. Add the Domino servers that will participate to the Domino Server Names field. Click **Save & Close**. See Figure 2-15.

![Figure 2-15 Completed Web SSO Configuration document](image)

**Checklist for enabling SSO**

The SSO feature makes logging in and using multiple servers in a mixed environment easier for users. Use the following list to configure your Domino environment to ensure that your SSO configuration is successful:

- It is important that all servers participating in an SSO group use the same mechanism for configuring Internet access. Either they must all use Internet Site documents, or they must all have Internet access configured in the Server document.

- The DNS domain that applies to the participating SSO servers is specified in the Web SSO Configuration document. URLs issued to servers configured for SSO must specify the full DNS server name, not the host name or IP address. For Web browsers to be able to send cookies to a group of servers, the DNS domain is included in the cookie (as
specified by the configuration), and the DNS domain in the cookie must match the server URL. This is why cookies cannot be used across TCP/IP domains.

- Clustered servers must have the full DNS server name in the host name field of the Web Site or Server document. This enables the Internet Cluster Manager (ICM) to redirect to cluster members using SSO. If the DNS server host name is not there, ICM redirects URLs to clustered Web servers with only the TCP/IP host name, by default, and cannot send the cookie because the DNS domain is not included in the URL.

- If you enable Internet Sites in the Server document, any existing SSO configuration is automatically disabled.

- WebSphere and Domino do not have to be configured for the same LDAP directory. However, if WebSphere and Domino do not share the same directory, you likely will have to plan for and address a multi-identity problem.

- WebSphere configurations support two different formats of SSO LTPA cookies. One cookie has a name “LtpaToken”, and the other cookie format is named “LtpaToken2”. Domino SSO supports the LtpaToken cookie only; therefore, WebSphere must be configured to issue the correct format cookie in order for SSO to work between WebSphere and Domino.

### 2.2.2 Updating Domino server documents for SSO

To enable Domino servers to use the SSO token created, perform the following steps:

1. On the Domino Administrator client, access the Domino LDAP administration server. For our example, this is DOMLD7. Click the **Configuration** tab, select the **Current Server Document** view, and click **Edit Server**.

2. In the Domino Server document, click the **Internet Protocols → Domino Web Engine** tabs. Select the Session Authentication field keyword list and select **Multiple Servers (SSO)** from the drop-down menu as shown in Figure 2-16.

   A new field called Web SSO Configuration is now available (see Figure 2-16). Select the Web SSO Configuration field keyword list and select the LtpaToken name created in the previous steps. Click **Save and Close**.

![Figure 2-16 Domino Server document, Internet Protocols → Domino Web Engine tabs](image-url)
3. Select the Sametime Server document (for our example, this is STLD7) and repeat steps 1 and 2.

4. Replicate the changes in the Domino Directory LDAP administration server (for our example, this is DOMLD7) to the additional Domino server (for our example, this is STLD7).

5. Stop and restart all the Domino servers or execute the commands TELL HTTP QUIT and LOAD HTTP from the Domino server console of the participating SSO servers. You should see the following message (see Figure 2-17):

HTTP Server: Using Web Configuration View

```
> tell http quit
04/09/2007 16:15:20 HTTP Server: Shutdown

> load http
04/09/2007 16:15:36 HTTP Server: Java Virtual Machine loaded
04/09/2007 16:15:44 HTTP Server: Started
```

Figure 2-17  Domino server console, ending and restarting the Domino HTTP server

### 2.2.3 Verifying SSO for Domino and Sametime servers

At this point, SSO has been configured for both the Domino LDAP administration server and the Sametime server. This enables a user to log on to the Domino LDAP administration server and then access the Sametime server, and vice versa, without having to log on again. In this section we verify SSO across both Domino servers by performing the following steps:

**Important:** SSO works within the same Web browser session instance. If a new Web browser instance is launched, SSO does not work.

1. Open a Web browser and connect to the Domino LDAP administration server home page:

   http://<fully_qualified_DominoServer_hostName>/names.nsf
2. From the Domino LDAP administration server home page, enter the user name and password of a user who exists in the Domino LDAP directory. Click Log in as shown in Figure 2-18.

![Figure 2-18 Logging on to the Domino server home page](image)

3. As shown in Figure 2-19, you should successfully log on to the Domino server. This verifies the user exists in the Domino LDAP directory.

![Figure 2-19 User name exists in the Domino LDAP directory](image)

4. From the same Web browser session, connect to the Sametime home page on the Sametime server by typing the following URL into your Web browser. You should not be prompted to sign in again. For our example, we use the following URL:

5. The Sametime server should show the same user name logged on at the top right of the window. See Figure 2-20.

![Figure 2-20](image)

Figure 2-20 Verifying that SSO is working between the Domino servers

6. If the user name appears as logged on, SSO is working correctly. If not, you have a problem with SSO, which must be corrected before proceeding to the next section.

2.3 Configuring collaboration in WebSphere Portal Express V6

In this section we configure a WebSphere Portal Express profile and enable collaboration within that profile.

**Note:** Refer to the IBM Redpaper *Installing and Configuring WebSphere Portal Express V6 on i5/OS*, REDP-4303 for details on configuring a WebSphere Portal Express V6 profile.

We assume you have verified that all the Domino servers are configured to use a common Domino LDAP directory and that multisession SSO has been successfully configured across all the Domino servers.

A number of portlets can be installed when you configure a WebSphere Portal Express V6 profile. Some of these portlets are automatically installed, and others are optionally installable. For details see 1.1, “Collaborative portlets in WebSphere Portal Express V6” on page 2.

A portal is a Web site that provides users with a single point of access to Web-based resources by aggregating those resources in one place and by requiring that users log on only to the portal itself and not to each portlet they use.
2.3.1 Configuring a WebSphere Portal Express V6 profile

This section describes the steps required to create a new WebSphere Portal Express V6 profile. Before configuring the WebSphere Portal Express V6 profile, you must verify the i5/OS HTTP ADMIN is active. Perform the following steps:

1. From an i5/OS command line, enter the following Work with Active Jobs (WRKACTJOB) CL command:

   \texttt{WRKACTJOB SBS(QHTTPSVR)}

2. On the Work with Active Jobs display, the HTTP ADMIN server instance should be running as shown in Figure 2-21.

   If the i5/OS HTTP ADMIN server instance is not running, enter the following Start TCP/IP Server (STRTCPSVR) CL command to start the HTTP instance:

   \texttt{STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)}

![Figure 2-21 Work with Active Jobs display showing the QHTTPSVR subsystem](image)

Perform the following steps to create a WebSphere Portal Express profile on the i5/OS using the Create WebSphere Portal Express wizard:

1. Launch a Web browser and go to the HTTPAdmin or IBM Web Administration for i5/OS Web site. For our example, \texttt{RCHAS10.RCHLAND.IBM.COM} is the fully qualified host name of our i5/OS environment.

   \texttt{http://rchas10.rchland.ibm.com:2001/HTTPAdmin}

   ![Tip: HTTPAdmin can also be set to debug mode for verbose logging during the configuration of a WebSphere Portal Express instance. As you run through the steps in the wizard, the verbose output is placed in the i5/OS integrated file system directory of /QIBM/UserData/HTTPA/admin/logs/HTTPAdmin.log.](image)

   \texttt{http://<System i fully-qualified-hostname>:2001/HTTPAdmin?debug=}

2. On the Connect to i5/OS window, enter your i5/OS user profile and password to access the system. Click OK.
3. On the IBM Web Administration i5/OS window, Click the **Create WebSphere Portal** link located in the left navigation bar under the Setup tab.

4. On the Create WebSphere Portal page, review all of the information presented in the window and click **Next**.

**Note:** If you have not met all the prerequisites, error messages are displayed at the bottom of the window when you click **Next**. For example, you can check which Program Temporary Fixes (PTFs) are missing by clicking the link in the error message or continue by clicking **Next**.

5. On the Select WebSphere Portal Version page, select the version of WebSphere Portal server to create. For our example we select **IBM WebSphere Portal Express V6.0.0.1** and click **Next**.

6. On the Specify name for server - Step 1 of 14 page, enter a unique name and description for your WebSphere Portal Express profile. For our example, we entered **WPX6LD7** for the server name and a server description of **WebSphere Portal Express server running Domino LDAP**. Click **Next**.

7. On the next several pages, you must complete the necessary steps to create the WebSphere Portal Express instance. For our example WPX6LD7 instance, we entered the following values:
   - Specify Internal Ports Used by the Application Server - Step 2 of 14.
   - Create a new HTTP server (powered by Apache) - Step 3 of 14. Your HTTP server can listen for requests on a specific IP address or on all IP addresses of the system.
   - Create DB2® Database for Portal - Step 4 of 14. WebSphere Portal Express V6 requires several databases to store customized portal information, settings, Web pages, and configuration information. DB2 database schemas are created and used by this WebSphere Portal environment. For example, we specify the user to own the databases as WPX6LD7 (same as the portal profile name) and select the option to name the databases based on the server name for the specify database naming method.
   - Configure Proxy Information for Content Access Service - Step 5 of 14.
   - Deploy Default Portlets - Step 6 of 14.

**Note:** We recommend a user profile with SECOFR authority to perform the WebSphere Portal Express configuration. The user profile must have *ALLOBJ, *JOBCTL, and *IOSYS CFG special authorities to be able to configure a WebSphere Portal Express profile.

**Note:** If you have not met all the prerequisites, error messages are displayed at the bottom of the window when you click **Next**. For example, you can check which Program Temporary Fixes (PTFs) are missing by clicking the link in the error message or continue by clicking **Next**.
Configure Lotus Collaborative Components - Step 7 of 14. Lotus Collaborative Components provide the building blocks for integrating the functionality of Domino, Sametime, and QuickPlace into portals and portlets. Choose the collaborative components to configure as shown in Figure 2-22 and provide the appropriate name field values when prompted.

![Figure 2-22 Selecting the collaborative components to configure](image)

8. On the Secure Application Server and WebSphere Portal with LDAP - Step 8 of 14 page, specify the security options for the WebSphere Portal environment. For our example, we use the Domino LDAP administration server DOMLD7 as shown in Figure 2-23. Click Next.

![Figure 2-23 Specifying security options for the WebSphere Portal Express environment](image)
9. On the LDAP Authentication - Step 9 of 14 page, specify the access method to the LDAP directory. Enter the LDAP Administrator’s distinguished name and password. In our example the LDAP administrator DN is cn=ITSO Admin, and the LDAP administrator password is itso4all. Click **Next**. See Figure 2-24.

**Note:** In this example, we use a Domino LDAP server, so we use the Domino system administrator’s name in the LDAP administrator DN field. If you select the option **Allow read-only access to the LDAP Directory** in Figure 2-24, you must have previously created the WebSphere Portal Express administration user and group containers in the Domino LDAP as discussed in 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9.

10. Perform the following steps to manually create the WebSphere Portal Express administration user and group containers in the Domino LDAP if you selected **Allow read-only access to the LDAP Directory** in Figure 2-24. Otherwise, skip to the next step.

   a. Ensure the User name (cn) and Short name/UserID (uid) fields match for the user that is specified as the WebSphere administrator. See Table 2-5.

   
   **Table 2-5  LDAP Schema mapping to Domino Person document**

<table>
<thead>
<tr>
<th>LDAP attribute</th>
<th>Domino fields in Person document</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>User name</td>
</tr>
<tr>
<td>uid</td>
<td>Short name/UserID</td>
</tr>
</tbody>
</table>

   b. From the Domino Administrator client, open the Domino Directory and select the **People** view and click **Add Person**.
c. On the Basics tab of the Person document, specify the values shown in Table 2-6 where wpsadmin represents the administrator for the WebSphere Portal Express profile. See Figure 2-25.

Click **Save & Close**.

<table>
<thead>
<tr>
<th>Domino Person document field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last name</td>
<td>wpsadmin</td>
</tr>
<tr>
<td>User name</td>
<td>wpsadmin/Org, wpsadmin</td>
</tr>
<tr>
<td>Shortname/UserID</td>
<td>wpsadmin</td>
</tr>
<tr>
<td>Internet address</td>
<td>wpsadmin@&lt;domainName.com&gt;</td>
</tr>
<tr>
<td>Internet password</td>
<td>Specify password of choice</td>
</tr>
</tbody>
</table>

**Table 2-6  wpsadmin Person document values**

![Figure 2-25  Person document for wpsadmin](image)

**d. Select the Groups view and click Add Group.**
e. On the Basics tab of the Group document, specify the values from Table 2-7, where wpsadmin represents WebSphere Portal Express administrator and wpsadmins represents the administrator group. See Figure 2-26.

Click **Save & Close**.

<table>
<thead>
<tr>
<th>Domino Group document field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>wpsadmins</td>
</tr>
<tr>
<td>Group type</td>
<td>Multi-purpose</td>
</tr>
<tr>
<td>Members</td>
<td>wpsadmin/Org</td>
</tr>
</tbody>
</table>

**Table 2-7 Value used for wpsadmins Group document**

![Group document for wpsadmins](image)

**Important**: Repeat these steps and create the following groups: wpsContentAdministrators, wpsDocReviewer, and wcmadmins.

11. Continue with completing the LDAP Configuration Parameters - Step 10 of 14. Enter the appropriate distinguished names for your environment. For our example, we used the following values:

- Information describing user entries section:
  - Parent DN: O=ITSO
    
    This is the container where the WebSphere Portal Express administrator user wpsadmin and all new WebSphere Portal Express users will reside. If no wpsadmin Portal administrator exists in this LDAP server, the wizard creates a new wpsadmin entry in the user parent DN container that you specify. The users already in this user parent DN container now have access to the WebSphere Portal Express.

  - Object class: dominoPerson
    
    The List of Object classes is retrieved from the LDAP server schema. The list contains the object classes in the LDAP server’s schema that directly or indirectly inherit from the person object class (including the person object class itself). When using Domino LDAP, the dominoPerson and eDominoPerson are available.
- Naming attribute: cn
  The list of naming attributes is retrieved from the LDAP server schema. The list contains all of the attributes that are a part of the chosen user Object class.

- Information describing the administrative group entry section:
  - Parent DN: O=ITSO
    Specifying the group parent DN for the LDAP server. This is the container in which the WebSphere Portal Express administrator group (wpsadmins) must exist. If no wpsadmins Portal administrator group exists in this LDAP server, the wizard creates a new wpsadmins entry in the group parent DN container that you specify. The wizard makes the wpsadmin administrator a member of that group.
  - Object class: dominoGroup
    The list of object classes is retrieved from the LDAP server schema. The list contains the object classes in the LDAP server’s schema that directly or indirectly contain the member, uniqueMember, or memberURL attribute.
  - Naming attributes: cn
    The list of naming attributes is retrieved from the LDAP server schema. The list contains all of the attributes that are a part of the chosen group Object class.
  - Member attributes: member
    The member attribute is retrieved from the LDAP server schema and is based on the group Object class. This value cannot be edited.

When you have filled in all the values, click Next. Figure 2-27 illustrates the Domino LDAP configuration parameters.

![Figure 2-27 LDAP distinguished name entries for Domino LDAP](image-url)
12. **LDAP Administrative Group and Administrative User - Step 11 of 14 (Figure 2-28)**, requires an administrative group and user entry in the LDAP directory. If the group and user entries do not already exist, the wizard creates them. If the group and user entries already exist, the wizard validates them. The wizard also ensures the administrator user is added to the administrative groups. Specify and confirm the password for the portal administrator ID. Click **Next**.

**Note:** The value specified for the Administrative group name and the Administrator name are automatically created in the LDAP directory.

![Create WebSphere Portal Express, V6.0](image)

**Figure 2-28  LDAP Administrative Group and Administrative User**
13. On the Web Server Single Signon (SSO) Configuration Parameters - Step 12 of 14 page, we want to use SSO with Domino LDAP and Sametime so we click **Include other Web servers in your SSO environment** and specify the SSO Domain name. See Figure 2-29.

![Figure 2-29 Specifying Web SSO configuration parameters](image)

14. On the Configure Lightweight Third Party Authentication (LTPA) for Web Server Single Signon (SSO) Environment page, specify and confirm the LTPA password as shown in Figure 2-30.

![Figure 2-30 Specifying the LTPA password](image)
15. On the Summary - Step 14 of 14 page (Figure 2-31), review your WebSphere Portal Express profile configuration. Click **Finish**. The configuration can take some time to complete. You can monitor the progress from the WebSphere Portal Express server introduction page that is displayed after the Finish button has been clicked.

**Note:** The printable summary does not print out passwords that were specified, so remember to document them according to your system configuration.

![Figure 2-31 Summary pane](image)

16. Figure 2-32 shows the WebSphere Portal Express profile WPX6LD7 being created.

![Figure 2-32 WebSphere Portal Express profile configuration progress](image)
17. A completion message is shown after the WebSphere Portal Express profile is created (Figure 2-33). Notice the WebSphere Portal Express profile has automatically been started as seen in the top left side of the view pane. The status indicator has changed from Creating to Running.

Tip: Notice a link to the creation log files displayed in the left bottom navigation pane.

2.3.2  Updating the access control list (ACL) of the Domino Directory

The administrator group, wpsadmins, should be added manually to the Domino Directory ACL and assigned the proper permissions and roles. This group was created in the LDAP directory by the WebSphere Portal Express configuration wizard. The following steps should be performed to add the administrator group to the Domino Directory on the Domino LDAP administration server.

1. From the Domino Administrator client, open the Domino Directory (names.nsf) on the Domino LDAP administration server.

2. Click the pull-down menu options of File → Database → Access Control to open the Access Control List dialog box of the Domino Directory.
3. On the Access Control List, Basics tab, add the WebSphere Portal Express administrators group, wpsadmins, with Editor access as shown in Figure 2-34. Click OK to save these changes to the ACL of the Domino Directory.

![Access Control List](image)

**Figure 2-34  Domino Directory database ACL**

### 2.3.3 Verifying WebSphere Portal Express V6 integrated with Domino LDAP

Now that the WebSphere Portal Express profile has been created and the ACL of the Domino Directory LDAP server has been updated, we can verify the WebSphere Portal Express profile integration with LDAP by logging into the portal with any user ID and password listed in the Domino Directory.

**Tip:** Modifying the Person document user name field to add `cn=Short name/UserID`, allows logging by ShortName.
Perform the following steps to verify that your Domino LDAP server for WebSphere Portal Express has been properly configured.

1. To access the portal, in our example portal instance WPX6LD7, we can either click the URL as shown in the completion window in Figure 2-33 on page 53 or enter the following URL from a Web browser:
   
   http://<fully_qualified_hostname>/<default_url_path>

2. On the WebSphere Portal Express logon page, enter a user ID and password from the Domino LDAP Directory and click Log in as shown in Figure 2-35.

Figure 2-35  Logging on to WebSphere Portal Express
3. The default WebSphere Portal Express V6 main welcome page is displayed as shown in Figure 2-36. If you do not see this page, check and make sure access to the Internet from your Web browser is possible. Click Log out.

![WebSphere Portal Express V6 default welcome page](image)

**Figure 2-36** WebSphere Portal Express V6 default welcome page

### 2.4 Enabling SSO between WebSphere and Domino

In this section we configure single sign-on (SSO) between the WebSphere Portal Express Server profile and the Domino LDAP Administration and Sametime servers.

**Note:** You can enable SSO only if you configured an LDAP server in the WebSphere Portal Express configuration process.

Two steps are required to configure SSO between these servers:

- Export the WebSphere LTPA key
- Import the LTPA key into Domino

To enable SSO, you must share the same LTPA key between all servers configured in the environment for this purpose. If you specified a domain for SSO and the LTPA password when configuring the WebSphere Portal Express profile, the LTPA key is already generated. You then must export the LTPA key from WebSphere and import it into Domino.
2.4.1 Exporting the WebSphere LTPA key

WebSphere cannot use Domino LTPA tokens. To include Domino and WebSphere in the same LTPA group, you must export the LTPA token from WebSphere and import it into Domino. You must retrieve the WebSphere LTPA key from the WebSphere Portal Express server so you can use the key on the Domino servers. To export the LTPA key from the WebSphere Portal Express server, perform the following steps:

1. Start the IBM Web Administration for i5/OS server from a Web browser. For example:
   

2. Log on using your i5/OS user ID and password. At minimum, your user ID must have *
   ALLOBJ, *JOBCTL, and *IOSYSCFG special authorities.

3. Click the Manage → Application Servers tabs, select your WebSphere Portal Express server, and click Launch Administrative Console as shown in Figure 2-37.

Figure 2-37  Launching the WebSphere Administrative Console
4. If the Security Alert window is displayed (Figure 2-38), click **Yes**.

![Security alert](image)

*Figure 2-38 Security alert*

5. Sign on using the WebSphere Portal Express Administrator user ID and password as shown in Figure 2-39. In our example, we used `wpsadmin`, which we created in the Domino LDAP Directory. Click **Log in**.

![Logging on to the WebSphere Application Server Administrative Console](image)

*Figure 2-39 Logging on to the WebSphere Application Server Administrative Console*

6. If the WebSphere Portal Express instance is configured for multiple realms, perform the following steps. Otherwise go to next step.
   a. In the WebSphere Administrative Console, select **Security** → **Global Security** → **User Registry** → **Custom** → **Custom Properties**.
   b. Click **New** to add the `userRegistryRealm` key with the value `<ldapserverhostname:port>`.
   c. Save the changes.
7. Click **Security → Global security.** Under Authentication, click **Authentication mechanisms → LTPA** as shown in Figure 2-40.

8. Under Additional properties (right view pane), click **Single signon (SSO).**
9. On the Global security page (Figure 2-41), ensure that the **Enabled** check box is selected. Verify **Web inbound security attribute propagation** is not checked.

In the Domain name field, make sure the domain name for SSO is set properly. The Domain name field should include all servers that will be used for SSO. If this field is blank or set incorrectly, SSO can fail. In our example, the domain name is `rchland.ibm.com`.

If the fields are correct, you can click **Cancel**. Should you make any changes, click **Apply** and save the settings.

![Figure 2-41   Verifying the Domain name field for SSO](image)
10. Click **LTPA** to return to the Configuration tab. If the password field is blank, enter the Password and Confirm Password fields. Enter a path and file name in the Key file name field. Click **Apply** then **Save** to save the changes on the master configuration. See Figure 2-42.

Click **Export Keys**.

**Note:** The path is in the i5/OS integrated file system on which WebSphere Portal Express server resides. If you omit the path and enter only a file name, the key file is generated in the was_profile_root - for our example, this is:

/QIBM/UserData/WebSphere/AppServer/V6/Base/profile/wpx6ld7

![Figure 2-42 Exporting the WebSphere LTPA key](image)

11. Log out of the WebSphere Administrative Console.

For our example, the key file just created was saved to the i5/OS integrated file system directory of /QIBM/UserData/WebSphere/AppServer/V6/Base/profile/wpx6ld7.

12. Copy the key file to a location that is accessible to the Domino server.

**Note:** We FTPed the wpx6ld7.key file in binary format to a directory called c:\Stuff\TAE on the Domino server.
2.4.2 Importing the LTPA key into Domino

WebSphere Portal Express and the underlying WebSphere Application Server use the Lightweight Third Part Authentication (LTPA) mechanism for realizing SSO with other applications that reside in another WebSphere Application Server or in Domino. With LTPA, a cookie is sent to the client after successful authentication. During later requests, the client sends this cookie to the servers in the same SSO domain to authenticate itself. This cookie contains the distinguished name (DN) of the user as well as the Security Realm encrypted with cryptographic keys. The Security Realm is an alias for the user registry that is used (for example, with LDAP it is ldaphostname:port) This Security Realm is not related to the WMM realm that is required for Virtual Portal.

The cryptographic keys used to encrypt and decrypt the LTPA Token on the WebSphere Application Server and Domino server must be the same. You accomplish this by exporting and importing the keys.

In Domino, multi-server should have been enabled for single sign-on (SSO) authentication. So a Web SSO Configuration document should exist. However, you must modify the document for use with WebSphere Portal Express. After exporting the LPTA key from the WebSphere Application Server, you must import the LTPA key into Domino and make the appropriate configuration changes. Perform the following steps:

1. Open the Domino Administrator client and click the Configuration tab.
2. In the left navigation pane, expand Web → Web Server Configurations and scroll up to locate the Domino LDAP administration server Web SSO Configurations document. Select Web SSO Configuration for LtpaToken and click Edit Document. See Figure 2-43.

![Figure 2-43 Selecting the Web SSO Configurations document](image-url)
3. From the drop-down menu of the **Keys** button, select **Import WebSphere LTPA Keys**. See Figure 2-44.

![Figure 2-44 Importing the WebSphere LTPA keys](image)

4. Click **OK** if you get an error message that states the SSO Configuration has already been initialized as shown in Figure 2-45.

![Figure 2-45 Web SSO Configuration already configured warning message](image)

5. On the Enter Import File Name window (see Figure 2-46), type the path and file name for the LTPA key file. For our example, this is `C:\Stuff\TAE\wpx6ld7.key`. Click **OK**.

![Figure 2-46 Specifying the path to the WebSphere LTPA key file](image)

6. Type the password for the LTPA key and click **OK**.
7. You should see a message indicating the import was successful. Click **OK**.
8. You should see the WebSphere Information section with the default value of WMMRealm in the LDAP Realm field as shown in Figure 2-47. Click **Save & Close**.

![Web SSO Configuration for: L1paToken](image)

**Figure 2-47** Domino Web SSO Configuration document after importing the LTPA keys

9. Because you have enabled multi-server single sign-on, update the Domino Server document. Verify the configuration for each Domino server by performing the following steps:

   a. Open the Domino Server document of the LDAP Domino administration server (DOMLD7 in our example).
   
   b. Click **Internet Protocols → Domino Web Engine** tabs.
   
   c. Next to Session authentication, **Multiple servers (SSO)** should be selected.
   
   d. Click **Save & Close**.
   
   e. Replicate any changes made to the other Domino servers for this configured environment.
   
   f. Restart each of the Domino servers.
2.4.3 Verifying SSO between Domino and WebSphere Portal Express

Verify SSO works between Domino, Sametime, and the WebSphere Portal Express server by performing the following steps:

1. Launch a Web browser and log on to the WebSphere Portal Express server. For this example, we logged on as ITSO Admin.

2. Change the Web browser URL location to the Sametime server. For our example:
   

   You should see ITSO Admin already logged on for Sametime as shown in Figure 2-48.

![Figure 2-48 Verifying SSO with Sametime](image)
3. Likewise, when you switch the Web browser URL to access the ITSO Admin user mail file on the Domino LDAP administration server, you should see ITSO Admin still logged on without having to type a user ID and password again. See Figure 2-49.

![Welcome page with user ITSO Admin already logged on](image_url)

**Figure 2-49  Welcome page with user ITSO Admin already logged on**

### 2.5 Configuring the deployed Lotus collaborative portlets

The next step is to modify the portal so that you can begin using the new collaborative portlets. A portal generally is a converging point that offers a single point of interaction with applications, content, and processes to provide a unified user experience.

First we provide a quick overview of the main portal concepts and components:

- **Page**: A page contains one or more portlets, such as stock, weather, and news. It also can display other contents on the page - for example, a logon form or an error message. If you have the authorization to edit, order, and delete pages, labels, and URLs, you can see and
use the Administration option when you select **Launch → Main menu** from the portal. See Figure 2-50.

![Figure 2-50  WebSphere Portal Express Administration panel](image)

- **Page layout**: Page layout defines the area of real estate for each content type within the page. The portlet displays the contents within that real estate. The portal administrator defines the page layout in most cases. The portal administrator can permit a user or group of users to update their contents within their real estate on the portal page.

- **Portlet**: A portlet is an application that displays contents inside the WebSphere Portal Express page.

- **Portlet application**: Portlet applications are a collection of related portlets and resources - for example, skins and themes, properties files, and classes. They need to communicate with each other or work independently from other portlets within the overall portal application system. These portlets and resources are packaged together and deployed on the portal application server.

- **Roles**: WebSphere Portal implements a complex framework for access control. WebSphere Portal permissions are roles based. A role is mapped to a set of permissions. A role can be assigned or mapped to individual users or groups of users.

- **Administrator**: An administrator is allowed to have unrestricted access on all portal resources, such as creating, configuring, and deleting resources. They are also allowed to change access control configuration for users or group of users.
2.5.1 Accessing Domino mail

A Domino mail database that is enabled for Domino Web Access enables you to view and work with documents from a Web browser interface. This section shows you what the portlet looks like for a Domino mail user. Log on to the portal as a Domino user. In our example, we logged on as ITSO Admin as shown in Figure 2-51 and Figure 2-52.

![Figure 2-51 Domino Web Access portlet for a Domino mail user](image1)

![Figure 2-52 Domino Web Access portlet for a Domino mail user's calendar](image2)
2.5.2 Online awareness

Domino integration provides awareness through several components:

- People Finder
- Person tag
- Directory Search

Wherever person links appear, users can click the link to display a menu of actions for collaborating (contacting and working) with the person named by the link. If you, as a portal administrator, have also configured a Sametime server to work with the portal, person links indicate whether a person is Active, Away, Offline, or in a Do Not Disturb state. People awareness in the form of online presence (names displayed as hyperlinks) is supported by Collaborative Services.

In some contexts, the Person menu is available. The Person menu is provided by the Person JSP tag. The Person tag provides contextual collaboration functionality related to a named person. It generates the HTML that renders both the specific set of actions to display on the Person menu and the online presence state to display for that person, taking into account the Domino and Extended Products servers that are installed and enabled in the portal environment.

Person menu

When portal users click the name of (or the icon for) a person, a menu appears that provides actions linking them to other portal users. The actions that are visible on the person menu depend on the following factors:

- Whether Domino and Extended Products, the Lotus Collaborative Services, or both, are configured to work with the portal.
- The online status (Active, Away, Do Not Disturb, Offline) of the person appears only if Sametime is enabled.

Actions can include:

- **Show Person Record**: Appears only if the People Finder portlet is on the current page. This action displays the person’s record in the organization directory, including (by default) business card information, contact information, current job, and background.
- **Send E-mail**: Opens a new message in the user’s preferred e-mail client.
- **Chat**: Appears only if Sametime is enabled. Action is not available if the person is offline or has set status to “Do not disturb me.”
- **Show in Organization View**: Appears in the People Finder portlet if a portal administrator has selected Include Organization View when configuring the portlet. This action opens the person’s organizational context. The Organization View shows how the person fits into the organizational hierarchy.
- **Add to Sametime List**: Appears only if Sametime is enabled. Action displays a window where you can add the person to your contact list, as a member of a new or existing personal group.

This chapter provides all the necessary steps for configuring a WebSphere Portal Express environment with collaboration functionality using the IBM Directory Server (IDS) for user authentication at the portal site. This environment is complex because of the deployment of multiple directories. Some collaboration components such as the Domino Web Access (DWA) portlet require the Domino Directory, even though the WebSphere Portal Express server is deployed using the IDS Lightweight Directory Access Protocol (LDAP) directory.

Typically, the Domino Directory contains information about each Domino user, while the corporate, non-Domino, IBM Directory Server LDAP directory contains a super-set of the Domino users. This corporate LDAP directory is used in this scenario for authentication on the portal site, so a user record for every user that accesses the WebSphere Portal Express server is required. In the case where an authenticated portal user accesses the collaboration portlets and wants to access their mail or calendar information, certain information must be reconciled between Domino (either the Domino Directory or Domino database ACL) and the IDS LDAP.

For this approach to work, the single sign-on (SSO) LTPA relationship must be established between the WebSphere Portal Express and Domino environments. For information about the concepts of SSO and LTPA, see “Single sign-on and LTPA concepts” on page 14.

IBM Directory Server for i5/OS is part of i5/OS. With i5/OS V5R4, this IBM Directory Server is equivalent to IBM Tivoli Directory Server V5.2 and provides a network directory that can be accessed by network clients using the LDAP protocol. The example shown in this chapter uses the IBM Directory Server for i5/OS as the IDS.
Table 3-1 summarizes the necessary steps in the order they have to be performed to configure your portal environment with IDS LDAP and collaboration functionality. The example shown in this chapter assumes you are implementing this environment from scratch, which means you do not have a directory server or a Domino environment already configured.

Table 3-1  Summary of steps for configuring a WebSphere Portal Express environment with IDS LDAP

<table>
<thead>
<tr>
<th>Main tasks</th>
<th>Optional tasks</th>
<th>Prerequisites</th>
<th>Comments</th>
</tr>
</thead>
</table>
| 3.1, “Preparing the IDS LDAP server” on page 74 | Manage entries of your IDS directory server using the IBM Tivoli Directory Server Web Administration Tool.  
See 3.6.3, “Using the IBM Tivoli Directory Server Web Administration Tool” on page 153. | 3.6.1, “Enabling the system application server instance” on page 149.  
3.6.2, “Configuring the IBM Tivoli Directory Server Web Administration Tool” on page 150. | All the necessary steps are described in 3.1.1, “Basic IDS LDAP configuration on i5/OS” on page 74.  
You can manage the entries of your IDS directory server at any time after the basic IDS LDAP configuration has been completed and WebSphere Application Server V6 is installed.  
If you are working with a new IDS, we recommend you manage directory entries after the WebSphere Portal Express configuration is complete. This is because the i5/OS Create WebSphere Portal wizard automatically creates the users and groups containers as well as the portal administration user. |
| 3.7.1, “Publishing SDD data to the directory server” on page 168. | 3.6.4, “Setting up templates and realms” on page 161.  
3.7.2, “Setting up SDD publishing” on page 169. | You can publishing SDD data to the directory server any time after the basic IDS LDAP configuration has been completed. |  |
| 3.8, “Managing LDAP entries with LDIF” on page 187. |  | You can manage LDAP entries with LDAP data interchange format (LDIF) any time after the basic IDS LDAP configuration has been completed. |  |
| 3.2, “Setting up the Domino environment” on page 77 | 3.2.3, “Registering Domino users” on page 85. | 3.2.2, “Registering a Domino server” on page 81. | First complete the steps in 3.2.1, “Configuring the primary Domino server” on page 77.  
Then complete the steps in 3.2.2, “Registering a Domino server” on page 81.  
You can complete this step at any time after the Domino server has been set up. |
| 3.2.4, “Configuring the Sametime server” on page 88 |  |  |  |

If you have already implemented Domino or Sametime, the information provided in this chapter can be used for reference. For example, you can refer to this chapter to configure SSO between Domino and WebSphere Portal Express.

If you have already implemented IBM Directory Server for i5/OS and users are already defined in the directory that you want to use for the portal authorization, you must take into consideration several issues before you can create a portal profile with the i5/OS Create WebSphere Portal wizard. At a minimum, you have to define a container that holds your user entries. Refer to 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9 for more information.

Section 3.7, “Using information stored in the System Distribution Directory for LDAP publishing” on page 166 describes the steps necessary for implementing the same scenario covered in this chapter but using an already published LDAP directory. The section “Configuring the WebSphere Portal Express server for the SDD scenario” on page 178, provides an example of how to use the i5/OS Create WebSphere Portal wizard to configure a portal profile with an existing IDS LDAP directory.

<table>
<thead>
<tr>
<th>Main tasks</th>
<th>Optional tasks</th>
<th>Prerequisites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3, “Configuring the WebSphere Portal Express server” on page 95</td>
<td></td>
<td>You must configure the IDS LDAP server, Domino server, and Sametime server before this step. See the steps listed previously.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3, “Configuring the WebSphere Portal Express server” on page 95</td>
<td>You can perform this step only after the portal profile is configured.</td>
<td></td>
</tr>
<tr>
<td>3.5, “Integrating Domino mail and calendar” on page 119</td>
<td>3.7, “Using information stored in the System Distribution Directory for LDAP publishing” on page 166.</td>
<td>Describes the entire scenario using the SDD publishing function and solution 2 for mail auto-detection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.7.3, “Example using SDD publishing” on page 173.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.9, “Adding additional portlets to a WebSphere Portal page” on page 191.</td>
<td>Describes how to add the Domino Web Access (DWA) portlet to the default collaboration page of the WebSphere Portal Express profile.</td>
<td></td>
</tr>
</tbody>
</table>
3.1 Preparing the IDS LDAP server

If you have no LDAP directory in place, the easiest way to implement an IDS LDAP directory for your WebSphere Portal Express environment is to configure the IBM Directory Server for i5/OS. IBM Directory Server for i5/OS is part of i5/OS and is automatically installed with i5/OS.

In addition, the Create WebSphere Portal wizard provided in IBM Web Administration for i5/OS automatically creates all the required prerequisite entries in the LDAP directory. See 1.3, “LDAP servers” on page 5 for more information.

After completing the basic IDS LDAP configuration described in this section, you can create the WebSphere Portal Express profile as discussed in 3.3, “Configuring the WebSphere Portal Express server” on page 95. At any time after configuring the WebSphere Portal Express profile, you can create user entries in the IDS LDAP directory. You can do this in different ways:

- Using the IBM Tivoli Directory Server Web Administration Tool. See 3.6, “IBM Tivoli Directory Server Web Administration tool” on page 148, which provides information about how you can manage entries in your IDS LDAP on i5/OS.
- Publishing users from your SDD. See 3.7, “Using information stored in the System Distribution Directory for LDAP publishing” on page 166. This section describes a method for publishing System Directory entries from i5/OS into the IDS LDAP directory.
- Using an LDIF file. See 3.8, “Managing LDAP entries with LDIF” on page 187. This section describes a method for importing LDAP entries from an LDIF file into your IDS LDAP directory using iSeries Navigator.

For more information about LDAP, refer to the following IBM Redbooks publications:

- *Understanding LDAP - Design and Implementation*, SG24-4986
- *Using LDAP for Directory Integration*, SG24-6163
- *Implementation and Practical Use of LDAP on the IBM eServer iSeries Server*, SG24-6193

3.1.1 Basic IDS LDAP configuration on i5/OS

Because the IBM Directory Server for i5/OS is part of i5/OS, the Directory Server is automatically installed with a limited default configuration. Directory Server provides a wizard in iSeries Navigator to assist you in configuring the server for your specific needs. Use this wizard when you initially configure the Directory Server. You can also use the wizard to reconfigure the Directory Server.

**Tip:** When you use the Directory Server Configuration wizard to reconfigure the Directory Server, you start configuring from scratch. The original configuration is deleted rather than changed. However, the directory data is not deleted but instead remains stored in the library that you selected on installation (QUSRDIRDB by default). The change log also remains intact and is located in the QUSRDIRCL library by default. If you want to start completely from scratch, clear those two libraries before starting the wizard.
Your i5/OS user profile must have *ALLOBJ and *IOSYSCFG special authorities in order to configure the Directory Server. If you want to configure security auditing, you must also have *AUDIT special authority. To start the Directory Server Configuration wizard, perform the following steps:

1. From iSeries Navigator, expand Network → Servers and click TCP/IP (see Figure 3-1).

![Figure 3-1 iSeries Navigator](image)

2. In the right pane, right-click IBM Directory Server and select Configure. If you have already configured the Directory Server, click Reconfigure.

3. Follow the instructions in the Configure Directory Server wizard to configure your Directory Server. When the wizard is finished, your Directory Server has a basic configuration.
4. Create entries corresponding to the suffix or suffixes that you want to use. You can add or delete suffixes. In our example, we use a suffix that is equal to our LDAP Server name, which is RCHAS10.RCHLAND.IBM.COM. So we use the suffix dc=rchas10,dc=rchland,dc=ibm,dc=com (see Figure 3-2). If you want to add a new suffix, do the following:


b. On the IBM Directory Server Properties window, click the Database/Suffixes tab.

c. In the New suffix field, type the name of the new suffix and click Add.

d. Click OK to close the IBM Directory Server Properties window.

Tip: If you are running Domino on your system, port 389 (the default port for all LDAP servers) might already be in use by the Domino LDAP function. You must do one of the following:

- Change the default LDAP port that Domino uses.
- Change the default LDAP port that IDS Directory Server uses via iSeries Navigator.
- Use specific IP addresses for your Domino server, as we have done in our scenario.

3.1.2 Starting the IDS Directory Server

Perform the following steps to start the Directory Server:

1. From iSeries Navigator, expand Network → Servers and click TCP/IP.
2. In the right pane, right-click IBM Directory Server and select Start.
3.1.3 Stopping the IDS Directory Server

Perform the following steps to stop the Directory Server:

1. From iSeries Navigator, expand Network → Servers and click TCP/IP.
2. In the right pane, right-click IBM Directory Server and select Stop.

The Directory Server might take several minutes to stop, depending on the speed of your system, the amount of server activity, and the amount of available memory.

The Directory Server can also be stopped from a 5250 interface by entering the command ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL or ENDTCP.

Important: The commands ENDTCP$SRV *ALL and ENDTCP also affect any other TCP/IP servers that are running on your system.

3.2 Setting up the Domino environment

In the scenario covered in this chapter, the Domino server called DOMIDS is the messaging and application server hosting the source data for the Domino-based portlets of our WebSphere Portal Express site. It is also the prerequisite server (and registration server) for the Sametime server called STIDS.

The Sametime server is required to support the following Sametime portlets:
- Sametime Contact List
- Lotus Web Conferencing
- Who Is Here

In our scenario, the Domino Release 7.0.2 and Sametime Release 7.5 software is already installed on the system. This section shows you how to:
- Configure the primary Domino server called DOMIDS.
- Register the Sametime server called STIDS before configuring it.
- Configure the Sametime server STIDS

3.2.1 Configuring the primary Domino server

This section describes how to configure the primary Domino server DOMIDS using the Configure Domino Server (CFGDOMSRV) CL command from a 5250 interface.

When you configure the first Domino server in a new Domino domain, you must provide information that defines the key characteristics of the server. These characteristics include
the name of the Domino server, the location of the Domino server’s data directory, the name of your organization, details about the person who is the Domino server administrator, and the correct time zone.

Table 3-2 lists the important parameters to use in the CFGDOMSRV command. You can use this table as a template, filling in the values according to your environment from the “Value we used” column.

<table>
<thead>
<tr>
<th>Parameter description</th>
<th>Parameter name</th>
<th>Value we used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>SERVER</td>
<td>domids</td>
<td>Specifies the name of the Domino server.</td>
</tr>
<tr>
<td>Option</td>
<td>OPTION</td>
<td>*FIRST</td>
<td>For your first Domino server, specify *FIRST in this field.</td>
</tr>
<tr>
<td>Data directory</td>
<td>DTADIR</td>
<td>/domino/domids/data</td>
<td>Specify the directory path in the i5/OS integrated file system for your Domino server.</td>
</tr>
<tr>
<td>Organization</td>
<td>ORG</td>
<td>itsoids</td>
<td>This option is available only for the first server setup. Typically, the organization name is the name of your company or a major division within your company.</td>
</tr>
<tr>
<td>Administrator:</td>
<td>ADM</td>
<td>admin</td>
<td>This option is available only for first server setup. The administrator can perform operations on the Domino server such as starting and stopping the server. Although you need to provide only a last name, you can use a first name and, if needed, a middle name to make sure the administrator’s name is unique.</td>
</tr>
<tr>
<td>- Last name</td>
<td></td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>- First name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Password</td>
<td></td>
<td>password</td>
<td></td>
</tr>
<tr>
<td>- Minimum password length</td>
<td></td>
<td>8 (default)</td>
<td></td>
</tr>
<tr>
<td>- Internet password</td>
<td></td>
<td>*ADMIN</td>
<td></td>
</tr>
<tr>
<td>Time zone</td>
<td>TIMEZONE</td>
<td>CST</td>
<td>The Time zone field determines the time stamp that the server uses for documents and databases.</td>
</tr>
<tr>
<td>Daylight saving time</td>
<td>DAYSAVTIME</td>
<td>*YES</td>
<td>Use this option to select whether or not your server should adjust for daylight saving time. The default value is *YES.</td>
</tr>
<tr>
<td>Web browsers</td>
<td>WEB</td>
<td>*ALL</td>
<td>Use *ALL to activate the Internet Inter-ORB Protocol (IIOP) feature (also referred to DIIOP in Domino literature) and the HTTP feature. HTTP and DIIOP services are needed on each Domino mail server that supports collaboration portlets for mail and calendar (for example, the Lotus Notes View portlet). Also see “Summary of required Domino server configuration” on page 126.</td>
</tr>
</tbody>
</table>
### Internet mail packages

- **Parameter description**: Internet mail packages
- **Parameter name**: MAIL
- **Value we used**: *SMTP
- **Description**: Specifies which, if any, Internet mail packages should be included in the Domino server configuration. We use only SMTP.

### Directory services

- **Parameter description**: Directory services
- **Parameter name**: DIRSRV
- **Value we used**: *LDAP
- **Description**: We need the LDAP service to provide mail file auto-detecting for all our examples in this chapter.

### Connection services

- **Parameter description**: Connection services
- **Parameter name**: CNNSRV
- **Value we used**: *NONE
- **Description**: We do not need Domino Enterprise Connection Services (DECS), so we define *NONE here.

### Advanced services

- **Parameter description**: Advanced services
- **Parameter name**: ADVSRV
- **Value we used**: *PARTITION
- **Description**: Use the default value *PARTITION.

### TCP/IP Port options

- **Parameter description**: TCP/IP Port options
- **Parameter name**: TCPOPT
- **Value we used**: *NOENCRYPT (Default)
- **Description**: Specifies options for the TCP/IP port.

  - **Encrypt Network data**: *NOENCRYPT (Default)
  - **Internet address**: domids.rchland.ibm.com
    - **Description**: Use the Internet address option to specify a separate Internet (IP) address for the server’s port.
  - **Bind HTTP**: *YES (Default)
  - **Compress network data**: *NO (Default)

### Server host name

- **Parameter description**: Server host name
- **Parameter name**: SVRHSTNAME
- **Value we used**: domids.rchland.ibm.com
- **Description**: Define here the host name of your Domino server. We define domids.rchland.ibm.com, which is configured on the System i TCP/IP configuration with its own TCP/IP address. See the example in Figure 3-3 on page 80.

### System and object name

- **Parameter description**: System and object name
- **Parameter name**: SBS
- **Value we used**: DOMIDS
- **Description**: Use this option to use a specific name for the i5/OS subsystem and associated objects that are used by the Domino server. In our examples, each Domino server runs in a separate i5/OS subsystem.

### Text description

- **Parameter description**: Text description
- **Parameter name**: TEXT
- **Value we used**: Domino server with IDS LDAP
- **Description**: (Optional)
Perform the following steps to configure the Domino server:

1. From a 5250 emulation session, type the CL command CFGDOMSRV (Configure Domino Server) and press F4 to prompt the command.

2. On the Configure Domino Server panels, type the values for the required parameters listed in Table 3-2 on page 78. After entering all required parameters press Enter to configure the Domino server.

   We used the following CFGDOMSVR command to create our Domino server DOMIDS:

   ```cl
   CFGDOMSVR SERVER(DOMIDS) OPTION(*FIRST)
   DTADIR('/domino/domids/data') ORG(itoids) ADM(admin *N *N (password) 8
   (*ADMIN)) TIMEZONE(CST) DAYS HastIME(*YES) WEB(*ALL) MAIL(*SMTP) DIRSRV(*LDAP)
   CNNSR (*NONE) TEXT('Domino Server with IDS LDAP') TCPOPT(*NOENCRIPT
   DOMIDS.RCHLAND.IBM.COM) SVRHSTNAME(domids.rchland.ibm.com) SBS(DOMIDS)
   ```

   **Note:** Because we need the LDAP service for our solution 2 example for mail auto-detection, we specified the value of *LDAP for the DIRSRV parameter. If you instead follow our solution 1 example, the Domino LDAP service is not needed, so you should specify the value of *NONE for the DIRSRV parameter. For details, see 3.5, “Integrating Domino mail and calendar” on page 119.

3. When the Domino server has been successfully configured, you will see the following message:

   Command CFGDOMSVR ended successfully.

**Starting the Domino server**

The next step is to start the Domino server. You do this in the following way:

1. Enter the Work with Domino Server command, WRKDOMSVR, and press Enter.

2. On the Work with Domino Servers display, enter an option 1 (Start server) next to your just created Domino server (DOMIDS) and press Enter to start the Domino server.
3.2.2 Registering a Domino server

Before adding a Domino server to an existing Domino domain, you have to register the server. Our DOMIDS Domino server is the primary and registration server in our ITSOIDS Domino domain. Before configuring the Sametime server, you have to register the server as described in this section.

To register a new server from your workstation, you must have access to the registration Domino server and have at least Author access to the Domino Directory with the appropriate role in the access control list of the Domino Directory.

**Note:** For more detailed information about registering additional Domino servers, refer to the IBM Redbooks *IBM Lotus Domino 6 for iSeries Implementation*, SG24-6592.

Perform the following steps to register a Domino server. The registration server (the Domino server on which you register other servers) must be up and running on your network.

1. Launch the Domino Administrator client from your workstation desktop.
2. Select the registration Domino server (*domids* in our example) from the Bookmarks or click File → Open Server.
3. In the Open Server window, select the server to administer, which is *domids/itsoids* in our example. Click OK. See Figure 3-4.

![Figure 3-4 Opening the Domino registration server](image)

4. Select the Configuration tab.
5. In the left navigation pane, expand Server and select All Server Documents. See Figure 3-5.

![Figure 3-5 Domino Administrator client, All Server Documents view](image)
6. From the Tools pane (right side of the panel), click **Registration**. Under Registration, click **Server** (see Figure 3-6).

![Figure 3-6 Tools pane](image)

7. If you want to use a different Domino server to register your new server, click the **Server** button on the Choose a Certifier window (Figure 3-7). This enables you to change the Domino server on which the Domino Directory is updated with the new server details. If your Domino server is not listed, you can enter the name. You must be able to establish a network connection to the registration Domino server.

   If you must use a different certifier ID, click the **Certifier ID** button. Select the correct ID file for the organization (cert.id). Click **OK**.

![Figure 3-7 Choosing a registration server and certifier ID](image)

8. When prompted, enter the certifier password and click **OK**.

9. If you see a warning message about the Certifier Recovery Information, click **OK**. The ID recovery information creation is a separate process, which we do not explain in this context. Refer to the Domino administration documentation for more information about the ID recovery feature.
10. On the Register Servers window (Figure 3-8), you can again change the registration server and certifier settings. You also need to choose the security type of the server ID and verify whether you need to change the server certificate expiration date default. Click Continue.

![Figure 3-8 Register Servers information](image-url)
11. On the Register New Server(s) window, enter the required information (see Figure 3-9).

- **Server name**: Enter the name of the new Domino server. We use stids.
- **Server title**: This title is visible in the Domino Directory to identify the server.
- **Domino Domain name**: Enter the name of the existing Domino domain. We use itsoids, as this is the Domain name we used for the Organization, see Table 3-2 on page 78.
- **Server administrator name**: The name of the Domino Administrator or an Administration group, in our example it is admin/itsoids.
- **Location for storing server ID**: Deselect In Domino Directory and select **In file**. Click **Set ID File**. Now you can browse to the server and directory (we have mapped a network drive to our i5/OS integrated file system) where the server id file is stored. Select the target directory (we use our /domino/domids/data directory) and type a name for the id file that will be created and click **Save**. We named the id file stids.id.
- **Click the green check mark to add the Domino server to the registration queue.** The server registration queue located at the bottom of the window displays the Domino servers ready to be registered. Click **Register All**.

![Figure 3-9 Registering a new Domino server called STIDS](image)

12. After the registration process is completed, click **Done** to close the Register New Server(s) window.
3.2.3 Registering Domino users

In our example in this chapter, we register several users on the DOMIDS Domino server. The following steps show how to register a Domino user:

**Note:** Remember there is a difference between adding and registering users. Adding a user in a Domino Directory creates a Person record in the Domino Directory for that user. Registering a user through the Domino Administrator client creates a Person document in the Domino Directory and also creates a mail file for the person. Only registered users have access to mail on Domino. Refer to the Lotus Domino Administrator Help database for more information about registering users.

1. From the Domino Administrator client, click the **Configuration** tab.
2. In the upper-right pane, expand **Tools** → **Registration** and select **Person** as shown in Figure 3-10.

![Figure 3-10 Tools pane](image)

3. When prompted, enter your Certifier password for your administrator and click **OK**.
4. On the Register Person - New Entry window, Basics panel (Figure 3-11), type the values for First name, Middle name, Last name, Short name, and Password and select **Domino Web Access** from the Mail system selection list. Click the green check mark icon.

![Figure 3-11 Registering a person on the Domino server](image)

**Important**: If you plan to integrate collaboration and mail auto-detection into your WebSphere Portal Express server following the approach described in solution 2 (see 3.5.3, “Solution 2: Using the Domino Directory Assistance database” on page 133) consider that the short name in the Domino Person document is matched to the uid attribute in Domino LDAP by default. So use a value for short name here that is equal the value for the distinguished name (DN). In our example, the DN is the uid defined in the IDS LDAP directory for your users. The name mapping for mail auto-detection works easily when these values are the same in the Domino Person document and the IDS LDAP.

Table 3-3 shows our sample Domino users with their short name in the Domino Directory and the same value for uid in the LDAP directory, which is also the DN of our IDS LDAP. Also note that mixed case is not a problem.

**Table 3-3 Sample Domino users and their IDS LDAP distinguished name (in our example, uid)**

<table>
<thead>
<tr>
<th>Domino short name</th>
<th>Domino first name</th>
<th>Domino last name</th>
<th>Domino user name</th>
<th>Domino mail file name</th>
<th>IDS LDAP UID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Madan</td>
<td>Marcela</td>
<td>Adan</td>
<td>Marcela Adan/itsoids</td>
<td>madan</td>
<td>madan</td>
</tr>
<tr>
<td>UAlthoff</td>
<td>Ursula</td>
<td>Althoff</td>
<td>Ursula Althoff/itsoids</td>
<td>ualthoff</td>
<td>ualthoff</td>
</tr>
</tbody>
</table>
5. At this point, the Register Person - New Entry window shows the Registration Queue (local) list with the added user listed. You can add now additional people. When you are finished, click Register All. See Figure 3-12.

![Figure 3-12  Registration queue](image)

6. The registration process takes some time; when it is finished, you get the message Person registered successfully! Click OK. Then click Done to close the registration window.
7. Figure 3-13 shows all our registered Domino users in the Domino Directory.

![Figure 3-13 All users in the Domino Directory](image)

### 3.2.4 Configuring the Sametime server

In this section Sametime is added to an existing Domino server. Before you can create and add the Sametime server, the registration task has to be completed as described in 3.2.2, “Registering a Domino server” on page 81.

The Sametime server supports the following Sametime portlets:

- Sametime Contact List
- Lotus Web Conferencing
- Who Is Here

![Table 3-4 CFGDOMSVR parameters for the Sametime server, STIDS](image)

<table>
<thead>
<tr>
<th>Parameter description</th>
<th>Parameter name</th>
<th>Value we used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>SERVER</td>
<td>stids/itsoids</td>
<td>Enter the name of the Sametime server.</td>
</tr>
</tbody>
</table>

**Option**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value we used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ADD</em></td>
<td></td>
<td>Enter <em>ADD</em> to add a preregistered server (see 3.2.2, “Registering a Domino server” on page 81).</td>
</tr>
</tbody>
</table>

Note: For more information about installing and configuring Sametime on i5/OS, refer to the product documentation, *Installing and Managing Sametime 7.5 for i5/OS*, on the Web at:

http://www-12.lotus.com/ldd/doc/uafiles.nsf/70817c90542892178525695b0051105c/1aa62f6eb0a1a16c852571ce06f2b91/$FILE/stinstall.pdf

Before you add the Sametime server, decide which parameter values you want to use in your environment for creating your Sametime server.

Table 3-4 shows the important parameters to use in the Configure Domino Server (CFGDOMSRV) command. You can use this table as a template; filling in the values according to your environment in the “Value we used” column. Leave all those parameters not shown here at their default value.

Before you add the Sametime server, decide which parameter values you want to use in your environment for creating your Sametime server.

Table 3-4 shows the important parameters to use in the Configure Domino Server (CFGDOMSRV) command. You can use this table as a template; filling in the values according to your environment in the “Value we used” column. Leave all those parameters not shown here at their default value.

**Table 3-4 CFGDOMSVR parameters for the Sametime server, STIDS**

<table>
<thead>
<tr>
<th>Parameter description</th>
<th>Parameter name</th>
<th>Value we used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>SERVER</td>
<td>stids/itsoids</td>
<td>Enter the name of the Sametime server.</td>
</tr>
</tbody>
</table>

**Option**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value we used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ADD</em></td>
<td></td>
<td>Enter <em>ADD</em> to add a preregistered server (see 3.2.2, “Registering a Domino server” on page 81).</td>
</tr>
<tr>
<td>Parameter description</td>
<td>Parameter name</td>
<td>Value we used</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Data directory</td>
<td>DTADIR</td>
<td>/domino/stids/data</td>
</tr>
<tr>
<td>Time zone</td>
<td>TIMEZONE</td>
<td>CST</td>
</tr>
<tr>
<td>Daylight saving time</td>
<td>DAYSAVTIME</td>
<td>*YES</td>
</tr>
<tr>
<td>Get Domino Directory from: Domino server name</td>
<td>NABSVR</td>
<td>domids/itsoids</td>
</tr>
<tr>
<td>Domino Directory type</td>
<td>DIRTYPE</td>
<td>*CENTRAL</td>
</tr>
<tr>
<td>Additional server ID: ID file</td>
<td>ADDSVRID</td>
<td>/domino/domids/data/stids.id</td>
</tr>
<tr>
<td>Web browsers</td>
<td>WEB</td>
<td>*HTTP</td>
</tr>
<tr>
<td>Internet mail packages</td>
<td>MAIL</td>
<td>*NONE</td>
</tr>
<tr>
<td>Directory services</td>
<td>DIRSRV</td>
<td>*NONE</td>
</tr>
<tr>
<td>Connection services</td>
<td>CNNSRV</td>
<td>*NONE</td>
</tr>
<tr>
<td>Advanced services</td>
<td>ADVSRV</td>
<td>*PARTITION</td>
</tr>
<tr>
<td>Default ACL settings</td>
<td>DFTACL</td>
<td>*ADMGRP</td>
</tr>
<tr>
<td>Text description</td>
<td>TEXT</td>
<td>Sametime server using IDS LDAP</td>
</tr>
</tbody>
</table>

**TIP:** Press F9 to see all parameters.
After finishing the collection of the required parameters, perform the following steps to configure the Sametime server.

1. From a 5250 emulation session, type the CL command CFGDOMSRV (Configure Domino Server) and press F4 to prompt the command.

2. On the Configure Domino Server panels, enter the values for the required parameters listed in Table 3-4 on page 88. After entering all required parameters, press Enter to configure the Domino server.

We used the following CFGDOMSVR command to create our Sametime server STIDS:

```cl
CFGDOMSVR SERVER('stids/itsoids') OPTION(*ADD) DTADIR('/domino/stids/data') TIMEZONE(CST) NABSVR('domids/itsoids') ADDSVRID('/domino/domids/data/stids.id') WEB(*HTTP) CNNSRV(*NONE) TEXT('Sametimeserver using IDS LDAP') TCPOPT(*NOENCRYPT STIDS.RCHLAND.IBM.COM) SVRHSTNAME(stids.rchland.ibm.com) SBS(STIDS)
```

3. When the Domino server has been successfully configured, the following message is displayed:

```
Command CFGDOMSVR ended successfully.
```
Adding Sametime to the Domino server

It is necessary to add the Sametime server to an existing Domino server, so the Sametime services can be started and are known in your Domino domain.

**Important:** Before you add the Sametime server, you must stop the Domino server.

Perform the following steps to add Sametime to a Domino server using the Add Sametime to Domino (ADDLSTDOM) CL command from a 5250 emulation session:

1. Verify the Domino server, which you plan to add the Sametime server to, is stopped.
   
   You can do so by typing the Work with Domino Servers (WRKDOMSRV) command and checking that the status of your Domino server shows *ENDED. If the Domino server is not ended, type option 6 (End server) in the option field (Opt) next to your Domino server and press Enter.

2. Add Sametime to Domino by entering the Add Sametime to Domino (ADDLSTDOM) CL command and press F4 to prompt the command.

3. On the Add Sametime to Domino (ADDLSTDOM) display, enter the Domino server name. For our example, this is **STIDS**. Press F9 to display all parameters for this command.

4. Table 3-5 lists the important parameters for the ADDLSTDOM command and helps you define the right values. See Figure 3-14 on page 92. Leave all parameters not shown at their default values.

<table>
<thead>
<tr>
<th>Field label</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domino server name (SERVER)</td>
<td>Specify name of the Sametime server you want to add. In our example, this is STIDS.</td>
</tr>
<tr>
<td>Directory type (DIRTYPE)</td>
<td>*LDAP</td>
</tr>
<tr>
<td>LDAP server name (LDAPSVR)</td>
<td>Specify the fully qualified host name of your LDAP server. In our example, it is the IDS LDAP server RCHAS10.RCHLAND.IBM.COM.</td>
</tr>
<tr>
<td>LDAP server port</td>
<td>The default port is 389. If your LDAP server listens on another port, define it here.</td>
</tr>
<tr>
<td>Event server port (EVTSVRPORT)</td>
<td>See Note that follows.</td>
</tr>
<tr>
<td>Token server port (TKNSVRPORT)</td>
<td>See Note that follows.</td>
</tr>
</tbody>
</table>

**Note:** The Sametime server instance binds to localhost on the ports specified for:

- Event Server port (EVTSVRPORT)
- Token Server port (TKNSVRPORT)

You have to assign port values that are not used by other TCP/IP services running on your i5/OS environment. The ports have to be unique on the entire system.
Enabling Collaboration in WebSphere Portal Express V6 on i5/OS

Figure 3-14   ADDLSTDOM CL command

The following is how the ADDLSTDOM command looks on a 5250 command line:

```
ADDLSTDOM SERVER('stids/itsoids') DIRTYPE(*LDAP) LDAPSVR(RCHAS10.RCHLAND.IBM.COM) EVTSVRPORT(9097) TKNSVRPORT(9099)
```

5. Press Enter to add Sametime to the Domino server. The Add Sametime to Domino (ADDLSTDOM) display is refreshed with the values you entered and the option to start the Sametime server. In our example, we leave *NO value here.

6. When the add process is finished, which can take several minutes, you see the following message:

```
Command ADDLSTDOM ended successfully.
```

Starting the Sametime server

Next step is to start the Sametime server. Perform the following steps:

1. Enter the Work with Domino Server command, WRKDOMSVR, and press Enter.
2. On the Work with Domino Servers display, enter an option 1 (Start server) next to your Sametime server (STIDS) and press Enter to start the Sametime server.
Verifying the Sametime server

Now that you have started the Sametime server successfully, you can verify the configuration and settings by logging on to the Sametime server and testing some of the services. Perform the following steps:

1. Open your Sametime server home page (stcenter.nsf) in a Web browser. In our example, the URL is:

   \[http://stids.rchland.ibm.com/stcenter.nsf\]

   You see the Sametime home page similar to the one shown in Figure 3-15. Click the Log in to IBM Lotus Sametime link.

2. Enter a User name and Password that exists in your LDAP directory and click Log in. See Figure 3-16.

   ![Figure 3-15  Sametime home page](image)

   ![Figure 3-16  Logging on to Sametime](image)
3. On the Welcome to IBM Lotus Sametime window, you should see the name of the logged on user as shown in Figure 3-17. Use a Sametime function for testing the functionality. Click **Schedule a Meeting**.

![Figure 3-17 User logged on to Sametime](image)

4. On the New Meeting window, enter the required values for scheduling a new meeting as shown in Figure 3-18.

![Figure 3-18 Scheduling a Sametime meeting](image)

5. Once you have verified your Sametime server is working correctly, proceed with steps in the next section 3.3, “Configuring the WebSphere Portal Express server” on page 95.
3.3 Configuring the WebSphere Portal Express server

This section discusses the important panels of the IBM Web Administration for i5/OS Create WebSphere Portal wizard to create a WebSphere Portal Express profile that uses IDS LDAP for authentication. Refer to the IBM Redpaper *Installing and Installing and Configuring WebSphere Portal Express V6 on i5/OS*, REDP-4303, for detailed information and a description of the prerequisites before you start the wizard.

Perform the following steps to configure your WebSphere Portal Express profile:

1. Launch the IBM Web Administration for i5/OS tool by pointing your Web browser to:

   http://<systemi_hostname>:2001

2. Log on using an i5/OS user profile with *IOSYSCFG, *ALLOBJ, and *JOBCTL special authorities. Do not use the QSECOFR user profile.

3. Select **IBM Web Administration for i5/OS**.

4. Select **Create WebSphere Portal**.

5. On the Create WebSphere Portal Welcome panel, click **Next**.

6. Select **WebSphere Portal Express V6.0.0.1** and click **Next**.

7. On the Specify name for server - Step 1 of 14 window, enter the WebSphere Portal Express server name and click **Next**. In our example, the WebSphere Portal Express server name is **wpx6ids**.

8. On the Specify Internal Ports Used by the Application Server - Step 2 of 14 window, specify the first port in the range to be assigned to the WebSphere Portal Express profile and click **Next**. The wizard verifies that the port range you specify is usable and no port in the range is actually in use or that another WebSphere application server is not configured using any of the ports in the specified range.

9. On the Create a new HTTP server (powered by Apache) - Step 3 of 14 window, specify the name of your HTTP server (we use **wpx6ids**), the IP address of this HTTP server, and the port to be used. Click **Next**.

10. On the Create DB2 Database for Portal - Step 4 of 14 window, specify a user profile that will be created and will become the owner of the WebSphere Portal Express databases. We use **wpxids**. Select **Database based on the server name** and click **Next**.

   **Important:** The password for this user profile becomes the same value as the portal administrator password that you specify later in the wizard. This password must follow the i5/OS password rules.

11. On the Configure Proxy Information for Content Access Service - Step 5 of 14 window, select **Do no use proxy** and click **Next**.

12. On the Deploy Default Portlets - Step 6 of 14 window, select the portlets you want to implement and click **Next**.

13. On the Configure Lotus Collaborative Components - Step 7 of 14 window, select **Lotus Sametime**. Provide the host name of your Sametime server and the port. In our example, this is **stids.rchland.ibm.com**, and the port is 1533. Click **Next**.

14. On the Secure Application Server and WebSphere Portal with LDAP - Step 8 of 14 window, select **Configure security using LDAP with Realm support now** or **Configure...**
security using LDAP without Realm support now. Enter the LDAP server host name of your IDS LDAP directory and verify the port. Click Next.

In our example, we use the LDAP with Realm support and specify rchas10.rchland.ibm.com as our host name for the IDS LDAP server (see Figure 3-19).

Figure 3-19  Specifying the LDAP server host name

Note: If your decision is to use Realm support, you have complete the steps described in 3.4.1, “LDAP with realm support and SSO” on page 105 after your WebSphere Portal Express profile is created.
15. On the LDAP Authentication - Step 9 of 14 window (Figure 3-20), specify whether your WebSphere Portal Express server will have write access or read-only access to your LDAP server. Enter the LDAP user DN and password that has access to the LDAP directory. If you define write access, the LDAP administrator value is recommended.

In our example, we select **Allow write access to the LDAP directory** and our administrator's DN is `cn=administrator`. Click **Next**.

Refer to 1.3.3, “Read/write or read-only access to the directory server” on page 7 for more information about allowing the WebSphere Portal Express server read/write access or read-only access to your directory server.

16. On the LDAP Configuration Parameters - Step 10 of 14 window, we follow the approach in our example to use the default values WebSphere Portal Express uses for all entries in the LDAP directory. For more information about this topic see 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9. In our example, the IDS LDAP has only the basic configuration (see 3.1.1, “Basic IDS LDAP configuration on i5/OS” on page 74) and contains no additional entries.

If you select write access to the LDAP directory in the previous step, the default user and group containers do not have to exist in your IDS LDAP directory and are automatically created by the wizard. If the containers already exist, the wizard defaults to these values regardless of your LDAP access level.
Therefore, if your IDS LDAP is set up in this way, leave these default values as they are shown in the wizard (Figure 3-21) and click **Next**.

If you have another naming convention, click the **Browse** button (for both the user entries and administrative group entry) to choose the Parent DN. Then select the object classes and naming attributes from the selection lists in the wizard. All these values are retrieved by the wizard from your IDS LDAP server.

For an example of how to use the wizard when you already have an IDS directory in place, refer to “Configuring the WebSphere Portal Express server for the SDD scenario” on page 178.

---

**Note:** The wizard only creates the default Parent User DN or Parent Group DN and the corresponding containers in the LDAP directory. You can override these values by specifying other names in the wizard (or use the Browse button as described previously). However, these containers and DNs must exist in the LDAP directory prior to running the wizard.

---

**Create WebSphere Portal Express, V6.0**  
**LDAP Configuration Parameters - Step 10 of 14**

The Portal server utilizes LDAP to store user information for authentication purposes. Below is where the administrator user and group will reside in your LDAP directory.

**Information describing user entries**

- **Parent DN:** `cn=users, DC=rchas10, DC=rchland, DC=ibm, DC=com`  
  **Browse**

- **Object class:** `inetOrgPerson`  
  **Next**

- **Naming attribute:** `uid`  
  **Submit**

**Information describing the administrative group entry**

- **Parent DN:** `cn=groups, DC=rchas10, DC=rchland, DC=ibm, DC=com`  
  **Browse**

- **Object class:** `groupOfUniqueNames`  
  **Next**

- **Naming attribute:** `cn`  
  **Submit**

**Member attribute:** `uniqueMember`  
**Submit**

---

17. On the LDAP Administrative Group and Administrative User - Step 11 of 14 window, you define the name for the LDAP group where the Portal administrator will become a member.

In the Portal administrator information section, you provide the user name for the Portal administrator in the User name field and the password for this administrator in the Password and Confirm password fields. See Figure 3-22 on page 99.

You can also use the Browse buttons to select an existing group and an existing user. In this case, the entries have to exist in the LDAP directory before running the wizard.

The wizard automatically creates the Portal administrator user as an entry in the user container you specified in the previous step. The user you define here also becomes the WebSphere Application Server administrator.
In our example, we use the default values of wpsadmins for the group and wpsadmin for the portal administrator. See Figure 3-22.

Create WebSphere Portal Express, V6.0

LDAP Administrative Group and Administrative User - Step 11 of 14

WebSphere Portal requires an administrative group and user entry in the LDAP directory. If the group and user entries do not already exist, the wizard will create them. If the group and user entries already exist, the wizard will validate them. The wizard will also ensure the administrator user is added to the administrative group.

Note: The administrator user name specified here is the portal administrator, the WebSphere Application Server administrator, the LDAP authentication user and the Member Manager Enterprise Java Bean (EJB) user.

Portal administrative group information:

Group name: wpsadmins

Portal administrator information:

User name: wpsadmin
Password: **********
Confirm password: **********

Note: The password specified for this administrator will also be used for the password of the database owner User ID. The password entered should comply with your system password rules.

Figure 3-22 Creating the portal administrator and administrator group

18. In the Additional group names section (Figure 3-23), enter the Portal administrative group names for the additional groups such as Document manager group name, Document reviewer group name, and Web content management group name. You can override these names if you want.

All the portal groups you specify on this page are automatically created by the wizard if they do not exist. Additionally, the wizard automatically adds the portal administrator user you defined in step 17 on page 98 into these groups as a unique member.

In our example, we use the default names shown in the wizard. Click Next.

Figure 3-23 Specifying the additional portal group names
19. Figure 3-24 and Figure 3-25 show the LDAP entries after the wizard has created the WebSphere Portal Express profile. Your IDS LDAP will look similar if you followed the approach using the default values specified in the wizard.

At this point, your directory server has a group container for users called users with the administrator for the portal (in our example, **wpsadmin**) as a member, a group container called groups, which contains entries of the group names (see Figure 3-24).

![Figure 3-24 LDAP users and groups entries](image)

**Figure 3-24 LDAP users and groups entries**

Figure 3-25 shows the uniqueMember of the wpsadmins group. This is also the uniqueMember of the other portal group entries.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>objectClass</td>
<td>top</td>
</tr>
<tr>
<td>objectClass</td>
<td>groupOfUniqueNames</td>
</tr>
<tr>
<td>uniqueMember</td>
<td>uid=wpsadmin,cn=users,d=cmachl10,d=chland,d=bmi,d=com</td>
</tr>
<tr>
<td>cn</td>
<td>wpsadmins</td>
</tr>
<tr>
<td>modificationName</td>
<td>CN=ADMINISTRATOR</td>
</tr>
<tr>
<td>modifyTimestamp</td>
<td>20070411 21:05:23.000000Z</td>
</tr>
<tr>
<td>creationName</td>
<td>CN=ADMINISTRATOR</td>
</tr>
<tr>
<td>createTimestamp</td>
<td>20070411 21:05:23.000000Z</td>
</tr>
<tr>
<td>subschemaSubentry</td>
<td>cn=schema</td>
</tr>
</tbody>
</table>

**Figure 3-25 LDAP unique member of the wpsadmins group**
window, select **include other Web servers in your SSO environment**. Enter your SSO domain name - in our example, this is rchland.ibm.com - and click **Next**. See Figure 3-26.

Create WebSphere Portal Express, V6.0
Web Server Single Signon (SSO) Configuration Parameters - Step 12 of 14

Web Server Single Signon (SSO) will be configured by the wizard. SSO is a mechanism where a single user signon action permits access to multiple Web servers without the need to re-authenticate. The domain name identifies the Web servers that can be accessed within the SSO environment. SSO is useful when your Portal server needs to access information from other Web servers such as Domino, QuickPlace, Sametime, or WebSphere Application Servers.

- If your WebSphere Portal does not require information from other Web servers, the SSO domain should be limited to this Web server’s hostname.
- If your WebSphere Portal requires information from other Web servers, you will need to specify an SSO domain name. This domain name must be the portion of the fully qualified Domain Name System (DNS) hostname that is shared by all Web servers participating in your SSO environment. When accessing any of the Web servers in the SSO environment, you will only need to authenticate once.

Specify SSO domain:

- Limit SSO domain to this Web server’s hostname
- Include other Web servers in your SSO environment

SSO domain name: [rchland.ibm.com](rchland.ibm.com)

**Examples:** Based on the following server hostnames, the corresponding SSO domain name would be:

Figure 3-26   Specifying the SSO environment
21. On the Configure Lightweight Third Party Authentication (LTPA) for Web Server Single Signon (SSO) Environment window (Figure 3-27), enter and confirm the LTPA password and click **Next**. This password is required in the procedure in 3.4.3, “Importing the LTPA key into Domino” on page 110.

**Important:** Keep this password in a save place; you need it to import the LTPA key to the other servers in your domain - for example, to configure SSO for your Domino servers.

---

**Create WebSphere Portal Express, V6.0**

**Configure Lightweight Third Party Authentication (LTPA) for Web Server Single Signon (SSO) Environment**

Lightweight Third Party Authentication (LTPA) is the mechanism used to implement Web Server SSO. LTPA is a set of tokens or cookies which provide a means to share authentication and access control information between Web servers. The information in these tokens uniquely identifies the user. LTPA keys will be created by this application server. These keys must be exported from this application server and imported into the other application servers in your SSO environment. When importing these keys into the other application servers, a password is necessary to encrypt and decrypt the LTPA keys.

If you forget the LTPA keys password or need to change it, use the WebSphere Application Server Administrative Console. After changing the password, you will need to generate and export new LTPA keys and import these new keys into other application servers and into the SSO configuration for Domino servers.

LTPA password:  

Confirm password:  

Figure 3-27  Creating the LTPA token for SSO
22. On the Configure Identity Token SSO for Web to i5/OS Access - Step 13 of 14 window (Figure 3-28), select **Do not configure Identity Tokens** and click **Next**.

**Note:** EIM is needed to implement SSO by the Identity Token mechanism to provide SSO functionality to access i5/OS backend applications that are accessed through a Web-based interface. EIM maintains the relationship between Web users and i5/OS user profiles. Also, Access for Web portlets can use this mechanism to provide SSO in a portal environment.
23. The Summary - Step 14 of 14 window provides a summary of your WebSphere Portal Express profile configuration. When you review the configuration, you see all the definitions as shown in Figure 3-29 and Figure 3-30. You can also use the Printable Summary button to obtain a printout of the configuration. Click Finish.

![Create WebSphere Portal Express, V6.0](image)

Figure 3-29 Create Portal Summary, Servers tab, part 1

![WebSphere Application Server Information](image)

Figure 3-30 Create Portal Summary, Servers tab, part 2

24. The process of completing the configuration runs for a few hours (two to four hours, depending on the size of your system). You can close the Web browser at this point, and the configuration will continue. When the configuration finishes, you can access the WebSphere Portal Express server by entering the portal URL in a Web browser:

```
http://<servername>/wps/portal
```

In our example, this is http://wpx6ids/wps/portal.

25. Log on to the portal as any user defined in your IDS LDAP directory to verify the configuration.
3.4 Configuring SSO between Domino and WebSphere Portal

As described in “Single sign-on and LTPA concepts” on page 14, SSO is accomplished through the use of LTPA technology. Because the LTPA cookie is encrypted, all participating servers in a domain must have the same key to decrypt the LTPA cookie.

The WebSphere Portal Express server (and thus the underlying WebSphere Application server) is responsible for generating the LTPA key. This generated key must be exported into a file and imported to all servers in the domain - see 3.4.2, “Generating and exporting the LTPA key” on page 108 for details.

You import this LTPA key inside the Web SSO Configuration document for Domino servers - see 3.4.3, “Importing the LTPA key into Domino” on page 110 for details.

One Web SSO configuration document per Domino domain can be replicated to all the Domino servers in that domain, but you must enable multi-server authentication individually for every server in a Domino domain - see 3.4.4, “Enabling multi-server session-based authentication in Domino” on page 113.

If you have chosen to enable security with realm support in the Create WebSphere Portal wizard, you also have to complete the steps described in 3.4.1, “LDAP with realm support and SSO” on page 105.

In addition, to configure SSO for Sametime in your WebSphere Portal Express environment, you must perform the steps described in 3.4.5, “Configuring Sametime to use the IDS LDAP settings” on page 114.

To verify your SSO configuration after completing the steps mentioned previously, refer to 3.4.6, “Verifying SSO between Sametime, Domino, and WebSphere Portal” on page 117.

3.4.1 LDAP with realm support and SSO

If you enabled security with realm support using the Create WebSphere Portal wizard (and this also applies if you enabled it by running the configuration task enable-security-wmmur-ldap or enable-security-wmmur-db), you must manually synchronize the realm values in WebSphere Portal Express and Domino.

This section describes the configuration steps that you must complete if your WebSphere Portal Express server is configured with realm support.

To synchronize the realm values, you must set the userRegistryRealm value in the WebSphere Application server to the name of your LDAP host server. Perform the following steps:

1. Start the IBM Web Administration for i5/OS - for example, from a Web browser:
   

2. Log on using your i5/OS user ID and password. At minimum, your user ID must have 
   *ALLOBJ, *JOBCTL, and *IOSYSCFG special authorities.

3. Click the Application Servers tab and select the WebSphere Portal Express profile from the Servers list.

4. On the Manage WebSphere Portal Express window, in the left navigation pane, select Launch Administrative Console.
5. Log on to the WebSphere Administrative Console using the WebSphere Portal Express administrator user ID and password that you specified in the Create WebSphere Portal wizard. See Figure 3-22 on page 99.

6. Click **Security → Global security** as shown in Figure 3-31.

7. On the Global security window, under User registries, click **Custom**. See Figure 3-32.
8. On the Custom user registry window (Figure 3-33), click **Custom Properties**.

![Custom user registry](image)

**Figure 3-33  Custom user registry**

9. Check whether the property `userRegistryRealm` already exists. If so, select that property and click **Update**. Otherwise, click **New** and type `userRegistryRealm` in the Name field in the following panel.

10. Type your LDAP directory host server name in the Value field. In our example, this is `rchas10.rchland.ibm.com:389`. See Figure 3-34. Click **OK**.

![Update User Registry - userRegistryRealm](image)

**Figure 3-34  Update User Registry - userRegistryRealm**

11. Save your changes and restart the WebSphere Portal Express server so the changes become active.
3.4.2 Generating and exporting the LTPA key

The Create WebSphere Portal wizard generates the LTPA key as shown 3.3, “Configuring the WebSphere Portal Express server” on page 95. A good practice is to generate this key again before you export the key into a file.

To generate and export the LTPA key from the WebSphere Application server into a file, perform the following steps:

1. Open the WebSphere Application Server Administrative Console of the WebSphere Portal Express server. You can do this from the IBM Web Administration for i5/OS as described in the steps 1 on page 105 to 5 on page 106 in 3.4.1, “LDAP with realm support and SSO” on page 105, or you can directly type the following URL:

   https://System:WebSphereProfileAdministratorSecurePort/ibm/console/logon.jsp

   In our example this is: https://rchas10:10129/ibm/console/logon.jsp.

2. Log on to the WebSphere Administrative Console using the WebSphere Portal Express administrator user ID and password that you specified in the Create WebSphere Portal wizard. See Figure 3-22 on page 99. In our example, we used user wpsadmin.


4. Under Additional properties (located on the right of the window), click Single signon (SSO).

5. As shown in Figure 3-35, make sure the Domain name field is set correctly, which is required so SSO works properly. SSO can fail if this field is blank or incorrectly set. The Create WebSphere Portal wizard sets this value according to the definitions made in Step 12 of 14 panel for the SSO domain name (see Figure 3-26 on page 101).

   Also make sure that the Web inbound security attribute propagation field is deselected. If you make any changes, make sure to click Apply.

Figure 3-35 LTPA, SSO General Properties
6. Click the **LTPA** link (located at the top of the window) to return to the **Global Security → LTPA** tab.

7. The Password and Confirm Password fields in the LTPA panel should also contain the values you set in the Create WebSphere Portal wizard (see Figure 3-27 on page 102). You can change these values here if you want. When changing these values, save the settings and restart your WebSphere Portal Express server. You can do this restart after finishing the Export Keys task (which you do in one of the next steps).

8. At this point, all the parameters are set. This is the time to generate the LTPA key. Click the **Generate Keys** button.

Click **Apply** to apply the changes to the master configuration

Click **Save** to save your changes to the master configuration.

9. Back on the LTPA panel, you can export the LTPA keys. Enter a path (optional) and file name in the Key File Name field. In our example, we used the name *wpx6ids.key*.

**Note:** If you omit the path and type only the file name (with any extension), the key file is exported to the was_profile_root directory of your i5/OS integrated file system. In our environment this directory is:

/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6ids/

Click **Export Keys** (see Figure 3-36).

![Figure 3-36 Specifying the LTPA export key file name](image)

10. Click **Apply** to apply the changes to the master configuration.

11. Click **Save** to save your changes to the master configuration.
12. Click **Log out** on the WebSphere Administrative Console.

13. Restart the WebSphere Portal Express server if you have made any changes.

### 3.4.3 Importing the LTPA key into Domino

To configure SSO on Domino and Sametime, you need to create a Web SSO Configuration document and import the LTPA key into it. Also, you must enable multi-server session-based authentication on all the Domino servers.

Perform the following steps to configure SSO in your Domino and Sametime environment:

1. Make sure the Domino Directory (names.nsf) has been replicated among all the Domino servers and Sametime servers. In our scenario, we do it from our Domino server DOMIDS console by typing the command:

   ```
   rep stids/itsoids names.nsf
   ```

2. Launch Domino Administrator client and log on with the Domino administrator’s ID.

3. Select **File → Open Server** to open the Administration server for the Domino Directory, which is domids/itsoids in our example.

4. Click the **Configurations** tab.

   If you have Sametime installed, the Web SSO configuration document should already exist. Perform the following steps to edit it:
   
   a. In the left navigation pane, expand **Web** and select **Web Server Configurations**.
   
   b. Scroll the scroll bar on the right pane to the top so you can see the Web SSO Configurations section.
   
   c. Select the **Web SSO Configuration for LtpaToken** document.
   
   d. Click **Edit SSO Document**.

   If you do *not* have Sametime installed, perform the following steps to create a new Web SSO configuration document:
   
   a. In the left navigation pane, expand **Server** and select **All Server Documents**.
   
   b. In the right pane, select the Domino server that will participate in the SSO. Choose **Web → Create Web SSO Configuration**.
   
   c. In the Web SSO Configuration document, leave the Configuration Name as LtpaToken. Do *not* enter any content into the Organization field.

5. Verify (or enter if not there already) the SSO domain name in the DNS Domain field. This name must match the SSO domain name entered when you created the WebSphere Portal Express profile (see Figure 3-26 on page 101). In our example, this is rchland.ibm.com. Domino sets this name with a leading period (.) in the Domino Web SSO Configuration document (see Figure 3-37 on page 111).
6. Under the Participating Servers section, type the Domino server names for the servers that reside in your domain in the Domino Server Names field. Use a comma (,) as a separator. Or click the drop-down button to select servers from the address book (see Figure 3-37).

![Figure 3-37 Selecting participating Domino servers in the SSO](image)

7. From the drop-down menu of the **Keys** button, select **Import WebSphere LTPA keys** (Figure 3-38).

![Figure 3-38 Importing the WebSphere LTPA key](image)
8. Click **OK** if a warning message is displayed, stating that the Web SSO configuration has already been initialized, as shown in Figure 3-39.

![Warning message for Web SSO configuration already initialized](image)

**Figure 3-39** Warning message for Web SSO configuration already initialized

9. On the Enter Import File Name window (Figure 3-40), type the path and file name for the LTPA key file. In our example, we exported our key file to the i5/OS integrated file system directory of `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6ids`. We then mapped a network drive to this directory so we can access the `wpx6ids.key`. See Figure 3-36 on page 109. Click **OK**.

![Specifying the path for the LTPA key file](image)

**Figure 3-40** Specifying the path for the LTPA key file

10. When prompted, type the password for the LTPA key and click **OK**. Remember, this is the password you defined in the WebSphere Application Server Administrative Console in the Global security - LTPA panel (see Figure 3-36 on page 109).

11. You should see a message indicating the import was successful, as shown in Figure 3-41. Click **OK**.

![Successfully imported WebSphere LTPA keys](image)

**Figure 3-41** Successfully imported the WebSphere LTPA keys
12. A new section entitled WebSphere Information is displayed in the Web SSO Configuration document. Make sure the LDAP Realm field contains your IDS LDAP host server name and port. In our example, this is rchas10.rchland.ibm.com:389. See Figure 3-42.

![Web SSO Configuration for: LtpaToken](image)

**Figure 3-42 WebSphere Information**

13. Click **Save & Close** to save the Web SSO Configuration document.

14. Perform the steps described in the next section, 3.4.4, “Enabling multi-server session-based authentication in Domino” on page 113.

### 3.4.4 Enabling multi-server session-based authentication in Domino

For each Domino server you added to the Web SSO Configuration document in 3.4.3, “Importing the LTPA key into Domino” on page 110, perform the following steps to enable Multi-server session-based authentication:

**Note:** The Sametime installation program automatically enables multi-server session-based authentication. So for our STIDS server this setting is already completed.

1. From the Domino Administrator client, select the **Configurations** tab.
2. In the left navigation pane, select **Servers → All Server Documents**.
3. From the server list shown in the right pane, select a Domino server and click **Edit Server**.
4. In the Domino server document, select the **Internet Protocols → Domino Web Engine** tabs.
5. Under the Domino Web Engine tab, select **Multiple Servers (SSO)** for the Session authentication field. Select **LtpaToken** for the Web SSO Configuration field. See Figure 3-43.

![Figure 3-43 Enabling multiple server SSO in Domino](image)

6. Click **Save & Close** to save the Domino server document.

7. Repeat the previous steps for each Domino server added to the Web SSO Configuration document Participating Servers list.

8. Replicate the Domino Directory (names.nsf) among all the Domino servers. In our example, we type the command `rep stids/itsoids names.nsf` from the Domino server console.

9. Restart each Domino server involved in the SSO.

10. When you restart your Domino servers, look for the following message in the Domino server console for the Sametime server. You should see that the HTTP Server service shows the following message:

    HTTP Server: Using Web Configuration View

### 3.4.5 Configuring Sametime to use the IDS LDAP settings

At this point, you should have the WebSphere Portal Express server set up and running and have configured SSO between the WebSphere Portal Express and Domino. The next step is to configure your Sametime server to use the IDS LDAP directory settings. The Sametime Contact List portlet works properly only when you set the attribute of the person entry that defines the person’s name according your definitions in your LDAP directory. Perform the following steps:

1. Verify the Sametime server is started successfully:
   - Open a 5250 emulation session and enter the Work with Domino Servers (WRKDOMSVR) command.
   - Find your Sametime server in the list of Domino servers. If it is not started, type option 1 (Start server) in the Option field to start it.
c. Type option 8 (Work console) in the Option field to see the Domino server console messages.

d. You should see the following messages on your console. You might need to press F5 to refresh the display:

   Sametime: All services started successfully
   Sametime: Server startup successful

2. Configure the LDAP settings for Sametime:
   a. Launch a Web browser and enter the URL for the Sametime home page:
      In our example the URL is:
      http://stids.rchland.ibm.com/stcenter.nsf
   b. On the Sametime home page, click **Log in to IBM Lotus Sametime**.
   c. Log on with the Domino server administrator's name.
   d. Click **Administer the server**.
   e. In the left navigation pane, expand **LDAP Directory** and click **Connectivity**.
   f. Verify that the Host name or IP address of the LDAP server field has the value of your LDAP server and the Port field is set to the value you are using. Change the values if necessary according to your environment and click **Update**. See Figure 3-44.

   ![Figure 3-44  Sametime - LDAP Directory - Connectivity](image)

   g. In the left navigation pane, click the **Basics** link.
h. On the LDAP Directory - Basics window, People section (Figure 3-45), enter the following values:

- In the Where to start searching for people field, enter the Parent Distinguished Name of your LDAP users container. In our example, this is:
  
  cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com

- In the Scope for searching for a person field, use the default value of recursive.

- In The attribute of the person field, enter the value of your Naming attribute for your users. In our example, we use cn.

- In The object class used field, enter the value of the object class in which your users are defined in the LDAP directory. In our example, we use inetOrgPerson.

**Note:** The organizationalPerson class also works because it is the parent class of inetOrgPerson.

<table>
<thead>
<tr>
<th>LDAP Directory - Basics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People</strong></td>
</tr>
<tr>
<td>Where to start searching for people (Base object for person entries)</td>
</tr>
<tr>
<td>Scope for searching for a person (The number of levels below the base object, for example, subtree or one level)</td>
</tr>
<tr>
<td>The attribute of the person entry that defines the person's name (for example, cn or mail)</td>
</tr>
<tr>
<td>Attribute used to distinguish between two similar person names</td>
</tr>
<tr>
<td>Attribute of a person entry that defines the person's e-mail address</td>
</tr>
<tr>
<td>The object class used to determine if an entry is a person (for example, organizationalPerson)</td>
</tr>
</tbody>
</table>

*Figure 3-45  Sametime LDAP Directory Basics, People section*
i. On the LDAP Directory - Basics window, Groups section (Figure 3-46), enter the following values:
   - In the Where to start searching for groups field, enter the Parent Distinguished Name of your LDAP groups container. In our example, this is:
     \texttt{cn=groups,dc=rchas10,dc=rchland,dc=ibm,dc=com}
   - In the Scope for searching for groups field, use the default value of \texttt{recursive}.
   - In the Attribute or the group that defines the group name field, enter the value of your Naming attribute of your group. In our example this is \texttt{cn}.
   - In the group object class used field, enter the value of the object class in which your group is defined in the LDAP directory. In our example, we use \texttt{groupOfUniqueNames}.

j. After defining the values for the People and Groups sections, click Update.

![Figure 3-46  Sametime LDAP Directory Basics, Groups section](Image)

k. In our environment, we do not have to change the default values for all other LDAP Directory panels such as Authentication, Searching, and Group Contents. In your environment, you may have to set up some definitions for your LDAP environment.

l. Close your Sametime Administration Web browser session.

m. After updating the definitions made in the Sametime LDAP Directory administration panels, you have to restart the Sametime server to make the changes effective.

### 3.4.6 Verifying SSO between Sametime, Domino, and WebSphere Portal

After you have configured SSO and configured your Sametime server according your to LDAP settings, you can test the operation of SSO between WebSphere Portal Express, Sametime, and Domino. To verify SSO works, perform the following steps:

1. Log on to your WebSphere Portal Express server by typing the URL of the WebSphere Portal Express server. In our example, this is:
   \texttt{http://wpx6ids.rchland.ibm.com/wps/portal}
2. Log on with a user that is defined in your LDAP directory. We use the uid value from our user entry Debra Landon, which is dlandon. You can see the WebSphere Portal Express home page as shown in Figure 3-47. The logged on user is shown in the upper-right corner.

![Figure 3-47 WebSphere Portal Express home page](image)

3. Change the URL in the same Web browser to the home page of your Sametime server (http://<yourSametimeServer>/stcenter.nsf). In our example, this is:

   http://stids.rchland.ibm.com/stcenter.nsf

   As shown in Figure 3-48, you should get the Sametime home page and see that the user you used to access the WebSphere Portal Express server is already logged on to Sametime without providing a user and password for the Sametime server. The name you see in the upper-right corner is the value of the cn for the user entry in the LDAP directory.

![Figure 3-48 Sametime home page](image)
4. Change the URL in the same Web browser to the IBM Domino Directory (http://<yourDominoServer>/names.nsf). In our example, this is:

http://domids.rchland.ibm.com/names.nsf

As shown in Figure 3-49, you should see the Domino Directory (names.nsf) opened in the Web browser without providing logon information to the Domino server.

![Figure 3-49 Accessing the Domino Directory (names.nsf) from a Web browser](image)

3.5 Integrating Domino mail and calendar

In the scenario covered in this chapter, the WebSphere Portal Express server authenticates against an IBM Tivoli Directory Server (IDS LDAP) directory, which is a non-Domino LDAP directory. However, the Lotus Collaborative Services must authenticate against a Domino LDAP directory to get user information such as mail file and mail server names. In this situation, we have a dual directory-type environment where one LDAP directory (IDS LDAP) is used for the WebSphere Portal Express server and another directory (Domino LDAP) is used for Sametime and Domino.

To integrate Domino mail and calendar functions into WebSphere Portal Express in this environment, you have to implement mail auto-detection and provide name mapping between the two directories. This section provides two solutions for doing this:

- **Solution 1:** All customizing is performed in the Domino environment. See 3.5.2, “Solution 1: Synchronizing user names in Domino Person documents” on page 131.

- **Solution 2:** Only the Directory Assistance database is set up in the Domino environment, and all other customizing is performed in the non-Domino (IDS) directory. See 3.5.3, “Solution 2: Using the Domino Directory Assistance database” on page 133.

In general, mail auto-detection is required by the collaboration portlets that provide mail and calendar functions. For more information, see 1.4, “Key technical points for integration” on page 12. The following section “Difficulties when implementing mail auto-detection” on
page 121 provides an overview of the difficulties that must be resolved when implementing mail auto-detection and explains why you need name mapping.

From a performance point of view, solution 1 is faster, but you have to add user information manually in all the Domino Person documents for each of your users, or you can run an agent to populate all the Person documents in the Domino Directory with the distinguished user name used by the WebSphere Portal Express server for logon.

In solution 2, you also have to manually provide user information in one of your LDAP attributes, but the Tivoli Director Integrator software can help you. This tool provides a mechanism to automatically map the names according to the definitions you make in this tool.

Table 3-6 lists the tasks you have to perform for each solution.

<table>
<thead>
<tr>
<th>Task</th>
<th>Solution 1</th>
<th>Solution 2</th>
<th>Considerations</th>
<th>Name mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update the Domino Person documents</td>
<td>Add the IDS LDAP user DN in Domino notation</td>
<td>No</td>
<td>If you use only the Domino Web Access (DWA) portlet, you have another option for implementing mail, which is to use the DWA Redirect database as described in “Configuring the Domino Web Access Redirect database” on page 275.</td>
<td>No</td>
</tr>
<tr>
<td>Domino Redirect database</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory Assistance (DA) database</td>
<td>No</td>
<td>Define Attribute used as Notes DN. In our example, we use the attribute description. See “Setting up the Domino Directory Assistance database” on page 135.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start the LDAP service on Domino</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update the WebSphere Portal Express CSEnvironment.properties file</td>
<td>Define the Domino LDAP Host server name - see “Changing the CSEnvironment.proper ties file” on page 122</td>
<td>Define the Domino LDAP Host server name - see “Changing the CSEnvironment.properties file” on page 122.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Difficulties when implementing mail auto-detection

After signing on to the WebSphere Portal Express server in an environment where the authorization directory server is a non-Domino LDAP directory, the LTPA cookie contains the LDAP identity (from your IDS LDAP server) for the logged on user, and at that time, no information about the mail file for this user is available.

For example, when the IDS LDAP user Ursula Althoff logs on to the WebSphere Portal Express server, the LTPA cookie has the LDAP identity of uid=ualthoff,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com. When this user switches to a portlet that requires mail file information - for example, the Domino Web Access (DWA) portlet - to get her mail, the LTPA token is sent via HTTP to the Domino Web Access server. The Domino server then searches the Domino Directory to verify her identity (authorization), and based on her identity, the server decides whether to allow her to use of Domino Web Access resources (authorization). However, uid=ualthoff,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com does not exist in the Domino Directory when the authorization directory server is an non-Domino LDAP directory.

Table 3-7 lists examples of the different identity information about the IDS LDAP directory and the Domino Directory (names.nsf). If Domino LDAP is activated, Domino LDAP identity looks different in comparison to the IDS LDAP identity. In addition to the possibility that the names of the users in the two LDAPs can be different, consider also the different notation of the LDAP identities.

<table>
<thead>
<tr>
<th>Task</th>
<th>Solution 1</th>
<th>Solution 2</th>
<th>Considerations</th>
<th>Name mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend the Domino LDAP schema attribute type selection for anonymous LDAP queries</td>
<td>No</td>
<td>Yes. See “Extending the Domino LDAP schema attribute type selection” on page 140.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide information in the non-Domino LDAP (IDS)</td>
<td>No</td>
<td>Fill in the Domino user DN in LDAP notation for every user in the attribute you defined in the Directory Assistance (DA) database. For our example, we use the description field.</td>
<td>The uid value has to be the same in the IDS LDAP as the ShortName in the Domino Person document.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-7 Identities on IDS LDAP and Domino LDAP

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>uid=ualthoff,cn=users, dc=rchas10,dc=rchland,dc=ibm,dc=com</td>
<td>Ursula Althoff/itsoids</td>
<td>cn=Ursula Althoff/o=itsoids</td>
<td>uid=ualthoff/cn=users/dc=rchas10/dc=rchland/dc=ibm/dc=com</td>
<td></td>
</tr>
<tr>
<td>uid=madan,cn=users, dc=rchas10,dc=rchland,dc=ibm,dc=com</td>
<td>Marcela Adan/itsoids</td>
<td>cn=Marcela Adan/o=itsoids</td>
<td>uid=madan/cn=users/dc=rchas10/dc=rchland/dc=ibm/dc=com</td>
<td></td>
</tr>
</tbody>
</table>
You have to change the WebSphere CSEnvironment.properties file on the WebSphere Portal Express server for both of our solutions. This is because the Lotus Collaborative Services has to know the LDAP server to retrieve the user information needed to support collaborative portlet features.

### Changing the CSEnvironment.properties file

You have to define the Domino LDAP server host name in the WebSphere CSEnvironment.properties file. We also recommend that you set up a binded user instead of enabling anonymous access to the Domino LDAP. This is because the binded user solution is more consistent with the way WebSphere Portal Express accesses LDAP directories.

Perform the following steps to define the Domino LDAP server and the binded user in the CSEnvironment.properties file:

1. Stop the WebSphere Portal Express server.
2. Open the CSEnvironment.properties file in a text editor. For example, when using iSeries Navigator, you can right-click the file name and select **Edit**. You can find this file in the following i5/OS integrated file system directory:

   ```
   portal_server_root_user/shared/app/config
   ```

   In our example, the directory is:

   ```
   /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6ids/PortalServer/shared/app/config
   ```

   **Tip:** You should make a backup copy of this file before making any changes.

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>uid=dlandon,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com</td>
<td>Debra Landon/itsoids</td>
<td>cn=Debra Landon/o=itsoids</td>
<td>cn=Debra Landon,o=itsoids</td>
<td>uid=dlandon/cn=users/dc=rchas10/dc=rchland/dc=ibm/dc=com</td>
</tr>
</tbody>
</table>
3. In the CSEnvironment.properties file, locate the DOMINO DIRECTORY properties section as shown in Figure 3-50.

```properties
# DOMINO DIRECTORY properties
# (LDAP server)
# Important:
# Should always point to a Domino Server.
# Leave enabled flag as true.
# Use the custom_ldap_* settings to point to a any LDAP Server to
# get user information.

CS_SERVER_DOMINO_DIRECTORY.enabled=false
CS_SERVER_DOMINO_DIRECTORY_1.hostname=my.server.com
CS_SERVER_DOMINO_DIRECTORY_1.port=389
CS_SERVER_DOMINO_DIRECTORY_1.ssl=false
CS_SERVER_DOMINO_DIRECTORY_1.anonymous=true
```

Figure 3-50  CSEnvironment. properties file, Domino Directory section before updating

4. Change the CS_SERVER_DOMINO_DIRECTORY.enabled line to true. Change the CS_SERVER_DOMINO_DIRECTORY.hostname line to the Domino server host name. For our example, this is domids.rchland.ibm.com. See Figure 3-51.

```properties
# DOMINO DIRECTORY properties
# (LDAP server)
# Important:
# Should always point to a Domino Server.
# Leave enabled flag as true.
# Use the custom_ldap_* settings to point to a any LDAP Server to
# get user information.

CS_SERVER_DOMINO_DIRECTORY.enabled=true
CS_SERVER_DOMINO_DIRECTORY_1.hostname=domids.rchland.ibm.com
CS_SERVER_DOMINO_DIRECTORY_1.port=389
CS_SERVER_DOMINO_DIRECTORY_1.ssl=false
CS_SERVER_DOMINO_DIRECTORY_1.anonymous=true
```

Figure 3-51  CSEnvironment. properties file, Domino Directory section after updating
5. To define the binded user, locate the Add Default IIOP/SSL Port section as shown in Figure 3-52.

```
# Add Default IIOP/SSL Port
CS_SERVER_DOMINO_DIRECTORY_1.iiopport=63148

# Optional LDAP User credential overrides
# default - uses Portal credentials or anonymous
# Use tool PropFileEncoderPassword.bat to encrypt the password and copy
# the encrypted password to this file.
#CS_SERVER_DOMINO_DIRECTORY_1.userid=username
#CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=pwd
```

Figure 3-52  CSEnvironment. properties file, IIOP/SSL Port section before updating

6. Remove the comment tag (#) from the beginning of the line that contains:

   CS_SERVER_DOMINO_DIRECTORY_1.userid=username

7. At the end of the line, add a user ID for a user who has appropriate access to the Domino LDAP directory. In our example, we use the administrator of our Domino Directory:

   cn=admin,o=itsoids

8. Remove the comment tag (#) from the beginning of the line that contains:

   CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=pwd

9. Perform the following steps to get the encrypted password:

   a. Create a text file on your Windows workstation. For example, you can launch Notepad to do so.

   b. Enter a line such as the following:

      admin=<Domino user ID password>

      In our example, the line is:

      admin=itso4all

   c. Save the file as admin.txt and close it.

   d. Copy the file to i5/OS the app_server_root/bin directory by using a mapped network drive to your i5/OS integrated file system:

      /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/youProfileName/bin

      In our example, this is:

      /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6ids/bin

   e. Launch QShell from a 5250 comment prompt by typing the following command:

      strqsh

   f. Go to the app_server_root/bin directory using the following cd command:

      cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/youProfileName/bin

      In our example, this is:

      cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6ids/bin

   g. Run the following PropFilePasswordEncoder command to encrypt the password:

      PropFilePasswordEncoder <file name> <property name list>
In our example, the command is:

```
PropFilePasswordEncoder admin.txt admin
```

h. Use the `cat` command to display the contents of the admin.txt file. The password should be encrypted by the PropFilePasswordEncoder command. See Figure 3-53.

```
Figure 3-53 Using the PropFilePasswordEncoder to encrypt the password
```

i. Now you can copy the encrypted password to the CSEnvironment.properties file.

10. Go back to the CSEnvironment.properties file and paste the encrypted password after:

```
CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=
```

The line looks like:

```
CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd={xor}NissMGs+MzM\=
```

See Figure 3-54.

```
Figure 3-54 CSEnvironment.properties file, IIOP/SSL Port section after updating
```
11. Save and close the CSEnvironment.properties file.

12. Start the WebSphere Portal Express server.

**Summary of required Domino server configuration**

To provide support for the collaboration portlets such as mail, calendar, and Lotus Notes View, certain services are required on the Domino servers:

- To provide support for mail-related portlets, the HTTP service must be running on each Domino mail server.
- To provide support for the Lotus Notes View portlet, the HTTP and DIIOP services must be running on each Domino server.
- To support mail auto-detection, the LDAP service must be running on one Domino server. Typically this is the administrative server for the Domino Directory. It is not necessary to enable LDAP on all the Domino servers.

In our scenario, the Domino server domids/itsoids is both the administrative server and mail server. Therefore, we need to enable the LDAP, HTTP, and DIIOP services on this server. This was done when we created the Domino server with the CFGDOMSRV CL command using the parameters WEB and DIRSRV. See Table 3-2 on page 78.

Another option for validation is that you can inspect and, if required, change the notes.ini file of the Domino server. See “Validating and changing the Domino server notes.ini file” on page 130.

For your convenience, we provide here the steps for enabling the different services if they are not already enabled on your Domino server. All these services are defined in the Domino server document. Most of them have been modified already in the steps you have done so far.

Perform the following steps to open the Domino server document:

1. To open the Domino server document from your Domino Administrator client, click the **Configuration** tab and expand the **Server** view on the left navigation panel.

2. Click the **All Server Documents** view and then select your Domino server. In our example this is domids/itsoids.

3. Verify the HTTP service is enabled:
   
   a. In the Domino server document, click the **Internet Protocols → HTTP** tabs.
   
   b. Ensure the Host name(s) field is set properly. In our example, it is set to DOMIDS.RCHLAND.IBM.COM.
c. Ensure the Allow HTTP clients to browse databases field is set to Yes, as shown in Figure 3-55.

![Figure 3-55 Domino server document, HTTP settings](image)

4. Verify the Domino Web Engine settings:
   a. Select the Internet Protocols → Domino Web Engine tabs.
   b. Verify the Session authentication field is set to Multiple Servers (SSO) and the Web SSO Configuration field is set to LtpaToken as shown in Figure 3-56.

![Figure 3-56 Domino server document, Domino Web Engine settings](image)
5. Allow LotusScript/Java agents settings:
   a. Click the **Security** tab.
   b. Under the Programmability Restrictions section, verify the Run restricted LotusScript/Java agents field is set to *. See Figure 3-57.

   ![Figure 3-57 Allowing LotusScript/Java agents](image)

6. Verify Notes Network Ports:
   a. Click the **Ports → Notes Network Ports** tabs.
   b. Verify the Net Address field shows the correct name for your Domino server. In our example, it is **DOMIDS.RCHLAND.IBM.COM** as shown in Figure 3-58.

   ![Figure 3-58 Domino server document, Notes Network Ports tab](image)
7. Verify the Internet TCP/IP port status:
   a. Select the **Ports → Internet Ports → Web** tabs.
   b. Verify the TCP/IP port status field is set to **Enabled** as shown in Figure 3-59.

![Figure 3-59](image1)

8. Verify the LDAP TCP/IP port status:
   a. Select the **Ports → Internet Ports → Directory** tabs.
   b. Verify the TCP/IP port status field is set to **Enabled** as shown in Figure 3-60.

![Figure 3-60](image2)
9. Verify the DIIOP TCP/IP port status:
   a. Click the Ports → Internet Ports → DIIOP tabs.
   b. Verify the TCP/IP port status field is set to Enabled as shown in Figure 3-61.

![Figure 3-61 Domino server document, Internet ports, DIIOP tab](image)

**Validating and changing the Domino server notes.ini file**

Another option for validating that all the required Domino services are started is that you can inspect and, if required, change the Domino server’s notes.ini file. Perform the following steps to verify the LDAP, HTTP, and DIIOP tasks are automatically started on the Domino server:

1. Open the notes.ini file of the Domino server in the domino_server_root directory. Or from a 5250 emulation session, type the Work with Domino Servers (WRKDOMSVR) command and press Enter. On the Work with Domino Servers display, type option 13 (Edit notes.ini) next to the Domino server where you want to open the notes.ini file.
2. Locate the `ServerTasks=` entry as shown in Figure 3-62. The parameters on the `ServerTasks` line defines the services that are started by the Domino server. In our example, we are validating whether the DIIOP, HTTP, and LDAP services are defined. If a required service is not listed, add it to the `ServerTasks` line. Save and close the file.

```plaintext
Edit File: /domino/domids/data/NOTES.INI
Record :  1  of      78 by  10  Column :  1   98 by 126
Control :
**************Beginning of data**************
[Notes]
Directory=/domino/domids/data
KitType=2
NPN=1
UNICODE_DISPLAY=1
FaultRecovery_Build=Release 7.0.2FP1
SHARED_MAIL=0
DisableLDAPOnAdmin=1
Passthru_LogLevel=0
Console_LogLevel=2
DefaultMailTemplate=mail7.ntf
Preferences=32
ServerTasks=Update,HTTP,AMgr,AdminP,CalConn,Replica,Router,Sched,Stats,RnRmgr,DIIOP,LDAP
ServerTasksAt1=Catalog,Design
ServerTasksAt2=UpdAll
ServerTasksAt3=Object Info -Full
ServerTasksAt5=Statlog

F2=Save  F3=Save/Exit  F12=Exit  F15=Services  F16=Repeat find  F17=Repeat change
F19=Left  F20=Right
```

Figure 3-62  Domino server notes.ini file

3.5.2 Solution 1: Synchronizing user names in Domino Person documents

The solution 1 scenario (see 3.5, “Integrating Domino mail and calendar” on page 119) describes the steps that are required to synchronize user information between a Domino and a non-Domino LDAP (IDS in our example). This is accomplished by manually adding the non-Domino LDAP user entity definitions to the Domino Person documents. You can also implement an agent to populate all the Person documents in the Domino Directory with the distinguished user name of the IDS LDAP information.

The User Name field of the Person document is a multi-value field. It can contain many variations of the user’s name. As a best practice, each Person document entry should be unique in the Domino Directory. When a match is found against one of the entries in this field, Domino maps the identity to the first entry in the field for the purpose of authorization.

To add the non-Domino LDAP (IDS) user DN to the Person document in the Domino Directory perform the following steps:

1. From the Domino Administrative client, select the People & Groups tab of your Domino mail server (or the administrative server). In our scenario, Domino server domids/itsoids is both the administrative server and mail server.
2. Under **Domino Directories** → <your_organization> **Directory** → **People** → **by Organization** view, you see your Domino Person documents as shown in Figure 3-63.

3. Open the Domino Person document for every user that should have access to the WebSphere Portal Express server and click **Edit Person**. Type the IDS LDAP user DN in Domino notation (see column 5 of Table 3-7 on page 121) into the User name field of the Person document.

For example, if the WebSphere Portal Express user directory is IBM Directory Server (IDS), and you have a user's DN from this IDS:

uid=ualthoff, cn=users, dc=rchas10, dc=rchland, dc=ibm, dc=com

Then you must type the following in the User name field of the Person document for user Ursula Althoff:

uid=ualthoff/cn=users/dc=rchas10/dc=rchland/dc=ibm/dc=com

In other words, you add the user's IDS LDAP DN after the second line of the User Name field and replace the commas of the DN with a forward slash (/). See Figure 3-64. Click **Save & Close**.
3.5.3 Solution 2: Using the Domino Directory Assistance database

In solution 2, for collaboration integration when the LDAP directory that WebSphere Portal Express uses is an non-Domino LDAP, we use the following approach:

- The administrator of the LDAP server chooses which LDAP attribute to populate in the IDS LDAP directory with the Notes DN. The attribute can be one that already exists in the non-Domino (IDS) LDAP schema, or the administrator can choose to extend the LDAP schema by creating a new attribute. Either way, the attribute must be of type DN syntax. For more information about attribute syntax types, refer to RFC 2252, “Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions”:
  
  http://www.faqs.org/rfcs/rfc2252.html

After you decide which attribute to use in the IDS LDAP directory, you must add the value of the Notes DN (Domino LDAP identity, see Table 3-7 on page 121 in column 3) in this attribute for each identity (user) that requires SSO for Domino, using LDAP-style syntax (that is, Domino-formatted identity for non-Domino LDAP, see Table 3-7 on page 121, column 4).

In our scenario, we choose to use the description attribute in our IDS LDAP, which is already part of the inetOrgPerson person schema in the LDAP directory. We add the Notes DN for our users as a value of this description attribute. For example, we define

\[ cn=Ursula Althoff, o=itsoids \]

in the description attribute for our user entry

\[ uid=ualthoff, dc=rchas10, dc=rchland, dc=ibm, dc=com \]

- We configured our Domino Directory with Directory Assistance. Directory Assistance is configured with the Attribute to be used as Notes Distinguished Name feature, where we define the name of the attribute in our LDAP directory that holds the value of the Notes DN for the user. In our example, it is the description attribute.
Figure 3-65 shows the general flow of control for Ursula Althoff’s request as it progresses through the SSO environment using this approach.

The general flow of control for Ursula Althoff’s request as it progresses through the SSO environment is as follows. The numbers in this list correspond to the numbers in Figure 3-65.

1. Already authenticated user Ursula accesses portlets that access mail or calendar functions. The LTPA token including the DN of the authenticated user has the value of uid=ualthoff,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com.

2. The collaboration services reads the information defined in the CSEnvironment.properties file.

3. The Domino server extracts the user name from the LTPA token. Collaboration services does a lookup in the Domino Directory because CSEnvironment.properties points to the Domino LDAP directory.

4. The Domino Directory is configured with Directory Assistance and the Attribute to be used as Notes Distinguished Name field is set to the description field. Directory Assistance points to the IDS LDAP directory.

5. An LDAP search query to the IDS LDAP is issued for uid=ualthoff with a request to return the attribute description content (which contains the Notes DN). The search is performed with:

   BaseDN: cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com
   Filter: uid=ualthoff
   attrs to return: "description"
6. The IDS directory returns a match with the description attribute value containing the Notes DN with the value cn=Ursula Althoff,o=itsoids.

7. Because the value of description is returned, uid=ualthoff,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com in the LTPA token is mapped to the Notes distinguished name cn=Ursula Althoff,o=itsoids that is present on the mail file ACL. Ursula Althoff is now allowed to access to her mail file.

8. The mail or calendar portlets can now return the appropriate information to the user's Web browser.

Using this approach, you perform the steps described in the Solution 2 column in Table 3-6 on page 120. The steps are covered in detail in the following sections.

**Setting up the Domino Directory Assistance database**

Directory Assistance is a feature a Domino server can use to look up information in a directory other than the local primary Domino Directory (names.nsf). When Directory Assistance is defined, the Domino server can search one or more LDAP directories after it searches the Domino Directory for user authentication.

In general, you can set up Directory Assistance for a remote LDAP directory. A remote LDAP directory can be any remote LDAP-compliant directory, either one on a foreign LDAP directory server or one on another Domino server that runs the LDAP service.

**Changing and verifying settings in the Directory Assistance database**

During the configuration of your Sametime server as discussed in 3.2.4, “Configuring the Sametime server” on page 88, Directory Assistance is already configured for this Sametime server. You can deploy this configuration to all Domino servers that are hosting Domino applications.

**Note:** In the case where a Directory Assistance database is not created in your environment, you can create the Directory Assistance database using a Lotus Notes client by selecting File → Database → New. Select a Domino server, select Directory Assistance (7) as the template, and name the database da.nsf. Then create a Directory Assistance document and fill in all fields manually according to the steps that follow.
To verify the settings in an existing Directory Assistance database, perform the following steps:

1. Launch the Lotus Notes client and log on with the Domino server administrator’s ID.
2. Open the existing Directory Assistance database (da.nsf) on the Sametime server:
   a. Select the pull-down menu options of File → Database → Open.
   b. On the Open Database window (Figure 3-66), specify the Sametime server’s name in the Server field. In our example, the Sametime Server name is STIDS/ITSOIDS. Verify the Filename field shows da.nsf. Click Open.

![Figure 3-66 Opening the Directory Assistance database](image)

3. Select the only document listed in the right plane and click Edit Directory Assistance. See Figure 3-67.

![Figure 3-67 Directory Assistance database](image)
4. In the Directory Assistance document, leave all the settings on the Basics tab as shown in Figure 3-68.

![Figure 3-68 Directory Assistance document, Basics tab](image1)

5. On the Naming Contexts (Rules) tab, make sure Trusted for Credentials in the first row is set to Yes as shown in Figure 3-69.

![Figure 3-69 Directory Assistance document, Naming Contexts (Rules) tab](image2)
6. On the LDAP tab (Figure 3-70):
   a. Verify the Hostname field is set to the fully qualified host name of your IDS LDAP server. In our example, it is rchas10.rchland.ibm.com.
   b. In the Optional Authentication Credential section, verify the Username and Password is correct. In our example, we used the IDS LDAP administrator of cn=administrator and the corresponding password.
   c. Verify Base DN for search. This is the Parent DN of your LDAP users container. In our example, it is cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com.
   d. Verify Type of search filter to use is **Standard LDAP**.

![Directory Assistance - LDAP tab](image)

7. After verify and changing the content of all three tabs of the Directory Assistance document, click **Save & Close**.

**Deploying the Directory Assistance database to other Domino servers**

After verifying all the settings in the Directory Assistance database, you need to deploy the database to all Domino servers that host Domino application databases that will be accessed from the WebSphere Portal Express server. In our example, we used the Directory Assistance database to enable mail auto-detection, so our Domino server, DOMIDS, requires this database.

You can deploy the Directory Assistance database to other Domino servers by creating a new replica for da.nsf on all the Domino servers. Perform the following steps:

1. Launch the Lotus Notes client and log on with the Domino server administrator’s ID.
2. Open the existing Directory Assistance database (da.nsf) on the Sametime server.
3. Select the pull-down menu options of **File → Replication → New Replica**.
4. On the Create Replica For Database Directory Assistance (7) window (Figure 3-71), specify the destination Domino server name. In our example, we specify domids/itsids. Click OK.

![Figure 3-71 Creating a new replica for da.nsf](image)

5. Repeat the previous replication steps for each Domino server in your environment where the Directory Assistance database is required.

**Important:** After creating replicas of the Directory Assistance database on all the Domino servers, whenever you make changes in this database, make sure you replicate the changes to all servers.

**Enabling Directory Assistance on the Domino servers**

Once the Directory Assistance database is deployed to each Domino server, you need to enable Directory Assistance on the servers. Perform the following steps:

1. Launch the Domino Administrator client and log on with the Domino administrator’s ID.
2. Select File → Open Server to open the administration server for the Domino Directory. In our example, the administration Domino server is domids/itsoids.
3. Select the Configuration tab.
4. On the left navigation pane, select Server → All Server Documents.
5. On the right pane, select the Domino server for which you want to enable Directory Assistance. In our example, we select domids/itsoids and click Edit Server. See Figure 3-72.

![Figure 3-72 Editing the Domino server document](image)
6. In the Domino server document, Basics tab, type `da.nsf` in the Directory Assistance database name field as shown in Figure 3-73.

![Figure 3-73 Enabling Directory Assistance in the Domino server document](image)

7. Click **Save & Close**.

8. Repeat the previous steps for each Domino server that requires Directory Assistance enabled.

9. Replicate the Domino Directory (names.nsf) from the Administration server to all Domino servers in the domain to propagate the changes to all servers.

**Extending the Domino LDAP schema attribute type selection**

In addition to verifying the CSEnvironment.properties as described in “Changing the CSEnvironment.properties file” on page 122, you also have to add Domino LDAP schema attributes to enable anonymous access to the Domino LDAP directory. You need to do this because some attributes, such as the HTTP-HostName, do not display in the default LDAP schema of Domino for anonymous users.
To extend the Domino LDAP schema attribute type selection for anonymous LDAP queries in the Domino server document, perform the following steps:

1. From the Domino Administrator client, select the **Configuration** tab and select **Server → Configurations**.
2. Click the **Edit Configuration** button to edit the All Servers document. See Figure 3-74.

![Figure 3-74 Editing the All Servers document](image)

3. In the Configuration Settings document, Basics tab, make sure the check box for the Use these settings as the default settings for all servers field is checked. See Figure 3-75.

![Figure 3-75 Configuration Settings document, Basics tab](image)

4. Select the **LDAP** tab to display the LDAP configuration settings. Then click the **Select Attribute Types** button. See Figure 3-76.

![Figure 3-76 Configuration Settings document, LDAP tab](image)
5. On the LDAP Attribute Type Selection window, select dominoServer from the drop-down list in the Object Classes selection field and then click the Display Attributes button.

6. From the Selectable Attribute Types list, select the HTTP-HostName and the Net-Addresses attributes and click the Add>> button to add these attributes to the Queriable Attribute Types list box. See Figure 3-77. Click OK.

![Figure 3-77 Adding Domino server attributes for anonymous user queries through LDAP](image)

7. At this point, you have to add two other attributes for the dominoPerson object class. In the LDAP Attribute Type Selection window, select dominoPerson from the Object Classes selection drop-down list and then click the Display Attributes button.
8. From the Selectable Attribute Types selection list, select the **MailFile** and the **MailServer** attributes and click the **Add>>** button to add these attributes to the Queriable Attribute Types list box. See Figure 3-78. Click **OK**.

![Figure 3-78  Adding Domino person attributes for anonymous user queries through LDAP](image)

9. At this point, you are back in the Configuration Settings document. Verify the LDAP Attribute Types list contains all four attributes you added in the previous steps. This is required so anonymous users can query field content for the LDAP attribute values you added in the previous steps.

10. Keep all the other default LDAP settings in Configuration Settings document and click **Save and Close** to close the Configuration Settings document.

11. From the DOMIDS Domino server console, type the following command to reload the LDAP schema:

    ```
    tell ldap reloadschema
    ```

### 3.5.4 Verifying mail auto-detection

At this point, you can test your WebSphere Portal Express server and integrated collaboration environment. Users who will authenticate on the portal using the IDS LDAP directory should see their mail and calendar information in the collaboration portlets without providing additional user information.

The verification steps described in this section use the solution 2 implementation (see 3.5, “Integrating Domino mail and calendar” on page 119 for a description of the two solutions).
The solution 1 verification works in the same way, except the implementation completed before the verification is different. Perform the following steps:

1. From your Web browser, access the WebSphere Portal Express server. For our example, we use the following URL:
   http://wp6ids.rchland.ibm.com/wps/myportal
2. Log on to the WebSphere Portal Express server with a user identity that is in the IDS LDAP Directory. For our example, we use the user ualthoff.
3. Once you are signed on, select the **Collaboration** tab.
4. The Domino Web Access portlet shows the mail for our user Ursula Althoff. Remember this user accessed the portal using her portal account of ualthoff. See Figure 3-79.

**Note:** We added the Domino Web Access portlet to the Collaboration default site previously as discussed in 3.9, “Adding additional portlets to a WebSphere Portal page” on page 191.

---

![Figure 3-79 Domino Web Access portlet with mail for user Ursula Althoff](image-url)
5. The Common Mail portlet, which is assigned to the Collaboration page of WebSphere Portal Express Version 6 by default, shows the same mail for the user Ursula Althoff - see Figure 3-80.

![Common Mail portlet](image)

**Figure 3-80  Common Mail portlet**

6. The Common Calendar portlet, which is assigned to the Collaboration page of WebSphere Portal Express Version 6 by default, shows the entries in the Calendar for Ursula Althoff - see Figure 3-81.

![Common Calendar portlet](image)

**Figure 3-81  Common Calendar portlet**

### 3.5.5 Verifying the Sametime portlets

At this point, you can verify that the Sametime Contact List, the People Finder, and people awareness are handled correctly. These three functions are provided by the Sametime server and the appropriate collaborative portlets. For more information about Sametime integration and people awareness, see 4.6, “Sametime integration” on page 225.
These three functions do not need additional configuration; you have already completed the required configuration in these sections:

- 3.2.4, “Configuring the Sametime server” on page 88.
- 3.4, “Configuring SSO between Domino and WebSphere Portal” on page 105.
- 3.4.5, “Configuring Sametime to use the IDS LDAP settings” on page 114.

The verification described in this section is performed using the solution 2 implementation. The solution 1 verification works in the same way, except the implementation completed before the verification is different.

To begin, perform the steps described in 3.5.4, “Verifying mail auto-detection” on page 143 to log on to the WebSphere Portal Express server and access the Collaboration page. You should see a window similar to that in the Figure 3-79 on page 144. In addition to showing the Domino Web Access portlet, this figure also shows the People Finder and Sametime Contact List portlets. Both of these portlets are shown by default on the IntranetJumpStart → Collaboration site in WebSphere Portal Express Version 6.

Perform the following steps to use the People Finder portlet to search for a member by name:

1. In the Search by selection list, select Name.
2. In the Search for field, enter a name to search for and click Search. In our example shown in Figure 3-82, we entered Adan.
   The user Adan is found and her current status is offline.
3. Click the user link and select Add to Sametime List (see Figure 3-82).
4. On the Add to Sametime List window (Figure 3-83), select a group to add the user to. In our example, we selected an existing group of **ITSO Portal Project Members**. Click **OK**.

![Figure 3-83 Adding the user to a Sametime contact list](image)

5. As shown in Figure 3-84, the Sametime Contact List now shows user Marcela Adan in the list, and her status is now online. In addition, the Common Mail portlet displays an icon before the name of user Marcela Adan as well as before the names of other users. This icon indicates whether or not the users are currently online.

![Figure 3-84 Sametime Contact List with new user entry and Common Mail portlet](image)

6. You can also verify whether the chat functions that the Sametime server supports are working properly. The example shown in Figure 3-85 on page 148 shows that user Joing Xin Bai has user Ursula Althoff added to her Sametime Contact List inside the workgroup. User Ursula Althoff is currently online.

Joing Xin Bai selects the **Ursula Althoff** person link, and from the context menu selects **Chat**.
Jiong Xin Bai views the chat panel as shown in the upper-left corner of Figure 3-85. Here Jiong Xin types her message text to Ursula Althoff.

Ursula Althoff views a chat panel, as shown under the Jiong Xin chat panel in Figure 3-85, where she can answer Jiong Xin.

Figure 3-85   Sametime chat

3.6 IBM Tivoli Directory Server Web Administration tool

You can administrate the IBM Directory Server using the IBM Tivoli Directory Server Web Administration Tool. This Web administration console allows you to:

► Add or change the list of directory servers that can be administrated.
► Change Web administration console attributes.
► Administer a directory server.

The IBM Tivoli Directory Server Web Administration Tool runs as a Java application inside the system application server instance, which is accessed by the HTTP ADMIN server instance.

The prerequisite to working with the IBM Tivoli Directory Server Web Administration Tool is installation of the IBM WebSphere Application Server 6.0 (5733-W60 Base or Express option). We assume you have already completed this step. Refer to the IBM Redpaper Installing and Configuring WebSphere Portal Express V6 on i5/OS, REDP-4303, for details on how to install IBM WebSphere Application Server.
Before you can use the IBM Tivoli Directory Server Web Administration Tool for administration of a directory server, you have to complete the following configuration steps:

- 3.6.1, “Enabling the system application server instance” on page 149
- 3.6.2, “Configuring the IBM Tivoli Directory Server Web Administration Tool” on page 150

In section 3.6.3, “Using the IBM Tivoli Directory Server Web Administration Tool” on page 153, you find information about how to manage entries in your directory server.

3.6.1 Enabling the system application server instance

Before you can access the IBM Tivoli Directory Server Web Administration Tool, you must ensure that the system application server instance is always started when the HTTP ADMIN server instance is started. To do this, perform the following steps:

1. Start the HTTP ADMIN server instance by doing one of the following:
   - In iSeries Navigator, click Network → Servers → TCP/IP, right-click HTTP Administration, and select Start.
   - From a 5250 emulation session command line, enter the following Start TCP/IP Server (STRTCPSVR) command:

     ```
     STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
     ```

2. Log on to the i5/OS Tasks menu from a Web browser with the following URL:

   ```
   http://<your_server>:2001
   ```

   Where `<your_server>` is the TCP/IP host name of your System i machine and 2001 is IBM Web Administration for i5/OS port. In our example, the URL to access the i5/OS Tasks menu is:

   ```
   http://rchas10:2001
   ```

3. When prompted, sign on with an i5/OS user profile and password to connect to your System i machine.

4. On the i5/OS Tasks menu, click IBM Web Administration for i5/OS.

5. From the IBM Web Administration for i5/OS page, click the Manage tab and then the HTTP Servers tab. Make sure ADMIN - Apache is selected in the Server drop-down list and that Include /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf is selected in the Server area drop-down list as shown in Figure 3-86.

7. Set Start the system application server instance when the ‘Admin’ server is started: to **Yes** and set Stop the system application server instance when the ‘Admin’ server is stopped: to **Yes**. Click **OK**. See Figure 3-87.

![General Server Configuration](image)

**Figure 3-87**  HTTP ADMIN server, General Server Configuration

8. Restart the HTTP ADMIN server instance by clicking the restart button (the second green icon under HTTP Servers as shown in Figure 3-88).

![Restarting the HTTP ADMIN server](image)

**Figure 3-88**  Restarting the HTTP ADMIN server

### 3.6.2 Configuring the IBM Tivoli Directory Server Web Administration Tool

You can change the Web administration console attributes such as the default name of the console administrator (superadmin) and the default password (secret) to the values you want to work with. The Console Administration function of the IBM Tivoli Directory Server Web Administration Tool also enables you to add or change the list of directory servers that can be administered.

Perform the following steps to change the Web administration console attributes and to add the directory server you want to manage with the IBM Tivoli Directory Server Web Administration Tool:

1. Log on to the IBM Tivoli Directory Server Web Administration Tool in one of the two possible ways:
   - From iSeries Navigator, select your System i machine and click **Network → Servers → TCP/IP**, right-click **IBM Directory Server** and select **Server Administration**.
   - Log on to the i5/OS Tasks menu from a Web browser with the following URL:
     
     `http://<your_server>:2001`
Where <your_server> is the TCP/IP host name of your System i machine and 2001 is IBM Web Administration for i5/OS port. In our example, the URL to access the i5/OS Tasks menu is:

http://rchas10:2001

When prompted, sign on with an i5/OS user profile and password to connect to your System i machine. On the i5/OS Tasks menu, select IBM Directory Server for i5/OS.

2. The IBM Tivoli Directory Server Web Administration Tool Login page should appear. In the LDAP Hostname field select Console Admin. Type superadmin for the username and secret for the password (these are the default values). Click Login. See Figure 3-89.

3. If you want to change the default console administrator from superadmin to another value (we use administrator in our example), perform the following steps:

   a. From the left navigation pane of the console administration Introduction page, expand Console administration and select Change console administrator login. See Figure 3-90.
4. On the Console administrator window, enter the value you want for the console
administrator logon name in the Console administrator login field. (For our example, we
enter administrator.) Enter the current password (secret) in the Current password field
and click OK. See Figure 3-91.

![Console administrator login](image)

Figure 3-91  Changing the console administrator login name

5. Back on the console administrator Introduction page, you can also change the default
password of the console administrator from secret to another value. Select Change
console administrator password. On the Console administrator window, enter the
current password (secret) and the new password you want to use. Click OK. See
Figure 3-92.

![Console administrator](image)

Figure 3-92  Changing the console administrator password

6. Back on the console administrator Introduction page, you can add the directory server you
want to manage with the IBM Tivoli Directory Server Web Administration Tool by
performing the following steps:

- In the left navigation pane, select Manage console servers. On the Manage console
  servers panel, click Add.
b. On the Add server panel (Figure 3-93), type the name of the directory server (the TCP/IP host/domain name of your LDAP server) in the Hostname field and the corresponding LDAP port (default is 389). You can leave the other values at the default. Click OK.

![Console administrator](image)

**Figure 3-93  Adding a directory server**

c. Click OK in response to the confirmation message.

d. The directory server you just added appears in the Manage console servers panel as shown in Figure 3-94. Click Close.

![Console administrator](image)

**Figure 3-94  Managing console servers list**

7. Click Logout to exit the IBM Tivoli Directory Server Web Administration Tool.

### 3.6.3 Using the IBM Tivoli Directory Server Web Administration Tool

As mentioned in 3.6, “IBM Tivoli Directory Server Web Administration tool” on page 148, you can use the IBM Tivoli Directory Server Web Administration Tool to manage any entry in the IBM Directory Server for i5/OS LDAP directory.

**Note:** If you configure a new IDS Directory server for WebSphere Portal Express authentication, we recommend you manage entries after the WebSphere Portal Express server configuration is completed with the i5/OS Create WebSphere Portal wizard. This is because the wizard automatically creates all the required containers, groups, and portal administration users.
Starting the IBM Tivoli Directory Server Web Administration Tool

To start the IBM Tivoli Directory Server Web Administration Tool, perform the following steps:

1. Ensure the HTTP ADMIN server instance is started. See step 1 in section 3.6.1, “Enabling the system application server instance” on page 149.

2. Log on to the IBM Tivoli Directory Server Web Administration Tool in one of two possible ways:
   - From iSeries Navigator, select your System i machine and select Network → Servers → TCP/IP, right-click IBM Directory Server, and select Server Administration.
   - Log on to the i5/OS Tasks menu from a Web browser with the following URL:
     http://<your_server>:2001
     Where <your_server> is the TCP/IP host name of your System i machine and 2001 is IBM Web Administration for i5/OS port. In our example, the URL to access the i5/OS Tasks menu is:
     http://rchas10:2001
     When prompted, sign on with an i5/OS user profile and password to connect to your System i machine. On the i5/OS Tasks menu, select IBM Directory Server for i5/OS.

3. On the Login page, in the LDAP Hostname field, select the directory server you want to manage. Enter the distinguished name (DN) for the administrator (cn=administrator in our example) and the corresponding password that is configured in the IBM Directory Server properties. Click Login. See Figure 3-95.

Creating a container in the IDS LDAP Directory

This section describes how you create a container in the IDS LDAP directory. This container is used for the System Distribution Directory scenario covered in 3.7.3, “Example using SDD publishing” on page 173 and is also the equivalent for the groups container that WebSphere Portal Express uses by default for storing group entities.

Note: The example we provide here creates a container with a name other than the one the i5/OS Create WebSphere Portal wizard uses.

To create a container in your IDS LDAP directory, perform the following steps:

1. Start your IBM Tivoli Directory Server Web Administration Tool as described in “Starting the IBM Tivoli Directory Server Web Administration Tool” on page 154.
2. From the left navigation pane of the Introduction page, expand **Directory management** and select **Manage entries**. See Figure 3-96.

![Directory management navigation tree](Figure 3-96)

3. Select the appropriate domain suffix for your system and click **Expand**. In our example, shown in Figure 3-97, we expand our RDN of `dc=rchas10,dc=rchand,dc=ibm,dc=com`.

![Selecting a domain suffix](Figure 3-97)
4. At this point, you are in the hierarchy where the containers reside. You can view the entries that are already defined under the Current location that is your domain suffix (dc=rchas10,dc=rchand,dc=ibm,dc=com). See Figure 3-98. In a new LDAP directory, you see no entries here. Click the Add button to add an entry for a new container.

5. In the next panel displayed, select container from the Structural object classes selection list and click Next.

6. In the Select auxiliary object classes panel, make no changes and click Next.
7. On the Add an entry panel, enter the Relative DN for your new container in the Relative DN field. This is the naming attribute (cn) with the name of your new container. In our example, we specify cn=portalAdmins.

   In the Required attributes field, type the name value of the container you want to create in the cn field. In our example, we enter portalAdmins. See Figure 3-99. Click Finish.

    **Figure 3-99   Creating a container in the directory server**

8. Click Logout in the left panel to close the Tivoli Directory Server Web Administration Tool.

**Adding a user to the IDS directory**

This section shows you how to add a user in the IBM Directory Server for i5/OS LDAP directory. In this example, we assume you have used the i5/OS Create WebSphere Portal wizard in IBM Web Administration for i5/OS to create a WebSphere Portal Express instance using the default values for the LDAP users and groups entries. See 3.3, “Configuring the WebSphere Portal Express server” on page 95 for details.

Your directory server should have a structure similar to that shown in Figure 3-24 on page 100 and Figure 3-25 on page 100. But even if your directory has a different structure, the steps for adding a user to the directory with the IBM Tivoli Directory Server Web Administration Tool work in a similar way.

To add an user to your directory server, perform the following steps:

1. Start the IBM Tivoli Directory Server Web Administration Tool as described in “Starting the IBM Tivoli Directory Server Web Administration Tool” on page 154.

2. From the left navigation pane of the Introduction page, expand Directory management and select Manage entries. See Figure 3-96 on page 155.
3. Select the appropriate domain suffix of your system as shown in Figure 3-97 on page 155 and click **Expand**.

4. On the Manage entries panel, select the appropriate container you want to add a user to (in our example, this is `cn=users`), as shown in Figure 3-100 and click **Expand**.

5. The next panel shows the list of users defined in the Users container. As shown in Figure 3-101, only the WebSphere Portal Express administrator is listed. Click **Add**.

![Manage entries](image1)

*Figure 3-100  Selecting the Users container*

![Manage entries](image2)

*Figure 3-101  List of users in Users container*
6. In the Select object class panel (Figure 3-102), select the `inetOrgPerson` class from the Structural object classes selection list and click **Next**.

![Select object class panel](image)

**Figure 3-102** Selecting the structural object classes

7. On the Select Auxiliary Object Class panel, you are not required to specify an auxiliary object class. Click **Next**.
8. On the Add an entry panel (Figure 3-103), type `uid=user name` for the Relative DN field. In our example, we entered `uid=ualthoff`. If the Parent DN is not shown already, click the **Browse** button to select it.

Type the **cn** (common name) and **sn** (surname) under the Required attributes section. Click **Optional attributes**.

![Figure 3-103  Entering user attributes](image-url)

<table>
<thead>
<tr>
<th><strong>Enter the attributes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the values for the attributes of the new entry. For multiple values click <strong>Multiple values</strong> next to the attribute.</td>
</tr>
<tr>
<td>When you have entered all the required attributes and any of the other attributes click <strong>Finish</strong> at the bottom of the pages.</td>
</tr>
</tbody>
</table>

- **Object class inheritance**
  - `inetOrgPerson`

- **Distinguished name (DN)**
  - **Relative DN**: `uid=ualthoff`
  - **Parent DN**: `cn=users,dc=rchas10,dc=rchland,dc=ibm`
  - Click **Browse**...

- **Required attributes**
  - **cn**: ursula atlhoff
  - **sn**: atlhoff

- **Optional attributes**
  - **Multiple values**

---

*Figure 3-103  Entering user attributes*
9. In the next panel that is displayed (Figure 3-104), enter the values for the Optional attributes, such as displayName, givenName, uid, and userPassword. You have to scroll down to see all the attributes that are defined for the inetOrgPerson object class. Click Finish.

![Add an entry](Figure 3-104 Entering optional attributes for the user)

10. Click Logout in the left navigation pane to close the Tivoli Directory Server Web Administration Tool.

### 3.6.4 Setting up templates and realms

For the SDD publishing scenario covered in 3.7.3, “Example using SDD publishing” on page 173, we use the concept of templates and realms. This section provides a short overview of templates and realms in the directory server. For more information, refer to the IBM System i and i5/OS Information Center:

http://publib.boulder.ibm.com/iseries/

A template describes what a user looks like. It specifies the object classes that are used when creating users (both the structural object class and any auxiliary classes that you want). A template also specifies the layout of the panels used to create or edit users (for example, names of tabs, default values, and attributes to appear on each tab).

A realm identifies a collection of users and groups. It specifies information in a flat directory structure, such as where users are located and where groups are located. A realm defines a location for users (for example, cn=employees,dc=rchas10,dc=rchland,dc=ibm,dc=com) and creates users as immediate subordinates of that entry (for example, Walter Scalan is created as cn=Walter Scalan,cn=employees,dc=rchas10,dc=rchland,dc=ibm,dc=com).
This section describes how to create both a template and realm using the IBM Tivoli Directory Server Web Administration Tool.

Creating a user template
Perform the following steps to create a user template as an aid to adding the employee data:

1. Start your IBM Tivoli Directory Server Web Administration Tool as described in “Starting the IBM Tivoli Directory Server Web Administration Tool” on page 154.

2. In the left navigation pane, select Realms and templates → Add user template, as shown in Figure 3-105.

3. In the User template name field, type employee. Click the Browse button next to the Parent DN field.
4. Select the RDN for your IDS server. In our example, this is
dc=rchas10,dc=rchland,cd=ibm,dc=com. Click the Select button. See Figure 3-106.

![Browse entries](image)

Figure 3-106 Creating a user template, browsing entries

5. Back on the Add user template, click Next.
6. In the Structural object class drop-down list, select `inetOrgPerson` and click **Next** as shown in Figure 3-107.

![Add user template](image)

**Figure 3-107**  Creating a user template, specifying a structural object class
7. On the Edit the tabs and attributes panel, in the Naming attribute drop-down list, select **cn**. In the Tabs list, select **Required** and click **Edit**. See Figure 3-108.

![Figure 3-108 Creating a user template, specifying the naming attribute](image)

8. The Edit tab panel is where you choose which fields to include in the user template as required attributes. Attributes sn and cn are required. Select the attributes that are the required attributes in your template. In our example, we select **displayName** and click **Add>>** as shown in Figure 3-109. Click **OK** and then **Finish** after you have added all your required attributes.

![Figure 3-109 Creating a user template, defining the required attributes](image)
Creating a realm

Perform the following steps to create a realm:

1. Start your IBM Tivoli Directory Server Web Administration Tool as described in “Starting the IBM Tivoli Directory Server Web Administration Tool” on page 154.

2. In the left navigation pane, select Realms and templates → Add user template, as shown in Figure 3-105 on page 162.

3. In the Realm panel, type employee.

4. Click the Browse button to the right of the Parent DN field.

5. Select the parent DN. In our example, it is dc=rchas10,dc=rchland,cd=ibm,dc=com. Click Select on the right side of the window. Back on the Add realm panel, click Next.

6. In the Realm panel, you need to change only the User template drop-down list. Select the your user template you created - for example:

   cn=employee,dc=rchas10,dc=rchland,cd=ibm,dc=com

7. Click Finish. See Figure 3-110.

![Add realm](image.png)

**Figure 3-110** Adding a realm in the directory server

3.7 Using information stored in the System Distribution Directory for LDAP publishing

This section describes how to publish data residing in the System Distribution Directory (SDD) to the IBM Directory Server for i5/OS LDAP directory. The publishing task that publishes the SDD data to the LDAP directory synchronizes the LDAP directory with changes made in the SDD.
A published user in the LDAP directory has a uid attribute that makes the entry unique. The uid is populated with the value of the i5/OS user profile from the SDD entry. See Table 3-8 on page 168 for details. The userPassword attribute in the LDAP directory has no value in it (it is not published). When a bind or validation request is received for an entry such as this, the IBM Directory Server for i5/OS calls the i5/OS security functions to validate the provided user ID and password (for example, the values that have been entered in a Web browser logon) against the current password that belongs to the corresponding i5/OS user profile.

Figure 3-111 shows the process flow when a user for which the LDAP entry was created using the SDD publishing function of i5/OS logs on to WebSphere Portal Express. The password is validated against the i5/OS user profile.

If you are going to implement a directory server for authentication and would like to provide the option to enable your existing i5/OS users to authenticate (for example, when they want to access a WebSphere Portal Express server) with their i5/OS user ID and password, you should consider using the SDD publishing function and the implementation for collaboration integration as described later in this section.
You can configure i5/OS to publish SDD information to a directory server that is on the same System i machine or on a different System i machine. You can also publish to a non-System i machine where the IBM Tivoli Directory Server is implemented. In the case where your target directory server is not on the same System i, you can use the publishing function for one-time publishing.

Automatic publishing to the target directory can be defined using iSeries Navigator, see 3.7.2, “Setting up SDD publishing” on page 169. This automatic publishing function continually synchronizes the LDAP directory with changes that are made in the SDD. However, it is a one-way synchronization.

Your LDAP directory server can contain users published from the SDD as well as users added to the directory by other means.

The SDD entry is exported to the LDAP directory using the inetOrgPerson and ePerson object classes. Table 3-8 shows the mapping of SDD fields to attributes of the inetOrgPerson and ePerson object classes.

### Table 3-8  Mapping SDD fields to the inetOrgPerson and ePerson object classes

<table>
<thead>
<tr>
<th>System Distribution Directory (SDD) field</th>
<th>LDAP attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>User profile</td>
<td>uid</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td>Last name</td>
<td>sn (surname), cn (common name)</td>
</tr>
<tr>
<td>First name</td>
<td>givenName, cn (common name)</td>
</tr>
<tr>
<td>Preferred name</td>
<td>cn (common name)</td>
</tr>
<tr>
<td>Full name</td>
<td>cn (common name)</td>
</tr>
<tr>
<td>User ID</td>
<td>cn (common name)</td>
</tr>
<tr>
<td>Department</td>
<td>departmentNumber</td>
</tr>
<tr>
<td>Job title</td>
<td>title</td>
</tr>
<tr>
<td>Telephone number 1 and 2</td>
<td>Telephone number 1 and 2</td>
</tr>
<tr>
<td>FAX telephone number</td>
<td>fascimileTelephoneNumber</td>
</tr>
<tr>
<td>Office</td>
<td>roomNumber</td>
</tr>
<tr>
<td>Address lines 1-4</td>
<td>registeredAddress</td>
</tr>
<tr>
<td>SMTP name</td>
<td>mail</td>
</tr>
</tbody>
</table>
The common name (cn) uses the following formats:

- First name Middle Name Last name
- Preferred name Last name
- Full name
- UserID

For example, a user with the first name of Jonathan, preferred name of John, middle initial of T, last name of Smith, and user ID of JSMITH, has the following common names:

- cn=Jonathan T. Smith
- cn=John Smith
- cn=Smith, Jonathan T. (John)
- cn=JSMITH

The distinguished name (DN) of the published entry is the first cn combined with the directory path. For example, if the directory path is cn=employees, o=iseriesshop, the DN for this user is cn=Jonathan T. Smith,cn=employees,o=iseriesshop.

If two users in the SDD resolve to the same DN, they will overlay each other in the LDAP server. Sometimes overlaying names is what you want if you are merging multiple i5/OS SDDs into one LDAP server. However, if you have different users with the same name, ensure they have different DNs to prevent their overlaying each other.

### 3.7.2 Setting up SDD publishing

To configure i5/OS to publish data from the SDD into the IDS LDAP directory, perform the following steps:

1. From iSeries Navigator, right-click your System i machine name and select **Properties**.
2. In the Properties dialog box, select the **Directory Services** tab.
3. Select **Users** and click **Details**. See Figure 3-112.

![Figure 3-112 Directory Services properties](image)

4. On the User Information Details window (Figure 3-113 on page 170), select the **Publish user information** check box.
   
   a. In the Where to publish section, click the **Edit** button.
   
   b. In the next panel displayed, select or type your IDS server. In our example, we specify rchas10.rchland.ibm.com. Click **OK**.
c. In the Under DN field, click the **Browse** button. In the next panel displayed, expand the appropriate DN. In our example, it is `dc=rchas10,dc=rchland,dc=ibm,dc=com`. Select the template you created in “Creating a user template” on page 162 - in our example, this is employees. Click **Select**.

d. In the Server connection section, ensure that the default port number 389 is entered in the Port field. In the User type drop-down list, select **Distinguished name**. Enter the IDS Directory administrator DN in the Distinguished name field. In our example, it is `cn=administrator`.

e. Click **Password**. In the next panel displayed, enter the password for the administrator of your IDS LDAP directory and click **OK**.

f. Back on the User Information Details window (Figure 3-113), click the **Verify** button. This ensures that you have entered all the information correctly, and you can connect to the LDAP directory.

g. Click **OK** to close the User Information Details window.

![User Information Details window](image)

Figure 3-113 Configuring i5/OS to publish SDD data to the LDAP directory

5. Click **OK** to close the Properties window.

The publishing function starts. After approximately five minutes, the users in the SDD are published to the IDS LDAP directory.
In our example, the directory structure looks similar to that in Figure 3-114 after the publishing function has run. Entries for our i5/OS users in the SDD directory have been created under the employees realm.

Figure 3-114   Directory structure after SDD publishing

Figure 3-115 shows the attributes for user Petty Smith; this user has the i5/OS user profile SMITH (which is matched to the attribute uid).
Figure 3-116 shows the parameters in the SDD for i5/OS user SMITH. Use the i5/OS CL command of Display Directory Entry (DSPDIRE) to get a list of SDD entries. Use option 5 (Display details) to see the user details.

<table>
<thead>
<tr>
<th>Display Directory Entry Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID/Address . . . . : SMITH RCHAS10</td>
</tr>
<tr>
<td>Description . . . . . : cn=Petty Smith,o=itsoids</td>
</tr>
<tr>
<td>System name/Group . . . : RCHAS10</td>
</tr>
<tr>
<td>User profile . . . . : SMITH</td>
</tr>
<tr>
<td>Network user ID . . . . : SMITH RCHAS10</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Last . . . . : Smith</td>
</tr>
<tr>
<td>First . . . . : Petty</td>
</tr>
<tr>
<td>Middle . . . . :</td>
</tr>
<tr>
<td>Preferred . . . . :</td>
</tr>
<tr>
<td>Full . . . . : Petty Smith</td>
</tr>
<tr>
<td>Department . . . . :</td>
</tr>
<tr>
<td>Job title . . . . :</td>
</tr>
<tr>
<td>Company . . . . : More...</td>
</tr>
</tbody>
</table>

Press Enter to continue.

Figure 3-116  SDD entry for i5/OS user SMITH

The publishing task
By default, the publishing task will take place every five minutes after it has been configured. You can also manually start the publishing task (after setup) by calling the program QGLDSSDD. Following are two examples of how to call the publishing task from an i5/OS command line:

- To publish all users in the SDD to the LDAP directory:
  
  ```
  CALL PGM(QGLDSSDD) PARM(*ALL 'cn=administrator' 'secret' 0 0 0)
  ```

- To publish only users where changes in the SDD occurs:
  
  ```
  CALL PGM(QGLDSSDD) PARM(*CHG 'cn=administrator' 'secret' 0 0 0)
  ```

In these examples, the administrator (cn=administrator) and the following password (secret) should be replaced with the values of your environment. For more information about the publishing tasks jobs, see the System i Information Center.

Excluding SDD entries from being published
The following users from the SDD are published to the LDAP directory:

- Local users
- Remote users that have been added to the local system and have a Simple Mail Transfer Protocol (SMTP) address

The following SDD users are not published:

- Some entries are automatically prevented from being published to LDAP. They are the "ANY SDD entries and some other entries that are IBM-supplied starting with the letter "Q". For example, QSECOFR, QDOC, QSYS, QDFTOWN, and QUSER.
Remote users who do not have a SMTP address.

Shadowed users.

In some cases, you might want to prevent additional users from being published to the LDAP directory. For example, some system or software product users that must be in the SDD but do not represent real people.

A specific user can be prevented from being published to LDAP by doing the following:

1. Add the user-defined field QREPL QLDAP to the SDD. This needs to be done only once per system.

   CHGSYSDIRA USRDFNFLD((QREPL QLDAP *ADD *DATA 4))

2. Specify *NO as the value for the QREPL QLDAP user-defined field for those users that you do not want to publish to the LDAP directory. Any other value or absence of the QREPL QLDAP user-defined field will publish the user. We recommend that you either leave the QREPL QLDAP value blank or specify *YES if you want the user to be published.

   For example, using the Work with Directory Entries (WRKDIR) command, option 1 to add a user or option 2 to change a user, press the F20 key to specify user-defined fields. See Figure 3-117. When using the ADDDIRE or CHGDIRE commands, specify USRDFNFLD((QREPL QLDAP *NO)) to prevent the user from being published.

3. If the user is already published to the LDAP directory and *NO is specified in the QREPL QLDAP user-defined field, the user is deleted from the LDAP directory. Likewise, if the value of the QREPL QLDAP user-defined field is changed to anything but *NO, the user is added to the LDAP directory.

3.7.3 Example using SDD publishing

The example scenario covered in this section uses the SDD publishing functionality to populate users into the IDS LDAP directory that will be used for authentication to the WebSphere Portal Express server. In this example, we implement this SDD scenario using solution 2, described in 3.5.3, “Solution 2: Using the Domino Directory Assistance database” on page 133, for name mapping and mail auto-detection. Therefore, we complete the steps described in the “Solution 2” column of Table 3-6 on page 120 for this example.

For this SDD scenario, we use the same Domino (domids) and Sametime (stids) servers that we used earlier in this chapter. The steps for setting up the Domino and Sametime environment for this SDD scenario are the same. Only some configuration documents have different content for some parameters. This section covers only the differences in these documents.
To use a different LDAP structure than the structure used in the example earlier in this chapter, we use realms and templates (see 3.6.4, “Setting up templates and realms” on page 161) to define the users container with the name of employees instead of the container called users. We also create the group container called portalAdmins, which will hold the Portal administration groups. See “Creating a container in the IDS LDAP Directory” on page 154.

With this SDD solution, we describe how to use SDD publishing, and we explain your choices when you already have an IDS LDAP directory with user definitions in place before implementing WebSphere Portal on i5/OS.

We use the Create WebSphere Portal wizard to create a WebSphere Portal instance with the name wpx6sdd.

To implement this SDD scenario, follow the steps shown in the Table 3-9:

<table>
<thead>
<tr>
<th>Task</th>
<th>Prerequisites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1, “Basic IDS LDAP configuration on i5/OS” on page 74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.1, “Enabling the system application server instance” on page 149</td>
<td>Can be done at any time after WebSphere Application Server V6 is installed and should be done before creating a WebSphere Portal profile.</td>
<td></td>
</tr>
<tr>
<td>3.6.2, “Configuring the IBM Tivoli Directory Server Web Administration Tool” on page 150</td>
<td>This task can be performed after you have completed the basic IDS LDAP configuration and enabled the system application server instance. Do this task before creating a WebSphere Portal profile.</td>
<td></td>
</tr>
<tr>
<td>“Creating a container in the IDS LDAP Directory” on page 154</td>
<td>You can perform this task after you have completed the basic IDS LDAP configuration and configured the IBM Tivoli Directory Server Web Administration Tool. Do this before creating a WebSphere Portal profile.</td>
<td></td>
</tr>
<tr>
<td>“Creating a user template” on page 162</td>
<td>Perform this task after you have completed the basic IDS LDAP configuration and have configured the IBM Tivoli Directory Server Web Administration Tool. Do this before creating a WebSphere Portal profile and before publishing the SDD entries.</td>
<td>Alternatively you can create a container for the users you want to publish from the SDD.</td>
</tr>
<tr>
<td>“Creating a realm” on page 166</td>
<td>Do this task after you have created a user template and before you create a WebSphere Portal profile and publish the SDD entries.</td>
<td></td>
</tr>
<tr>
<td>3.2.1, “Configuring the primary Domino server” on page 77</td>
<td>This task must be done before creating a WebSphere Portal profile.</td>
<td></td>
</tr>
<tr>
<td>“Preparing the SDD” on page 175</td>
<td>You can complete this task any time but before you complete the steps in 3.7.1, “Publishing SDD data to the directory server” on page 168.</td>
<td></td>
</tr>
</tbody>
</table>
## Preparing the SDD

Because we use the SDD publishing function to populate our IDS LDAP directory, we choose to use the SDD description field, which is published to the LDAP description attribute, to provide the Domino user DN in LDAP notation. Remember, you need this information in the LDAP directory for name mapping and mail auto-detection when using our solution 2 example for solving this problem.

<table>
<thead>
<tr>
<th>Task</th>
<th>Prerequisites</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Registering Domino users for SDD scenario” on page 176</td>
<td>You can perform this task any time after configuring the Domino server.</td>
<td></td>
</tr>
<tr>
<td>3.2.2, “Registering a Domino server” on page 81</td>
<td>Do this task after you configure the Domino server and before you create a WebSphere Portal profile with the wizard.</td>
<td></td>
</tr>
<tr>
<td>3.2.4, “Configuring the Sametime server” on page 88</td>
<td>Do this after registering a Domino server and before creating a WebSphere Portal profile.</td>
<td>As an alternative to the tasks of creating a template and a realm, you can create a container for the users you want to publish from the SDD.</td>
</tr>
<tr>
<td>3.3, “Configuring the WebSphere Portal Express server” on page 95</td>
<td>Complete this task after you have configured the basic IDS LDAP and set up the Domino and Sametime servers. In addition, you perform this task after creating a container, template, and realm.</td>
<td></td>
</tr>
<tr>
<td>3.7.2, “Setting up SDD publishing” on page 169</td>
<td>You can complete this task any time after creating a template and a realm or by doing the alternative of creating a container for the users you want to publish from the SDD.</td>
<td></td>
</tr>
<tr>
<td>3.4, “Configuring SSO between Domino and WebSphere Portal” on page 105</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5, “Integrating Domino mail and calendar” on page 119</td>
<td>In the SDD scenario, we implement solution 2 in the same way as we did in the example earlier in this chapter. Follow the steps described in 3.5, “Integrating Domino mail and calendar” on page 119 and use the different settings described in 3.7, “Using information stored in the System Distribution Directory for LDAP publishing” on page 166.</td>
<td></td>
</tr>
<tr>
<td>3.9, “Adding additional portlets to a WebSphere Portal page” on page 191</td>
<td>Describes how to add the Domino Web Access (DWA) portlet to the default Collaboration site of your WebSphere Portal Express profile.</td>
<td></td>
</tr>
</tbody>
</table>
You have to update the SDD entry for each user by providing the Domino user DN in LDAP notation in the SDD description field.

Figure 3-118 shows some of our users where we provided this information already. We use the Work with Directory Entries (WRKDIRE) i5/OS CL command to get this list. By using option 2 (Change) in the Opt field, you can change the contents of the SDD entry. You can use also the Change Directory Entry (CHGDIRE) CL command to change the content of an SDD entry.

```
Work with Directory Entries

Type options, press Enter.
1=Add     2=Change   4=Remove   5=Display details   6=Print details
7=Rename  8=Assign different ID to description   9=Add another description

Opt  User ID   Address   Description
HUNT  RCHAS10   cn=Aleken Hunt,o=itsoids
MCATHUR  RCHAS10   cn=Paul McAthur,o=itsoids
REDDING  RCHAS10   cn=Otis Redding,o=itsoids
SCALAN  RCHAS10   cn=Walter Scalan,o=itsoids
SMITH  RCHAS10   cn=Petty Smith,o=itsoids

F3=Exit      F5=Refresh   F9=Work with nicknames   F11=Sort by description
F12=Cancel   F13=Work with departments   F17=Position to   F24=More keys
```

Figure 3-118  Users with the Domino user DN in LDAP notation in the SDD Description field

Registering Domino users for SDD scenario

Refer to 3.2.3, “Registering Domino users” on page 85 for steps to register Domino users, and consider the information in this section to use as the values for the Short name in the Domino Person document.

Unlike the earlier example covered in this chapter where we created users in our IDS LDAP directory with values for the uid attribute equal to the values for the Short name in the Domino Person document, we use a different method in this SDD scenario.
We register our users in Domino using the i5/OS user profile name value for the Short name value (see the example for user HUNT in Figure 3-119). We do so because we want to make it possible for our i5/OS users to access the WebSphere Portal Express server (authenticating via the LDAP directory) by using the well-known i5/OS user profile name.

The i5/OS user profile name is coupled with the SDD user profile, and this is mapped to the LDAP attribute uid (for the mapping from SDD to LDAP attributes, see Table 3-8 on page 168). So the uid attribute has the value of HUNT, and the user can access the WebSphere Portal Express server by using this i5/OS user profile name.

Figure 3-120 on page 178 shows the content of the SDD entry for user HUNT. We use the i5/OS CL command Display Directory Entry Details (DSPDIRE) to get the information.

![Figure 3-119 Registering a Domino user for the SDD publishing example](image)
Enabling Collaboration in WebSphere Portal Express V6 on i5/OS

Figure 3-120   SDD content for user Hunt

The uid in the LDAP directory and the Short name in the Domino Person document have to be equal for name mapping and mail auto-detection to be successful. Thus we register our users in Domino using the i5/OS user profile name value for the Short name value. See the example for user HUNT in Figure 3-119 on page 177.

Configuring the WebSphere Portal Express server for the SDD scenario
To create the WebSphere Portal profile with the name wpx6sdd for our SDD example scenario, follow the steps described in 3.3, “Configuring the WebSphere Portal Express server” on page 95 and consider the information described in this section. This section describes only the important differences in the two procedures.
Before we describe the different steps, we want to provide information about our IDS LDAP structure before starting the Create WebSphere Portal wizard. Figure 3-121 shows our IDS LDAP structure before starting the wizard. We have the employee template that we defined in “Creating a user template” on page 162 and we have the employees realm that we defined in “Creating a realm” on page 166.

The employees realm is equivalent to a container; it holds our user entries for the users we publish from the SDD. See 3.7.1, “Publishing SDD data to the directory server” on page 168.

The employees realm has the object class of ibm-realm and ibm-staticGroup but not object class container. Because of the missing object class of container, the wizard cannot browse in the Step 10-14 panel to the Parent DN in the Information describing the user entries section. However, you can override Parent DN cn=users to cn=employees, which is described later in this section.

The PortalAdmins is a container (has object class container) that we use for the Portal administration group. It does not have an entry at this time (see Figure 3-122). We created this container as described in “Creating a container in the IDS LDAP Directory” on page 154.

The differences in the steps to create the WebSphere Portal Express profile wpx6sdd are the following:

1. In the Step 1-14 panel, we use the name wpx6sdd for the WebSphere Portal Express server name.
2. In the Step 2-14 panel, we use the port range of 10500.
3. In the Step 3-14 panel, we use the name wpx6sdd for the HTTP server and an IP address of 9.5.92.18.
4. In the Step 4-14 panel, we specify the user profile WPX6SDD for the owner of the WebSphere Portal Express database.
5. In the Step 10 of 14 panel, the LDAP Configuration Parameters, we do the following:
   
   a. In the user entries section, we override the shown value of cn=users in the Parent DN field with the value cn=employees. The rest of the Parent DN we leave unchanged. So we have the value for the Parent DN of:
      
      `cn=employees,dc=rchas10,dc=rchland,dc=ibm,dc=com`.
   
   b. In the user entries section, we select the Naming attribute of `cn` from the selection list. See Figure 3-123.

   ![Figure 3-123](image)

   **Note:** Because the DN of a published entry in the LDAP directory is the first common name (cn) from the SDD combined with the directory path, we have to use the naming attribute of cn.

   c. In the administrative group entry section, we override the value of cn=groups in the Parent DN field with the value cn=portalAdmins. The rest of the Parent DN we leave unchanged. So our value for the Parent DN is:
      
      `cn=portalAdmins,dc=rchas10,dc=rchland,dc=ibm,dc=com`
   
   See Figure 3-124.

   ![Figure 3-124](image)
6. In the Step 11 of 14 panel, the LDAP Administrative Group and Administrative User, we do the following (see Figure 3-125):

a. For the Group name field, we enter portalAdministrators, which is the Group name that will be created in the LDAP directory by the wizard.

b. In the Portal administrator information section, we enter portaladmin for the Portal administrator.

c. We leave the additional group names section unchanged.

![Figure 3-125 Information for portal administrator and groups](image-url)
Our IDS LDAP directory structure after creating the WebSphere Portal Express looks as shown in Figure 3-126. The portaladmin entry for the Portal administrator is added under the realm of employees. The portalAdministrators group, as are the three other groups we did not override in the Step 11-14 panel of the creation wizard, are added under the portalAdmins container.

![Figure 3-126 Directory structure after creating the WebSphere Portal Express profile](image)

The portaladmin administrator user is added as uniqueMember in the portalAdministrators group as shown in Figure 3-127. It is also added to the three other admin groups of wpsDocReviewer, wpsContentAdministrators, and wcmaadmns.

![Figure 3-127 portalAdmins group after creating the WebSphere Portal profile](image)

### Configuring Sametime according to your LDAP settings

Because our IDS LDAP directory in the SDD solution is different in comparison to our earlier example in this chapter, we have to change the Sametime configuration. Perform the following steps:

1. Complete the steps described in 3.4.5, "Configuring Sametime to use the IDS LDAP settings" on page 114 to open the Sametime administration.
3. In the Where to start searching for people field, enter the Parent Distinguished Name (DN) of your LDAP users container. In our example, it is:
   \texttt{cn=employees,dc=rchas10,dc=rchland,dc=ibm,dc=com}

4. In the Scope for searching for a person field, use the default value of recursive.

5. In The attribute of the person entry that defines the person’s name field, enter the value of your naming attribute for your users. In our example it is \texttt{cn}.

6. In The object class used to determine if an entry is a person field, enter the value of the object class your users are defined as in the LDAP directory. In our example, we define \texttt{organizationalPerson}. See Figure 3-128.

\textbf{Note:} The \texttt{inetOrgPerson} class also works because it inherits the attributes from its parent class of \texttt{organizationalPerson}.

---

**LDAP Directory - Basics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic settings for server</strong></td>
<td>RCHAS10.RCHLAND.IBM.COM</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td></td>
</tr>
<tr>
<td>Where to start searching for people (Base object for person entries)</td>
<td>\texttt{cn=employees,dc=rchas10,dc=rchland,dc=ibm,dc=com}</td>
</tr>
<tr>
<td>Scope for searching for a person (The number of levels below the base object, for example, subtree or one level)</td>
<td>recursive</td>
</tr>
<tr>
<td>The attribute of the person entry that defines the person's name (for example, \texttt{cn} or \texttt{mail})</td>
<td>\texttt{cn}</td>
</tr>
<tr>
<td>Attribute used to distinguish between two similar person names</td>
<td></td>
</tr>
<tr>
<td>The attribute of a person entry that defines the person's e-mail address</td>
<td></td>
</tr>
<tr>
<td>The object class used to determine if an entry is a person (for example, \texttt{organizationalPerson})</td>
<td>\texttt{organizationalPerson}</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td></td>
</tr>
<tr>
<td>Where to start searching for groups (Base object for group entries)</td>
<td>\texttt{cn=portalAdmin,dc=rchas10,dc=rchland,dc=ibm,dc=com}</td>
</tr>
<tr>
<td>Scope for searching for groups (The number of levels below the base object)</td>
<td>recursive</td>
</tr>
</tbody>
</table>

\textit{Figure 3-128   Sametime LDAP directory basics}
Verifying the Domino Directory Assistance database

Change the LDAP configuration of the Domino Directory Assistance database according to the IDS LDAP definitions for the SDD solution. To verify all the settings in the existing Directory Assistance database, perform the following steps:

1. Launch the Lotus Notes client and log on with the Domino server administrator’s ID.
2. Open the existing Directory Assistance database (da.nsf) on the Domino server by:
   a. Selecting the pull-down menu options of File → Database → Open.
   b. In the next panel displayed, enter the Domino server’s name in the Server field. In our example, the Sametime server name is STIDS/ITS0IDS. Verify the Filename field shows da.nsf. Click Open.
3. In the Directory Assistance database, select the only document listed in the right pane and click Edit Directory Assistance. See Figure 3-129.

![Figure 3-129 Directory Assistance database](image)

4. In the Directory Assistance document, click the LDAP tab:
   a. Verify the Base DN for the search field, which is the Parent Distinguished Name (DN) of the LDAP users container. In our SDD example scenario, it is:

      
      cn=employees,dc=rchas10,dc=rchland,dc=ibm,dc=com
b. Verify the Type of search filter to use field is set to **Standard LDAP**. See Figure 3-130.

![Figure 3-130 Directory Assistance document, LDAP tab](image)

Verifying mail auto-detection in the SDD example scenario

At this point, we can test our WebSphere Portal Express and integrated collaboration environment. Users who authenticate on the WebSphere Portal Express server using the IDS LDAP directory should see their mail and calendar information in the collaboration portlets without providing additional user information. Perform the following steps:

1. From your Web browser, access the WebSphere Portal Express server. For example:
   
   http://wpx6sdd.rchland.ibm.com/wps/myportal

2. Log on to the WebSphere Portal Express server using a user name that is in the IDS LDAP directory. For our example, we use **Redding** (which is also the name of the i5/OS user profile).

3. Select the **Collaboration** tab.

c. Click **Save & Close**.

d. Stop the Domino LDAP task on the Domino server from the Domino server console with the following command:

   `tel Ldap quit`


e. Start the Domino LDAP task on the Domino server from the Domino server console with the following command:

   `load LDAP`

Verifying mail auto-detection in the SDD example scenario

At this point, we can test our WebSphere Portal Express and integrated collaboration environment. Users who authenticate on the WebSphere Portal Express server using the IDS LDAP directory should see their mail and calendar information in the collaboration portlets without providing additional user information. Perform the following steps:

1. From your Web browser, access the WebSphere Portal Express server. For example:

   http://wpx6sdd.rchland.ibm.com/wps/myportal

2. Log on to the WebSphere Portal Express server using a user name that is in the IDS LDAP directory. For our example, we use **Redding** (which is also the name of the i5/OS user profile).

3. Select the **Collaboration** tab.
4. The Domino Web Access portlet shows the mail for user Redding. On the right side of the panel (see Figure 3-131), you also see that the Sametime Contact List portlet is working and that user Hunt is active.

5. The Common Mail portlet also shows the mail for user Redding, as shown in Figure 3-132.
6. The Common Calendar portlet shows the appointments for user Redding, as shown in Figure 3-133.

![Common Calendar portlet for user Redding](image)

### 3.8 Managing LDAP entries with LDIF

You can also import LDAP entries into your IDS LDAP using a LDAP data interchange format (LDIF) file. LDIF is used to represent LDAP entries in text form. Using an LDIF file, you can import container, group, or user entries. LDAP information from the IDS LDAP directory can be imported from an LDIF file and also exported to an LDIF file using iSeries Navigator. By using an LDIF file, you can transfer information from one LDAP server to another.

This section provides an example of importing entries from an LDIF file into the IDS LDAP. For more information about using LDIF files, refer to the i5/OS Information Center:

http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp
The content of our example LDIF file is shown in Figure 3-134.

```
version: 1

dn: cn=users,DC=rchas10,DC=rchland,DC=ibm,DC=com
objectClass: top
objectClass: container
cn: users

dn: cn=groups,DC=rchas10,DC=rchland,DC=ibm,DC=com
objectClass: top
objectClass: container
cn: groups

dn: uid=wpsadmin,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: wpsadmin
userPassword: e1NIQX15AIwKMdVZPa/ys3+Nv2GfPDA87A==
sn: wpsadmin
cn: wpsadmin

dn: cn=wpsadmins,cn=groups,dc=rchas10,dc=rchland,dc=ibm,dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: wpsadmins
ibm-entryuuid: 08ba9801-c317-18d0-9187-0004ac083063
uniqueMember: uid=wpsadmin,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com
PWDRESET: true

dn: uid=tedwards,cn=users,dc=rchas10,dc=rchland,dc=ibm,dc=com
uid: tedwards
displayname: tedwards
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
cn: tedwards
sn: edwards
givenname: theo
description: cn=Theo Edwards,o=itsoids
userpassword: e1NIQX15AIwKMdVZPa/ys3+Nv2GfPDA87A==
```

Figure 3-134  Example LDIF file

Perform the following steps to import the contents of an LDIF file into an IDS LDAP directory:

1. Open iSeries Navigator, select your System i machine, and expand **Network** → Servers → TCP/IP.
2. Be sure the IDS Directory server is stopped. If it is running, right-click **IBM Directory Server** and select **Stop**.
3. Right-click **IBM Directory Server** and select **Tools → Import File** (see Figure 3-135).

4. On the Import LDIF File window, enter the path and file name of your LDIF file. You can use the Browse button to select it. In our example, we use the file shown in Figure 3-134 on page 188, which is stored in the i5/OS integrated file system directory shown in Figure 3-136. Click **OK** to start the import process.

5. You then get a Display Message panel that tells you the results of the import process. Select **Job Log**.
6. In the job log, you see information about the import process. The result of our example is shown in Figure 3-138.

![Job log for the import process](image1.png)

**Figure 3-138** Job log for the import process

7. If you get an error, you can click any message in the job log. Figure 3-139 is an example of a detailed error message.

![Error message details](image2.png)

**Figure 3-139** Error message details
8. In our example, the import was successful, and the LDAP structure after the import looks like the structure shown in Figure 3-140.

![LDAP structure after import of LDIF file](image)

**Figure 3-140  LDAP structure after import of LDIF file**

### 3.9 Adding additional portlets to a WebSphere Portal page

This section shows you how to add an additional portlet to the Collaboration page of the WebSphere Portal Express server. In this example, we add the Domino Web Access (DWA) portlet. To add the DWA portlet so that every portal user has this portlet on the Collaboration page, perform the following steps:

1. Log on to the WebSphere Portal Express server as your portal administrator user (wpsadmin in our example).
2. Click **Collaboration**.
3. Click **Portlets** (see Figure 3-141).

![WebSphere Portal Express home page](image)

**Figure 3-141  WebSphere Portal Express home page**

4. On the Portlets panel, type `Domino` in the Search field and click the **Search** icon (which looks like a magnifying glass). See Figure 3-142.

![Portlets panel](image)

**Figure 3-142  Portlets panel**
As shown in Figure 3-143, you see the portlets listed beginning with the word “Domino”.

5. Position the cursor over the icon to the left of the Domino Web Access portlet and hold down the left mouse button and drag it. As you drag, you can see the drop zones (dark orange versus light orange), see Figure 3-144. Drag the icon to the top left part of the page and release the mouse button. At this point you should see the Domino Web Access portlet on the page.

6. Click the Portlets link again to close the Portlets panel.
7. At this point, the DWA portlet is defined to be rendered on the Collaboration page as shown in Figure 3-145. All your portal users can see this portlet when they access the Collaboration page.

![Figure 3-145 DWA portlet on the Collaboration page](image)

8. To see the configuration parameters of the DWA portlet, click the small triangle to open the Portlet menu as shown in Figure 3-146.

![Figure 3-146 DWA portlet configuration settings](image)
9. At this point, you do not have to make any changes. Notice the setting for the mail source file, which is set to **Automatically find my mail database**, as shown in Figure 3-147.

You can use the DWA Redirect database as described in Appendix A, “Using Domino Redirect with the Domino Web Access portlet” on page 273. In that scenario, the setting on the Domino Web Access window would be **Let the DWA Redirector find my mail database**. Click **Cancel** to close this panel without making any changes.

![Figure 3-147   Domino Web Access settings](image)
Scenario 3: Using Microsoft Active Directory

This chapter shows you how to configure WebSphere Portal Express with Microsoft Active Directory as the LDAP server. Different scenarios and methods of enabling collaboration in this environment are discussed.

IBM Lotus provides various products that can be integrated to WebSphere Portal Express to enable various collaboration features. This chapter focuses on the following collaboration features:

- Online awareness - provided by Sametime
- Mail and Calendar - provided by Domino
- Web applications - provided by Domino
- Mail and Calendar - provided by Microsoft Exchange
4.1 Typical integration scenarios

When planning for integration of collaboration features into WebSphere Portal Express, there are typically four different scenarios:

- Integrating Sametime
- Integrating Domino mail, calendar, and Web applications
- Integrating Domino Web applications only
- Integrating Microsoft Exchange mail and calendar

This section discusses these four scenarios and provides a checklist for each of these scenarios outlining the tasks necessary for implementing each.

4.1.1 Scenario 1 - Integrating Sametime

You can integrate Sametime into WebSphere Portal Express to get instant messaging features including online awareness, chat, and Web conferencing.

Sametime can use either an LDAP server or the Domino Directory as the user registry. When integrating with WebSphere Portal Express, the best solution is configuring Sametime and WebSphere Portal Express to use the same LDAP server.

To implement this scenario, you must complete the following tasks:

- 4.2, “Preparing the Microsoft Active Directory” on page 198
- 4.3, “Setting up the Domino and Sametime environment” on page 203
- 4.4, “Configuring the WebSphere Portal Express V6 profile” on page 209
- 4.5, “Enabling SSO between WebSphere and Domino” on page 214
- 4.6, “Sametime integration” on page 225

4.1.2 Scenario 2 - Integrating Domino mail, calendar, and Web applications

In your organization you have Microsoft Active Directory as the enterprise directory, and WebSphere Portal Express uses Microsoft Active Directory as the LDAP server. Meanwhile, you want to integrate Domino mail, calendar, and Web applications into WebSphere Portal Express.

To integrate these components, you need to synchronize users between Domino and Microsoft Active Directory. To simplify the synchronization process and reduce administration overhead for maintaining two sets of user information, you can use a tool called ADSync that is available with Domino to synchronize the users. The benefit of this solution is you can have Domino mail, calendar, and Web applications all enabled for WebSphere Portal Express users while using Microsoft Active Directory as the LDAP server.

To implement this scenario, you must complete the following tasks:

- 4.2, “Preparing the Microsoft Active Directory” on page 198
- 4.3, “Setting up the Domino and Sametime environment” on page 203
- 4.4, “Configuring the WebSphere Portal Express V6 profile” on page 209
- 4.5, “Enabling SSO between WebSphere and Domino” on page 214
- 4.6, “Sametime integration” on page 225 (optional if Sametime is also needed)
- 4.7, “Integrating Domino mail, calendar, and applications” on page 230
4.1.3 Scenario 3 - Integrating Domino Web applications only

In your organization you have Microsoft Active Directory as the enterprise directory, and WebSphere Portal Express uses Microsoft Active Directory as the LDAP server. Meanwhile, you want to integrate Domino Web applications into WebSphere Portal Express to leverage the features in Domino discussion, teamroom, or other customized applications.

To integrate these components, you can use the same solution as described for scenario 2 to synchronize all users between Domino and Microsoft Active Directory. However, in some cases, you might not want to synchronize all users into Domino because Domino mail is not in use, and the number of Domino applications is probably limited. This scenario provides an alternate solution so you can enable all Microsoft Active Directory users to access the Domino application databases directly. You can accomplish this by utilizing the Directory Assistance feature in Domino. You do not have to duplicate all Microsoft Active Directory users into Domino.

The benefit of this solution is ease in configuring and administrating - especially because you do not have to maintain two sets of user information. The drawback is that you have to manually modify the access control list (ACL) for each Domino database. This might not be suitable if you have a large number of users who need to use Domino mail.

To implement this scenario, you must complete the following tasks:
- 4.2, “Preparing the Microsoft Active Directory” on page 198
- 4.3, “Setting up the Domino and Sametime environment” on page 203
- 4.4, “Configuring the WebSphere Portal Express V6 profile” on page 209
- 4.5, “Enabling SSO between WebSphere and Domino” on page 214
- 4.6, “Sametime integration” on page 225 (optional if Sametime is also needed)
- 4.8, “Integrating Domino applications only” on page 257

4.1.4 Scenario 4 - Integrating Microsoft Exchange mail and calendar

In this scenario you have the Microsoft Exchange server as your mail server. The Microsoft Exchange server shares the same Microsoft Active Directory server with WebSphere Portal Express.

Single sign-on (SSO) and mail file auto-detection are not supported in the Microsoft Exchange portlets. Every user must manually enter their Microsoft Exchange account information into the portlet.

To implement this scenario, you must complete the following tasks:
- 4.2, “Preparing the Microsoft Active Directory” on page 198
- 4.4, “Configuring the WebSphere Portal Express V6 profile” on page 209
- 4.8, “Integrating Domino applications only” on page 257

This scenario can be combined with Scenario 1 to enable people awareness for Microsoft Exchange mail in WebSphere Portal Express. It can also be combined with scenario 3 to integrate Domino Web applications and Microsoft Exchange mail into your WebSphere Portal Express instance.
4.2 Preparing the Microsoft Active Directory

In your organization, Microsoft Active Directory may be already installed and have existing containers, users, and groups. To use Microsoft Active Directory as the LDAP server for WebSphere Portal Express and Sametime, you need to obtain the required information from your Microsoft Active Directory administrator.

In this section we describe the requirements for using WebSphere Portal Express and Sametime. We also provide steps for setting up the Microsoft Active Directory server used in the examples in this chapter.

4.2.1 Required information

To utilize Microsoft Active Directory as the LDAP server for WebSphere Portal Express and Sametime, you need to gather the information listed in Table 4-1.

Table 4-1 Required information from Microsoft Active Directory

<table>
<thead>
<tr>
<th>Required information</th>
<th>Example used in our testing environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for user distinguished name</td>
<td>CN=&lt;user name&gt;,CN=Users,DC=itso,DC=rchland, DC=ibm,DC=com</td>
</tr>
<tr>
<td>Microsoft Active Directory administrator name and password (or other user with write access)</td>
<td>CN=administrator,CN=Users,DC=itso,DC=rchland,D C=ibm,DC=com</td>
</tr>
<tr>
<td>Parent DN for users</td>
<td>CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com</td>
</tr>
<tr>
<td>Parent DN for groups</td>
<td>CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com</td>
</tr>
<tr>
<td>WebSphere Portal Express administrator user name and password</td>
<td>CN=wpsadmin,CN=Users,DC=itso,DC=rchland, DC=ibm,DC=com</td>
</tr>
<tr>
<td>Group names (required only if you do not have write access to Microsoft Active Directory)</td>
<td>Not used in our example</td>
</tr>
<tr>
<td>WebSphere Portal Express administrator group name</td>
<td>CN=wpsadmins,CN=Users,DC=itso,DC=rchland, DC=ibm,DC=com</td>
</tr>
<tr>
<td>Document manager group name</td>
<td>CN=wpcContentAdministrators,CN=Users,DC=itso, DC=rchland,DC=ibm,DC=com</td>
</tr>
<tr>
<td>Document reviewer group name</td>
<td>CN=wpsDocReviewer,CN=Users,DC=itso, DC=rchland,DC=ibm,DC=com</td>
</tr>
<tr>
<td>Web content management group name</td>
<td>CN=wcmadmins,CN=Users,DC=itso,DC=rchland, DC=ibm,DC=com</td>
</tr>
</tbody>
</table>

This information is used in all of the sections in this chapter. To gather this information, consult your Microsoft Active Directory administrator. Optionally, you can follow the steps in 4.2.4, “Exporting Microsoft Active Directory user information to an LDIF file” on page 201 to export the information from Microsoft Active Directory.
4.2.2 Installing Microsoft Active Directory

This section describes how to set up a Microsoft Windows Server® 2003 domain controller, also known as a Microsoft Active Directory server.

**Important:** The description in this section is based on the Microsoft document available at:

The following steps are for demonstration purpose only. For more information about how to set up Microsoft Active Directory server in your production system, consult your Windows administrator or refer to Microsoft documentation:
http://www.microsoft.com

Perform the following steps to install Microsoft Active Directory as a first domain controller:

1. Install Microsoft Windows.

2. Promote the server to domain controller. Click **Start → Run**, and then type dcpromo to start the Microsoft Active Directory Installation wizard. Configure the wizard pages as shown in Table 4-2.

   **Table 4-2  Microsoft Active Directory Installation wizard information**

<table>
<thead>
<tr>
<th>Microsoft Active Directory Installation wizard page</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller Type</td>
<td>Select <strong>Domain controller</strong> for a new domain.</td>
</tr>
<tr>
<td>Install or Configure DNS</td>
<td>If you see this page, select <strong>No, just install and configure DNS on this computer.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Typically you see this wizard page when you run the Microsoft Active Directory Installation wizard (dcpromo.exe) right after installing the operating system on this computer.</td>
</tr>
<tr>
<td>Create New Domain</td>
<td>Select <strong>Domain in a new forest</strong>.</td>
</tr>
<tr>
<td>New Domain Name</td>
<td>For <strong>Full DNS name for new domain</strong>, type the name of the test domain. For our example, this is itso.rchland.ibm.com.</td>
</tr>
<tr>
<td>NetBIOS Domain Name</td>
<td>Verify that the domain name that you typed appears on this page.</td>
</tr>
<tr>
<td>Database and Log Folders</td>
<td>Accept the defaults.</td>
</tr>
<tr>
<td>Shared System Volume</td>
<td>Accept the defaults.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Select <strong>Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems.</strong></td>
</tr>
</tbody>
</table>
4.2.3 Adding users and groups in Microsoft Active Directory

When using Microsoft Active Directory as the LDAP server to create a WebSphere Portal Express profile, the i5/OS Create WebSphere Portal Express wizard requires that an administrative user and group already exist in the Microsoft Active Directory. This section describes how to create this administrative user and group. For additional information about this topic, see 1.3.4, “LDAP directory entries required for WebSphere Portal Express” on page 9.

You can use the Microsoft Active Directory Users and Groups tool to add new users and groups. Perform the following steps to create a user called wpsadmin:

1. From the Windows Start menu, select Programs → Administrative Tools → Active Directory Users and Computers.
2. Right-click Users and select New → User.
3. Leave the First name field blank, type wpsadmin in the Last name, Full name, and User login name fields for the new user. Click Next.
4. Enter the password for the new user. Confirm the password. Click Next.
5. Click Finish to create the user.

If you do not have an account that has write access to the Microsoft Active Directory to use in the i5/OS Create WebSphere Portal Express wizard, you also need to create four groups and add the WebSphere Portal Express administrator user as a member of these groups. The group names are:

- wpsadmins
- wcadmins
- wpsDocReviewer
- wpsContentAdministrators

Perform the following steps to create a group and add a user in the group (you need to repeat the steps for all four groups):

1. From the Windows Start menu, click Programs → Administrative Tools → Active Directory Users and Computers.
2. Right-click Users and select New → Group.
3. Enter the group name and click **Next**.

4. Click **Finish**.

5. Find the newly created group in the user list, right-click it and select **Properties**.

6. Click the **Members** tab, **Add** button.

7. Enter the user name and click **OK**.

8. Click **OK** again to finish adding members into the group.

### 4.2.4 Exporting Microsoft Active Directory user information to an LDIF file

Microsoft Active Directory Administration Tools display user and group information in a graphical user interface. Because we use Microsoft Active Directory as the LDAP server, it is important that we clearly understand the LDAP schema. To confirm the required information listed in Table 4-1 on page 198, you can export user and group information from the Microsoft Active Directory to an LDIF file.

A utility called LDIFDE is included in the Windows 2000/2003 operating system to support batch operations based on the LDIF standard. We use this utility to export user and group information from the Microsoft Active Directory.

To export all objects in the Microsoft Active Directory using LDIFDE, perform the following steps:

1. Access a command line prompt on the Windows 2003 server by select **Start** → **Programs** → **Accessories** → **Command Prompt**.

2. At the command prompt, type:

   ```
   ldifde -f adusers.ldif
   ```

   The command and result are shown in Figure 4-1.

![Figure 4-1 Exporting information from the Microsoft Active Directory to an LDIF file](image)

3. Use a text editor to open the adusers.ldif file. Find the entry for user wpsadmin and group wpsadmins that you created. Verify wpsadmin is a member of wpsadmins. Write down the DN attributes for future use. See Example 4-1 and Example 4-2 on page 202.

#### Example 4-1 Entry for wpsadmin in the exported LDIF file

`dn: CN=wpsadmin,CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com`

`changetype: add`
Example 4-2  Entry for group wpsadmins in the exported LDIF file

dn: CN=wpsadmins,CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com
changeType: add
objectClass: top
objectClass: group
cn: wpsadmins
member: CN=wpsadmin,CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com
distinguishedName: CN=wpsadmins,CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com
instanceType: 4
whenCreated: 20070405211136.0Z
whenChanged: 20070405211207.0Z
uSNCreated: 13815
uSNChanged: 13818
name: wpsadmins
objectGUID:: vGrpOpz8D0Kvu8XvQMGz/Q==
objectSid:: AQUAAAAAAAUVAAAAD15UpCPOnt87pmsfVwQAAA=
sAMAccountName: wpsadmins
sAMAccountType: 805306368
userPrincipalName: wpsadmins@itso.rchland.ibm.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=itso,DC=rchland,DC=ibm,DC=com
uid: wpsadmins
4.3 Setting up the Domino and Sametime environment

This section describes briefly the steps used to configure the Domino and Sametime servers used in our testing environment.

In our example, we need two Domino servers in the same domain. One Domino server works as the Domino Directory administration server, mail server, and application server, and the other Domino server hosts the Sametime server.

We complete the following tasks in this section:

- 4.3.1, “Configuring the Domino server” on page 203
- 4.3.2, “Configuring the Sametime Domino server” on page 203

4.3.1 Configuring the Domino server

To configure the Domino server, you can use the Configure Domino Server (CFGDOMSVR) CL command. Perform the following steps:

1. Open a 5250 emulation session and log on to i5/OS.
2. Type the CFGDOMSVR command on a command line and press F4 to prompt the command.
3. Enter a name for the Domino server. For our example, we enter dommad. Press F10 for more parameters.
4. Enter all the necessary information. Make sure you write down the password for the Certifier and administrator IDs. Press Enter to run the command.

Following is the complete CFGDOMSVR command used for configuring the first Domino server in our example:

```
CFGDOMSVR SERVER(dommad) OPTION(*FIRST) DTADIR('/domino/dommad/data') ORG(itsoad) ADM(admin *N *N () 1 ()) TIMEZONE(CST) CNNSRV(*NONE) TEXT('Domino server using MS Active Directory') SVRHSTNAME(dommad.rchland.ibm.com)
```

4.3.2 Configuring the Sametime Domino server

The Sametime server runs on top of a Domino server. To set up a Sametime server, you first must configure a Domino server and then add the Sametime component on top of it.

Configuring a secondary Domino server

Perform the following steps to configure a secondary Domino server in same domain as the Domino server configured in 4.3.1, “Configuring the Domino server” on page 203:

1. Register the secondary Domino server:
   a. If you have not done so already, get the user.id and cert.id files from the first Domino server. The two ID files can be found in the data directory of the first Domino server. In our example these files are located in the i5/OS integrated file system directory of the /domino/dommad/data directory.
b. From the Domino Administrator client, select the pull-down menu options of **File → Open Server** to open the first Domino server. In our example this is dommad/itsoad.

c. Select the **Configuration** tab.

d. Click the drop down for the Tools list and select **Registration → Server**.

e. On the Register Servers window (Figure 4-2), enter the following information:
   i. Click **Registration Server** and select the first Domino server.
   ii. Click **Certifier ID** and select the cert.id from the first Domino server. Click **OK**.
   iii. Enter the password for the certifier and click **OK**.
   iv. On the Register Servers window (Figure 4-2), make sure the Registration Server is the first Domino server configured and that the Certifier is correct. Click **Continue**.

![Register Servers](image)

*Figure 4-2  Registering the secondary Domino server*
f. On the Register New Server(s) window (Figure 4-3), enter the following information:
   - Enter a name for the secondary Domino server. In our example, it is stmad.
   - Under Location for storing server ID, deselect the option In Domino Directory and select the In file option. Change the path for the ID file if necessary.
   - Leave the ID file password field blank.
   - Click the green check mark to add the new server to the registration list.
   - Click Register All to register the new Domino server.

![Register New Server(s) window](image)

Figure 4-3   Registering the secondary Domino server continued

2. Configure the secondary Domino server:
   a. Open a 5250 emulation session and log on to i5/OS.
   b. Type CFGDOMSVR on a command line and press F4 to prompt the command.
   c. Enter a name for the Domino server. For our example, we enter stmad. Press F10 for more parameters.
   d. Enter all the necessary information. Make sure HTTP task is enabled. Input other necessary information. Press Enter to run the command.

   Following is the complete CFGDOMSVR command used for configuring the Sametime Domino server in our example:

   ```
   CFGDOMSVR SERVER('stmad/itsoad') OPTION(*ADD) DTADIR('/domino/stmad/data ') TIMEZONE(CST) NABSVR('dommad/itsoad') ADDSVRID('/domino/dommad/data/stmad.id') WEB(*HTTP) CNNSRV(*NONE) TEXT('Sametimeserver using Active Directory') TCPOPT(*NOENCRYPT STMAD.RCHLAND.IBM.COM) SVRHSTNAME(stmad.rchland.ibm.com) SBS(STMAD)
   ```
Configuring the Sametime server

Perform following steps to configure the Sametime server:

1. Make sure the Domino server for Sametime is stopped. You can verify this by performing the following steps:
   a. Open a 5250 emulation session and log on to i5/OS.
   b. Type the Work with Domino Servers (WRKDOMSVR) CL command on a command line and press Enter.
   c. Make sure the status for the Domino server is Ended.
   d. If the Domino server status is Started, use option 6 (End server) to end it.
2. Enter the Add Sametime to Domino (ADDLSTDOM) command and press F4 to prompt the command.
3. On the Add Sametime to Domino (ADDLSTDOM) display (Figure 4-4):
   a. Enter the Domino server name. In our example, this is stmad.
   b. Change Directory type to *LDAP and Press F10 for additional parameters.
   c. Enter the LDAP server name and port. For our example, they are the LDAP server name pk186522.itso.rchland.ibm.com and port 389.
   d. Make sure the Event server port and Token server port are not in use by any other application on this i5/OS partition.
   e. Press Enter to run the ADDLSTDOM command.

| Domino server name | STMA  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory type</td>
<td>*LDAP</td>
</tr>
<tr>
<td>LDAP server:</td>
<td>pk186522.itso.rchland.ibm.com</td>
</tr>
<tr>
<td>Port</td>
<td>389</td>
</tr>
<tr>
<td>HTTP tunneling</td>
<td>*NO</td>
</tr>
<tr>
<td>Event server port</td>
<td>9096</td>
</tr>
<tr>
<td>Token server port</td>
<td>9098</td>
</tr>
<tr>
<td>Slide conversion server</td>
<td>*NONE</td>
</tr>
</tbody>
</table>

Figure 4-4 Adding the Sametime server
Sametime configuration and verification

After the ADDLSTDOM command completes, you must perform the following steps to verify Sametime is configured correctly. You also need to add some configurations according to your Microsoft Active Directory settings. Perform the following steps:

1. Verify the Sametime server starts successfully:
   a. Open a 5250 emulation session and log on to i5/OS.
   b. Type the Work with Domino Servers (WRKDOMSVR) CL command on a command line and press Enter.
   c. Find the Sametime server just configured and enter an option 1 (Start server) next to it to start the server.
   d. Enter option 8 (Work console) to display the console for this Domino server.
   e. You should see the following messages displayed on the console (you may need to press F5 to refresh the display):
      
      Sametime: All services started successfully.
      Sametime: Server startup successful.

2. Configure the LDAP settings for Sametime:
   a. Launch a Web browser and enter the following URL for the Sametime home page:
      http://<servername>/stcenter.nsf
      In our example, the URL is:
      http://stmad.rchland.ibm.com/stcenter.nsf
   b. Click Log in to IBM Lotus Sametime and log on with the Domino server administrator name.
   c. Click Administer the Server.
   d. In the left navigation pane, click to expand LDAP Directory and select Connectivity.
e. In the right pane, in the Administrator distinguished name field, enter the Microsoft Active Directory administrator DN. See Figure 4-5. For example:

   CN=Administrator,CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com

   In the Administrator password field, enter the password for the Active Directory administrator user.

   **Note:** You must add this user name and password because Microsoft Active Directory does not allow anonymous bind.

f. Click the **Update** button at the bottom of the window to save the changes.

g. In the left navigation pane, select the **Basics** link.

h. In the Where to start searching for people field (Figure 4-6), enter the parent DN of users. In our example, this is:

   CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com

i. Click the **Update** button at the bottom of the window to save the changes.
3. Restart the Sametime server to make the changes take effect.
4. Optionally, you can use a Sametime Connect client to verify whether users in the Microsoft Active Directory can log on and chat normally.

4.4 Configuring the WebSphere Portal Express V6 profile

This section describes the steps required to create a new WebSphere Portal Express V6 profile. Perform the following steps to create a WebSphere Portal Express profile on the i5/OS using the Create WebSphere Portal Express wizard:

1. Launch a Web browser and go to the HTTPAdmin or IBM Web Administration for i5/OS Web site. For our example, RCHAS10.RCHLAND.IBM.COM is the fully qualified host name of our i5/OS environment.


   **Tip:** HTTPAdmin can also be set to debug mode for verbose logging during the configuration of a WebSphere Portal Express instance. As you run through the steps in the wizard, the verbose output is placed in the i5/OS integrated file system directory of /QIBM/UserData/HTTPAdmin/logs/HTTPAdmin.log.


2. On the Connect to i5/OS window, enter your i5/OS user profile and password to access the system. Click OK.

   **Note:** We recommend a user profile with SECOFR authority to perform the WebSphere Portal Express configuration. The user profile must have *ALLOBJ, *JOBCTL, and *IOSYSCFG special authorities to be able to configure a WebSphere Portal Express profile.

3. On the IBM Web Administration i5/OS window, click the Create WebSphere Portal link located in the left navigation bar under the Setup tab.

4. On the Create WebSphere Portal page, review all of the information presented in the window and click Next.

   **Note:** If you have not met all the prerequisites, error messages are displayed at the bottom of the window when you click Next. For example, you can check whether PTFs are missing by clicking on the link in the error message or continue by clicking Next.

5. On the Select WebSphere Portal Version page, select the version of WebSphere Portal server to create. For our example, we select IBM WebSphere Portal Express V6.0.0.1. Click Next.

6. On the Specify name for server - Step 1 of 14 page, enter a unique name and description for your WebSphere Portal Express profile. For our example, we entered WPX6MAD for the server name. Click Next.

7. On the next several pages, you should complete the necessary steps to create the WebSphere Portal Express instance. For our example WPX6MAD instance, we entered the following values:

   a. The Specify Internal Ports Used by the Application Server - Step 2 of 14 page. Specify the first port in the range to be assigned to the portal profile and click Next. The wizard
verifies that the port range you specify is correct, and no port in the range is in use. If another server is configured using any of the ports in the specified range, an error message is displayed, and you cannot proceed until a range of free ports is chosen.

b. The Create a new HTTP server (powered by Apache) - Step 3 of 14 page. Your HTTP server can listen for requests on a specific IP address or on all IP addresses of the system. Click Next.

c. The Create DB2 Database for Portal - Step 4 of 14 page. WebSphere Portal Express V6 requires several databases to store customized portal information, settings, Web pages, and configuration information. DB2 database schemas will be created and used by this WebSphere Portal environment. In our case, we specify the user to own the databases as WPX6MAD (the same as the portal profile name) and select the option to name the databases based on the server name for the specify database naming method. Click Next.

d. The Configure Proxy Information for Content Access Service - Step 5 of 14 page. Select Do not use proxy and click Next.

e. The Deploy Default Portlets - Step 6 of 14 page. Keep the default settings and click Next.

f. The Configure Lotus Collaborative Components - Step 7 of 14 page. Lotus collaborative components provide the building blocks for integrating the functionality of Domino, Sametime, and QuickPlace into portals and portlets. Choose the collaborative components to configure as shown in Figure 4-7 and provide the appropriate name field values when prompted. Click Next.

Figure 4-7 Selecting the collaborative components to configure
8. On the Secure Application Server and WebSphere Portal with LDAP - Step 8 of 14 page (Figure 4-8), specify the security options for the WebSphere Portal environment. For our example, we select **Configure security using LDAP with Realm support now** and enter the LDAP server (Microsoft Active Directory server) host name and port. Click **Next**.

**Create WebSphere Portal Express, V6.0**
Secure Application Server and WebSphere Portal with LDAP - Step 8 of 14

Securing a Web environment is critical for protecting an organization's resources. If selected, the wizard will configure security for the WebSphere Portal environment with the following:

- Global security will be turned on for the application server hosting the portal environment.
- Access to a LDAP server is required. The directory server specified will contain the registry of users that will be used to secure the portal environment.
- The LDAP server must be active to set up and use the portal environment.
- An LDAP administrator name and password must be provided to set up the portal environment. The wizard updates the directory if necessary.
- Web Server Single Sign On (SSO) is configured for the application server hosting the portal environment.
- WebSphere Member Manager (WMM) and a Lookup database will be configured to store additional information for the users of the portal environment.

Specify security options for the WebSphere Portal environment:

- Configure security using LDAP with Realm support now (Recommended).
- Configure security using LDAP with Realm support as an option.
- Configure security using LDAP without Realm support now.
- Configure security using LDAP at a later time.

Figure 4-8   Specifying security options for the WebSphere Portal Express environment

9. On the LDAP Authentication - Step 9 of 14 page, specify the access method to the LDAP directory. Enter the LDAP Administrator's distinguished name (DN) and password and then click **Next**. In our example, the LDAP administrator our Microsoft Active Directory is the following:

   
   CN=Administrator,CN=users,DC=itso,DC=rchland,DC=ibm,DC=com

10. On the LDAP Configuration Parameters - Step 10 of 14 page (Figure 4-9), confirm the Parent DN for users and groups. If you want to use a suffix other than default, you can click the **Browse** button to select them. When finished, click **Next**.

**Create WebSphere Portal Express, V6.0**
LDAP Configuration Parameters - Step 10 of 14

The Portal server utilizes LDAP to store user information for authentication purposes. Below is where the administrator user and group will reside in your LDAP directory:

Information describing user entries

| Parent DN: | cn=Users,DC=itso,DC=rchland,DC=ibm,DC=com |
| Object class: | user |
| Naming attribute: | cn |

Information describing the administrative group entry

| Parent DN: | cn=IT,DC=itso,DC=rchland,DC=ibm,DC=com |
| Object class: | group |
| Naming attribute: | cn |
| Member attribute: | member |

Figure 4-9   LDAP configuration parameters
11. The LDAP Administrative Group and Administrative User - Step 11 of 14 page
(Figure 4-10) requires an administrative group and user entry in the LDAP directory. Enter
the WebSphere Portal administrative group name and the WebSphere Portal administrator
user ID and password. This user is also be the WebSphere Application Server
administrator.

**Important:** The wizard cannot create the WebSphere Portal administrator user
automatically in Microsoft Active Directory. Create the user manually as described in
4.2.3, “Adding users and groups in Microsoft Active Directory” on page 200, or use an
existing user.

In our example, we use the group `wpsadmins` and user `wpsadmin`, which was previously
created in the Microsoft Active Directory.

![Create WebSphere Portal Express, V6.0](image)

Figure 4-10   LDAP administrative group and administrative user information
12. On the Web Server Single Signon (SSO) Configuration Parameters - Step 12 of 14 page, we want to use SSO with Sametime so we select **Include other Web servers in your SSO environment**, specify the SSO Domain name, and click **Next**. See Figure 4-11.

![Figure 4-11 Specifying Web SSO configuration parameters](image)

13. On the Configure Lightweight Third Party Authentication (LTPA) for Web Server Single Signon (SSO) Environment page, specify and confirm the LTPA password as shown in Figure 4-12 and then click **Next**. This password is required in completing the steps in 4.5.2, “Importing the LTPA key into Domino” on page 219.

![Figure 4-12 Specifying the LTPA password](image)

14. Select **Do not configure Identity Tokens** on the next page displayed and click **Next**.
15. On the Summary - Step 14 of 14 page, review your WebSphere Portal Express profile configuration. Click Finish. The configuration can take some time to complete. You can monitor the progress from the WebSphere Portal Express server introduction page displayed after you click the Finish button.

Note: The printable summary does not print passwords that were specified so remember to document them according to your system configuration.

16. When the configuration ends, you can access the WebSphere Portal Express server by entering the following URL in a Web browser:

http://<servername>/wps/portal

17. Log on to the WebSphere Portal Express server as a Microsoft Active Directory user to verify the configuration.

4.5 Enabling SSO between WebSphere and Domino

This section describes how to configure single sign-on (SSO) between the WebSphere Portal Express server profile and the Domino servers.

Note: You can enable SSO only if you configured an LDAP server in the WebSphere Portal Express configuration process.

Two steps are required to configure SSO between these servers:

- Export the WebSphere LTPA key
- Import the LTPA key into Domino

To enable SSO, you must share the same LTPA key among all servers configured in the environment for this purpose. If you specified a domain for SSO and the LTPA password when configuring the WebSphere Portal Express profile, the LTPA key is already generated. You then must export the LTPA key from WebSphere and import it into Domino.

To ensure SSO works properly, all servers must be in same DNS domain - tor example, rchland.ibm.com. In previous sections, we already configured our test environment as listed in Table 4-3.

<table>
<thead>
<tr>
<th>Server host name</th>
<th>Role</th>
<th>Domino server name</th>
</tr>
</thead>
<tbody>
<tr>
<td>wpx6mad.rchland.ibm.com</td>
<td>WebSphere Portal Express server</td>
<td>N/A</td>
</tr>
<tr>
<td>dommad.rchland.ibm.com</td>
<td>Domino mail and application server</td>
<td>dommad/itsoad</td>
</tr>
<tr>
<td>stmad.rchland.ibm.com</td>
<td>Sametime server</td>
<td>stmad/itsoad</td>
</tr>
<tr>
<td>pkil86522.itso.rchland.ibm.com</td>
<td>Microsoft Active Directory (LDAP) server</td>
<td>N/A</td>
</tr>
</tbody>
</table>
4.5.1 Exporting the WebSphere LTPA key

WebSphere cannot use Domino LTPA tokens. To include Domino and WebSphere in the same LTPA group, you must export the LTPA token from WebSphere and import it into Domino.

You must retrieve the WebSphere LTPA key from the WebSphere Portal Express server so you can use the key on the Domino servers. To export the LTPA key from the WebSphere Portal Express server, perform the following steps:

1. Start the IBM Web Administration for i5/OS server by opening the following URL from a Web browser, for example:
2. Log on using your i5/OS user ID and password. At minimum, your user ID must have *ALLOBJ, *JOBCTL, and *IOSYSCFG special authorities.
3. Select the Manage → Application Servers tabs, select your WebSphere Portal Express server, and click the Launch Administrative Console link as shown in Figure 4-13.

![Figure 4-13  Launching the WebSphere Administrative console](image)

4. If the Security Alert window is displayed, click Yes.
5. Sign on using the WebSphere Portal Express Administrator user ID and password as shown in Figure 4-14. Click Log in. In our example, we used wpsadmin, which we created in the Microsoft Active Directory.

![Figure 4-14 Logging on to the WebSphere Application Server Administrative console](image)

6. If the WebSphere Portal Express instance is configured for multiple realms, perform the following steps. Otherwise go to step 7 on page 209.


   b. Click New to add the userRegistryRealm key with the value <ldapserverhostname:port>. In our example, we type pk186522.itso.rcland.ibm.com:389. See Figure 4-15.

   c. Save the changes.

![Figure 4-15 Adding a custom property called userRegistryRealm](image)
7. Select **Security → Global security.** Under **Authentication,** click **Authentication mechanisms → LTPA.**

8. Under the Additional properties section (located on the right in Figure 4-16), click the **Single signon (SSO) link.**
9. On the Global security page (Figure 4-17), ensure that the **Enabled** check box is selected. Verify **Web inbound security attribute propagation** is not checked.

In the Domain name field, make sure the domain name for SSO is set properly. The Domain name field should include all servers that will be used for SSO. If this field is blank or set incorrectly, SSO can fail. In our example, the Domain name is `rchland.ibm.com`.

If the fields are correct, you can click **Cancel**. Should you make any changes, click **Apply** and save the settings.

![Figure 4-17  Properties for single sign-on](image)
10. Select **LTPA** to return to the Configuration tab. If the password field is blank, enter the password and confirm it. Enter a path and file name in the Key file name field. Click **Apply** then **Save** to save the changes on the master configuration. See Figure 4-18.

11. Click **Export Keys**.

**Note:** The path is in the i5/OS integrated file system on which WebSphere Portal Express server resides. If you omit the path and only enter a file name, the key file will be generated in the was_profile_root, for our example this would be: 
/QIBM/UserData/WebSphere/AppServer/V6/Base/profile/wpx6mad

![Figure 4-18 Exporting the WebSphere LTPA key](image)

12. Log out of the WebSphere Administrative console.

13. For our example, the key file just created was saved to the i5/OS integrated file system directory /QIBM/UserData/WebSphere/AppServer/V6/Base/profile/wpx6mad. Copy the key file to a location that is accessible to the Domino server.

### 4.5.2 Importing the LTPA key into Domino

To configure SSO on the Domino and Sametime servers, you need to create a Web SSO Configuration document and import the WebSphere LTPA key into it. Also, you need to enable multi-server session-based authentication on all servers. Perform following steps to configure SSO on Domino and Sametime:

1. Launch the Domino Administrator client and log on with the Domino administrator ID.
2. Select the pull-down menu options **File** → **Open Server** to open the Domino Administration server for the Domino Directory. For our example, this is dommad/itsoad.
3. Click the **Configurations** tab.

   If you have Sametime installed, the Web SSO configuration document should already exist. Perform following steps to edit it:
   
   a. Make sure the names.nsf file has been replicated among all the Domino and Sametime servers.
   
   b. On the left pane, expand **Web** and select **Web Server Configurations**.
   
   c. Scroll to the top of the right pane, so you can see the Web SSO Configurations section.
   
   d. Select the **Web SSO Configuration for LtpaToken** document and click **Edit Document**.

   If you do not have Sametime installed, perform the following steps to create a new Web SSO configuration document:
   
   a. On the left pane, expand **Server** and select **All Server Documents**.
   
   b. On the right pane, select one server that will participate in the SSO. Click **Web → Create Web SSO Configuration**.
   
   c. In the Web SSO Configuration document, leave the Configuration Name as LtpaToken. Do not enter any content in the Organization field.
   
   d. Enter the SSO domain name in the **DNS Domain** field. This name must match the SSO domain name entered when you configured the WebSphere Portal Express server. In our example, this is rch1and.ibm.com.
   
   e. In the Participating Servers section, type the Domino server names; use a comma (,) as the separator. Or click the drop-down button to select servers from the address book. See Figure 4-19.

   ![Web SSO Configuration for LtpaToken](image)

   *Figure 4-19  Creating the Web SSO Configuration document*
4. From the drop-down menu of the **Keys** button, select **Import WebSphere LTPA Keys** (Figure 4-20).

![Figure 4-20 Importing the WebSphere LTPA key](image)

5. Click **OK** if you get an warning stating that the Web SSO configuration has already been initialized (Figure 4-21).

![Figure 4-21 Warning message that Web SSO configuration already initialized](image)

6. On the Enter Import File name window (Figure 4-22), type the path and file name for the LTPA key file. For our example, it is `c:\baijx\wpx6mad.key`. Click **OK**.

![Figure 4-22 Specifying the path to the WebSphere LTPA key file](image)

7. Type the password for the LTPA key and click **OK**.

8. You should see a message indicating the import was successful (Figure 4-23). Click **OK**.

![Figure 4-23 Successfully imported the WebSphere LTPA key into Domino](image)
9. In the WebSphere Information section in the Web SSO Configuration document (see Figure 4-24), make sure the LDAP Realm field contains <ldapservername>:389. In our example, this is pkl86522.rchland.ibm.com:389.

10. Click **Save & Close**.

For each Domino server added to the Web SSO Configuration document, perform the following steps to enable multi-server session-based authentication:

1. From the Domino Administrator client, click the **Configurations** tab.
2. On the left pane, click **Servers → All Server Documents**.
3. From the server list shown in the right pane, select a Domino server and click **Edit Server**.
4. In the Domino server document, click the **Internet Protocols → Domino Web Engine** tabs.
5. Select **Multiple Servers (SSO)** for the Session authentication field and **LtpaToken** for the Web SSO Configuration field. See Figure 4-25.

6. Click **Save & Close**.
7. Repeat the preceding steps for each Domino server added in the Web SSO Configuration document Participating Servers list.

8. Replicate the Domino Directory (names.nsf) among all the Domino servers.

9. Restart each Domino server involved in the SSO.

4.5.3 Verifying SSO between Domino and WebSphere Portal Express

After configuring SSO between WebSphere Portal Express and Domino and restarting the Domino servers, you can use a Web browser to test the SSO. Perform the following steps:

1. Log on to WebSphere Portal Express server. In our example, we enter the following URL in the Web browser:

   http://wpx6mad.rchland.ibm.com/wps/portal

2. Log on with user wpsadmin. See Figure 4-26.

![WebSphere Portal Express home page after logging on](image)

Figure 4-26   WebSphere Portal Express home page after logging on

3. From the same Web browser, change the URL to the Sametime server. In our example, we enter the following URL:

   http://stmad.rchland.ibm.com/stcenter.nsf
4. You should see user wpsadmin automatically logged on to the Sametime server. See Figure 4-27.

![Sametime Welcome page with user already logged on](image)

Figure 4-27   Sametime Welcome page with user already logged on

5. From the same Web browser, change the URL to the Domino server. In our example, we enter the following URL:

http://dommad.rchland.ibm.com/names.nsf

You should see the names.nsf file opened in the Web browser directly with no need to supply a user name and password.

6. Click the Back button in the Web browser to go back to the Sametime Welcome page and then click it again to return to the WebSphere Portal Express home page. You should still see the user wpsadmin logged on.
4.6 Sametime integration

In previous sections of this chapter, you configured the Sametime server and WebSphere Portal Express server to use the same Microsoft Active Directory as the LDAP server. You also selected the Sametime integration option when creating the WebSphere Portal Express instance (see Figure 4-7 on page 210). Finally, you configured SSO between Domino, Sametime, and WebSphere Portal Express. At this point, Sametime is already integrated with WebSphere Portal Express. WebSphere Portal Express comes with people awareness features and some Sametime portlets, such as People Finder and Sametime Contact List. At this point, you can verify and utilize these features.

4.6.1 How people awareness works

The essence of Sametime integration is to enable the online people awareness feature. People awareness is handled by the STLinks applet provided by the Sametime server.

When a user logs on to the portal, Lotus Collaborative Services checks the CSEnvironment.properties file on the WebSphere Portal Express server to determine whether Sametime is configured. If it is, Collaborative Services authenticates the user with the Sametime server and builds the STLinks applet into the user’s Web browser.

The STLinks applet handles all awareness in the portal. If a portlet is enabled to show awareness, it sends names to show awareness to STLinks. STLinks contacts the Sametime server directly to determine the user’s status (Active, Away, Do not disturb, or Offline) and passes this information back to the portlet to display the user’s status in the portlet.

Requirements for Web browsers and JRE

For Internet Explorer® users, as long as the Web browser and JRE™ version meet the STLinks requirement, the people awareness feature works. For Mozilla users, perform the steps in 4.6.2, “Configuring people online awareness for a Mozilla Web browser” on page 228 to enable the people awareness feature.

The STLinks applet has its own requirements for Web browser and JRE versions. The requirement can vary depending on your Sametime version. For example, the STLinks applet that comes with Sametime Release 7.5 has the following requirements:

Web browsers supported:
- Internet Explorer V6.0 on Windows XP Professional
- Mozilla V1.7.12 on Windows XP Professional
- Mozilla V1.7.6 on RedHat Enterprise Linux® V4.0 or Novell Linux Desktop V9.0
- Firefox V1.5 on Windows XP Professional, RedHat Enterprise Linux V4.0, and Novell Linux Desktop V9.0

Java JDK/JRE supported:
- IBM or Sun JDK/JRE V1.4.2 or later for Internet Explorer V6.0 on Windows XP Professional
- IBM or Sun JRE V1.4.2 or later for RedHat Enterprise Linux V4.0 and Novell Linux Desktop V9.0

Note: Microsoft VM is not supported by Sametime Release 7.5.
Refer to the Sametime documentation for detailed requirements for different Sametime versions. Sametime documentation can be found on the Lotus Documentation Web site:

**Examples of online awareness in portlets**
Portlets that can show person online awareness include:

- People Finder
- Who is Here
- Sametime Contact List
- Common PIM portlet

In Figure 4-28, you see people online status in the People Finder, Sametime Contact List, and Common PIM portlets.

![Figure 4-28 People online status shown in various portlets](image)

We can use the Sametime Contact List portlet as an example to verify that the online awareness works properly in WebSphere Portal Express. By default, the Sametime Contact List portlet is deployed on the Collaboration page of WebSphere Portal Express. You can add
contact people or groups to the list. The Sametime Contact list shows the online status for each of the users in the list as shown in Figure 4-29.

![Figure 4-29  Sametime Contact List portlet](image)

You can click the online user names to start a chat with them. Figure 4-30 shows a chat window initialized from the WebSphere Portal Express Collaboration page.

![Figure 4-30  Sametime chat window from WebSphere Portal Express](image)

The People Finder portlet is also deployed by default as shown in Figure 4-31.

![Figure 4-31  People Finder portlet](image)
4.6.2 Configuring people online awareness for a Mozilla Web browser

The STLinks applet provides people awareness in all the Domino and Extended Products Portlets. For users of the Mozilla Web browser, the STLinks applet must be the version installed by default on the Sametime server. To configure the STLinks applet properly for the Mozilla Web browser, you need to copy files from the Sametime server to the WebSphere Portal Express server. Perform the following steps:

1. Launch iSeries Navigator and connect to the system on which the WebSphere Portal Express server is configured.

2. Locate the following directory in the i5/OS integrated file system:
   `<was_profile_root>/installedApps/cell_name/wps.ear/wps.war`
   
   In our example, the directory is:
   `/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6mad/installedApps/RCHAS10_wpx6mad/wps.ear/wps.war`

3. Create a new folder called sametime under the previously cited directory.

4. Locate the following directory in the i5/OS integrated file system:
   `<domino_data_root>/domino/html/sametime/STLINKS`

5. Copy the entire STLINKS folder to the sametime folder you created on the WebSphere Portal Express server. The new directory name should be:
   `<was_profile_root>/installedApps/cell_name/wps.ear/wps.war/sametime/STLINKS`

6. A sub-folder called signed is within the STLINKS folder you just created. Copy the stlinks.jar and stlinks.cab files to the STLINKS folder, replacing the original files. This ensures the jar file is the signed version so the Mozilla Web browser allows it to run.

7. Launch the WebSphere Portal Express server URL in the Mozilla Web browser. Click **Run** if you see the prompt shown in Figure 4-32. The people awareness feature should now work in the Mozilla Web browser.

![Security warning for STLinks applet in a Mozilla Web browser](Figure 4-32)
4.6.3 Troubleshooting online awareness problems

This section describes some common problems for enabling people online awareness.

Verifying SSO configuration
If you cannot see any user’s online status, first make sure you have verified that SSO between the WebSphere Portal Express server and the Sametime server works. To verify whether SSO works, follow the steps described in 4.5.3, “Verifying SSO between Domino and WebSphere Portal Express” on page 223.

Verifying online awareness configuration in page source
When online awareness is not available after configuring SSO, you need to examine the page source in a Web browser to determine whether online awareness provided by the Sametime server and the STLinks applet is properly configured. Perform the following steps:

1. Log on to the portal (with SSO enabled, logging onto the portal also authenticates you as a user of the Sametime server).
2. Select View → Source. If you see the following information in the source, the STLinks applet is loaded:

   ```html
   <script type="text/javascript" >if (typeof writeSTLinksApplet == "function")
   writeSTLinksApplet("cn=jx bai,cn=users,dc=itso,dc=rchland,dc=ibm,dc=com",
   "<LTPA token>", true);
   </script>
   ```

STLinks applet not loaded
If the STLinks applet has not loaded, see Technote 1163790: “Troubleshooting Sametime Awareness in WebSphere Portal” for several tests you can perform to troubleshoot the issue:

http://www.ibm.com/support/docview.wss?rs=899&uid=swg21163790

Tip: You can also use the search function from the IBM Support Web page to find technotes by number.

STLinks applet loaded but no online awareness is shown
If the STLinks applet is loaded but you cannot see online awareness, verify your browser meets the requirements of the STLinks applet for the version of Sametime you are using.

For Sametime Release 7.5, the default Microsoft VM that comes with Internet Explorer is not supported. You can install IBM or SUN JRE to make the applet run. After installing IBM or SUN JRE, check the Internet Options to verify the newly installed JVM™ is used for applets:

1. Launch the Internet Explorer Web browser and select Tools → Internet Options.
2. On the Internet Options window, click the **Advanced** tab. Make sure the option **Use Java 2 v1.4.2 for <applet>** is checked. See Figure 4-33.

![Figure 4-33 Verifying the JVM for applets in the Internet Explorer Web browser](image)

### 4.7 Integrating Domino mail, calendar, and applications

To integrate Domino mail, calendar, and applications into WebSphere Portal Express, you need to enable Microsoft Active Directory users to authenticate to Domino servers and authorize to their mail files and other application databases. Depending on your needs or existing configurations, you have several approaches for doing this. In this section, for authentication and authorization, we use the ADSync Domino tool to synchronize users between Microsoft Active Directory and Domino.

#### 4.7.1 Configuring Active Directory Synchronization (ADSync)

Domino includes a set of tools to make synchronization between Domino and Microsoft Active Directory simple and easy. Using these directory synchronization tools, you can keep both the Domino Directory and Microsoft Active Directory current without having to update both when either changes. Also, you can manage user and group information in the Domino Directory and the Microsoft Active Directory through a single interface of your choice, either Domino or Windows.

You must have a properly certified Lotus Notes ID and appropriate access to make any changes to the Domino Directory. Use a Lotus Notes Release 6 or more recent client, and Domino Release 6 or more recent server as your registration server. You must create policies that contain registration settings documents, either implicit or explicit, for all Domino certifiers with which you are going to certify new users. Also, you must have appropriate rights in the Microsoft Active Directory enabling you to add user accounts and synchronize passwords.
In our example the environment for configuring ADSync is:

- Domino Release 7.0.2 installed on i5/OS
- Microsoft Active Directory installed on Windows 2003 server
- Domino Administrator client installed on a Windows XP workstation

The following steps are written based on this environment. The steps may be slightly different if your Domino or Microsoft Active Directory are a different version.

To configure Domino Active Directory synchronization, perform the following steps:

1. From a Windows workstation, log on to the Windows domain using a user account with administrative rights.

2. From the Windows 2003 Server CD, install the Windows 2003 Administration Tools Package on the workstation. From the CD, run \i386\adminpak.msi.

   **Important:** This file is not on the Windows 2000 Professional or Windows XP workstation CD. You must install the file from the Windows 2003 Server CD.

3. After installation, access the four Active Directory administrative tools located in **Start** → **Programs** → **Administrative Tools**, or **Control Panel** → **Administrative Tools**. See Figure 4-34.

4. From the **Start** menu, click **Programs** → **Administrative Tools** → **Active Directory Users and Computers** and verify that the workstation has connected to the domain controller.

5. Install the Domino Administrator client on this workstation.

6. Make sure the Domino Administrator client is *not* running. Open a command prompt and from the Notes install directory type:

   ```
   regsvr32 nadsync.dll
   ```

   **Important:** This file is not on the Windows 2000 Professional or Windows XP workstation CD. You must install the file from the Windows 2003 Server CD.
7. A message box is displayed (Figure 4-35), indicating that registration is complete. This can take up to one minute. Click OK.

![Figure 4-35 nadsync.dll registered successfully](image)

8. Launch the Domino Administrator client.

**Tip:** If this is the first time you launch the Domino Administrator client, you need to complete the Notes configuration process.

9. From the Domino Administrator client, create an organizational policy or an explicit policy and a Registration policy settings document. You must have at least one policy to use with ADSync. For example, we created the policy described in the following steps:

**Note:** We use an Explicit policy here just for demonstration purpose. You can choose a different policy type according to your requirements. For more information about policies, refer to Domino Administrator Help.

a. On the Domino Administrator client, select **File → Open Server** to open the Domino Administration server. For our example, this is dommad/itsoad.

b. Click the **People & Groups** tab. Select **Policies** from the left navigation pane.

c. Click **Add Policy**. See Figure 4-36.

![Figure 4-36 Adding a new policy](image)

d. Keep the Policy type as Explicit. Enter a name for the policy. For example, AD-Policy.
e. Click the **New** button to the right of the Registration field. See Figure 4-37.

![Figure 4-37  Creating a new policy](image)

f. Complete the fields in the Registration Settings document, Basics tab as shown in Figure 4-38. Make sure the **Set Internet Password** check box under the Password Options section is checked.

![Figure 4-38  Basics tab of the Registration Settings document](image)
g. Complete the fields in the Registration Settings document, Mail tab as shown in Figure 4-39.

![Registration Settings: AD-Reg](image)

<table>
<thead>
<tr>
<th>Mail User Registration Options</th>
<th>Inherit from parent policy</th>
<th>Enforce in child policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose the mail system:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domino Web Access</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>Other Internet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Choose the mail server:       |                           |                          |
| dommaditload                  | Inherit                   | Enforce                  |

| Mail Templates:               |                           |                          |
| dwa7.mtf                      | Inherit                   | Enforce                  |

| Internet Address Options      |                           |                          |
| Internet Domain:              |                           |                          |
| isoc.rchland.ibm.com          | Inherit                   | Enforce                  |

| Choose an internet address format: |                           |                          |
| FirstName LastName             | Inherit                   | Enforce                  |
| FirstName MI LastName          |                           |                          |
| FI LastName                    |                           |                          |
| FI MI LastName                 |                           |                          |

| Choose an internet address separator: |                           |                          |
| None                                 | Inherit                   | Enforce                  |
| Underscore                          |                           |                          |
| Dot                                  |                           |                          |
| Equal                                |                           |                          |

| Advanced Mail Options            |                           |                          |
| Mail file owner access:          |                           |                          |
| Manager                            | Inherit                   | Enforce                  |
| Designer                           |                           |                          |
| Editor                             |                           |                          |

| Create full text index:          | Inherit                   | Enforce                  |
| Set database quote:              | Inherit                   | Enforce                  |
| Set warning threshold:           | Inherit                   | Enforce                  |

*Figure 4-39  Mail tab of the Registration Settings document*
h. Complete the fields in the Registration Settings document, ID/Certifier tab as shown in Figure 4-40.

![Image of Registration Settings document]

**Figure 4-40   ID/Certifier tab of the Registration Settings document**

<table>
<thead>
<tr>
<th>Field</th>
<th>Inherit</th>
<th>Enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Notes ID</td>
<td>✓</td>
<td>Inherit</td>
</tr>
<tr>
<td>Security Type</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>North American, International</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key Specification:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatible with all releases (630 bits)</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>Compatible with 6.0 and later (1024 bits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Key Width:</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>Base strength on RSA key size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatible with all releases (64 bits)</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>Compatible with 6.0 and later (128 bits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Expiration Date:</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>Static Date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Months from user creation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04/13/2009 11:44 AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location for Storing User ID</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>In Domino Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In File</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
<tr>
<td>In Mail File</td>
<td>Inherit</td>
<td>Enforce</td>
</tr>
</tbody>
</table>

i. Click **Save & Close** to save the Registration Settings document.

j. In the Policy document, select the Registration setting just created from the Setting name drop-down list.

k. Click **Save & Close** to save the Policy document.

10. From the Windows Start menu, select **Programs → Administrative Tools → Active Directory Users and Computers**.
11. On the Active Directory Users and Computers window, click the **Lotus Domino Options** folder. See Figure 4-41.

12. Right-click **Domino Directory synchronization** and select **Options**.

13. At this point, ADSync is initializing. Select a Domino server when prompted (see Figure 4-42). Typically this server is the administration server of the Domino Directory. For our example, it is dommad/itsoad. Click **OK**.

14. You should see a prompt indicating Lotus ADSync is initialized as shown in Figure 4-43. Click **OK**.

15. Enter your Lotus Notes password when prompted.
16. On the Lotus ADSync Options window, click the Notes Settings tab (Figure 4-44). Click the Registration Server button and specify a registration server. This server is typically the administration server of the Domino Directory. Click OK.

![Lotus ADSync Options](image)

**Figure 4-44 Notes Settings tab in Lotus ADSync Options**

17. Close and restart Active Directory Users and Computers to allow these changes to take effect.

### 4.7.2 Synchronizing users between Domino and Microsoft Active Directory

After configuring ADSync, you can synchronize users between Domino and Microsoft Active Directory. The three different methods for synchronizing users are:

- Registering existing Microsoft Active Directory users in Domino
- Creating new users in both directories using Microsoft Active Directory
- Creating new users in both directories using Domino Administrator client

This section provides detailed steps for implementing all three methods. You can choose any method for the synchronization.
Registering existing Microsoft Active Directory users in Domino

To register existing Microsoft Active Directory users in Domino, perform the following steps:

1. From the Windows Start menu, click Programs → Administrative Tools → Active Directory Users and Computers.

2. From the user list, select a user and right-click the name. Select Register in Lotus Domino. You can select more than one user in this step and register them all in Domino.

3. On the Choose Registration Options for Windows Users and Groups (Figure 4-45), keep the default options and click Register now.

4. Select the policy you created for Microsoft Active Directory users in 4.7.1, “Configuring Active Directory Synchronization (ADSync)” on page 230.

5. Select Use common password. Enter and confirm the password for the user.

   Note: Selecting the Use common password option replaces the current Windows password for this user. The new password works in Windows, Notes, and Notes Internet authentication.

6. You should receive a message that the users were successfully registered as shown in Figure 4-46. Click OK.

Creating users in both directories using Microsoft Active Directory

When creating new users in Microsoft Active Directory, you can also create them in Domino simultaneously by performing the following steps:

1. From the Windows Start menu, click Programs → Administrative Tools → Active Directory Users and Computers.

2. Right-click Users and select New → User.
3. On the New Object - User window (Figure 4-47), enter the First name, Last name, Full name, and User logon name for the new user. Click **Next**.

![New Object - User window](image)

*Figure 4-47 Creating a new user in Microsoft Active Directory*

4. Enter a password for the new user. Confirm the password. Click **Next**.
5. Check the **Register in Domino Directory** check box.
6. From the Explicit Policy list, select the policy created for Microsoft Active Directory users in 4.7.1, “Configuring Active Directory Synchronization (ADSync)” on page 230.
7. Select **Use common password**. Enter and confirm the password for the user.
8. Click **Next**.
9. Click **Finish** to register the new user in both the Microsoft Active Directory and Domino. See Figure 4-48.

![Image](image-url)

**Figure 4-48   Summary for the new user**

**Creating users in both directories using Domino Administrator client**

You can also use the Domino Administrator client to register new users in both directories. Perform the following steps:

1. Make sure you log on to the Windows workstation with the Microsoft Active Directory administrator's account.
2. Launch the Domino Administrator client and click the **People & Groups** tab.
3. Expand the **Tools** section located on the right side of the window and select **People** → **Register**. See Figure 4-49.

![Image](image-url)

**Figure 4-49   Registering a new user from the Domino Administrator client**
4. On the Choose a Certifier window (Figure 4-50), select a Domino server on which to register the new user by clicking the **Server** button. Typically it is the administration server of the Domino Directory. For our example, it is dommad/itsoad. Select a certifier ID by clicking the **Certifier ID** button. Click **OK**.

![Figure 4-50 Specifying the Domino server and certifier ID to register the new user](image)

The Register Person window is shown in Figure 4-51.

![Figure 4-51 Basic information for the new Domino user](image)
5. On the Register Person window (Figure 4-51 on page 241), enter the following information:

a. On the Basics tab:
   i. Fill in the First name, Last name, and Short name fields.
   ii. From the Explicit policy list, select the policy created for Microsoft Active Directory users in 4.7.1, “Configuring Active Directory Synchronization (ADSync)” on page 230.
   iii. For Mail systems, select Domino Web Access from the list (optional).
   iv. Click the Password Options button and make sure the Set Internet password check box is checked.
   v. Check the Advanced check box to show more tabs.

b. On the Mail tab, make changes to the Mail server, Mail file (include file path and name), and Mail file template fields if necessary.

c. On the Other tab, click the Windows User Options button.

d. On the Add Person to Windows 2000 window (Figure 4-52), check the Add this person to Windows 2000 check box. Under the Add person to Active Directory container section, select a container for the user. In our example, this is itso.rchland.ibm.com/Users. Under the Add person to Windows 2000 groups section, select one or more groups from the list. Click OK.

![Add Person to Windows 2000](image)

*Figure 4-52   Adding a new user to Windows*
6. The user name should be displayed next to the Windows User Options button. Click the green checkmark to add the user to registration queue. See Figure 4-53.

![Figure 4-53 Ready to register the new user](image)

7. Click **Register All** to register the new user.

### 4.7.3 Name mapping between Domino and Microsoft Active Directory

After synchronization, the user exists in both the Microsoft Active Directory and the Domino Directory. Because the Domino naming convention is different from the naming convention in Microsoft Active Directory, the user may have a different distinguished name. For example, in Microsoft Active Directory, the distinguished name (DN) for user `wpsadmin` is `CN=wpsadmin,CN=users,DC=itso,DC=rchland,DC=ibm,DC=com`. In Domino, the corresponding user name is `CN=wpsadmin/O=itsoad`.

During the user registration process, Domino automatically creates a mail file for the user. Also, Domino adds the user name in the mail file access control list (ACL) to grant proper access for the user. For example, user `CN=wpsadmin/O=itsoad` is added automatically in the ACL for `wpsadmin.nsf` as Editor.

When user `wpsadmin` logs in to WebSphere Portal Express, WebSphere Portal Express uses the name `CN=wpsadmin,CN=users,DC=itso,DC=rchland,DC=ibm,DC=com` to generate an LTPA token. With SSO configuration, Domino is able to recognize the user as `CN=wpsadmin,CN=users,DC=itso,DC=rchland,DC=ibm,DC=com`, but how will Domino enable this user to access the mail file, when the ACL entry of the mail file only enables access for `CN=wpsadmin/O=itsoad`?
In this case, we need manual name mapping between the Microsoft Active Directory user name and the Domino user name. We achieve this by adding the Microsoft Active Directory user name to the Domino user Person document.

When evaluating a user's authorization to use a database, Domino searches in the Domino Directory for the value contained in the LTPA token. It finds a match because that value is contained in the Person document. When it finds a match, Domino resolves the name to the Domino distinguished name, which is contained in the ACL of the mail file. So the portlet is granted access to the user's mail.

You need to keep these rules in mind for name mapping:

- When modifying the User Name (fullname) field of a Domino Person document, enter the LDAP DN in Domino format - that is, use a slash (/) instead of comma (,).
  
  - LDAP format: CN=wpsadmin,CN=users,DC=itso,DC=rchland,DC=ibm,DC=com
  - Domino format: CN=wpsadmin/CN=users/DC=itso/DC=rchland/DC=ibm/DC=com

- Add the LDAP DN to the User Name field as a secondary value. Do not add the LDAP DN as the first of second value. Domino expects the primary value to be the Domino DN and the second value to be a Domino common name.

Perform the following steps for adding name mapping in the Domino person document:

1. Launch the Domino Administrator client and select **File → Open server** to open the administration server for the Domino Directory. For our example, the Domino server is dommad/itsoad.

2. Click the **People & Groups** tab.

3. Click **People** in the left navigation pane.

4. From the right pane, select a user that exists in both the Domino Directory and the Microsoft Active Directory. For example, wpsadmin.

5. Click **Edit Person**. See Figure 4-54.

![Figure 4-54 Editing a Person document in the Domino Directory](image)
6. Add the user's LDAP DN in the User name field. By default, this field contains at least two entries. Place the cursor at the end of last entry and press Enter. Add the LDAP DN in the new line with the Domino format (see Figure 4-55). For example:

CN=wpsadmin/CN=users/DC=itso/DC=rchland/DC=ibm/DC=com

![Figure 4-55 Adding LDAP DN to User name field with “Domino format”](image)

7. Click **Save & Close** to save the Person document.

8. Repeat the preceding steps for each user. When finished, replicate names.nsf to all Domino servers.

**Tip:** It is possible automate the preceding steps by creating an agent in Domino.

After adding the LDAP DN to the Person documents, users should be able to access their mail file directly. You can verify this by performing the following steps:

1. Open a Web browser and log on to the WebSphere Portal Express server. For example, we log on with the user wpsadmin.

2. Change the URL to the user's mail file. For example:

   http://dommad.rchland.ibm.com/mail/wpsadmin.nsf

3. The user's mail file should open in the browser. If you see a **You are not authorized** message, it means the name mapping is not correct or not taking effect. Go back and confirm all previous steps in this section.

### 4.7.4 Services required on Domino for Collaboration portlets

To provide the necessary support for Collaboration portlets, such as mail, calendar, Lotus Notes View, certain services are required on the Domino servers:

- To support mail file auto-detection, you need the LDAP service on one Domino server. Typically this service is the administrative server for the Domino Directory. It is not necessary to enable LDAP on all Domino servers.
- To provide support for mail-related portlets, you need the HTTP service on each Domino mail server.
- To provide support for the Lotus Notes View portlet, you need the HTTP and DIIOP services on the Domino servers.
In our example, the Domino server dommad/itsoad works as both administrative server and mail server. So we need to enable the LDAP, HTTP, and DIIOP services on this server. In your production system, you enable only the required services on each server.

Perform the following steps to start these services automatically on the Domino server:
1. Open the notes.ini file in the domino_server_root directory of the Domino server. Or alternatively, from a 5250 emulation session, enter the Work with Domino Servers (WRKDOMSVR) CL command and then enter option 13 (Edit Notes.ini) for the Domino server.
2. In the Domino server’s notes.ini file, locate the following entry:
   `ServerTasks=`
3. Make sure the following values, if they do not already exist, are appended to the line:
   `diiop,http,ldap`
4. Save and close the file.
5. Restart the Domino server.

### 4.7.5 Configuring mail auto-detection in WebSphere Portal Express

When users log on to WebSphere Portal Express, their mail and calendar are displayed in the corresponding portlet. How can WebSphere Portal Express know where each user’s mail file is located? There are two possible ways:

- Utilize Domino LDAP service to auto-detect the user’s mail file
- Expand the LDAP schema to add the mail server and mail file information

In our example, we already synchronized users between Domino and the Microsoft Active Directory. Each Active Directory user has a corresponding Person document in Domino Directory, which contains the required mail server and mail file information. Therefore we can use the Domino LDAP service to provide the necessary information to WebSphere Portal Express.

**Configuring WebSphere Portal Express to bind to Domino LDAP server**

After starting the LDAP service on the Domino server, you need to tell WebSphere Portal Express about the Domino LDAP server address and binding information. Perform the following steps:

1. Stop the WebSphere Portal Express server from IBM Web Administration for i5/OS:
   a. Launch IBM Web Administration for i5/OS by opening its URL in a Web browser. For example:
   b. Log on with an i5/OS user ID and password.
   c. Click the Application Servers tab.
   d. From the Servers drop-down list, select the WebSphere Portal Express instance and click the Stop button
   e. Wait until the status of the WebSphere Portal Express instance changes to Stopped.
2. Launch iSeries Navigator and connect to the system on which WebSphere Portal Express is installed.
3. Locate the CSEnvironment.properties file in the following directory:
   `<portal_server_root_user>/shared/app/config`
In our example, the directory is:
/QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6mad/PortalServer/shared/app/config

4. Open the file in a text editor. For example, when using iSeries Navigator, you can right-click the file name, select **Edit**.

   **Note:** You should make a backup copy of this file before making changes.

5. Locate the **DOMINO DIRECTORY** properties section as shown in Example 4-3.

   **Example 4-3  Default Domino Directory properties section in CSEnvironment.properties file**
   
   #
   # DOMINO DIRECTORY properties
   # (LDAP server)
   # Important:
   # Should always point to a Domino Server.
   # Leave enabled flag as true.
   # Use the custom_ldap_* settings to point to a any LDAP Server to
   # get user information.
   #******************************************************************************
   CS_SERVER_DOMINO_DIRECTORY.enabled=false
   CS_SERVER_DOMINO_DIRECTORY_1.hostname=my.server.com
   CS_SERVER_DOMINO_DIRECTORY_1.port=389
   CS_SERVER_DOMINO_DIRECTORY_1.ssl=false
   CS_SERVER_DOMINO_DIRECTORY_1.anonymous=true

6. Change **CS_SERVER_DOMINO_DIRECTORY.enabled** to true. Change the other properties according to the Domino LDAP server settings. In our example, the values after modification are shown in Example 4-4.

   **Example 4-4  Modified Domino Directory properties section in CSEnvironment.properties file**
   
   CS_SERVER_DOMINO_DIRECTORY.enabled=true
   CS_SERVER_DOMINO_DIRECTORY_1.hostname=dommad.rchland.ibm.com
   CS_SERVER_DOMINO_DIRECTORY_1.port=389
   CS_SERVER_DOMINO_DIRECTORY_1.ssl=false
   CS_SERVER_DOMINO_DIRECTORY_1.anonymous=true

7. Locate the Add Default IIOP/SSL Port section as shown in Example 4-5.

   **Example 4-5  Add Default IIOP/SSL Port section in CSEnvironment.properties file**
   
   CS_SERVER_DOMINO_DIRECTORY_1.iiopport=63148

   # Optional LDAP User credential overrides
   # default - uses Portal credentials or anonymous
   # Use tool PropFileEncoderPassword.bat to encrypt the password and copy
   # the encrypted password to this file.
8. Remove the comment tag (#) from the beginning of the line that contains:

   CS_SERVER_DOMINO_DIRECTORY_1.userid=username

9. At the end of the line, add a user ID that has appropriate access to the Domino Directory. Type the Domino LDAP fully qualified name for the user. In our example, we use the user ID cn=admin,o=itsoad.

   Note: On a Domino LDAP server, this user ID must have at least Reader access to the Domino Directory (names.nsf) file.

10. Remove the comment tag (#) from the beginning of the line that contains

    CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=pwd

11. Perform the following steps to get the encrypted password:

    a. Create a text file on your Windows workstation. For example, you can launch Notepad.

    b. Enter the following line:

        dominopassword=<Domino user ID password>

        In our example we enter:

        dominopassword=itso4all

    c. Save the file as pwd.txt and close it.

    d. Copy the file to the i5/OS integrated file system directory of <app_server_root>/bin using iSeries Navigator. Or you can use FTP to upload the file to this directory. Make sure you are using ASCII format during FTP. In our example, the directory is:

        /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6mad/bin

    e. Start a 5250 emulator session and start the QShell environment by typing the STRQSH command and pressing Enter.

    f. In the QShell environment, go to the <app_server_root>/bin directory using the cd command:

        cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6mad/bin

    g. Run the command PropFilePasswordEncoder to encrypt the password. The syntax is:

        PropFilePasswordEncoder <file name> <property name list>

        In our example, the command is:

        PropFilePasswordEncoder pwd.txt dominopassword
h. Use the `cat` command to display the content of the `pwd.txt` file. The password should be encrypted by the PropFilePasswordEncoder utility. See Figure 4-56.

i. Select the text after the equal (=) sign and select **Edit → Copy**.

```bash
QSH Command Entry

$ cd /QIBM/UserData/WebSphere/AppServer/V6/Base/profiles/wpx6mad/bin
$ PropFilePasswordEncoder pwd.txt dominopassword
$ cat pwd.txt
#Wed Apr 18 11:32:51 CDT 2007
  dominopassword={xor}NissMGs+MzM=
$

Figure 4-56   Using PropFilePasswordEncoder to encrypt the password
```

12. Go back to the CSEnvironment.properties file and paste the encrypted password at the end of the `CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd=` line. Now the line should look like:

    CS_SERVER_DOMINO_DIRECTORY_1.encryptedpwd={xor}NissMGs+MzM=

13. Save and close the CSEnvironment.properties file.

14. Start the WebSphere Portal Express instance from IBM Web Administration for i5/OS.
Verifying mail auto-detection
After modifying the CSEnvironment.properties file and restarting the WebSphere Portal Express instance, you can log on to the portal and verify whether the user's mail file can be auto-detected.

By default, portlets for Mail and Calendar are already deployed on the Intranet JumpStart™ → Collaboration page. After logging on with a valid user ID, you should see the mail Inbox and calendar as shown in Figure 4-57 and Figure 4-58.

![Figure 4-57  Inbox after configuring mail auto-detection](image)

![Figure 4-58  Calendar after configuring mail auto-detection](image)
4.7.6 Displaying a Domino application in the Lotus Notes View portlet

The Lotus Notes View portlet is a commonly used portlet for displaying content from a Domino application database.

The Lotus Notes View portlet is dependent on two parameters in the CSEnvironment.properties file:

- CS_SERVER_DOMINO_DIRECTORY.enabled
- CS_SERVER_DOMINO_DIRECTORY_1.hostname

Make sure the parameters are set as the following:

CS_SERVER_DOMINO_DIRECTORY.enabled=true
CS_SERVER_DOMINO_DIRECTORY_1.hostname=dommad.rchland.ibm.com

If you already configured mail auto-detection by following the steps in 4.7.5, “Configuring mail auto-detection in WebSphere Portal Express” on page 246, the CSEnvironment.properties file should already have the proper settings. If you have not yet done so, refer to “Configuring WebSphere Portal Express to bind to Domino LDAP server” on page 246 for steps describing how to make changes in the CSEnvironment.properties file.

You can enable HTTP users to browse databases on the Domino server, which in turn enables the Lotus Notes View portlet to retrieve a list of all databases on the Domino server. Perform the following steps:

1. Launch the Domino Administrator client and log on with the Domino administrator ID.
2. Select File → Open Server to open the Administration server for Domino Directory. In our example, the Administration server is dommad/itsoad.
3. Click the Configurations tab.
4. On the left navigation pane, select Server → All Server Documents.
5. On the right pane, select a Domino application server and click Edit Server.
6. From the **Internet Protocols → HTTP** tab, set the option Allow HTTP clients to browse databases to **Yes**. See Figure 4-59.

![Figure 4-59  Enabling HTTP clients to browse Domino databases](image)

7. Click **Save & Close**.

8. Repeat the previous steps for each Domino application server.

9. Replicate the Domino Directory (names.nsf) from the Administration server to all Domino servers in the domain to propagate the changes to all servers.

You have completed all the necessary steps to use the Lotus Notes View portlet. You can use the Lotus Notes View portlet to display Domino application databases on a WebSphere Portal Express page.

**Using the Lotus Notes View portlet**

In our example, we create a test page in our WebSphere Portal Express instance and deploy the Lotus Notes View portlet on it. We use the forum.nsf Domino database to demonstrate how to configure Lotus Notes View portlet. Perform the following steps:

1. Log on to your WebSphere Portal Express instance as the Portal administrator, wpsadmin.
2. Click the upper-right corner of Lotus Notes View portlet to show the drop-down menu and select **Configure** as shown in Figure 4-60.

![Figure 4-60 Drop-down menu for the Lotus Notes View portlet](image)

3. Keep the portlet type as Any Notes View and click **Next**. See Figure 4-61.

![Figure 4-61 Selecting the portlet type for Lotus Notes View portlet](image)
4. Click the **Add** button to add views into the portlet (Figure 4-62).

![Figure 4-62 Adding a Notes view to the Lotus Notes View portlet](image-url)
5. Enter a description of the view in View Title field. Enter the Domino server host name in the Server field. In our example, the server name is dommad.rchland.ibm.com on which the forum.nsf database resides. Click the check mark to the right of the Server field. You will view a list of all the databases on this Domino server in the Database list box. See Figure 4-63.

![Figure 4-63 List of all databases on the Domino server](image)

6. Select the desired database from list or type the database file name. Click the check mark to the right of Database filename field. A list of all views in the selected database is displayed. See Figure 4-64.

![Figure 4-64 List of all views in the selected Domino database](image)
7. Select a view from the list. For example, All Documents. Click the check mark to the right of the View field. Click **Next**.

8. Change the settings in the Style section as necessary. In our example, we leave these settings at their default values.

9. In the Columns section, select the column names from the Available columns section and add them into Columns to display list by clicking the **Add** button. These columns are displayed in the Lotus Notes View portlet. In our example, we select the Date and Topic columns to display. Select the column Topic for the Column for launching documents field. Click **Done**. See Figure 4-65.

![Figure 4-65 Selecting the columns to display in the Lotus Notes View portlet](image)

10. Click **Save** to save the view settings.

11. Figure 4-66 shows the Lotus Notes View portlet, which displays the content of the All Documents view in the forum.nsf database.

![Figure 4-66 Lotus Notes View portlet showing a view from a Domino application](image)
4.8 Integrating Domino applications only

In 4.7, “Integrating Domino mail, calendar, and applications” on page 230, we described a way of integrating mail, calendar, and applications into WebSphere Portal Express. If you do not have Domino mail users and want to integrate only Domino applications into WebSphere Portal Express, you can use the procedure described in this section.

Important: The procedure described in this section presents a different way from that which we described in 4.7, “Integrating Domino mail, calendar, and applications” on page 230. Select only one procedure according to your requirements. Do not mix the two methods.

Integrating only Domino applications into WebSphere Portal Express requires the following steps:

- Configuring Domino to authenticate Microsoft Active Directory users
- Enabling the Lotus Notes View portlet to gather the required information from Domino
- Authorizing users from Microsoft Active Directory to use Domino applications
- Configuring the Lotus Notes View portlet

The following sections describe each of these steps in detail.

4.8.1 Configuring Domino

This section discusses two tasks that enable:

- Domino to authenticate Microsoft Active Directory users using Directory Assistance
- Lotus Notes View portlet to gather the necessary information using the HTTP and DIIOP services of Domino

Because both tasks require that you modify the Domino server settings and restart Domino, we combined the steps, to avoid extra restarts of the Domino server.

Verify settings in the Domino Directory Assistance database

During the configuration of the Sametime server, Directory Assistance was already configured on the Sametime server. We can deploy this configuration to all Domino servers that are hosting Domino applications. To verify the settings in the existing Directory Assistance database, perform the following steps:

Note: In case the Directory Assistance database was not created automatically, you can create the database from a Lotus Notes client by selecting File → Database → New. Select a Domino server and select Directory Assistance (7) as the template. Name the database da.nsf. Then create a Directory Assistance document and fill in all fields according to the following steps.

1. Launch the Lotus Notes client and log on with the Domino server administrator ID.
2. Open the existing Directory Assistance database (da.nsf) on the Sametime server:
   a. Select File → Database → Open.
b. On the Open Database window (Figure 4-67), type the name of the Sametime server in the Server field and press Enter. In our example, the Sametime server name is STMAD/ITSOAD.

c. In the Databases list, select **Directory Assistance (7)**. Verify the file name listed in the Filename field is da.nsf.

d. Click **Open**.

![Figure 4-67 Opening the Directory Assistance database from a Lotus Notes client](image)

3. Select the only document listed in the right pane and click **Edit Directory Assistance**. See Figure 4-68.

![Figure 4-68 Editing the Directory Assistance document](image)
4. In the Directory Assistance document, Basics tab (Figure 4-69), leave all the settings unchanged.

![Figure 4-69 Basics tab of the Directory Assistance document](image)

5. On the Naming Contexts (Rules) tab (Figure 4-70), make sure the Trusted for Credentials field in the first row is set to Yes.

![Figure 4-70 Naming Context tab of the Directory Assistance document](image)
6. On the LDAP tab (Figure 4-71):
   a. Verify Hostname is the fully qualified host name for the Microsoft Active Directory server. In our example, this is PKL86522.ITSO.RCHLAND.IBM.COM.
   b. Verify Username and Password are valid in the Microsoft Active Directory. In our example, the user name is:
      
      CN=Administrator,CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com
   c. Verify Base DN for search is the base DN for users in the Microsoft Active Directory. For our example, this is CN=Users,DC=itso,DC=rchland,DC=ibm,DC=com.
   d. Verify Type of search filter to use is Active Directory.
   e. Click Save & Close.

Deploying the Directory Assistance database to other Domino servers

After verifying all the settings in the Directory Assistance database, you must deploy the database to all the Domino servers that host Domino application databases. You can do this by creating a new replica for the da.nsf database on all the Domino servers. Perform the following steps:

1. Launch the Lotus Notes client and log on with the Domino server administrator ID.
3. On the Overwrite Replica for Database Directory Assistance (7) window (Figure 4-72), type or select the destination Domino server name - for example, dommad/itsoad. Click OK.

![Figure 4-72 Creating a new replica for the da.nsf database to other Domino servers](image)

4. Repeat the preceding steps for each Domino server.

**Note:** After creating replicas of the Directory Assistance database on all the Domino servers, whenever you make changes in the database, make sure you replicate the changes to all the Domino servers.

**Changing settings in the Domino server documents**

Once you deploy the Directory Assistance database to each Domino server, you need to enable Directory Assistance on the Domino servers. Meanwhile, you can also enable HTTP users to browse databases on the server, which in turn enables the Lotus Notes View portlet to retrieve a list of all the databases on the Domino server. Perform the following steps:

1. Launch the Domino Administrator client and log on with the Domino administrator ID.
2. Select **File → Open Server** to open the Administration server for the Domino Directory. In our example, the Administration server is **dommad/itsoad**.
3. Click the **Configurations** tab.
4. On the left navigation pane, select **Server → All Server Documents**.
5. On the right pane, select the Domino server name that you want to enable Directory Assistance on and click **Edit Server**.
6. On the Domino Server document, Basics tab (Figure 4-73), type da.nsf in the Directory Assistance database name field.

![Figure 4-73   Enabling Directory Assistance in the Domino server document]
7. On the **Internet Protocols → HTTP** tab (Figure 4-74), set Allow HTTP clients to browse databases to **Yes**. Click **Save & Close**.

![Figure 4-74   Enabling HTTP clients to browse Domino databases](image)

8. Repeat the previous steps for each Domino application server.

9. Replicate the Domino Directory (names.nsf) from the Administration server to all the Domino servers in the domain to propagate the changes to all the servers.

**Configuring Domino to enable the Lotus Notes View portlet to gather information**

To enable the Lotus Notes View portlet to gather all the required information from Domino, you must enable the HTTP and DIIOP tasks on the Domino server. DIIOP is required to gather critical information used by the Lotus Notes View portlet. The following items are supplied by DIIOP, and without its being enabled, the Lotus Notes View portlet cannot function properly. DIIOP gathers the following items of information:

- The current portal user’s name in the Domino Directory
- The list of Domino databases available for selection as a source for the portlet
- The list of view categories for selection
- Calendar information (when the Domino release is unknown)
- The number of entries (count) in a categorized view
- The name of the design template used for the source Domino database once selected
Starting the DIIOP and HTTP tasks automatically on Domino
Perform the following steps to start the DIIOP and HTTP tasks automatically on each of the Domino servers:

1. Open the notes.ini file in the domino_server_root directory of the Domino server. Or alternatively, from a 5250 emulation session, enter the Work with Domino Servers (WRKDOMSVR) CL command and then enter option 13 (Edit Notes.ini) for the Domino server.
2. In the Domino server notes.ini file, locate the following entry:
   ServerTasks=
3. Make sure the following values, if they do not already exist, are appended to the line:
   diiop,http
4. Save and close the file.
5. Restart the Domino server.

Important: At this point, you have finished all configurations on the Domino server. Make sure the da.nsf and names.nsf databases are replicated to all the Domino servers. In addition, make sure each Domino server is restarted after a Domino server document or notes.ini file is changed.

4.8.2 Authorizing users from Microsoft Active Directory to Domino applications

Every Domino database has an access control list (ACL) that specifies users’ and servers’ level of access to that database. To control the access rights of users, you must select the access level, user type, and access level privileges for each user or group in a database.

Changing the Domino application database ACL
To provide access to Microsoft Active Directory users to Domino databases through portlets, you must give them the proper access level. We use a Notes Discussion database called forum.nsf as our example in the following steps:

1. Launch the Lotus Notes client and log on as a user with the Manager access level to the forum.nsf database.
2. Open the forum.nsf database and select File → Database → Access Control.
3. On the Access Control List window, click Add to add a new Access Control list entry.
4. Type the name of Microsoft Active Directory users. The name format should be adjusted to Domino format - that is, use a slash (/) instead of a comma (.). For example:
   */CN=users/DC=itso/DC=rchland/DC=ibm/DC=com
   Or:
   CN=wpsadmin/CN=users/DC=itso/DC=rchland/DC=ibm/DC=com
5. Click OK. The name you just typed should appear in the access control list.
6. Select the appropriate user type, access level, and privileges. In our example, 
*/CN=users/DC=itso/DC=rchland/DC=ibm/DC=com is a Person group. We give these users 
Author access with Create document and Delete documents privilege. See Figure 4-75.

7. You can add more entries as needed. Click **OK** when finished.

![Figure 4-75 Adding Microsoft Active Directory users in the Domino database ACL](image)
Verifying Microsoft Active Directory users can access the database

After making the changes in the database ACL, you can perform a simple test to verify that the Microsoft Active Directory users have the expected access to the Domino application. Perform the following steps:

1. Open a Web browser and enter the URL to access the Domino application directly. In our example, the URL is:
   http://dommad.rchland.ibm.com/forum.nsf

2. Log on as a Microsoft Active Directory user (Figure 4-76).

3. The Discussion database should open in the Web browser window (Figure 4-77). Click New Main Topic to create a new document and save it. Verify the user can create a document successfully in this database.

You can use the same procedure as described in “Using the Lotus Notes View portlet” on page 252 to view Domino applications from the WebSphere Portal Express instance.
4.9 Integrating Microsoft Exchange mail and calendar

If your organization is using a Microsoft Exchange server as your mail server, you can integrate the Exchange mail and calendar into your WebSphere Portal Express instance.

**Note:** The Microsoft Exchange server uses Active Directory as the user registry. In this section, we assume your Microsoft Exchange server and WebSphere Portal Express server share the same Active Directory server.

By default, the Common PIM portlet is deployed on the **Intranet Jumpstart → Collaboration** page of WebSphere Portal Express. You can configure it to display Exchange mail and calendar. This section provides the necessary steps for this configuration.

**Common PIM portlet limitations with Microsoft Exchange**

When the Common PIM Mail portlet uses Microsoft Exchange, the following features are not available:

- Finding a message
- Single sign-on (SSO)
- Auto-detection of users’ mail files when users authenticate with the LDAP server

When the Common PIM Calendar portlet uses Microsoft Exchange, the following features are not available:

- Creating anniversaries or reminders on the events page
- FYI fields on the events page, print page, and so on
- Accepting with comments
- View Invitee Status feature
- Group Calendar feature
- Single sign-on (SSO)
- Auto-detection of users’ mail files when users authenticate with the LDAP server

### 4.9.1 Configuring the credential vault

The Common PIM portlet uses a WebSphere Portal credential vault slot to store the Microsoft Exchange user account names and passwords. The credential vault is a portlet service that helps portlets and portal users manage multiple identities. The credential vault stores credentials that make it possible for portlets to log on to applications outside the portal realm on behalf of the user. While active credentials enable you to establish connections through basic authentication, Lightweight Third Party Authentication (LTPA) token authentication, or simple form-based user ID/password logon challenges passive credentials to allow the retrieval of stored secrets such as, but not limited to, user ID and password or certificates.

Perform the following steps to create a credential vault:

1. Log on to the WebSphere Portal Express server as the portal administrator.
2. Click the **Administration** link at the bottom of the window.
3. In the left navigation pane, select **Credential Vault** under the Access section. See Figure 4-78.

![Credential Vault in portal administration](image)

**Figure 4-78** Credential Vault in portal administration

4. In the right pane, click **Add a vault slot**.

5. On the Credential Vault page, create a vault slot section (Figure 4-79), entering the following information:
   - Enter a name for the vault slot you are creating. In our example, we enter `ForExchange` in the Name field.
   - Click the **New** radio button for the Vault resource associated with vault slot field and enter a name to describe the vault resource you are creating. In our example, we type `ExchangeRSC`.

Click **OK**. You should see a message that verifies the vault slot was created successfully.

![Creating a vault slot](image)

**Figure 4-79** Creating a vault slot
4.9.2 Configuring the Common PIM portlet for Microsoft Exchange

To configure the Common PIM portlet for Microsoft Exchange mail and calendar, the portal administrator and each user must manually complete a number of steps.

**Note:** The configuration for mail and calendar are identical. The following steps are written based on the Mail portlet. You can follow the same steps to configure the Calendar portlet.

**Configurations required for a portal administrator**
As a portal administrator, you must perform the following steps so that users can configure and use the Common PIM portlet to access their own Microsoft Exchange mailbox:

1. From a Web browser, access the WebSphere Portal Express server and log on as the portal administrator. In our example, this is *wpsadmin*.
2. Select the **Collaboration** page.
3. Click the drop-down icon on the upper-right corner of the portlet. Select **Configure** from the drop-down menu. The Mail Configuration page as shown in Figure 4-80 is displayed.
4. Click the radio button for **Exchange 2000/2003** to make it the default.

![Mail Configuration for Common PIM portlet](image)

Figure 4-80  Mail Configuration for Common PIM portlet

5. Click the **Configure** button for Exchange 2000/2003.
6. Referring to Figure 4-81, complete the following settings:
   - Enter your Microsoft Exchange server host name in the Mail server name field. In our example, this is `pkl86522.itso.rchland.ibm.com`.
   - Enter the HTTP port number for your Microsoft Exchange server. In our example, the port number is `80`.
   - Under **Credential vault slot**, select the slot created in 4.9.1, “Configuring the credential vault” on page 267 from the list. In our example, it is `ForExchange`.
   - Change other settings if necessary. Click **OK**.

   ![Mail configuration for Microsoft Exchange server](image)

7. Click **Done** to complete the configuration.

**Configurations required for each user**
As an user, you must provide your user ID, password, and other information to access your Microsoft Exchange mail in WebSphere Portal Express. Contact your Microsoft Exchange server administrator if you are not sure about this information.
Perform the following steps to configure the portlet:

1. From a Web browser, access the WebSphere Portal Express server and log on as a user. In our example, we use the user jx bai for demonstration purposes.

2. Select the **Collaboration** page.

3. Click the drop-down icon on the upper-right of the portlet. Select **Personalize** from the drop-down menu.

4. Complete the following fields in the Mail Preferences page (Figure 4-82):
   a. Enter your log on name for accessing the Microsoft Exchange server.
   b. Enter your password.
   c. Enter a display name for yourself (optional).
   d. Enter your e-mail address. For example, baijx@itso.rchland.ibm.com.

5. Click the **Edit Mail Source** button.

6. In the Mail Configuration page, complete the following fields:
   - Enter a description for your mail (optional).
   - Enter the domain name for your mail account.
   - In our example, the user's Internet address is baijx@itso.rchland.ibm.com, so we enter the domain name itso.rchland.ibm.com in this field.
   - Enter your mailbox alias (optional).
   - Click **OK**.

7. Back on the Mail Preference window, click **OK** to finish the personalization.
8. Your Microsoft Exchange mail box should be displayed in the Mail portlet as shown in Figure 4-83.

![Mail portlet displaying user's Microsoft Exchange mailbox](image)

**Figure 4-83  Mail portlet displaying user’s Microsoft Exchange mailbox**

**Known problem: Users cannot access new Microsoft Exchange 2000/2003 mailboxes**

According to the IBM WebSphere Portal Version 6.0 Release Notes, new Microsoft Exchange users receive a *Missing or unrecognized user name or password* error in Common Mail portlet if they have not previously accessed the mailbox from other clients.

When new Microsoft Exchange 2000/2003 users try to access their mailboxes for the first time using the Common Mail portlet, an error (*Missing or unrecognized user name or password*) occurs. This problem is due to a known Exchange 2000/2003 Web Distributed Authoring and Versioning (WebDAV) issue.

The solution to this problem is that users must log on to new Exchange 2000/2003 mailboxes using a non-WebDav client, such as Microsoft Outlook or Microsoft Outlook Web Access (OWA), at least once before trying to access the mailboxes using the Common Mail portlet.

The IBM WebSphere Portal Version 6.0 Release Notes can be found at the following Web site:

Using Domino Redirect with the Domino Web Access portlet

This appendix describes the steps for configuring the Domino Web Access (DWA) portlet to use the Domino Redirect database for mail auto-detection.
Using the Domino Web Access template

Before deploying the Domino Web Access portlet, you must verify that the user’s mail file is using the Domino Web Access template. To verify which template is in use by the user’s mail file, perform the following steps:

1. Launch the Lotus Notes client.
2. Open a mail file:
   a. Select the pull-down menu options of File → Database → Open.
   b. Select or enter the Domino mail server name.
   c. Navigate to the mail directory (or other directory where the mail file is located), select the mail file, and click Open.
3. Select the pull-down menu options of File → Database → Properties.
4. On the Database properties window, click the Design tab. Verify the option Inherit design from master template is checked and the Template name is dwa7. See Figure A-1.

If the template is not set to the Domino Web Access template, you can change the template using the Domino mail conversion utility. Perform the following steps:

1. Launch a 5250 emulation session and log on to the system where the Domino mail server installed.
2. From the 5250 command line, enter the Work with Domino Servers (WRKDOMSVR) command and press Enter.
3. On the Work with Domino Servers display, type option 8 (Work console) next to the Domino mail server and press Enter.

4. In the Domino server console, enter the following commands:
   – If you want to change the template for a single mail file:
     ```bash
     load convert <path>/<filename> * dwa7.ntf
     ```
     For example:
     ```bash
     load convert mail/wpsadmin.nsf * dwa7.ntf
     ```
   – If you want to change the template for all mail files in a mail directory:
     ```bash
     load convert <mail/*.nsf> * dwa7.ntf
     ```

## Configuring the Domino Web Access Redirect database

The Domino Web Access Redirect database is an application that comes with Domino. With Domino Web Access Redirect, users do not need to know the name of their mail file and mail server; they can be redirected to their mail file automatically after logon.

By default, the Domino Web Access Redirect template (IWAREDIR.NTF) is installed in the Domino server data directory. To configure the Domino Web Access Redirect database, perform the following steps:

1. Launch the Lotus Notes client and log on with the Domino server administrator ID.
2. Create a database from the IWAREDIR.NTF template:
   a. Select the pull-down menu options of **File → Database → New**.
   b. In the Specify New Database Name and Location section:
      - In the Server field, enter or select a Domino server name. The Domino Web Access Redirect database will be created on this server.
      - In the Title field, enter dwa redirect.
      - In the File name field, enter dwaredir.nsf.
c. In the Specify Template for New Database section:
   - In the Server field, enter or select a Domino server name. Normally this is the same server as specified in the previous step.
   - In the Template list, select **Domino Web Access Redirect**. See Figure A-2.

d. Click **OK** to create the database.

![Figure A-2 Creating the Domino Web Access Redirect database](image)

3. The new database is automatically opened in the Lotus Notes client. See Figure A-3. Click **Setup**.

![Figure A-3 Domino Web Access Redirect database](image)
4. Click **Server Settings**. See Figure A-4.

*Figure A-4  Setup page in Domino Web Access Redirect database*
5. Select a Redirect Type that fits your configuration. You can click the Help icon for an explanation of each option. In our example, we select MailServer to use the mail server field in each user’s Person document. In the Please enter a valid TCP/IP domain for the mailserver field (Figure A-5), enter the domain name. For our example, we enter rchland.ibm.com.

**Note:** If you select MailServer as the Redirection Type under Server Settings, the common name of the Domino mail server must be the same as its fully qualified TCP/IP domain name. For example, if the mail server field in the Person document is set to serverA/domainA, the server’s TCP/IP fully qualified domain name must be serverA.lotus.com.

Leave all other fields at their default values and click the UI Setup icon.

![Figure A-5  Server Settings page in the Domino Web Access Redirect database](image-url)
6. The settings on the UI Setup page define the UI for the Domino Web Access Redirect database. Review each setting and make changes if necessary. In our example, we keep all settings at their default values. See Figure A-6.

![UI Setup page in the Domino Web Access Redirect database](image)

**Figure A-6** UI Setup page in the Domino Web Access Redirect database
7. Click the **Application Setup** icon.

8. On the Application Setup page, click the **Click to Auto Set ACL Settings** button. See Figure A-7.

```
7. Click the Application Setup icon.
8. On the Application Setup page, click the Click to Auto Set ACL Settings button. See Figure A-7.

Figure A-7   Application Setup page in the Domino Web Access Redirect database
```

9. Click **Save & Exit** to save the settings.

**Verifying the Domino Web Access Redirect settings**

To verify that the Domino Web Access Redirect database is properly configured, perform the following steps:

1. Launch a Web browser and enter the URL of the Domino Web Access Redirect database. In our example, we used:
   
   http://dommad.rchland.ibm.com/dwaredir.nsf

2. When prompted, enter your Domino user name and password. You should be redirected to your mail file.
Configuring the Domino Web Access portlet

The Domino Web Access portlet is installed with WebSphere Portal Express Version 6. To use the portlet, you can find it in the portlet list and add it to any WebSphere Portal Express page.

As a portal administrator, you must configure the Domino Web Access portlet to make it work properly. Perform the following steps:

1. Log on to the WebSphere Portal Express server as a portal administrator.
2. In the upper-right corner of the Domino Web Access portlet, click the drop-down icon and select **Edit Shared Settings**.
3. Set the Source field to **Let the DWA Redirector find my mail database**.
4. Click **Save**. See Figure A-8.

![Figure A-8 Domino Web Access portlet settings](image)

5. Click the **Administration** link at the bottom of the window to launch the Portal Administration page.
6. From the left navigation pane, select **Portlet Management** → **Portlets**.

7. On the Manage Portlets page, enter **Domino Web Access** in the search box (Figure A-9) and click the **Search** button.

8. To access the Domino Web Access portlet, click the **Configure Portlet** icon (the third icon).

9. Click the **Edit parameter** icon (the first icon) for **DWARedirectDB**.

10. Enter the Domino Web Access Redirect database file name as the value for the **DWARedirectDB** parameter. In our example the database name is **dwarendir**. See Figure A-10.

    **Important:** Do not add the file extension of .nsf to the file name. Otherwise, the redirect can fail.

   Click **OK**.

---

**Figure A-9   Managing portlets in Portal Administration**

**Figure A-10   Entering value for DWARedirDB parameter**
11. The value just entered should be displayed in the Value column for the DWARedirDB parameter as shown in Figure A-11. Click OK to save the settings.

![Figure A-11 Domino Web Access portlet parameters]

12. You should see a message like the one shown in Figure A-12, indicating the settings were saved successfully.

![Figure A-12 Domino Web Access portlet settings saved successfully]

13. Log on to the WebSphere Portal Express server with different users. Verify their mail can be displayed successfully as shown in Figure A-13.

![Figure A-13 Example of Domino Web Access portlet]
Related publications

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

IBM Redbooks

For information about ordering these publications, see "How to get Redbooks" on page 286. Note that some of the documents referenced here may be available in softcopy only.

- Installing and Configuring WebSphere Portal Express V6 on i5/OS, REDP-4303
- IBM Lotus Domino 6 for iSeries Implementation, SG24-6592
- Understanding LDAP - Design and Implementation, SG24-4986
- Using LDAP for Directory Integration, SG24-6163
- Implementation and Practical Use of LDAP on the IBM eServer iSeries Server, SG24-6193

Other publications

These publications are also relevant as further information sources:

- IBM WebSphere V5.0 Security WebSphere Handbook Series, SG24-6573
- Installing and Managing Sametime 7.5 for i5/OS
  http://www-12.lotus.com/ldd/doc/uafiles.nsf/70817c905428921785256955b0051105c/1a62f6eb0a0a16cc852571ce006f2b9f/$FILE/stinstall.pdf

Online resources

These Web sites are also relevant as further information sources:

- Lotus documentation
- IBM WebSphere Portal, Version 6.0 Information Center
  http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/index.jsp
- WebSphere Version 6 Information Center
  http://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp
- IBM Tivoli Directory Integrator
- Technote 1163790: "Troubleshooting Sametime Awareness in WebSphere Portal"
  http://www.ibm.com/support/docview.wss?rs=899&uid=swg21163790
IBM WebSphere Portal Version 6.0 Release Notes

IBM System i and i5/OS Information Center:
http://publib.boulder.ibm.com/iseries/

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:
ibm.com/redbooks

Help from IBM

IBM Support and downloads
ibm.com/support

IBM Global Services
ibm.com/services
Enabling Collaboration in WebSphere Portal Express V6 on i5/OS
Enabling Collaboration in WebSphere Portal Express V6 on i5/OS
Enabling Collaboration in WebSphere Portal Express V6 on i5/OS

Examples using IBM Directory Server, Domino LDAP, and Microsoft Active Directory

Comprehensive step-by-step guide

Tips and common pitfalls explained

This IBM Redpaper publication shows you how to integrate collaboration into WebSphere Portal Express Version 6 running on i5/OS. Specifically this paper shows you how to integrate IBM Lotus Domino mail and applications, IBM Lotus Sametime, and Microsoft Exchange into a WebSphere Portal environment. Three different scenarios are presented. The first scenario focuses on using Domino LDAP as the common directory server between Domino and WebSphere Portal. Scenario two uses IBM Directory Server. The third scenario shows you how to use Microsoft Active Directory as the common directory server between Domino and WebSphere Portal.

This Redpaper is for system administrators who need to understand how to configure and enable collaboration in a WebSphere Portal Express V6 environment running on i5/OS.