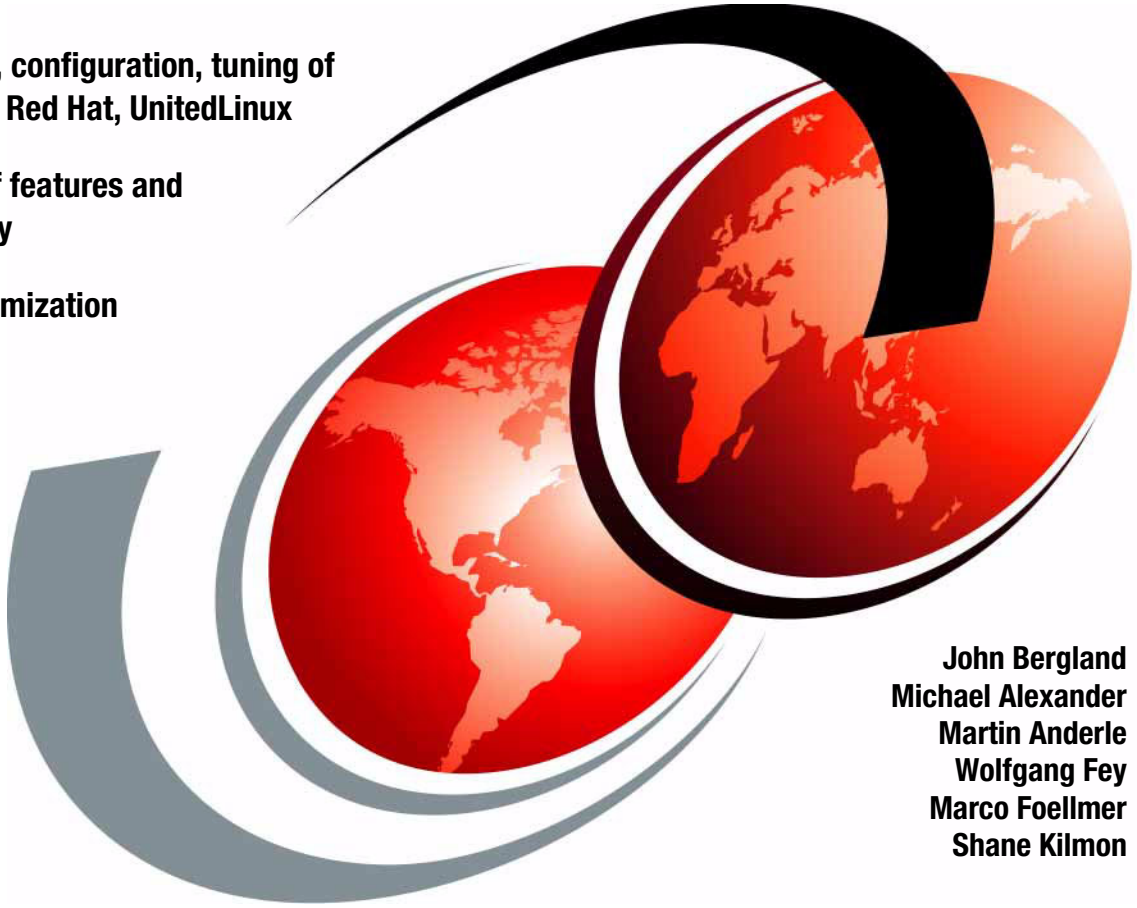
Lotus. software

IBM

Domino Web Access 6.5 on Linux

- Installation, configuration, tuning of DWA 6.5 on Red Hat, UnitedLinux
- Overview of features and functionality
- Basic customization techniques



John Bergland
Michael Alexander
Martin Anderle
Wolfgang Fey
Marco Foellmer
Shane Kilmon

Redbooks

ibm.com/redbooks

International Technical Support Organization

Domino Web Access 6.5 on Linux

April 2004

SG24-7060-01

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

Second Edition (April 2004)

This edition applies to Domino Web Access Release 6.5

Contents

Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

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

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

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

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

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

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

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

Trademarks

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

AIX®
Domino Designer®
Domino®
DB2®
@server®
IBM®
ibm.com®
iNotes™
iSeries™
Lotus®
Lotus Enterprise Integrator®
Lotus Notes®
Notes®
OS/2®
pSeries®
Redbooks™
Redbooks (logo) ™
Sametime®
ServeRAID™
SP2®
Tivoli®
WebSphere®
Workplace Messaging™
xSeries®
zSeries®

The following terms are trademarks of other companies:

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

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

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

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

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

Preface

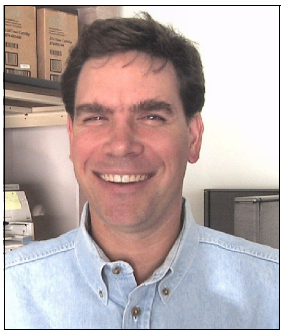
This IBM® Redbook provides a detailed technical overview of IBM Lotus® Domino® Web Access 6.5 (IBM Lotus iNotes™ Web Access), discussing how to install, configure, and deploy an end-to-end Linux solution for Domino. In addition to setting up Domino Web Access 6.5, the book discusses how to integrate Lotus Sametime® for real-time collaboration and awareness. Finally, we explore key deployment considerations, integration points between Domino Web Access and IBM WebSphere® Portal, and some possible approaches and techniques to customizing the program.

Domino Web Access 6.5 is a sophisticated Web client that gives end users many of the messaging and collaboration features previously available only with an Lotus Notes® client. Browser users can take full advantage of Domino services through an ultra-intuitive, easy-to-use interface—both online and offline, seamlessly. Domino Web Access was architected using the latest Web application development technologies and can be centrally administered, helping organizations to drive down deployment costs and reduce Total Cost of Ownership.

Beginning with Domino 6.5, you can access Lotus Domino on a Linux server and use Domino Web Access on a Linux desktop for a leading-edge, end-to-end collaborative solution for Linux.

The team that wrote this redbook

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



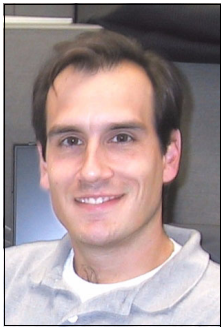
John Bergland is a Project Leader at the International Technical Support Organization, Cambridge Center. He manages projects that produce Redbooks™ about Lotus software products. Before joining the ITSO in 2003, John worked as an Advisory IT Specialist with IBM Software Services for Lotus (ISSL), specializing in Notes and Domino messaging and collaborative solutions.

Michael Alexander is an Advisory Software Engineer in Austin, Texas, where he works on the Lotus Support Engineering Team (SET). In this role he is responsible for investigating, troubleshooting, and providing resolutions to customer issues being worked by several support teams around the Lotus Brand and Software Group. Originally joining IBM to support cc:Mail, Michael has been in the Lotus brand since 1998. He enjoys his job as a hobby (most of the time) and has worked in the past on the cc:Mail and Notes/Domino products and more recently has worked with IBM Lotus Instant Messaging (Sametime).

Martin Anderle is an independent consultant who works with AdHoc Ltd., Prague, Czech Republic. (http://www.adhoc.cz). He has in-depth knowledge of Linux, Domino, and relational database (Oracle). As a principal Domino on Linux consultant, he leads and participates in projects focused on system architecture, planning and overall system tuning. Martin has more than six years of experience in system administration and integration. His time is dedicated mainly to European pharmaceutical giant Alliance-Unichem CZ.

Wolfgang Fey works for ebf-EDV Beratung Foellmer GmbH in Muenster, Germany (http://www.ebf.de). He is a Lotus Certified Professional Administrator R5 at the Principal level. He has more than 10 years of experience in solution design and architecture, as well as in system consulting and integration and project management. He has in-depth knowledge of the banking and insurance industries and in the operation of data processing centers. He has successfully managed various projects in which he was involved in the design and architecture of Lotus Notes/Domino infrastructure and the development of several Notes/Domino applications for the Notes Client and the Domino Web interface.

Marco Foellmer is President and Co-Founder of ebf-EDV Beratung Foellmer GmbH in Cologne, Germany (http://www.ebf.de). He is an IBM Certified Professional for Lotus and Tivoli®. He has more than 15 years of experience in solution design and architecture, as well as in system consulting and integration. He has in-depth knowledge of the banking and insurance industries and in operation of data processing centers. Marco has successfully managed various projects in which he was involved in the design and architecture of a large-scale Lotus Messaging infrastructure and tight integration with Lotus products and LDAP, SAP, and DB2®. Since the beginning of iNotes (now Domino Web Access), he has worked very closely with Lotus Development. He offers a sincere “thank you” to the iNotes Development team.



Shane Kilmon is an Advisory Software Engineer with IBM, based in Westford, Mass. He currently has the lead role of planning and tracking RAS features for Notes/Domino and Extended Products, as part of the RAS (Reliability, Availability, Serviceability) Engineering team. Prior to joining this group, he was the Primary for the UNIX® PAE team in Lotus Support for five years. He has been with IBM/Lotus for seven years, and has more than 12 years of experience in administering and supporting UNIX operating systems.

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

Scott Knupp, *Business Executive, Corporate Linux*
IBM

The entire redbook team wishes to extend a sincere thank you to the Domino Web Access Development team for their help and support in writing this book.

Vinod Seraphin, *Lead Architect, Domino Web Access Development*
IBM, Westford, Mass.

John LeJeune, *Domino Web Access Development*
IBM, Westford, Mass.

Jason Dumont, *Product Management Team, Domino Web Access*
IBM, Westford, Mass.

John Immerman, *Software Programming Manager, Domino Web Access*
IBM, Westford, Mass.

Jeff Jablonski *Domino Web Access Development*
IBM, Westford, Mass.

Linda Sharar, *Advisory Software Engineer, Domino Web Access*
IBM, Westford, Mass.

Mark Oslowski, *Domino Web Access Development*
IBM Westford, Mass.

Become a published author

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

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

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. JLU Building 107-2
  3605 Highway 52N
  Rochester, Minnesota 55901-7829

Part 1

Introduction to Domino Web Access 6.5

1

Introduction to Domino Web Access 6.5 on Linux

IBM Lotus Domino Web Access 6.5 (IBM Lotus iNotes Web Access) is a sophisticated Web client that gives end users many of the messaging and collaboration features previously available only with an Lotus Notes client. Browser users can take full advantage of Domino services through an ultra-intuitive, easy-to-use interface both online and offline, seamlessly. Domino Web Access was architected using the latest Web application development technologies and can be centrally administered, helping organizations to drive down deployment costs and reduce Total Cost of Ownership.

Beginning with release of Domino 6.5, you can access Lotus Domino on a Linux server, while using Domino Web Access on a Linux desktop making for a leading-edge, end-to-end collaborative solution for Linux.

Within this book, we provide a detailed technical overview of Domino Web Access 6.5 and discuss how to install, configure, and deploy an end-to-end Linux solution for Domino. When the environment is set up and configured, we also discuss how to integrate Lotus Sametime for real-time collaboration and awareness. Finally, we discuss key integration points between Domino Web Access and IBM WebSphere Portal, as well as some possible approaches and techniques to customizing Domino Web Access 6.5.

1.1 Overview of Domino Web Access 6.5

Domino Web Access 6.5 (DWA 6.5) delivers Lotus Notes and Lotus Domino capabilities on the Web, providing users with fully functional access to corporate messaging services, collaborative services, and personal information management regardless of where or how they may be working. Figure 1-1 illustrates the Welcome Page from within a Mozilla 1.3.1 browser. By clicking one of the tabs across the top of the Welcome Page, users can access their mail, calendar, to-do list, contact list, or notebook. Chapter 2 provides an in-depth review of these features and functionality.

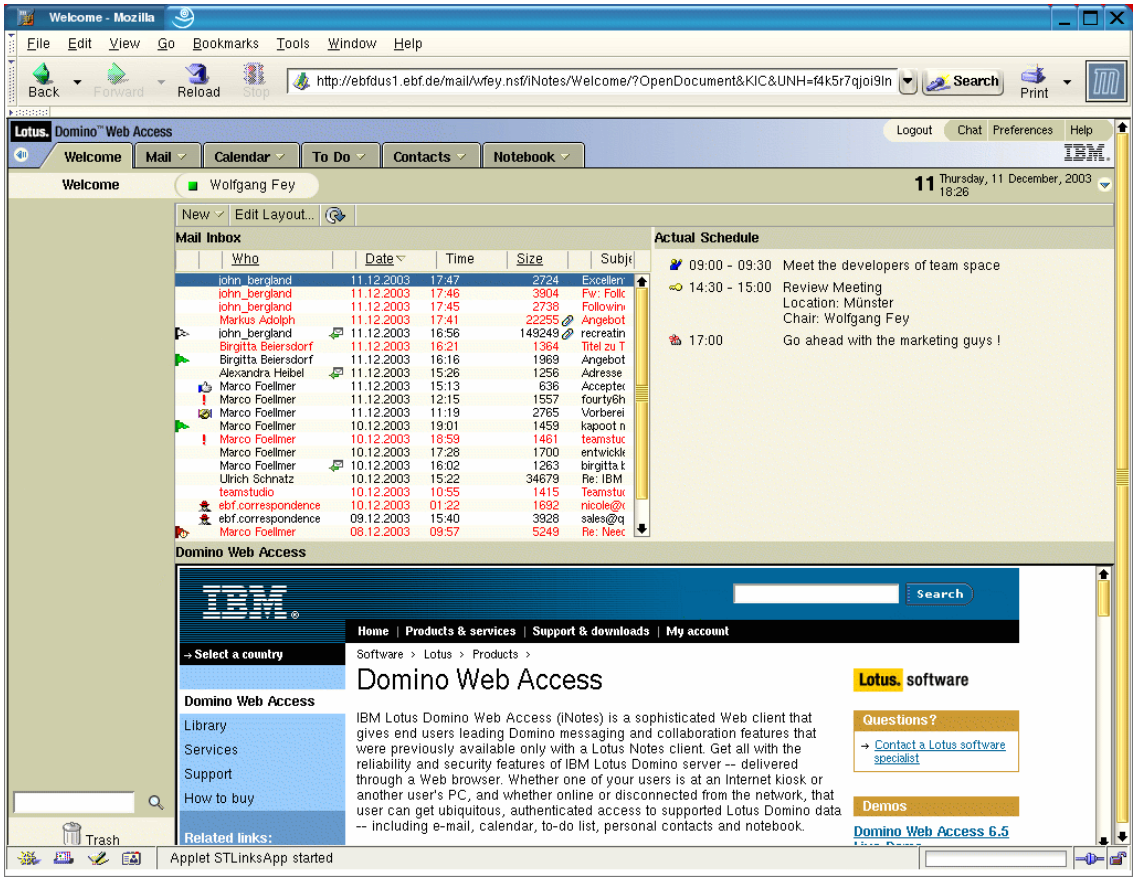


Figure 1-1 Domino Web Access 6.5 Welcome page on Linux

The key goals and functional improvements for this release of Domino Web Access are as follows:

- **End-to-End Linux solution**. Domino Web Access 6.5 enables you to access Lotus Domino on a Linux server, from a Linux desktop, giving you a leading-edge, end-to-end collaborative solution for Linux. This is especially significant as the application is the first Domino messaging client available for Linux.
- **Integrated Lotus Sametime Instant Messaging**. Integrates Lotus Instant Messaging function to provide presence awareness and enable users to initiate chats and collaborate with colleagues without launching a separate application.
- **Performance and scalability improvements**. Domino Web Access software delivers new levels of scalability and support for large numbers of concurrent users. For example, it caches static data, such as e-mail forms, for greater efficiency. eliminating the need for Domino Web Access to pull this data from disk for each session. Users should see a marked improvement in performance. Additionally, when combined with Linux (as a supported platform for Lotus Domino server) as the back end for Lotus Domino Web Access software, this provides several options for increased flexibility and scalability.
- **Security-rich environment**. Security is paramount in a browser client. Domino Web Access supports basic authentication, session authentication, secure logoff, Secure Sockets Layer encryption, local offline file encryption, and active content filtering.
- **Usability and productivity improvements**. In addition to overall usability improvements, specific functionality and tools have been improved to help make users more productive. Some of the highlights include:
  - Follow-up flags: Users can mark entries in their mail with a follow-up flag to indicate that further action is warranted, maximizing user responsiveness to incoming requests.
  - Mail rules and spam-blocking functionality: The Block Mail from Sender function enables users to block future messages from a specified sender, prevent displaying them in the Inbox view, and automatically move them to the Junk Mail folder.
  - Enhanced calendaring and scheduling tools: Advanced calendaring and scheduling capabilities in Lotus Domino Web Access 6.5 enable users to perform even more actions from a browser, further enhancing productivity.

Chapter 2 provides much greater detail about features and the functionality of Domino Web Access 6.5.

1.2 Why Domino Web Access 6.5?

IBM estimates that as many as to 20% of employees are considered "*deskless* workers: those who do not have a dedicated workspace but still need to access the same messaging and back-end business applications as the rest of the company. This new category of users, such as factory floor workers, airline pilots, and retail workers, represents a new market opportunity for Lotus Software, as most browser-based messaging solutions do not have the security features, performance, feature set, or reliability that Domino Web Access delivers to the corporate market.

Domino Web Access 6.5 allows businesses to easily integrate remote workers with critical data and applications. Users have access to Lotus Domino-based applications, including e-mail, calendaring, and scheduling, anywhere they can find an Internet connection, without sacrificing the full application functionality of a standard Lotus Notes client. Combining the flexibility and manageability of a corporate-level, fully functional Web client with the performance and security features of Linux will help IBM reach an emerging market of new users and can help customers lower the overall costs of their messaging solutions.

1.2.1 Positioning of Domino Web Access as a messaging client

Given the recent introduction of Lotus Workplace Messaging™ 1.0, it is important to understand the positioning of Domino Web Access 6.5 against both Lotus Workplace Messaging 1.0 and the "rich" functionality of the Notes 6.5 client.

Domino Web Access 6.5 is positioned to provide both a very high level of functionality and rich user experience, while also providing key flexibility by offering its features through a browser. Office workers may need browser-based access to their Lotus Notes data while at home or traveling. Additionally, workers who receive only a moderate amount of e-mail may not require a full IBM Lotus Notes client, because they access e-mail through a shared workstation.You can help meet these varying requirements by providing critical messaging, collaboration, and personal information management access when users need it. Figure 1-2 on page 7 illustrates how Domino Web Access 6.5 fits into the Notes and Domino client strategy in terms of both required functionality and frequency of use.

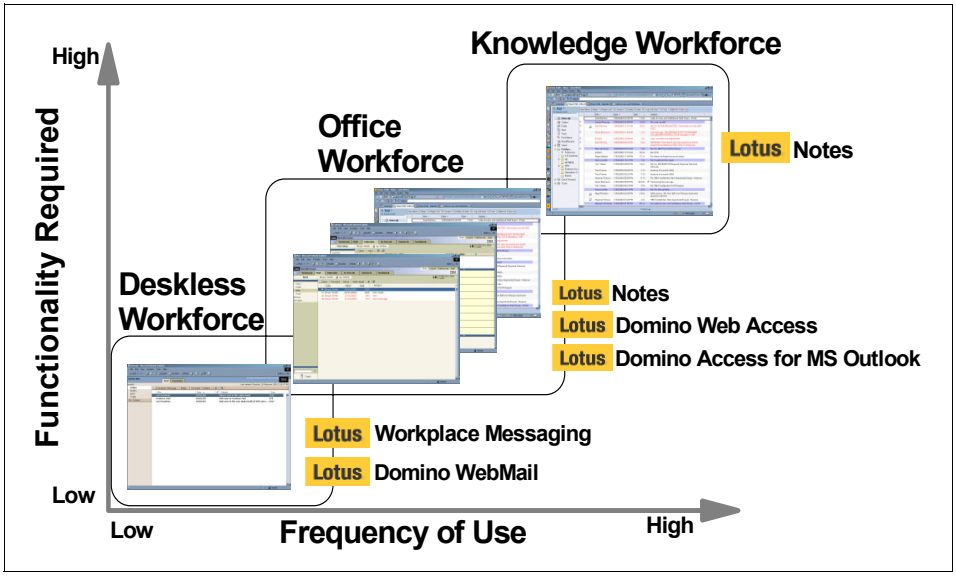


Figure 1-2 Positioning of Domino Web Access against other Notes mail clients

1.3 Overview of Domino Web Access architecture

Domino Web Access is composed of three main components that we need an understanding of to put together a picture of how the system works:

- The client side, which includes the user interface and several distributed elements, such as much of the integration with IBM Lotus Instant Messaging
- The server side, where administration is done and broad customizations are set
- The offline component that lives on the client and requires minimal configuration on the server

In this section, we provide a general picture of what makes these pieces work and give background helpful to understanding the following chapters.

1.3.1 Domino Web Access as a client application

The majority of the Domino Web Access user interface is built around parts standardized Web technologies that are broadly implemented and agreed on by the W3C (http://www.w3c.org). Having said that, it is important to recognize that Domino Web Access uses several elements of DHTML and makes some specific requirements of the browser that will be used. For that reason, IBM currently

certifies only Internet Explorer for Microsoft® Windows®, and Mozilla for Linux clients. The specific requirements of a browser to host Domino Web Access are beyond the scope of this book. The exact browser elements required to make a browser certified are not specifically published, both to insulate against changing technologies and to ensure that implementers of Domino Web Access recognize the supported platforms. Here, we simply discuss the architecture underlying the application to enable a better understanding of how and why it works.

If you have seen the Domino Web Access interface, you might ask yourself "what cool Java/Active X/plug-in are they using to do that?" When you recognize that you can right-click on elements to open context-sensitive menus, press <F9> to refresh the Inbox, and take advantage of sortable columns, it is clear that the DWA development team has gone to great extremes to provide rich client functionality *through a Web browser*. As previously stated, these and other features are implemented in an essentially platform-neutral (standardized) way, which greatly reduces the maintenance costs associated with proprietary plug-in technologies. The heart of Domino Web Access is driven by JavaScript, Cascading Style Sheets, and current HTML standards. These forms and components have been created to provide a rich interface that delivers the most useful features of the Notes client for e-mail and Personal Information Management (PIM) usage, while keeping a small footprint. These features and look and feel can be customized to a large degree, as will be discussed in Chapter 11, "Customizing Domino Web Access" on page 349.

From an architectural perspective, the main considerations that are required of your browser are support for JavaScript and HTML layers (using tags) for the user interface. The client is delivered in a total of up to 23 HTTP requests when initially loaded, depending on the configuration. These requests include most of the icons, style sheets, and HTML pages, as well as the JavaScript files that provide functions referenced in the client application. All of this is required to present the rich interface that we expect from a top-tier client. However, due to the compression technology incorporated into the Domino 6.5 HTTP stack, and the supported browser clients, the footprint to download all of these elements is minimal at about 15K. This excludes one-time download elements such as stlinks.jar (used for Sametime integration).

1.3.2 Domino Web Access as a server application

The Domino Web Access server components are housed primarily in three locations:

- Flat file resources (discussed in the next section)
- Common elements that are shared by all DWA users
- The user mail file itself

We could extend this model one step further to say that user mail files are based on a shared common template, but it is unimportant to DWA proper and can be left for our readers to explore.

The primary difference between Domino Web Access as a Web application and a Web application created outside of IBM Lotus is that the level of integration here goes deeper than can be achieved within the Domino Designer® or even DSAPI, LSX, or other API interfaces that are exposed publicly. The Web server actually identifies most DWA-related requests and handles them differently from URLs that identify resources within a given database.

Because Domino Web Access is driven over the Web, the server application is affected by changes to the HTTP stack between Domino R5 and 6 as well. The most obvious of these changes are new controls on the server document and the ability to configure Internet Site documents to refine control of servers that host multiple sites and sites that are hosted over multiple nodes. Additionally, there are new rules for redirection, URL substitution, Directory Rules (replacing Directory Mapping), and a new facility to use HTTP headers to control sites. None of these requires additional configuration in most cases but can be used to ease server consolidation, migration from external systems, and scalability.

Later in this book we cover administration and customization issues that are important for administrators, designers, and users. At this point, the goal is simply to understand that Domino Web Access is functionally quite different from the typical Domino Web application.

1.3.3 Domino Web Access as an offline application

One of the very appealing characteristics of Domino Web Access is the ability to take mail offline and operate with almost full functionality while accessing only local data. This is done by having a well-designed client that can adapt to and handle being run locally, while also using the Domino Offline Services to provide a locally executed Domino server. The structure of this is worth some note on the Linux platform because it differs from the Windows version in some ways. A brief introduction here is helpful for background information when reading Chapter 3, “Deployment considerations” on page 59, and Chapter 8, “Linux Clients for DWA 6.5” on page 263.

The moving parts here are the same as those described in 1.3.1, “Domino Web Access as a client application” on page 7, with the addition of a plug-in that is used to install and set up our local subscription. The workflow is simply that a plug-in is installed in the browser when the *offline* button is clicked the first time. On the second click, you are given the opportunity to install a subscription locally. Subsequent clicks of this button then enable you either to synchronize a mail file subscription or go offline.

The plug-in setup is done by a small installer in the standard Netscape/Mozilla format (xpi). The installer contains two files in particular that must be installed locally. At this time they must go into a shared directory, as discussed Chapter 8, “Linux Clients for DWA 6.5” on page 263. (More specifically, this topic is discussed in depth in 8.4.4, “Working offline” on page 301.) After these files are installed and you restart the client (browser), you can create a local subscription.

Creating a local subscription involves a six-part installation. The install is delivered over HTTP or HTTPS and downloads approximately 180 MB of Domino program files and support files. These files provide services to access mail offline, look up names offline, search mail, and replicate/synchronize mail when you get back online. This is in addition to the size of the mail file that is being taken offline and, as such, suggests that one should only do this initial setup over a fast connection in order to see acceptable performance.

After it is installed, the local subscription is accessed by clicking the **offline** button in the mail interface again. This starts the HTTP server and manages DOLS processes. (This is reviewed in greater detail in Chapter 8, “Linux Clients for DWA 6.5” on page 263.) As an alternative to starting the offline services by clicking the link in the online client, you can start it by clicking an icon that is installed on the desktop for most KDE and Gnome users or by creating your own link to start the local server.

1.4 Why Linux?

The benefits of Linux as an operating system (OS) is a broad topic, and Linux enthusiasts could provide many pages of details here. The objective of this section is to focus on some of the key reasons for its increasing popularity.

Linux is not just another operating system. Since its introduction in 1991, no other OS in history has grown in popularity as quickly and across as wide a range of systems. The primary reason for this is *flexibility*. Unlike other OSs, Linux can run on any hardware. It enables companies to unify their diverse operating environments without replacing current hardware. In the end, Linux simplifies application development and lowers costs.

IBM continues to demonstrate strong support for Linux, as it is a key component in the IBM strategy for moving away from closed, proprietary systems and opening up its software and services to the outside world. Linux was developed for an open world, too. By running on everyone’s technology, it neutralizes any vendor’s ability to exercise control over customers and developers.

Customers want to know how IBM Linux solutions can improve their performance, reduce their costs, and ultimately generate revenue. By providing support for Linux, benefits may be realized in the following ways:

- **Workload consolidation**: Customers can achieve substantial savings by using Linux to consolidate workloads from multiple servers onto a single server. It is possible to replace existing multiple-server installations of UNIX or Windows NT® with IBM eserver zSeries®, iSeries™, pSeries®, and xSeries® servers running Linux in dozens, or even thousands of partitions, with each partition simulating an individual, independent server.
- **Linux clusters**: Combining the power of Linux with IBM clustering experience can provide customers with supercomputing capability and scalability at a much lower price point. Case in point: Customers have experienced a performance improvement of 2% to 3% at a price that is 50% less. By installing large Linux superclusters, it is possible to take collections of independent boxes, with all of the infrastructure and management functions, and transform them into complete systems.
- **Distributed enterprise**: Linux is the ideal platform for enterprises that have branch offices, stores, or even kiosks and point-of-sale (POS) terminals requiring low-cost, centrally managed, robust servers that are easy to replicate, highly reliable, and simple to roll out. Complex pricing and inventory structures can be set at a headquarters location and published globally to all POSs, while Linux works in the background to keep information moving and provide rock-solid performance for users.
- **Infrastructure solutions**: The huge installed base of aging Windows and Novell NetWare file and print servers offers a great opportunity to upgrade to more powerful xSeries or Intel®-based servers running Linux. We can help customers build a compelling business case on the cost and performance advantages of Linux over NT.

1.4.1 Domino Web Access 6.5 on Linux: a compelling solution

By combining the functionality of the rich feature set of Domino Web Access 6.5 with support for both server and client platforms running on Linux, a very compelling case can be made for running a complete collaborative solution on Linux. As you can see from Figure 1-3 on page 12, DWA 6.5 on Linux provides benefits in terms of broad-based coverage, comprehensive server support, and rich functionality:

- **Broad-based coverage**: DWA 6.5 on Linux provides the end-to-end Linux solution, leveraging the benefits and flexibility of Linux on both the server and the client platforms.

- **Comprehensive server support**: Linux runs on a broad range of server architectures. Within the IBM series of servers, this includes servers from the Intel-based xSeries to the large-scale zSeries mainframe-based servers.
- **Rich functionality**: Domino Web Access 6.5 provides a very rich feature set, including integrated instant messaging, with all features accessible through a Web browser.

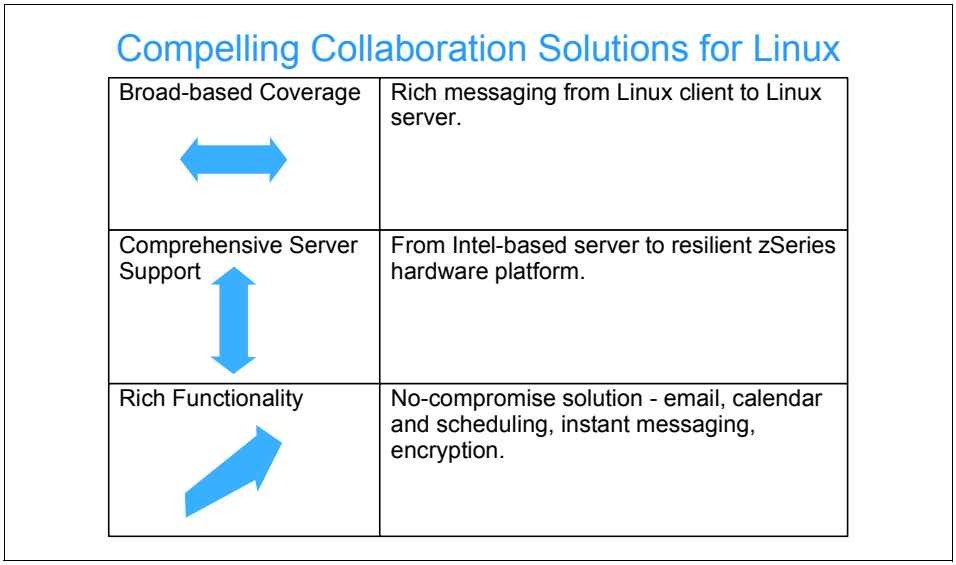


Figure 1-3 Collaborative solutions on Linux

1.5 The structure of this book

This book has four parts:

- **Part 1, “Introduction to Domino Web Access 6.5” on page 1**

  The current chapter provides an overview of Domino Web Access, its capabilities, and positioning, and a high-level architectural overview.

  In Chapter 2, “New features of Domino Web Access 6.5” on page 15, we discuss the new features in significant detail. We also provide a comparison of functionality between Domino Web Access 6.5, the Lotus Notes client, Domino Web Mail 6.5, and Lotus Workplace Messaging 1.0. This comparison should help customers better understand the positioning of Domino Web Access 6.5 against other Lotus messaging clients.

- **Part 2, "Deployment and administration" on page 57**

  Chapter 3, "Deployment considerations" on page 59, discusses key issues that should be taken into consideration when planning a deployment of Domino Web Access 6.5., such as the measures that should be taken to ensure high availability, scalability, security, and integration with other systems or portal environments.

  Chapter 4, "Installing Linux" on page 75, describes how to install Red Hat and UnitedLinux on your server. Each of the chapter's two parts gives detailed instructions for these particular distributions of Linux, which are the two officially supported Linux distributions for Domino Web Access 6.5.

  Chapter 5, "Installation and setup of Domino Web Access 6.5 on Linux" on page 153, discusses how to install and configure Domino Web Access 6.5 on a Linux server. First, we address how to ensure that your Linux system is properly configured for Domino. Next, we describe in detail how to install, configure, and launch the Domino server. Finally, we provide tips for how to make your environment more user-friendly.

  Chapter 6, "Security and administration" on page 205 describes the basics of Linux and Domino security and what you can do to achieve an appropriate level of security. We touch on physical, system, and network security for Linux, then discuss partitions, scripts, and scheduling jobs. For Domino, we review steps that you should take to secure your new server, then discuss the enhanced Web administration client and the new Domino Controller available with Domino 6.

  Chapter 7, "Configuration and tuning" on page 245 discusses some ways to configure and tune Domino Web Access 6.5. It begins with some Linux OS considerations, and follows with ways to modify the behavior and performance of Domino Web Access itself. There are already many available references that cover overall Linux OS tuning, so this topic is not discussed in depth here. Instead, the primary focus is to cover items that are necessary for the proper operation of Domino and Domino Web Access. Finally, some good resources for more detailed information on Linux OS tuning are provided.

- **Part 3, "Clients for Domino Web Access" on page 261**

  Chapter 8, "Linux Clients for DWA 6.5" on page 263, provides an overview of supported browsers for Domino Web Access 6.5. We discuss how to install Mozilla 1.3.1., and then provide an in-depth look at installing and configuring the DOLS client for offline usage.

- **Part 4, "Customization and integration" on page 323**

  Chapter 9, "Integrating Sametime with Domino Web Access 6.5" on page 325, discusses the key new feature of integrating the Lotus Sametime real-time instant messaging and presence awareness capabilities into

Domino Web Access 6.5. It discusses integration of Sametime 3.1 in the following aspects:

- Configuration of Domino Web Access and the Sametime servers
- Configuration of the Mozilla browser on Linux
- Using the Chat feature within the Domino Web Access client

Chapter 10, “WebSphere Portal integration” on page 339, provides an overview of portlets that can be used for integration between Domino Web Access 6.5 and WebSphere Portal 4.1.2 and WebSphere Portal 5.

Finally, Chapter 11, “Customizing Domino Web Access” on page 349, discusses the Domino Web Access 6.5 template architecture and why it is difficult to customize the design beyond the documented ways. However, some things can be customized with a reasonable amount of work. Several specific examples are covered in this chapter.

- **Part 5, “Appendixes” on page 385**

Appendix A, “WebSphere Portal 5 installation on Linux” on page 387 provides a walkthrough of installing WebSphere Portal 5 on Linux. In addition to providing readers with instructions about installing Portal, this serves to further demonstrate a complete end-to-end solution on Linux.

Appendix B, “Configuring Internet Cluster Manager” on page 435, describes how to configure the Internet Cluster Manager (ICM). It serves as a reference point for ICM installation and configuration from the discussion in Chapter 3, “Deployment considerations” on page 59.

2

New features of Domino Web Access 6.5

This chapter outlines the new features and enhancements in Domino Web Access 6.5. It also provides a detailed comparison table illustrating the key feature comparisons between IBM/Lotus messaging clients: Domino Web Access 6.5, Lotus Notes Client 6.5, Domino Webmail 6.5, and IBM Lotus Workplace Messaging 1.0.

2.1 Domino Web Access 6.5: true Web-based application fidelity

With the introduction of Domino Web Access 6.5, Lotus has set a new standard for application fidelity. This is an important design goal, and the term deserves further clarification as we set the context for describing the new features and functionality in Version 6.5.

In the primary sense, application fidelity means that the application functions the same way whether online or offline. This includes the ability to create, edit, and delete data. This is one of the unique features of Lotus Domino because only through Domino replication can an application be taken offline and used with full fidelity and access to data from a Web browser or Lotus Notes client. When the user reconnects, the offline work is fully synchronized with the server, and the integrity of the data is maintained.

In terms of Web-based functionality, Domino Web Access 6.5 also achieves application fidelity through functional parity with the Lotus Notes client. As of this writing, DWA 6.5 is the most comprehensive breed of application fidelity in Web browser access to messaging and advanced calendaring and scheduling. It can even be used in conjunction with the Lotus Notes client in any mixed environment. Use of either client is not mutually exclusive: The Domino Web Access browser client and the Lotus Notes Client can be used together in a seamless manner. The mail template and the Lotus Domino Server processes support concurrent user scenarios for each platform. Even if the browser is unsupported by Domino Web Access 6.5, you have the ability to work with Domino Webmail as an alternative.

With the introduction of Version 6.5, Lotus extends the benefits of this application fidelity to the Linux platform. One major goal of Domino Web Access 6.5 is to support an additional platform and browser: namely Mozilla 1.3.1 on Linux.

2.2 Overview of new features

IBM Lotus Domino Web Access 6.5 delivers advanced functionality and an enhanced user interface. The new functionality is described in the subsequent sections to give you a thorough overview. Accompanying each description of functionality, we have added a screen shot taken from a Mozilla browser running on Linux. We discuss new features and functionality in the following topics:

- General enhancements
- Linux platform support
- Mail enhancements

- Calendar and To Do enhancements
- Print enhancements
- Usability enhancements
- New administrative features
- Template customization
- Server-side enhancements

2.2.1 General enhancements

The following section discusses several of the most notable enhancements to Domino Web Access.

Lotus Instant Messaging integration

Domino Web Access now provides integration with Lotus Instant Messaging to provide presence awareness and instant messaging capability directly from within the Domino Web Access client. The user can see who is online in the Inbox view without having to launch a separate Instant Messaging client or separate browser window. From any name entry, a user can open a chat session with another user by clicking the green or yellow (on-line) indicator. With Domino Web Access 6.5, single sign-on is used to log into both your mail client and Lotus Instant Messaging. Additionally, there is a built-in buddy list, which is stored on the server and reloaded from the server each time a user logs on. Figure 2-1 shows the new, integrated Lotus Instant Messaging functionality.

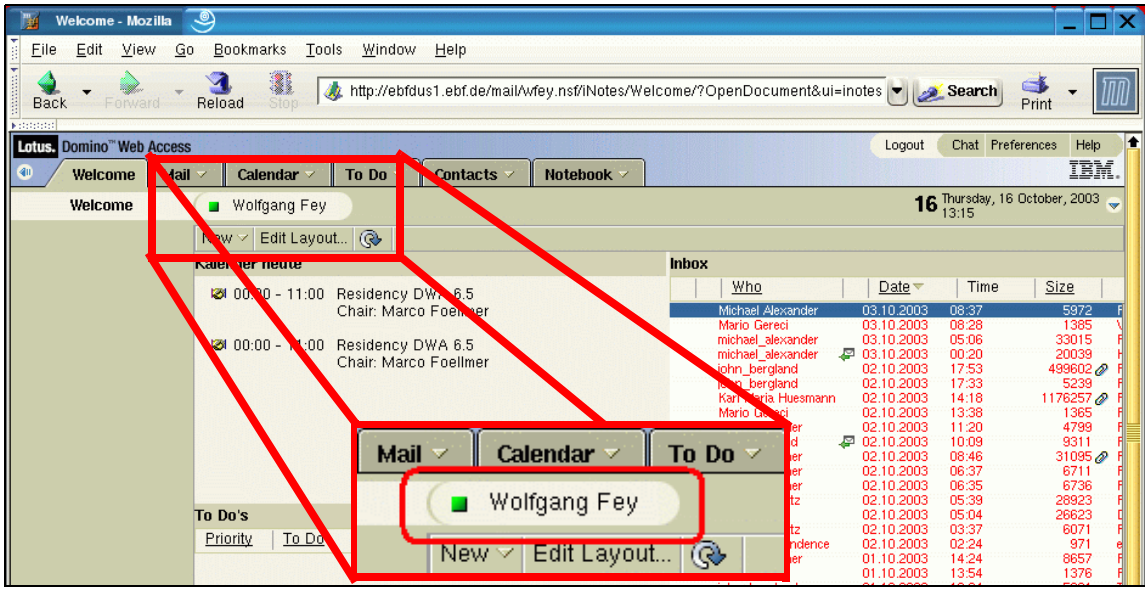


Figure 2-1 Sametime online status in Domino Web Access

Clicking the user name opens a dialog box in which the user can set online status to three different options, as shown in Figure 2-2.

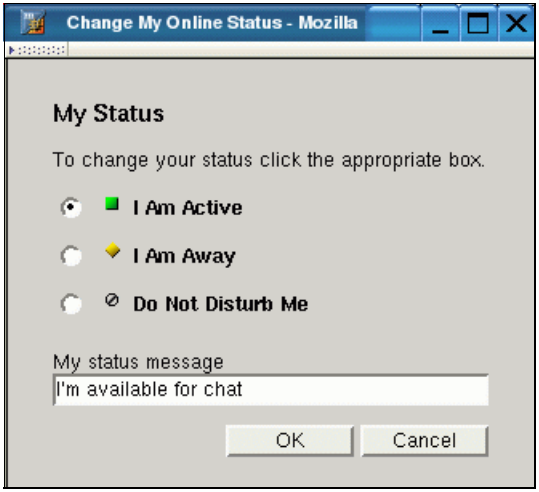


Figure 2-2 Setting the current online status

The online status of any person within the active online community is displayed in any view or folder of Domino Web Access. The user can also click on any active name to open a chat window. This chat dialog interface is similar to the original Sametime user interface and has most of the same capabilities. For example, the user can create an *n*-way chat to communicate with multiple people in the same window. Users can also access tools such as screen sharing and whiteboard capabilities directly from within the Domino Web Access client by clicking the **Add Tools** button.

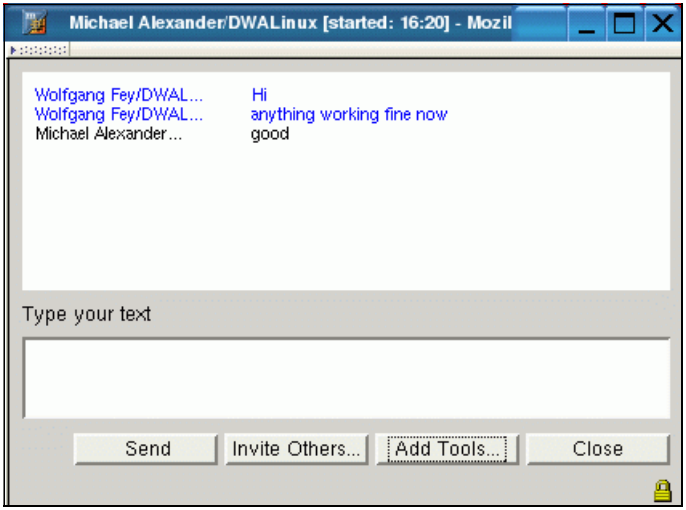


Figure 2-3 Chat window

There is also an interface window for listing users in a Buddy List and displaying their presence awareness status within the community. From within this window, you can add users to the online community, as Figure 2-4 shows.

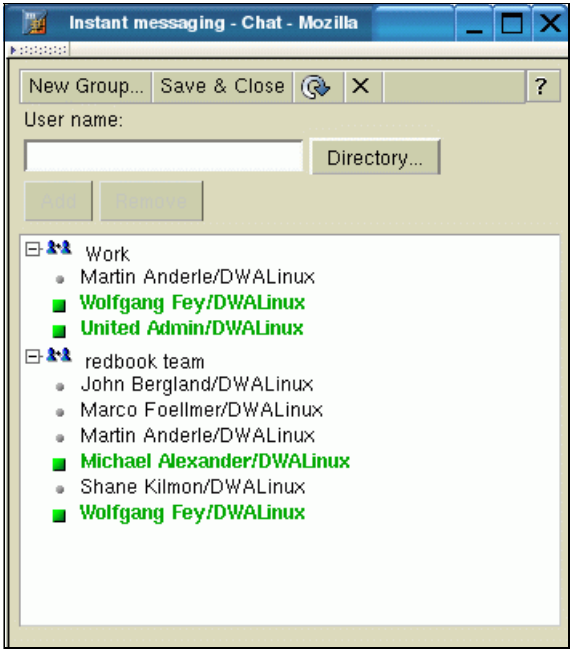


Figure 2-4 Online awareness

Domino Web Access Redirect

Domino Web Access Redirect is a database that resides on the server and processes URLs. With Domino Web Access Redirect, users do not need to know the name of their mail file or mail server. Instead, they need only to know the name of the Domino Web Access Redirect server. This can be any server in their Domino infrastructure.

Domino Web Access Redirect uses Domino authentication methods to access the person document in the public name and address book (the Domino Directory) to learn which server is storing the user's mail file. It takes this information to redirect a user's browser to their mail file. For more about setting up and customizing Domino Web Access Redirect, see 11.5.1, "Setting up Domino Web Access redirector database" on page 371.

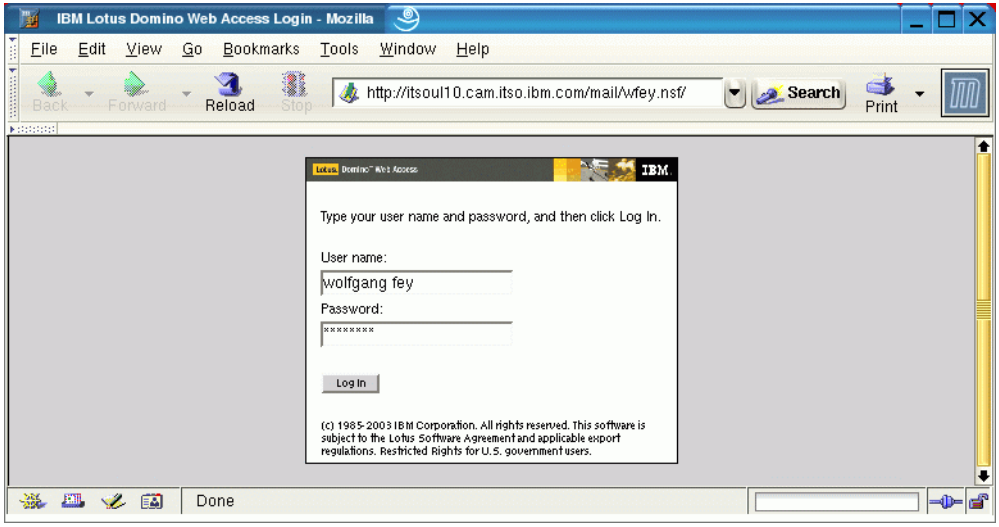


Figure 2-5 Domino Web Access Redirect in Mozilla

Archive locally with offline support

Beginning with Lotus Notes/Domino 5.0.8, users had the ability to create a server-based archive of their mail file. Domino Web Access 6.5 users (using Internet Explorer) now can create and store an archive locally, thereby extending offline support. This further allows users to maximize their productivity while offline. Users can easily access their local or server-based archive from a link in the Domino Web Access user interface. Since this feature is currently only supported using Internet Explorer, and the primary focus of this book is to discuss Linux and Mozilla-supported functionality, further details of this feature are beyond the scope of this book.

2.2.2 Linux platform support

The following sections discuss the highlights of the new Linux support for Domino Web Access.

Linux client support delivered via the Mozilla browser

Domino Web Access 6.5 extends messaging and collaboration to Linux clients with support for the Mozilla browser. This is a very significant enhancement for Domino Web Access, making it the *first-ever* fully supported end-to-end, client-to-server collaboration solution for Linux.

Domino Web Access is now an ideal solution for customers who want to realize the potential cost savings of deploying Linux at both the server and the client side. Because it is a browser-based messaging solution, Domino Web Access can be deployed with little or no client-side deployment cost, which means large potential savings for any organization looking to extend messaging and collaboration to additional users. With the Mozilla browser, the mail file can be taken offline, and a user can take advantage of Lotus Instant Messaging integration when online. Figure 2-6 shows the welcome page from within the Mozilla browser running on Linux.

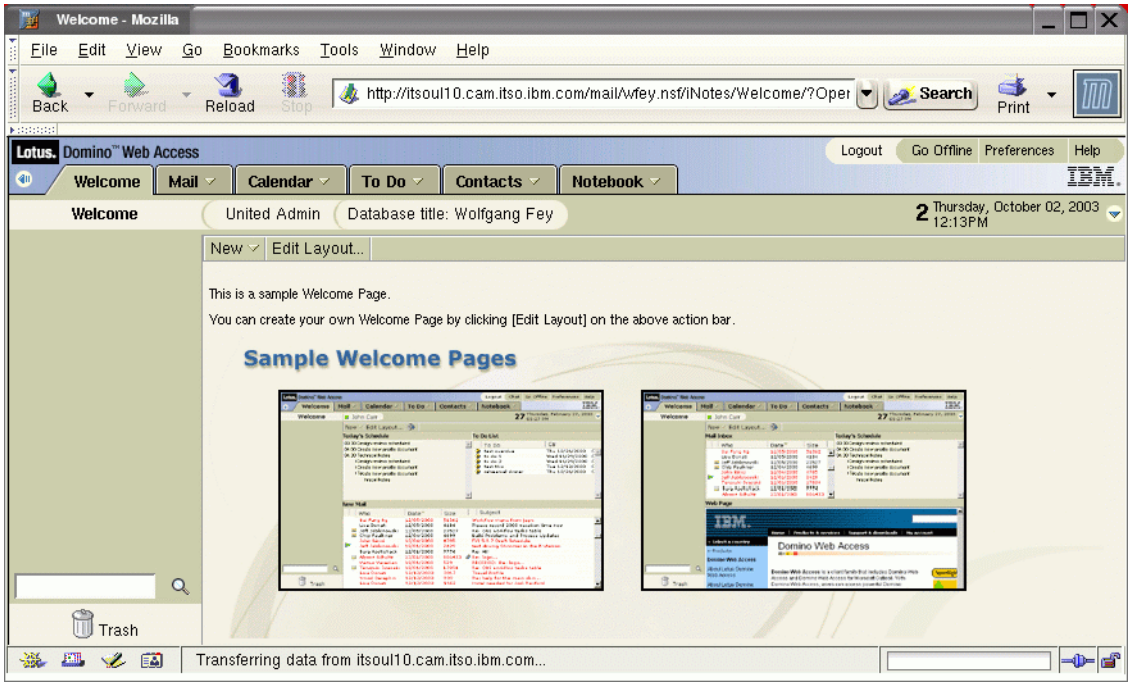


Figure 2-6 Welcome page of Domino Web Access in a Mozilla browser running on Linux

Support for Domino Offline Services on Linux

With the new Domino Offline Services (DOLS) support for Linux, Domino Web Access is the first product available for taking Personal Information Management (PIM) offline, while including the capability to keep the data synchronized with a server. This synchronization capability is required in order to provide normal browser access to Domino Web Access, Lotus Instant Messaging integration, and DOLS support under Linux. Figure 2-7 illustrates DOLS in offline mode.

Note: Be aware, in regard to browser support for Mozilla, that the only version currently supported is 1.3.1 with the Java™ plug-in 1.4.2 patch level 1 running under Linux. See the readme.nsf file that is included with the Domino installation for more information about the supported Linux distributions.

Figure 2-7 DOLS in offline mode

2.2.3 Mail enhancements

This section discusses functional enhancements that have been made to mail handling within Domino Web Access.

Block-Sender Mail Rule

The Block-Sender Mail Rule function within Domino Web Access enables users to add a specified sender name to a block sender list, so that future messages from that address are blocked from displaying in the Inbox view. Future mail from this sender will be moved automatically to the Junk Mail folder. Users can potentially benefit from less junk mail in the Inbox, helping them to more quickly navigate to the important messages and ultimately be more productive. In order

to configure a block-mail rule for a specific name, simply move one mail message from the specific sender to the Junk Mail folder. This automatically configures a rule, causing all subsequent mail from that particular sender address to be automatically moved to the Junk Mail folder.

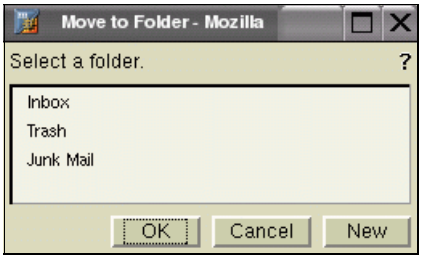


Figure 2-8 Move to Folder dialog with the Junk Mail folder entry

There is also a new function in the Tools menu called Block Sender. Selecting this function while a specific mail message is marked in the Inbox invokes a confirmation dialog box for the blocking request. After confirmation, the sender address can no longer send new mail messages to the user's Inbox.

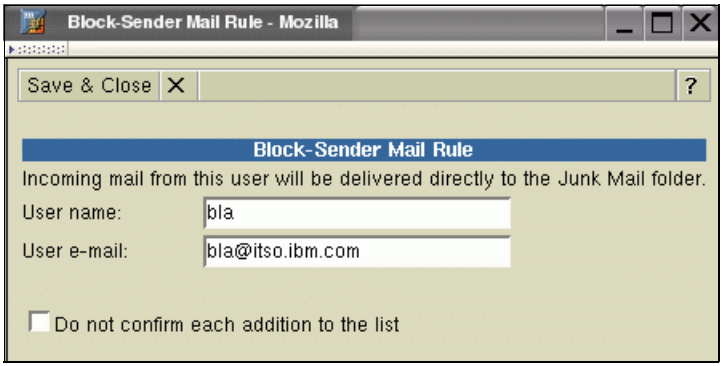


Figure 2-9 Block-Sender Mail Rule dialog

Copy into function

Domino Web Access users now have the ability to copy the body of a received message into a new To Do item or Calendar entry with a single click. This saves time and enables users to manage their daily tasks more efficiently. Note that this function works on the entire rich-text body field, including inline images, tables, and so on. This functionality is supported both in Internet Explorer and in Mozilla under Linux.

While performing basic testing for this book, we found this function to be very robust. We did not encounter any mail messages or content that did not copy correctly. All content was copied and worked as expected.

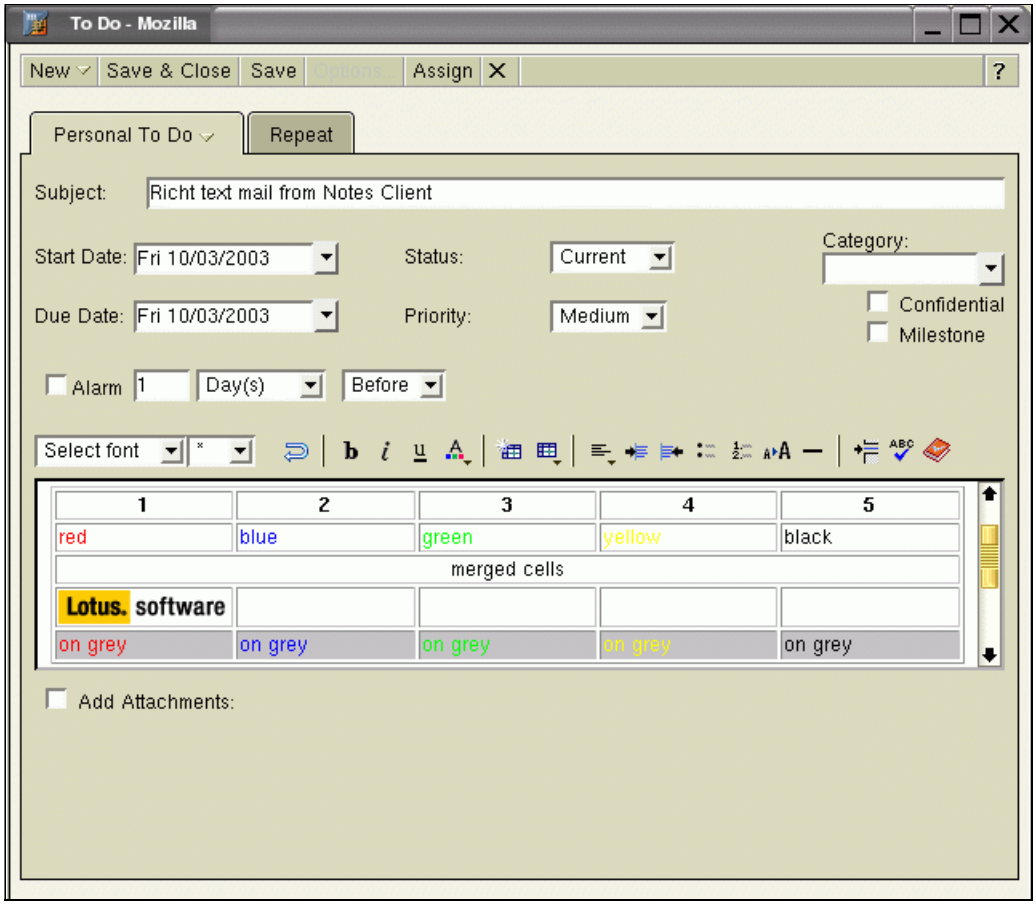


Figure 2-10 Sample To Do dialog showing rich text

Send & File

Similar to Notes client functionality, the Domino Web Access user can now send and file new messages in a single step. Clicking the **Send & File** button sends the document and files it into a folder all in one step, saving time and helping users efficiently manage their Inbox and folders.

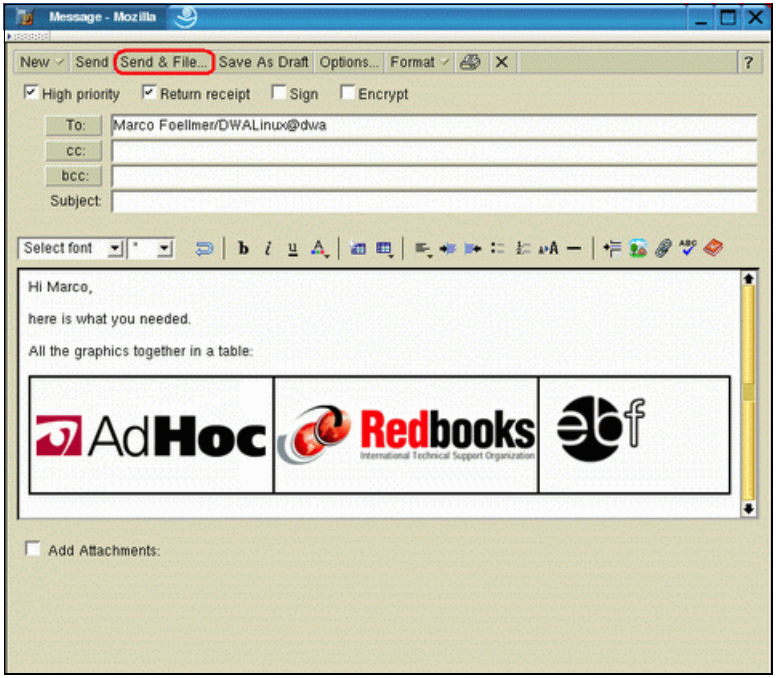


Figure 2-11 Send & File button in new mail message

When using the Send & File button to send a message, a dialog box appears and prompts the user to select the destination folder (Figure 2-12).

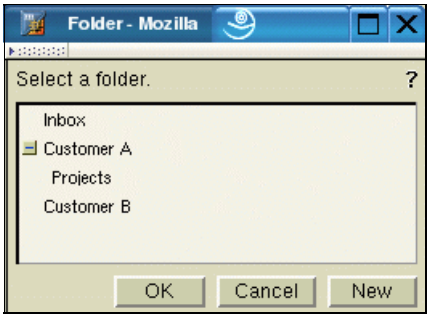


Figure 2-12 Selecting the destination folder for Send & File operation

Create page breaks in new messages

While creating new messages, a user can now insert a page break directly into the rich-text body of the mail message. This ultimately provides the user with much greater control over the pagination and appearance of the message.

Adding public contacts to the personal contact list

In the Select Addresses dialog, a user now can add anyone from the public Domino Directory to the personal contact list by simply clicking the **Copy** button.

View only unread mail

In the View menu (Figure 2-13), the new function Show Unread Only displays only the unread mail in the user's view or folder.

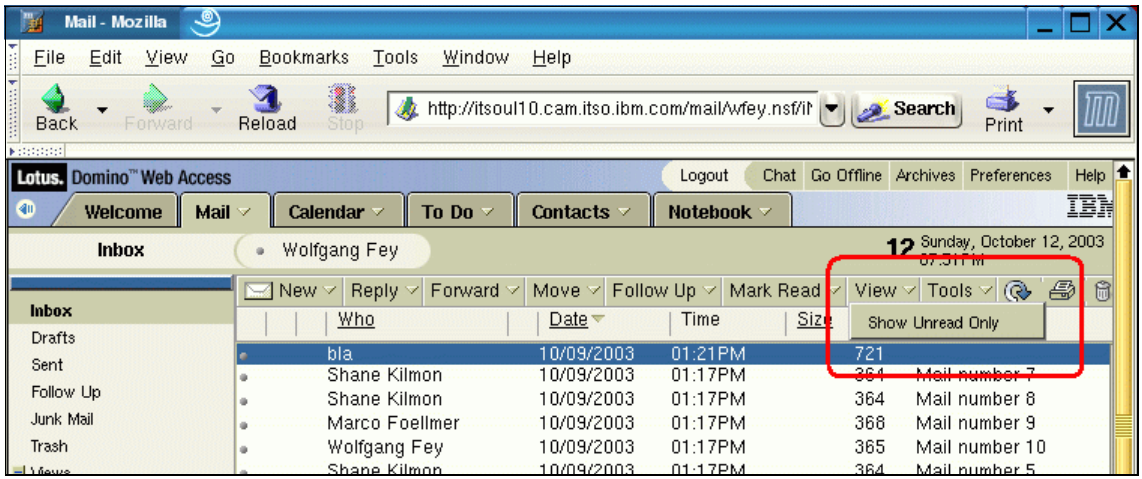


Figure 2-13 View unread only

Multiple browser window support

Every functional area of Domino Web Access can now be opened in a separate browser window. This includes the Welcome Page, Mail, Calendar, To Do list, and a user's Personal Address book and Notebook.

Send, sign, and verify encrypted mail messages

Domino Web Access builds on its state-of-the-art, security-rich features with the addition of new delivery options for sending secure mail. Users can now send encrypted and signed messages, as well as verify digital signatures, using the same security delivered in Notes.

Note: Before being able to use this feature, a user's Notes ID file must be attached to the profile document of his mailfile. The Administrator also can do this for a user.

See 6.4.1, "Encrypted mail support" on page 219 for a detailed explanation of how to set up a browser for encrypted mail support.

Figure 2-14 and Figure 2-15 illustrate an example of sending and receiving signed and encrypted messages.

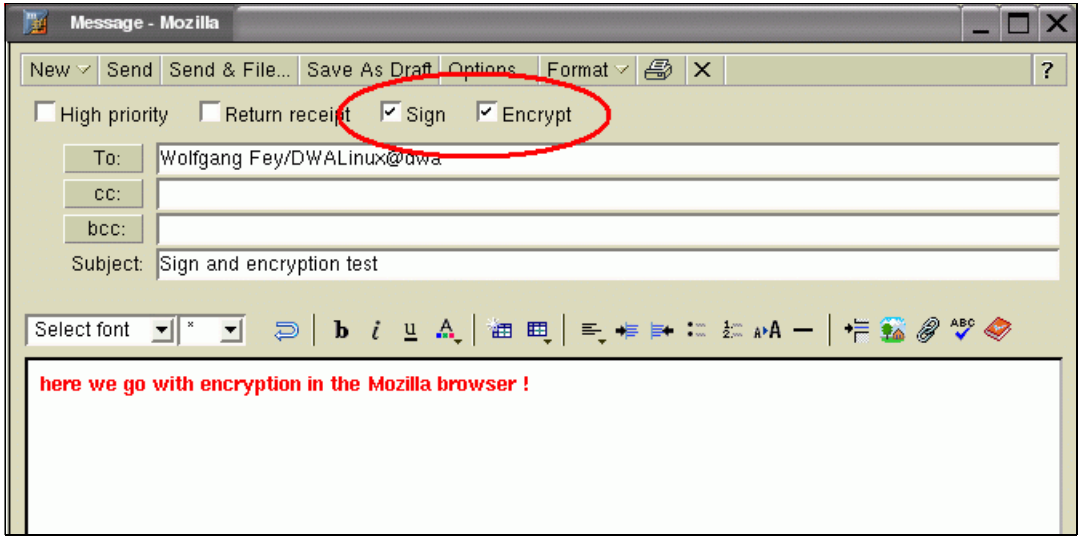


Figure 2-14 New mail with check boxes for signature and encryption selected

Receiving this mail results in a fully readable, decrypted mail. It is marked with two special signs showing the encryption and the approved signature.

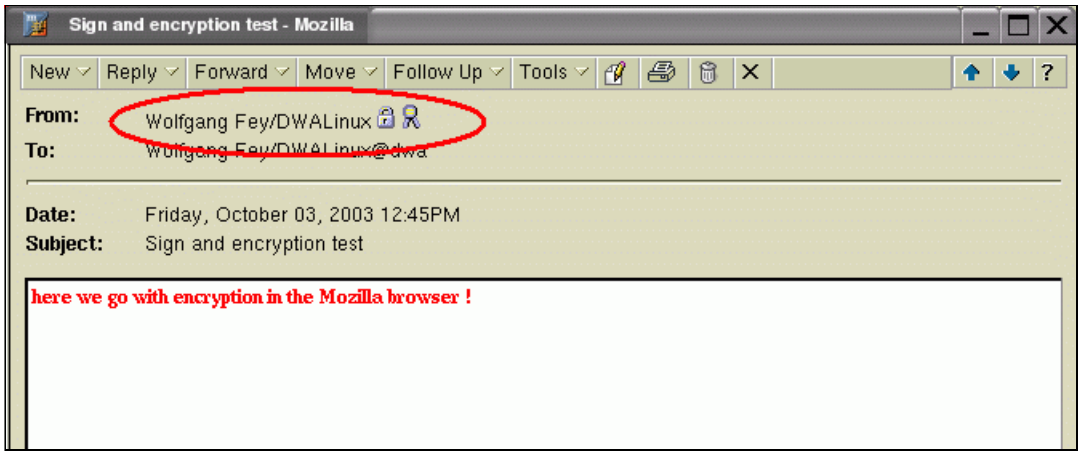


Figure 2-15 Receiving signed and encrypted mail

Note: Encryption and signing mail in Domino Web Access only interoperates with another Domino Web Access or with the Notes client. It does not interoperate with S/MIME encryption.

Unread marks

Since the introduction of Domino Web Access 6.5, the new and unread mails in the mailbox can be shown in two different styles: either in red or in boldfaced black. The user can select the style using the preferences dialog.

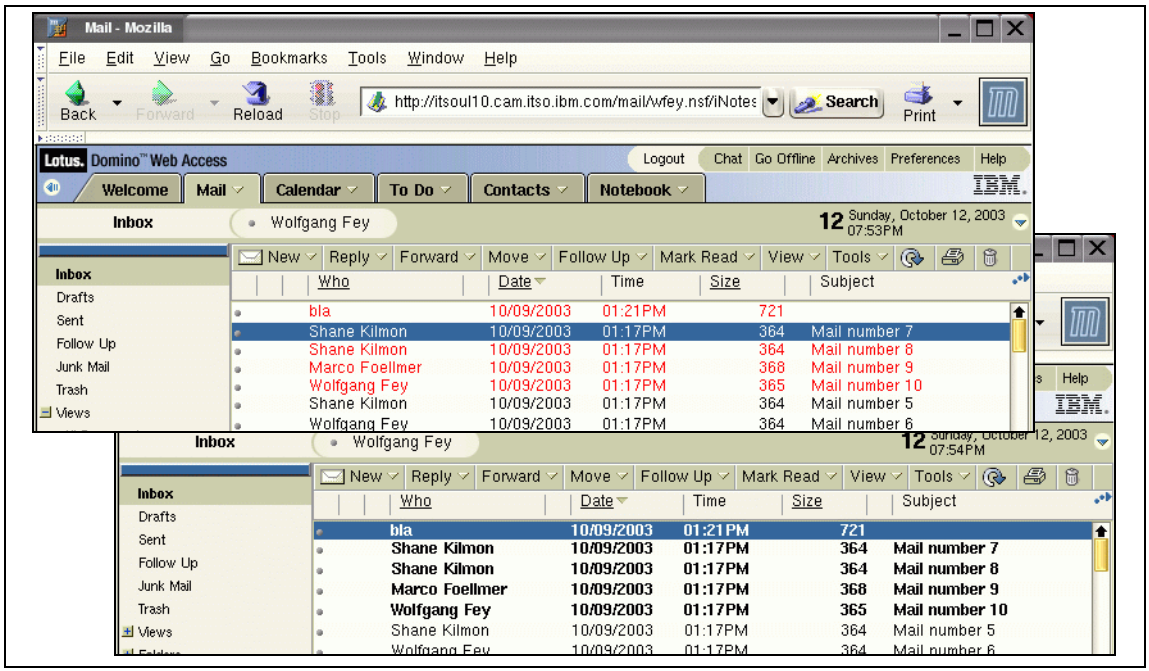


Figure 2-16 Different styles of unread documents

Reply with History using Internet-style formatting

The new Reply with History feature enables a user to select Internet-style formatting that begins each line of the original message with an angled bracket (>). After the message is converted to plain text, the brackets make it easier for the user to distinguish the new response text from the original text.

Note: The message loses all rich-text elements in this reply style. Any table, inline image attachment, and colored, bold, or italicized text formatting will be lost.

New phone message form

Domino Web Access 6.5 provides a new form as an easy way to record phone messages. This form has been available in the Notes client for several releases, so this represents one more improvement to the interoperability aspect between Domino Web Access and the Notes client.

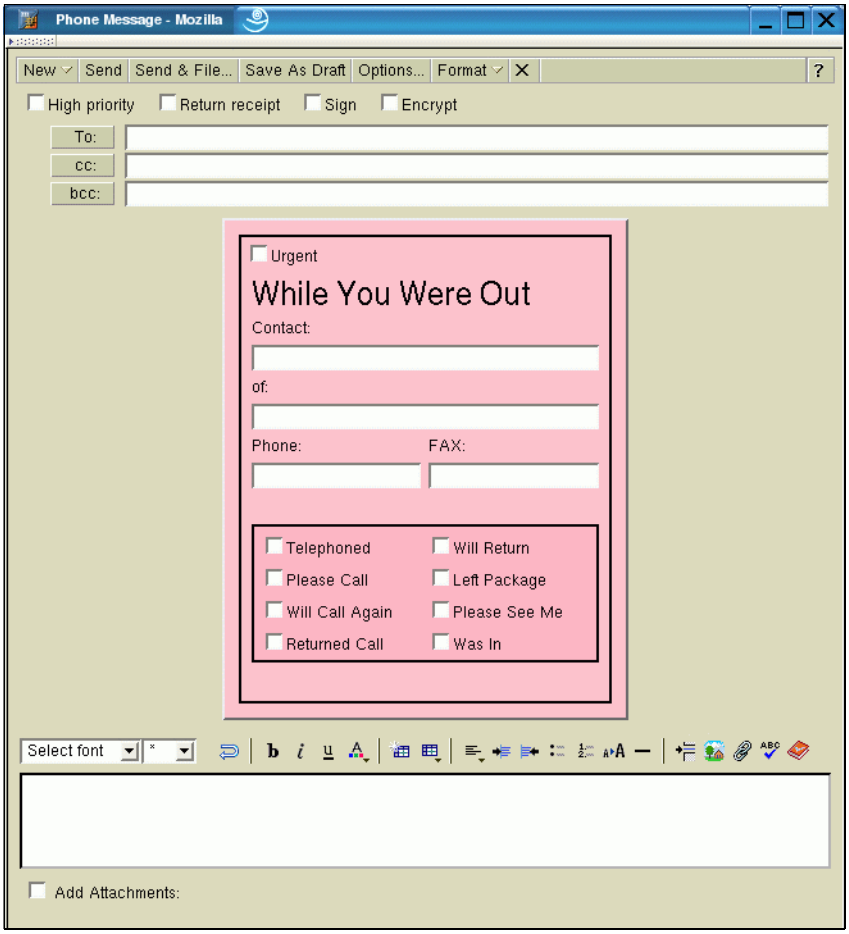


Figure 2-17 New phone message form

2.2.4 Calendar and To Do enhancements

The following section discusses enhancements made within the functional areas of calendering, scheduling, and To Do entries.

Editing in view

This feature, which was introduced in the Lotus Notes client in Version 6.0, is now available for Domino Web Access 6.5. It is used to create and edit calendar entries directly in the view *without opening any document in the browser*.

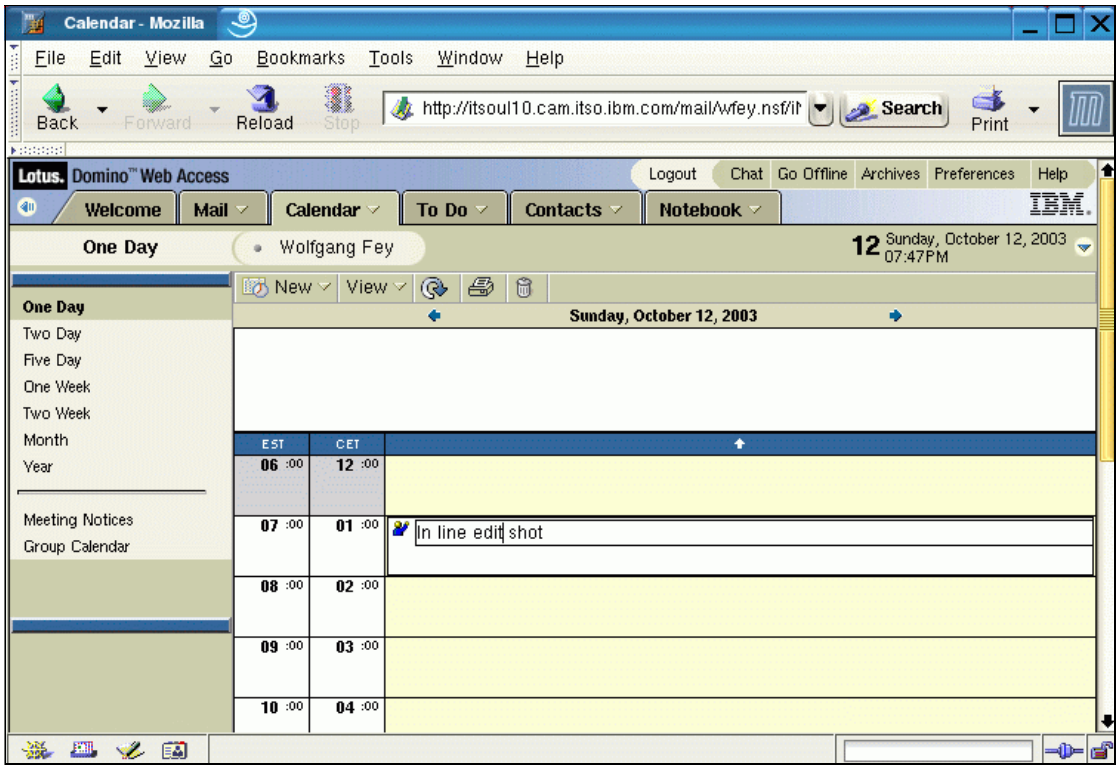


Figure 2-18 Inline edit example

Multiple time zone support

Domino Web Access now provides support for multiple time zones in calendar entries and in the calendar view, enabling users to understand calendar commitments across different time zones. Set up this feature in the Preferences dialog by entering the proper information into the Time Zone Settings fields.

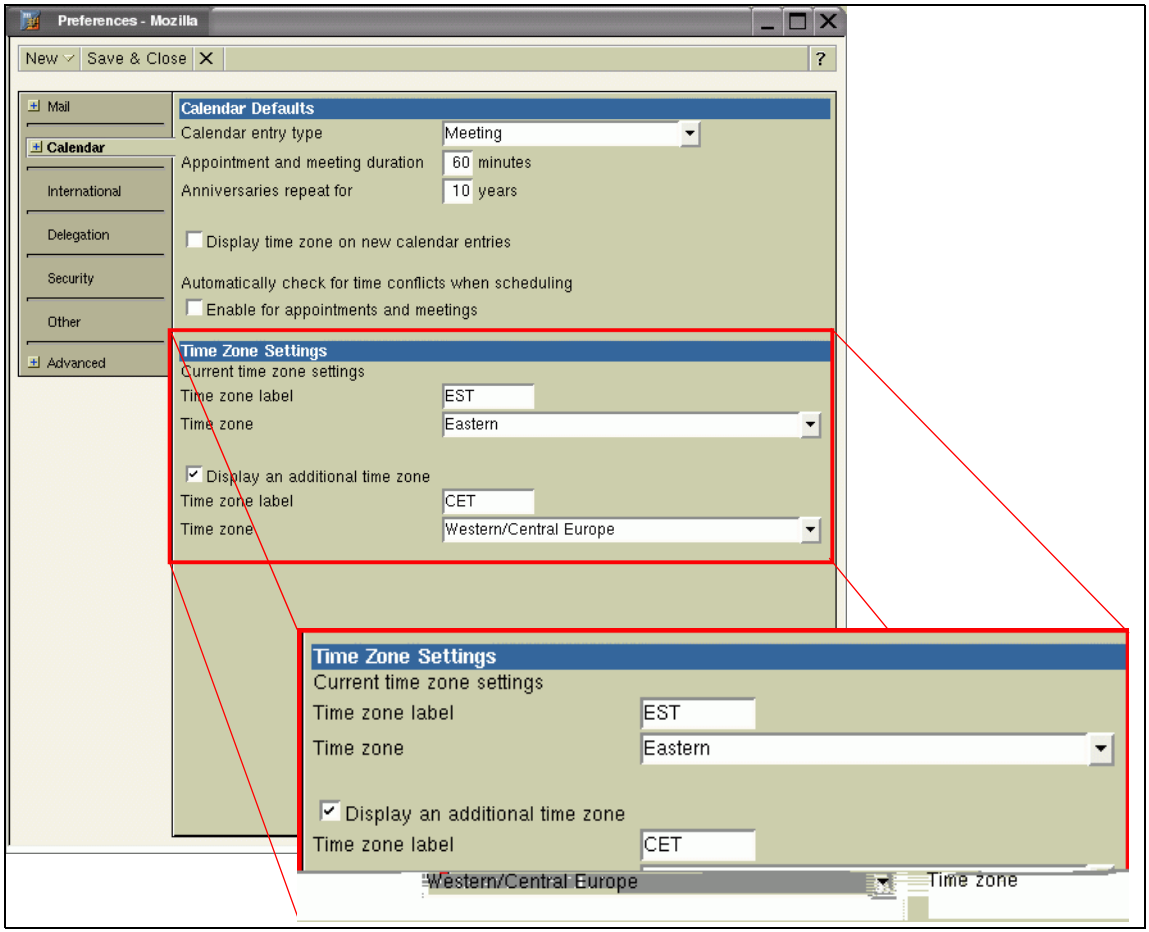


Figure 2-19 Preferences dialog with time zone settings

After setting this up, the different time zones appear in the Calendar view, as shown in Figure 2-20 on page 32.

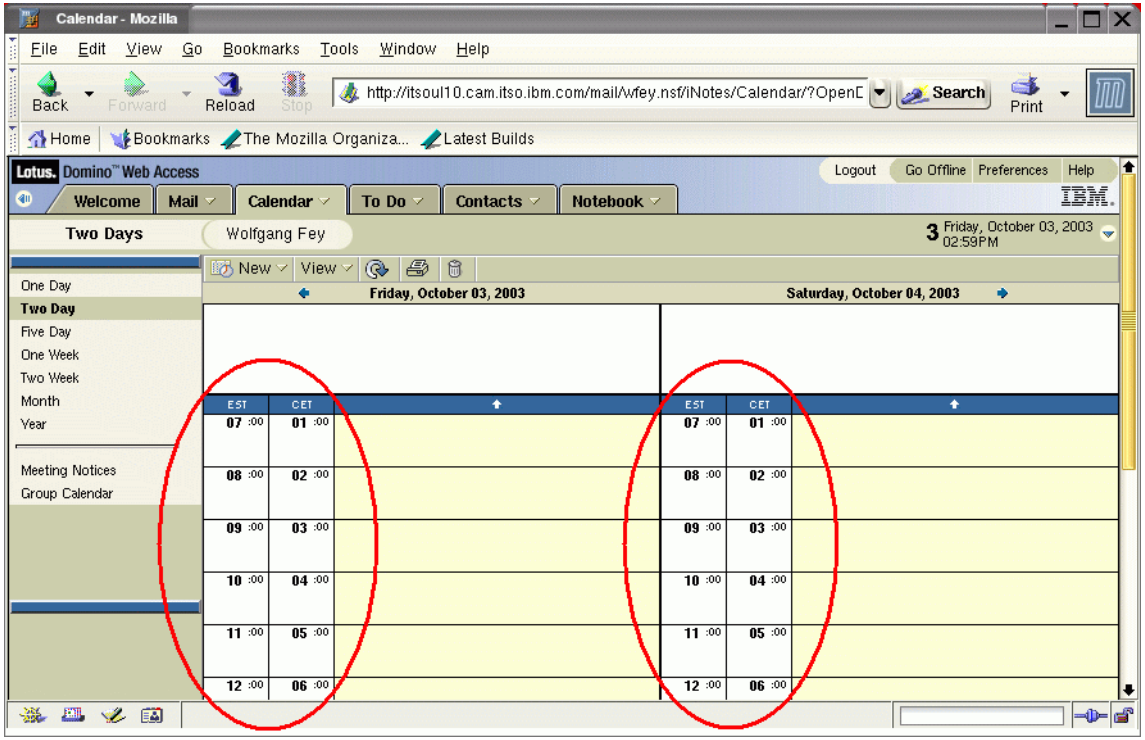


Figure 2-20 Calendar view displaying two different time zones

More options for calendar display in the Welcome page

A user can now display the schedule in single-day or multiple-day formats (up to 10 days) on the Domino Web Access Welcome page.

Pencil in meetings

Any meeting invitation, appointment, anniversary, event, reminder, and To Do can now be marked with the *Pencil In* option. Anyone with access to a calendar can view the details of a penciled-in entry. Penciled in entries appear as free when a free-time search is performed.

Unaccepted calendar invitations appear on Calendar view

Any received calendar invitation now appears not only in the user's Inbox view, but also in the Calendar view.

Delegation of the calendar

A user now can let other users schedule and respond to meeting invitations by delegating the calendar to them (Figure 2-21 on page 33).

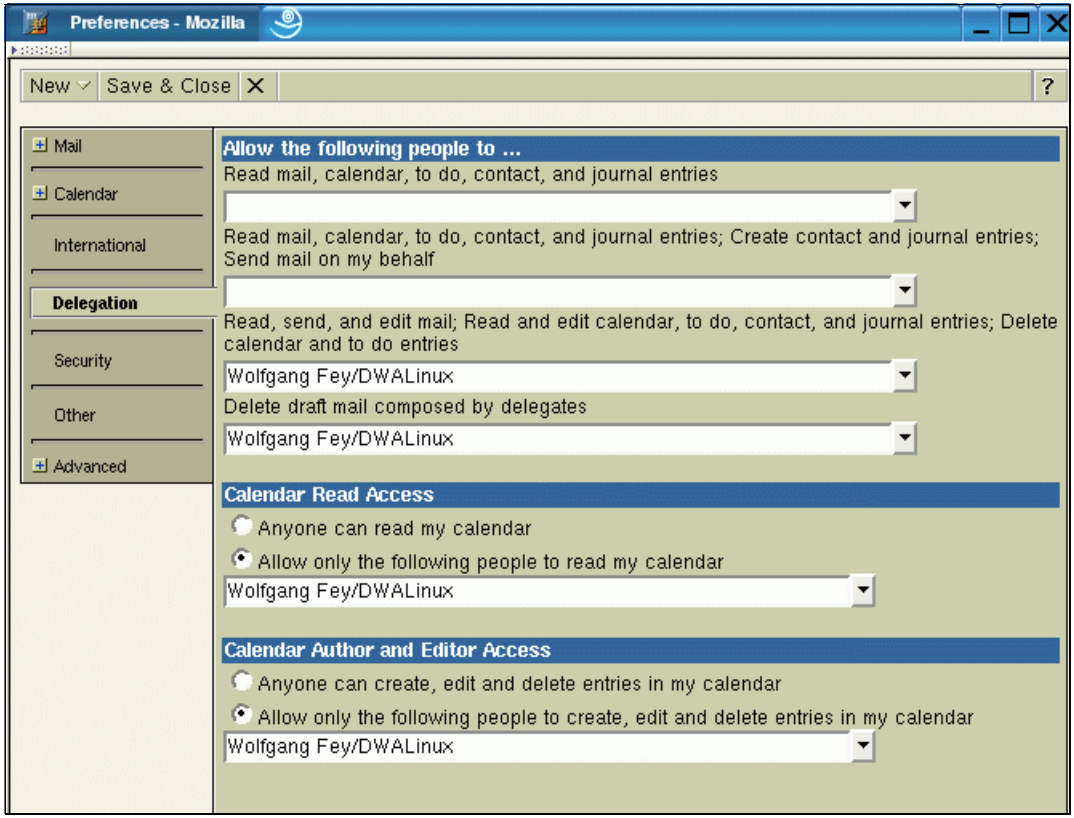


Figure 2-21 Delegation options in preferences dialog

To Do enhancements

Users can create To Do items that can be assigned to another individual or group. Figure 2-22 on page 34 shows the dialog window for creating a Group To Do list.

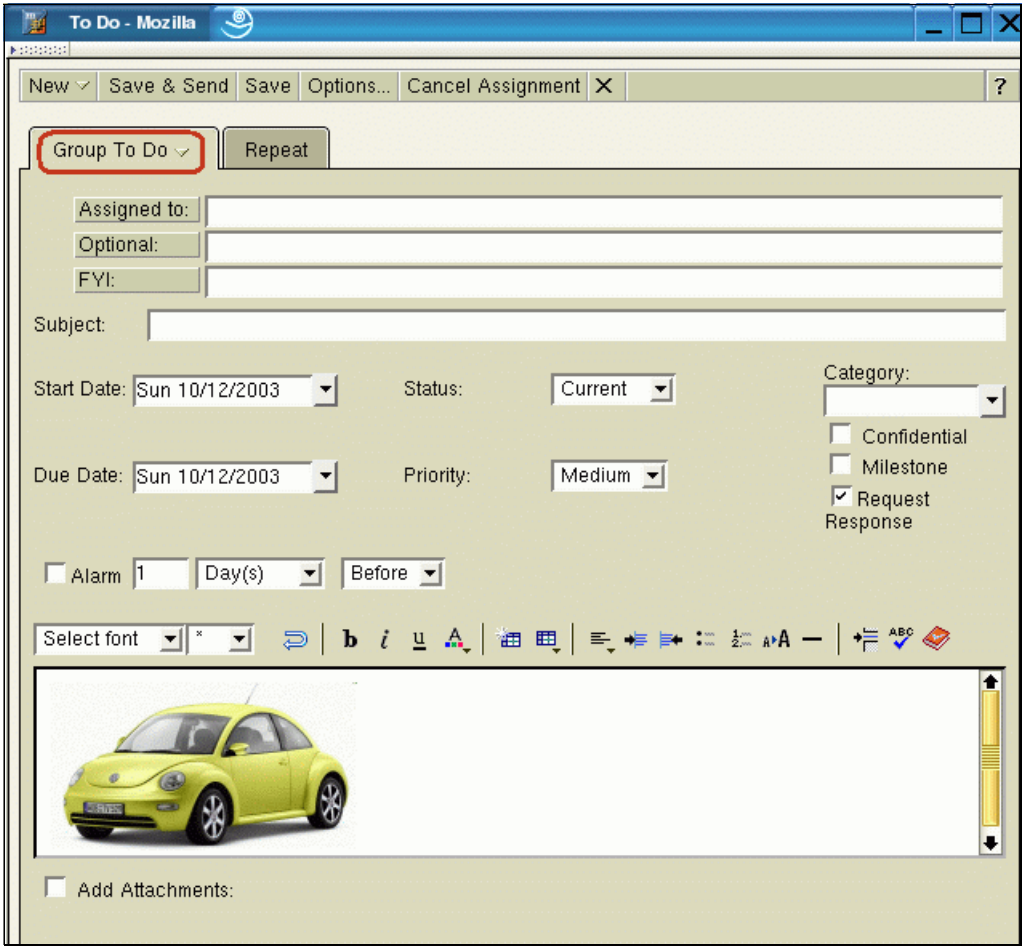


Figure 2-22 Group To Do dialog

Follow-up flags

Important entries in a mail file can be marked with a follow-up flag. The follow-up flag signals that further action should be taken on an item. Ultimately, this further helps to maximize responsiveness to incoming requests. There are three levels of importance that can be assigned, and nates can be made in a descriptive field. Additionally, there are input fields for setting up the follow-up date and time and an alarm notification.

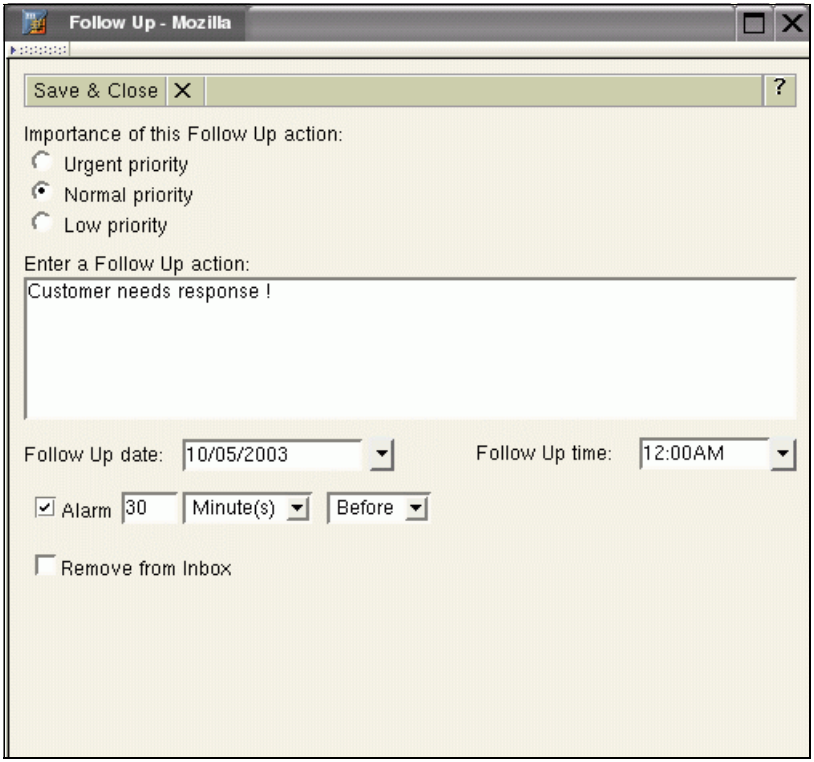


Figure 2-23 Follow Up dialog box

After setting the follow-up flag, the message is marked with a green, yellow, or red flag (for normal, low, or high importance of each follow-up action). All documents marked with a follow-up flag are shown in a new folder called Follow Up. If a flagged message is opened again, the follow-up information is shown (Figure 2-24).

Figure 2-24 Follow-up information in an opened document

If the follow-up alarm feature is set up for a document, it displays a pop-up window, shown in Figure 2-25 on page 36, when the follow-up alarm time is reached.

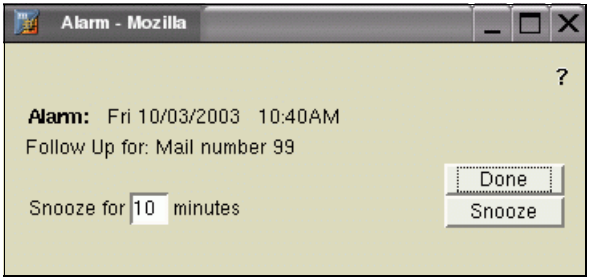


Figure 2-25 Follow-up alarm notification

2.2.5 Print enhancements

With Domino Web Access 6.5, you can now:

- Select multiple documents from a view for printing.
- Select a view and print its contents.
- Select entries in your Contact view and print them in summarized or detailed format.
- Print a document while in edit mode.
- Print multiple documents from a view.

Domino Web Access users can now select and print multiple documents in a view. Users are presented with three options to help them easily print in their preferred format. These options are shown in Figure 2-26.

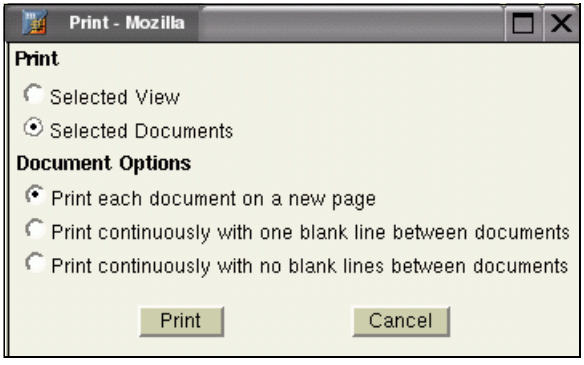


Figure 2-26 New Print dialog box

Enhanced calendar printing

When a user prints calendar entries, Domino Web Access adds both a date stamp and a time stamp.

2.2.6 Usability enhancements

Several usability enhancements have been made within this release. We describe the most significant ones in this section.

Customize the terms in a dictionary

In Domino Web Access 6.5, you can customize your personal dictionary by adding or removing your own terms in the window shown in Figure 2-27.

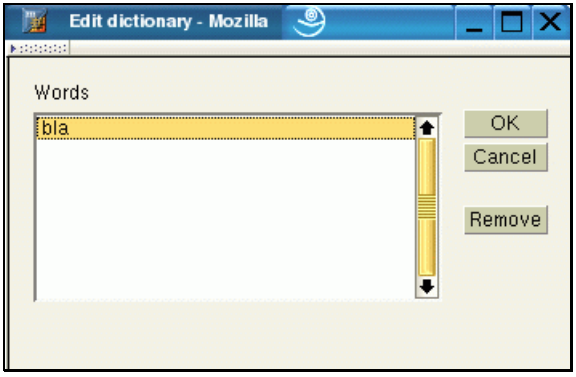


Figure 2-27 Edit personal dictionary

Viewing the database size and properties

Domino Web Access 6.5 provides the ability to view your total database size to see if you are nearing your database quota.

Figure 2-28 on page 38 shows the window that displays the database properties. The About window can be viewed by clicking the Domino Web Access logo in the upper-left corner of the window. Some significant and interesting information about the currently open mail database can be seen from within the About window, including each of the following attributes:

- Database title
- Database file name
- Fully qualified server name
- Server build
- Database template
- Active language
- Number of documents in database

- Database size
- Quota size
- Quota warning threshold

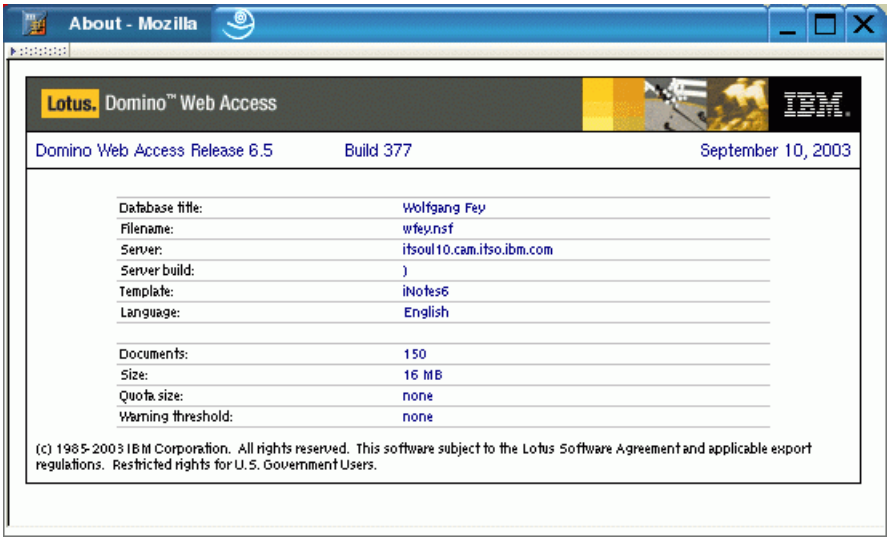


Figure 2-28 Database properties window

2.2.7 New administrative features

To ease the Domino Web Access server administrator's job, this release includes the following new administrative features and enhancements:

- Support for name change requests

  The Domino Administration Process (AdminP) handles the client interaction necessary to do name change requests.

- Domino Offline Services (DOLS) replication setting enhancement

  DOLS supports replication of truncated documents to determine the size of attachments replicated to the client. The administrator can also filter replication to not allow replication of attachments. Figure 2-29 on page 39 shows the Preferences page where these settings can be entered.

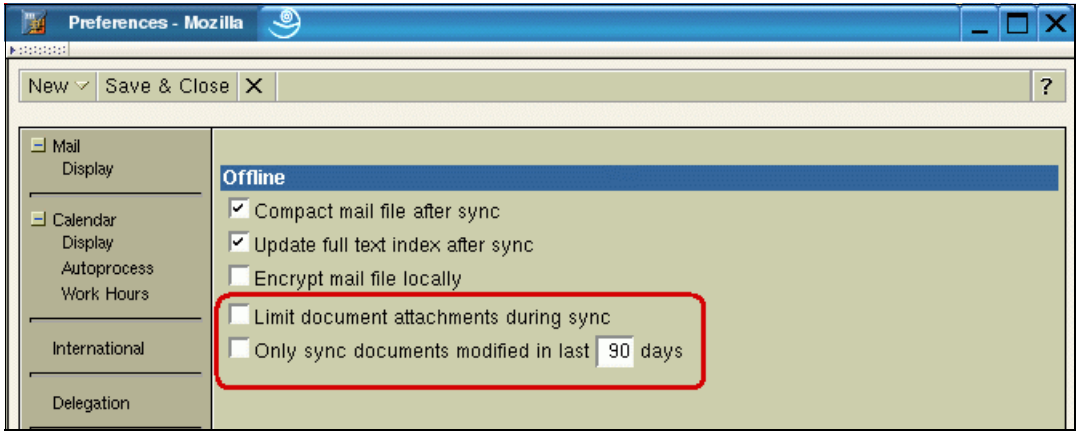


Figure 2-29 Limiting DOLS attachments in the Preferences dialog

2.2.8 Template customization

The Domino Web Access template gives Notes and Domino application developers additional customization options to better suit the needs of their users. With the Forms6.ntf file, they can create action buttons for the Domino Web Access views or dialog boxes, provide more options for the Domino Web Access Welcome Page, and substitute the Domino Web Access logo with a corporate logo. Domino developers can customize the design of select forms of the Domino Web Access template using Lotus Domino Designer. Modifications can include:

- Adding action buttons to views or dialog boxes
- Providing additional choices for the Welcome Page
- Replacing the Domino Web Access logo with a corporate logo

Modification samples and how to maintain them are shown and explained in much greater detail in Chapter 11, “Customizing Domino Web Access” on page 349.

2.2.9 Server-side enhancements

The following section discusses some of the server-side enhancements to improve the scalability and performance of Domino Web Access.

Attention: Chapter 7, “Configuration and tuning” on page 245 includes more detailed information about specific server parameters and notes.ini settings. This section is intended to provide an overview of the key performance enhancements built into the Domino Web Access template 6.5 server.

Server-side caching of generated and compressed content

Domino Web Access now caches certain static data, such as forms. As a result, the mail client only has to bring down the data once instead of requesting the data from the server each time. This results in improved scalability and performance.

GZIP compression

By default, Domino Web Access uses compression (GZIP format) to reduce network bandwidth consumption and provide better performance. This particularly benefits users with slow network connections. You can use NOTES.INI settings to turn GZIP compression on and off and to specify the types of content to compress. For a detailed explanation of setting NOTES.INI settings for compression, see 7.2.2, “GZIP network compression” on page 251.

After compression, pages generated in Domino Web Access are cached in the Web server’s page cache. This improves server performance and can help improve client-side performance, especially in regions where bandwidth is at a premium.

The last two mentioned improvements are not immediately visible to the end user. Although not directly visible, the results of both features improve performance and reduce network traffic.

2.3 Detailed feature comparison

Table 2-1 shows a detailed comparison of the features and functions in the portfolio of Lotus messaging clients. It highlights IBM Lotus Domino Webmail 6.5, IBM Lotus Workplace Messaging 1.0, IBM Lotus Domino Web Access 6.5, and the IBM Lotus Notes Client 6.5 regarding the messaging, calendaring, and scheduling functionality.

Table 2-1 Feature comparison in the Lotus Messaging portfolio

Feature	**IBM Lotus Domino WebMail 6.5**	**IBM Lotus Workplace Messaging 1.0**	**IBM Lotus Domino Web Access 6.5**	**IBM Lotus Notes Client 6.5**
File type used	NSF (server)	DB2 (server)	NSF (server)	NSF
Views and Folders				
Inbox View	X	X	X	X

Feature	IBM Lotus Domino WebMail 6.5	IBM Lotus Workplace Messaging 1.0	IBM Lotus Domino Web Access 6.5	IBM Lotus Notes Client 6.5
Drafts View	X	X	X	X
All documents view	X	X	X	X
Discussion thread view	X			X
Folders	X	X	X	X
Nested Folders	X		X	X
Create and delete folders	X	X	X	X
Drag-and-drop messages into folders			X	X
Copy and move to folder	X		X	X
Soft deletes	X	X	X	X
Junk mail folder		X	X	X
From action bar, open mail into specific view (Inbox, sent, drafts, and so on)		X	X	
Message creation and addressing				
Create new memo	X	X	X	X
Type-ahead addressing			X	X
Support file attachments	Limit of 2	X	X	X
View file attachments from within message		X	X	X
Spell checking		X	X	X
Alternate name support			X	X
Instant messaging integration		X	X	X
Perform name & address book lookup	X	X	X	X

Feature	IBM Lotus Domino WebMail 6.5	IBM Lotus Workplace Messaging 1.0	IBM Lotus Domino Web Access 6.5	IBM Lotus Notes Client 6.5
Display contacts sorted by organizational unit	X	X	X	X
Perform integrated address book lookup when sending a message			X	X
Name lookups to LDAP directories		X	X	X
Personal contacts address book	X	X	X	X
Delivery options (importance, delivery priority, delivery report)	X	X	X	X
Forward message	X	X	X	X
Save message as draft	X	X	X	X
Create serial route memo				X
Forward Web pages and documents from any IBM Lotus Notes application				X
Forward document as bookmark link message				X
“Copy into” convert item to task, calendar entry or new memo	X		X	X
Return receipt	X	X	X	X
Event copying			X	X
Apply mood stamps to messages				X
Create / use stationery				X
Choose letterhead				X
Create message containing a signature file	X	X	X	X
Type-ahead within “move to folder” dialog box				X
Specify message expiration date				X

Feature	IBM Lotus Domino WebMail 6.5	IBM Lotus Workplace Messaging 1.0	IBM Lotus Domino Web Access 6.5	IBM Lotus Notes Client 6.5
Specify outbound message with a “reply by” date				X
Specify Internet message format	X		X	X
Viewing and responding to message items				
Support for unread marks		X	X	X
Navigate to next document without returning to view	X		X	X
Perform mail file delegation	X		X	X
Reply with history	X[1]	X	X	X
Reply to memo	X	X	X	X
Reply to all	X	X	X	X
Reply without attachments			X	X
Automatically create reply message by clicking on from name			X	X
View rich text within a message	X	X	X	X
Support for doclinks, viewlinks, and database links	X		X	X
View tables within messages	X	X	X	X
Create tables within messages		X	X	X
Resend documents from within a delivery failure	X	X	X	X
View sections	X		X	X
Action bar	X	X	X	X
Add sender of message to personal contact list	X	X	X	X

Feature	IBM Lotus Domino WebMail 6.5	IBM Lotus Workplace Messaging 1.0	IBM Lotus Domino Web Access 6.5	IBM Lotus Notes Client 6.5
Modify / view the file's ACL from client				X
Display of importance / type icons in views	X	X	X	X
Read encrypted mail			X	X
Verify signature of signed mail			X	X
Next / previous navigation from within an open mail message			X	X
Preference setting for new mail on top or bottom of Inbox			X	X
Automatically check for new messages		X	X	X
Advanced editing features in rich text fields				
Left, right, center, indent, outdent text justification	X	X	X	X
Tables		X	X	X
Sections			X	X
Support for embedded OLE objects				X
Java applet support	X			X
Page break				X
Horizontal line		X	X	X
Hotspots				X
Insert image resources		X	X	X
Ability to switch language dictionary for spell checking		X	X	
Bulleted and numbered lists	X	X	X	X

Feature	IBM Lotus Domino WebMail 6.5	IBM Lotus Workplace Messaging 1.0	IBM Lotus Domino Web Access 6.5	IBM Lotus Notes Client 6.5
Undo			X	X
User preferences				
New mail notification		X	X	X
Default mail send / save setting		X	X	X
Archive messages and calendar items			X	X
Lookup across multiple address books	X	X	X	X
Security				
Send signed and / or encrypted mail			X	X
Read encrypted mail			X	X
Field, form, view, document, section level security				X
User roles			X	X
Local encryption of mail database			X	X
Other features				
Control of database properties / design				X
Alternate memo editor support				X
Built-in news reader, POP3, IMAP mail				X
IBM Lotus Domino subscription support				X
Extended search		X		X

Feature	IBM Lotus Domino WebMail 6.5	IBM Lotus Workplace Messaging 1.0	IBM Lotus Domino Web Access 6.5	IBM Lotus Notes Client 6.5
User can change own password		X	X	X
Mail rules			X	X

1Reply with history in IBM Domino Webmail sends only the text content, not the rich text items, such as in-line images or tables.

2.4 Understanding user profiles

To develop products that more specifically meet the messaging requirements of every kind of user, IBM surveyed many organizations of varying sizes. A segmentation of the user communities reveals three common workforce roles: deskless, office, and knowledge workers. Each role differs based on messaging and collaboration requirements and frequency of use. Figure 2-30 on page 47 illustrates each of these different tiers, relative to a scale of frequency of messaging use and the level of functionality (and price) required of a messaging client.

2.4.1 Tier 1: deskless workforce (line employees, shop floor)

The term *deskless worker* describes users who require only occasional access to e-mail and perhaps a calendar. These users typically do not have e-mail, and they rely instead on paper memos, physical bulletin boards, and face-to-face meetings to receive or communicate job-related information. For example, expansive retail home-improvement stores have employees who spend most of their workdays walking the floor and assisting customers. They probably do not have desks, and they need occasional access to a computer to check e-mail for communications from department managers or from the corporate Human Resources office. They have a very low volume of e-mail and personal contacts, and they use the mail system mainly for information distribution. Besides retail, other industries including industrial (manufacturing, distribution, transportation), government, health care, and education, typically have large numbers of deskless workers.

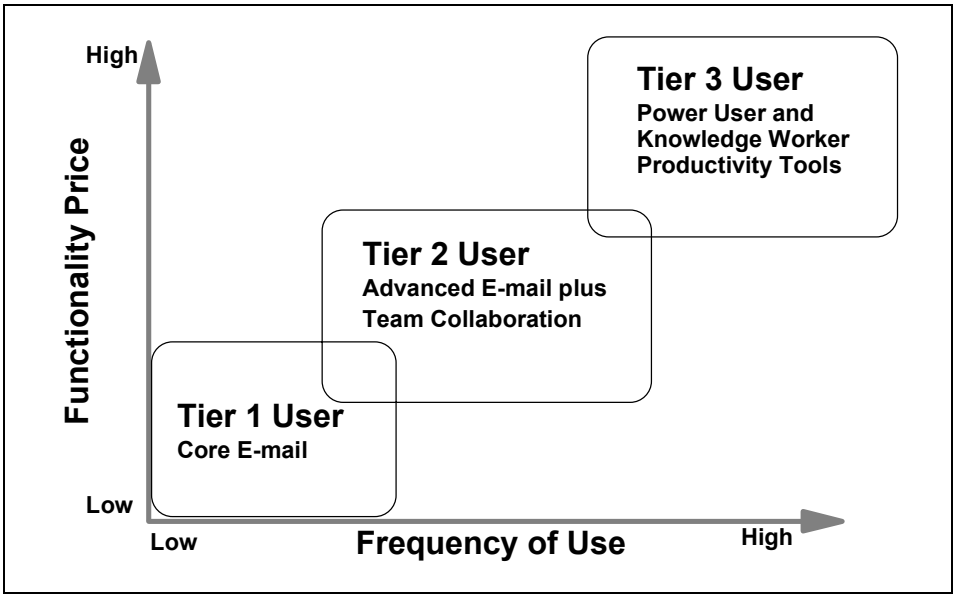


Figure 2-30 Employees require different messaging solution functions based on their roles

2.4.2 Tier 2: office workforce (advanced users, team leader, staff)

Typical office workers are employees who require richer messaging and collaboration capabilities than deskless workers in order to accomplish a different set of job-related tasks. Office workers commonly use e-mail, a calendar, and even workflow functions to manage higher volumes of messages on a daily basis. They often have a medium volume of e-mail, To Do tasks, contacts, and calendaring and scheduling, and they require some collaborative application functionality. Finally, they might have a task-oriented portal.

2.4.3 Tier 3: knowledge workforce (power users, senior managers)

The knowledge worker typically includes executives and senior managers. These users require the highest levels of functionality to manage hundreds of e-mail messages a day. These messages are often compounded by high volumes of other communications from voice mail, instant messages, and various devices including personal digital assistants (PDAs), mobile phones, and pagers. Their messages frequently include rich graphics and object components. The knowledge worker makes extensive use of e-mail, To Do, contacts, calendaring and scheduling, and collaborative applications. Typically, mobility is essential to these people.

2.4.4 Messaging solutions targeted to every kind of user

The portfolio of Lotus messaging products is designed to solve the specific messaging challenges of businesses, from small and mid-size businesses to large enterprises. The goal is to help different types of users work more efficiently. Lotus messaging solutions can help deliver the appropriate level of functionality to each of the three worker roles in businesses of nearly any size.

The demonstrated leadership of Lotus software in the messaging market is strengthened by the scalability, low cost of ownership, and flexibility of e-mail services delivered by Lotus Domino and Lotus Workplace Messaging. This value is then delivered through various client experiences. The following sections describe how each Lotus messaging product meets the explicit productivity needs of each type of end user.

2.4.5 IBM Lotus messaging solution choice based on needs

Figure 2-31 on page 49 shows a decision support tool for companies or users to find the right solution for their particular company needs. From IBM Domino WebMail, up to the feature-rich IBM Lotus Notes client, there are many differences. Some of the most important features are shown.

The factors that influence the selection of the appropriate client is based on your specific situation, rather than specific features within a client.

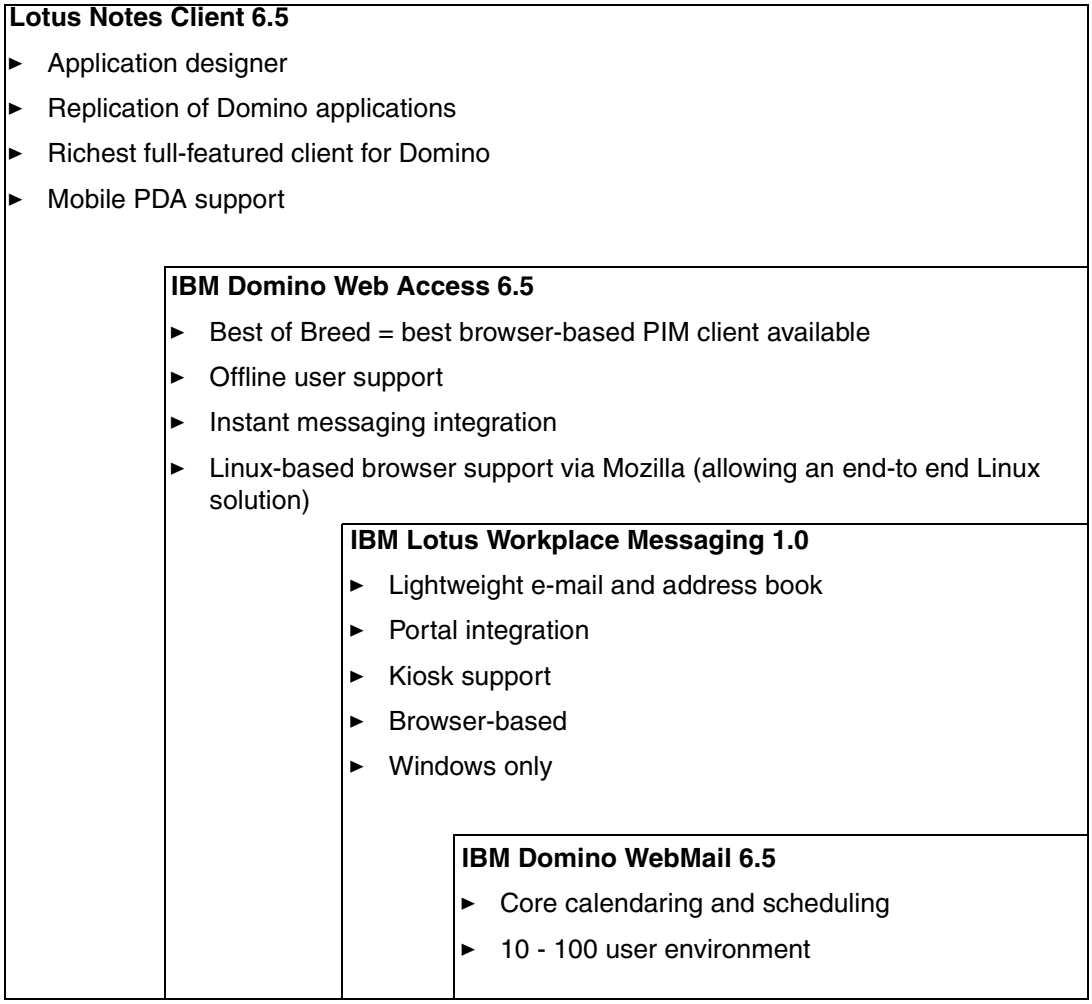


Figure 2-31 Decision tree for the different user and company needs in messaging solutions

Table 2-2 on page 50 shows a direct comparison of the IBM Lotus messaging products regarding the needs of the specific customer environment. Although the feature list is not as complete as the detailed feature comparison shown in Table 2-1 on page 40, the compelling decision drivers are listed. The value from this table is to understand the needs from the current infrastructure environment and to fit in the user requirements.

Table 2-2 Needs based feature comparison

Key need	Lotus Notes and Lotus Domino 6.5	Lotus Domino Web Access 6.5	Lotus Domino Access for Microsoft Outlook 6.5	Lotus Workplace Messaging 1.0	Lotus Domino WebMail 6.5
What is user population?					
Limited to between 10 and 100					X
100 and up	X	X	X	X	
What are the functional needs?					
E-mail and PIM only				X	
E-mail, PIM, and calendar	X	X	X	X[1]	X
E-mail, calendar, and workflow	X	X			
E-mail, calendar, workflow, and application development	X				
What are the client needs?					
Web client (browser) access		X		X	X
Third-party standards-based (POP3, IMAP) access	X[2]			X[3]	
Access to Microsoft Outlook client			X	X[3]	
Detached mobile client support (offline)	X	X		X[3]	
Desktop client	X				
What is the feature profile?					

Key need	Lotus Notes and Lotus Domino 6.5	Lotus Domino Web Access 6.5	Lotus Domino Access for Microsoft Outlook 6.5	Lotus Workplace Messaging 1.0	Lotus Domino WebMail 6.5
Extensive features	X				
Mid-level features		X	X		
Basic features				X	X
What are the infrastructure needs?					
Existing or new Domino platform	X	X	X		X
Existing or new WebSphere or DB2 platform				X	
Java 2 Enterprise Edition (J2EE) architecture (Java-centric)				X	
Uses existing or new LDAP directory				X	
Portal deployment	X	X		X	
Kiosk deployment		X		X	

[1]Calendar available in a future release
[2]Back-end infrastructure supporting POP3 and IMAP access
[3]Access through POP3 protocol (IMAP supported in an upcoming release)
Source: Lotus_Messaging_Solutions_flyer_v17.pdf (G325-2301)

Note: Version 1.1 of IBM Lotus Workplace Messaging should be announced soon. Prior to starting the selection of the right solution, the features of this product should also be included in this table to ensure a complete and comprehensive comparison.

2.5 Strategic impact of the product decision

This remaining section has been adapted from a series of IBM Lotus Software whitepapers, including *Technical Strategy and the Domino Developers' Roadmap* and *Domino Applications and the Lotus Workplace Technical*

Strategy. We are including this here because we believe that it will be helpful in further understanding the importance and advantages in choosing Domino Web Access 6.5 as a strategic platform.

Finally, when choosing the most appropriate messaging solution from the Lotus portfolio, it is very important to consider the impact and implications of the underlying platform. This section covers the strategic impact on the platform decision between Lotus Domino and Lotus Workplace for the messaging and collaborative client environment.

2.5.1 Lotus Domino platform

The Lotus Domino application development and deployment environment enables you to develop collaborative applications quickly and to take them online. This enables you to bring people, processes, and data together quickly and effectively to facilitate both productivity in e-business and quick decision-making. Existing custom applications built with Lotus products also support the Lotus Workplace platform, allowing further leveraging of your application investments. Lotus will continue to enhance the Domino application development model and data store and eventually plans to enhance it by providing IBM DB2 database management as an alternative data store.

Lotus Domino is a comprehensive application platform for collaboration that handles both connected and disconnected requirements for applications and data. Most customers initially purchase Lotus Domino for the built-in enterprise e-mail, calendar, and scheduling applications, making those types the most widely deployed collaborative applications. However, the majority of customers exploit the capabilities beyond mail that support core business processes, which enable employees to work together efficiently and securely. Lotus Domino is comprehensive because it provides the complete infrastructure needed to create, test, deploy, and manage distributed, multilingual applications including directory, database, application server, administration, connectivity, security, Web server, e-mail server, calendaring engine, and so on, in one system.

Domino developers can design applications for the Lotus Notes client, Web browsers, mobile phones, and handheld devices, or most commonly, for a hybrid environment accessed by multiple types of clients. Hybrid-client Domino applications can leverage replication and offline services for secure, synchronized applications that work as well in a disconnected mode as when accessed on a server over a network. Replication enables users to save a local copy of a Domino application and its data on a file system and to periodically synchronize the data, so that users can be productive and efficient even when they are disconnected from the network.

Examples of Domino solutions include document-centric and workflow process routing, such as project team rooms, document repositories, discussion forums, sales-force enablement, and employee self-service applications. Businesses of all sizes have benefited from Domino applications.

As a comprehensive application platform, Lotus Domino includes a tool for rapid application development (RAD), a document-based object model and broad programming language support for building custom collaborative applications. With these choices, your organization can leverage many developer skills to develop a Domino application. Domino developers can quickly build a collaborative application by applying one of the many templates that ship with Domino.

If requirements dictate application functionality beyond the one provided by one of the included templates, that application can be modified or new applications can be developed using Lotus Domino Designer. A RAD tool, Domino Designer provides an intuitive integrated development environment for developing and managing Domino applications.

Domino applications can implement business logic through the use of formula or the BASCI-like LotusScript language on an event-driven or scheduled basis. For more advanced solutions, developers can use Java, Microsoft® COM, C/C++, or CORBA. The multiple interfaces to a single-object model that Lotus Domino provides enable developers to pick the best language for the task, reusing their skills in new applications and solutions.

Some solutions require non-Notes data and globalization support. Lotus Domino add-on tools facilitate such solutions. Using visual data-mapping techniques, a developer can easily and quickly integrate relational data with Domino data. No programming is required when using tools such as Lotus Enterprise Integrator® (LEI) to integrate data from a wide variety of systems such as IBM DB2, Oracle, and Microsoft SQL Server. Domino applications that require global deployment can be translated into a variety of languages by using straightforward forms. The same application can be delivered to multiple users in their native language.

The Domino road map for application development builds on the fundamental premise that Lotus Domino is a flexible and open platform, which is demonstrated by Extensible Markup Language (XML) and broad programming-language support. Flexibility and openness are key to a Domino application's ability to leverage J2EE and the Lotus Workplace platform. You can extend your Domino application investment in data and application logic in a number of ways. For example, you can expose Domino data using Web services (through LotusScript or Java) or JSP tags to integrate with Lotus Workplace or WebSphere applications. Another option is to surface your Domino application directly in WebSphere Portal.

Along with the progressive innovation that Lotus will add to Domino Designer and to the Domino programming model, there will be continued integration with WebSphere Studio and WebSphere Portal development tools. This integration will not replace Domino Designer, but will help facilitate teams of developers using Domino, WebSphere Application Server, and WebSphere Portal in their environments. Such teams will benefit by using the strengths of each system when building applications.

2.5.2 The WebSphere platform

The WebSphere software platform for e-business delivers one of the most powerful and flexible Web application servers on the market, partly because of the broadest implementation of the widest range of leading-edge open standards. The application server is complemented by a range of products that leverage this foundation to provide functions, such as personalization and mobile computing. The WebSphere software platform also includes an award-winning line of tools, including IBM WebSphere Studio, which provides a highly integrated development and deployment environment. The platform is organized into three areas of functionality:

- Foundation and tools for building, running, and deploying applications.

  WebSphere Application Server, WebSphere MQ messaging, and state-of-the-art development tools form a solid base for the platform. The foundation and tools provide the Internet expertise that you need, enable you to build and use Web services, and link you to a greater technical community of developers and other WebSphere users.

- Business integration for integrating internal business processes, including processes that involve business partners.

  WebSphere offerings such as WebSphere Business Integrator make it easy for your company to implement applications and business processes, including supply chain management and the integration of existing processes with the Web.

- Business portals for personalizing Web-based content and for making this content accessible to any device.

  These WebSphere products fine-tune your users' experiences and provide broad access for your customers, employees, business partners, and remote branch offices. WebSphere Portal leads the business-portals part of the WebSphere platform. It provides an extensible framework for interacting with enterprise applications, content, people, and processes. Self-service features enable end users to personalize and organize their own view of the portal, to manage their own profiles, and to publish and share documents with their colleagues. WebSphere Portal provides additional services such as a single sign-on, security, Web-content publishing, search and personalization,

collaboration services, enterprise application integration, support for mobile devices, and site analysis.

2.5.3 Domino and J2EE

One of the key differences between WebSphere Application Server and the Domino application server is that Lotus Domino provides a fully integrated environment: application execution, user authentication, directory services, data hosting, and presentation display all in one system.

The J2EE model differs in that it has elements for providing the application with all of the same information, but the J2EE server is not responsible for fulfilling all of the aspects that the Domino server fulfills. The J2EE server calls out to different parts of the customer environment to fulfill the requests of data, directory information, and so on. For example, whereas the J2EE specification outlines how the server can get data from a data store into the application using the JCA or Java Database Connectivity (JDBC), J2EE does not require that the server contain the database manager itself.

2.5.4 Leveraging your investment in Domino

One of the greatest benefits of developing applications for the Domino platform is that applications written for Lotus Notes Version 1 can be run unaltered on a Domino 6 server. That means that your company is still realizing value from an investment that it made 13 or more years ago, and those applications can now be accessed by Web browsers, Java APIs, and Web services. As Domino moves forward and becomes one of the server platforms for Lotus Workplace, it is important that IBM continues to protect customers' investments.

One conclusion that may have been reached by now was that the application requires the rich client experience provided by the Lotus Notes client. IBM plans to continue to support and enhance Domino as an application server for Lotus Workplace.

Part 2

Deployment and administration

3

Deployment considerations

This chapter discusses important deployment and planning considerations that apply to Domino Web Access 6.5 on Linux.

When architecting a solution that will include Domino Web Access, as with any other software products, there are many aspects of the deployment to keep in mind. We must think about the server configuration and client configurations, as well as all of the layers in between that have an impact on the application, and consider how each of these elements will be affected as the application grows over time and the requirements of the environment become increasingly complex.

It is beyond scope of this book to detail all complex deployment scenarios, but we try to help in laying out the foundation of some specific integration points with other IBM Lotus technologies in later chapters. This chapter attempts to answer some of the more abstract questions about how different deployment environments might affect or be affected by Domino Web Access 6.5.

Finally, note that this chapter is focused primarily on the server aspect of Domino Web Access 6.5. Client considerations, including the topics related to offline use, are discussed in significant detail within Chapter 8, “Linux Clients for DWA 6.5” on page 263.

3.1 Deployment goals

The following section discusses specific deployment goals and key considerations in terms of high availability, security, integration with LDAP, and particular demands on the network.

3.1.1 High availability

Native clustering

In practice, most deployments of Domino Web Access require some form of high availability (HA) as part of the deployment. Some of these scenarios and HA strategies may also affect performance, but within this section the primary focus is to examine the role of HA as it relates to continued uptime.

Domino Clustering and ICM

The core Domino technology used to increase availability is Domino Clustering, which provides almost real-time replication of data between cluster-mates.

Tip: For an in-depth look at clustering strategies, this article may be helpful: *Predicting Domino Cluster Performance* by Masud Khandker. It can be found in the Iris Archives of the Lotus Developer Domain at:

http://www-10.lotus.com/ldd/today.nsf/0/2e0d8fb64ff811e985256832006d5b8c?OpenDocument

As it relates to DWA, clustering enables users to have a ready and running backup of their mail file. In order to get a browser redirected to the failover cluster server if the primary mail server fails, it is necessary to configure the Internet Cluster Manager as well.

Internet Cluster Manager (ICM) is a Domino server task. It runs on one or more Domino servers that are members of the Domino cluster but do not necessarily serve data at all. The role of the ICM is to redirect client requests to the host that can best service them. This is done based on the clustered server's awareness of the Domino Server Availability Index (SAI), and which databases are housed on which server. Accordingly, this means that you can put up one or more ICMs that service more than one cluster each.

ICM works as a redirector technology by sending 302 status codes to clients to point them to the right server. (Fortunately, DWA is built around an awareness that 302 redirects happen.) The immediate concern then moves to what other technologies match with the DWA Online configuration. As of Domino version 5.0.5, Domino Off-Line Services (DOLS) supports Domino clusters, so that part is straightforward. For step-by-step instructions for setting up Domino Off-Line

Services to take advantage of clustering, see the tech note *Guidelines for Clustering with Domino Off-Line Services (DOLS)* at:

http://www-1.ibm.com/support/docview.wss?rs=474&uid=swg27002831

Additionally, refer to Appendix B, “Configuring Internet Cluster Manager” on page 435 for detailed steps in configuring ICM.

Figure 3-1 provides an overview of how ICM works using 302 status codes.

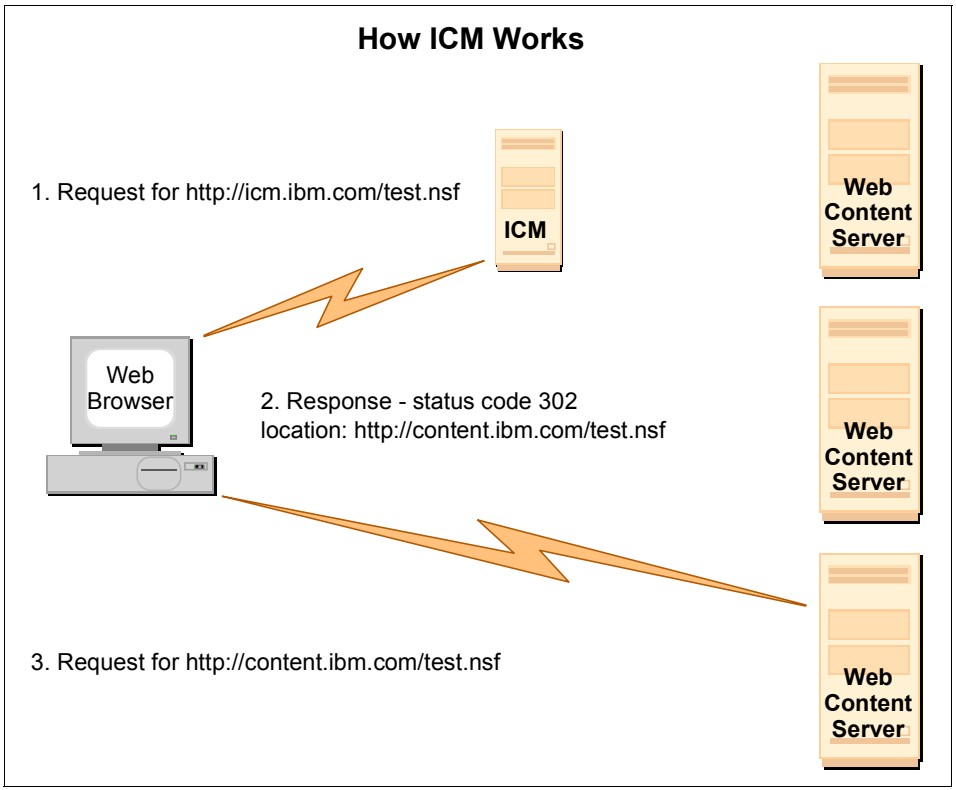


Figure 3-1 Overview of ICM functionality

High Availability and Sametime Integration

The other key element of DWA that requires additional configuration for high availability is Sametime integration. In order to cluster Sametime technology, we need to have a basic understanding of how both the base technology and the integration points work.

Sametime community services are built on a model that consolidates network traffic through a component called a MUX (short for multiplexer), which is by default installed on the Sametime server itself. In a high availability deployment,

the workload of the MUX can be both moved off to the Sametime server machine, and the load can be distributed across multiple machines each running a MUX for a given community. When supported by either round-robin DNS or a network sprayer, this can provide for failover if a MUX fails in production. However, if the Sametime server failed, then none of the MUXES would be able to operate. Fortunately, another layer of clustering is available for the Sametime community server components to take care of this situation.

The first requirement for a Sametime community cluster is to cluster the Domino servers that host Sametime. This is done to keep the community consistent. In this case, the Sametime community services are actually clustered by configuration in the STConfig.nsf with the creation of a cluster document. Specific instruction to do this are beyond the scope of this book, but is documented in greater detail in the Sametime 3.1 product documentation.

Domino Web Access is Sametime-enabled by STLinks, as discussed in Chapter 9, “Integrating Sametime with Domino Web Access 6.5” on page 325, which provides a very lightweight applet to enable chat services and give an interface to meeting services. However, with this integration come some considerations. The STLinks client does support clustering in Sametime 3.1, but the behavior is not identical to that of the familiar connect client. In the connect client when one server goes down, the algorithm for getting back online polls every 30 seconds for 10 minutes. In the STLinks environment, there is only one reconnect attempt, and then a refresh of the browser/frame is required. There is no need to quit and restart the browser.

Architecturally, High Availability for DWA is available with relatively few steps. It is important to recognize, however, these different layers of technology and how they relate to each other. This is critical both for a successful deployment and for troubleshooting any problems while in production.

Linux-specific HA open source clustering

Linux has native clustering capabilities in the form of Beowulf Clustering (http://www.beowulf.org), as well as other projects and subprojects that can be used to support various high-availability goals. At this writing, our team could not find reference to any Domino deployments on such a cluster. Additionally, Domino does not have any code to make use of cluster schedulers and heartbeat software that are available on Linux. While such an investigation is of interest, theoretical or practical implementation considerations around this were outside the scope of the team’s primary focus. A basic investigation did not reveal any other site that was using this clustering strategy, either in a testing capacity or in a production environment.

A recommended resource for learning more about options for Linux clustering can be found at OSCAR (Open Source Cluster Application Resources) at:

http://oscar.openclustergroup.org/tiki-index.php

3.1.2 Reverse proxy

Next to clustering, one of the most frequent configurations for increasing accessibility to Domino Web Access is use of a reverse proxy. A reverse proxy is software that can either be put on a server or packaged as a device that is used for limiting data storage server access to a machine or machines that are known. Another common use would be to divide content sources and use a proxy as a way to split a load, such that several sources can provide data instead of just one host. Figure 3-2 illustrates these two possible uses for a reverse proxy configuration within a Domino Web Access deployment.

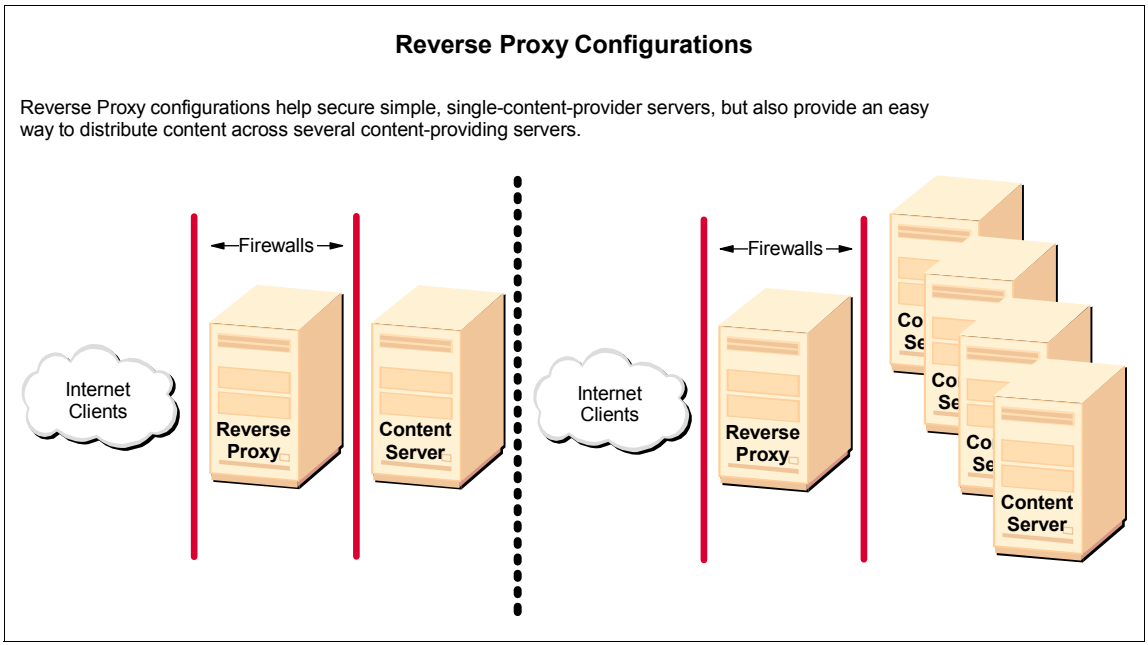


Figure 3-2 Two uses for reverse proxy configurations

Domino Web Access has been designed to work well with reverse proxy configurations from the ground up. DWA uses JavaScript code to determine whether the host name that is in the location is in fact the DWA server. It also enables any adjustments to be made to URLs within the application. The HTTP task is unaware that there is a proxy between the client and the server, which results in a need for the reverse proxy to touch up the location header with the

proper host name per RFC. This means that we expect the proxy server to rewrite the HTTP location header so that external clients do not try to resolve and connect directly to the content server.

Tip: Some tested proxy servers that are known to meet these requirements are

- IBM WebSphere Edge Server, Version 2.0.1 with efix 35
- IBM Tivoli Access Manager, Version 4.1
- Sun iPlanet Portal Server, Version 3.0 with Service Pack 3 and Hot Patch 3

Sametime integration through a reverse proxy

For Sametime integration, the key to making Sametime work through a reverse proxy is to make sure that the host name for the Sametime community server resolves both internally and externally to the IP address that you expect to get. In most situations this requires a split-horizon DNS that allows a given host name to return different IP addresses depending on which DNS server you access. Figure 3-3 on page 65 provides an overview of a split-horizon DNS configuration for Sametime, and the following section explains how this configuration works.

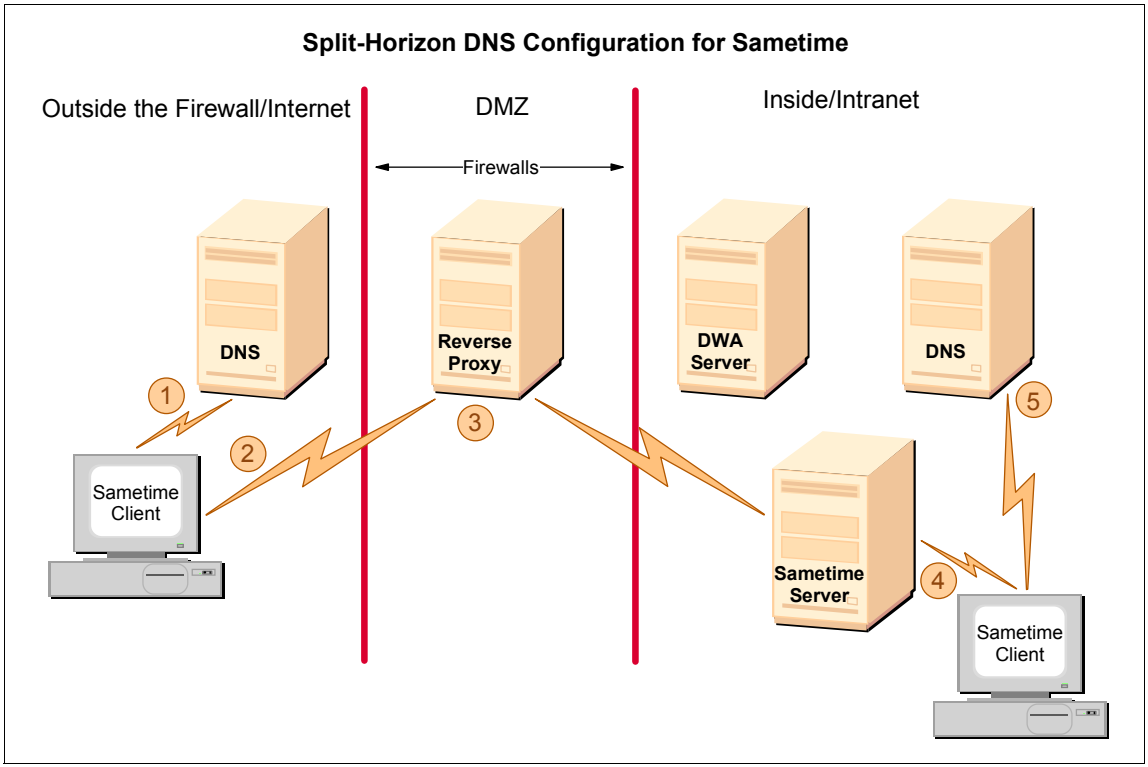


Figure 3-3 Split-horizon DNS configuration for Sametime

Referring to Figure 3-3, the process for the client outside of the firewall to properly resolve the name of the Sametime server behind the reverse proxy server is as follows:

1. Client outside firewall looks up `sametime.ibm.com`.
2. DNS server returns IP address `129.42.19.49`.
3. Reverse Proxy knows that requests for sametime.ibm.com resolve to an internal address to reach the proper host.
4. Client on intranet looks up sametime.ibm.com.
5. DNS server returns IP address `9.33.10.20`.

Note: Reverse proxy support is a new feature in Sametime 3.1 and is known to fail with prior versions.

Tuning configurations for a reverse proxy server

Reverse proxy servers are essentially Web servers and as such have similar tuning considerations. In general, parameters that one might want or need to check and adjust for performance reasons are as follows:

- Cache size: DWA utilizes Domino Web server caching. While some content is static and could potentially be cached on the proxy, the requirement to check that the cache is valid requires as much overhead as using the optimized HTTP stack from Domino. Use of the cache for images is good, but caching the script files seems of limited value.
- Number of active threads: Depending on the threading model used by the proxy, the number of active threads available to service requests could be very important. This should probably be sized slightly higher than the expected concurrent user count.
- Number of requests over a single connection: While this may not be applicable to all reverse proxy servers, the ability to control and allow several requests over a single connection significantly reduces the overhead of pulling down the multipart rich HTML interface. For DWA, a normal load of the interface will make about 15 requests against the Web server and several against a Sametime server if present. (These values will vary with different configurations and customizations.)
- If using DOLS, the retrieval of the filesets used to do the install is on the order of 75 MB with the largest two files being greater than 30 MB each, so if the installation of the offline client works without the reverse proxy but fails behind it, this could be a problem.

3.1.3 Reverse proxy with ICM

Reverse proxy support with Internet Cluster Manager (ICM) is the next interesting setup to address. This is especially important in order to support DOLS, so be sure to understand the technologies behind each component. The reverse proxy shields your internal content servers from the Internet, whereas the ICM is responsible for picking which content server should satisfy a given request. The interesting part is that the proxy server has to hide the identity of the content server, as that is its job. This means that the 302 redirect has to be rewritten (as described in both the reverse proxy case and accelerator case) not only to change the host that is being accessed, but also to modify the URI so that it will match a junction on the reverse proxy to direct it to the right content server. Both of these steps are required to keep the internal host name hidden and to keep from looping the request. The internal host name is most likely not resolvable via external DNS.

Figure 3-4 on page 67 illustrates this scenario, and the detailed steps occurring within this process follow it.

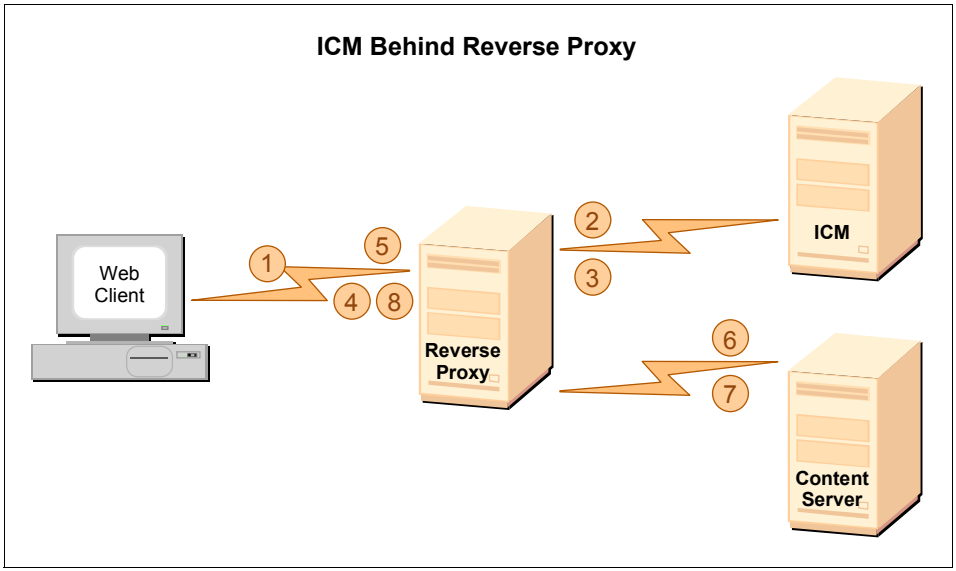


Figure 3-4 ICM behind a reverse proxy

Referring to Figure 3-4, this is how ICM works behind a reverse proxy:

1. Client requests `http://icm.ibm.com/mail/malexander.nsf`.
2. Reverse Proxy requests /mail/malexander.nsf from “real” icm.ibm.com.
3. ICM returns `http://contentserver.ibm.com/mail/malexander.nsf` to the reverse proxy server as a 302.
4. Reverse Proxy rewrites the location header to Web client as location: `http://icm.ibm.com/mail1/mail/malexander.nsf` with the `/mail1/` inserted so that when followed, this link is different from the first request.
5. Client requests: `http://icm.ibm.com/mail1/mail/mail/malexander.nsf`
6. Reverse Proxy has junction or rule for `/mail1/*` to strip `/mail1/` and request from content server with the shorter URI: `contentserver.ibm.com/mail/mailalexander.nsf`
7. Content server delivers initial request data with status 200.
8. Reverse Proxy returns status 200 to client with data where data was not manipulated.

3.1.4 SSL accelerators

Along with a reverse proxy, another excellent device to use in a large-scale DWA environment is an SSL accelerator. This enables the encryption of data to be off-loaded to other specialized hardware. An SSL Accelerator is essentially a reverse proxy at its core, with the added ability to encrypt traffic typically on one, but potentially both, ends of a connection. The significant configuration that has

to take place with an SSL accelerator is that it has to be able to rewrite the location header of the HTTP response for 302 redirects. Because the server does not have knowledge that it is behind a proxy or SSL accelerator, it will go ahead and send back a 302 redirect with a location of `http://<host>/<uri>`, while the intention is for the browser to be redirected back to the SSL port. This is similar to the case of the non-secured reverse proxy. Instead of touching the host part of the URL, however, the proxy must modify the protocol element.

Figure 3-5 illustrates the concept of the SSL accelerator and how it functions to off-load the encryption data to a specialized server.

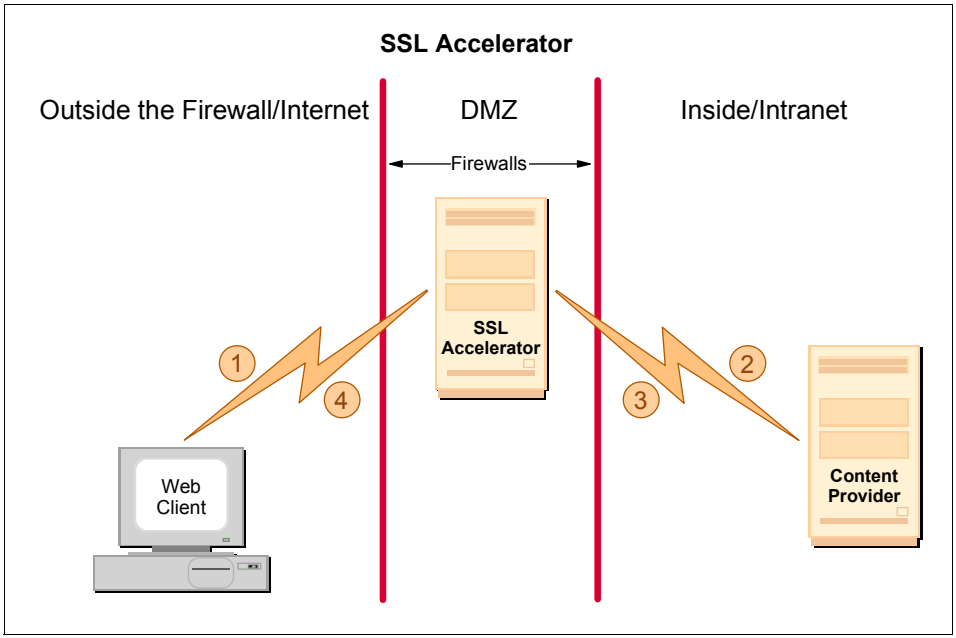


Figure 3-5 SSL accelerator

The process of an SSL accelerator functioning to off-load the encrypted data to another server is explained as follows:

1. Client requests `https://www.ibm.com/mail/malexander.nsf` over standard port 443.
2. SSL accelerator decodes request and requests `http://contentserver/mail/malexander.nsf` over port 80, thus offloading the SSL processing from the content provider.
3. DWA provides a 302 redirect with location `http://contentserver/mail/malexander.nsf`.

4. SSL Accelerator must then rewrite the location header of the 302 redirect to `https://www.ibm.com/mail/malexander.nsf`. Some SSL accelerators do not alter the protocol of 302 redirects by default, or on a per-URI basis, which should be considered before investing in such hardware.

3.1.5 Integration within a portal environment

The integration of Domino Web Access with a portal environment is covered in detail within Chapter 10, “WebSphere Portal integration” on page 339, including deployment considerations with both Portal Server versions 4.2.1 and 5.0. Appendix A, “WebSphere Portal 5 installation on Linux” on page 387, reviews installation of Portal 5. This appendix is written for Domino administrators with little WebSphere Portal experience.

3.1.6 LDAP environments

One of the functions of Domino Web Access being hosted on a Domino Server is that with some configurations, you can be very flexible in your user administration. On Linux, a Web browser interface is supported to do many of the required administrative actions. However, if you typically use LDAP tools for user administrative tasks, some of these tasks may still be available, while there may be limitations to accessing other tasks. In the following sections, some of these limitations are described and should be noted.

Note: Much of the information provided within the following section, “Admin considerations,” is also available within the Administrator Help files for DWA 6.5. We felt that this information is very important for users and administrators and therefore wanted to include it in this section as well.

Admin considerations

By default, the LDAP service does not allow LDAP clients to modify the directories that the LDAP service serves. However, you can enable LDAP write access for any of the following directories to enable LDAP users with the required database access to modify the directories:

- Primary Domino Directory of the LDAP service
- Secondary Domino Directory or Extended Directory Catalog that LDAP services serves

You control LDAP write access separately for each directory. For example, you could enable write access for the primary Domino Directory but leave write access disabled for an Extended Directory Catalog.

Note: You cannot enable LDAP write access to a condensed Directory Catalog served by the LDAP service.

Keep the following points in mind if you enable LDAP write access for a directory:

- Domino does not provide a tool for doing LDAP write operations, so you must develop or obtain one.
- If you allow LDAP write access, use the directory database ACL and, optionally, extended ACL, to control the directory changes that LDAP users can make.
- Enable schema checking for the LDAP service to require that directory changes made via LDAP conform to the directory schema. By default, schema checking is disabled so if you allow LDAP write operations, enabling it is recommended to maintain consistent directory contents.
- The Administration Process server task does not respond to LDAP write operations. For example, if an LDAP user deletes a Person document, the Administration Process cannot delete the associated user name from database ACLs.
- The LDAP service can carry out an LDAP write operation in a secondary Domino Directory or Extended Directory Catalog only if that directory is stored locally on the server that runs the LDAP service. If the LDAP service receives a write operation request for a Domino Directory on a remote server, it sends an LDAP referral to the client. The LDAP service refers the client to the administration server for the directory. If there is no administration server specified, it refers the client to the remote server that stores the directory. The client must then follow the referral itself.

  Note: If you enable LDAP write access to a secondary Domino Directory, do not use a condensed Directory Catalog that aggregates that directory on a server that runs the LDAP service.

- The distinguished names of directory entries are limited to 256 characters. Distinguished names do not have to conform to the standard Notes naming model of organizational unit (ou), organization (o), and country (c). For example, distinguished names such as these are acceptable:

  ```
  dn: cn=Jay Walker + uid=123456,u=Sales,o=Widget Inc.,c=GB
  dn: foo=Bar, o=Acme
  dn: cn=L. Eagle,o=Sue\, Grabbit and Runn,c=GB
  ```

  Names such as these are recommended primarily for entries that are accessed through LDAP only, as Notes users may find them confusing.

- Prior to doing batch adds of 100 or more directory entries, you can use the NOTES.INI setting LDAPBatchAdds to process the additions more quickly. Disable the setting when the batch adds are complete.
- You cannot modify the value of an entry's structural object class attribute.
- Another consideration for using LDAP with Domino Web Access is to have clients look up users in other directories via LDAP. This is accomplished via directory assistance. Directory assistance allows for users who need to look up a name to ask the server to do an LDAP query on their behalf based on a partial identifying information. For example, a user could look up "Smith" and pick between John Smith and Jane Smith if both are returned by the search. DWA would then use the response from directory assistance to finish the job by inserting the mail address in the appropriate field.

3.1.7 Network demands

The section is a high-level analysis of the of data requests required by Domino Web Access and the corresponding demands on a network.

Several tools were used to collect information for this book, and one tool in particular stands out as useful and easily available for use in validating and updating this information. Short of using a sniffer with advanced analysis tools, the size and content of the requests being made by a Web application from a Windows machine can be determined with a small tool from IBM AlphaWorks called IBM Page Detailer, which is available at:

`http://www.alphaworks.ibm.com/tech/pagedetailer`

With this tool, an administrator or power user can observe HTTP (or other) network traffic at a level that may reveal what requests might be causing delays or what requests require the most bandwidth. This tool is also very good at illustrating some of the overhead of network traffic, including the time it takes to establish the TCP socket and the time taken to do name resolution. It should be noted that IBM Page Detailer shows the elapsed time for the request, the server processing (which could be matched against server logs), and the delivery time back to the client. The monitoring is done at the network, which excludes monitoring of how long it takes for a browser to actually render the page. In most cases this will not be a significant issue, but it should be noted.

Online

As Domino Web Access is a client server application, with a new client a complete login to the DWA interface requires about 50 requests. (This was simulated by clearing the cache and deleting jar and class files that have been delivered.)

Note: This number can vary due to customizations and specific configurations.

To consider the impact of possible customizations and specific configurations, we examine the impact of adding Sametime and, later in this chapter, the use of DOLS.

By default for this testing, we load the Inbox view initially, instead of loading the Welcome page, which could add considerably to these figures. Of these requests, nine are requests for scripts and they all come from /iNotes/Forms6.nsf or the user mail file:

```
/mail/malexand.nsf/iNotes/Mail/?OpenDocument&ui=inotes
/mail/malexand.nsf/iNotes/Proxy/?OpenDocument&Form=s_Toc
/mail/malexand.nsf/iNotes/Proxy/?OpenDocument&Form=s_SessionInfo
/mail/malexand.nsf/iNotes/Proxy/?OpenDocument&Form=s_MailOutline
```

Data comes from the mail file, because it is user specific. Alternatively, the parts that come from the Forms6 database are general design concerns that are similar for all users. Looking at the requests that generate the UI of DWA, we get:

```
/iNotes/Forms6.nsf/iNotes/Proxy/?OpenDocument&Form=s_MinUtils
/iNotes/Forms6.nsf/iNotes/Proxy/?OpenDocument&Form=qpbase
/iNotes/Forms6.nsf/iNotes/Proxy/?OpenDocument&Form=qpview
/iNotes/Forms6.nsf/iNotes/Proxy/?OpenDocument&Form=Custom_JS
/iNotes/Forms6.nsf/iNotes/Proxy/?OpenDocument&Form=s_StyleSheet
```

All of these script requests (as well as the one style-sheet request) have query strings that identify a validity period when compared to the current version on the server. They also take advantage of the HTTP stack's GZIP compression algorithm by default.

In total, these scripts (both from the forms6.nsf and mail file) add up to about 162 KB of data transmitted across the wire. (This includes the total content length, HTTP headers, and some additional overhead.) Compare that to the uncompressed size of about 624 KB, and you can see that any time these documents get pulled you see a substantial benefit.

The other 40 requests loaded on the initial download are GIF elements that make up the page. These images are all very small and set an expires header well into the future, which allows for minimal overhead on subsequent page loads.

Sametime

When you configure Sametime and enable Instant Messaging, you add some overhead on the network, but no more than the standard chat activity from using

Java Connect or the Connect client. The elements that are added to the Web application are the STLinks files, which are downloaded from the DWA server:

- stlinks.ccs
- stlinks.js
- hostinfo.js
- a language-specific res.js file

Offline setup

The offline setup requires users to pull a mini-Domino server to their workstation in several parts. As mentioned above, the setup files range in size from 37 MB for the l_DOLBASE archive to several kilobytes for the license. The bulk of the delivery is in the largest two files, l_DOLBASE and l_JAVA_APPLETS. These files are only slightly larger than the Windows versions, which are also required for download. Accordingly, there is only minimal cost difference on transfer of files.

This should be noted as the first of two key considerations for performance of the offline client. To effectively be able to take a subscription offline, users will want to be connected to a high-speed network if possible, in order to minimize download time.

The second key consideration is the extent to which users have mail of any significant volume. If they do, they will need to be on a workstation that has enough processor and memory to index the file in a timely way. The release notes indicate that “based on customer feedback, Lotus Software/IBM recommends that users have at least a Pentium® II 400 MHz machine with 128 MB of memory in order to have reasonable client-side performance.“

The experience in our lab environment was that such a machine provides adequate performance for a small mail file. However, as the mail file grew beyond a few hundred messages, the initial indexing took a large percent of the computing resources, leaving us waiting for several minutes. As is the case with most software, somewhat quicker response was easy to demonstrate on a Thinkpad T30 or T40 with later-generation processors and hundreds of megabytes of RAM. The best advice for quick indexing time would be to keep mail file size down. A fast client can help to quickly index even a large inbox.

4

Installing Linux

This chapter describes how to install Red Hat and UnitedLinux on your server. We focus on these two specific distributions because they are the officially supported versions of Linux for a server running Domino Web Access 6.5.

The chapter has three parts, beginning with prerequisite steps for the installation, then giving detailed instructions for each of the supported distributions of Linux. An overview of the organization of this chapter is as follows:

- 4.1, “Before you begin” on page 76, provides a list of preparatory steps you will want to review to make sure that your hardware is Linux-ready. This section also provides a brief overview of the different Linux distributions.
- 4.2, “Installing Red Hat 2.1AS” on page 82 describes the step-by-step process of installing this Red Hat Linux Advanced Server distribution.
- 4.3, “Installing UnitedLinux 1.0, SLES 8” on page 114 describes the process of installing UL 1.0 on your server.

4.1 Before you begin

Before you can install Linux, be sure that your machine is Linux-ready, and choose a Linux distribution to install. The pre-installation checklist may help you organize configuration data before you begin.

Read the following section before performing the installation of Linux. There are several things you must do or should be aware of to make the installation process easier. In addition, make note of the following information about your system, which will be useful when you perform the installation:

- Network card type
- Network information
  - IP address
  - Gateway information
  - DNS servers
- Video card type
- Number and types of hard drives
- Monitor information

The following Web sites offer a complete listing of hardware supported and certified by Linux:

http://www.suse.de/us/business/certifications/certified_hardware/
http://sources.redhat.com/ecos/hardware.html
http://en.tldp.org/HOWTO/Hardware-HOWTO/

We recommend that before beginning the installation, you collect and briefly review any hardware-related manuals. In addition to knowing the details of the machine, you will need to know the network card type, video card type, the number and types of hard drives, and other information about any peripheral devices.

4.1.1 Making the CD-ROM/DVD drive bootable

The recommended way to install Linux is to boot from the installation CD-ROM. If you plan to boot your system directly from the CD-ROM, ensure that the CD-ROM is the initial boot device. Do this by following these steps:

1. Power on your server.
2. Enter the BIOS setup utility.
3. Make sure that your CD-ROM is the initial boot device.

4. Save the settings.
5. Exit the setup utility.

The alternative is to make boot diskettes from the Distribution CDs and use those to boot the system. Do this by following these steps for Red Hat:

1. Insert *Red Hat Installation CD 1* into a Windows machine.
2. Use RAWRITE from the DOSUTILS directory to write the disk image to a Floppy disk. The disk images are stored in the IMAGES directory on the Red Hat install CD. The files in this directory are raw disk images. Some are boot disks for booting the Red Hat Linux installation program. Others are driver disks supporting less-common hardware. Follow the instructions in the *Red Hat Linux Installation Guide* to create the disks.

   For an example of this command, see “RAWRITE utility” on page 77.

Follow these steps to create the boot disks for UnitedLinux:

1. Insert *UnitedLinux Installation CD 1* into a Windows machine.
2. Use RAWRITE from the DOSUTILS\RAWRITE directory to write the disk image to a Floppy disk. The disk images are stored in the DISKS directory on the UnitedLinux install CD. The files in this directory are raw disk images. The following files are boot images: bootdisk, i386, and rescue. Only a few modules fit on the boot disk. Therefore, three modules floppy disks exist. You will need these diskettes if you cannot find the driver for your hardware on the normal disk. The modules disks contain the following files:
   - Modules1: USB and file system modules
   - Modules2: SCSI/RAID/IDE modules and old (non-ATAPI) CD-ROM drivers
   - Modules3: Network, PCMCIA, and FireWire (IEEE1394) modules

RAWRITE utility

RAWRITE is a utility usually shipped with the Linux distribution; it is used to write the prepared diskette images to diskettes, enabling them to be used in the installation process.

To create a diskette from one of these prepared images:

1. Load the Linux CD on a Windows machine.
2. Open an MS-DOS prompt.
3. Change the default directory to the directory where the diskette images are stored (this varies according to the distribution of Linux used).

4. Run the following command by pre-pending the directory where the RAWRITE program is stored:

```
\path\rawrite image a:
```

For Red Hat, replace *x* with your CD-ROM driver letter and run:

```
x:
cd \images
\dosutils\rawrite -f boot.img -d a
```

For UnitedLinux, replace *x* with your CD-ROM driver letter and run:

```
x:
cd \disks
\dosutils\rawrite\rawrite
bootdisk
a
```

There is a version of RawWrite for Windows. This is available from:

http://uranus.it.swin.edu.au/~jn/linux

4.1.2 RAID configuration

If you have a machine with a RAID controller, you must configure the disks before you install Linux. Use the same procedure to configure your RAID sets as you would for a Windows NT or Windows 2000 machine. After your RAID is configured and the logical disk is online, you can proceed with the installation of Linux. You may need a driver disk for the Linux installation.

4.1.3 Partitions

We have simplified the typical UNIX partitioning scheme. A conventional UNIX-style install would include partitions for /home, /usr, and more. However, a Domino server does not require or use a number of these partitions, so they are simply a waste of disk space. Therefore, we have concentrated on the ones important for Domino.

Attention: One reason for a conventional UNIX-style install is to prevent users of your system from filling your hard drive. Therefore, if you are installing Linux on an external system that will have exposed volumes, such as an FTP area, you should create a partition specifically to hold the FTP data. While this will limit the total amount of available disk space, it will keep your system from crashing if someone intentionally or unintentionally uses all remaining disk space.

Table 4-1 An example of partitioning on a Domino server

Partition	Description	Minimum size	Recommended size
/	Root partition	2 GB	3 - 9 GB
/local	Partition for data		See Note 1
/translogs	For transaction logs		See Note 2
/var	For system files, such as log files	256 MB	512 MB
<swap>	Page file		See Note 3

Table notes:

1. This is where your Notes data is stored. Depending on the number of users and amount of data you keep, this partition can require a lot of disk space.
2. This partition is needed if you will be using Domino transaction logs. We recommend that you do so and that you dedicate a 4 GB RAID1 to the transaction logs. You may skip creating this partition if you are not going to make use of transaction logs.
3. See Table 4-2 for recommended SWAP partition sizes.

Table 4-2 SWAP memory size

Amount of physical memory	Size of SWAP partition
< 256 MB	4 times physical memory
512 MB	2 times physical memory
1024 MB	1 times physical memory
2048 MB >	2048 MB

4.1.4 Time configuration

During the Linux installation process, you will be asked whether your system clock is set to UTC (Coordinated Universal Time) or to local time. We recommend that you set the system clock (the BIOS clock) to UTC/GMT. This way Linux can keep the clock on the correct time when the change for Daylight Saving Time occurs. The safest way is to set your clock to UTC before beginning the installation process. If you have missed this, you can still set the system clock immediately after you have completed the installation and before the first time your machine reboots.

Coordinated Universal Time is the international time standard. It is the current term for what was commonly referred to as Greenwich Meridian Time (GMT).

Zero hours UTC is midnight in Greenwich, England, which lies on the zero longitudinal meridian. Universal time is based on a 24-hour clock; therefore, afternoon hours such as 4 p.m. UTC are expressed as 16:00 UTC.

4.1.5 Video card and monitor

It is not as easy to configure your monitor and video card in Linux as it is in Windows. If you currently have Windows installed on the machine that you are going to use for Linux, check the video card and monitor and their respective settings before starting the Linux installation. This will help you later in the install process to select the right settings. You could also open the machine and check which video card is installed.

4.1.6 File systems in Linux

Linux supports multiple file system types. Examples of file systems in Windows are FAT, FAT32, and NTFS. As new or better file systems are developed, they are incorporated into the kernel. In Linux, as in other UNIX derivatives, the separate file systems that are available for use by the system are combined into a single hierarchical tree structure rather than being addressed by drive names. Each new file system is added into this single tree structure by mounting the file system onto a specified directory. This directory is known as the mount point. The files and directories in the mounted directory are then accessible through this directory. If a file system is mounted onto a directory that already contains files, these files are masked by the new file system and are unavailable. When the file system covering them up is unmounted, the files become visible again.

Initially, Linux used the *minix* file system. This had restrictions and performance problems, which were solved in April 1992 by the introduction of the *Extended File System* (ext). The ext file system was developed as an expandable and powerful file system for Linux. In January 1993, the *Second Extended File System* (ext2) was released. It has become the most successful file system for Linux and is the standard file system for most Linux distributions. While being a very solid, stable file system with good performance, it is quite slow to run a file system check (similar to CHKDSK). This occurs when the system fails and is being brought back up, or every 20th time the file system is mounted. On a system with big partitions, this check can take a while, and the system is inaccessible during the check.

To solve these problems, new journaled file systems were introduced with the 2.4 Linux kernel; we briefly discuss them in the following paragraphs.

Journaling ensures consistency of the file system. This means that you do not have to run the file system check if the system goes down unexpectedly. In order to minimize file system inconsistencies and restart time, journaling file systems

keep track of changes that they are about to make to the file system. These records are stored in a separate area of the file system, which is known as the journal or log. After the journal records have been written successfully, the changes to the file system will be applied and the journal entries purged. If the system goes down unexpectedly, this process ensures that the file system is consistent without the need for a lengthy check.

- ext3: ext3 extends the ext2 file system by adding journaling. This means that it shares the robustness and performance of ext2. One major advantage of ext3 compared to other journaled file systems is that it is forward-compatible and backward-compatible with ext2. You may freely switch between ext2 and ext3 as long as the file system has been cleanly unmounted or a file system check has been run.
- ReiserFS: ReiserFS stores not just the file names, but also the files in a balanced tree. Balanced trees have a sophisticated algorithmic foundation and are more robust in their performance. Storing small files in large partitions is very efficient. Being more efficient at small files, however, does not mean it is inefficient at storing larger files. ReiserFS is considered a truly multipurpose file system.

We have opted to use the ext3 file system for the Linux servers used in writing this book.

Note: The ext2 is a faster filesystem due to the fact it is not journaling everything, but it takes a lot longer to recover from a system failure than a journaling filesystem.

An excellent source of information about file systems is the File Systems HOW-TO. You can find this HOW-TO document, as well as numerous others, on The Linux Documentation Project Web site at:

`http://tldp.org/docs`

Additional information about the ext3 file system can be found on:

`http://www.redhat.com/support/wpapers/redhat/ext3`
`http://www.linuxplanet.com/linuxplanet/reports/4136/1/`

The home page for ReiserFS is located at:

`http://www.namesys.com`

4.1.7 Different Linux distributions

Domino 6.5 for Linux supports different Linux distributions, as identified in Table 4-3 on page 82.

Table 4-3 Supported Linux distributions

Distributions	Kernel version	Home page
Red Hat Advanced Server 2.1 (Uni-Processor Only)	2.4.9	http://www.redhat.com
SUSE LINUX Enterprise Server (SLES) 8.0	2.4.21	http://www.suse.com
All “UnitedLinux/Powered by UnitedLinux 1.0 SP2 for Linux on Intel distribution” That includes: - SUSE LINUX Enterprise Server (SLES) 8.0 - Turbo Linux Enterprise Server - Connectiva Linux Enterprise Server	2.4.21	http://www.unitedlinux.com

4.2 Installing Red Hat 2.1AS

In this section we show you how to install Red Hat 2.1 Advanced server on your server.

To capture the screens shown in this book, we have installed and configured Linux in a VMware window. VMware is a product by VMware, Inc. (http://www.vmware.com) that enables you to run one operating system as a guest of another. This means that some of the screens might look slightly different from what you would see on your system. These differences are hardware-related, as VMware emulates different hardware devices for the guest operating system.

Be sure to read 4.1, “Before you begin” on page 76 to make the installation easier.

To start the installation, insert the Red Hat 2.1AS CD-ROM and turn on or reboot the server.

Attention: The installation process destroys any existing data stored on your hard disk drives.

1. When the screen shown in Figure 4-1 is displayed, you can start the Linux installation. Press Enter to begin installation immediately or wait for it to start automatically after a short pause.

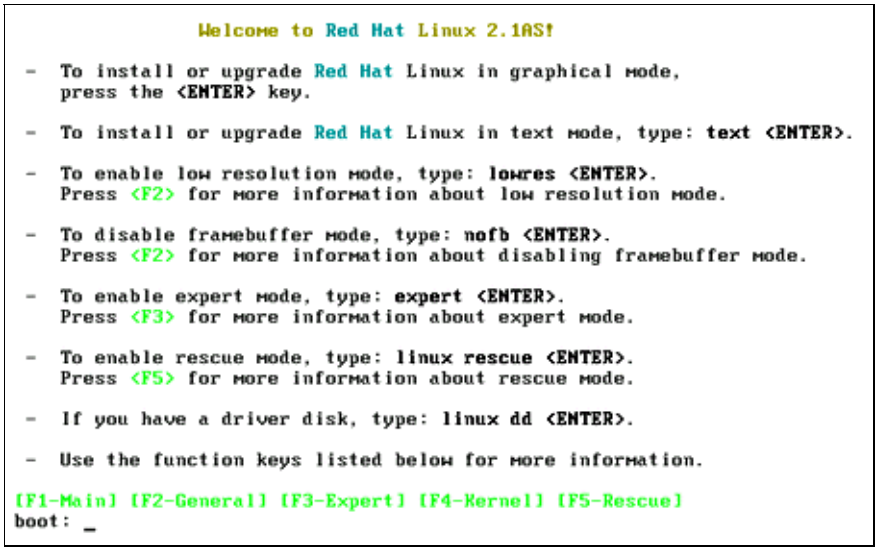


Figure 4-1 Red Hat 2.1AS: Initial boot screen

2. The system begins to probe (detect) the hardware installed on your system and load the appropriate drivers for it. The Welcome to Red Hat Linux window is displayed while this is happening.

   After the drivers are loaded, the Red Hat Install Program starts. We used the graphical setup program, so this is what is described here. If the graphical installation fails to start, consult your *Red Hat Installation Guide*.

3. Select the language from the list shown in Figure 4-2 that you would like to use *during the installation*. You will be prompted later for the languages that the OS should support. Click **Next** to continue.

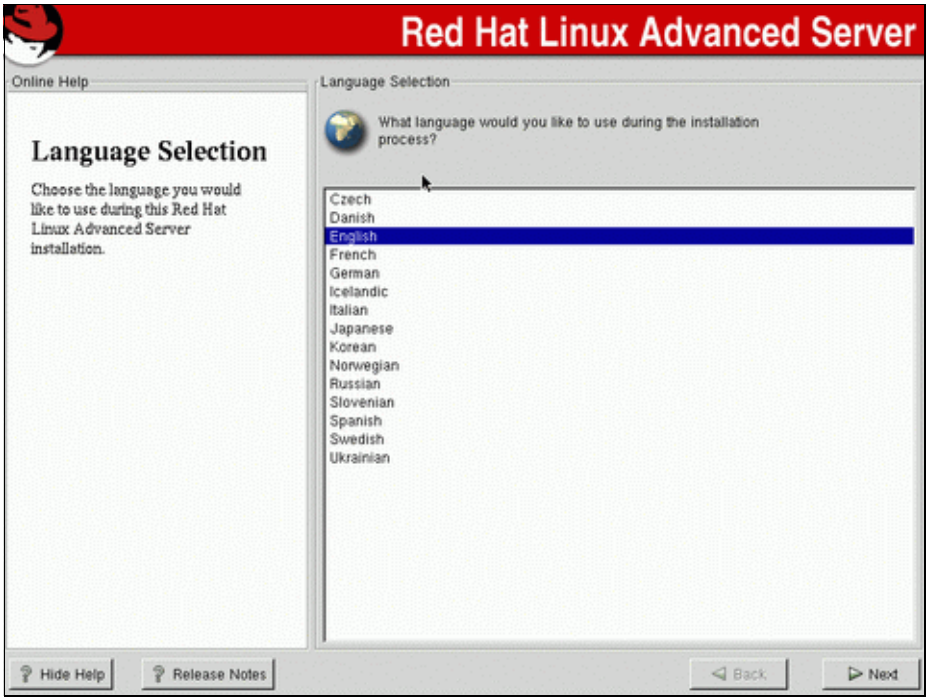


Figure 4-2 Red Hat 2.1AS: Language selection

Tip: If you do not need the Online Help bar on the left-hand side of the screen, you can disable it by clicking the **Hide Help** button in the bottom left corner of your screen. To see the help again, click the **Show Help** button.

4. The Keyboard Configuration screen is shown in Figure 4-3. Specify the keyboard attached to your computer. If in doubt, select **Generic 101-key**. Click **Next** to continue.

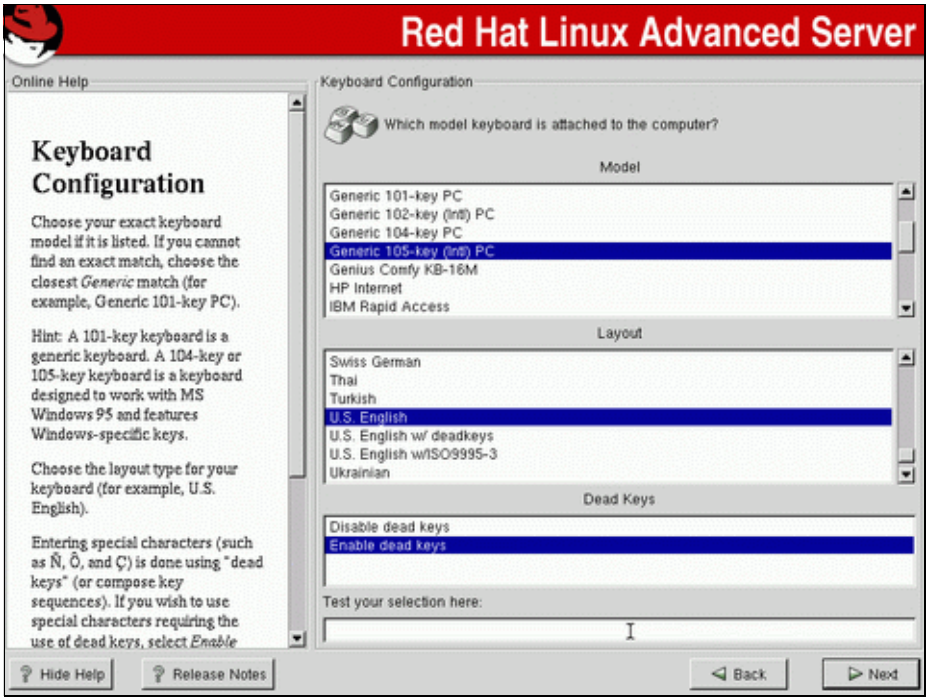


Figure 4-3 Red Hat 2.1AS: Keyboard configuration

5. As shown in Figure 4-4, you can select different mouse settings. Specify the type of mouse attached to your system and click **Next**.

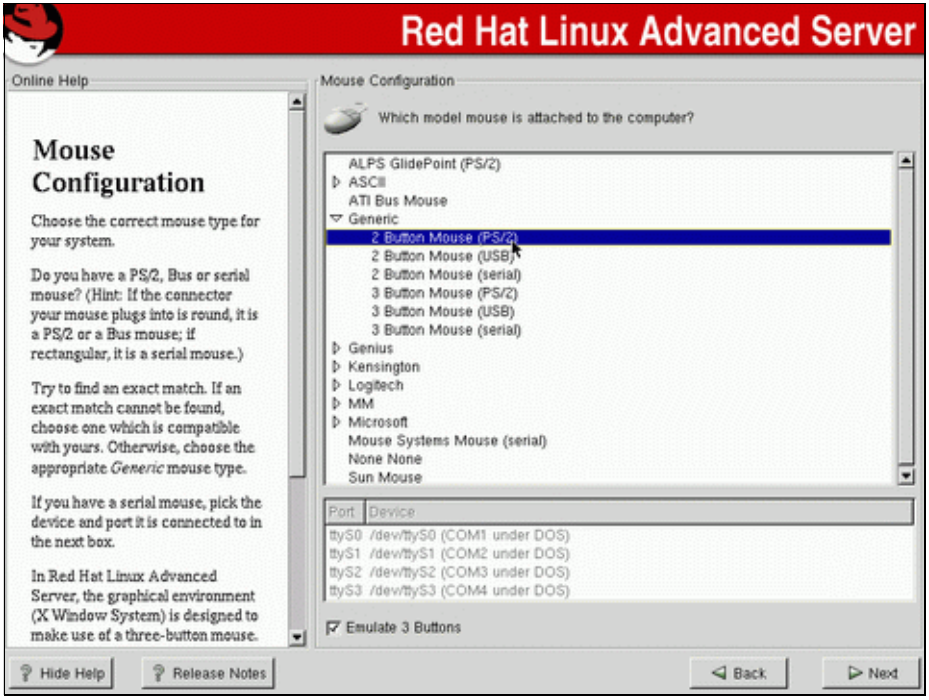


Figure 4-4 Red Hat 2.1AS: Mouse Configuration

6. On the welcome screen shown in Figure 4-5, click **Next** to start the Red Hat System Installer. The Install Options screen shown in Figure 4-6 on page 88 will be displayed.

Figure 4-5 Red Hat 2.1AS: Welcome

7. On the Install Options screen, select **Custom** and click **Next**.

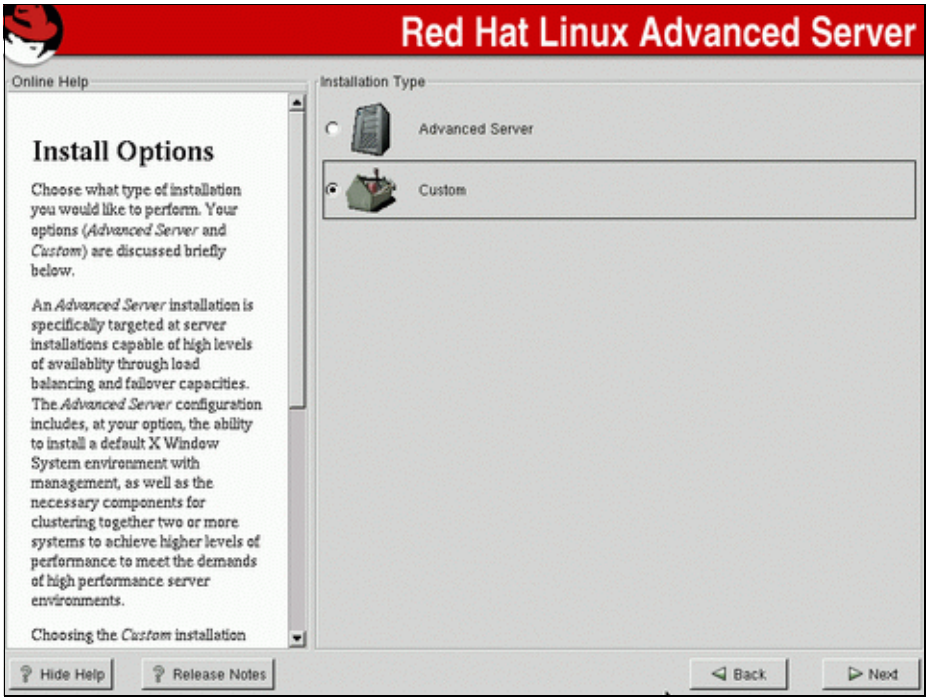


Figure 4-6 Red Hat 2.1AS: Install options

Note: Some disk controllers require drivers supplied by the manufacturer and are not supported out of the box. For more information about installing disk drivers, visit: `http://www.redhat.com/docs/manuals/linux/`.

8. On the next screen, shown in Figure 4-7, select the method you would like to use to partition your hard disk(s). We selected **Manually partition with Disk Druid** to partition the disk because the automatic process does not provide an optimal partitioning scheme. Click **Next** to continue.

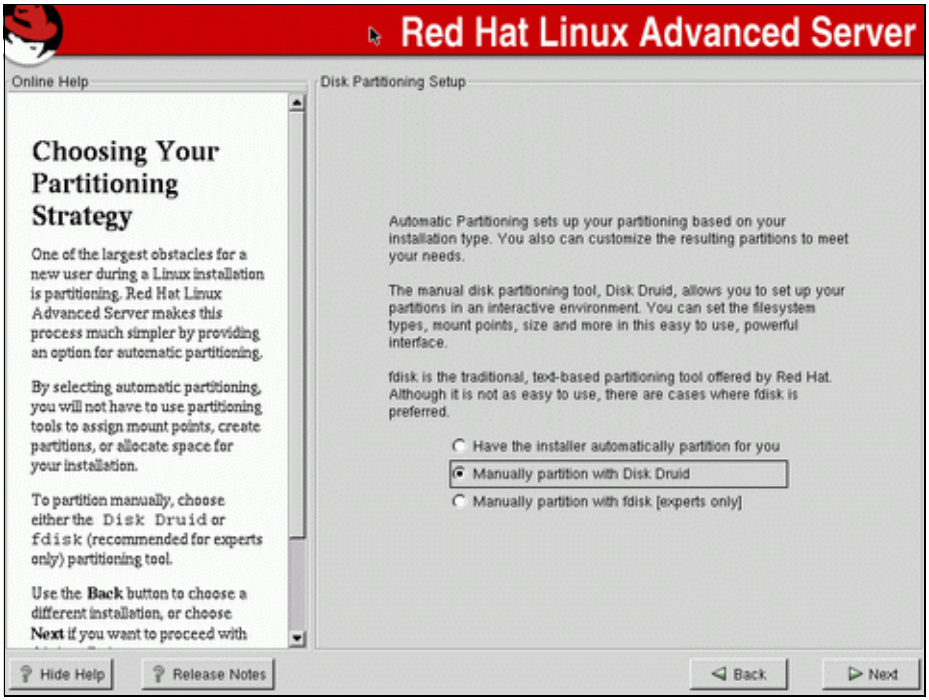


Figure 4-7 Red Hat 2.1AS: Partitioning

9. You may see a message indicating that the partition table is unreadable, as shown in Figure 4-8. This usually happens when you have new, unformatted disks. Click **Yes** to initialize each of the drives installed in your system. This message will not always appear.

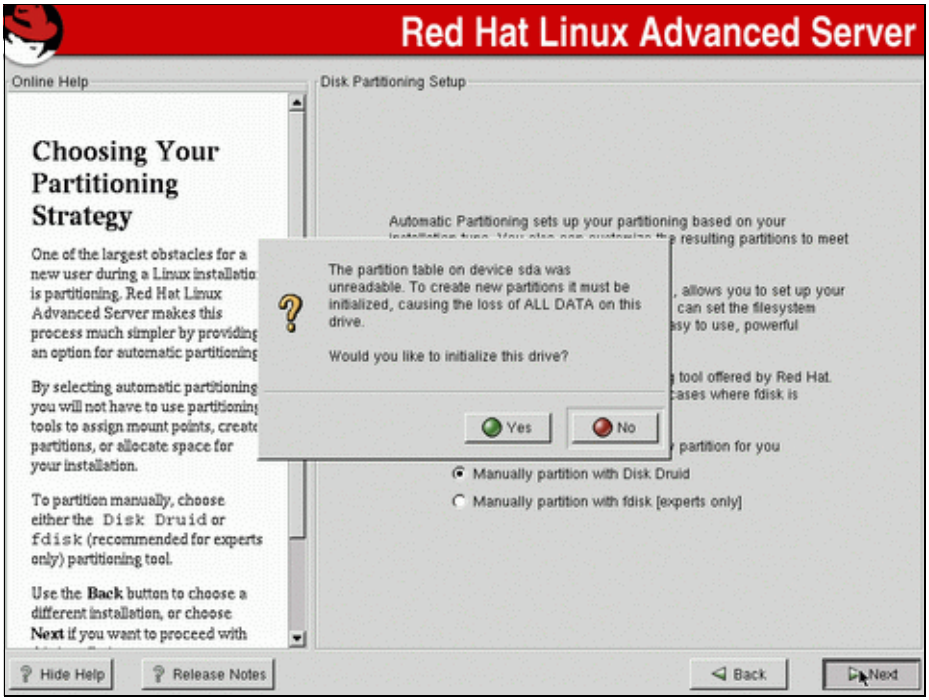


Figure 4-8 Red Hat 2.1AS: Unreadable partition table notice

10. We are now ready to partition our disks. See 4.1.3, “Partitions” on page 78 for the recommended partitions and their respective sizes.

> **Important:** If you have existing partitions from another operating system on your machine, you must delete them before you can create the Linux partitions. After the old partitions are deleted, proceed with the next step.

11. As shown in Figure 4-9, click **New** to create your partitions.

> **Important:** You can only have four primary partitions for each hard disk drive. If you need to create more than four partitions, create three *primary* partitions and one *extended* partition that uses all of the remaining disk space. You can then create all subsequent partitions in this extended partition.

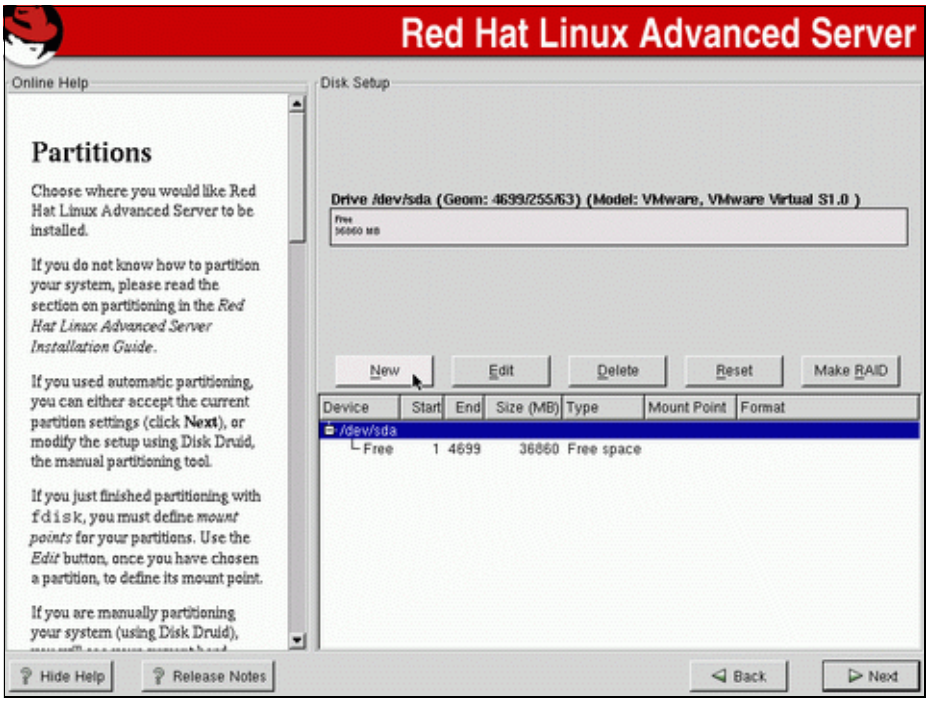


Figure 4-9 Red Hat 2.1AS: Drive geometry

12. A window is displayed, as shown in Figure 4-10, to enter all relevant information for creating a partition:

    a. To specify the mount point of a partition, either select it from the Mount Point pull-down list or type it in the field provided. We selected **/** in order to create the root partition.

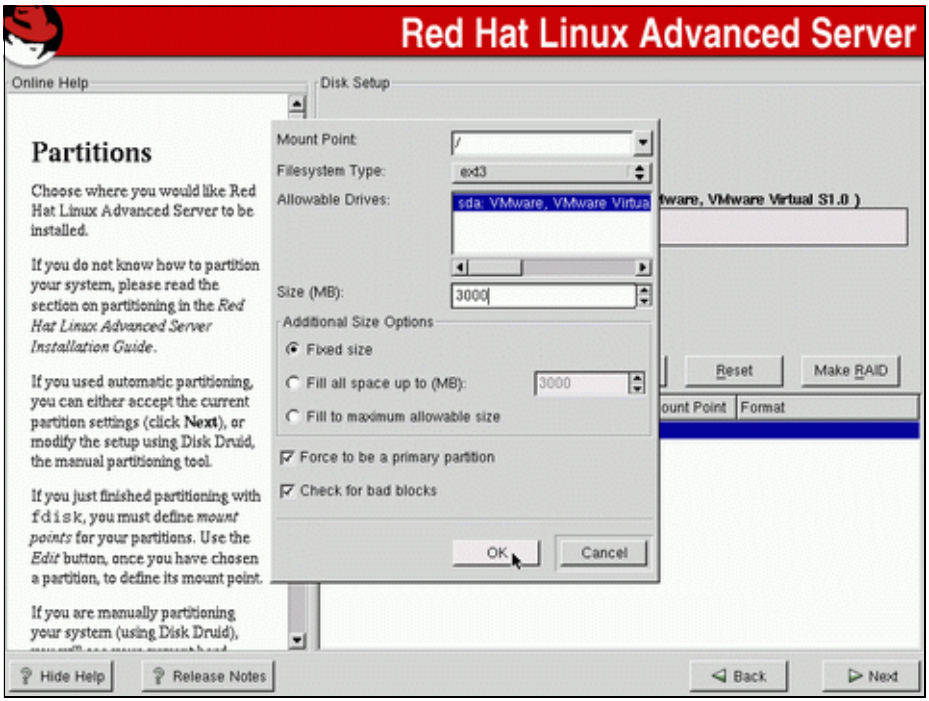


Figure 4-10 Red Hat 2.1AS: Creation of the / (root) partition

    b. If you have more than one hard drive in your system, the partition will be created on any one of the selected drives. Unselect all drives except the one that is to hold the partition. The blue line indicates that the / root partition should only be created on sda.

> **Note:** /dev/sda is the first disk connected to a SCSI controller in the machine. Subsequent disks will be sdb, sdc, and so on. If you have multiple controllers, the disks will be numbered sequentially starting on the first controller and continuing on the second controller. Depending on the implementation of the RAID controller in your machine it could be known as /dev/sda for a IBM ServeRAID™ Controller or /dev/ida/c0d0 for a Compaq Smart Array Controller. The first IDE drive would be /dev/hda.

c. Enter the size of the partition. We have a 36 GB (36000 MB) drive, and we need 1 GB for swap and roughly 500 MB for /var, so we allocated 3 GB to the root partition. Refer to Table 4-2 on page 79 to determine the appropriate size of swap partition for your system.

d. In the Additional Size Options box, you have several options. We selected **Fixed size** because we wish to specify a 3 GB partition size.

e. Because it is safer to boot off a primary partition, we recommend that you select **Force to be a primary partition** for the boot partition (the partition that contains your root file system).

f. Select **Check for bad blocks** to be confident that your drives are in good shape; this will take quite a bit of time for large drives.

> **Tip:** To be safe, you should always select **Check for bad blocks** for all partitions you create.

g. When all information is entered correctly, click **OK** to create the partition.

13. To create the Swap partition, click **New** on the Disk Setup Screen. Click the **Filesystem Type** pull-down menu and select **swap**, as shown in Figure 4-11.

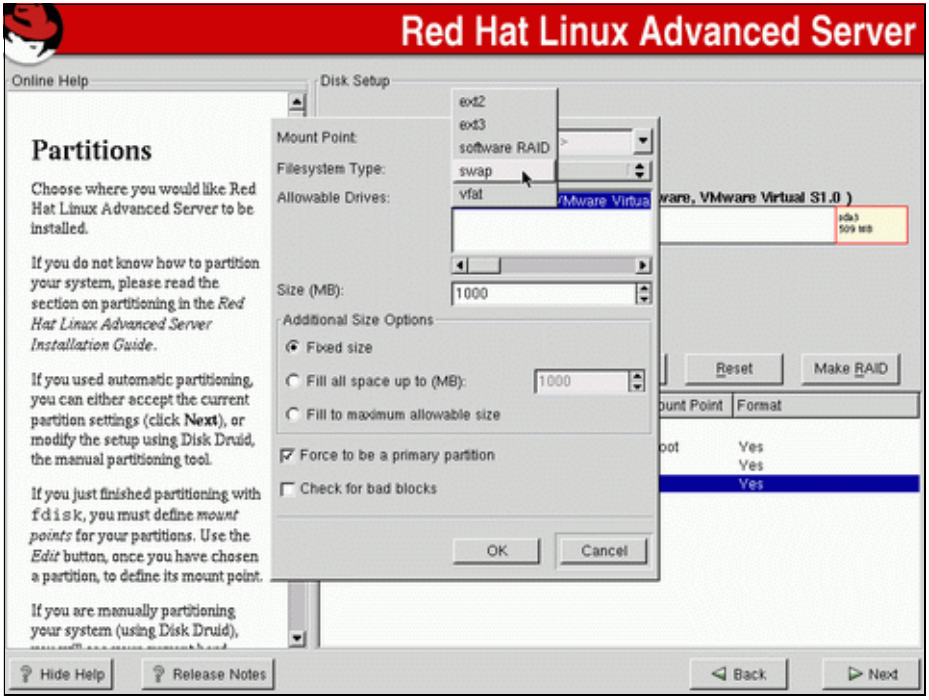


Figure 4-11 Red Hat 2.1AS: Selecting swap as the filesystem type

14. Select the appropriate disk array (**sda** in our case) from the Allowable Drives list, enter the size of the swap partition, and select **Fixed Size**. Click **OK** to create the swap partition. Our choices are shown in Figure 4-12.

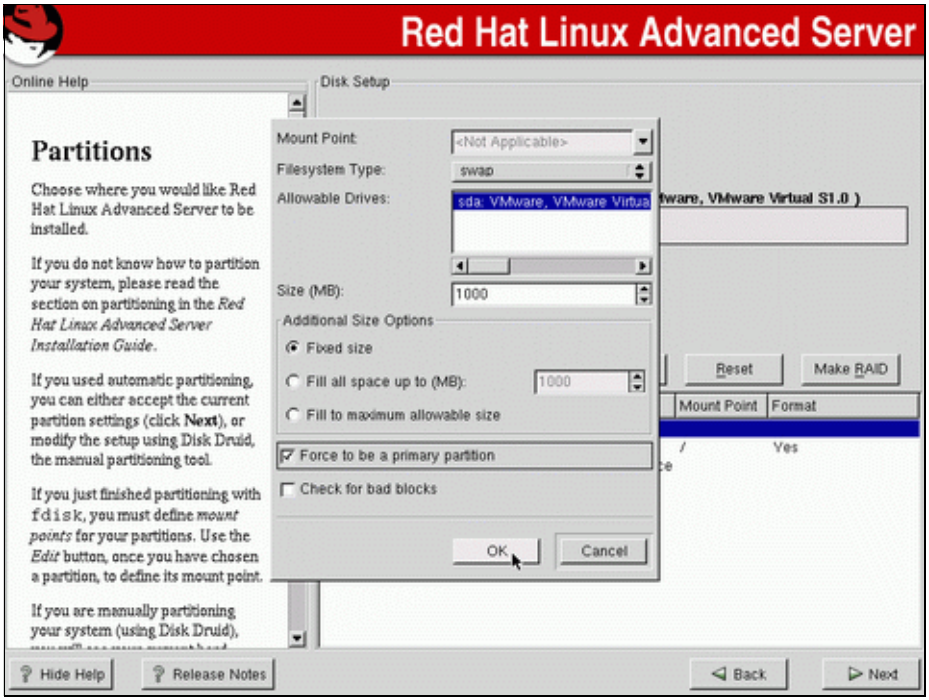


Figure 4-12 Red Hat 2.1AS: Creation of the swap partition

15. Create the /var partition in the same manner described previously for the other partitions on sda. The results of our selections are shown in Figure 4-13.

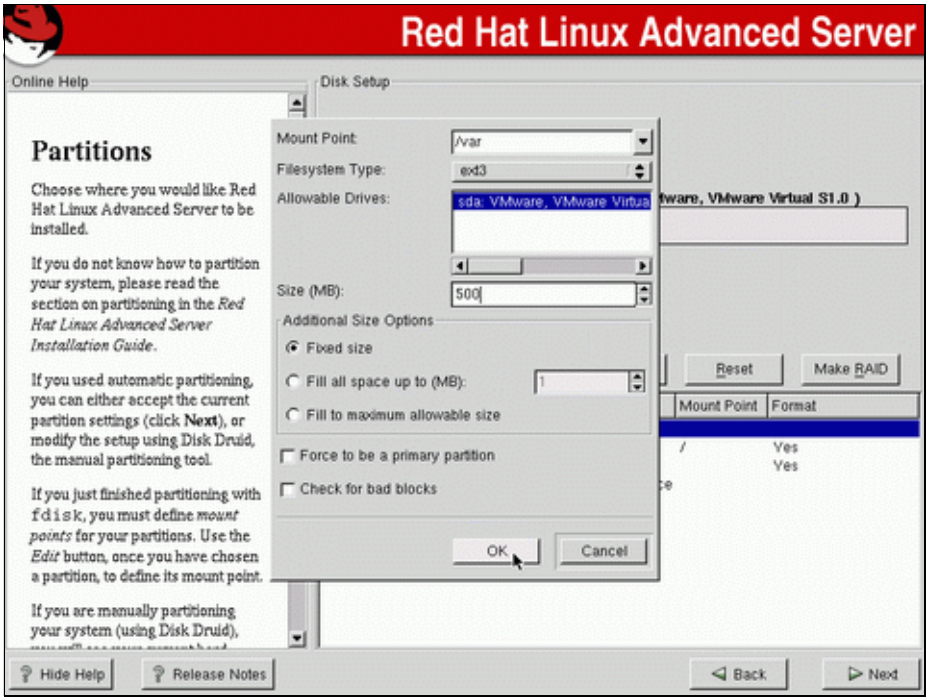


Figure 4-13 Red Hat 2.1AS: Creation of the /var partition

16. The next partition to create is /translogs for the Domino Transaction Logs. Type `/translogs` into the Mount Point field. Figure 4-14 shows how to enter a mount point that is not available in the drop-down list. Click **OK** to create the partition.

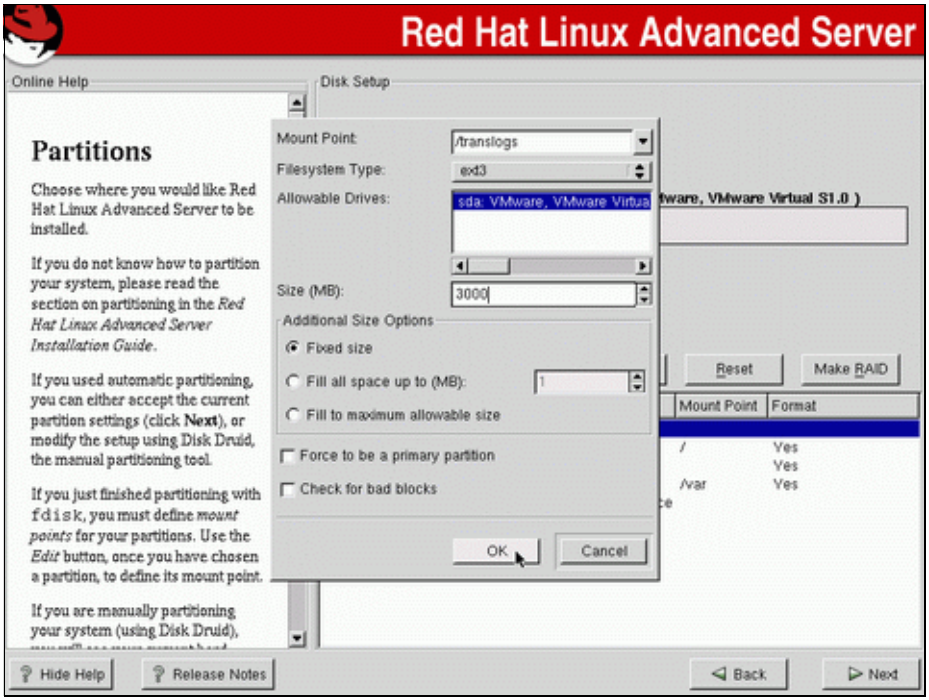


Figure 4-14 Red Hat 2.1AS: Creation of the /translogs partition

17. Click **New**, then enter `/local` in the Mount Point field. Because `/local` utilizes the entire disk, specify disk array **sda** in the allowable Drives section, then select **Fill to maximum allowable size** as shown in Figure 4-15. This is the easiest way to utilize the entire disk. Click **OK** to create the partition.

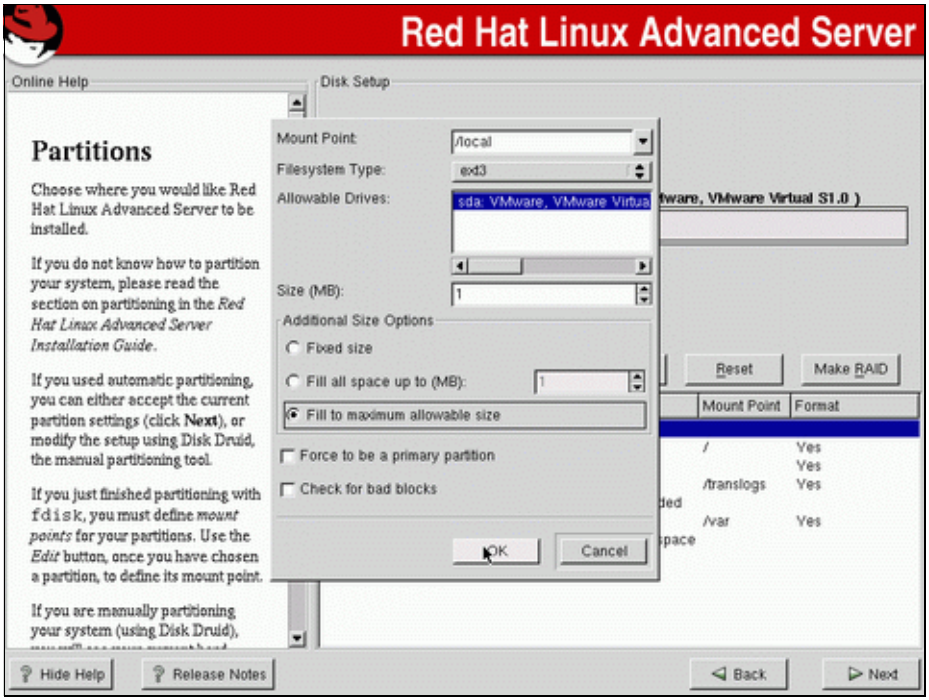


Figure 4-15 Red Hat 2.1AS: Creation of the /local partition

18. Figure 4-16 shows all of the partitions that have been created. Click **Next** to write the partition table to disk.

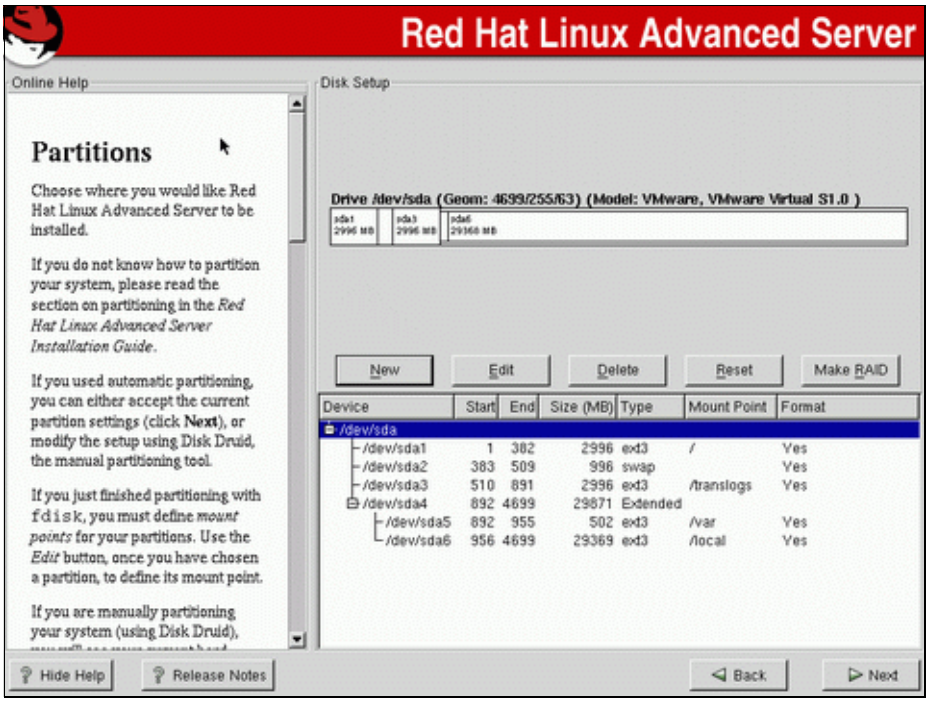


Figure 4-16 Red Hat 2.1AS: Final partition list

19. Figure 4-17 on page 99 shows the boot loader options.

    A boot loader is the first software program that runs when a computer starts. It is responsible for loading and transferring control to the operating system kernel software, which then loads the operating system. A boot loader can be used to start Linux and other operating systems, such as Windows or OS/2®. Examples of boot loaders are GRUB and LILO for Linux and NTLDR for Windows NT/2000.

We used GRUB (Grand Unified Boot Loader) for our installation because it is the default boot loader for Red Hat. Be sure to specify that the boot record should be installed in the MBR (Master Boot Record). All other default options can be accepted.

Attention: If the boot partition of the system you are installing is on an IDE hard drive and it is stored on a section of the hard drive that is located beyond 1024 cylinders, select **Force use of LBA32**. The boot loader has to do special processing to address more than 1024 cylinders when booting the system from such a partition.

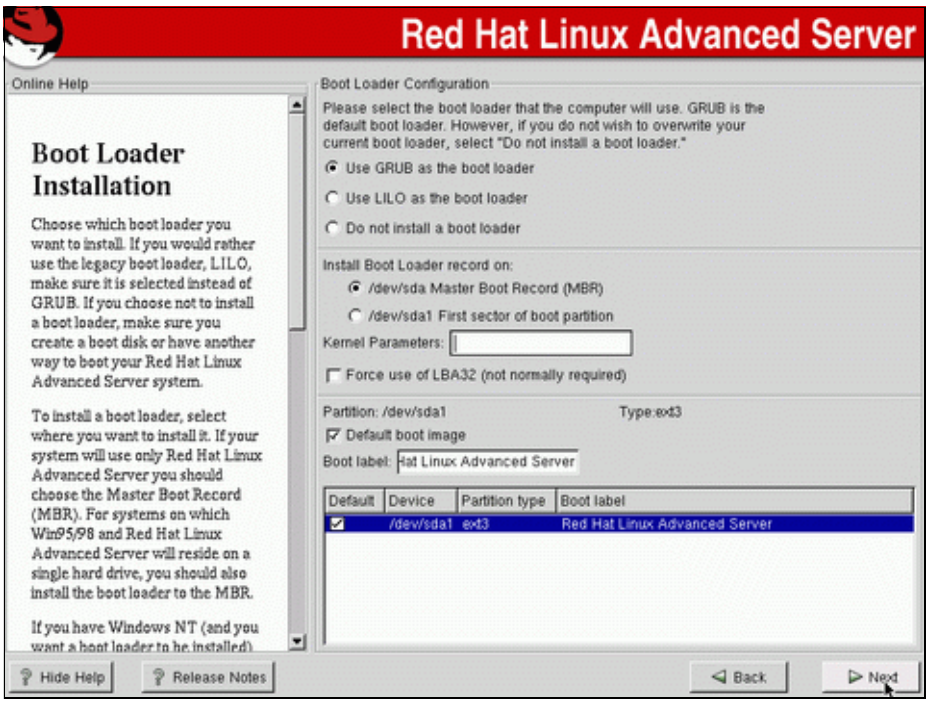


Figure 4-17 Red Hat 2.1AS: Boot loader installation

Tip: If you are removing Linux from a machine and re-installing another operating system, first you must clear the Master Boot Record. Otherwise, the system will try to boot Linux, which was just overwritten with the re-installed operating system.

To clear the MBR, first boot up with a Windows 98 diskette, and run the following command:

```
FDISK /MBR
```

Now you can reboot the system and start the installation of your new OS.

20. You can set a password to protect GRUB, as shown in Figure 4-18. We recommend that you set a password to prevent unauthorized changes to the GRUB boot parameters. If the password is too short, a message will be displayed to enter a longer password.

Figure 4-18 Red Hat 2.1AS: GRUB password

21. Figure 4-19 shows the window used to set up networking. Enter the following information:

    a. Deselect **Configure using DHCP**.

    b. Select **Activate on Boot**.

    c. Enter a suitable IP Address, Netmask, Hostname, Gateway, and Domain Name Server. The Network and Broadcast addresses are automatically calculated for you. These are the lowest and highest IP addresses of your IP network. If you have alternate DNS servers, they can be specified in Secondary DNS and Ternary DNS.

    d. Click **Next** to continue.

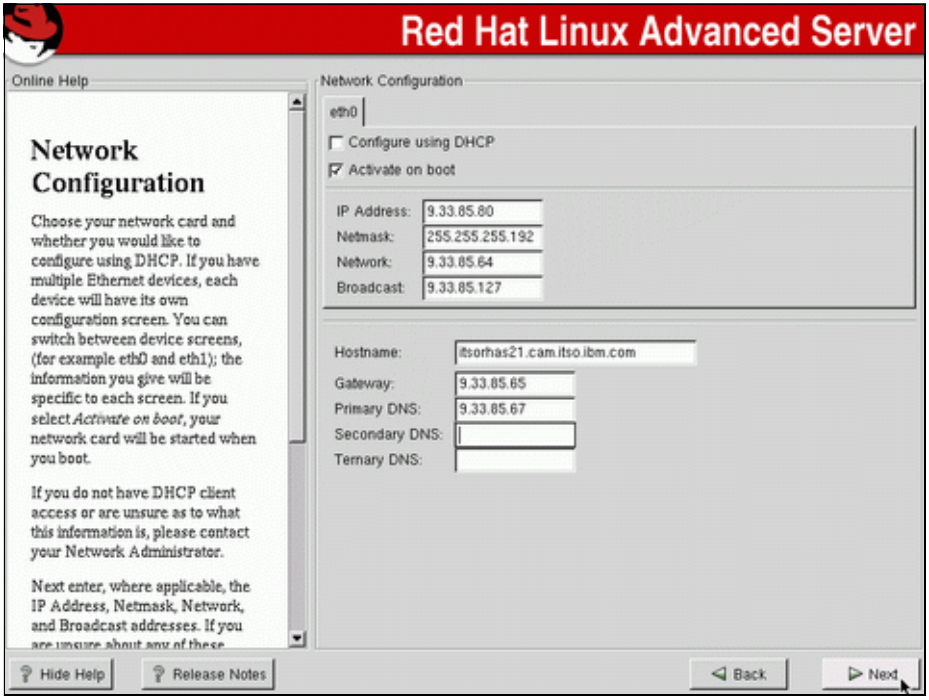


Figure 4-19 Red Hat 2.1AS: Network configuration

22. Red Hat gives you the option to utilize a firewall. Our network has a dedicated firewall, so we chose not to install one on the server. Click **Next** to continue.

> **Note:** For performance reasons the Domino server should not act as a firewall.

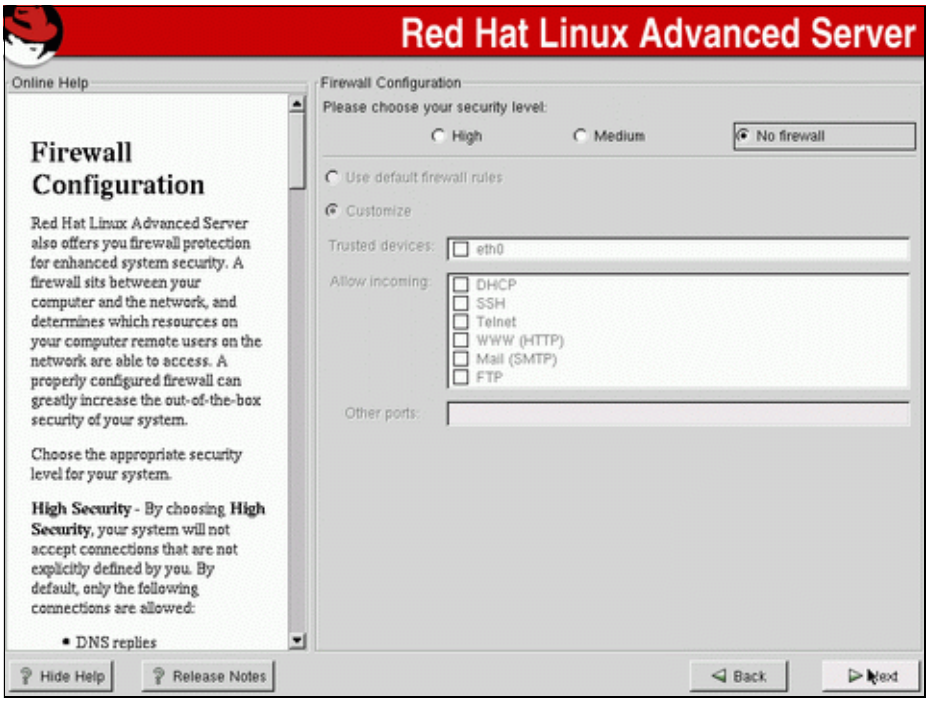


Figure 4-20 Red Hat 2.1AS: Firewall configuration

23. Select the default language, and any additional languages, that will be used on your Red Hat system after installation.

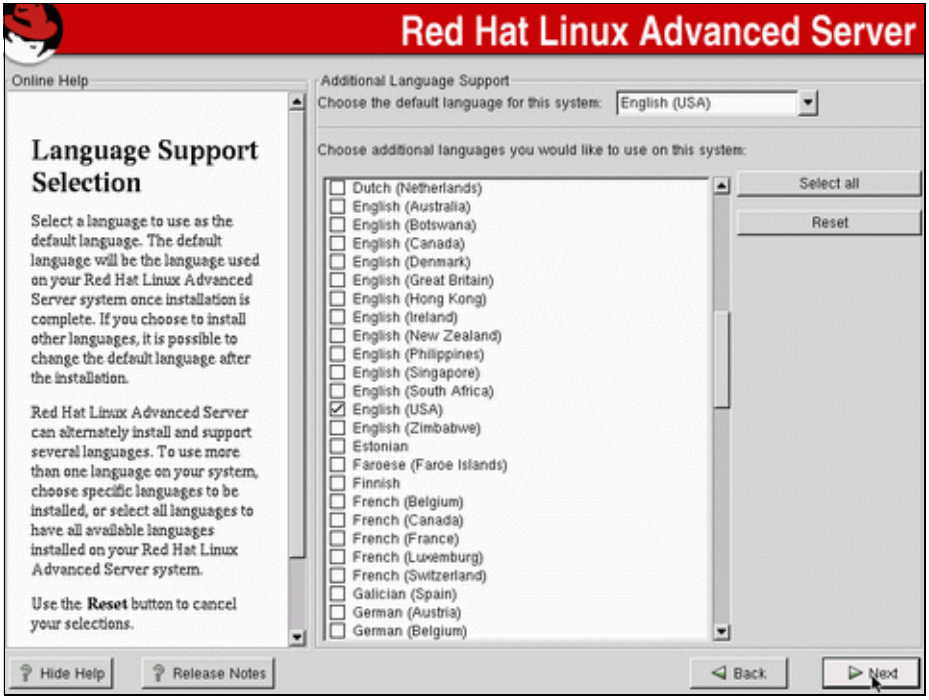


Figure 4-21 Red Hat 2.1AS: Language support selection

24. The Time Zone Selection window is displayed as shown in Figure 4-22. Set the correct time zone for your installation. Be sure to choose the correct hardware clock setting for your system. If your PC's clock is set to UTC or GMT, select **System clock uses UTC**. Change the view of the map by selecting your area from the **View** drop-down list. Select your time zone by clicking on a specific city. Click **Next** when you have made your selections.

> **Tip:** For countries with Daylight Saving, we recommend that you set the BIOS clock to GMT and select **System clock uses UTC**.

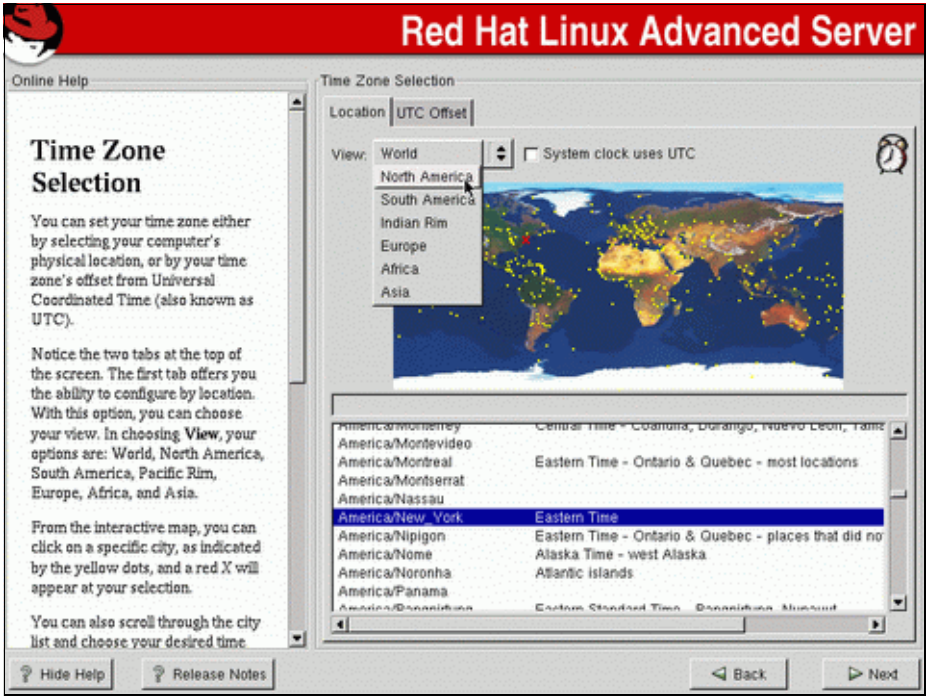


Figure 4-22 Red Hat 2.1AS: Time zone selection

25. Enter the password you want to set for the root user. The root user is also known as the *Super User*, and is equivalent to the NT Administrator account. This account has full control over the system.

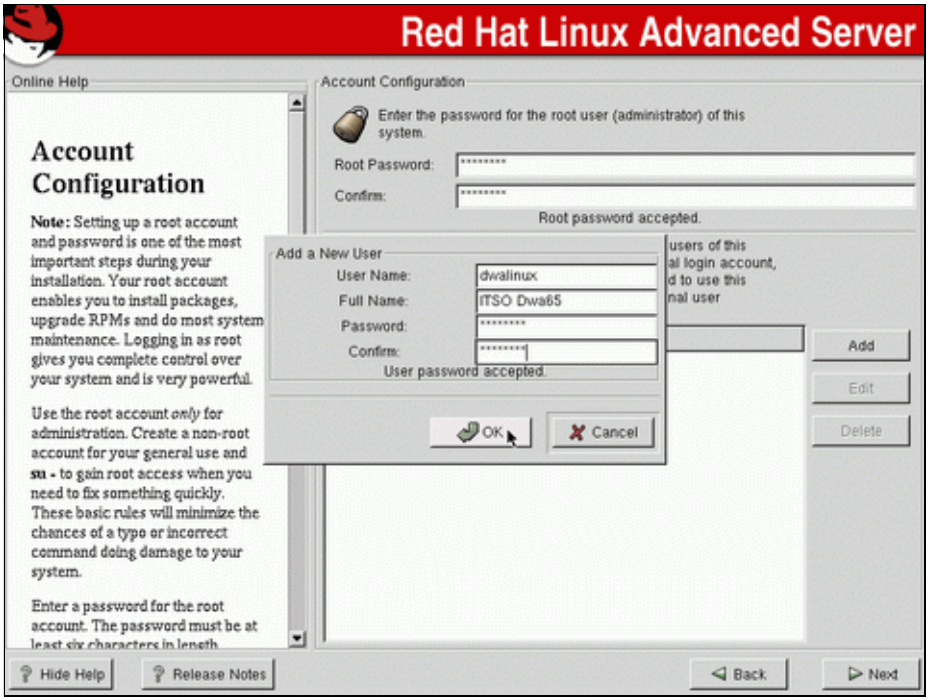


Figure 4-23 Red Hat 2.1AS: Root password and Notes account creation

You should add at least one user to the system to proceed, so you might as well add the Notes account now. When the root password has been accepted, click **Add** to add a new user to the system, as shown in Figure 4-23. After you enter the requisite information and click **OK**, you can add more users or click **Next** to continue.

26. The Authentication Configuration screen is displayed. Make certain that both **Enable MD5 passwords** and **Enabled shadow passwords** are checked, then click **Next** to continue.

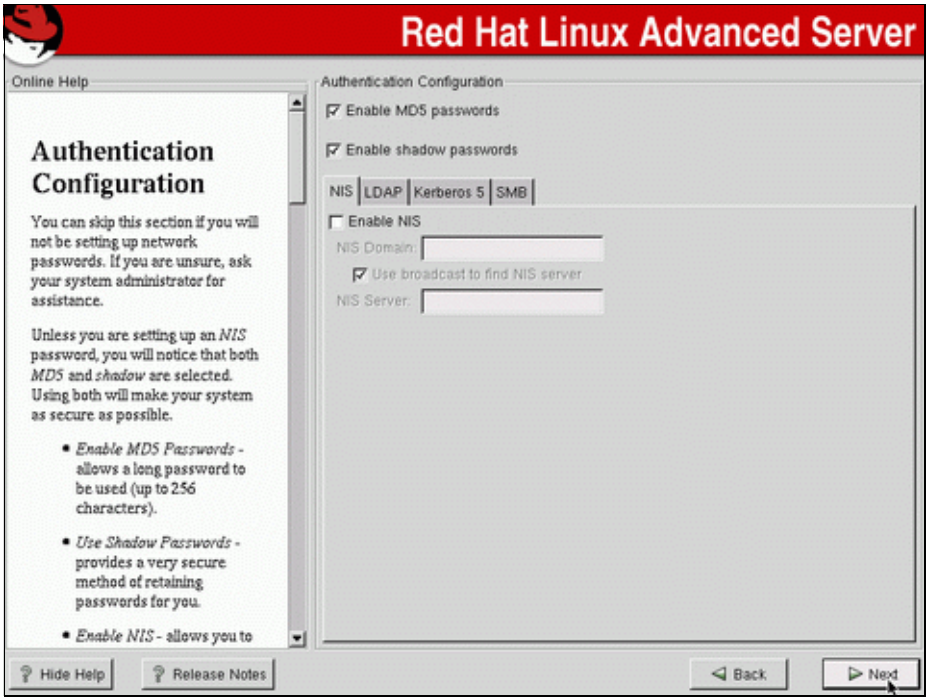


Figure 4-24 Red Hat 2.1AS: Authentication configuration

27. The Package Group Selection screen is displayed. Use the scroll bar on the side of the screen to see more selections. If a box has a check mark, the package is selected for installation. If a box is blank, it will not be installed.

Figure 4-25 Red Hat 2.1AS: Package selection

We recommend that you select the same packages for your installation as we did. If you are going to use Gnome for your graphical user interface (GUI), select KDE only if you want both GUIs available to your administrators. To add other packages, such as Telnet or FTP, check the **Select individual packages** check box shown in Figure 4-25. The packages we selected are:

- **X Window System**: The base X-Window manager
- **KDE**: Graphical user interface
- **Network Support**: Enables TCP/IP networking
- **Utilities**: Various system utilities
- **Software Development**: Various compilers needed for system adjustments
- **Kernel Development**: Useful for several reasons, including enabling you to recompile the kernel to reduce its size by removing unnecessary drivers

Deselect everything else and click **Next** to continue.

28. The Graphical Interface (X) Configuration screen is displayed. The installation will select a card based on the results of its probe; you can override this and select the graphics card that is installed in your machine from the list. If you are uncertain of the specific card installed in your system, *Generic SVGA* will usually work.

    Click **Next** when you are satisfied with the selections.

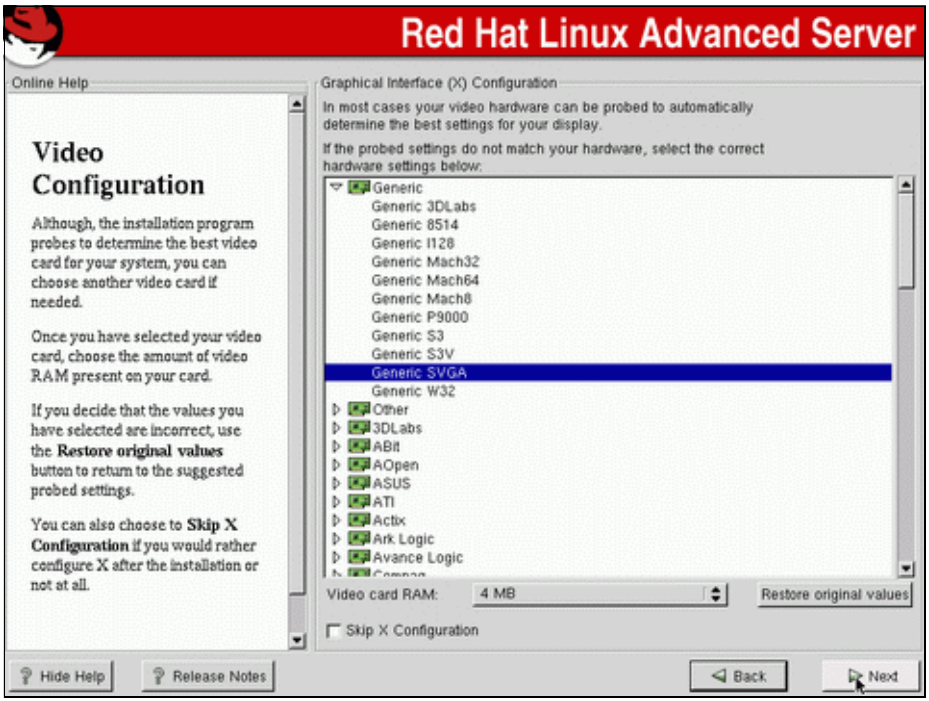


Figure 4-26 Red Hat 2.1AS: Video configuration

29. The install program is now ready to copy the software from the CD-ROM to your hard disk drive (Figure 4-27).

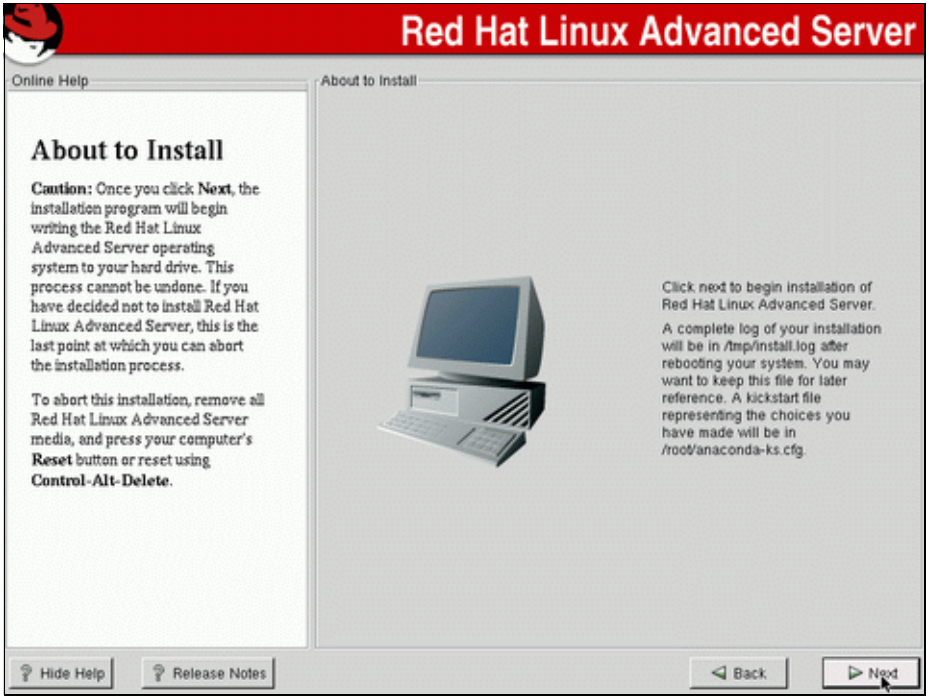


Figure 4-27 Red Hat 2.1AS: About to Install

30. Click **Next** to start the process, which is shown in Figure 4-28. First, the partitions are checked for errors, then they are initialized (formatted). When this is done, the actual installation begins.

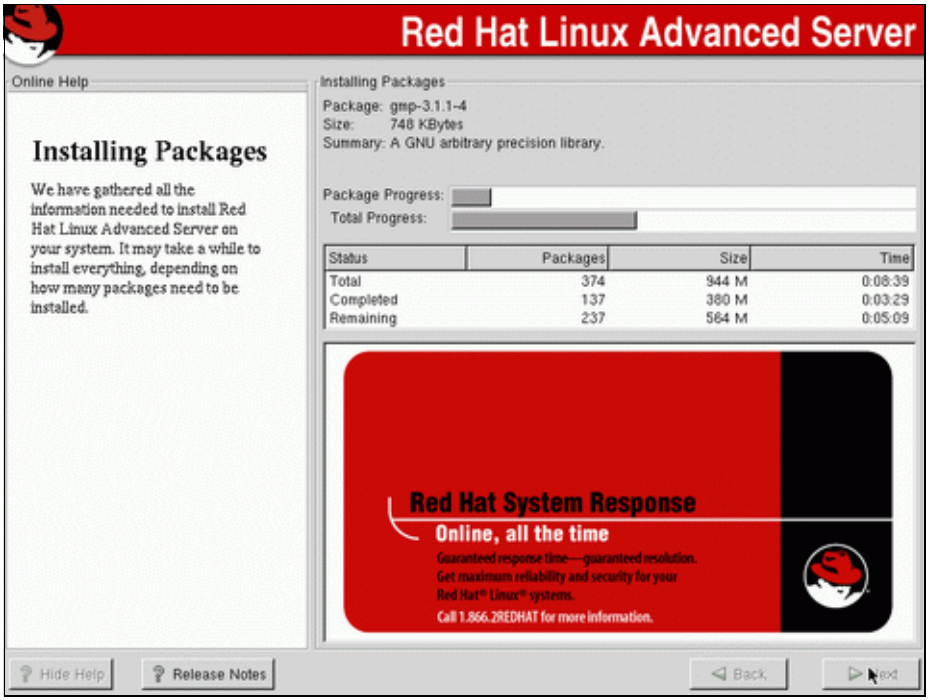


Figure 4-28 Installation of packages

31. After all packages are copied from the first CD, you might be prompted to insert additional CDs depending on the packages selected. When prompted, change CDs and click **Continue**.

> **Note:** If you are installing from DVD you will not have to change the disc.

32. When the installation is complete, you can create a boot disk that will be used to recover your system if it becomes unbootable. We recommend that you create this boot disk and keep it in a safe place.

    Insert a floppy disk that can be overwritten into the floppy drive of your machine and click **Next** to create the boot disk.

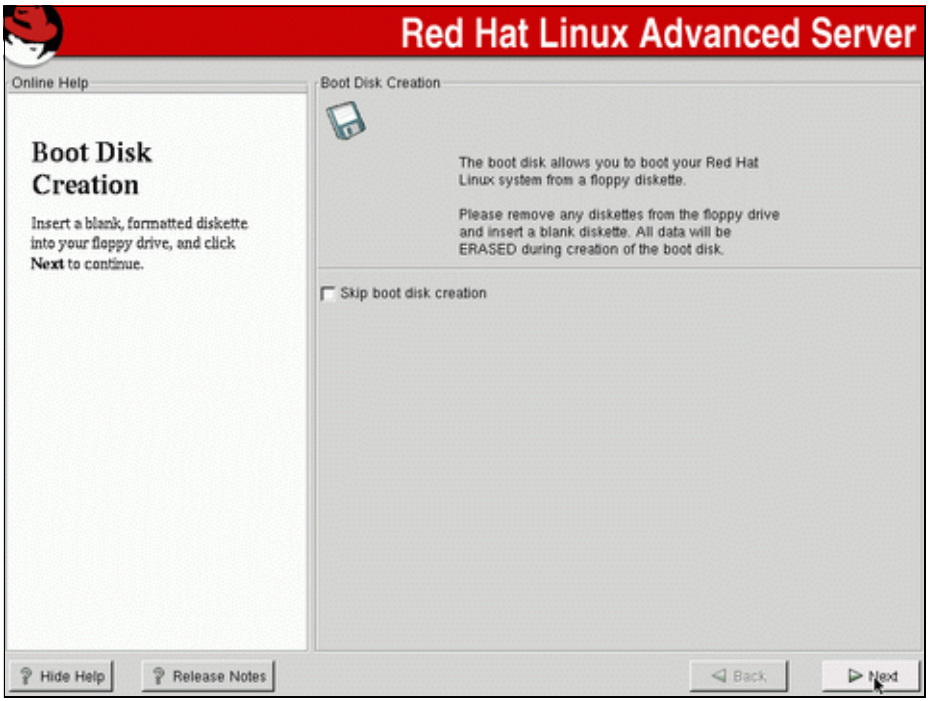


Figure 4-29 Red Hat 2.1AS: Boot disk creation

33. On the Monitor Configuration screen, specify the monitor that is attached to your machine.

    We selected a Generic Monitor with a 1024x768 resolution because it works for most monitors. If your monitor is not listed and you know its capabilities, specify the Horizontal and Vertical refresh rates that your monitor supports. Click **Next** to continue.

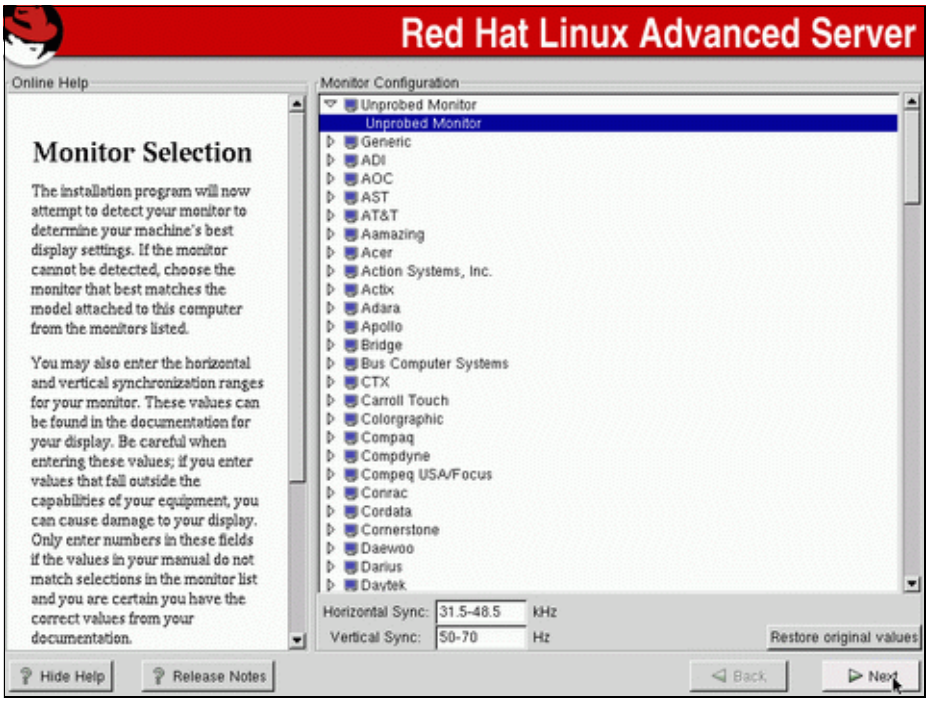


Figure 4-30 Red Hat 2.1AS: Monitor selection

34. On the Customize Graphics Configuration screen (Figure 4-31), you can select the color depth, screen resolution, desktop environment, and login type. We recommend that you run a graphical login, using the KDE desktop with 1024x768 screen resolution.

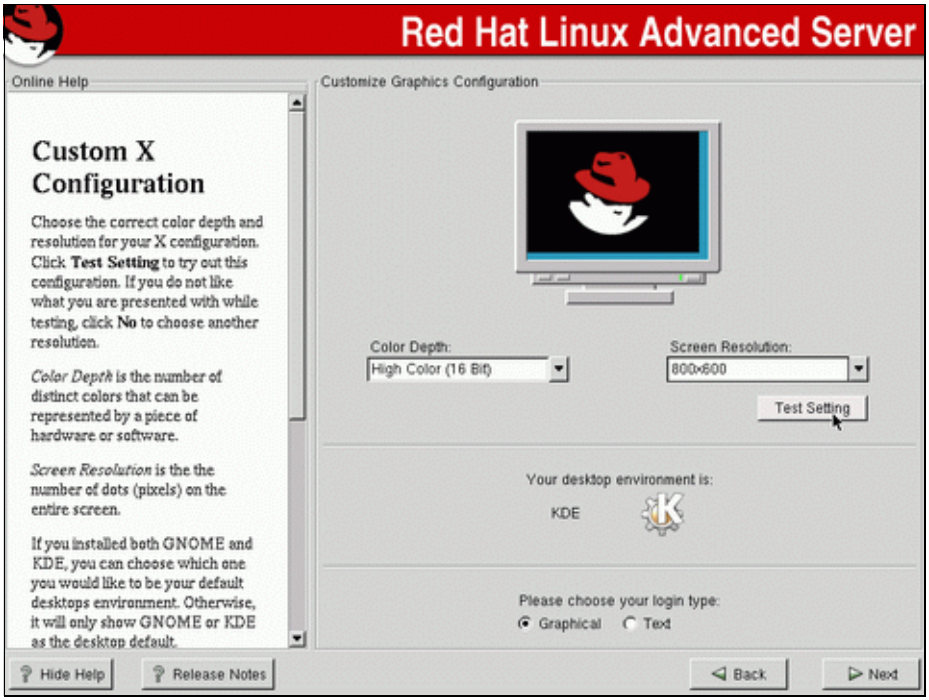


Figure 4-31 Red Hat 2.1AS: Custom X configuration

After you have made your selections, click **Test Setting** to ensure that your system will function when you reboot.

When the screen displays correctly, click **Next** to accept your settings.

35. When the window shown in Figure 4-32 is displayed, the installation of Red Hat 2.1AS is complete. Click **Exit** to restart the system.

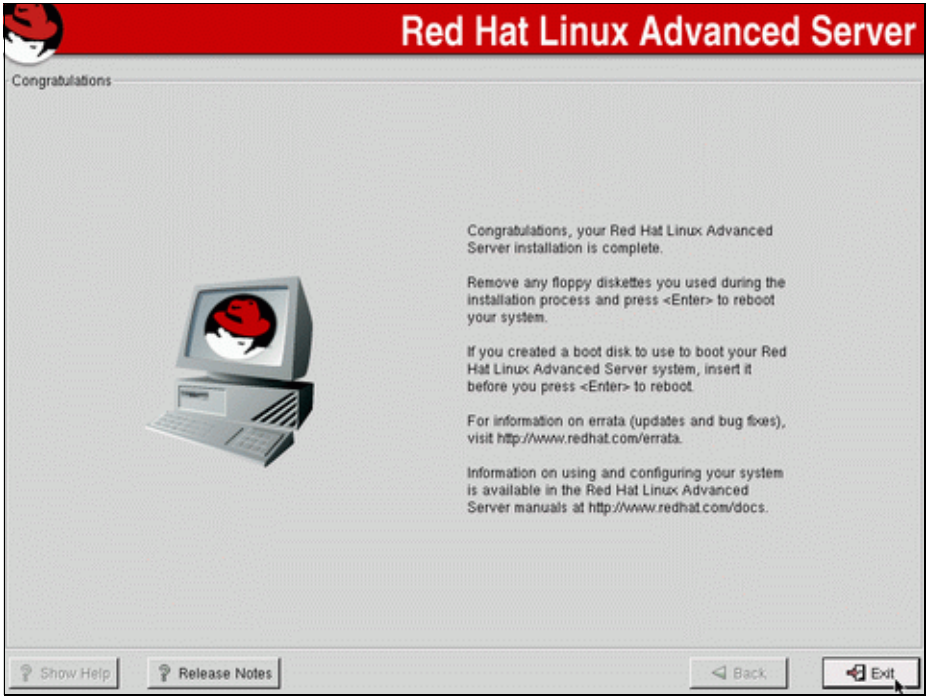


Figure 4-32 Red Hat 2.1AS: Installation complete screen

This completes the Red Hat 2.1AS installation process.

If you would like to view the KDE logon process, look at step 39 on page 152 because KDE is very similar for both Red Hat 2.1AS and UnitedLinux 1.0.

4.3 Installing UnitedLinux 1.0, SLES 8

In this section, we show you how to install UnitedLinux 1.0 on your server. Note that for SUSE LINUX Enterprise Server 8, there are many parallels in the installation process.

Note: We recommend using SUSE LINUX Groupware Server 8 with Lotus Domino or later instead of the UnitedLinux 1.0 Personal or UnitedLinux 1.0 Professional version. SUSE LINUX Groupware Server contains SUSE Enterprise Server 8 and Lotus Domino Server. The SUSE Enterprise Server version has an extended release cycle and has been certified by the top ISVs, such as IBM. The installation of the SUSE Groupware Server is similar to the installation of the SUSE Professional version, which we detail here.

To capture the screens you see in this book, we installed and configured Linux in a VMware window. VMware enables you to run one operating system as a guest of another. This means that some of the screens might look sightly different from what you would see on your system. These differences are hardware-related, as VMware emulates different hardware devices for the guest operating system.

Additional information about VMware is available at:

`http://www.vmware.com`

Be sure to read “Before you begin” on page 76 in order to make the installation easier.

To start the installation, insert the UnitedLinux 1.0 CD-ROM/DVD and turn on or reboot the server.

Attention: The installation process destroys any existing data stored on your hard disk drives.

1. When the screen shown in Figure 4-33 is displayed, you are ready to start the Linux installation. Ensure that **F3=640x480** is highlighted and press **Enter** to begin the installation, or wait for it to start automatically after a short pause.

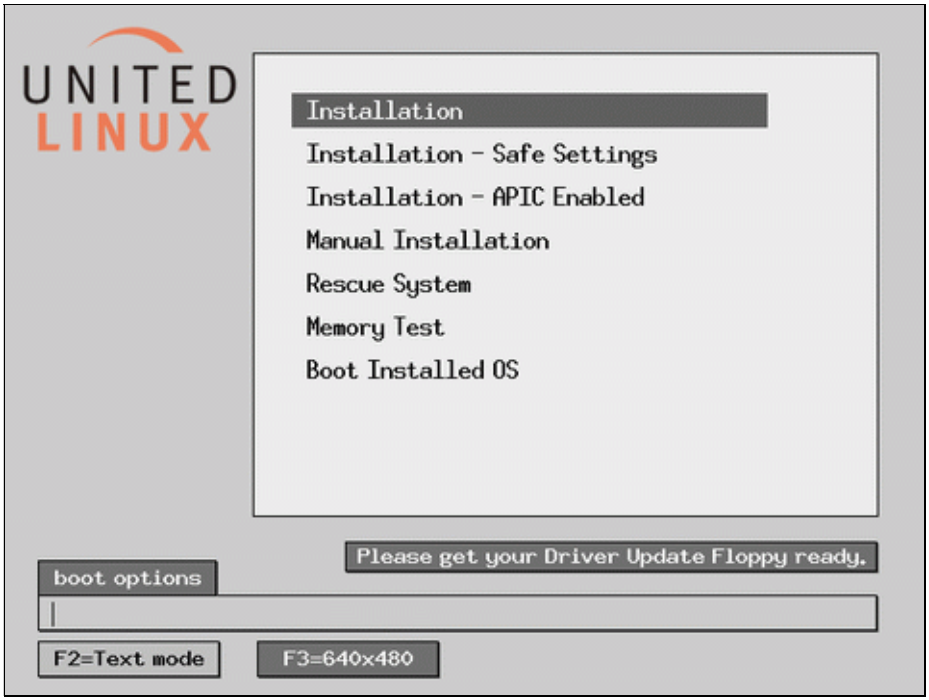


Figure 4-33 UnitedLinux 1.0: Welcome screen

When the kernel is booted and all device drivers are loaded, the SUSE installation process is ready to install the operating system. If the graphical installation fails to start, see the SUSE installation manual.

2. After you have read and accepted the license shown in Figure 4-34, click **Accept**.

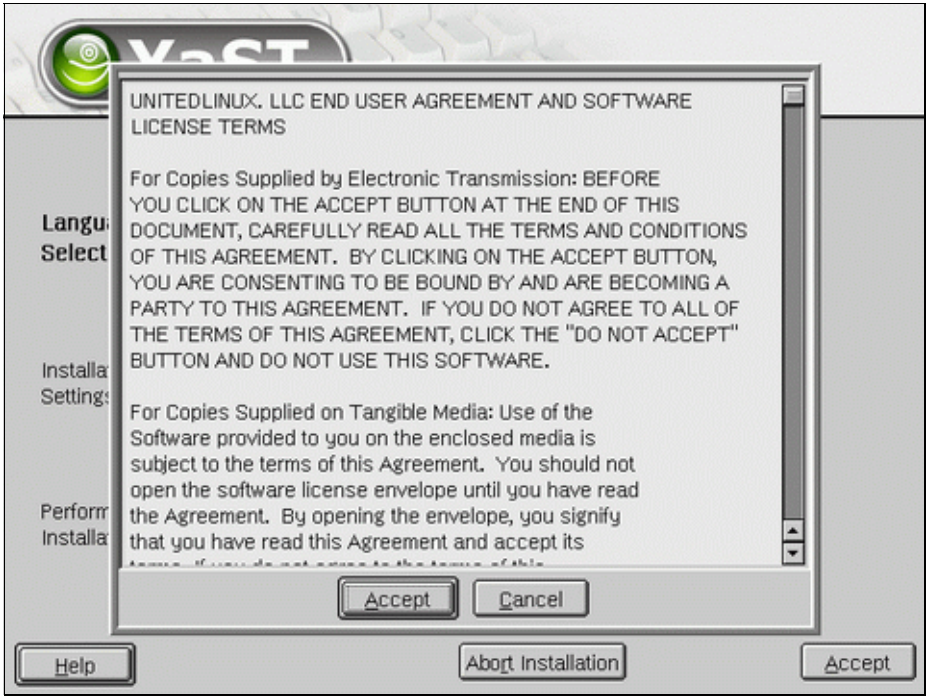


Figure 4-34 UnitedLinux user agreement

3. As shown in Figure 4-35, you can select the language you would like to use on your system. Specify the appropriate language and click **Accept**.

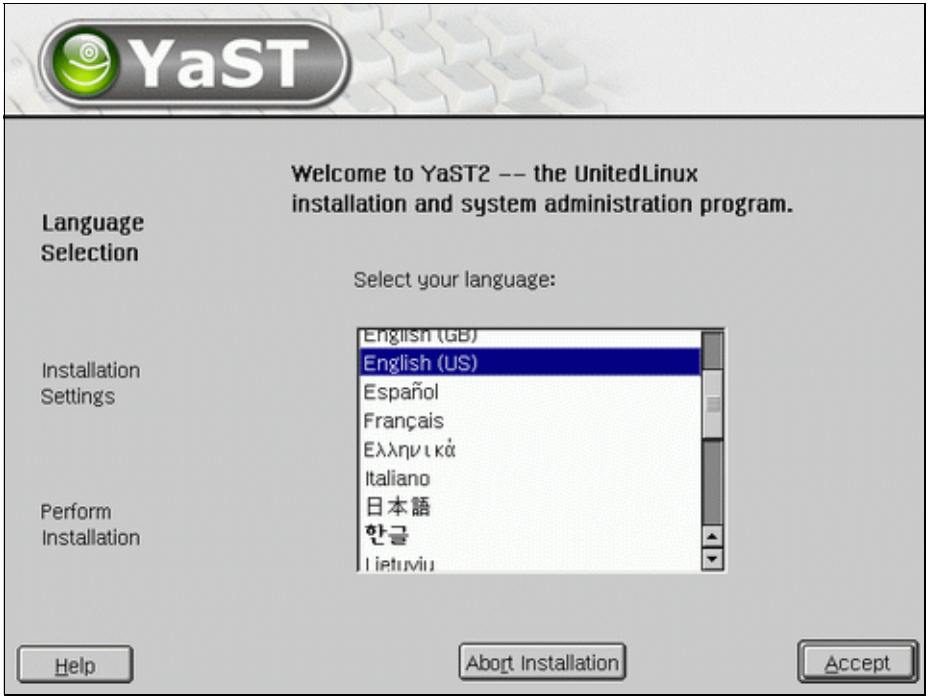


Figure 4-35 UnitedLinux 1.0: Language selection

4. The system begins to probe (detect) the hardware installed in your system and load the appropriate drivers for it. While this is happening, the screen shown in Figure 4-36 is displayed.

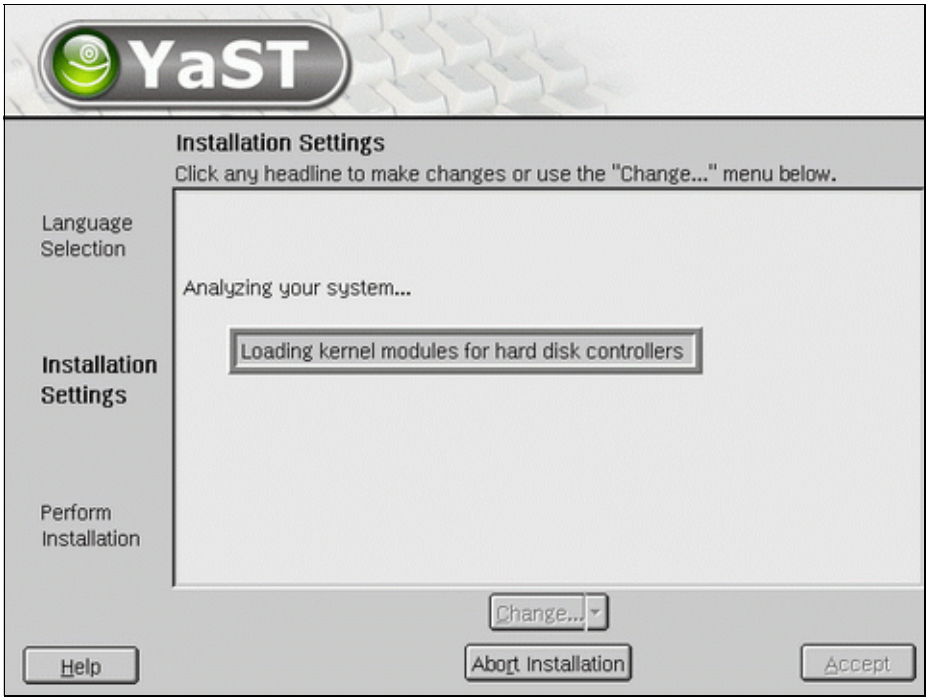


Figure 4-36 UnitedLinux 1.0: Analyzing system

Note: Some disk controllers require drivers supplied by the manufacturer and are not supported out of the box. Visit `http://sdb.suse.de/en/sdb/html/` for more information about installing disk drivers.

5. When all hardware has been detected, the window shown in Figure 4-37 appears. You need to change the partitioning scheme because the installer's automatic settings do not provide an optimal partitioning scheme. Click **Partitioning** to change the partition configuration.

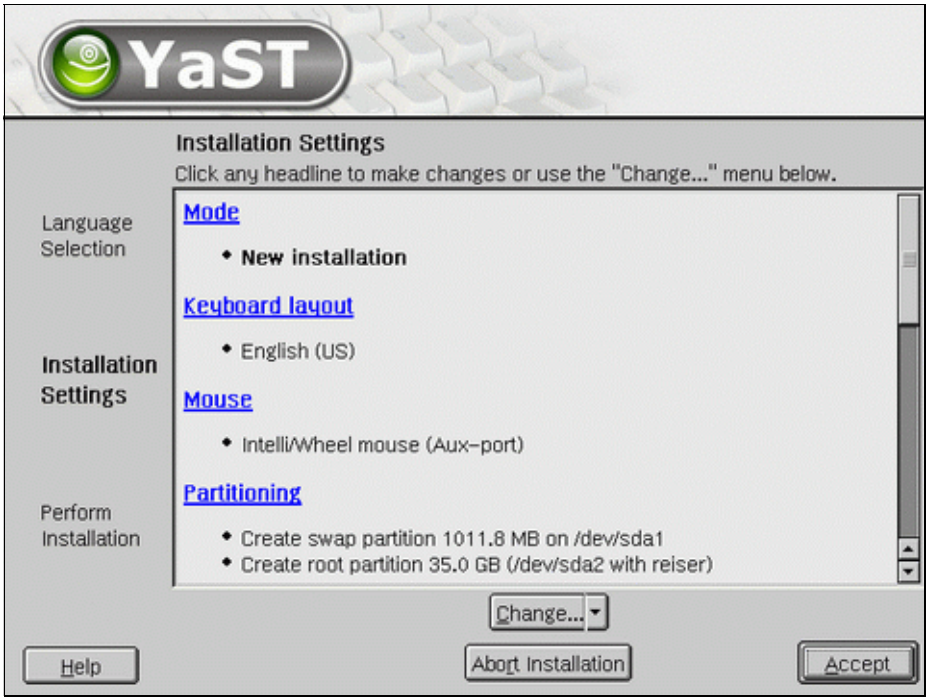


Figure 4-37 UnitedLinux 1.0: Default installation settings

6. Select **Modify** and click **Next** to change the partition configuration.

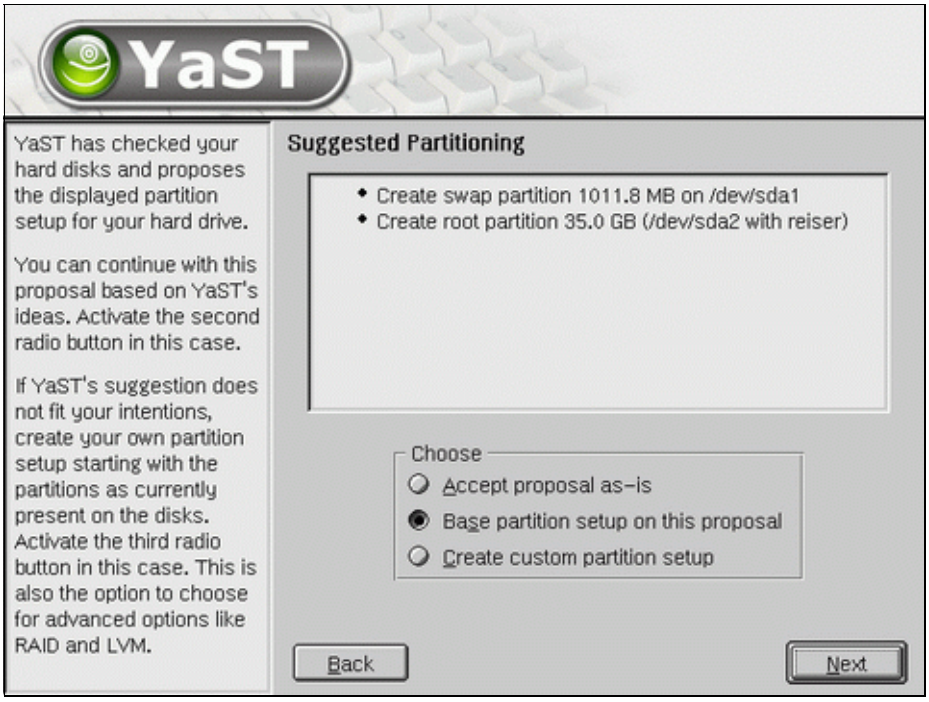


Figure 4-38 UnitedLinux 1.0: Partitioning

Important: You can have only four primary partitions for each hard disk drive. If you need to create more than four partitions, create three *primary* partitions and one *extended* partition that uses all of the remaining disk space. You can then create all subsequent partitions in this extended partition.

7. You see the disks installed in your system and the current partitioning structure. (See 4.1.3, “Partitions” on page 78 for the recommended partitions and their respective sizes.)

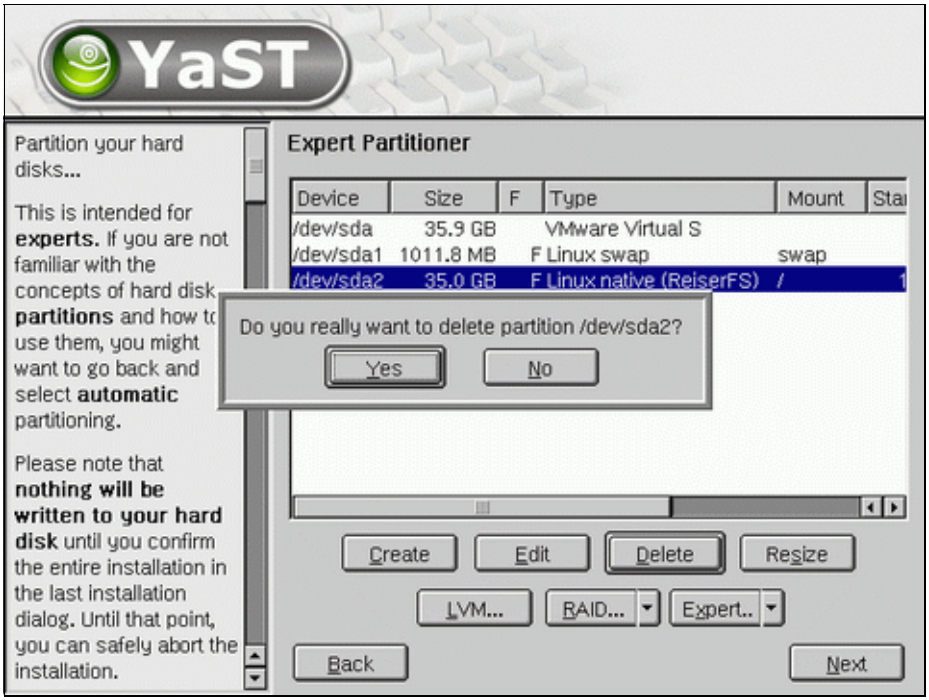


Figure 4-39 UnitedLinux 1.0: Default partitions

There are two ways to change from the SUSE-selected structure to the structure used in this book. Select the partition and click **Delete** to remove it, or **Edit** to change its settings. If the default setup is close enough to your desired partition, it may be easier to edit the options. In these instructions, we describe how to delete all partitions and then set each one up.

First, delete the root partition that the Installer has created by selecting it and clicking **Delete**. Click **Yes** to confirm that you want to delete the partition.

8. Figure 4-40 shows the option to create a Primary or Extended partition. For the root partition, select **Primary** and click **OK**.

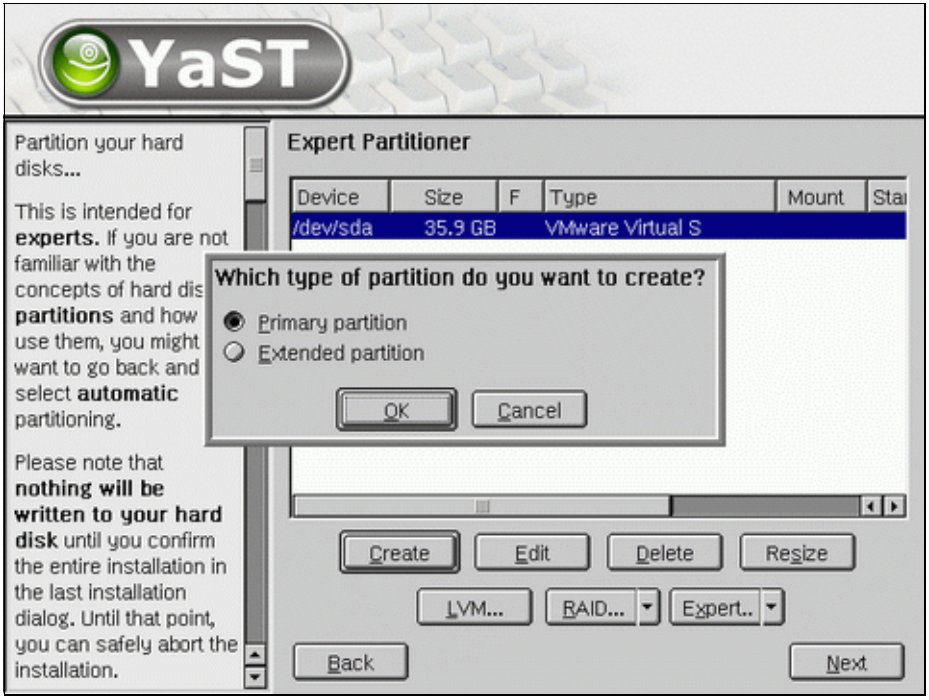


Figure 4-40 UnitedLinux 1.0: Primary partition

9. Select **Format**, then change the File system to **Ext3**.

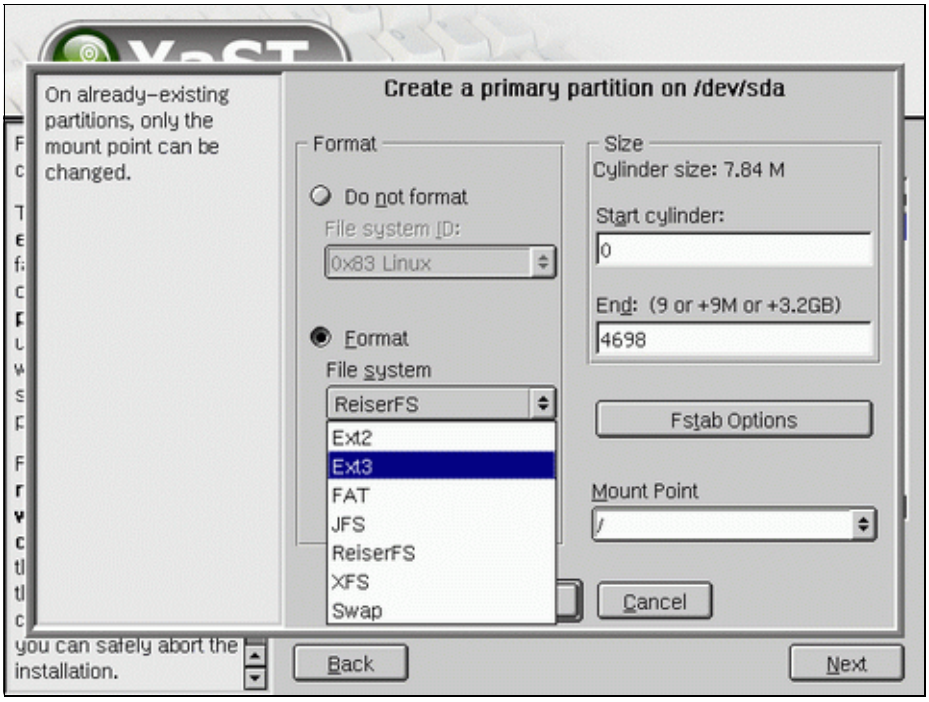


Figure 4-41 UnitedLinux 1.0: Creation of / root partition

10. In the Size section, enter the size of the partition. The default is to specify the start and end cylinders of the partition, but an easier method is to specify the size in megabytes or gigabytes by entering a plus sign, the size, and M or GB in the End field.

    After you specify the size (we chose 3 GB based on a 4 GB drive) and the correct Mount Point (the default is /, which is correct for this partition), click **OK**.

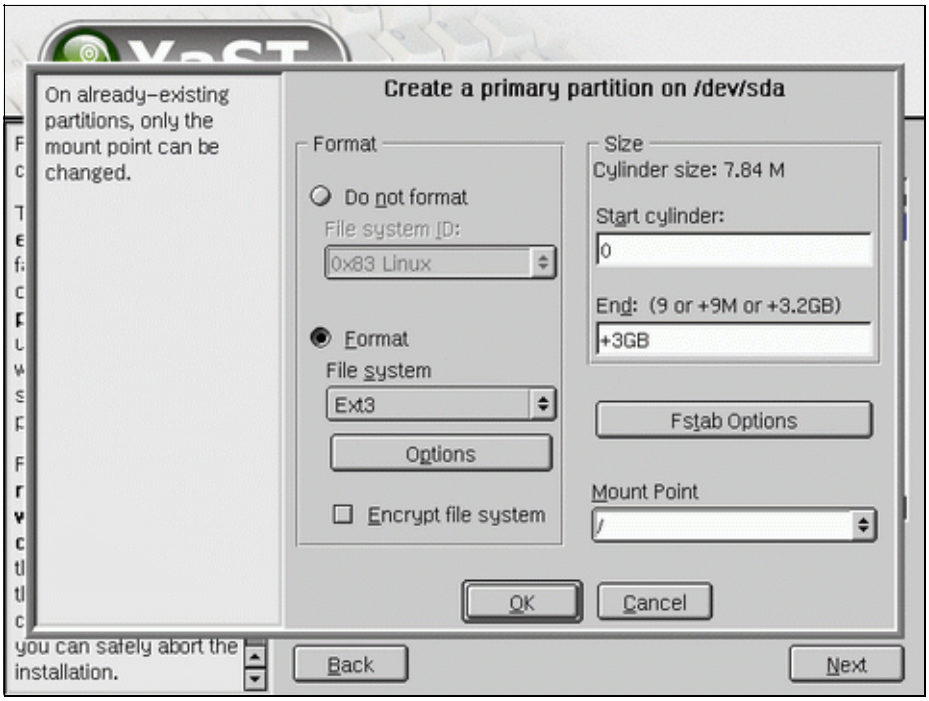


Figure 4-42 UnitedLinux 1.0: Entering the size of the partition

11. Next, create the swap partition. Click **Create** and select the array as you did in step 8 on page 123, then select **Primary**.

    Select **Format**, then change the File system to **Swap**.

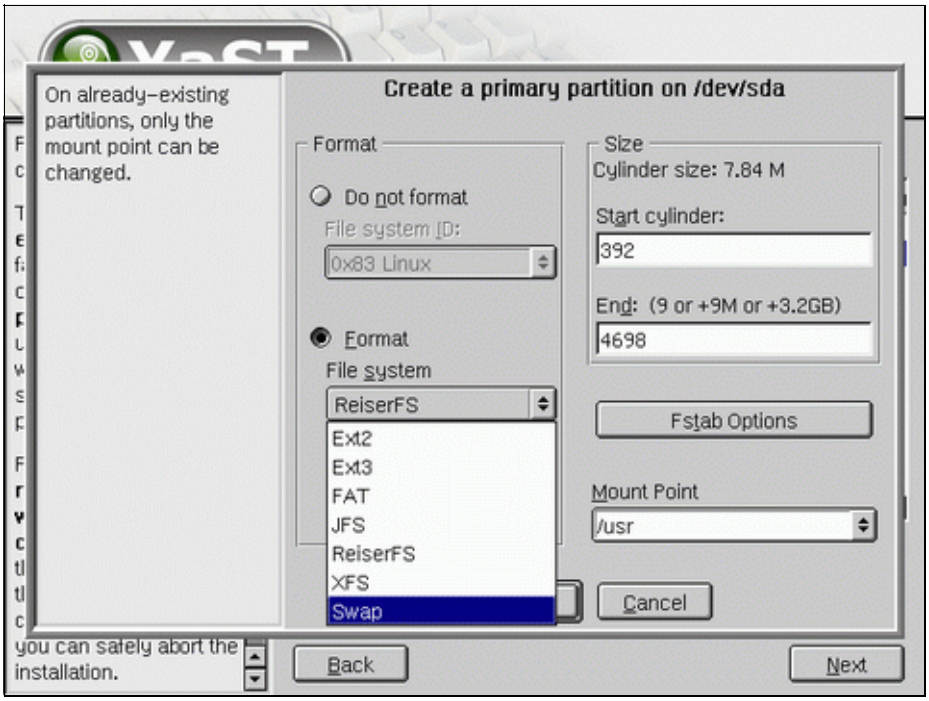


Figure 4-43 UnitedLinux 1.0: Changing to Swap for the file system

12. Enter the size of the swap partition. The installation automatically calculates the start cylinder based on your previous selections, so you do not need to change this value. Click **OK** to create the swap partition.

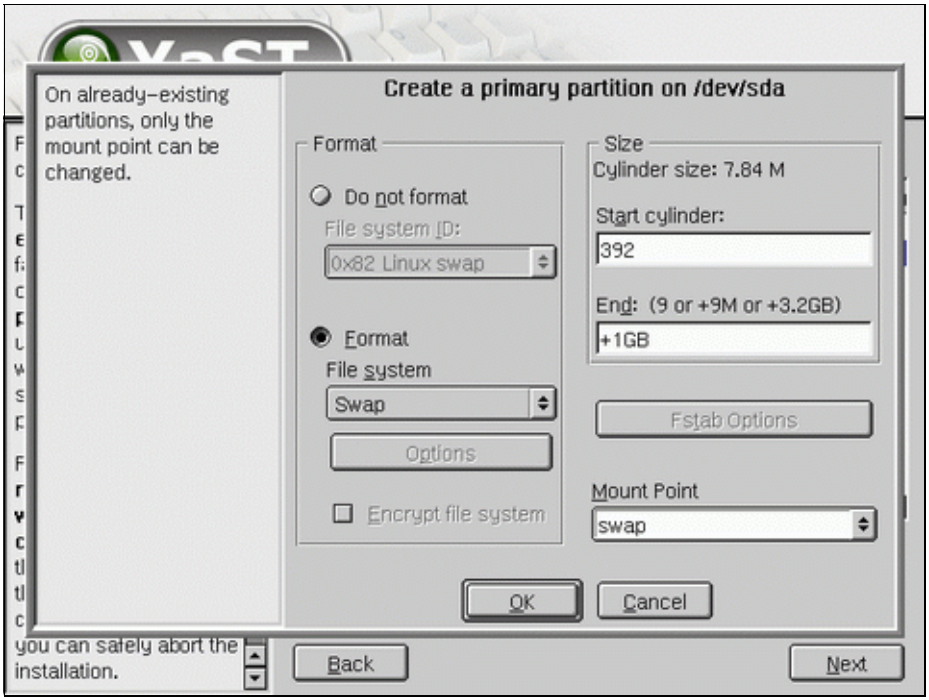


Figure 4-44 UnitedLinux 1.0: Entering the swap size

13. Click **Create**, then select **Extended partition**. You can have up to four partitions per hard disk drive or array, so you could opt to create /var as a primary partition. We chose to create it as an extended partition to demonstrate how to do so. If you would like more traditional UNIX-style partitioning, then you would use an extended partition to enable you to create the additional partitions.

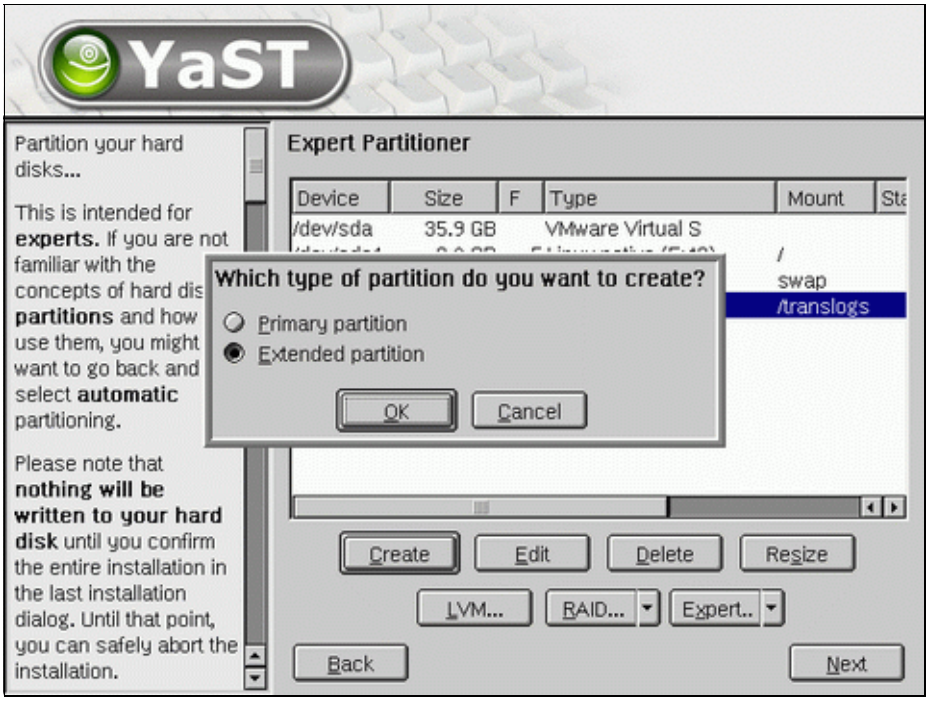


Figure 4-45 UnitedLinux 1.0: Choosing a disk for the /var partition

14. You can accept the default value to use the remaining space. If you enter a value larger than the remaining space, SUSE will automatically reduce it to fit.

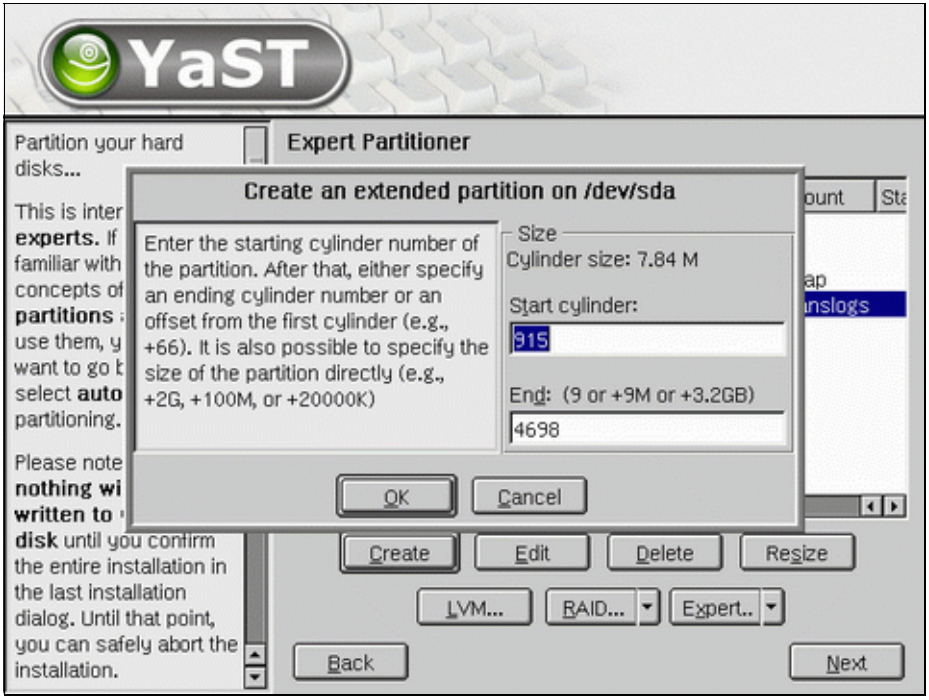


Figure 4-46 UnitedLinux 1.0: Assigning remaining space to extended partition

15. Click **Format**, select **Ext3** from the File system pull-down list, and leave the default value in the End field to use all remaining disk space. Select **/var** from the Mount Point pull-down list. Click **OK** to continue.

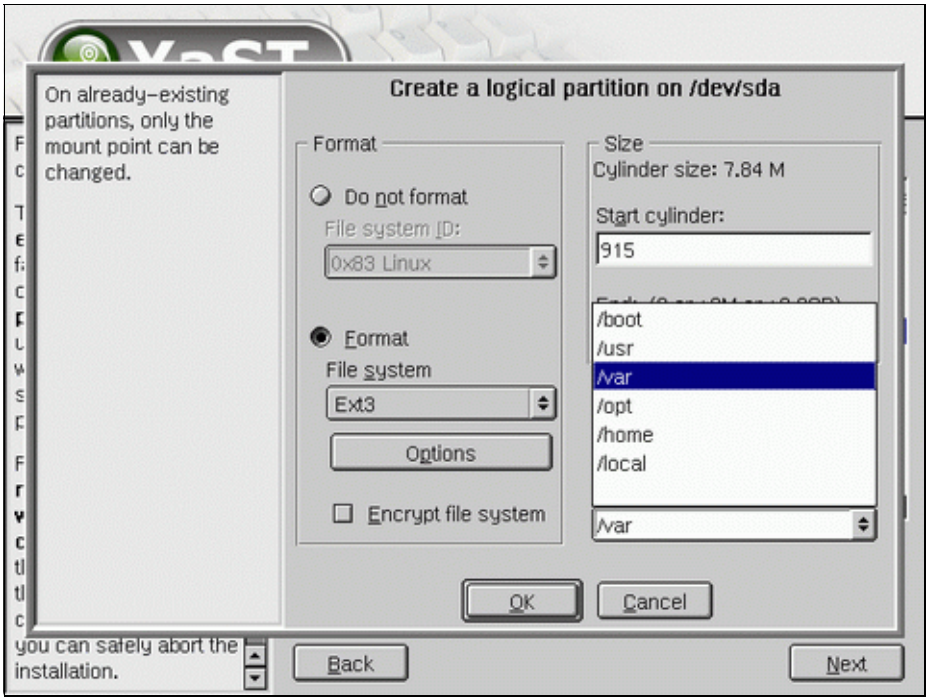


Figure 4-47 UnitedLinux 1.0: Selecting /var as the mount point

16. Click **Create** and select the next available array (sdb for our installation), then select **Primary**. (This is the same procedure described in steps 7 on page 122 and 8 on page 123.)

17. Next, fill in the necessary information. Click **Format**, select **Ext3** from the File system pull-down list, use all of the disk space (which is the default), and type `/translogs` in the Mount Point field. This creates a partition specifically for the Domino Transaction Logs. Click **OK** to continue.

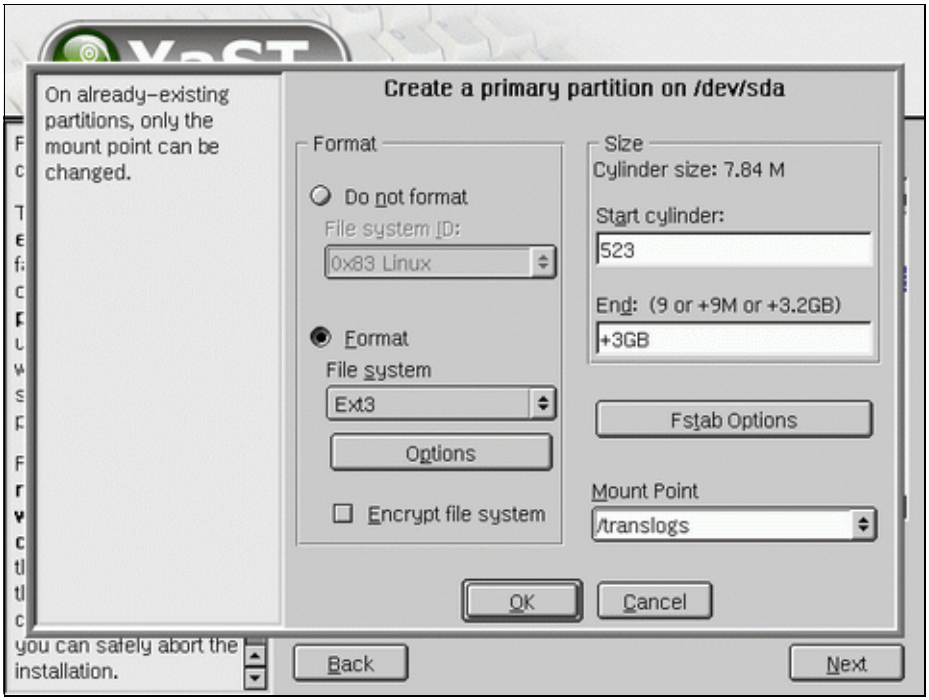


Figure 4-48 UnitedLinux 1.0: Creation of the transaction logs

18. Click **Create** and select the next available array (sdc for our installation), then select **Primary**. (This is the same procedure described in steps 7 on page 122 and 8 on page 123, and also in step 16 on page 130.)

    Again, complete the necessary information. Click **Format**, select **Ext3** from the File system drop-down list, use all disk space (which is the default), and type `/local` in the Mount Point field. This will create a partition specifically for your Domino data. Click **OK** to continue.

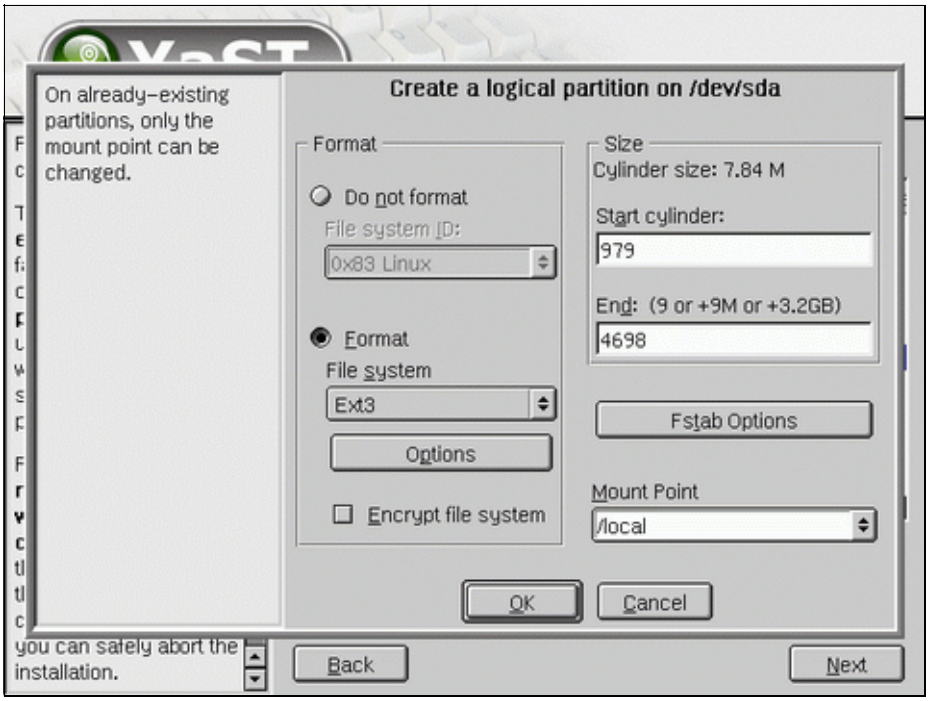


Figure 4-49 UnitedLinux 1.0: Creation of the /local partition

19. Figure 4-50 shows the final partition list. Click **Next** to continue. The partitions will not be written to disk until you reach the end of the setup.

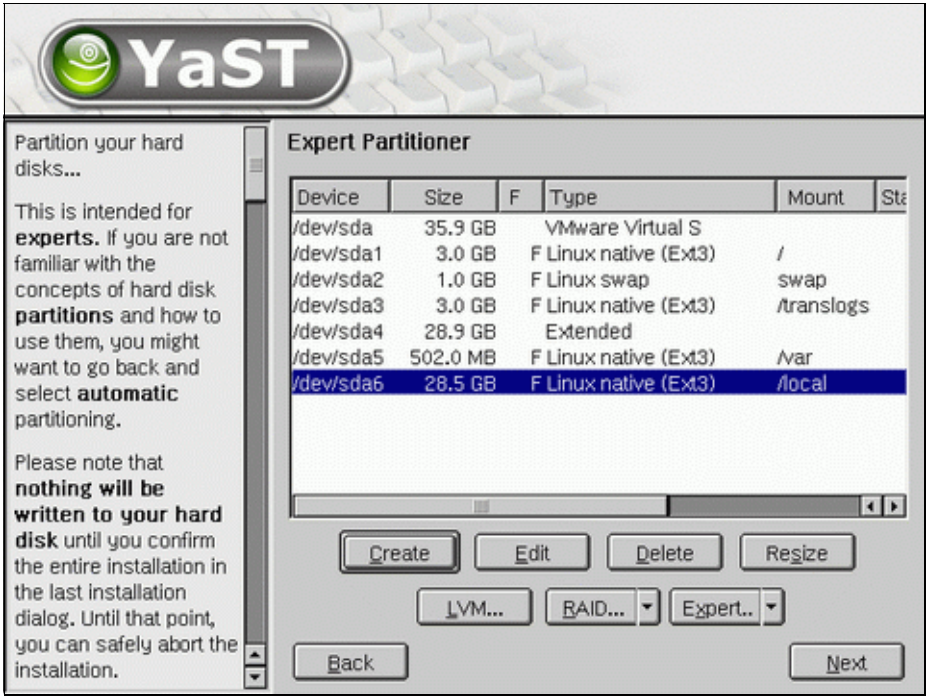


Figure 4-50 UnitedLinux 1.0: Final partition list

20. Select **Default System**, and click **Detailed Selection** as shown in Figure 4-51.

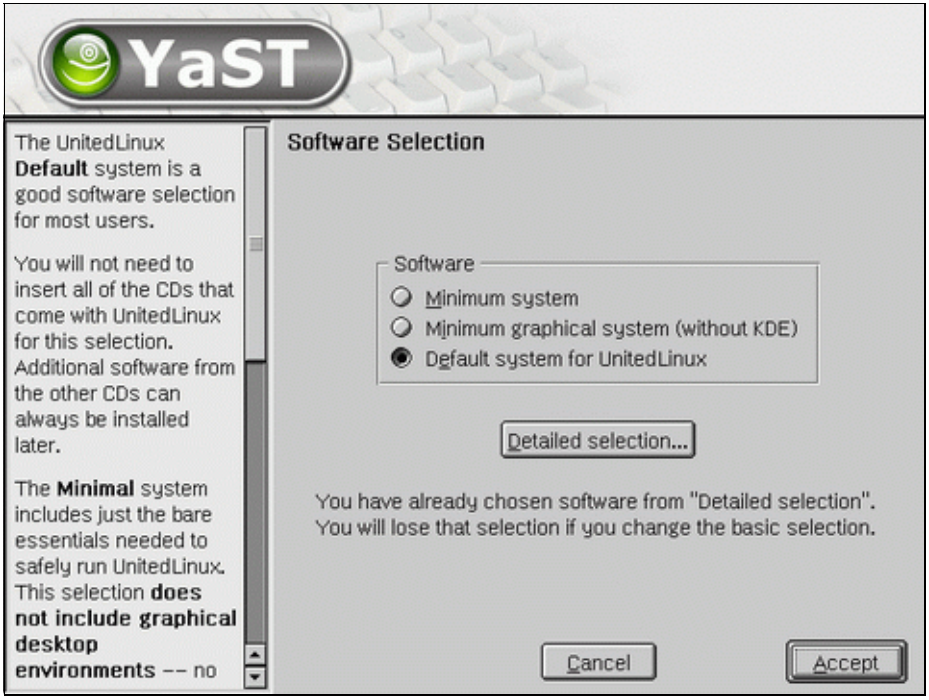


Figure 4-51 UnitedLinux 1.0: Software selection

21. Figure 4-52 shows the screen used to make your detailed software selections. If a box has a check mark, the package is selected for installation; if it is blank, it will not be installed. We recommend that you select the same packages for your installation as we did. The software we selected is:
    - LSB Runtime Environment
    - Graphical Base System
    - KDE Desktop Environment
    - Analyzing Tools
    - File & Print Server

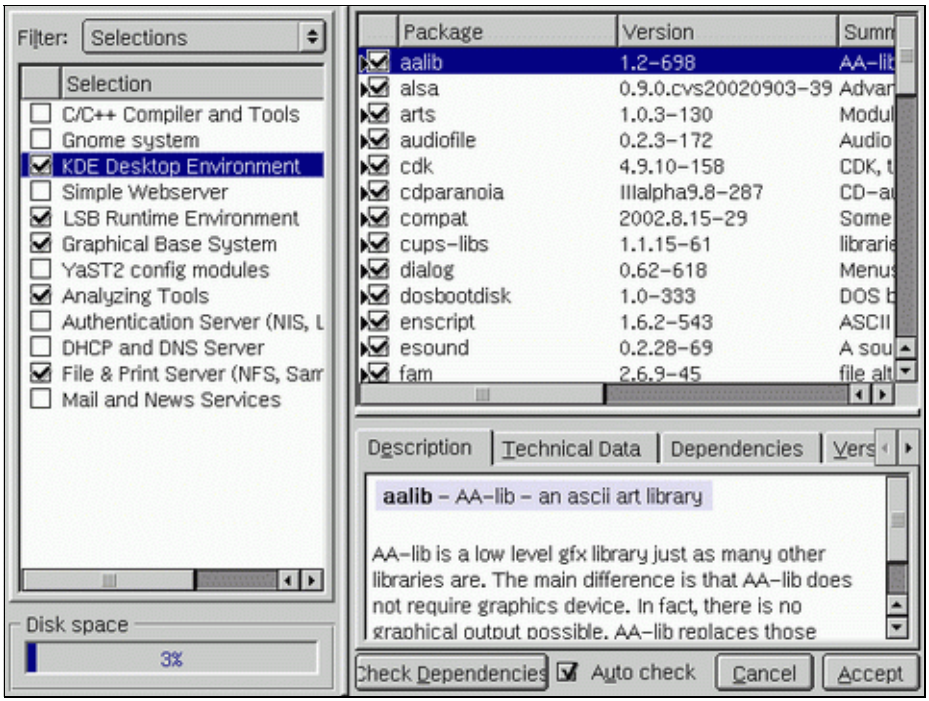


Figure 4-52 UnitedLinux 1.0: Detailed software selection

22. Use the scroll bar on the side to scroll through the installation settings. Click **Time Zone** to change your time zone settings.

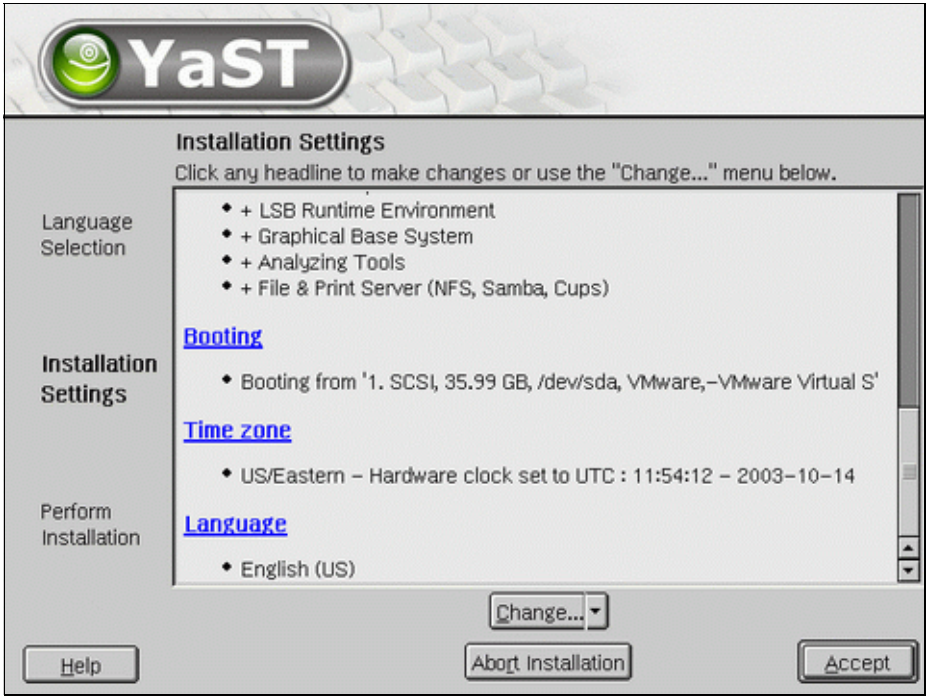


Figure 4-53 UnitedLinux 1.0: Time zone

23. Use the scroll bar to scroll through the Time Zone list. Click your time zone and ensure that you have selected the correct Hardware clock setting. Click **Accept** to return to the Installation Settings screen.

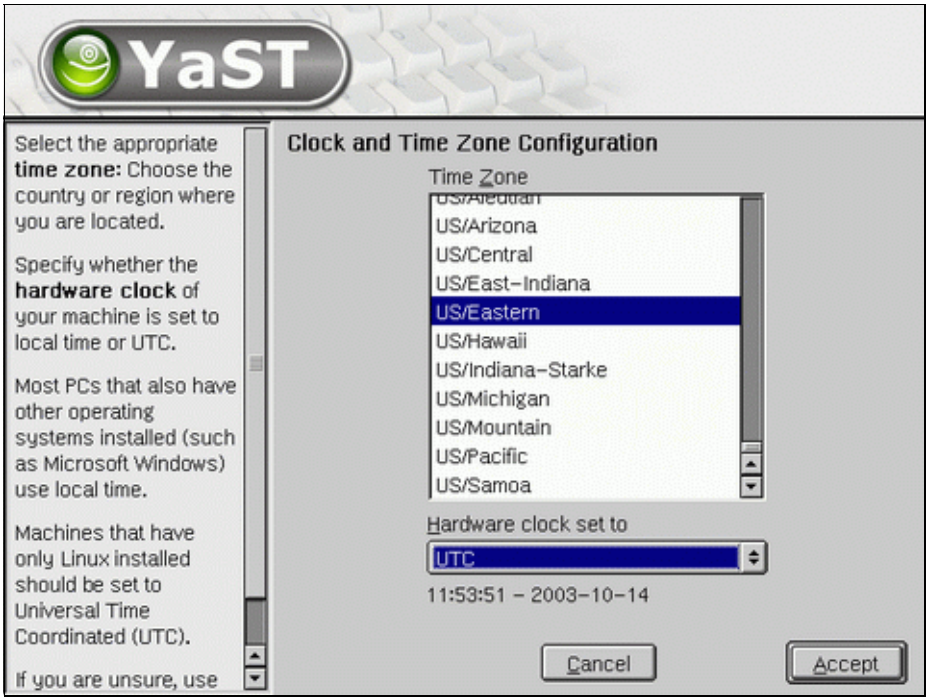


Figure 4-54 UnitedLinux 1.0: Time Zone selection

Tip: For countries with Daylight Saving Time, we recommend that you set the BIOS clock to GMT and select **Hardware clock set to UTC (GMT)**.

24. When all of the settings are correct, you can proceed with the installation. Click **Accept** to start the install.

    You will be prompted to confirm that the installation can be done. Click **Yes** to proceed with the installation as shown in Figure 4-55.

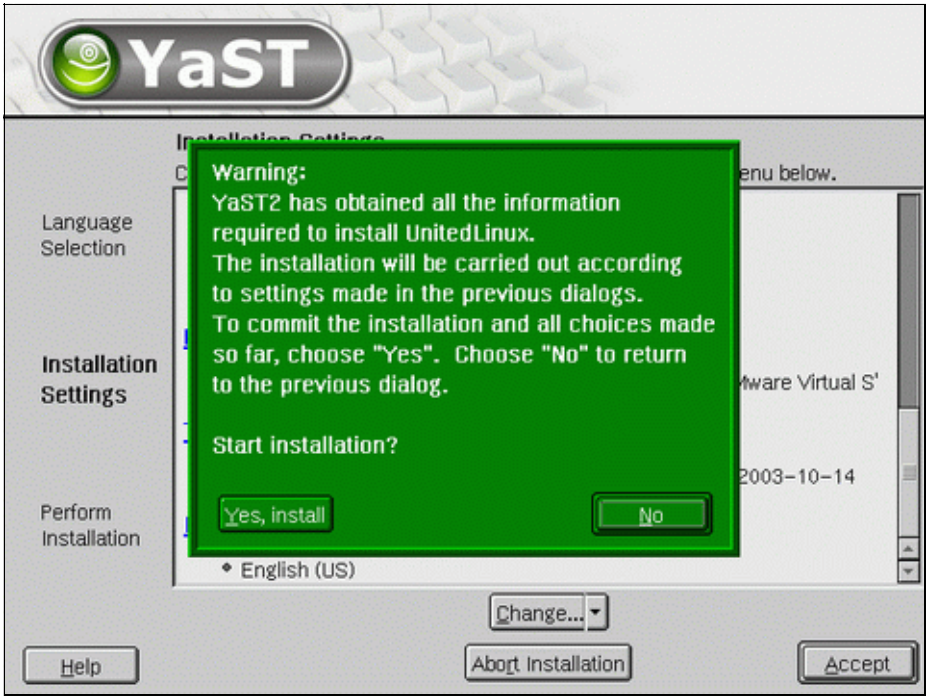


Figure 4-55 UnitedLinux 1.0: Ready to start installation

25. You will see several screens as your partitions are formatted, then the actual installation starts. The package names are displayed as they are installed. As each package installation finishes, a line is added to the Installation Log window shown in Figure 4-56.

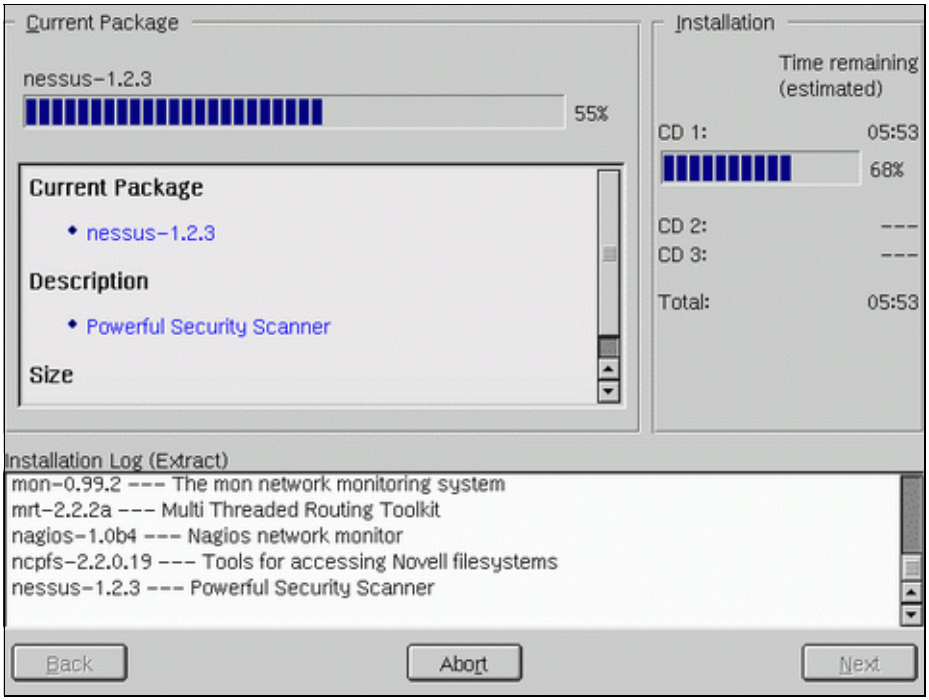


Figure 4-56 UnitedLinux 1.0: Package installation

26. When the basic installation is complete, several tasks are performed. These can be seen in the background of Figure 4-57.

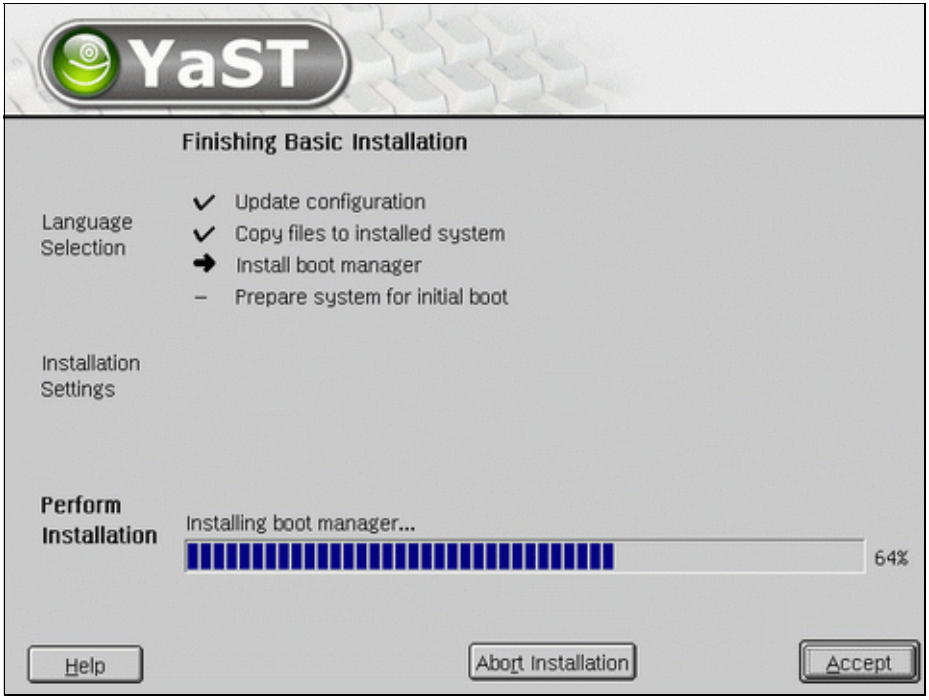


Figure 4-57 UnitedLinux 1.0: Finishing basic installation

27. When the window shown in Figure 4-58 is displayed, the installation of UnitedLinux 1.0 is complete. Click **OK** to restart the system. UnitedLinux 1.0 is ready for configuration.

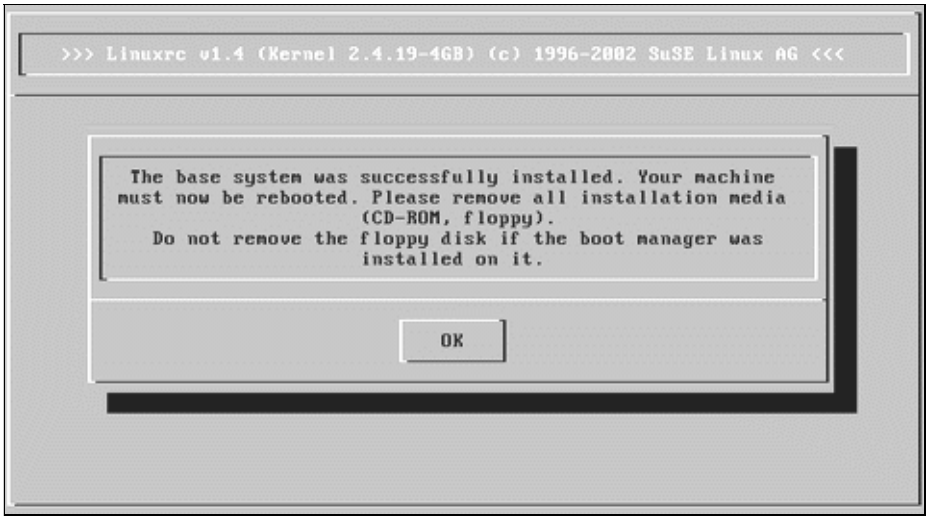


Figure 4-58 UnitedLinux 1.0: Installation complete screen

28. The screen switches to text mode and several lines scroll across it as subsystems are started. If the next CD is required, you will be prompted to insert it. Click **OK** when the correct CD is loaded. Repeat this process for all remaining CDs.

    Next, you are prompted for the system administrator (root) password as shown in Figure 4-59. The root user is also known as the *Super User* and is equivalent to the NT Administrator account. This account has full control over the system.

    Enter the password, then click **Expert Options** to change security settings.

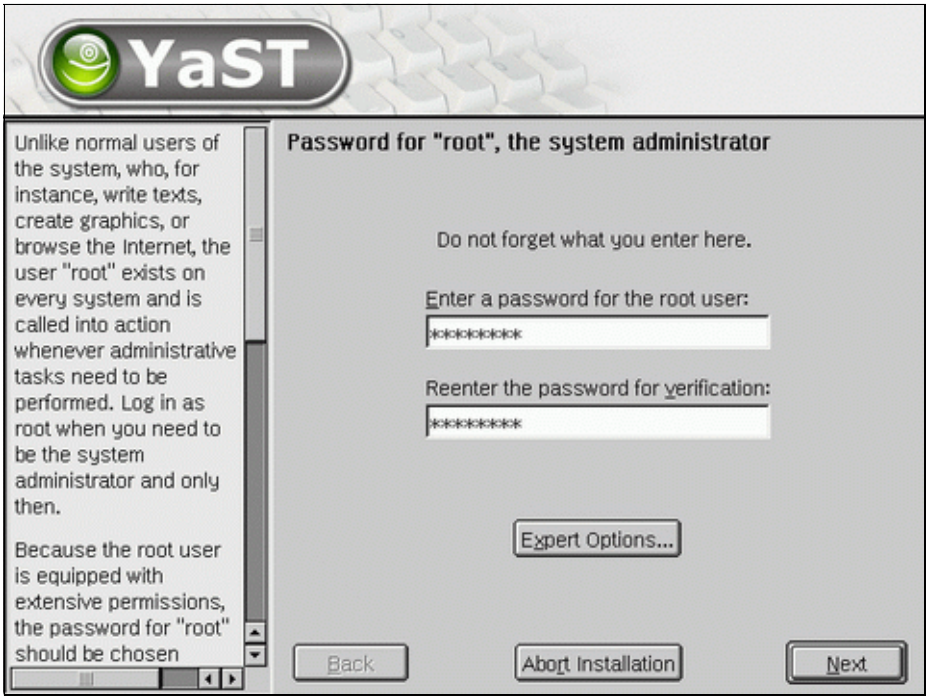


Figure 4-59 UnitedLinux 1.0: System administrator password

29. Select **MD5** for Password Encryption, click **OK**, then click **Next**.

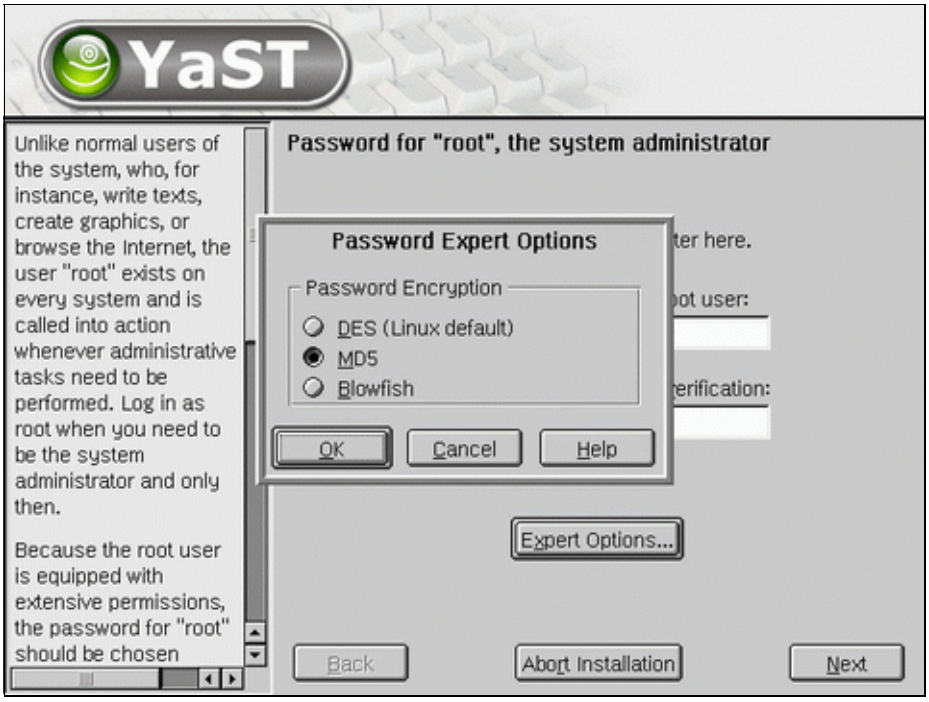


Figure 4-60 UnitedLinux 1.0: MD5 password option

30. Add a Domino user to the system. When you have entered all of the required information, click **Next** to continue.

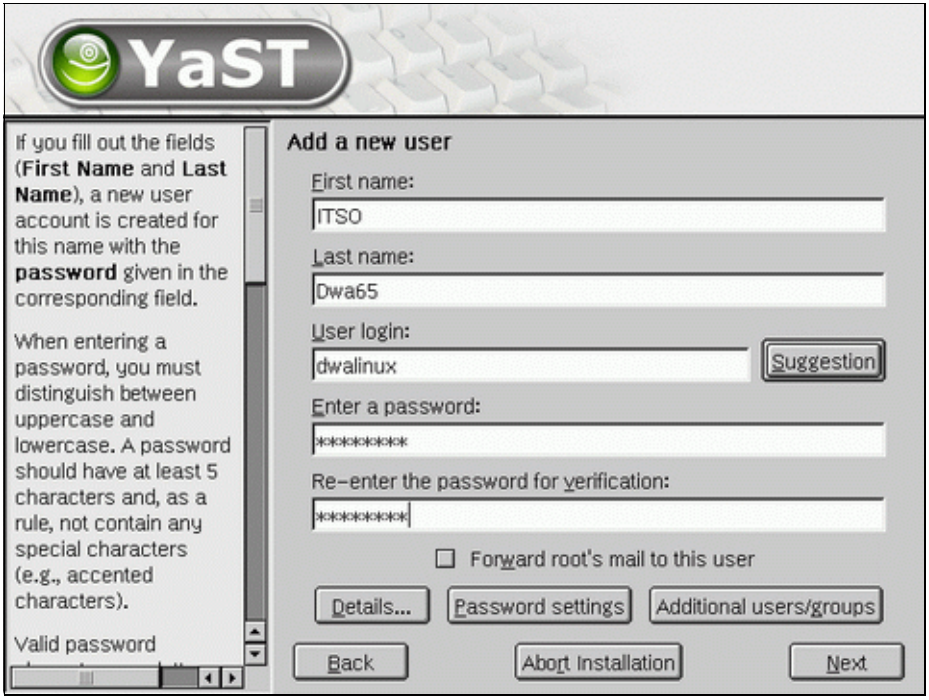


Figure 4-61 UnitedLinux 1.0: Add a new user

Tip: After filling in the requisite information, you can click the **Additional users/groups** button. Click the **Group** tab, create a group called `notes`, and add the user account you just created (dwalinux in our case) to the notes group. This ensures that your user and group are ready for the Domino 6 installation.

31. On the next few screens your monitor and video card will be configured. As shown in Figure 4-62, the installer tries to determine which monitor you have attached to your system.

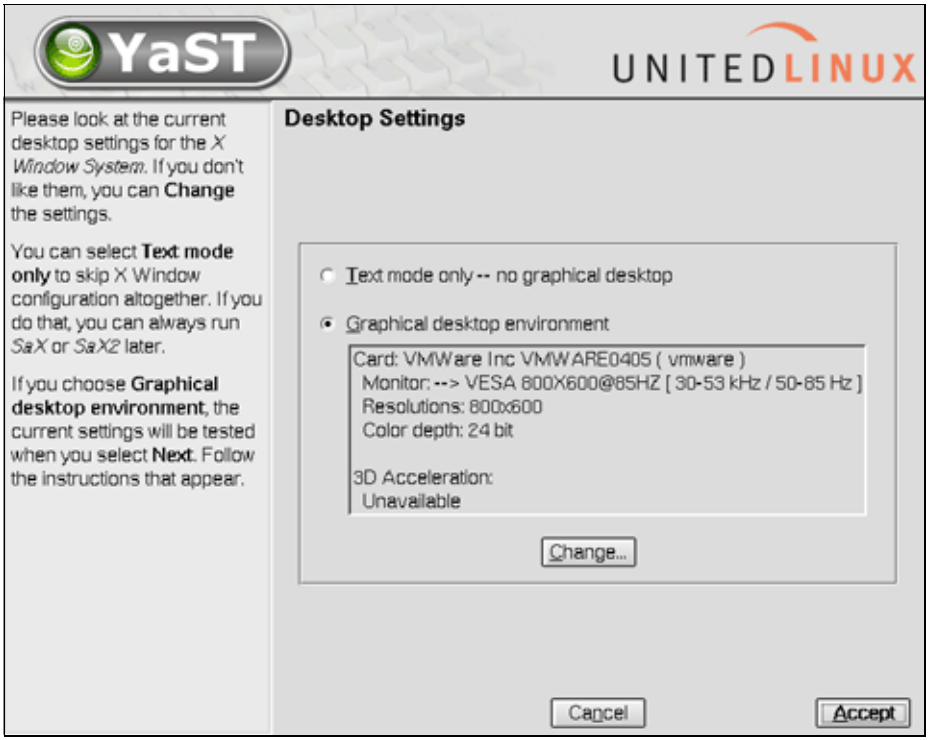


Figure 4-62 UnitedLinux 1.0: Desktop settings

This screen is displayed if the video card in your machine and its capabilities can be determined.

If the settings are incorrect, click **Change**.

32. If the installer was unable to determine your monitor, you can select it from a list of monitors (Figure 4-63). If your monitor is not listed, use VESA since most monitors comply with this standard.

    Pick a resolution that is as high as your monitor can display or that is comfortable for you. Linux displays are quite big, so they work better at 1024x768 or higher resolutions.

    If you have the monitor driver disk that came with your monitor, you can insert that and let the installation program read the settings from the disk. Click **Manufacturer disk** to make use of this feature.

    Click **OK** and **Accept** to continue. This will automatically test your settings.

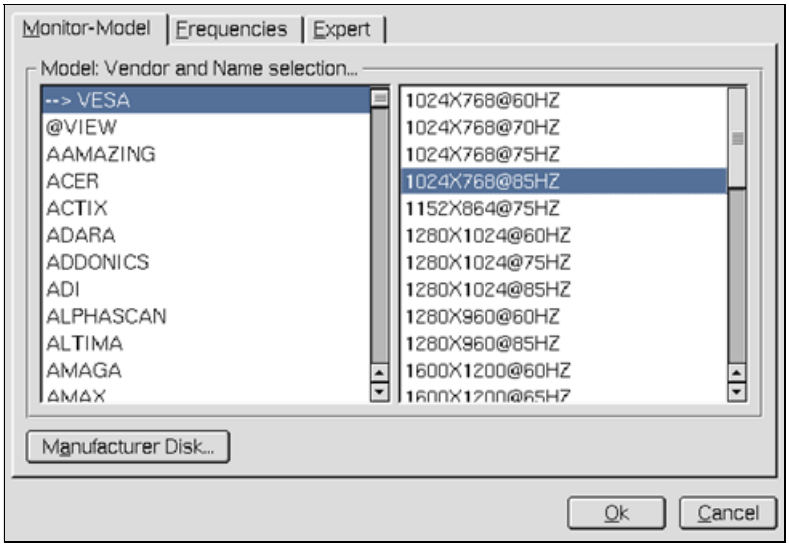


Figure 4-63 UnitedLinux 1.0: Configure monitor

33. The Installation Settings screen will be displayed. Here you can configure various peripherals, such as Networking, Printers, Modems, and so forth.

    You need to configure your network interface. Click **Network interfaces** to change its settings.

34. A list of detected network cards installed in your system is displayed as shown in Figure 4-64. Click the name of the network card you would like to configure, then click **Configure**.

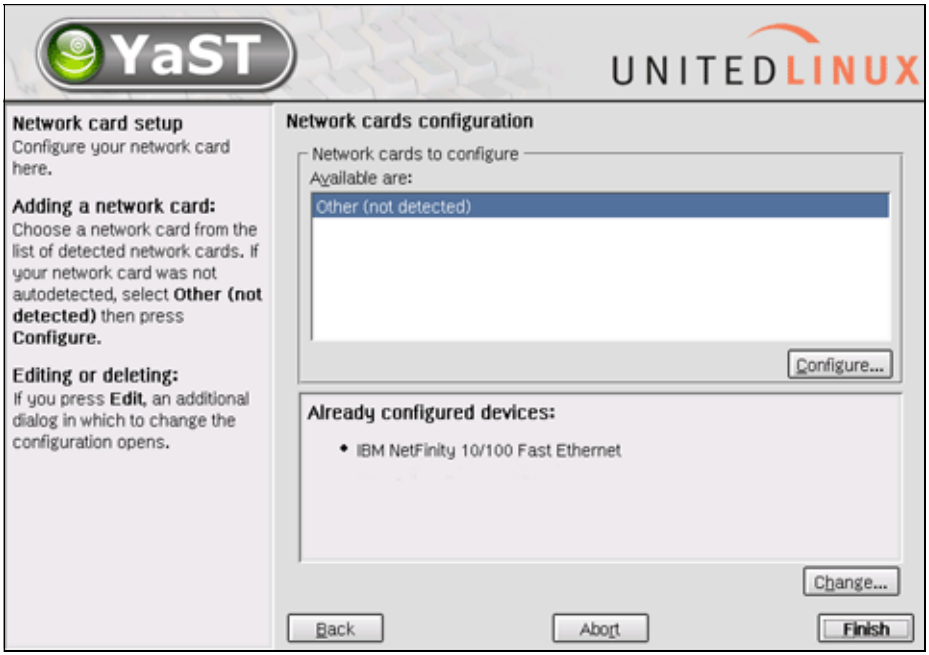


Figure 4-64 UnitedLinux 1.0: Network cards configuration

35. Change to **Static address setup** and enter the IP Address and Subnet mask in the fields provided. When your settings are correct, click the **Host name and name server** button.

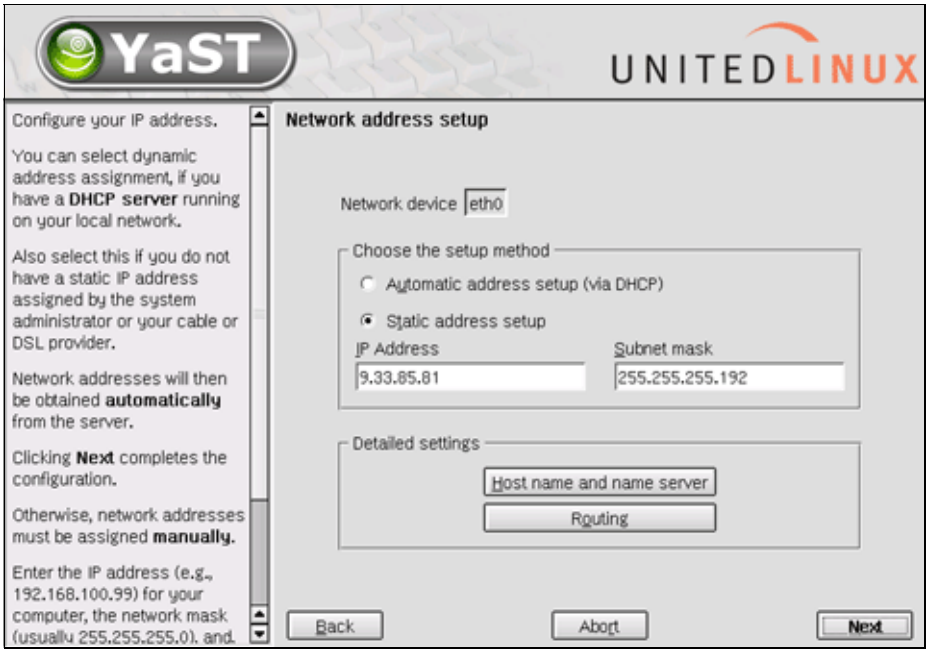


Figure 4-65 UnitedLinux 1.0: Network address setup

36. Enter the Host name and Domain name of your system, the Name server IP addresses, and any additional domains to search in the domain search list. Click **Next** to return to the Network Address Setup screen.

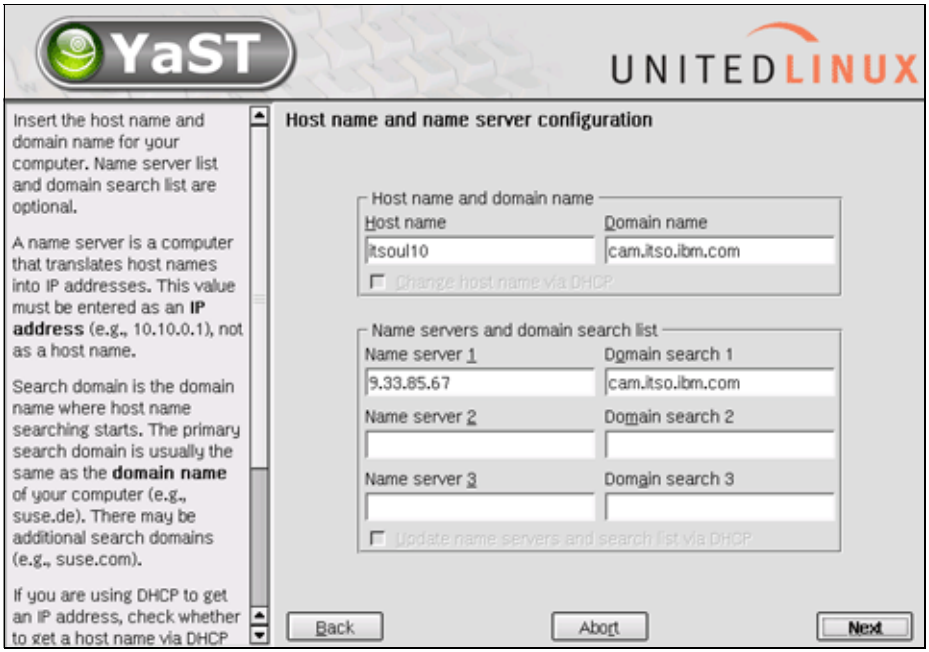


Figure 4-66 UnitedLinux 1.0: Host name and name server configuration

37. Before you configure another card, click the **Routing** button shown in Figure 4-65 on page 148 and enter the Default gateway for your network as shown in Figure 4-67. Click **Next**.

Figure 4-67 UnitedLinux 1.0: Routing configuration

38. Click **Next** again to return to the Network Card Configuration screen shown in Figure 4-68.

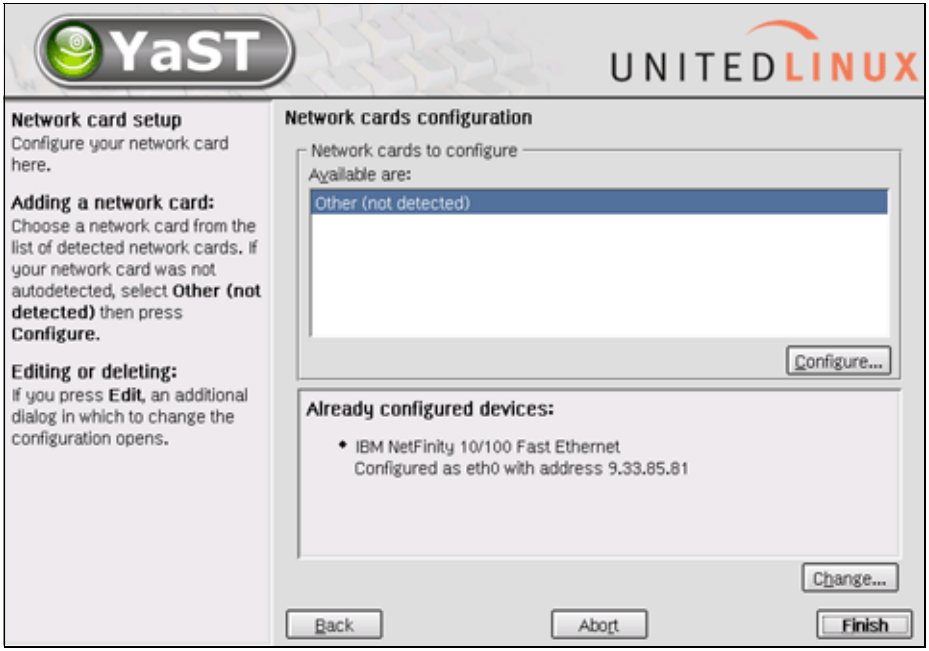


Figure 4-68 UnitedLinux 1.0: Network card configured

You can repeat these steps to configure additional network cards installed in your system. Click **Finish** to return to the Installation Settings. You can configure the other peripheral.

For the purpose of these instructions we continue with the installation by clicking **Finish**.

39. The configuration of your system is written to disk. A window appears to inform you that the configuration has been saved successfully. Let it time out to start up the system. Several lines of text scroll across your monitor as the system is started.

    When the system has loaded, you can log in with the account you created during installation, as shown in Figure 4-69.

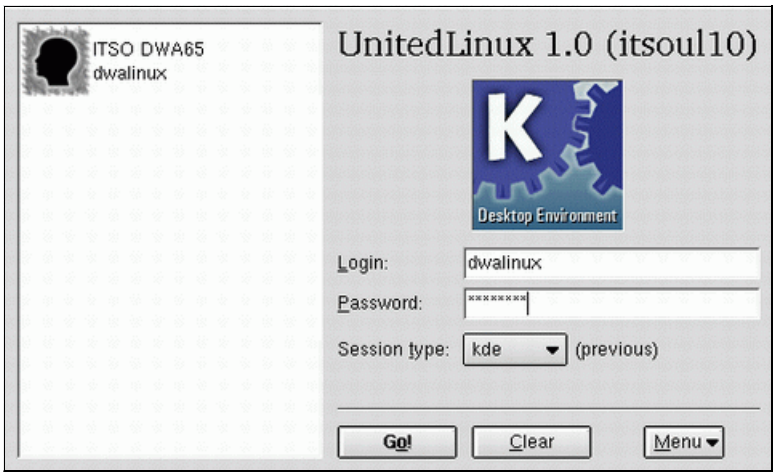


Figure 4-69 UnitedLinux 1.0: Graphical log in

This completes the UnitedLinux 1.0 installation process.

5

Installation and setup of Domino Web Access 6.5 on Linux

In this chapter, we discuss how to install and configure Domino Web Access 6.5 on a Linux server.

First, we address pre-installation tasks for creating both a user account and a group account that can install and run Domino. For those users interested in an especially easy way to pre-configure your Linux server for Domino, we introduce the UnitedLinux Extension Pack for Domino. This is an installation package by SUSE LINUX that provides a start/stop environment for Domino and allows for an easy way to set up user accounts and configure key parameters for a Domino installation. For those users interested in the more traditional approach to manually preparing the server, we also discuss the pre-installation tasks as you would perform them while working directly within a shell console.

We then describe in detail how to install and configure the Domino server.

Finally, we briefly discuss ways to start the Domino server, including some ways that make administration a little easier.

5.1 Preconfiguring your Linux server: the easy way

This section describes the UnitedLinux Extension Pack for Domino, an install package provided by SUSE LINUX that creates a start/stop environment for Domino on your Linux server. You can read about this extension pack at:

http://www.suse.de/en/business/products/server/sles/domino.html

5.1.1 Install UnitedLinux (SLES 8) Extension Pack for Lotus Domino

We recommend installing this package, because it creates a start/stop environment for a Lotus Notes Domino Server. Additionally, this package contains an optimized libpthread.so for Lotus Domino to increase the number of threads per processor in order to allow more concurrent users on one server.

Before you can install UnitedLinux (SLES 8) Extension Pack for Lotus Domino, confirm that your system is ready by performing the following steps:

1. Start YaST2 Control Center with this command: **`yast2`**
2. Select **Software** → **Install/Remove software** as shown in Figure 5-1. Click **Launch.**

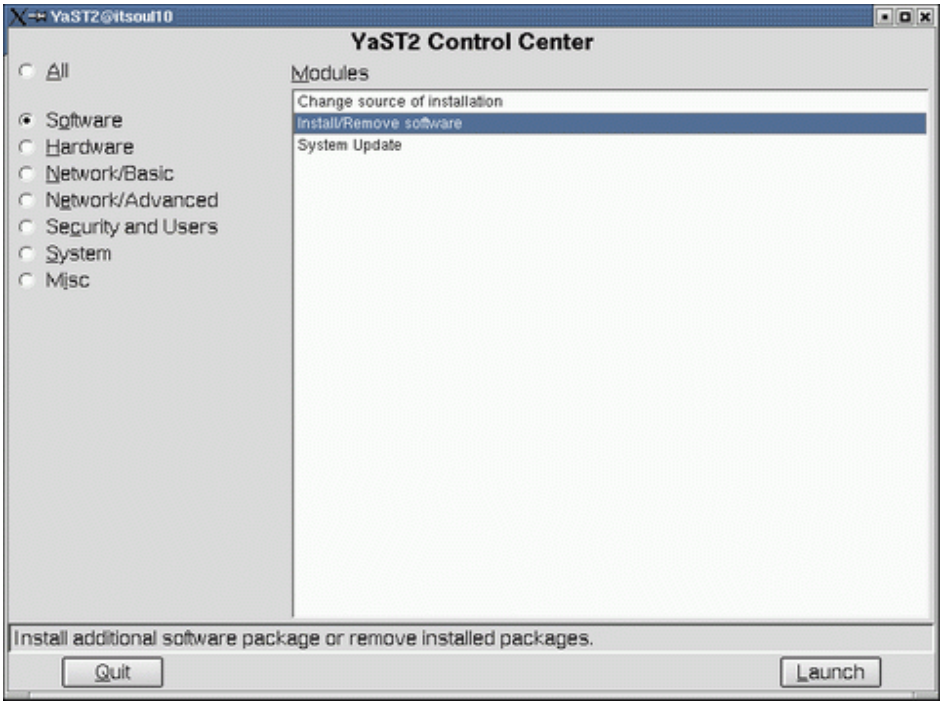


Figure 5-1 YaST2 Control Center

3. To determine whether the `compat` package is installed, click the **Filter** drop-down and select **Search.** Type `compat` into the Search field, then click the **Search** button to search for the package, as shown in Figure 5-2.

   As shown, compat is already installed.

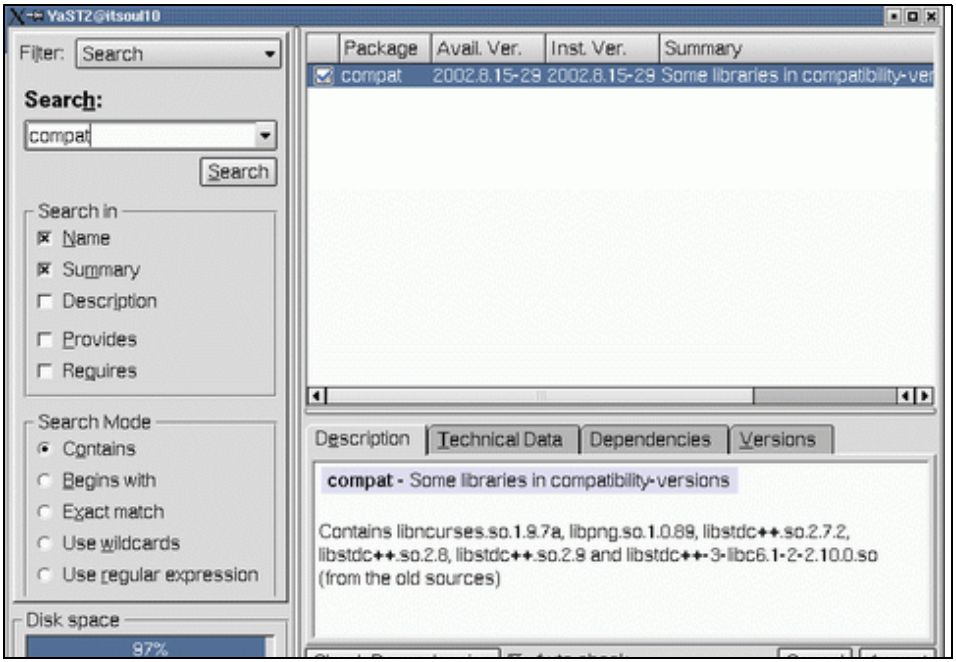


Figure 5-2 Search compat package

4. Open the Shell Console and create a temporary directory. For example, create an `install` directory by entering the command **`mkdir install`**.
5. Next, navigate to the site from which you can download the UnitedLinux (SLES8) Extension Pack for Lotus Domino. The specific file to download is the installer tar file called domino-runtime-2.2-4.i686.rpm. This is available for download at any of the following Web sites:

   `http://www.suse.de/en/business/products/server/sles/domino.html`
   `http://ftp.sunet.se/pub/os/Linux/distributions/suse/people/iboernig/domino/sles8/`
   `http://ftp.sunet.se/pub/os/Linux/distributions/suse/people/iboernig/domino/sles8/domino-runtime-2.2-4.i686.rpm`
6. Switch to the temporary directory, **`cd install`**
7. Type **`ls`** to view the directory contents. (This is the same as **`dir`** in DOS.)

8. Type the command `rpm-Uvh domino-runtime-2.2-4.i686.rpm` to launch it, as shown in Figure 5-3.

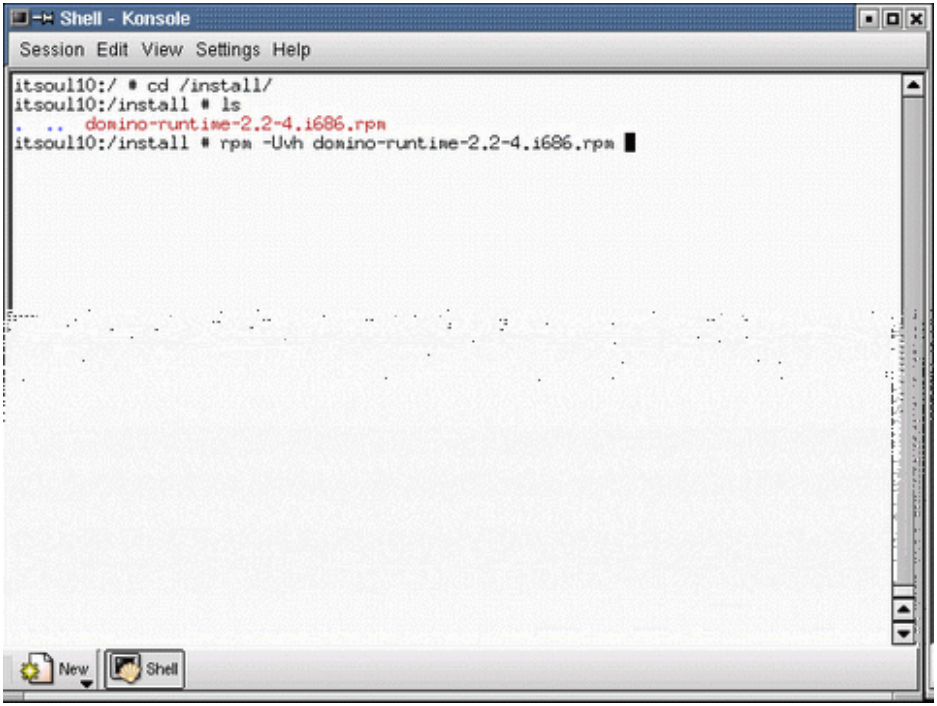


Figure 5-3 Launching the install program

As the installation begins, the console shows that the system parameters are being updated, as shown in Figure 5-4. This package handles these tasks:

- Setup of the user `notes` and the group `notes`
- Installation of the start/stop script
- Specification of environment variables and kernel parameters

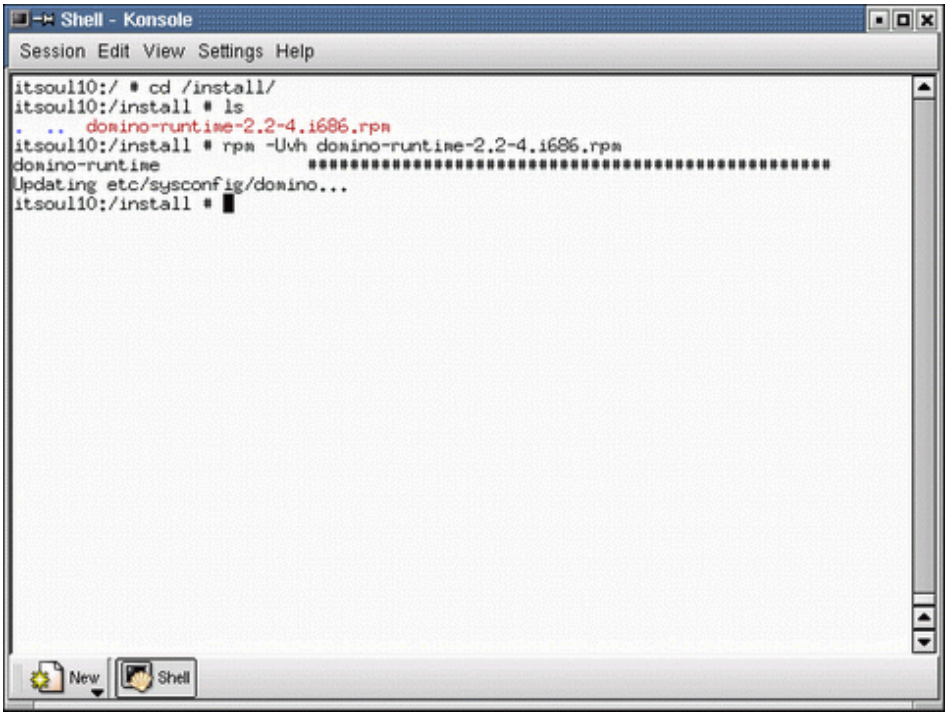


Figure 5-4 Updating system parameters

5.1.2 Edit UnitedLinux (SLES 8) Extension Pack for Lotus Domino

In this next section, we describe how to edit the /etc/sysconfig/domino file in order to complete the installation of the init script.

To continue to use the init script, you must first edit the /etc/sysconfig/domino file and provide entries for some of the key variables. (See the example shown in Figure 5-5 on page 158.) You may edit this file with a text editor of your choice.

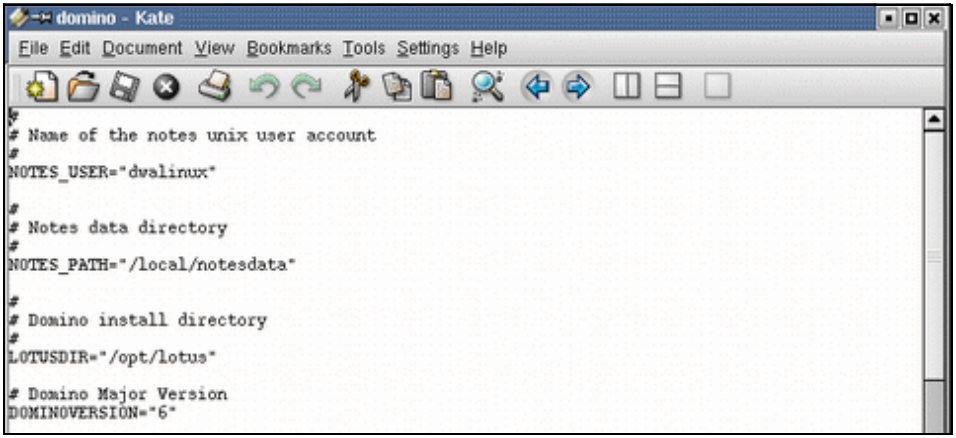


Figure 5-5 Script parameter

In this file, you can customize the following variables:

NOTES_USER	Name of the Domino UNIX user account.
NOTES_PATH	Domino data directory.
LOTUSDIR	Domino install directory.
DOMINOVERSION	Domino major version.
NOTESLANG	Domino language setting.
DOMINO_JAVA_CONSOLE	Enable or disable Java console. Disable login to /var/log/notes/domino.log.
NOTES_MAXSHAREDMEM	Size of largest shared memory segment.
NOTES_SHMMNI	Maximum number of shared memory segments.
NOTES_SEM	Semaphore settings.
NOTES_USERPROC	Maximum process per UNIX user.
NOTES_JAVA_PATH	The path under which notes can find libjitc.so (Domino 5 only).
NOTES_PTHREAD_EXTENSION	Set the variable to `yes` if you want to manage more than 1000 concurrent users on your Domino server.

After entering this information, save and close the file. Subsequently, the start script should work. You do not need to specify the user group.

Note: If you edit the init script and change the name of the notes UNIX user account, remember that it is also very important to change file owner to correspond with this name. See Figure 5-6.

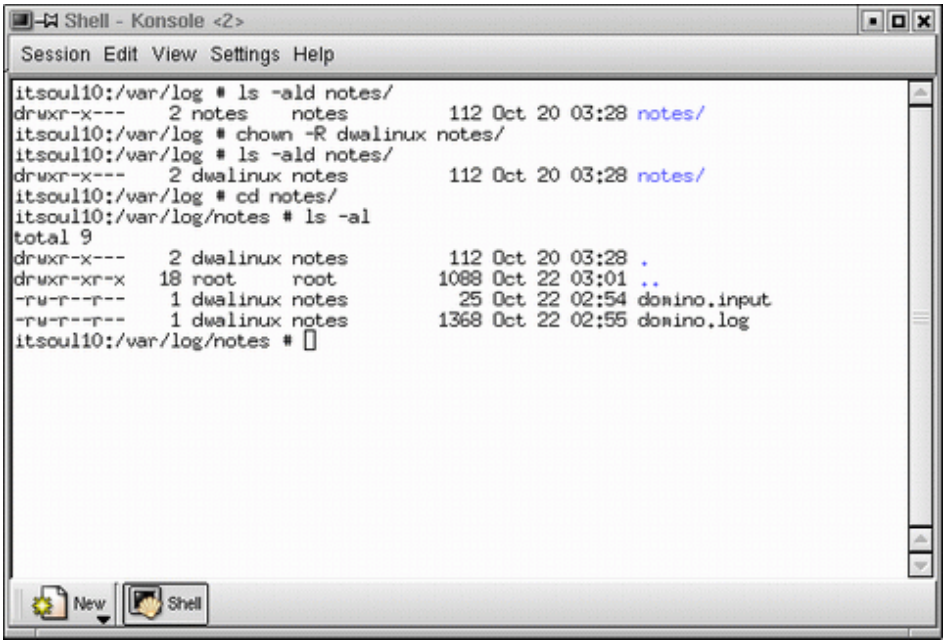


Figure 5-6 Change file owner

Executing the init script

At this point, the init script is ready for use. You can use the following commands to start and interact with the server after the server is installed. To begin installation of the Domino 6.5 server, proceed to 5.3, “Domino 6.5 server install” on page 168.

- To start your server, simply reboot the machine or execute the command **`rcdomino start`** as the user `root`.
- To view all messages of the Domino server from the operating system, open the /var/log/notes/domino.log file.
- To interact with the server from the shell or by means of a script, you can send your input to the /var/log/notes/domino.input file. To test this, write the command:

  ```
  echo "show server" >>/var/log/notes/domino.input
  ```

  You will then see the output of the file /var/log/notes/domino.log.

5.2 Before you begin: pre-installation tasks

This section describes the manual approach to setting up user accounts and group accounts for installing and running Domino. This approach assumes that you have not installed the UnitedLinux Extension Pack for Domino as described in 5.1.1, “Install UnitedLinux (SLES 8) Extension Pack for Lotus Domino” on page 154.

First, ensure that you have a Linux user account, as well as a group, under which to run Domino. After booting the system, log in as the root user, using the password you created during installation. Depending on whether you elected to have X-Windows launch automatically, you will be at the command line prompt or at an X-Windows prompt. If you are at the command line (with no GUI), log in as `root` then type `startx` to begin an X-Windows session. Otherwise, log in as `root` and the graphical desktop environment of your choice will load. (Ours is KDE.)

The bottom of a typical KDE or GNOME desktop has a task bar. Locate the shell icon, which in KDE is a monitor with a sea shell superimposed, and click the icon *once*.

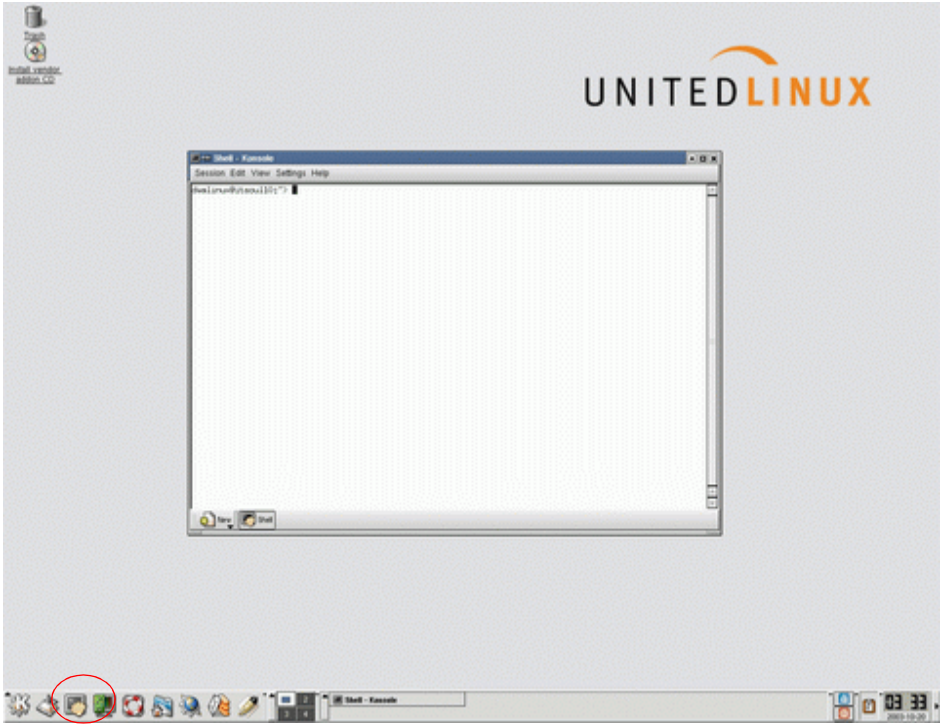


Figure 5-7 The Shell Console in KDE

Tip: If you are accustomed to double-clicking icons in order to launch applications, you can change the default behavior of KDE via the Control Center. Click the **Start Applications** icon (first icon starting from the left of the task bar), click **Control Center**, and go to **Peripherals** → **Mouse**.

1. Ensure that the account that will be used to run Domino exists.

   When the shell is running, you can check for the existence of the Notes account. Figure 5-8 shows one way: The **`tail`** command shows you the last x number of lines for a file as specified by the command line parameter. We used `tail -20 /etc/passwd` to view the last 20 lines of the passwd file. The names of user accounts are kept in this file and located in the first position of each line.You can see our account, `dwalinux`, listed at the very bottom.

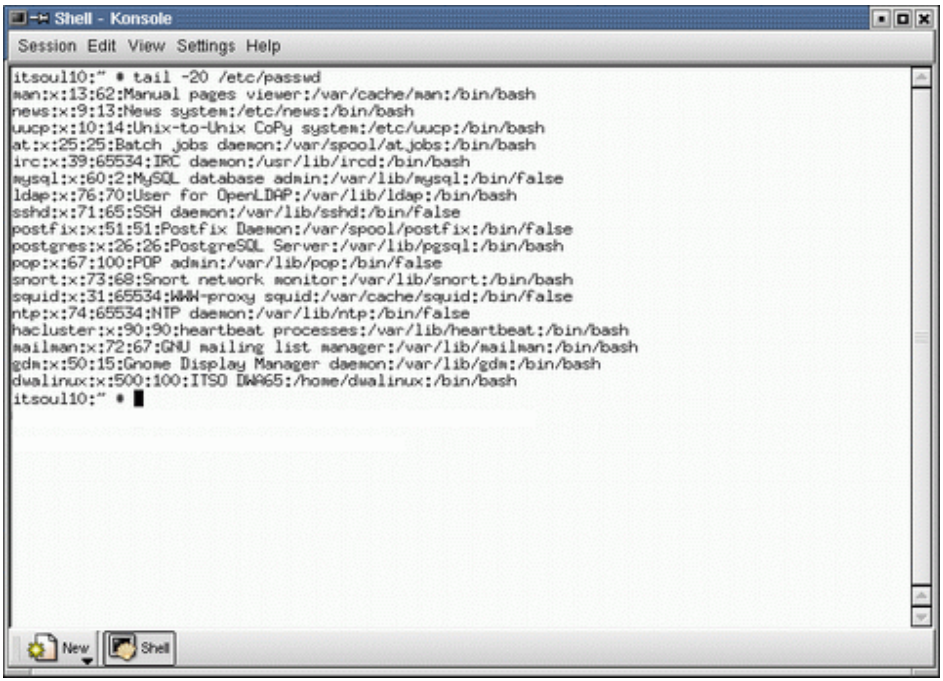


Figure 5-8 Portion of the passwd file

2. Ensure that the user group for Domino exists.

   Next, we ensure that we created a user group for Domino and that our account, dwalinux, is a member of that group. Those familiar with Lotus Notes will understand the use of users and groups. The main difference is that in Linux you cannot nest a group within another group.

To check for the group, we launch KATE by navigating to **Start Application** → **Editors** → **KATE** (UnitedLinux) or **Start Application** → **Editors** → **KATE** (Red Hat). KATE is a simple GUI text editor suitable for use in viewing the /etc/group file. You can see that the group `notes` is listed at the bottom and that our `dwalinux` account is a member.

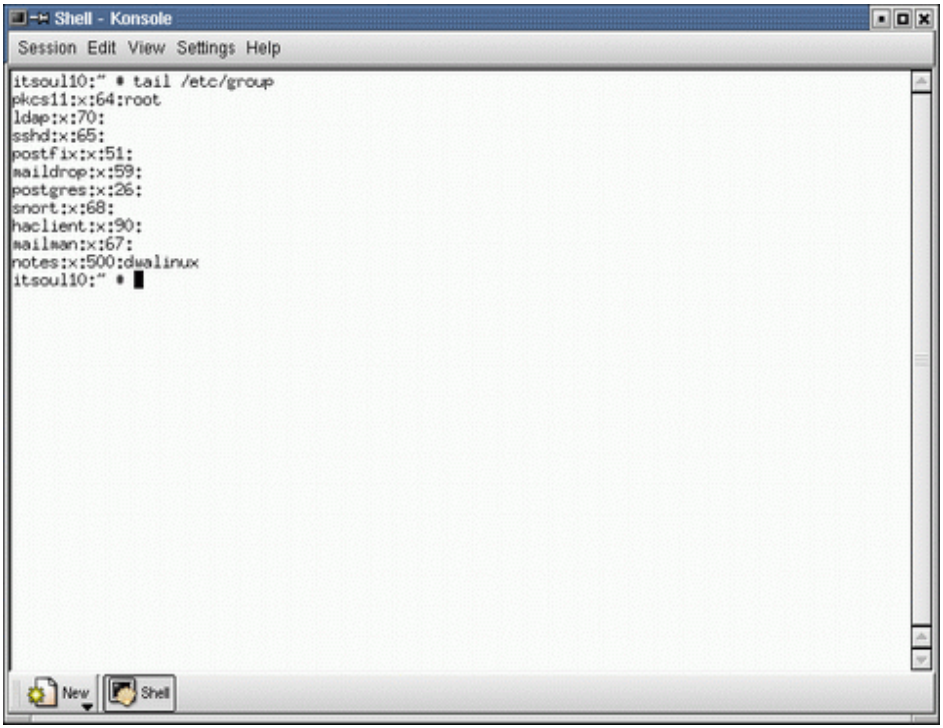


Figure 5-9 The contents of the /etc/group file

In the second-to-last line of the user file, notice that the number `500` is located between the group `notes` and the `dwalinux` account member name. Just as DNS is a human-friendly version of numerical IPs, Linux associates the names of users and groups with unique numbers so that we can refer to them by name instead of number.

In our example, we created the appropriate user account and group during installation. If you did so as well, you can skip ahead to Step 6 on page 168.

3. Create the Linux user group to run Domino.

   If the user and group do not exist, you need to launch a user manager program. From the command line, you can run **`useradd`**, **`userdel`**, or **`usermod`** and **`groupadd`**, **`groupdel`**, or **`groupmod`**, depending on whether you want to add, delete, or modify a user or group. With a graphical desktop environment, you

can use **Red Hat User Manager** and UnitedLinux **YAST2**, as well as **KDE User Manager**.

We used Yast2 Control Center because it is easy to use. From UnitedLinux 1.0 write to Shell Console Yast2. First, create the `notes` group before adding the user. This makes the notes group an available selection for the user account you will create next.

a. Select **Security and Users** → **Edit and create groups** as shown in Figure 5-10 and click **Launch**.

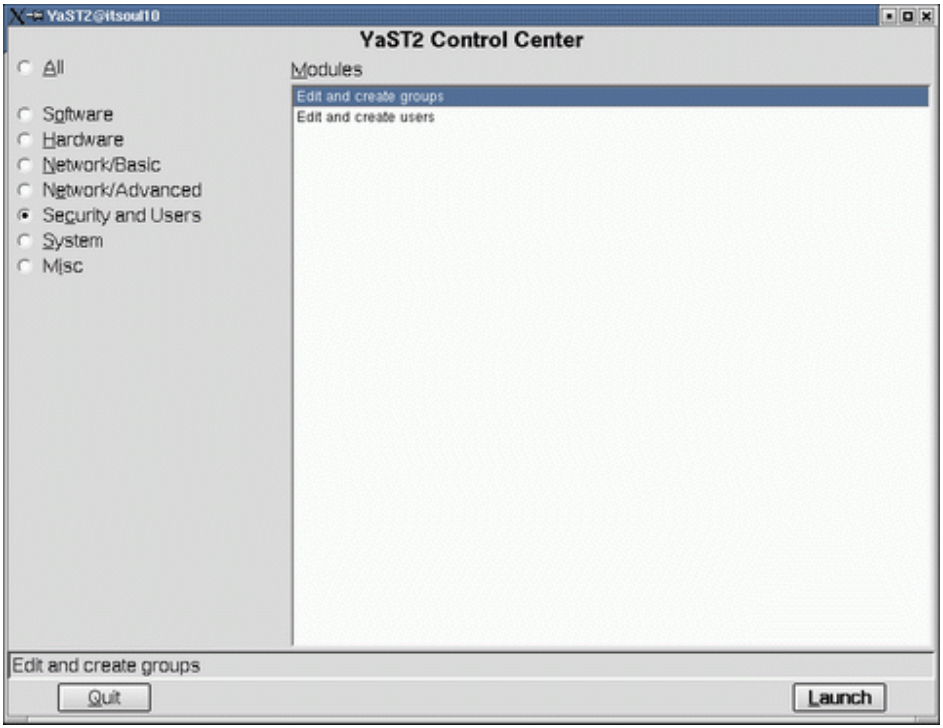


Figure 5-10 Add Group with Yast2 Control Center

b. Select **Groups administration** and click **Add** to add a new group.

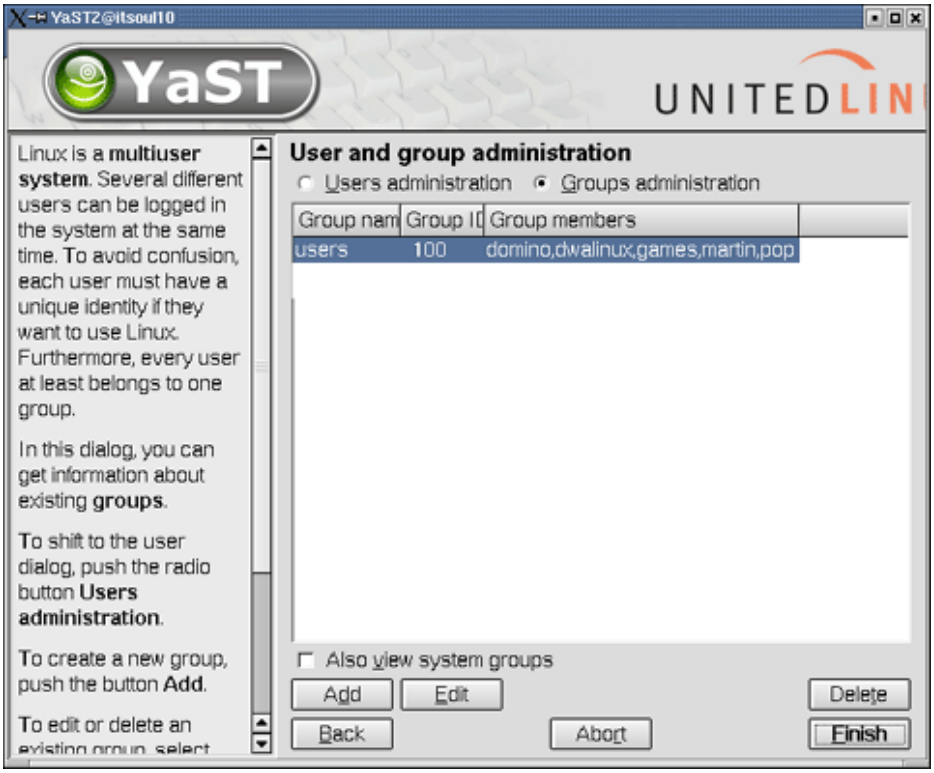


Figure 5-11 Users and groups administration

c. Add a `notes` group to the system. After you have entered all required information, click **Create** to continue.

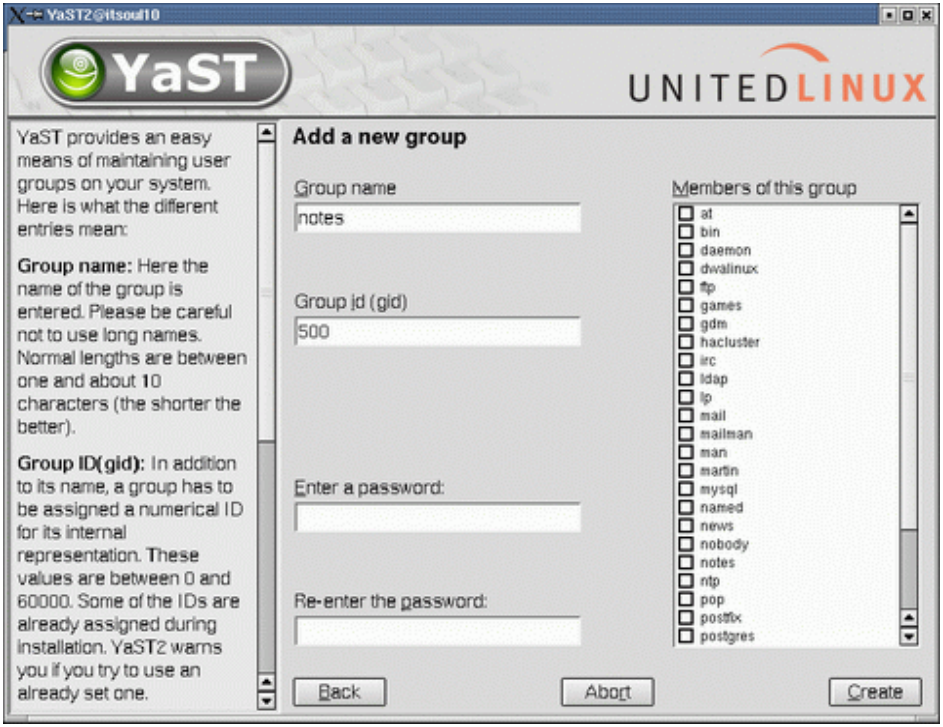


Figure 5-12 Add a new group

4. Create a Linux user account to run Domino.

   Now that you have created the group, you can create the account that will run the Domino server:

   a. Select **Users administration** and click **Add** to add a new user. You are prompted to enter the user name.

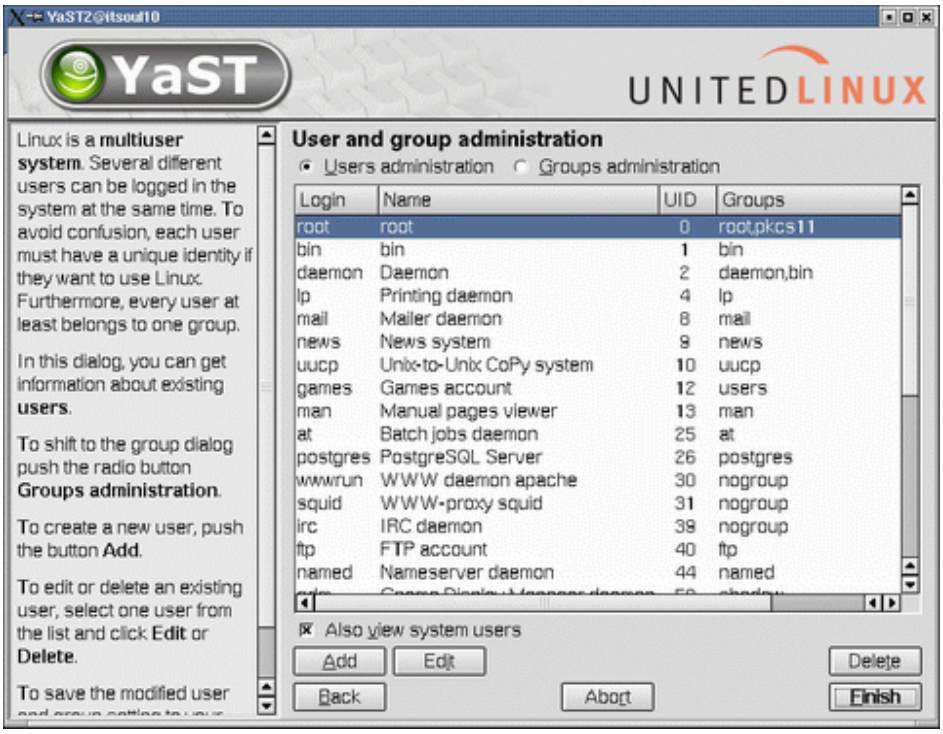


Figure 5-13 Add user with YaST2 Control Center

b. Add a Domino user to the system. After you have entered all of the required information, click **Next**, as shown in Figure 5-14.

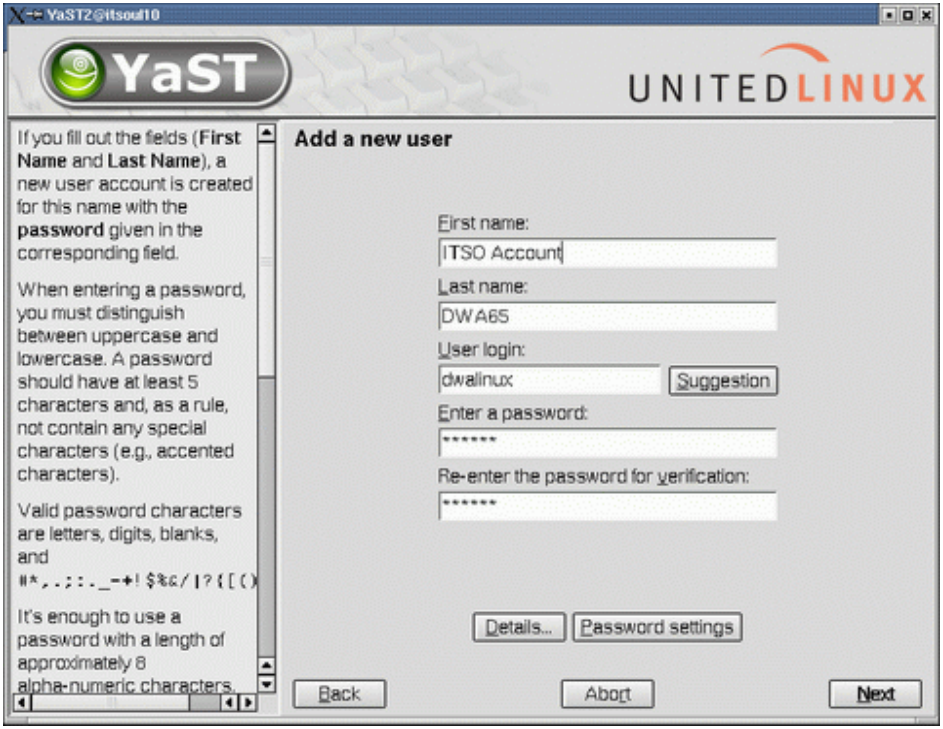


Figure 5-14 User properties

5. Make the user part of the group.

   When you are finished with this window, click the **Groups administration** radio button. Scroll down the list of groups until you see the `notes` group we created earlier. Click the check box to make the new user a member of that group, then click **OK** to save your changes and exit the YaST Control Center.

6. Check the available diskspace.

   After ensuring that both the user and group exist and that they are correctly associated, the next step is to double-check the available disk space. The command **`df -k`** and the human-readable **`df -h`** show the devices on the system and usage statistics.

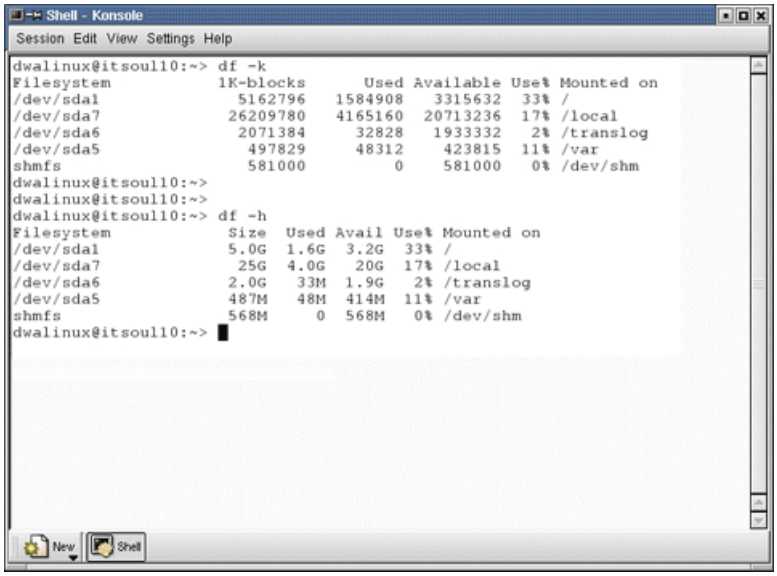


Figure 5-15 Checking for available disk space on the server

As you can see in Figure 5-15, we have enough space to install Domino into /opt/lotus because the / mount point has approximately 3 GB free. Since you are going to install the Domino 6.5 program files to the same mount point as the rest of the OS (this is equivalent to installing to the c: drive on a Windows NT system), you should have at least 500 MB free. Refer to the Lotus Domino 6.5 documentation for the exact disk space requirements. If you do not have enough disk space, the Domino installation program will detect this condition and abort with an error message.

KDiskFree is a graphic tool to show free disk space. Invoke it by clicking **Start** → **System** → **KDiskFree** on UnitedLinux, or **Start** → **System** →**KDiskFree (View Disk Usage)** on Red Hat.

5.3 Domino 6.5 server install

This section guides you through installation of the Domino server.

5.3.1 Installation

You can install from a tar file, where the files and directory information have been gathered into one file, or from a CD. This section assumes that you are installing from a CD. If you have a tar file, follow the directions that came from the download site. Generally, you will issue the command **`tar -xvf`** to unpack the files, **`cd`** to change to the appropriate directory, and **`./install`** to begin. If the file ends with .gz or another symbol denoting compression, unzip it first with **`gzip -d`** or another appropriate program before using the **`tar`** command.

5.3.2 Starting the Domino server installation

Use the following steps to start installation:

1. Change to the CD-ROM with **`cd /media/cdrom`** (UnitedLinux) or **`cd /mnt/cdrom`** (Red Hat).
2. Change to the Linux folder with **`cd linux`**.
3. Type **`ls`** to view the directory contents (same as DOS **`dir`**).
4. Type **`./install`** to launch it.

   The `./` in step 4 tells the OS to look in the current directory for the executable named `install`. For security reasons, ./ is not added to the root PATH environment variable because you could be tricked into launching a malicious program from a current directory, such as the /tmp folder. The PATH environment variable is the same as the PATH variable in DOS and Windows NT.
5. At this point, the Domino server installation program launches and opens the Welcome screen (Figure 5-16 on page 170).

Note: There is no graphical interface as with other installation platforms.

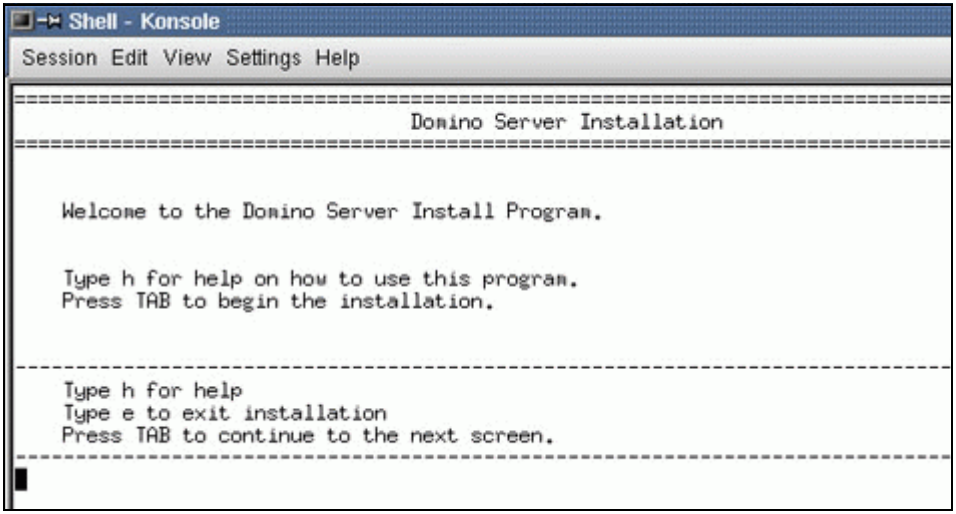


Figure 5-16 Domino install welcome screen

> **Note:** Throughout the installation, you will press the Tab key to move ahead. (This is comparable to clicking Next in a standard GUI).

6. Press Tab to open the second screen (Figure 5-17), which is simply an alert regarding new features available in Domino 6.5. Press Tab to continue.

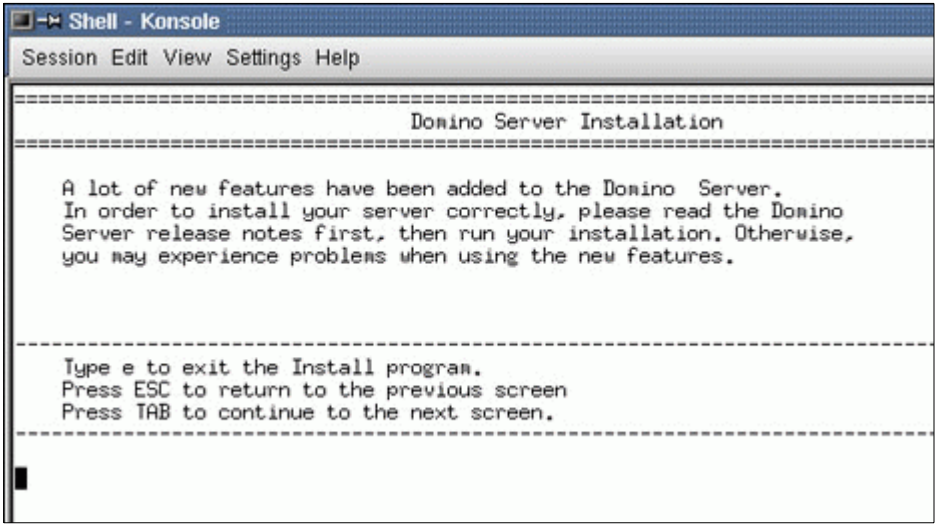


Figure 5-17 Domino new feature alert

7. After you have read and accepted the license shown in Figure 5-18, press Tab.

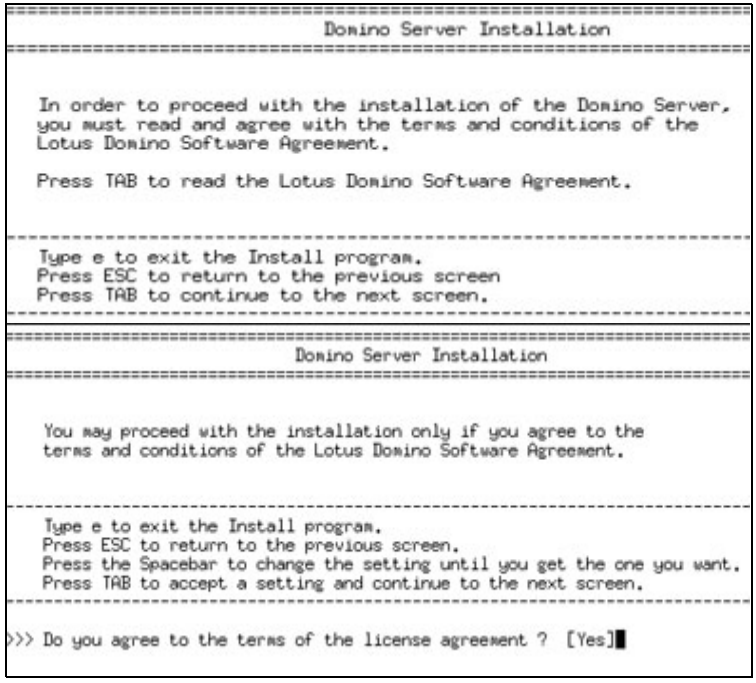


Figure 5-18 Domino license agreement

8. At the next screen, shown in Figure 5-19, you will be prompted about whether you wish to install Data Directories only. Enter `No` (assuming that you do not have an existing Domino Server already on your system).

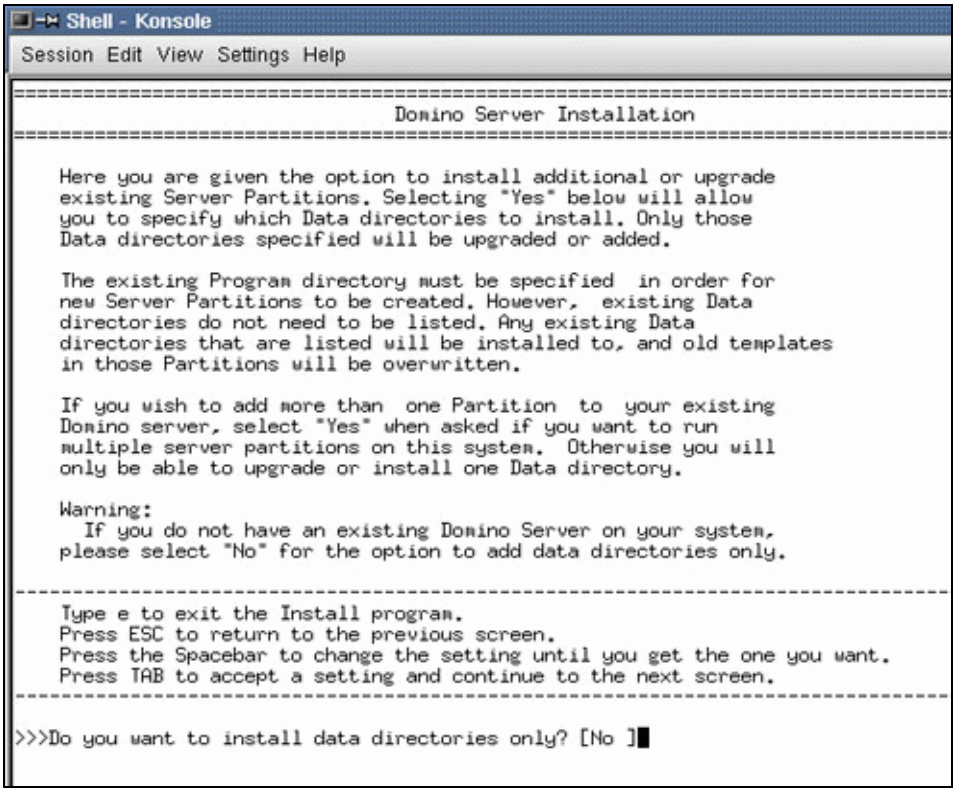


Figure 5-19 Install data directories only? screen

9. Select the type of server you wish to install: Utility, Messaging, or Enterprise. To cycle through the available choices, press the spacebar until the option you want is displayed. We selected `Domino Enterprise Server`, as shown in Figure 5-20.

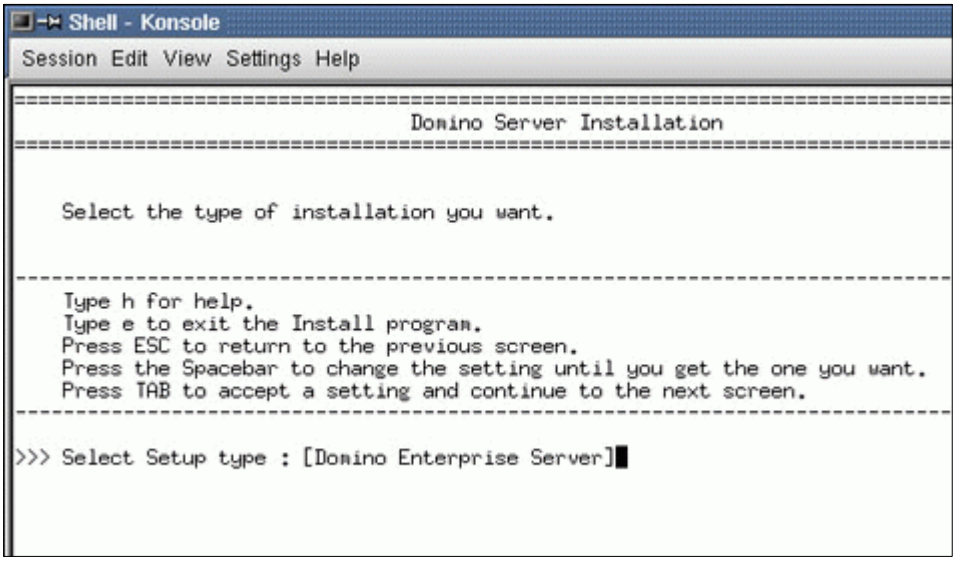


Figure 5-20 Type of Domino server to install

10. An option with Domino 6.5 is the ability to install a subset of templates instead of automatically installing every template. In general, however, you probably want to install all templates in order to take advantage of new features and bug fixes (Figure 5-21).

    If your company has customized any of the templates, evaluate the changes made in light of the new functionality provided by Domino 6.5. If the customizations are still required, you will have to apply them *after* the installation completes. Press Tab to accept the default and install all templates.

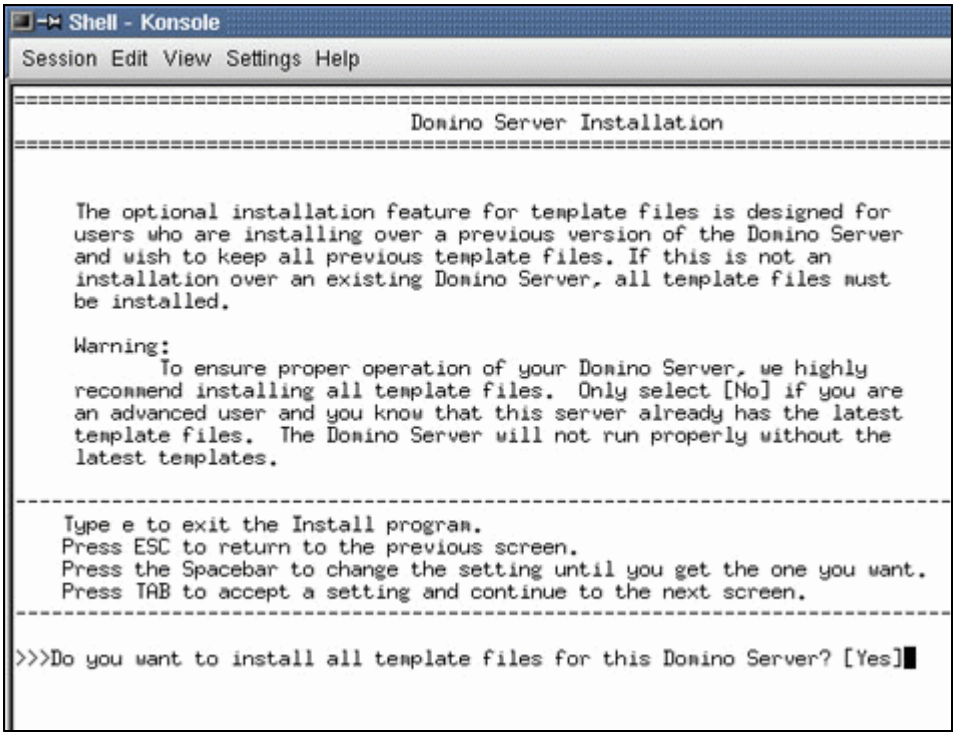


Figure 5-21 Template selection

11. At the next screen, shown in Figure 5-22, press Tab. `ASP support` is Application Service Provider and has nothing to do with Active Server Pages.

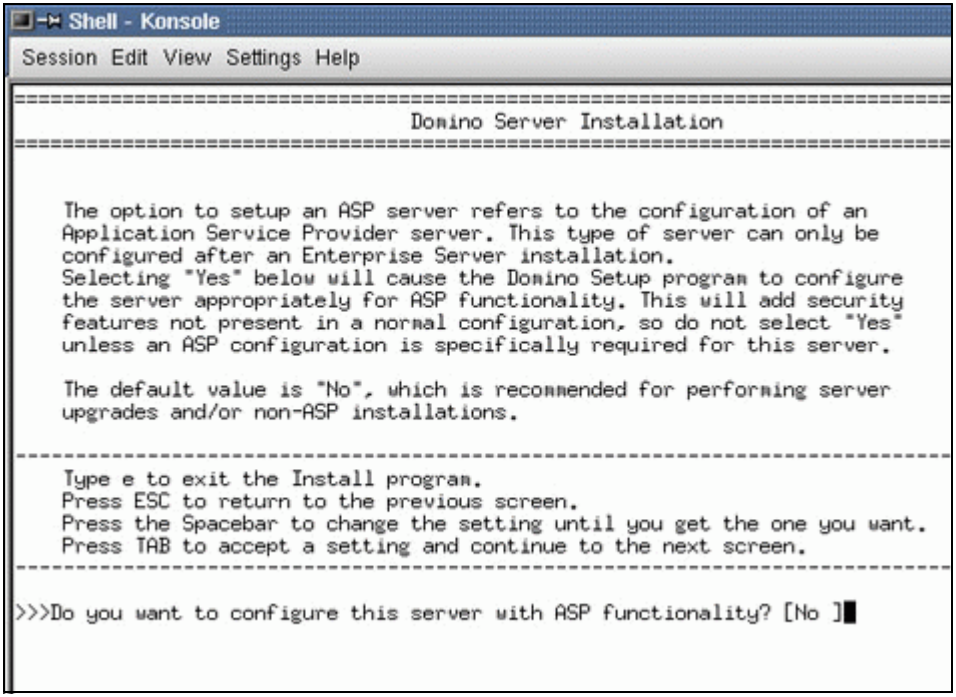


Figure 5-22 Configure ASP functionality

12. With Domino R5, you did not have to install the program files to /opt/lotus, but the server required an /opt/lotus symbolic link in order to function properly. As of Domino 6.0, the server no longer requires the /opt/lotus link, and so Domino 6.5 can coexist with R5 (still using /opt/lotus) or other installations of Domino 6.x (Table 5-1).

Table 5-1 Example of multiple installations

Version of Domino	Program file installation path
Domino R5	/opt/lotus
Domino 6	/opt/dom60/lotus
Domino 6.5	/opt/dom65/lotus

Important: If you have Domino R5 installed on a server, then even if the program files are *not* installed in /opt/lotus, you cannot install Domino 6.5 to that directory. Doing so will overwrite the symbolic link and the R5 install will no longer function properly.

13. For our single server, we chose to install only one version of Domino and so pressed Tab at the screen shown in Figure 5-23 to accept the default path.

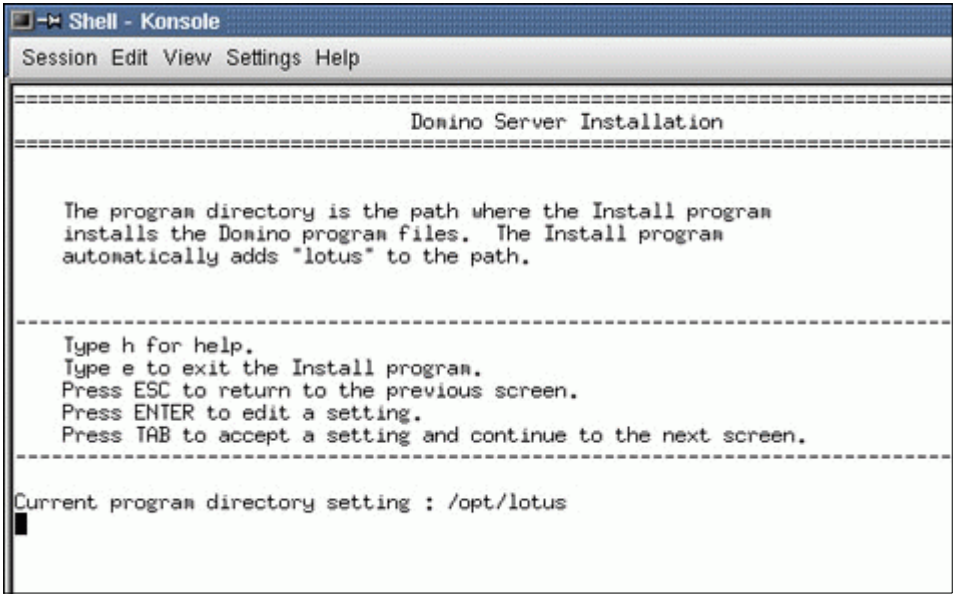


Figure 5-23 Location for the Domino program files

14. Figure 5-24 outlines the basic file ownership concept of Domino running on Linux. The user and group you specify will own the data and will be used to launch the server. The file permissions for the program files, however, will be set to `root` for required access to the system.

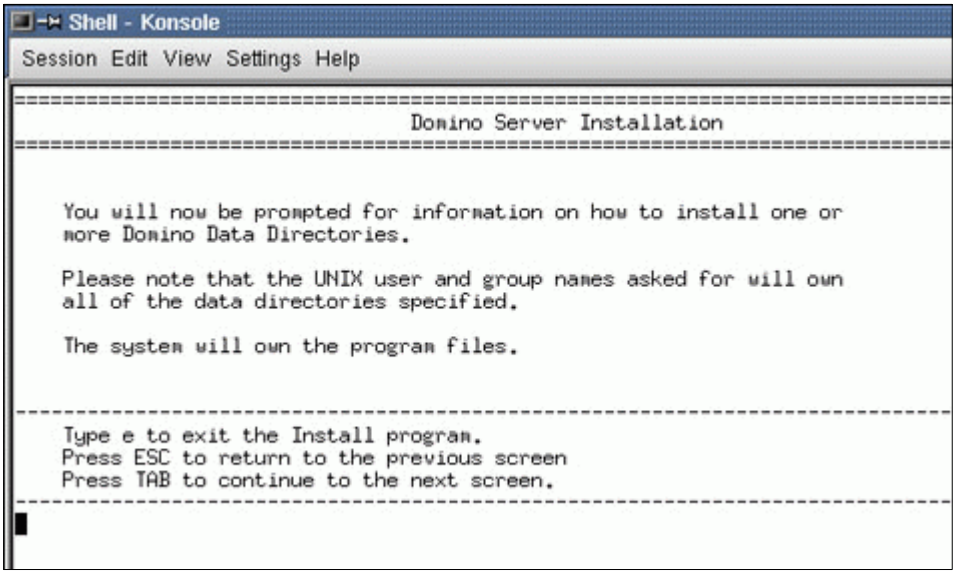


Figure 5-24 Explanation of Linux file ownership

15. You can run different versions of Domino on a single server, but you have the option to partition a server (Figure 5-25 on page 178). If you partition the server, multiple instances of Domino will share *one* set of program files but each installation will have a separate data directory. The new Domino 6.x feature that enables multiple installs requires *separate* program files, as well as *separate* data directories, for every instance, and so requires more disk space than partitioning. For our server, we chose not to partition it.

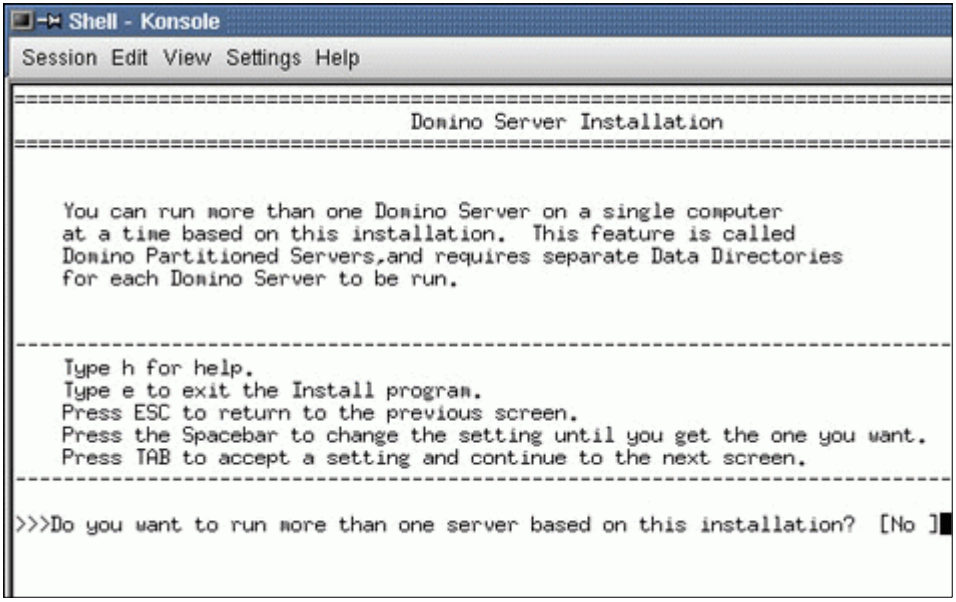


Figure 5-25 Partition server option

16. Press Tab to accept the default directory for Domino data files shown in Figure 5-26.

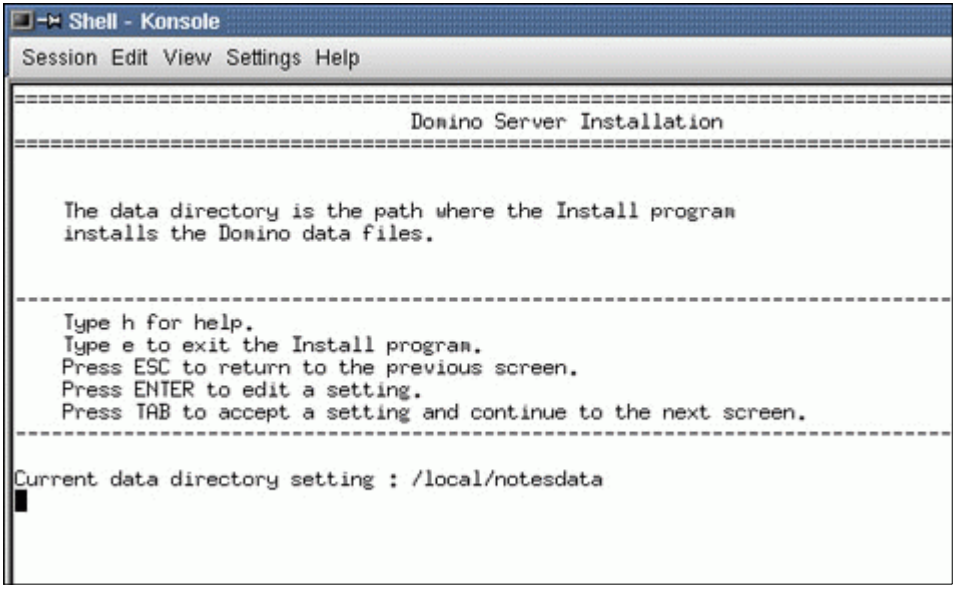


Figure 5-26 Location for the Domino Data Directory

17. Because hackers can break into your system more easily if they can readily guess an account name, you might not wish to use the default user name of `notes` (Figure 5-27). We opted to name our account `dwalinux` to reflect our group and the topic about which we are writing.

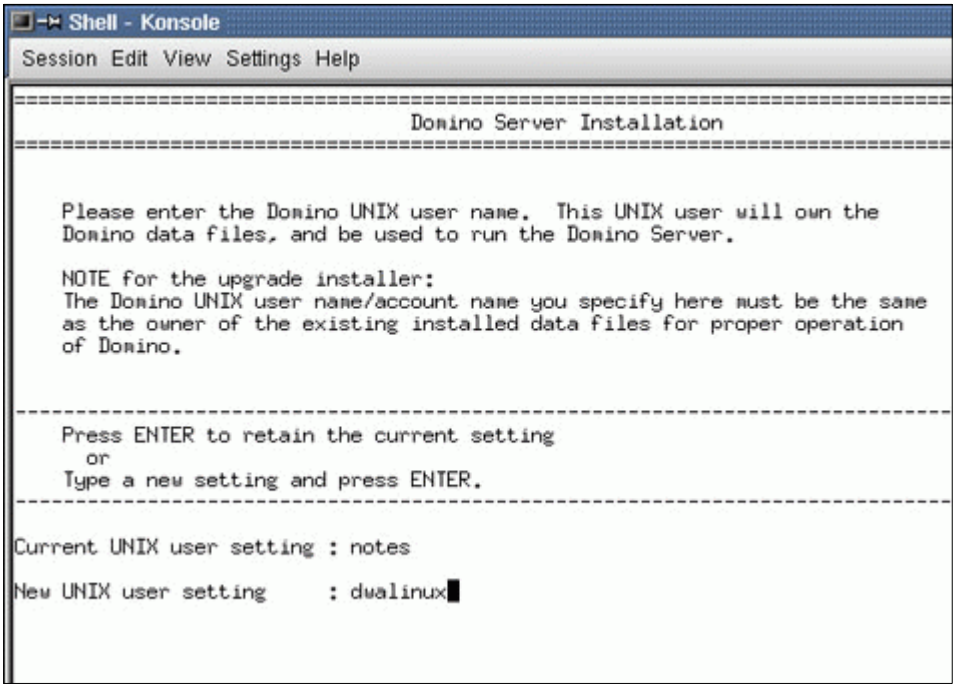


Figure 5-27 Linux user account setting for Domino

> **Attention:** Simply changing the name of the account does *not,* by itself, make your installation secure.

To change the account name, press Enter, type in the user name, press Enter again, then Tab.

18. Enter the name of the group you created earlier. We chose the default of `notes`.

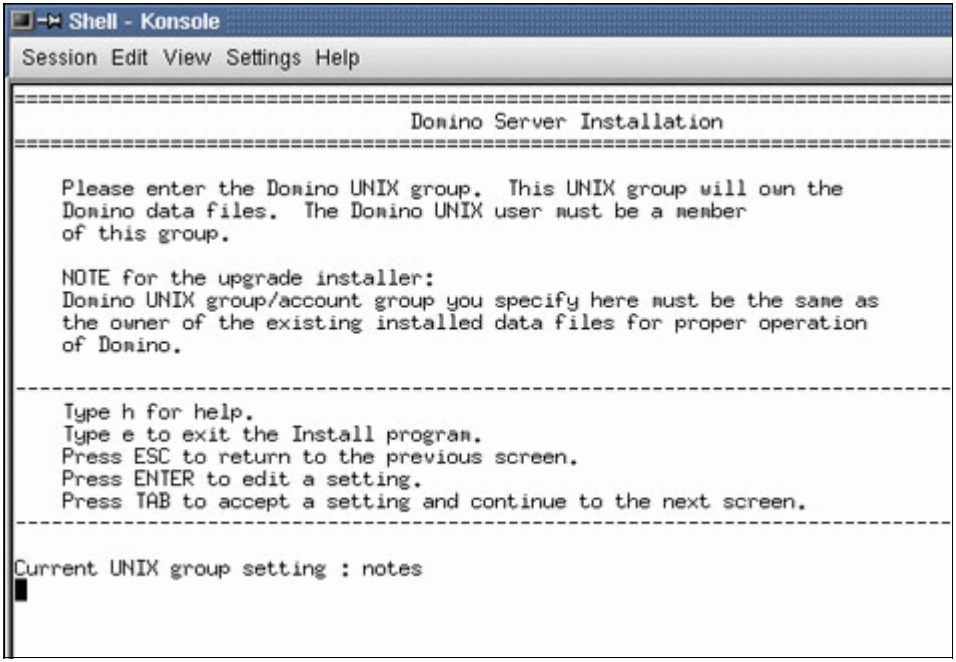


Figure 5-28 Linux group for Domino

19. You will need to select the type of method setup: Manual, Local, or Remote. To cycle throughout the available choice, press the spacebar until the option you want is displayed. We selected Manual Server Setup.

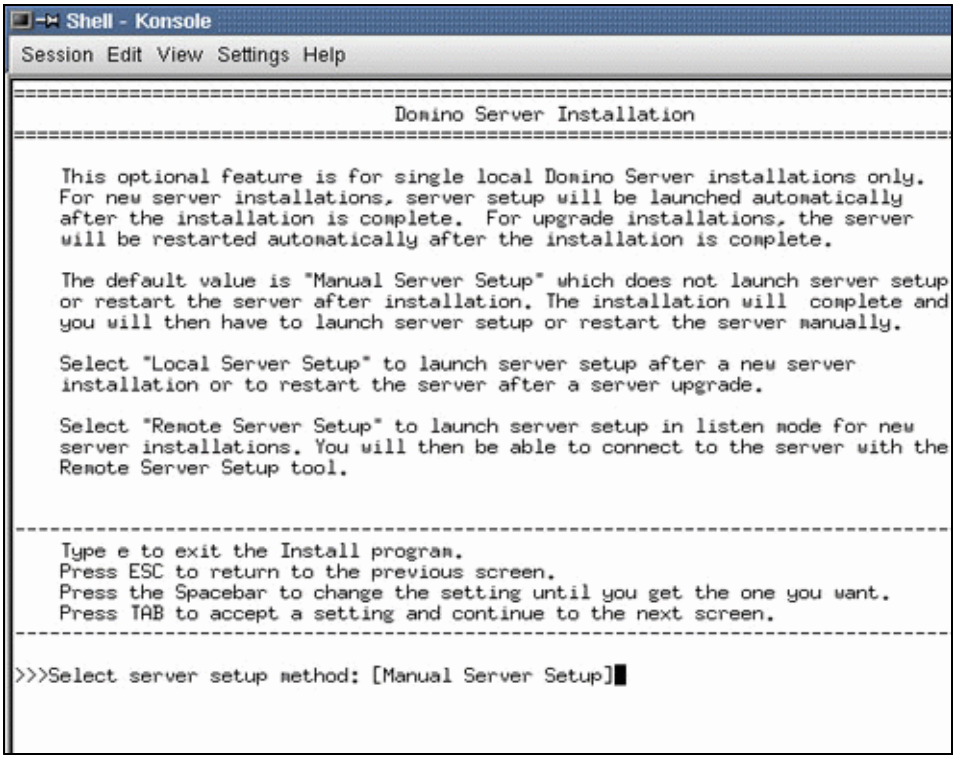


Figure 5-29 Select server setup method

At the screen shown in Figure 5-30, press Tab to continue the installation.

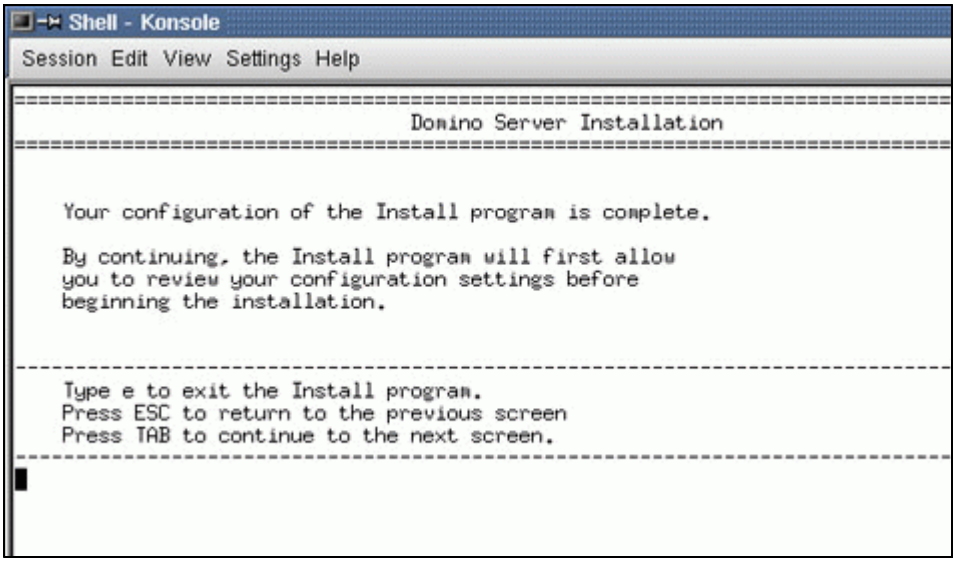


Figure 5-30 Configuration complete

At the next screen (Figure 5-31), review the information you have entered. If you entered something incorrectly, press the esc key (this is comparable to clicking Back in a GUI) to correct it. When ready, press Tab to install Domino 6.5.

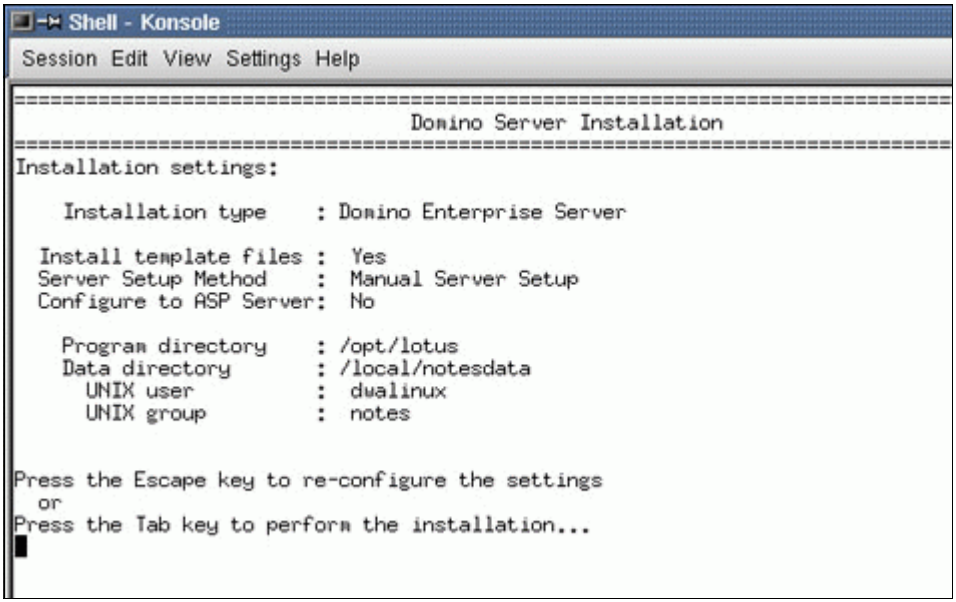


Figure 5-31 Perform installation

20. When installation completes, the screen in Figure 5-32 on page 184 opens.

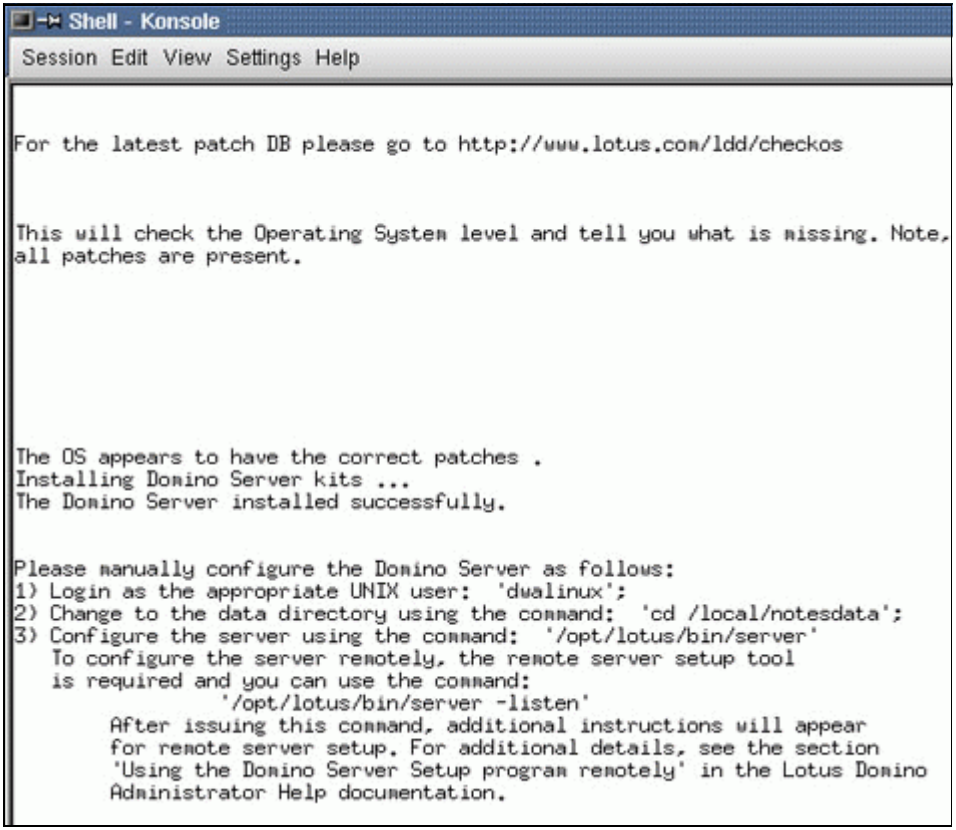


Figure 5-32 Installation complete

Important: For those familiar with R5 or earlier versions of Domino: Do *not* type `http httpsetup` unless you do not have X-Windows installed. Domino 6.5 ships with a new Java installation program that can be run locally or remotely.

If you receive an error message, fix it and then run the installation again, from the start. A typical error message involves either incorrectly specifying the user or group, or failing to create the user or group before beginning the installation. Another common error message concerns lack of disk space.

When the installation is final, you will be returned to the command prompt.

5.3.3 Configure and set up the Domino server

Now that you have successfully installed Domino 6.5, it is time to configure and set up the server. Log out as `root` and log back in under the `dwalinux` account so that it, and not root, owns the X-Windows session.

Setting the Linux PATH environment variable

Normally, commands are given with the full path, such as /opt/lotus/bin/server for the server executable. Linux searches your PATH environment variable for executables, so you add /opt/lotus/bin, as well as the current directory, to your PATH. Make certain you are logged in with the Domino user account and not as root. You can check this by issuing the command **`whoami`** or **`id`**.

1. Start the Kate editor (Figure 5-33).

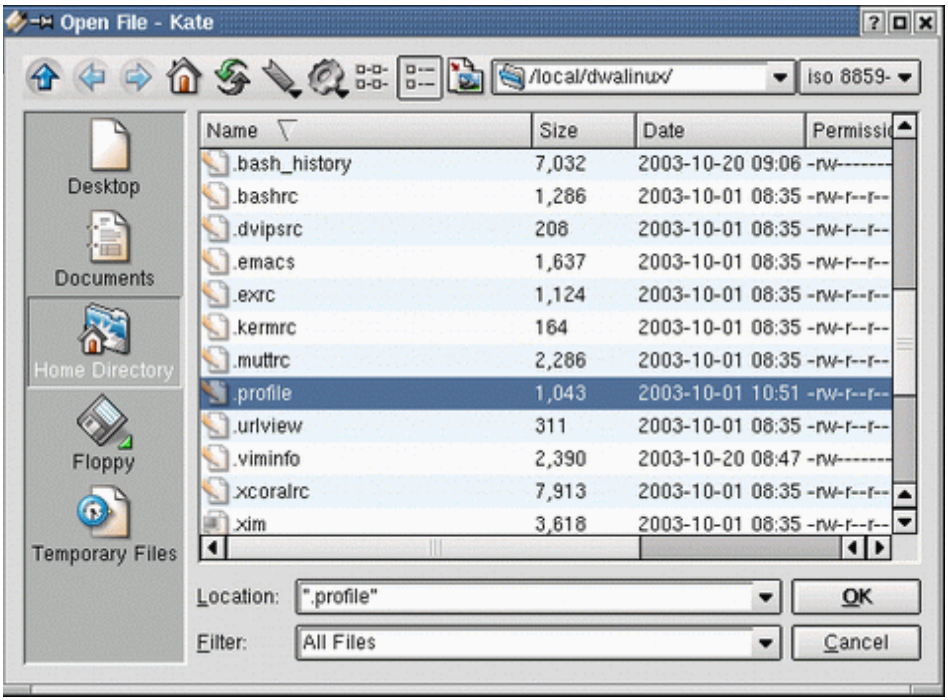


Figure 5-33 Kate Open File dialog box

2. The program automatically begins with a new file (this file should be called `.bash_profile`, as shown later) so that all you have to do is enter the following line:

   ```
   export PATH=$PATH:/opt/lotus/bin:/local/notesdata:
   ```

   This preserves the existing path and simply appends our additions.

Note: Linux code is case-sensitive, so PATH must be uppercase.

3. Click **OK**.
4. Log out and log back in for the changes to take effect.

Note: If you started X-Windows from the **startx** command, make sure that you log out; do *not* just restart X-Windows. To log out, use the **exit** command or **ctrl-d**.

5. You can confirm that the PATH variable was set correctly by launching a shell and typing `echo $PATH` at the command prompt. To verify that you are using the Domino server executable, type `which server` and check the path.

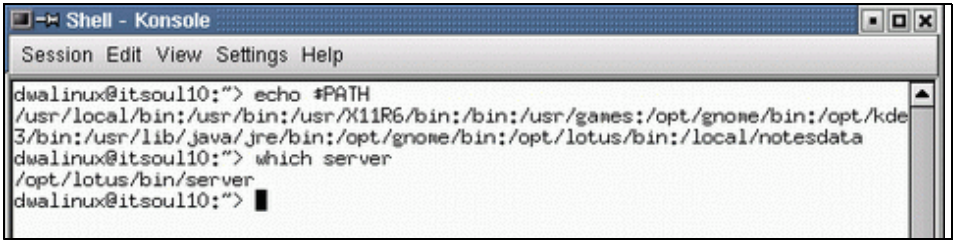


Figure 5-34 Showing the echo and which commands

Be sure to change to your Domino data directory (in our case it was the /local/notesdata directory) before starting the Domino Server setup. You must be in the Domino data directory when you start the server.

Note: When the notes user account was set up, the home directory should have been set to the Lotus Domino data path: /local/notesdata.

5.3.4 Set up the Domino server

This section discusses how to set up your Domino server.

1. Log on to your server with the Domino user account (`dwalinux`), change to the Domino data directory (/local/notesdata) and start the Domino server (Figure 5-35 on page 187).

Important: Make sure that the system LANG variable is set correctly for your language (that is, LANG=en_US, LANG=de_DE@euro). To set the system variable, type `LANG=`.

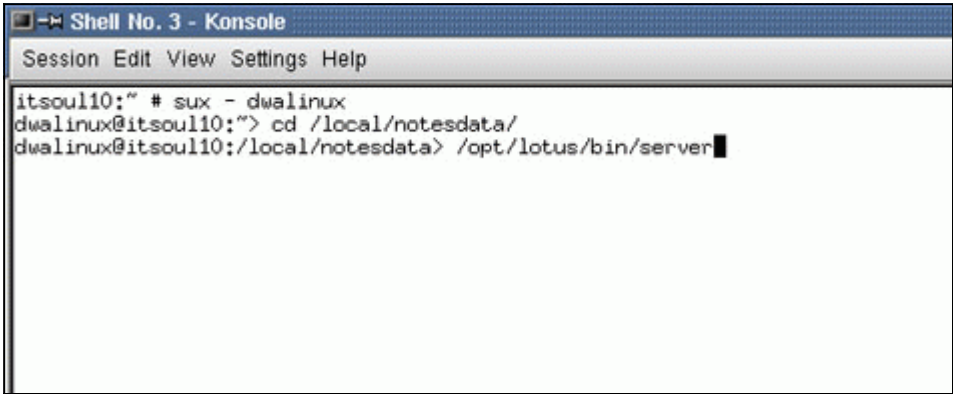


Figure 5-35 Domino server first screen

2. Click **Next** and you will see the screen shown in Figure 5-36.

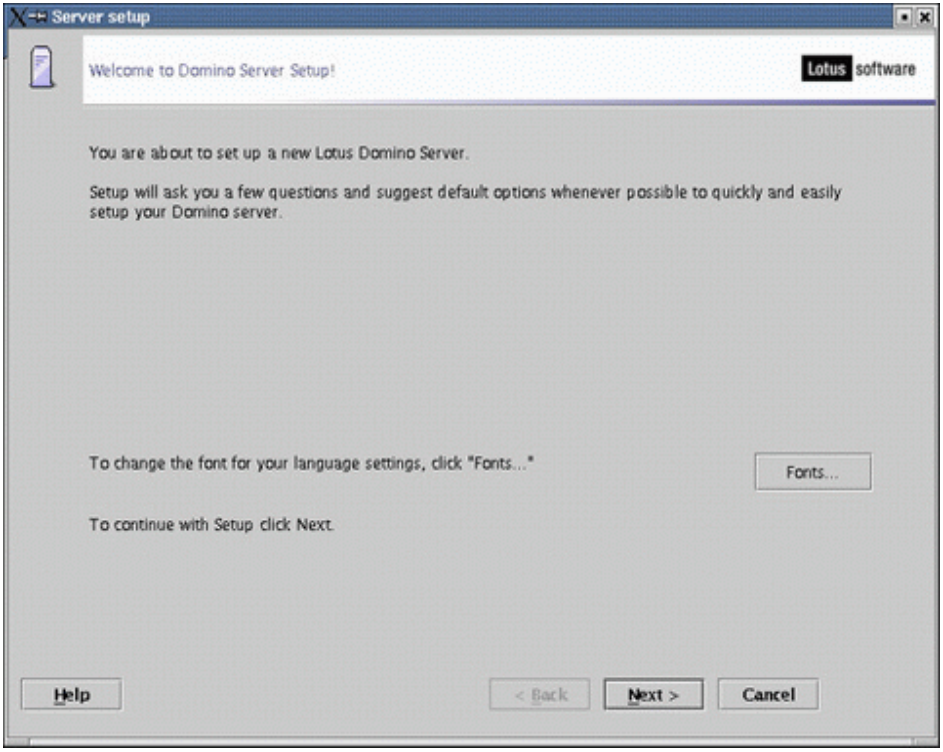


Figure 5-36 Starting configuration

3. You are setting up the first server in what will be your new DWALinux domain. If you are setting up an additional server, you will be prompted to specify the

location of your server ID and the hierarchical name of the additional server, as shown in Figure 5-37. Click **Next** to continue.

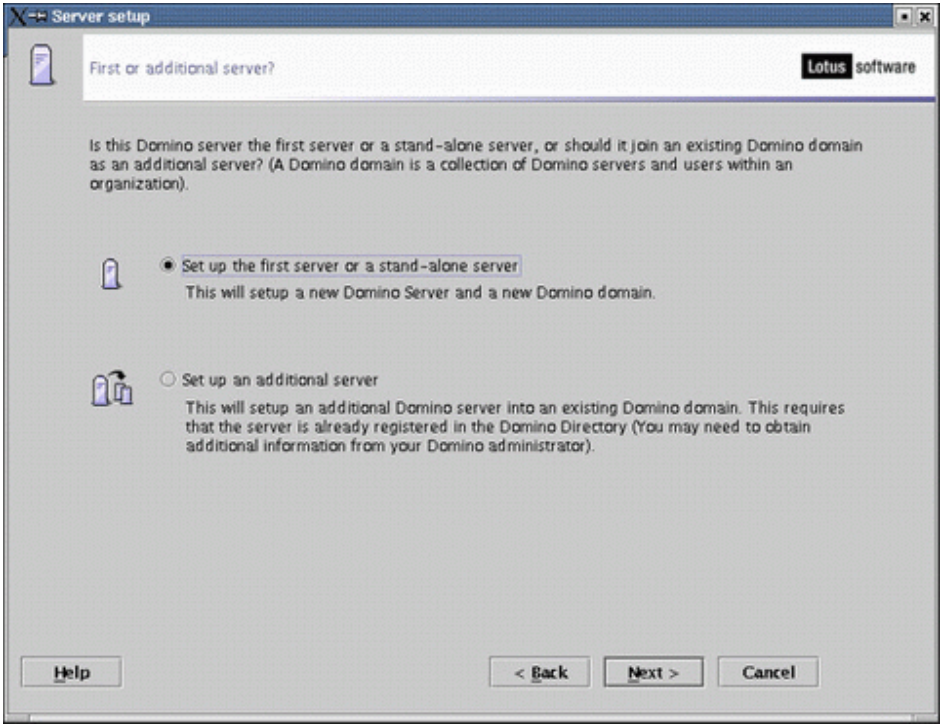


Figure 5-37 First or additional Domino server

4. Enter a server name and server title (Figure 5-37 on page 188). The server title gives you an opportunity to provide a short description of the server's main function or the organization to which it belongs.

   Click **Next** to continue with the installation.

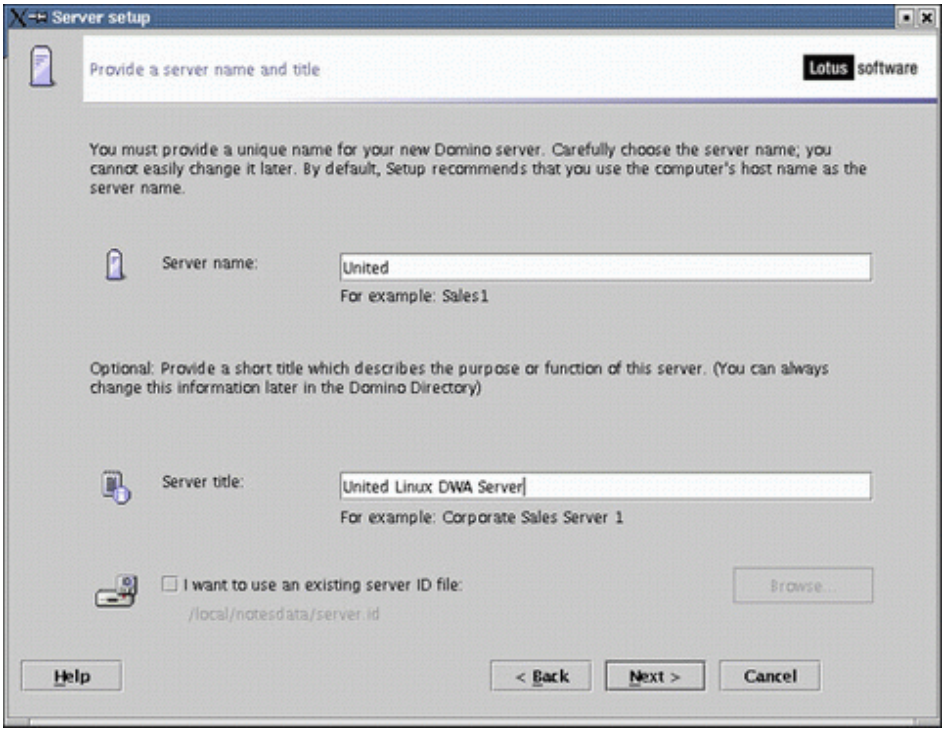


Figure 5-38 Domino server name and title

5. On the next screen (Figure 5-39), set a meaningful Organization name, and make certain to enter a secure password for your Certifier ID.

   If you are rebuilding your Domino domain, check the **I want to use an existing certifier ID file** check box.

   Click **Next** to proceed.

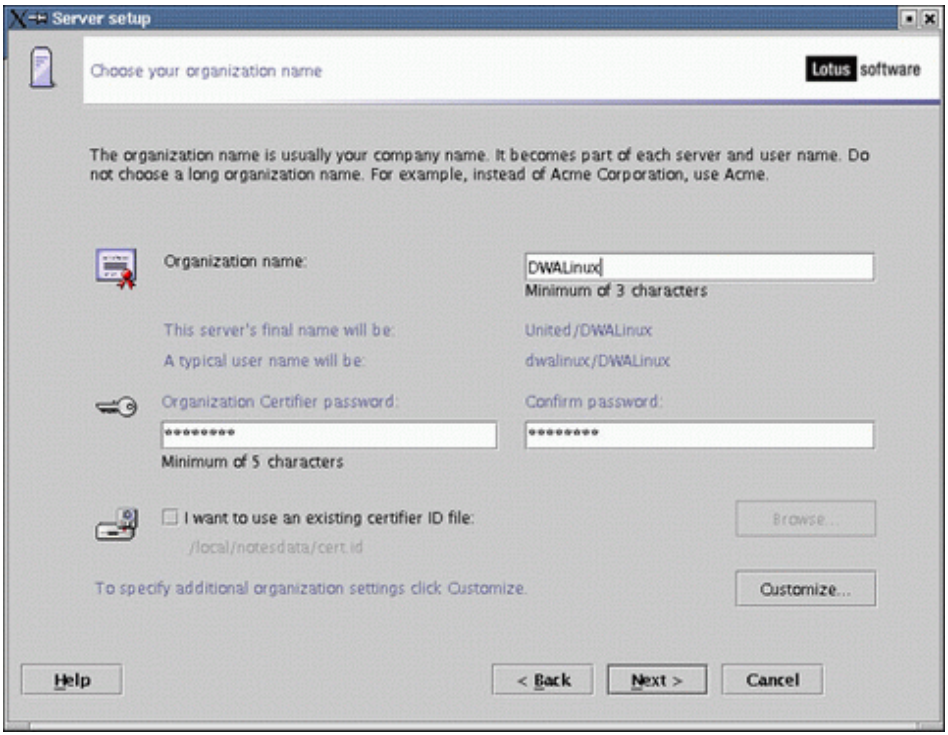


Figure 5-39 Domino organization name

Important: The Certifier ID is the key to all user and server authentication; it should be removed from the server immediately after you have finished the setup and stored in a secure location. You should also rename the file (it will be named cert.id by default) to include the Domino domain name, especially if you manage or intend to manage multiple domains. Do not forget, however, that you will need the Certifier ID in order to create subsequent Organizational Units (OUs). Additional OUs are useful for distinguishing people from servers, as well as distinguishing departments or regions. You should settle on a scheme that minimizes the number of OUs but provides sufficient detail. See *Domino 6.5 Administration Help* for further details.

6. At the next screen (Figure 5-40), type the domain name you would like to use and click **Next**.

> **Tip:** If you intend to have multiple domains, you should decide on a naming scheme now and make certain the first domain conforms to the scheme you will use for all subsequent domains.

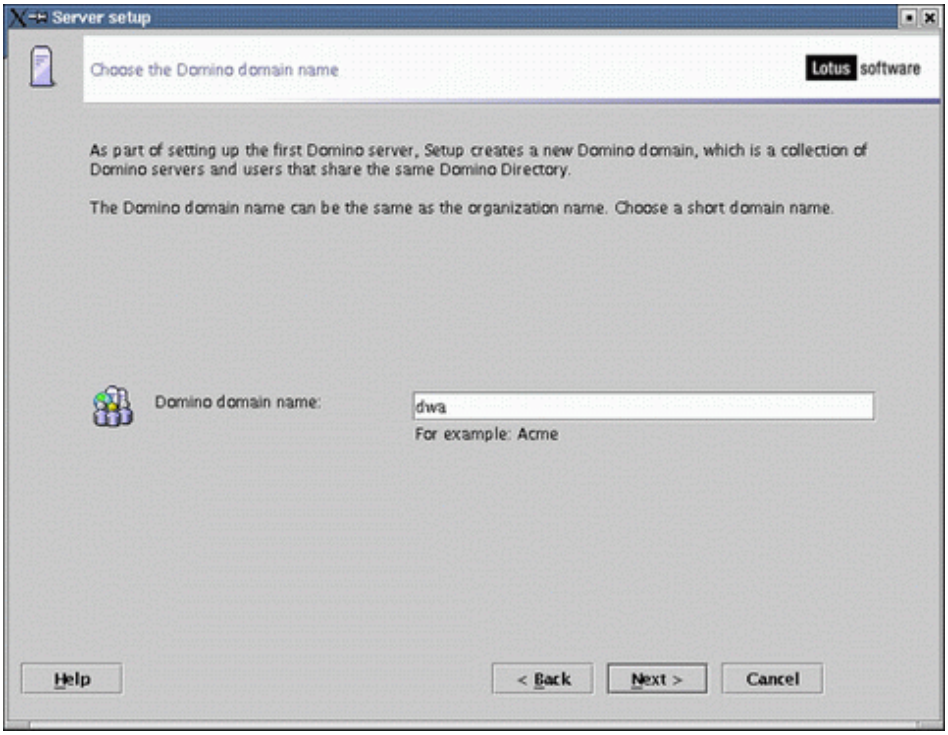


Figure 5-40 Domino domain name

7. Enter an administrator name and password (Figure 5-41), then click **Next**.

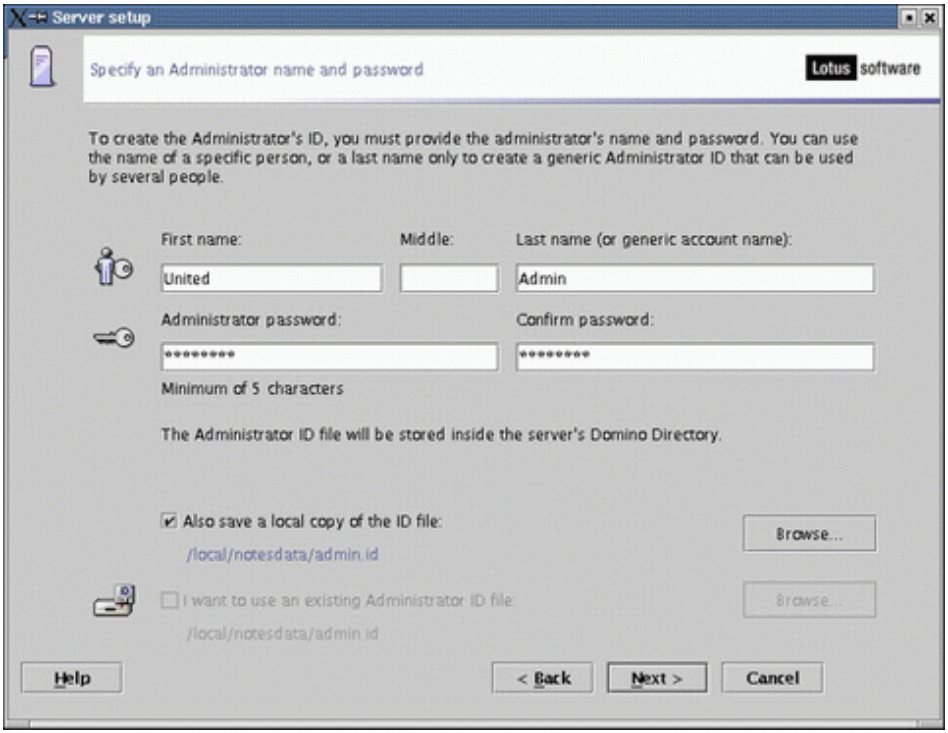


Figure 5-41 Domino Administrator name and password

We opted to create a generic Administrator ID and download it to our client via a Web browser. If you intend to use the ID locally, check the **Also save a local copy of the ID file** option so that you will have easy access to the ID. The Administrator ID will have full access to the Domino Directory, so we removed the ID from the Person document after we downloaded it.

Important: Do not select **Also save a local copy of the ID file** if you are running a remote installation because it will try to access the path you are using locally, which will not exist on the server. There is an option later in the remote setup to copy the ID files to your local workstation.

8. Select all three options shown in Figure 5-42, then clicked **Customize** to further refine your selections.

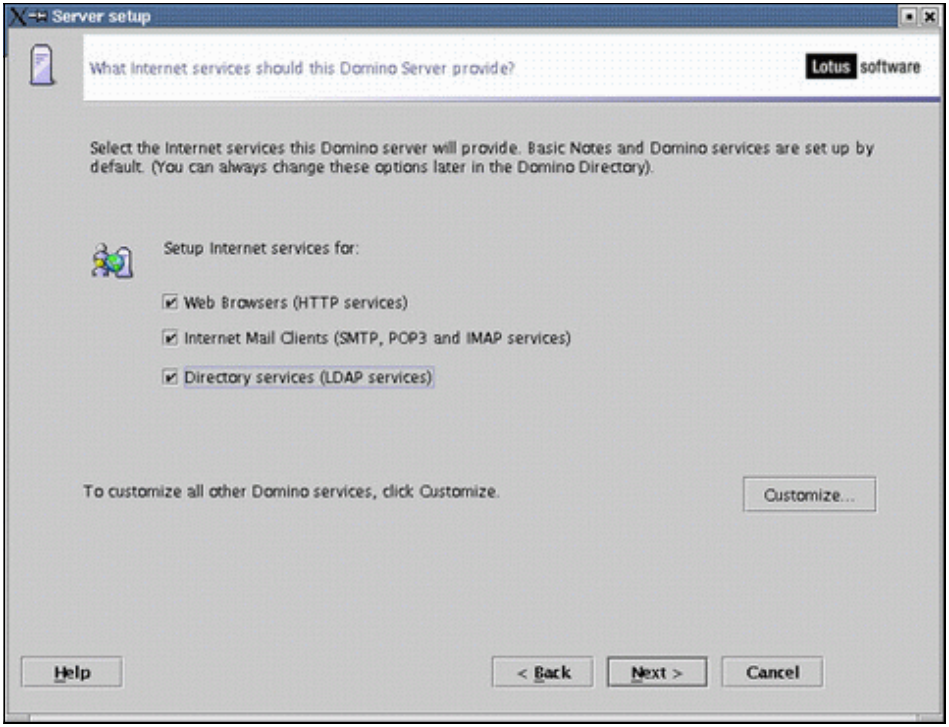


Figure 5-42 Choosing Internet services provided by Domino

9. We selected **Calendar Connector**, **Schedule Manager**, and **Statistics** to provide the features needed for this server. You should consider which services are appropriate for the server you are setting up and select only those that you need.

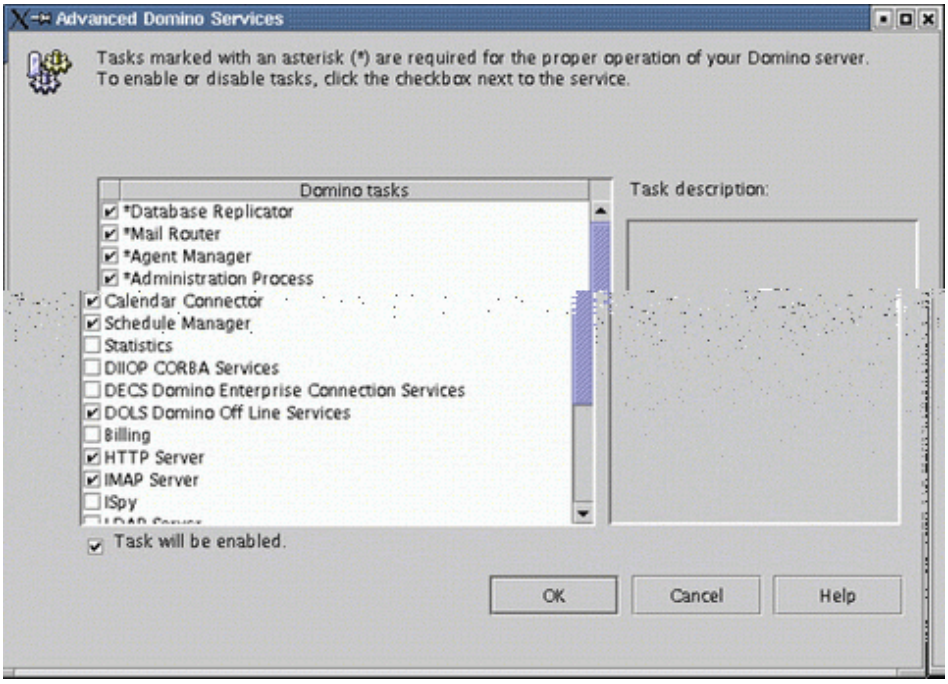


Figure 5-43 Advanced Domino services: Part I

Tip: You can always add a service later by modifying the `ServerTasks=` line of the notes.ini or issuing a **`set config servertasks=`** command from the Domino console. With the **`set config`** command, enter every service you would like to have running, not just the ones to add. You can see the existing services by typing **`show config servertasks`**.

10. Scrolling down the list in same screen, we selected **HTTP** for Web services; **IMAP** and **POP3** for mail client access; **SMTP** for native mail delivery; **LDAP** to provide the Domino directory to LDAP clients; and **Stats** for on-demand statistics. Again, you should select only the services you need based on the intended use of your server. Click **OK**, then click **Next**.

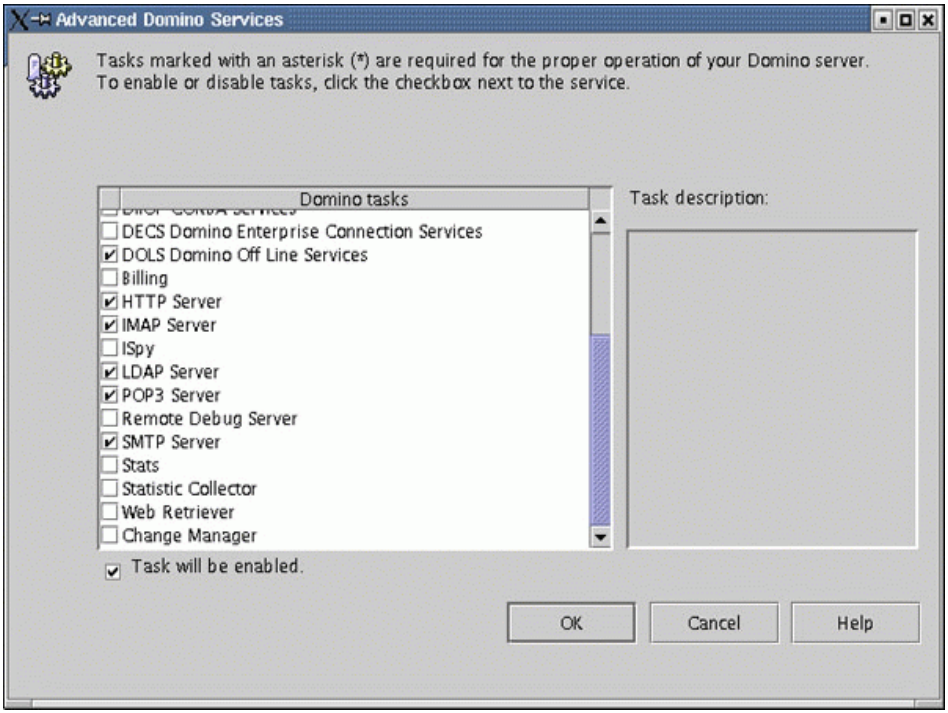


Figure 5-44 Advanced Domino services: Part II

11. The auto-detect correctly determined our network port and host name, as shown in Figure 5-45. We then clicked **Customize** to enable encryption. You would also click **Customize** to correct the detected network ports.

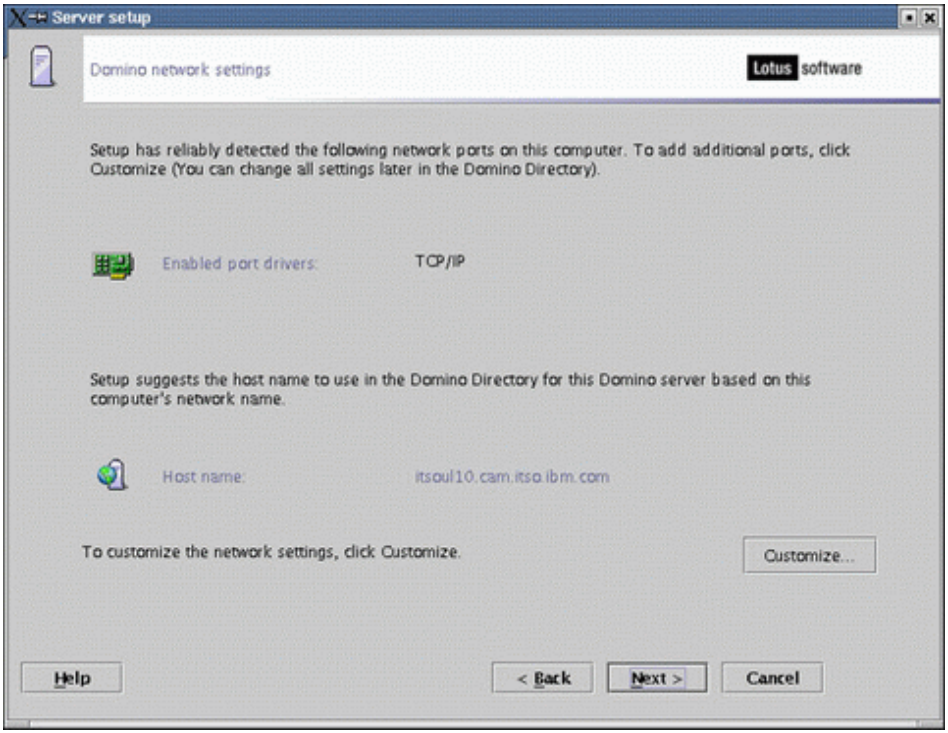


Figure 5-45 Domino network settings

12. We checked the **Encrypt** check box for the network traffic in order to guard against anyone sniffing the packets during transmission. For a WAN server with sufficient processing power and memory, we could have selected the Compress option instead. Click **OK**, then click **Next**.

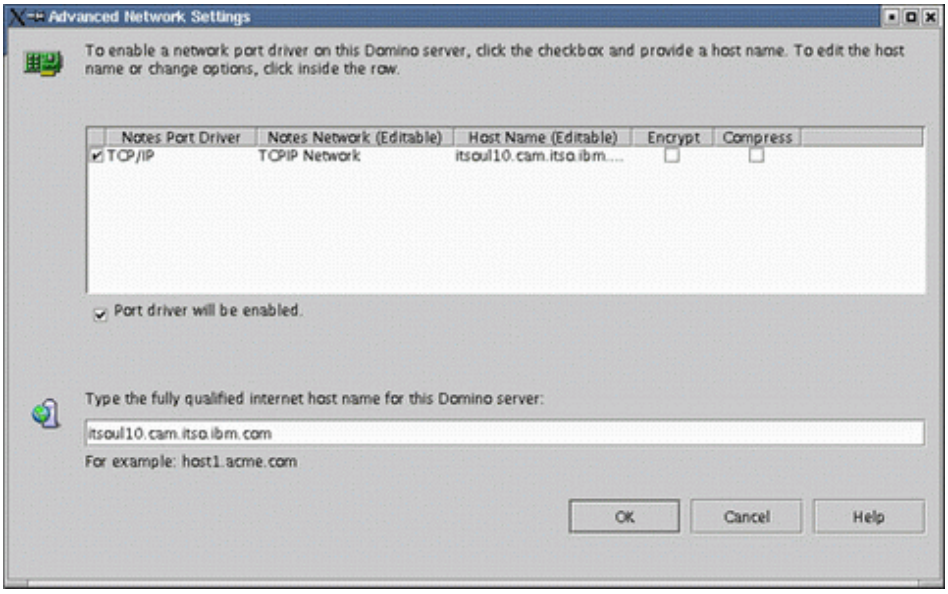


Figure 5-46 Domino advanced network settings

13. To increase security, ensure that the two security boxes in Figure 5-47 are checked (this is the default) and click **Next**.

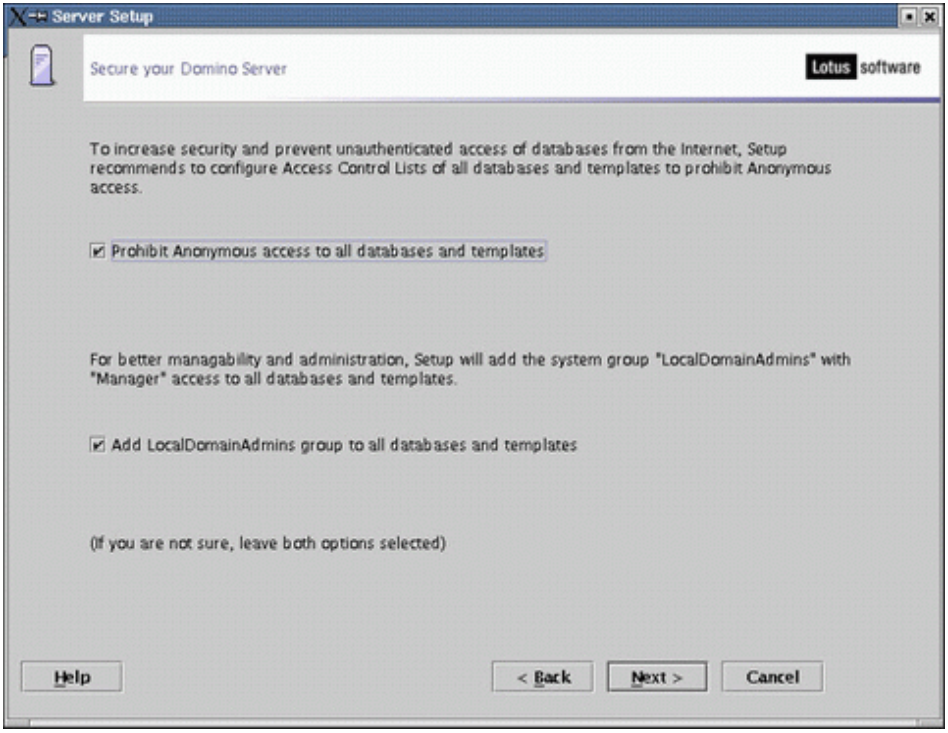


Figure 5-47 ACL settings

14. When you are satisfied the information is correct, click **Setup** to finish the process.

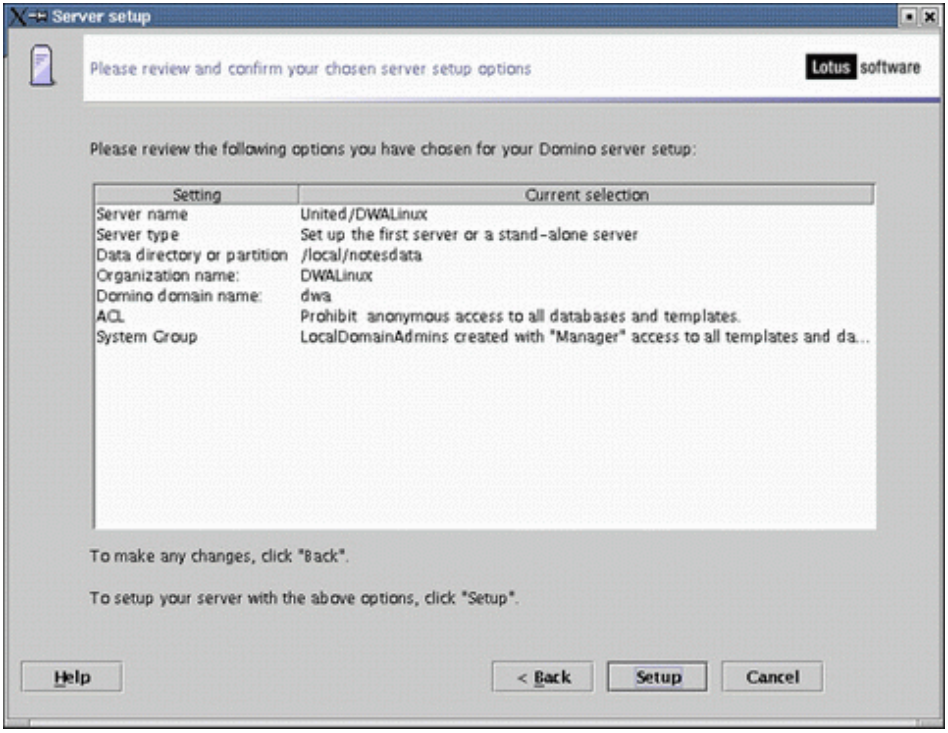


Figure 5-48 Server setup summary screen

15. Click **Finish** to acknowledge that the server setup process is complete (Figure 5-49). You may now start the Domino server and begin the administration process.

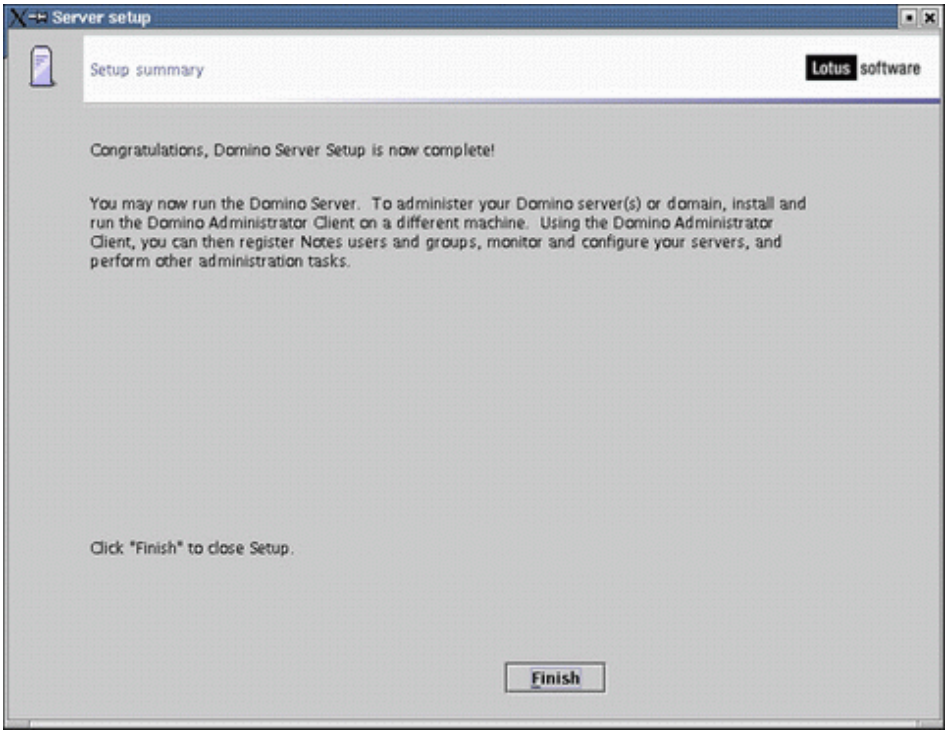


Figure 5-49 Completing the setup

Re-running the Domino server setup

If you need to re-run the setup from scratch, you can remove all lines from the notes.ini after the `CleanupScriptPath=` line, and run /opt/lotus/bin/server again.

This, of course, means that you will lose all previously configured information and customized notes.ini settings.

5.3.5 Starting the Domino server

To start the server, you can simply run `/opt/lotus/bin/server` from a command prompt. This starts the program running in the foreground, and you should leave the shell window open until the program is complete.

An alternate way that offers more administrative flexibility is to run it using the Java Domino Console. To start the server with the Java Console, issue the **`server -jc &`** command.

This command launches all three components: the Domino Server itself, the Domino Controller, and the Domino Console. Those familiar with the Win32 Domino Administration client will recognize the interface.

Note: Java Domino Console is new to Domino 6 and it replaces the cconsole, which was the built-in console program in Domino R5. The **`cconsole`** command is still available if you do not have access to a GUI system. See the *Lotus Domino R5 for Sun Solaris 8,* SG24-5969 redbook for more information about the **`cconsole`** command.

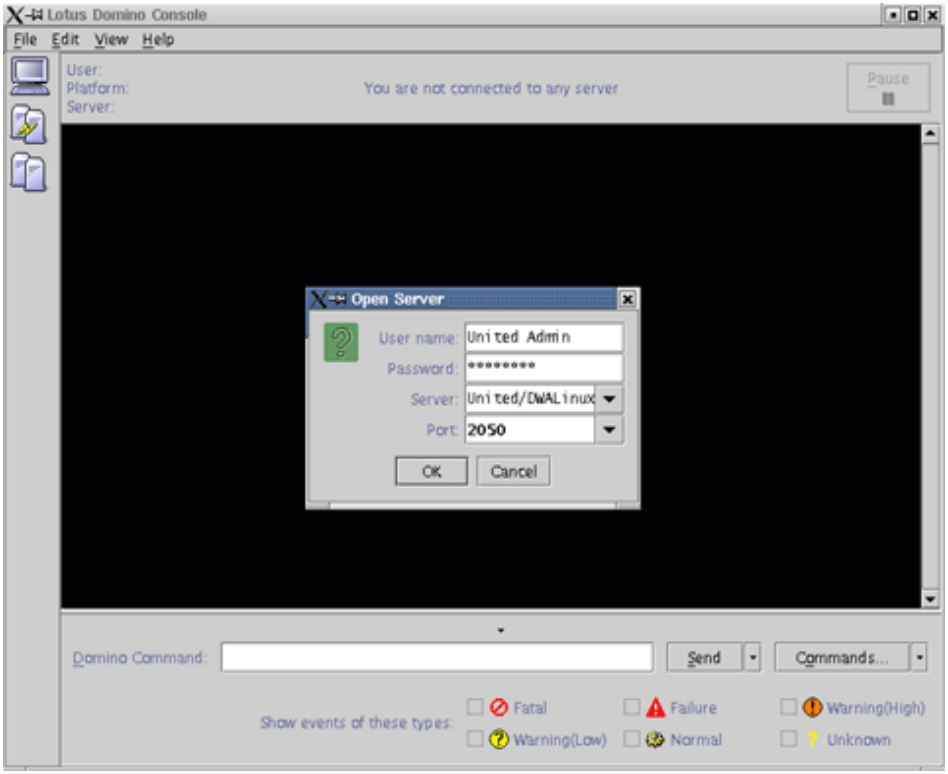


Figure 5-50 The new Domino console

Essentially, the Controller runs on the server and listens for connection requests from the Console. When it receives a connection request, it authenticates the connection using information that it has cached from the Domino Directory, then

allows access to the server and the Linux environment according to the rights granted in that particular server document.

In this case, we launched the Java console as part of the initial server startup, so we were granted rights as a local administrator. However, you can start the Domino Console at any time, either locally, or remotely on systems where the Notes client is installed. To do so, run **`jconsole`**.

Even when the Domino server has been shut down, you can start it again if the Domino Controller is still running. All of the data between the Console and the Controller is encrypted using SSL.

Starting Domino from a script

We recommend that you start Domino from a script. This ensures that the server is always started when the system is rebooted. Starting Domino via a script is akin to the service feature available with Windows NT. The advantage of a script over a pre-defined GUI or simple command-line execution, is that you can configure the script to carry out specialized tasks and to start Domino in the manner best suited to your operating environment. In the scripts we provide as an example, we check to see whether the Domino Controller, Domino server, or both are already running, and if so, take the correct action accordingly. A script can be used to do any number of other tasks, such as archiving old log files, e-mailing notification to an Admin when the server starts, and so on.

Attention: You do not need to use these scripts if you installed the UnitedLinux Extension Pack for Lotus Domino. That package contains similar startup scripts that are configured automatically when the package is installed. See 5.1, “Preconfiguring your Linux server: the easy way” on page 154 for more information.

The startup script included here can be downloaded from the Redbooks Web site. See Appendix C, “Additional material” on page 443 for information about downloading this file.

To install this script on your Linux system:

1. Log in to the system as `root`.
2. From a shell command line, navigate to /etc/init.d (issue the command **`cd /etc/init.d`**).
3. Copy the Domino file from the Web site into this directory using FTP or SSH, or create a new file with a text editor and paste the text of the script into it.
4. After you have copied or saved the file (it should be named `domino`) set the permissions and the owner. These should be the same as the other files in

the /etc/init.d directory. This is usually root:root for the owner and group and -rwxr-xr-x for file permissions.

5. Issue the command **chkconfig --add domino** to register the script with the Linux startup process.

The domino startup script is meant to be run automatically during system startup. If you need to restart Domino without rebooting the entire system, use the startserver script. The startserver script should be placed in the Domino data directory and given execute permissions as outlined in Step 4. However, the owner should be the Linux account used to run Domino and the script should be started by that account as well.

Example 5-1 domino script example

```
#!/bin/sh
#
# A startup script for the Lotus Domino server
#
# chkconfig: 345 95 5
# description: This script is used to start the domino \
# server as a background process.\
#
# Usage /etc/init.d/domino start|stop

# You should change the 3 following variables to reflect your environment.

# DOM_HOME is the variable that tells the script where the Domino Data resides
DOM_HOME=/local/notesdata

# DOM_USER is the Linux account used to run the Domino server
DOM_USER=notes

# DOM_PROG is the location of the Domino executables
DOM_PROG=/opt/lotus/bin

start() {
   echo -n "Starting domino: "
   if [ -f $DOM_HOME/.jsc_lock ]; then
                rm $DOM_HOME/.jsc_lock
        fi
   su - $DOM_USER -c "$DOM_PROG/server -jc -c" > /dev/null 2>&1 &
   return 0
}

stop() {
   echo -n "Stopping domino: "
   su - $DOM_USER -c "$DOM_PROG/server -q"
   return 0
```

```
}

case "$1" in
start)
   start
   ;;
stop)
   stop
   ;;
*)
   echo "Usage: domino {start|stop}"
   exit 1
esac
```

6

Security and administration

Domino Web Access security begins with both Linux OS and Domino server security. We discuss these foundations briefly but try to focus on the security considerations unique to a Domino Web Access environment. A complete Domino Web Access security discussion must include both a server component and security concepts for the client files and workflow. Accordingly, we touch on both sides of the equation.

Similarly, Domino Web Access administration also begins with both Linux OS and Domino server administration. However, there are fewer Domino Web Access administration-specific considerations than there are security considerations. Domino Web Access administration is tied very closely to general Domino server administration. We will therefore cover some general topics that pertain mainly to Domino, with additional information relative to Domino Web Access where appropriate.

6.1 Linux security

Linux security (as with any other OS security topic) is a much more in-depth discussion than this book is intended to cover. Many other resources are focused on the topic and should be consulted for a more complete picture of the various aspects of Linux security. Some good references can be found at

http://www.linuxsecurity.com

With that said, there are a few basics we think we should cover. There are various levels of security such as:

Physical security Applies to the concept that the actual server hardware has to be safe from unauthorized access (in other words, locked in a room somewhere)

System security Applies to the concepts related to user account access: password protection, file permissions, and so on

Network security Applies to the concepts related to network traffic to and from the server: locking down network ports, firewalls, proxy servers, private LANs, and so on

Backup security Applies to the concepts related to securing and preserving your data: encryption of backup tapes/files, physical security of backups, and so on

6.1.1 System security

System security in Linux begins with the concept of user levels. There is the root user, which is the equivalent of the Administrator account on a Windows OS, and then there is everyone else. The root user is intended to be able to do anything he or she wants. Domino must be installed by the root user, and some tuning we require has to be done by root, but other than that, Domino should be confined to the permission levels granted to an account created specifically to run Domino. This brings us to the concept of file permissions.

File permissions

In Linux almost every resource (files, directories, symbolic links, disks, modems, and so forth) is considered a *file*, and file permissions give access to the resource. From a shell, you can view the permissions of a file if you issue the command **ls -l** at the command line, as shown in Example 6-1.

Example 6-1 Example of file permissions for /etc/passwd

```
   # ls -l /etc/passwd
-rw-r--r--  1 root  root    873 Apr  4 15:27 /etc/passwd
```

The **ls** command is similar to **dir** in MS-DOS. Using the -l flag, it prints the file name, file type, permissions, number of hard links, owner name, group name, size in bytes, and time stamp (by default, the modification time). The type and the permission is the cryptic string of letters and dashes at the beginning of the example above. The first character of the 10-character-long code is the type of the file; in this case it is a dash, which means that this is a plain file. The possible file types are:

-	Plain file
d	Directory
l	Symbolic link (such as a Windows shortcut)
b	Block device (drives)
c	Character device (terminals, modems)

The next nine characters describe the permissions on the file. They are organized in groups of three. The first group indicates what permissions the owner of the file (in this case the user root) has. The second indicates the permissions the group (in this case the group root) has, and the last three characters give the permissions for any other user on the system.

A group of three characters is built as follows:

- First character is an **r**, which means permission to read the file.
- Second is a **w**, which stands for write permission.
- The last character is **x** for execute rights on a program or list rights if the file is actually a directory. Also **s**, **S**, **t**, and **T** are possible values for this character, but these permissions are less frequent and beyond the scope of this book.

In our example, the permissions **-rw-r--r-- root root** mean read and write access for the user root, read rights for anyone who is a member of the group root, and read rights for any other user on the system.

On a Linux system, ordinary users only have write access to their $HOME directory (also known as ~) and the /tmp directory. This is different on Windows NT systems, where every user has access to all of the disks except where access has been specifically denied. Because the Domino server runs as an ordinary user under Linux, you have to be sure that ownership of files and directories is set correctly. This applies to any directory hierarchy that Domino may try to read or write from, such as a separate file system that stores transaction logs. The transaction log directory should be owned by the Domino administrator user, and given write permission.

Network security

Network security is a particularly prevalent topic of concern, given the client/server nature of Domino and Domino Web Access.

Basic network security

In the UNIX system world, software that is able to connect to (exchange information with) other software on the same system or another system is called a daemon. Usually, the daemon listens on a specified IP address and port; Domino Web Access uses port 80, which is the default HTTP port. A server normally has many daemons running at the same time, such as the ftp daemon, telnet daemon, and so forth. Through these daemons, another system can connect to the server and exchange information.

Daemons have two categories: those started by the root user; and the rest, which are started by other users. The daemons started by root listen on ports below 1024. Minimizing the number of daemons run by root is an important step in securing your server. After the installation of Linux, there may be many ports open by default, depending on what the administrator chose to enable during the installation. To increase security, as well as performance, you should stop daemons that you do not need.

In Table 6-1, we explain some of the frequently used services available for Linux. On a Domino server, you will not need to run many of these daemons. In the table, the column labeled **Enable?** indicates whether we recommend this daemon for a Linux Domino 6.5 server.

Tip: You can always enable a service, such as **`ftpd`**, when you need to transfer files and then disable it when you are done.

Table 6-1 Linux daemons

Name of the service	Enable?	Observations	Port
crond	Yes	It runs user-specified programs at periodically scheduled times. It it useful for log rotation, for example.	N/A
ftpd	No	This is an FTP (file transfer protocol) daemon common on SUSE. Use it to move files from one server to another. You can use the **`scp`** command with an SSH shell.	21
gpm	Yes	It adds mouse support to a text console.	N/A
httpd	No	Linux Web server.	80
ipchains	No	Firewall tool.	N/A
iptables	No	Firewall tool.	N/A
keytable	Yes	It loads the selected keyboard map.	N/A

Name of the service	Enable?	Observations	Port
kudzu	No	This runs a hardware probe akin to plug and play. After you install your server hardware, you can turn this off.	N/A
lpd	No	Print daemon.	515
network	Yes	Activates and deactivates all network interfaces configured to start at boot time.	
nfs	No	A file sharing protocol across TCP/IP.	2049
sendmail	No	An SMTP server.	25
snmpd	No	A management protocol. You should enable this daemon only if you have implemented SNMP.	161
ssh	Yes	A secure shell for remote administration. Use it to remotely administer the server from a shell.	22
syslog	Yes	The facility by which many daemons log messages to various system files.	N/A
telnet	No	A shell for remote administration. Use SSH for secure remote administration.	23
wu-ftpd	No	An ftp (file transfer protocol) daemon. It can be used to move files from one server to another. Alternately, you can use the **scp** command within an SSH shell.	21
xfs	Yes	The X Font Server.	N/A
xinetd	Yes	Runs other daemons on demand.	N/A

Starting and stopping daemons

Starting and stopping daemons can be done by logging in as root to KDE and launching the SysV - Init Editor by selecting **Start Application** → **System** → **SysV Init Editor** on Red Hat Advanced Server 2.1. (See Figure 6-1 on page 210.). The ksysv tool, which that menu selection actually runs, was not installed by default on our UnitedLinux server. One of the strengths of UNIX-like operating systems is that you can do just about everything from the command line if need be, including starting and stopping daemons. Most variants of Linux (including UnitedLinux) have small scripts that are used at boot time to start services. These can also be run after the system has been brought up successfully. These can be found in /etc/init.d, and they accept certain flags,

such as start and stop. So, to stop sendmail, for example, as root you can run the following command to shut down sendmail:

```
/etc/init.d/sendmail stop
```

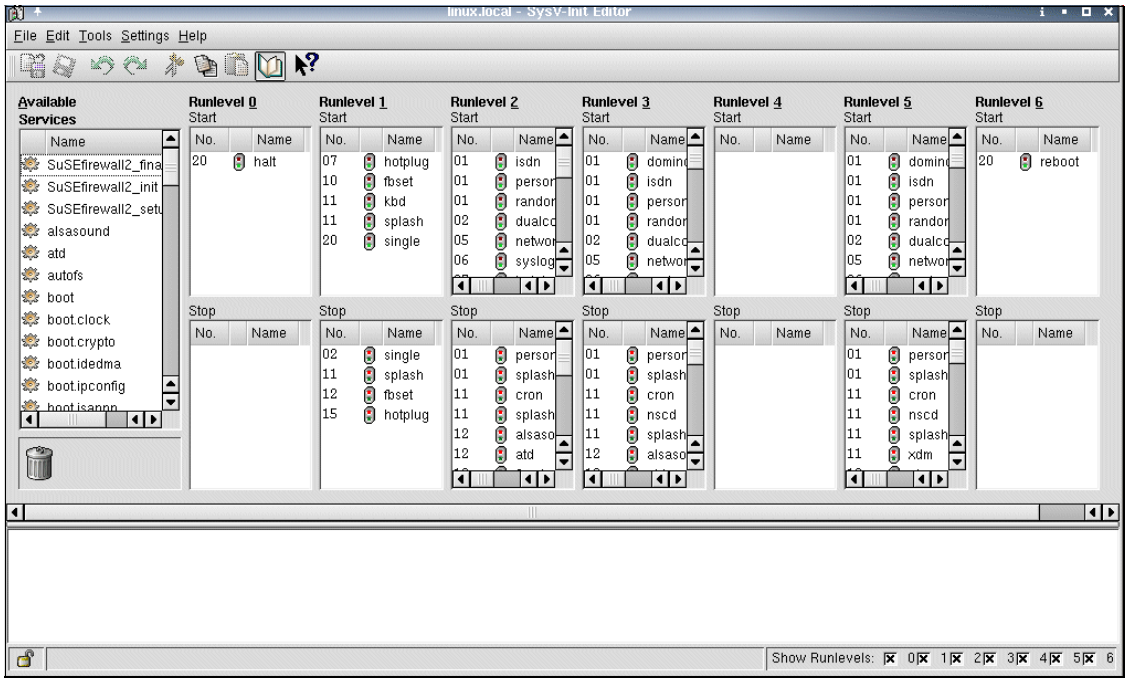


Figure 6-1 SysV Init Editor

Runlevels and services

Before using the SysV Init Editor you should first understand runlevels. Windows really has only two runlevels: Recovery and Normal. *Recovery* is only used when there is a problem with the system. Most of the time Windows runs in *Normal* mode.

Linux usually has six runlevels. Runlevel 0 (zero) is used to shut down the server; runlevel 6 is used to restart the server. Runlevel 1 (Single user mode) is used like the Windows recovery mode. Most systems normally run at runlevel 3 (command line) or runlevel 5 (X-Windows).

The top row of boxes in Figure 6-1 shows the services that start when the system enters each runlevel, and the bottom row of boxes shows what services will be stopped when the system enters that runlevel.

Note: A service should *not* appear in both the Start and Stop boxes for a runlevel.

To stop or start a service, click on the service (see Figure 6-1 on page 210) and then go to the Service tab and click the **Start** or **Stop** button (see Figure 6-2).

To prevent a service from starting when entering a runlevel, drag and drop the service from the runlevel to the Trash can.

To start a service when entering a runlevel, drag and drop the service from the Available Services list to the Start box of the appropriate runlevel.

To stop a service when entering a runlevel, drag and drop the service from the Available Services list to the Start box of the appropriate runlevel.

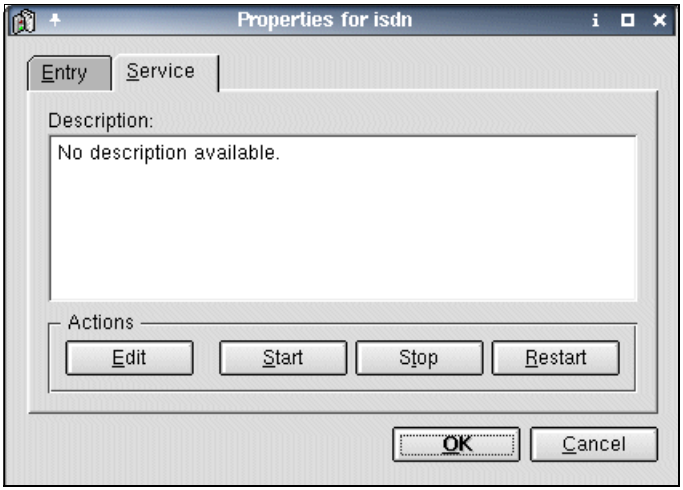


Figure 6-2 Start or stop a service

Showing running daemons

To see what daemons are listening (accepting connections) on your server, log in as root and issue the command **`netstat -a | grep "LISTEN "`** as shown in Figure 6-3 on page 212. In this way, you can always check to see if your daemons are listening.

Note: Linux is case-sensitive, so LISTEN must be uppercase in this example.

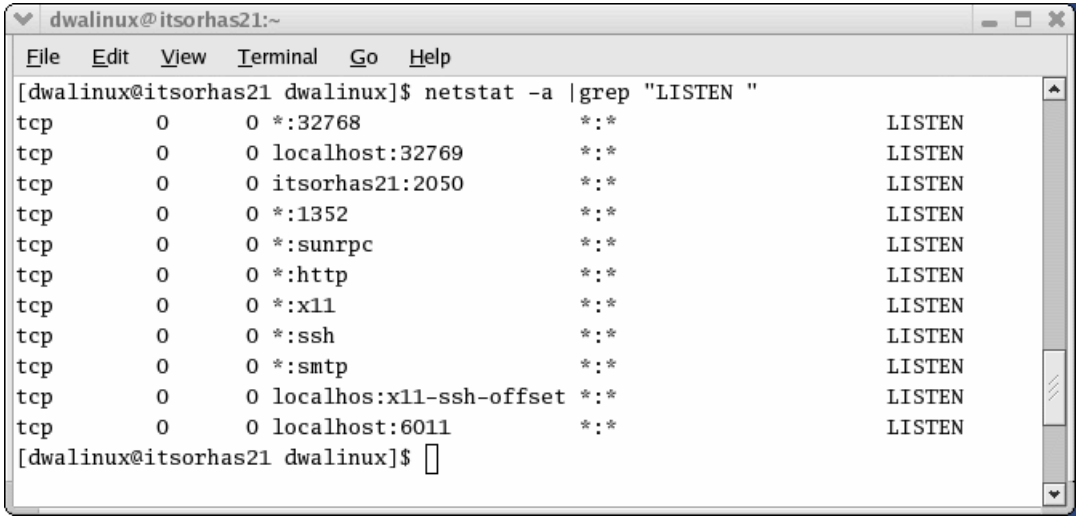


Figure 6-3 netstat -a | grep "LISTEN " command output

6.2 Linux administration

Linux administration is another vast topic that is beyond the scope of this book. There are, however, some concepts that we believe will benefit anyone trying to administer a Domino Web Access server.

6.2.1 Scripting

In this section we describe how to create a shell script. Shell scripts are a powerful method by which to customize your Linux server. As an example, we create a simple script. This script will erase the log files that are more than two months old. Example 6-2 gives the actual code.

Note: Each shell has its own syntax for scripts. The scripts we created are made for the **BASH** shell.

Example 6-2 Log eraser

```
#!/bin/bash

## Log eraser ##

LPATH=/var/log
NR_OF_DAYS=60
```

```
for i in 'find $LPATH -atime +$NR_OF_DAYS'
do
rm -f $i
done
```

- The first line `#!/bin/bash` tells the environment that the script will run. This line is to be treated as is and should not be modified.
- The sixth line sets the variable `LPATH` to equal /var/log, and the seventh line sets the variable `NR_OF_DAYS` to 60. We recommend that you use variables because it makes it easier to debug your script.
- **$**LPATH and **$**NR_OF_DAYS indicate that you wish to use the value of the specified variable.
- `find $LPATH -atime +$NR_OF_DAYS` searches in the /var/log directory for files that are older than 60 days.

> **Note:** For more information about `find` consult the man page: *man find.*

- Next is a `for` loop. For every value of **`i`**, we will run the command `rm -f $i` which will remove every file specified by the value of `i`.
- Lines that start with a `#` are comments but there are special cases, such as the first line or the comments utilized by the **`chkconfig`** command.

Save the file as log_erase.sh. We recommend that you create a directory, such as /scripts, in order to keep your scripts in a single location. To be able to execute the script, you have to modify the rights of the file. Run the command **`chmod 700 /scripts/log_eraser.sh`**. You will be the only one who can read, write, and execute the file.

> **Tip:** The `7` in the **`chmod`** command comes from adding the numerical values of the read(4), write(2), and execute(1) permissions together: 4+2+1 = 7. The two zeros in the **`chmod`** command indicate that the group and the world (all other users) have no rights to the file. This parallels the division of file permissions described in “File permissions” on page 206.

To run the script, you would type `/scripts/log_eraser.sh` if you placed the file in the /scripts directory.

Attention: This script is intended primarily as an example that can be adapted to other situations. Although it works, you might want to consider a more sophisticated algorithm for the management of your log files, or use the built-in logrotate daemon.

6.2.2 Remote administration

Linux servers can be administered remotely and there are many software programs available for this. VNC is one of the more popular.

VNC

VNC is remote-control software that can be used on a Linux server. You can download the VNC tool, as well as obtain more information about it, at:

http://www.realvnc.com/

VNC may already be installed on your system. On our Red Hat Advanced Server system, VNC was installed with the OS and put in /usr/bin. On our UnitedLinux system, the binaries were found in /usr/X11R6/bin. If you do not have VNC installed, grab whichever package version you prefer (tar or rpm) from the Web site, and install as root. Using the tar file format, you can execute:

```
tar zxvf vnc-<version>-x86_linux.tar.gz
```

where *<version>* is the VNC version you downloaded. This should create a vnc_<version> directory that will contain the necessary files. To install them to a general location that most users can access (for example, /usr/local/bin), it comes bundled with an install program that can be used to install the files in the proper locations. Execute:

```
vncinstall /usr/local/bin /usr/local/man
```

This installs the VNC binaries to /usr/local/bin, and the man pages (help files) to /usr/local/man. If you want to use the Java VNC viewer tool, you also need to copy the Java classes to a location that the binaries can find. The viewer will look for the classes in /usr/local/vnc/classes by default, so create that directory:

```
mkdir /usr/local/vnc/classes
```

then copy all of the classes you unpacked from the tar file to the new directory. From within the vnc_<version> directory:

```
cp classes/* /usr/local/vnc/classes/
```

For more detailed information about installing, refer to the README file included with the VNC distribution.

To start the server, run **vncserver** from a shell. This prompts for a password to be used when connecting from another machine. The machine name and the windows number will be displayed (Figure 6-4).

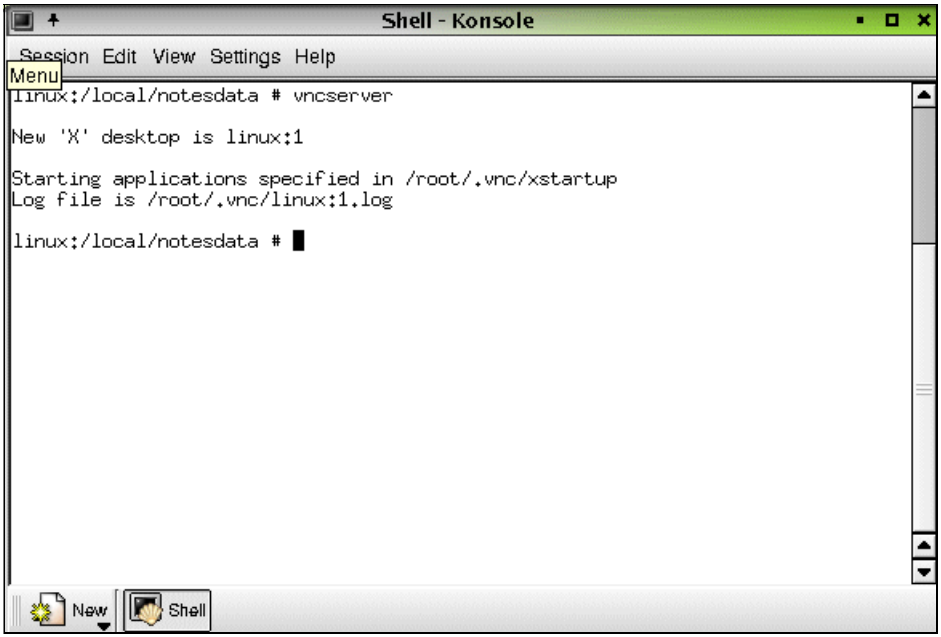


Figure 6-4 Starting VNC server on Linux

To connect to the VNC server, run the VNC viewer on your client and enter the *hostname*:*window* (see Figure 6-5) and click **OK**. Enter the password when prompted.

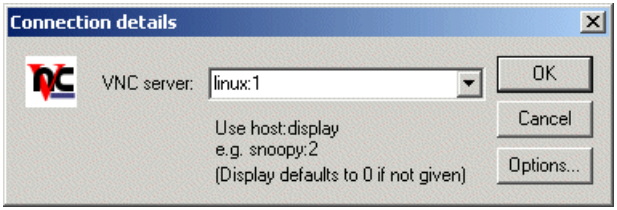


Figure 6-5 VNC viewer

This opens a session to the VNC host and gives you a root shell to use as you please. For more information about securing VNC sessions with SSH, see the article “Making VNC more secure using SSH” at:

http://www.uk.research.att.com/archive/vnc/sshvnc.html

6.3 Domino security

In general, the principles of Domino security are the same from platform to platform. This section provides an overview of initial options available for securing a Domino server.

6.3.1 Domino 6.5 server document

After you have set up the server, open the Domino Directory (names.nsf) and review the server document. This document controls myriad server functions, including security.

The Security tab contains settings such as the following (and others):

- Access server: The default is blank. At the very least, enter the organization name used during setup, which in our case was */ITSO*. This helps to ensure that only those to whom you have issued an ID can access the server.

  Tip: You can add other domains to the Access Server field after you have added the appropriate cross-certification. Remember that a Domino server will not be able to authenticate a user or server from a different organization unless it has a cross-certificate.

- Check passwords on Notes IDs: The advantage of enabling this feature is that when users listed in the Domino Directory lose their Notes ID, they will be able to change the password on the backup Notes ID and prevent the lost ID from accessing the Domino server. The disadvantage is that, as with many security options, it slightly increases the overall administrative burden.
- Create new databases: Enter individual names or, preferably, create an administration group and enter the name of the group. If you leave this field blank, anyone who can access the server can create new databases.
- Create replica databases: Enter individual names or, preferably, create an administration group and enter the name of the group. If you leave this field blank, no one can create new replicas.

  Important: If the Create new database field is empty, it means that anyone can create new databases, but if the Create new replica field is blank, it means that no one can create a new replica.

The Ports - Internet Ports tab contains settings for the following:

- On the Web tab, you can redirect HTTP to SSL after you have the SSL certificates in place. The same is true for the Directory tab and LDAP, as well

as the other listed services. All of these services can be redirected to SSL when the SSL certificates are in place.

The Internet Protocols tab contains numerous options for Web access. Consult the appropriate Lotus documentation for details.

Tip: If you are using a Lotus Notes 6.x client on a Windows machine, you can click and hold the mouse to view pop-up help on many items in the server document.

6.3.2 Database ACLs

You should review the ACLs of at least the following databases: names.nsf, admin4.nsf, and certlog.nsf.

- Set the Default entry to No Access. By doing so, you will force both Notes and Web clients to authenticate. With Default set to No Access, you do *not* need to add an Anonymous entry.

  Attention: For databases where Default is not set to No Access, you should make certain that there is an Anonymous entry set to No Access unless you specifically wish to allow anonymous access, such as with a Web home page or a Web registration database.

- Assign an appropriate User Type to each entry. Make certain to differentiate Person and Server, as well as single (Person or Server) and group entries (Person Group or Server Group). A wildcard entry should be treated as a group.
- Consider using Enforce a consistent ACL for the Domino Directory (names.nsf) and Administration Requests database (admin4.nsf). This will help ensure that only the appropriate administrators make changes to these databases. Enforce a consistent ACL across all replicas also applies to databases that users replicate to their local machines. Therefore users cannot access locally data that they could not access on the server.

  You must be careful with this option because if you accidentally omit the rights to access the database, it cannot be bypassed by accessing the database locally.

  See the Lotus Domino Administration 6.5 help database for more information about using this option and about its limitations.
- Further Domino system control over databases can be managed through the Security tab of the Server document. From there you can assign additional administrative privileges over databases. The added database access these

settings can have should be taken into account when configuring database security. Special attention should be given to the Full Access administrator field if Full Access Administration is being used because it can bypass all ACL settings, including Enforce consistent ACL.

- In order to delegate administrative access to a database based on pubnames.ntf, an administrator will want to look at implementing the Extended ACL (also known as the xACL). This enables you to further restrict access to a database down to the field level. See the Lotus Domino Administration 6.5 help database for more information about xACL.

You should also consider the ACL of log.nsf because quite a bit of information can be gathered from the logs. However, you should balance the need to secure the log.nsf database with the need for Domino administrators and developers to view it. One solution is to set the Default entry to No Access, add a group with Manager access for administrators, and either add your organizational unit, for example */DWALinux, with Reader access or else add a second group for developers and others. Whether the additional overhead of maintaining a second group for developers and others is worth the hassle depends on the location of the server (Internet, intranet, or internal) and the level of logging. Any server not located behind one or more firewalls blocking Internet traffic should be held to much more stringent ACL settings than internal servers.

6.3.3 Notes.ini settings for Domino administration

There are a number of notes.ini variables that help with security as well as administration. While setting these will generate useful information in the log.nsf database, remember that all logging comes with a performance price. Only use the level of logging required for the server.

- log_replication: As with all notes.ini settings, you can add this directly to the notes.ini by adding the line:

  ```
  log_replication=1
  ```

  Or you can issue the following command from the Domino console:

  ```
  set config log_replication=1
  ```

  A value of 1 provides a summary of the replication after it finishes. A log level of 2 is useful when you prefer to know the specific types of changes that were replicated (data, ACL, view design, and so forth).

- log_console: This is set to either 0 or 1. A value of 1 records commands entered at the console.
- log_sessions: This is set to either 0 or 1. A value of 1 records each user session and therefore generates many log entries.

- log_agentmanager: This is set to either 0 or 1. A value of 1 records the start of agents in the log, which is quite useful for troubleshooting.
- log_mailrouting: A value of 20 is normal, although 10 can be used to record minimal information. A value of 30 or 40 should only be used temporarily while troubleshooting a specific mail routing problem.

Important: The notes.ini file must have a blank line at the bottom.

More details about Domino security are in *Lotus Notes and Domino R5.0 Security Infrastructure Revealed*, SG24-5341.

6.4 Domino Web Access 6.5 security

Domino Web Access sessions have very specific security features and considerations. As these sessions are HTTP traffic, an administrator can choose to have users log in to the servers using SSL, for example. We explore some additional ways to make Domino Web Access more secure.

6.4.1 Encrypted mail support

Domino Web Access 6.5 introduces encrypted mail support for its users. By storing their Notes ID within their mail file, users can send and read encrypted mail messages. To enable, the administrator must edit the Configuration Settings document and select **Enable** in the Encrypted mail support field on the Domino Web Access tab. In order for Domino Web Access users to actually be able to encrypt or sign their mail messages, however, they first must make some changes within their user preferences. This can be accomplished through the following steps:

1. Log on to the mail file via a browser.
2. Select the **Preferences** button in the top right of the DWA session.
3. On the **Security** tab, check to see whether the mail file contains the Notes ID. (See Figure 6-6 on page 220.)

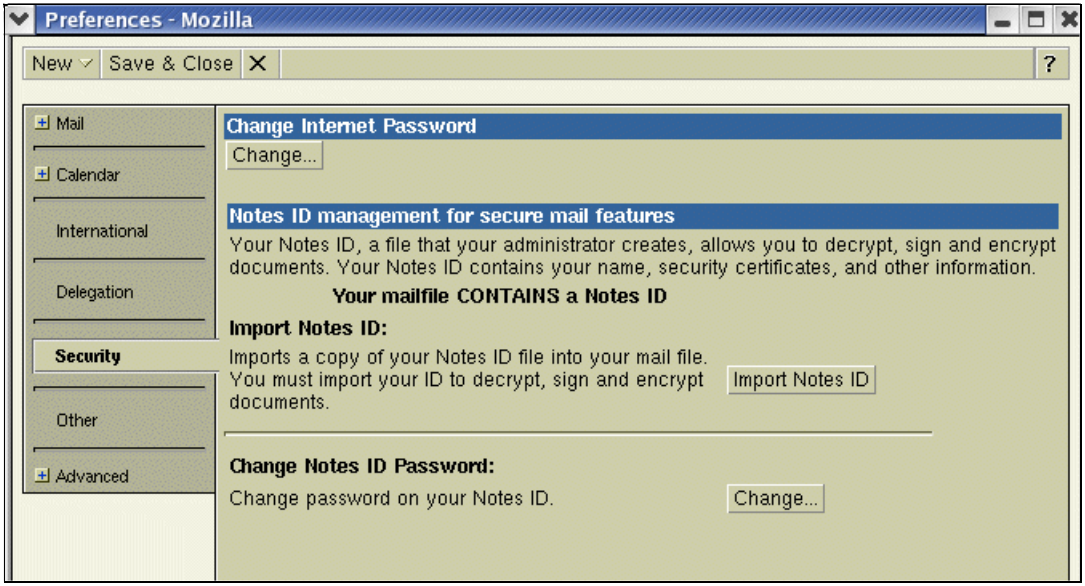


Figure 6-6 Security tab showing that the mailfile contains an ID file

4. If the mail file does *not* contain a copy of your ID, select the **Import Notes ID** button. This opens a dialog box that enables you to browse your local system for the ID file (Figure 6-7). Select it, enter your Notes ID password, and choose **OK**. The Notes ID will be imported into the mail file.

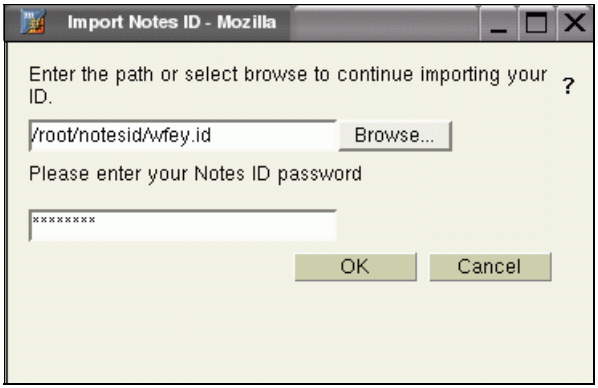


Figure 6-7 Import Notes ID dialog box

5. Select the **Mail** tab in the Preferences window, and the check boxes that toggle signed and encrypted mail should now be available. These are greyed out when there is no ID file present in the mail file.

6. Select one or the other, or both, of the secure mail options (Figure 6-8) and **Save & Close** the preferences.

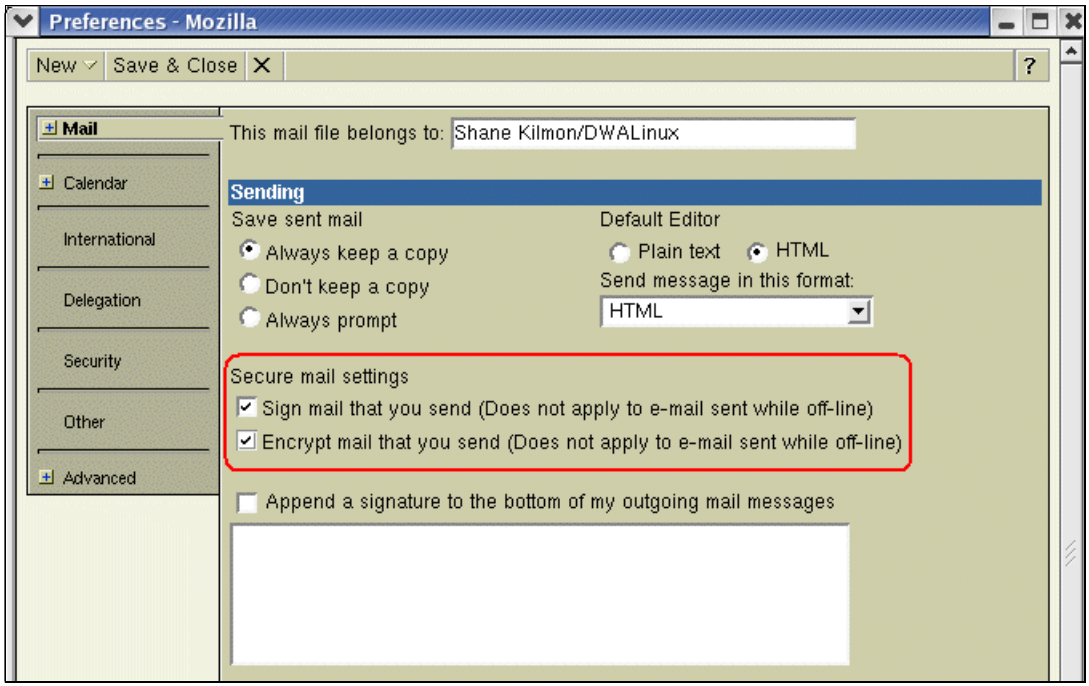


Figure 6-8 Check boxes to Sign and Encrypt all mail

The user should now be able to sign and encrypt mail messages.

Limitations for encrypted mail within DWA

There are some limitations with using encrypted mail in DWA. For example, if you are using SSL connections, or are offline, you will not be able to send encrypted mail. In addition, there are some differences between the secure mail environment of a Notes client session versus a Domino Web Access session:

- Domino Web Access cannot read S/MIME encrypted mail.
- Recovery authority: Domino Web Access does not support recovery authority unless it is already in the ID mailed to the user.
- Imported Notes IDs: Notes IDs cannot be Smartcard enabled.
- Cross certificates: Domino Web Access looks for cross certificates first in the Domino Directory and then in the personal address book. In Domino Web Access, you must create any required cross certificates in the Domino Directory.

- Multiple domains: If you are administering multiple domains, use Directory Assistance for an Extended Directory Catalog.
- Offline: If you are using a directory catalog, you must enable it for encrypted mail.

6.4.2 Secure logout

When closing out of a Domino Web Access session, it is always best to choose the **Logout** button on the top right of the DWA session, rather than simply closing the browser. Using the Logout option clears the browser cache and closes the browser window for you. (See Figure 6-9.) Alternately, the server administrator can choose to redirect DWA logouts to a different Web page. See 11.6.1, “Redirecting users to a Web page after logout” on page 382 for more information about how to configure this feature.

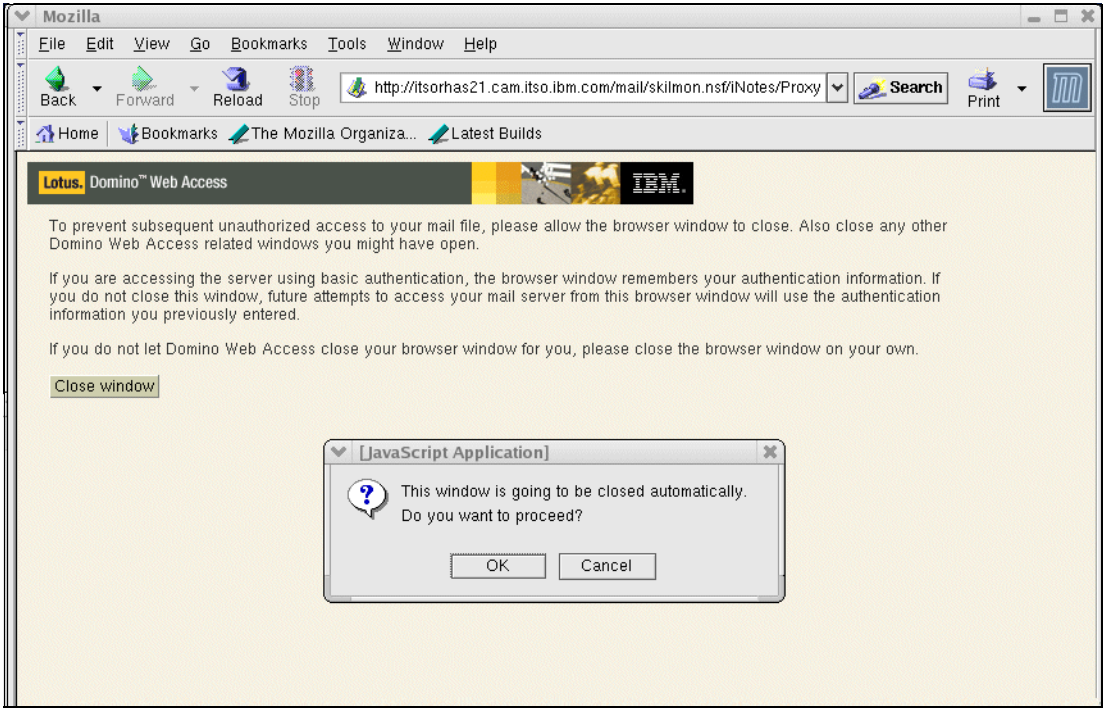


Figure 6-9 Logout screen in Mozilla client

To control how much information gets deleted from the browser cache, Lotus has provided a notes.ini parameter to enable the administrator to configure how secure the logout actually is. To customize, set the following in the notes.ini:

```
iNotes_WA_LogoutScrubType=<value>
```

From the Domino 6.5 Administrator Help, Table 6-2 shows the behavior of each <value>.

Table 6-2 Parameters for logout scrub type

Value	Description
1	Deletes all URLs that begin with the mail file path. This is the best balance between Domino Web Access performance and security. It does not affect caching used by other Domino or other Web applications, nor does it affect caching of pages on the same Domino server or on other servers. Examples of files deleted from the cache (in addition to those listed for type 0): ► Most list view and calendar view HTML top-level pages. ► The s_SessionInfo JavaScript page, which contains data about various preferences and relevant Domino Web Access configuration settings. Includes various variants of the current user's name (common name, abbreviated canonical name, full canonical name). ► The h_TOC JavaScript page, which contains information about the functional areas available for current user and initial URL information. ► The s_Outline, which contains information about folder names.
2	Deletes all URLs in the cache that originate from the server hostname, except for URLs that contain /iNotes/Forms6.nsf, the current Forms file (or iNotes/Forms5.nsf). The best balance of performance and security when the user might access other pages in Domino databases on the same server, or might access Domino Web Access and other reverse-proxied intranet sites that might be cached (for example, linking to sites via QuickLinks in the Welcome page or through document links in received mail). For pages accessed via reverse proxy, the server refers to the Reverse Proxy server. Does not affect the performance of other Web sites the user might visit after logout. Examples of files deleted from the cache (in addition to those listed for types 0 and 1): ► Pages generated from any other Notes or non-Notes Web application on the server ► In a reverse proxy scenario, pages generated from any other Notes or non-Notes Web application on the same server or any other server that is reachable from a reverse proxy server ► Domino view icons
3	Deletes all URLs in the cache that originate from the server hostname. Provides more security, but affects Domino Web Access performance negatively for subsequent logons because all cached static script and image pieces are deleted. Does not affect Web applications or pages generated from other servers, so does not negatively affect performance of other Web sites the user might visit after logout. Examples of files deleted from the cache (in addition to those listed for Types 0-2) are URLs to /iNotes/Forms6.nsf (or /iNotes/Forms5.nsf), as well as Domino Web Access static code pages, images, and style sheets.
4	(Secure option) Deletes all URLs in the cache except for URLs that contain /iNotes/Forms6.nsf, the current Forms file (or iNotes/Forms5.nsf). The best balance of performance and security for Domino Web Access, but may negatively affect the performance of other Web applications or pages the user might be using. Examples of files deleted from the cache (beyond those listed for type 0-2) are any external Web pages loaded by the Domino Web Access Welcome page, or traversed to via Domino Web Access or any other browser instance.

Value	Description
5	(More Secure option) Deletes all URLs in the cache. Provides the highest security, but has the greatest impact on Domino Web Access performance for subsequent logons because all cached static script and image pieces are deleted. Examples of files deleted from the cache (beyond those listed for all other types) are URLs to /iNotes/Forms6.nsf (or /iNotes/Forms5.nsf), as well as Domino Web Access static code pages, images, and style sheets.
0	(Default) Best for subsequent Domino Web Access performance. Deletes all URLs that begin with the mail file path, except those that have a strategically placed KeepInCache (&KIC) argument. This argument marks page pieces that contain mostly design. Keeping these pieces in the cache offers a significant performance improvement when next using Domino Web Access. Examples of files deleted from the cache: ► Parts to a MIME message retrieved via a separate URL ► Attachments opened when not using the Domino Web Access control

6.4.3 Additional security considerations

There are a number of client-side security factors with Domino Web Access similar to those of a standard Notes client. In addition to our previous logout discussion, physical security of your machine is critical (do not leave your browser session logged in while unattended, lock it down with Kensington lock or similar device, and so on.). Local (Offline) databases should be encrypted, and Domino Offline Security policy documents should be established. For more information, see Chapter 8, “Linux Clients for DWA 6.5” on page 263.

Finally, we must discuss the issue surrounding security liabilities that come from utilizing a browser itself as a client. By using browser client technologies as the main method of communication with the server, there is the increased potential for users to be subject to malicious code in the form of JavaScript, Java Agents, Active-X controls, and the like. To prevent bad agents/code from being triggered by the clients, Domino Web Access by default has an Active Content Filter in place that parses the HTML content of every mail message and rewrites it prior to having it display in the browser. This can affect server performance, so we have a notes.ini flag that enables you to disable it if you so choose. To disable the Active Content Filter, set:

```
iNotes_WA_DisableActCntSecurity=1
```

in the notes.ini, and restart HTTP. Setting this parameter to 0, or commenting out or deleting the line in the notes.ini will re-enable the filter.

6.5 Domino 6.5 administration

In this section, we highlight the use of the Domino Web Administrator Client. Although it is browser-based, the Web Administrator closely parallels the functionality of the native, windows-based Domino Administrator client. This new feature provides Domino administrators using a Web browser with much, if not all, of the functionality available with the Domino Administrator client.

We then discuss the new Domino Console, which is a separate console-controller pair, implemented with Java, that enables an administrator to work with a server even when the Domino Server is not responding.

6.5.1 Domino Web Administrator

The Domino Web Administrator is managed by the HTTP task. The first time this task starts, it automatically creates the webadmin.nsf database if it does not already exist. Default access to this database is permitted to all server administrators and full server administrators as defined in the Domino 6.5 server document under the Security tab. Administrators added to the server document are updated to the webadmin.nsf Access Control List by the HTTP task.

Note: Refer to the Domino 6.5 Administration Help for detailed instructions for administering the Domino server.

Domino 6.5 Web Administrator requirements

The requirements for using the Web Administrator are listed below.

Software requirements

To access the features of the Web Administrator, you need to have the following:

- Web browser
  - MS Internet Explorer 5.5 or 6.0 on Windows 98/NT4/2000/XP
  - Netscape 4.7x on Windows 98/NT4/2000/XP or Linux (RedHat 7.2 or SUSE 7.2)
- Domino 6.x Server

Domino tasks

The Domino Server must be running these tasks to support the Domino 6.5 Web Administrator:

- The Administration Process (AdminP) on the same server
- The Certificate Authority (CA) on the same server or another Domino 6.x server in order to register users

- Web server (HTTP)

> **Note:** The process of registering users also requires the migration of the Notes certifier to the Certificate Authority process. Refer to the Domino 6.5 Administration help database for more information.

People & Groups tab

Figure 6-10 illustrates the administration functions available to the administrator from a browser, including the Tools pull-down menu for user registration and group creation.

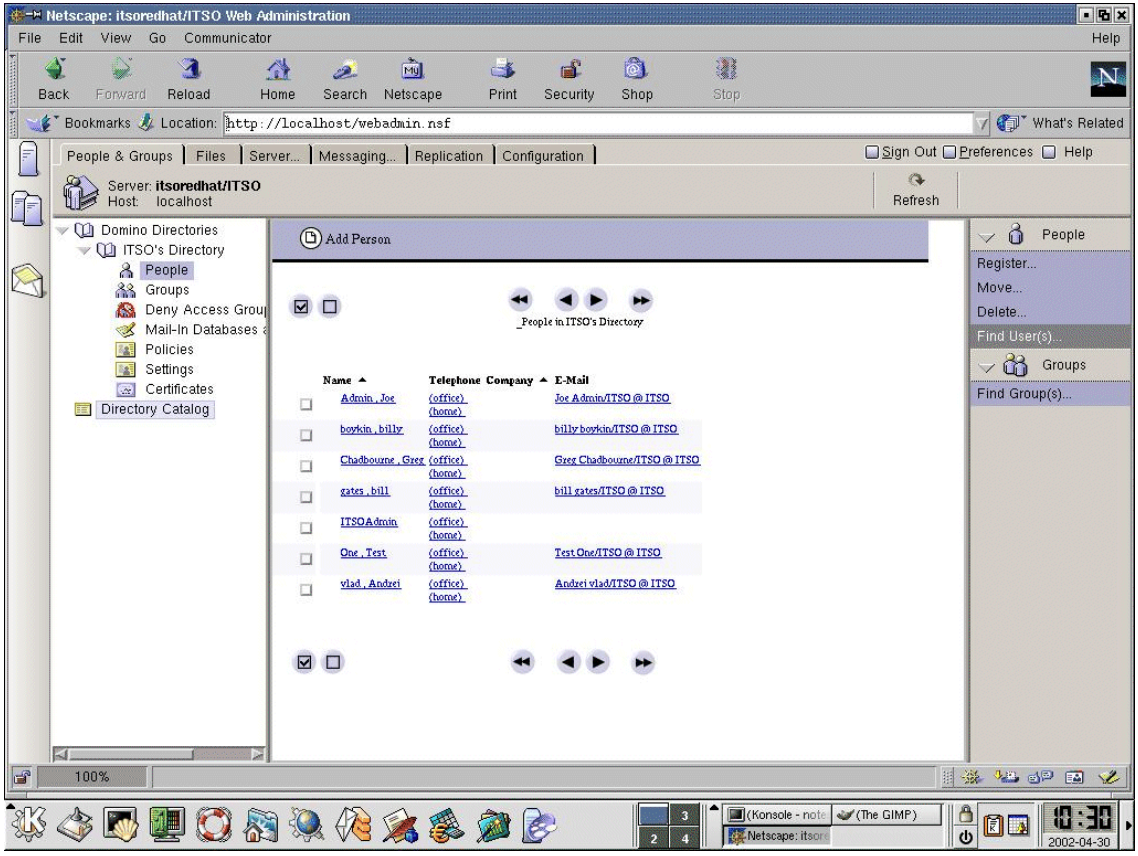


Figure 6-10 Domino Web Administrator: People view

In the People view of the People & Groups tab, you can see the registered users of your Domino domain. You can register, move, and delete users using the links in the Tools pane located on the right side of the window.

Figure 6-11 shows an example of the user registration window. In this window, you enter the basic information about the user and then register the user in the Domino Directory.

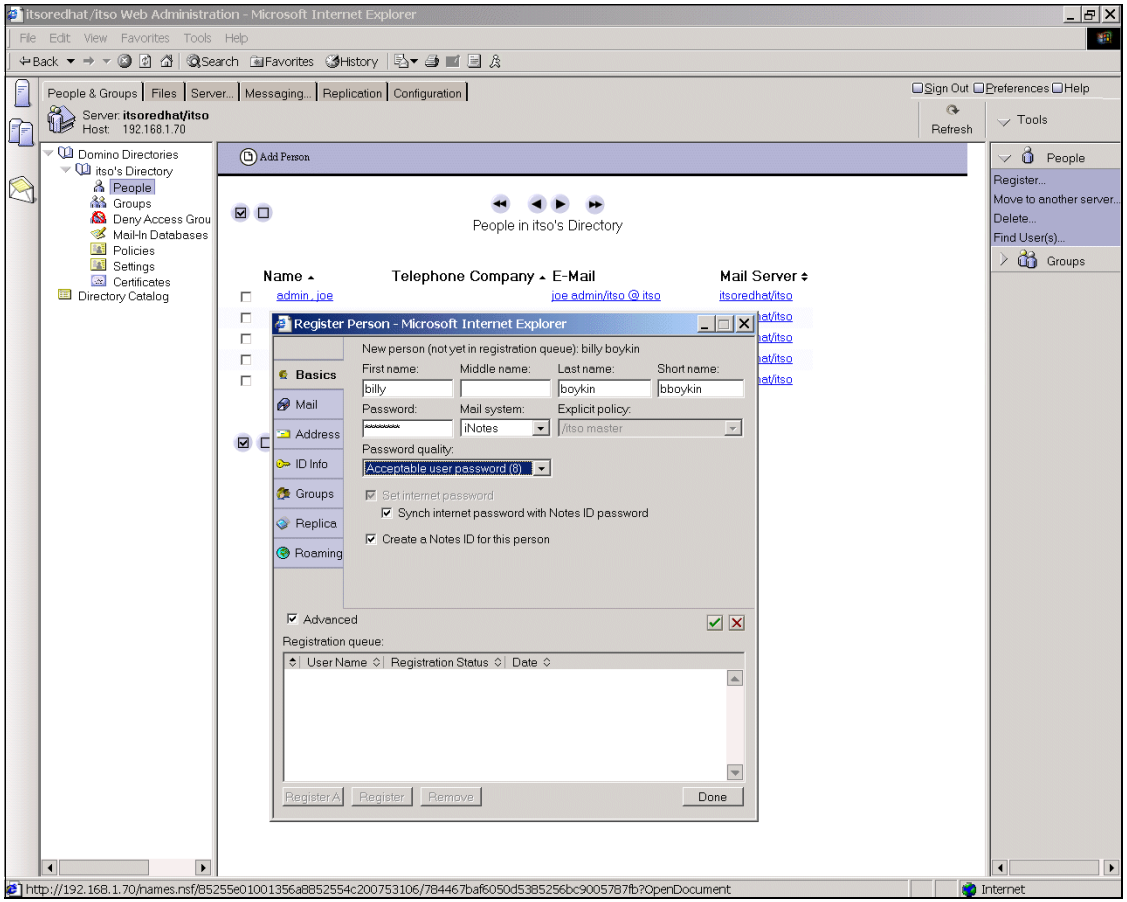


Figure 6-11 Domino Web Administrator: Register users

In the Groups view of the People & Groups tab, you can see all of the groups in your Domino Directory. Each group has a type, which can be mail, access-control, deny list, server only, or multi-purpose group. You can administer groups using the view buttons and the links in the Tools pane.

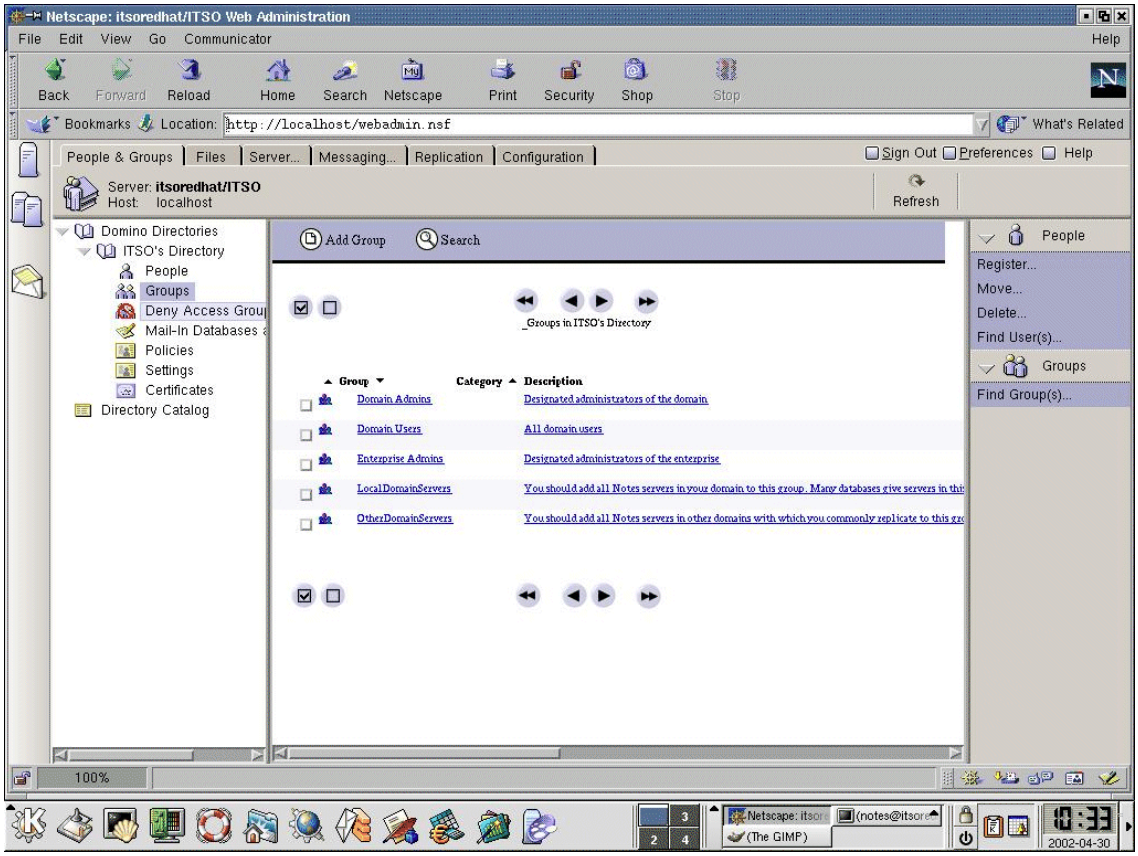


Figure 6-12 Domino Web Administrator: Group view

The Domino Web Administrator enables a Domino administrator to work with Mail-In Databases, Policies (both explicit and organizational), Settings, and Certificates.

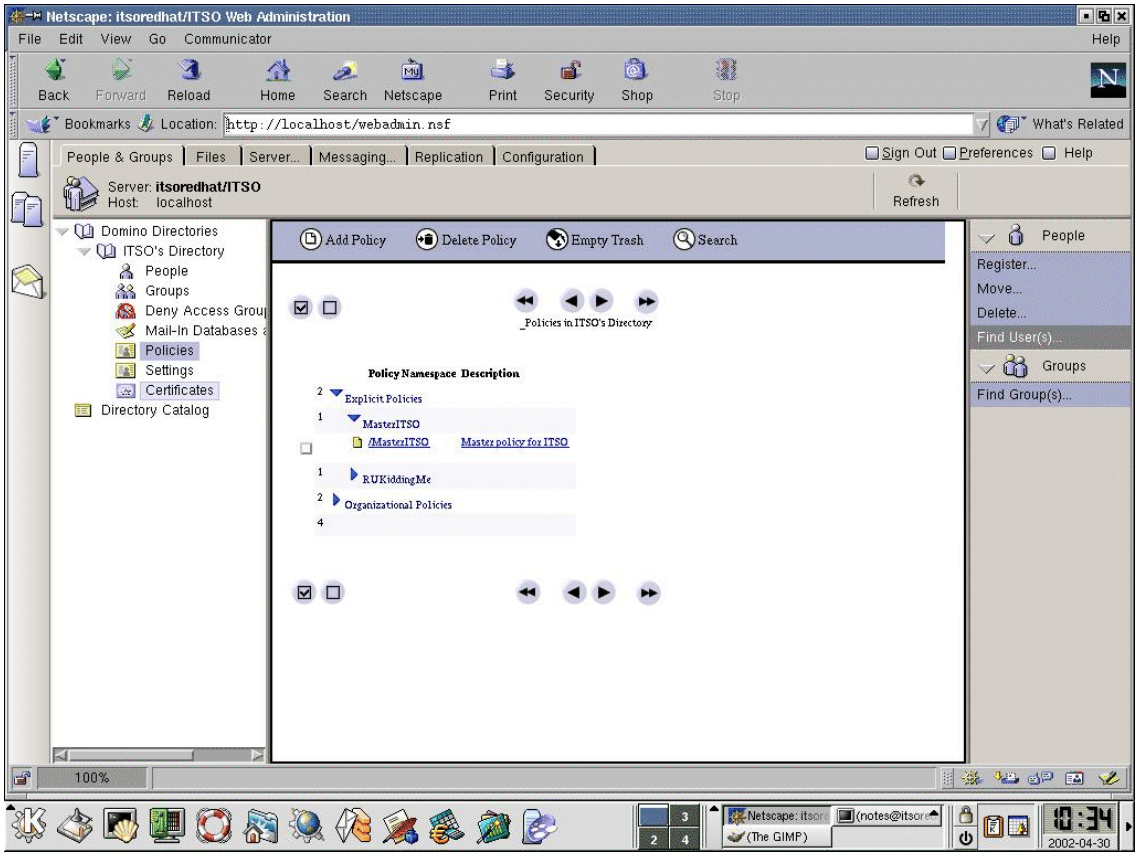


Figure 6-13 Domino Web Administrator: Policies view

Domino Administrators can create policies and, using an established hierarchy, automatically distribute those policies across a group, a department, or an entire organization. The use of policies makes it easy for administrators to establish and maintain standard settings and configurations. It also automates redundant administrative tasks.

Policy-setting documents organize settings by administrative function. The settings in these documents determine defaults, configuration, and rules that are applied to users or groups using Policy documents. Although policy-setting documents define the default settings for users, there is no vehicle for assigning policy settings, except by using a Policy document. Policy-setting documents are also where you control inheritance or enforcement of parent settings.

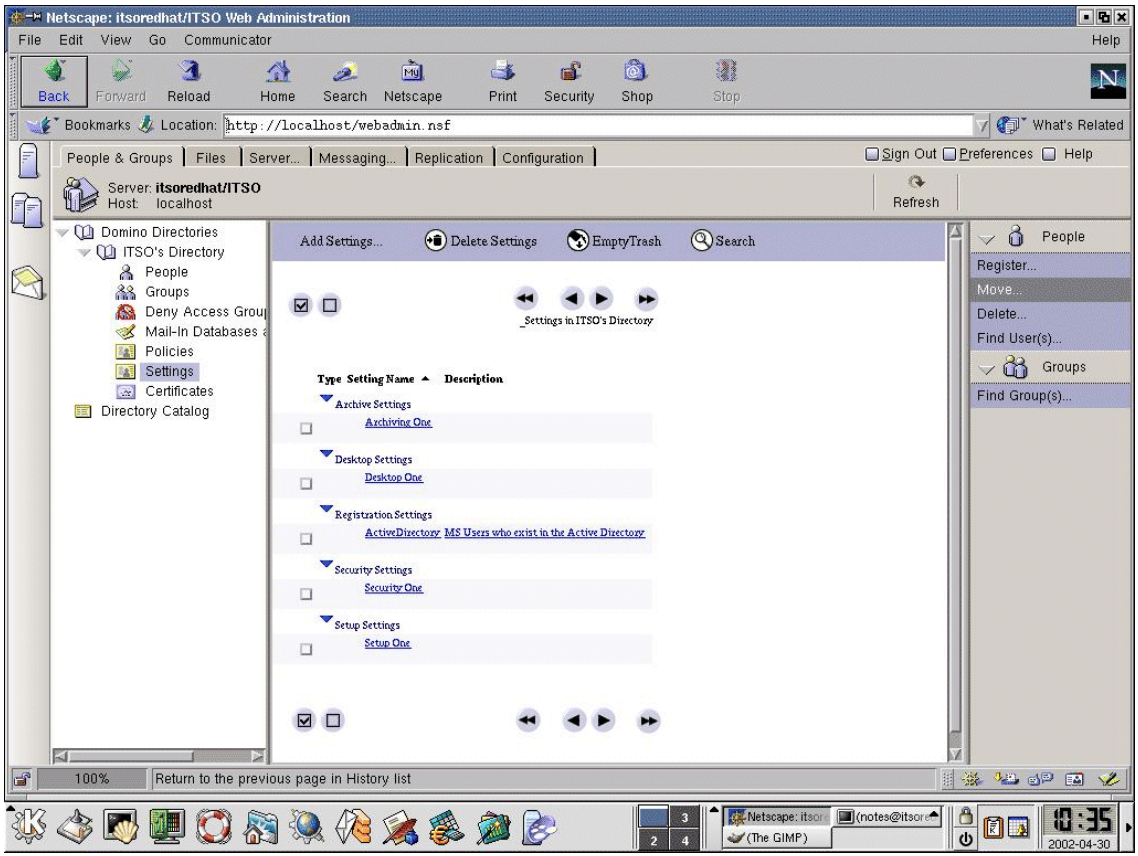


Figure 6-14 Domino Web Administrator: Settings view

The Certificates view enables you to view and administer the certificates used to authenticate users.

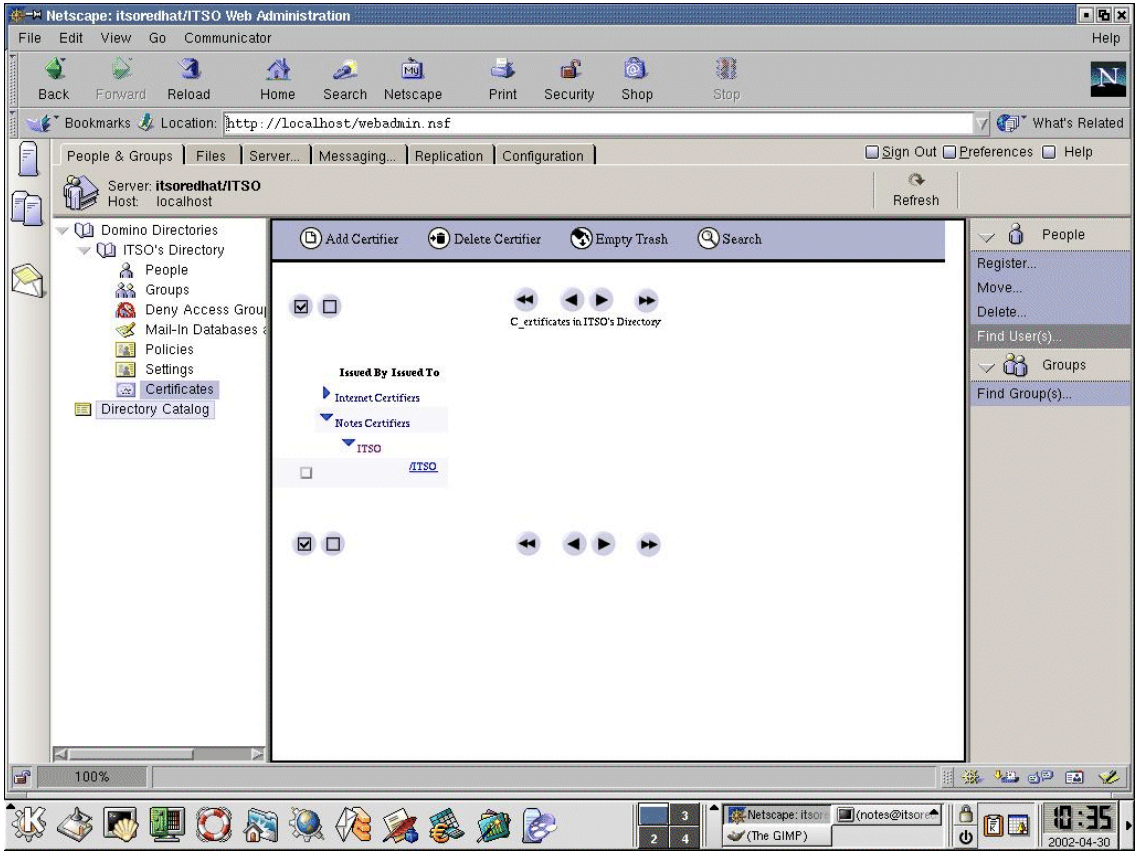


Figure 6-15 Domino Web Administrator: Certificates view

Files tab

The Domino Web Administrator provides file-level access to the operating system to the Domino administrator using a browser. The file-level view begins in the Domino data directory and includes all subdirectories of the data directory.

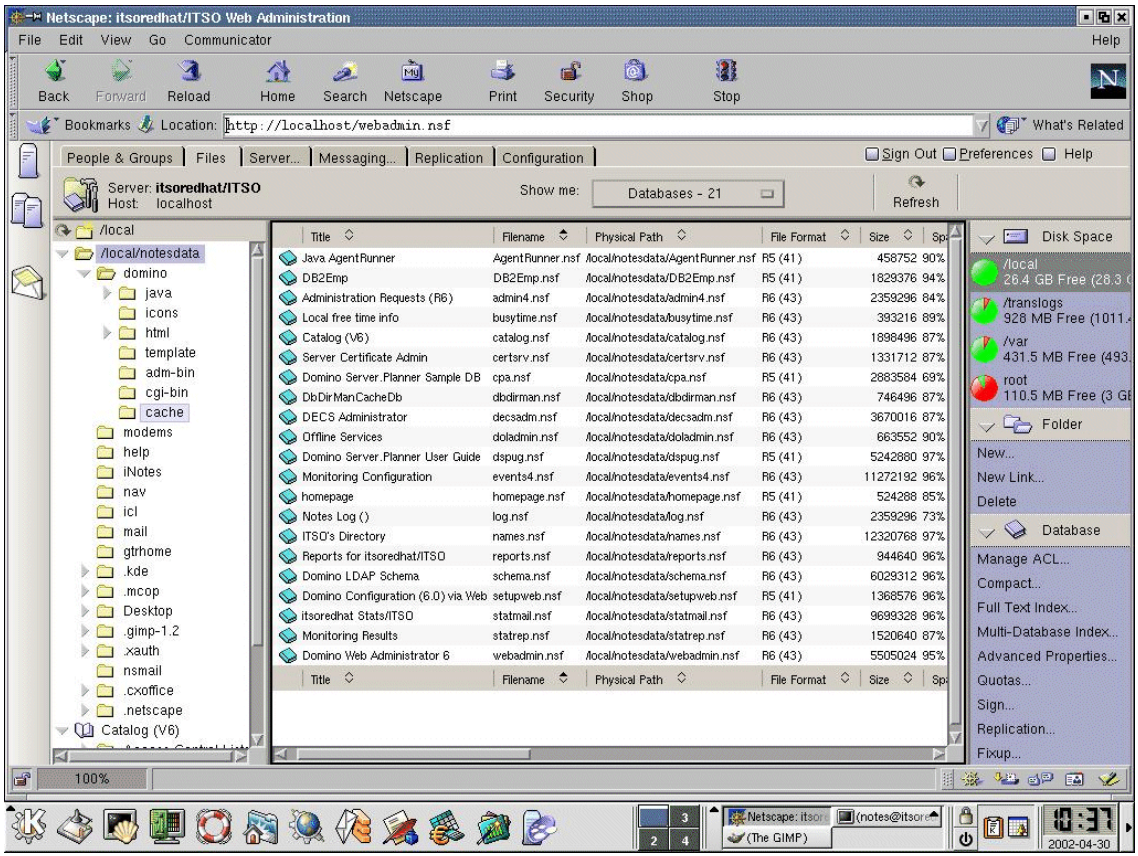


Figure 6-16 Domino Web Administrator: Files view

On the Files tab, you can see and manage Domino databases and templates, as well as folders and links. You can perform many database-management operations in this view, including compacting, signing, and managing database ACLs, and viewing available disk space. These functions are all available via the Tools pane.

6.5.2 Server tab

On the Server tab, the Domino Web Administrator provides the Domino administrator with the ability to:

- Review several forms of server status
- Analyze server activities
- Review server statistics

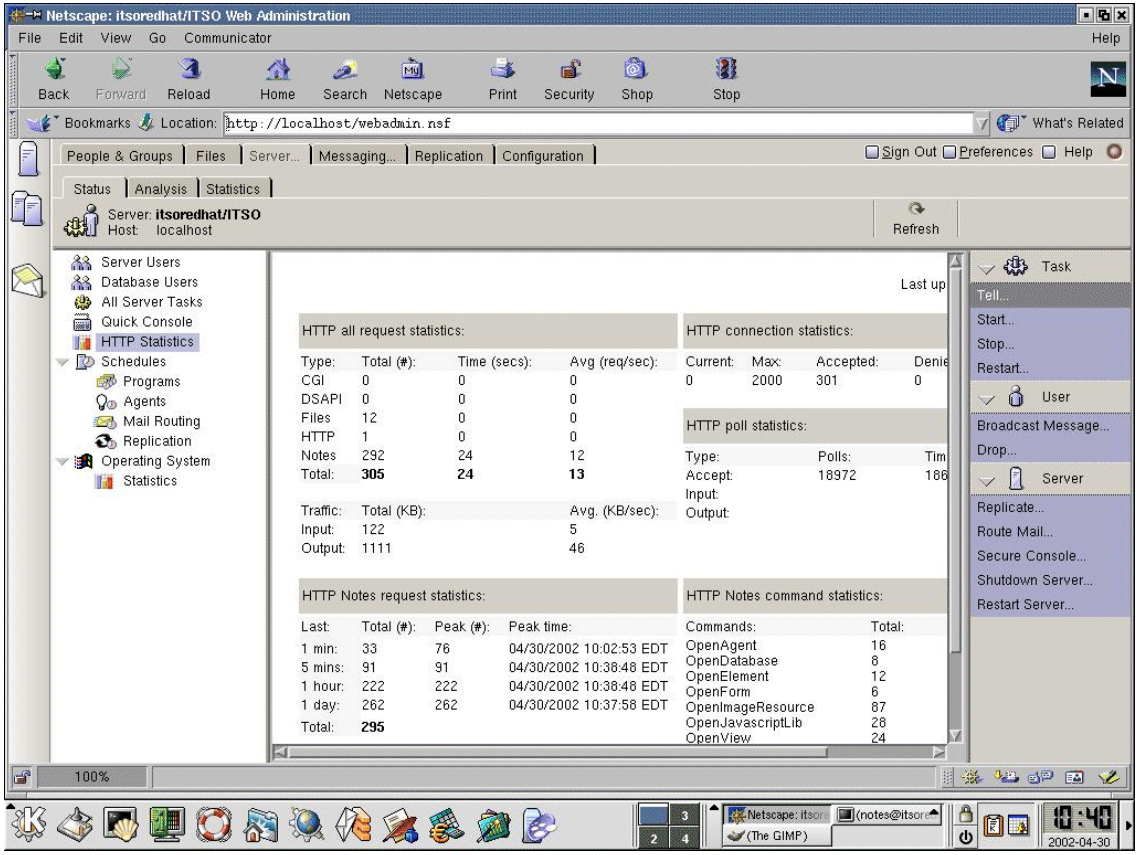


Figure 6-17 Domino Web Administrator: Server status view

From the Server status view, you can see the status of different elements of your Domino environment. These elements include:

- Server users: Shows who is using your Domino server
- Database users: Indicates which databases are being accessed on your Domino server, and by whom
- Quick Console: Enables you to issue console commands to the server

- All server tasks: Shows a list of server tasks that are active
- HTTP statistics: Shows various statistics about your Domino Web server (example statistics page shown in Figure 6-17 on page 233)
- Schedules: Displays schedules for programs, agents, mail routing, and replication
- Operation system statistics

You can perform several tasks by using the links in the Tools pane, including replicating databases and shutting down and restarting the Domino server.

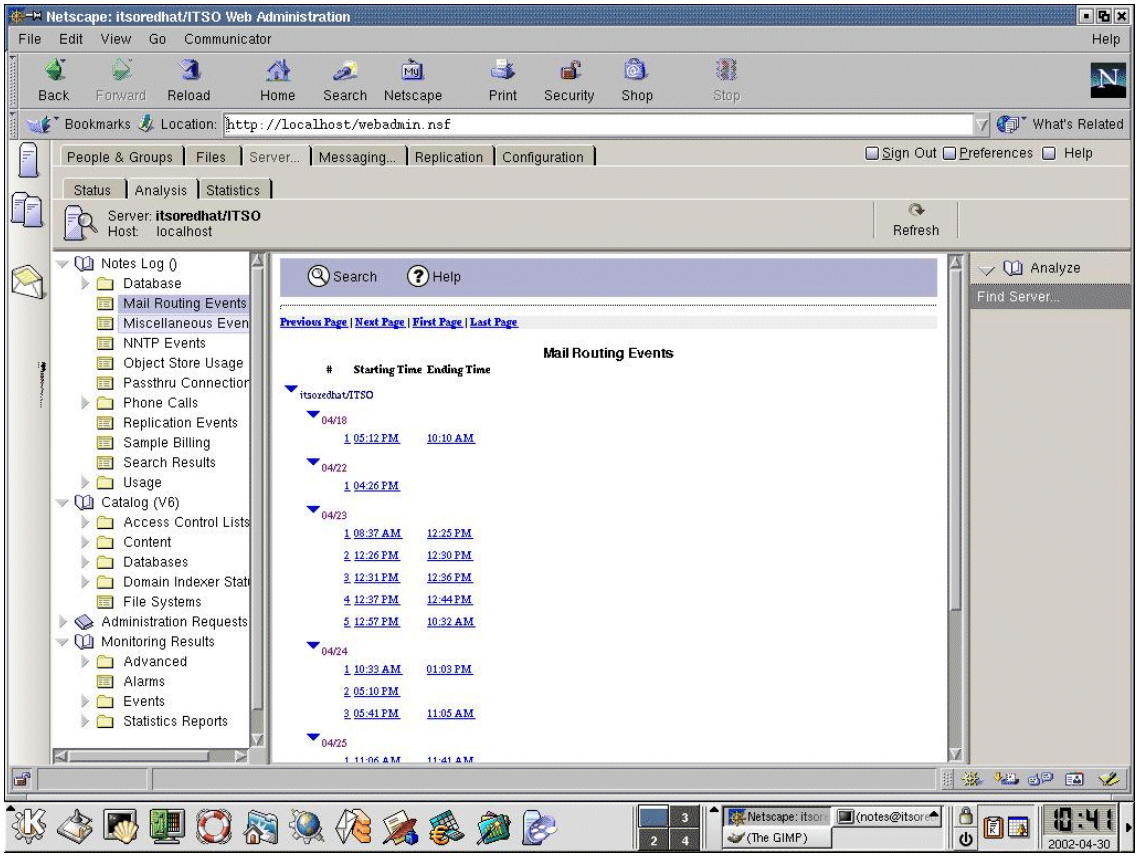


Figure 6-18 Domino Web Administrator: Server analysis view

The Server analysis view provides various representations of information regarding databases, mail routing, replication, logs, and administration requests. See Lotus Domino Administration help for more information about data analysis.

The final sub-tab of the Server tab is the Statistics tab, which shows voluminous statistics about processes running on your system. These statistics include information about agents, databases, HTTP, mail, and the server in general.

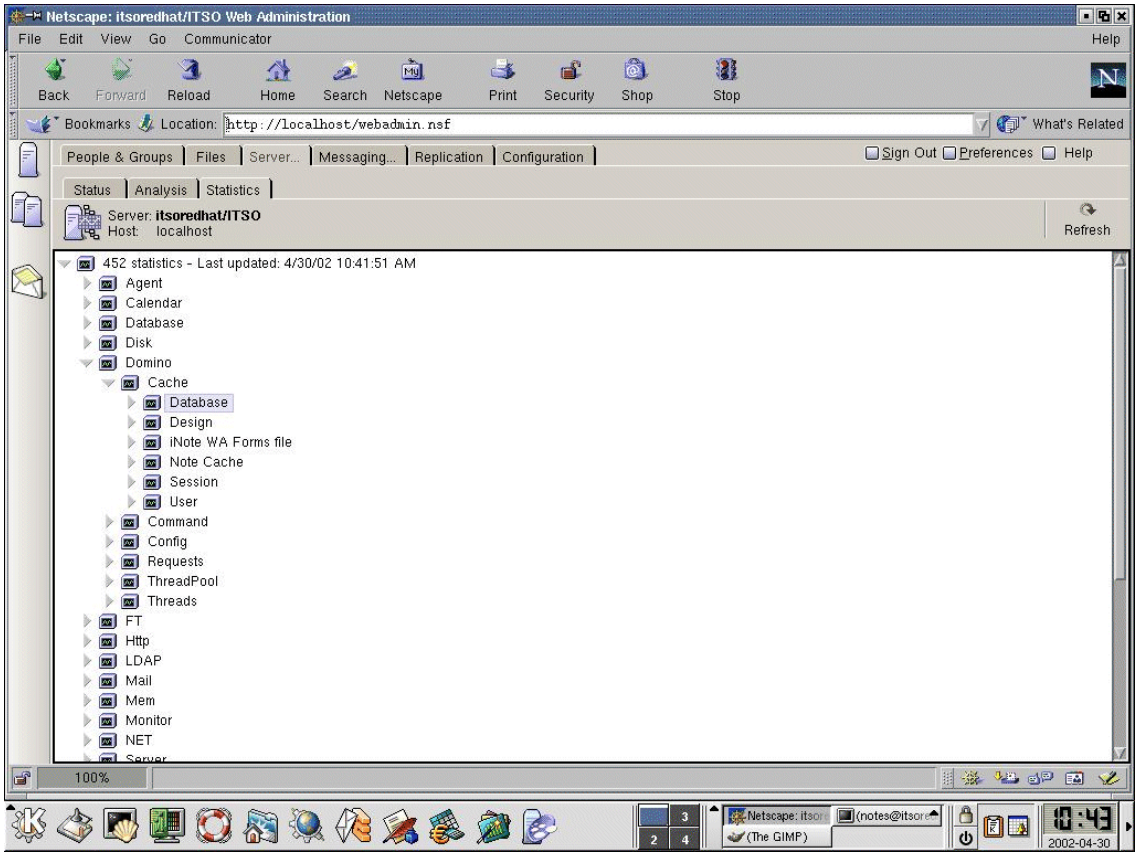


Figure 6-19 Domino Web Administrator: Server statistics view

Messaging tab

The Domino Web Administrator provides the administrator with the ability to manage every aspect of enterprise mail management from a Web browser. These tasks include:

- Mail server tasks
- Mail routing activities and events
- Mail reports

Within the Messaging tab, you can manage the mailboxes on your server, check mail routing, monitor the logfile, run reports on various messaging usage criteria, and use the Tracking Center tab to track messages. In Figure 6-20, you can see the Mail server tasks and the status of our Domino server.

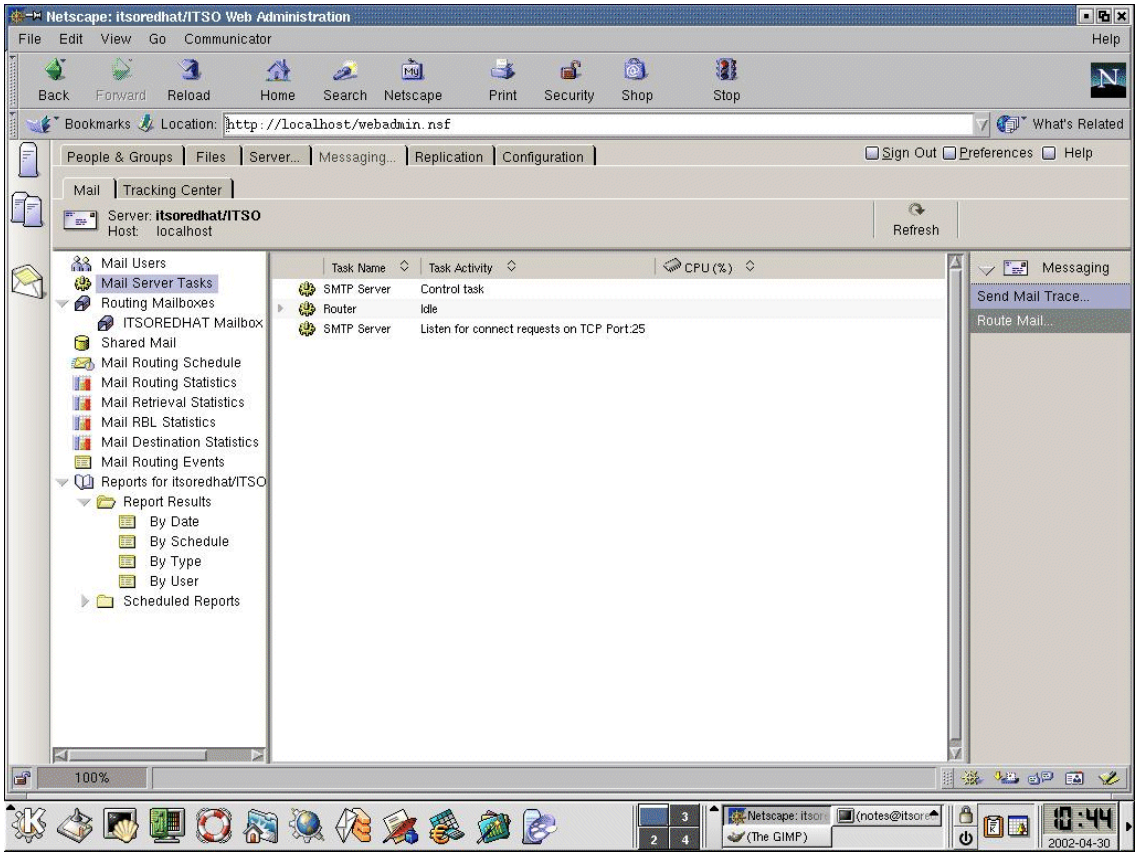


Figure 6-20 Domino Web Administrator: Messaging mail view

Replication

The Domino Web Administrator enables the administrator to control and manage the following replication activities:

- Replication tasks
- Replication schedules
- Replication events
- Replication statistics

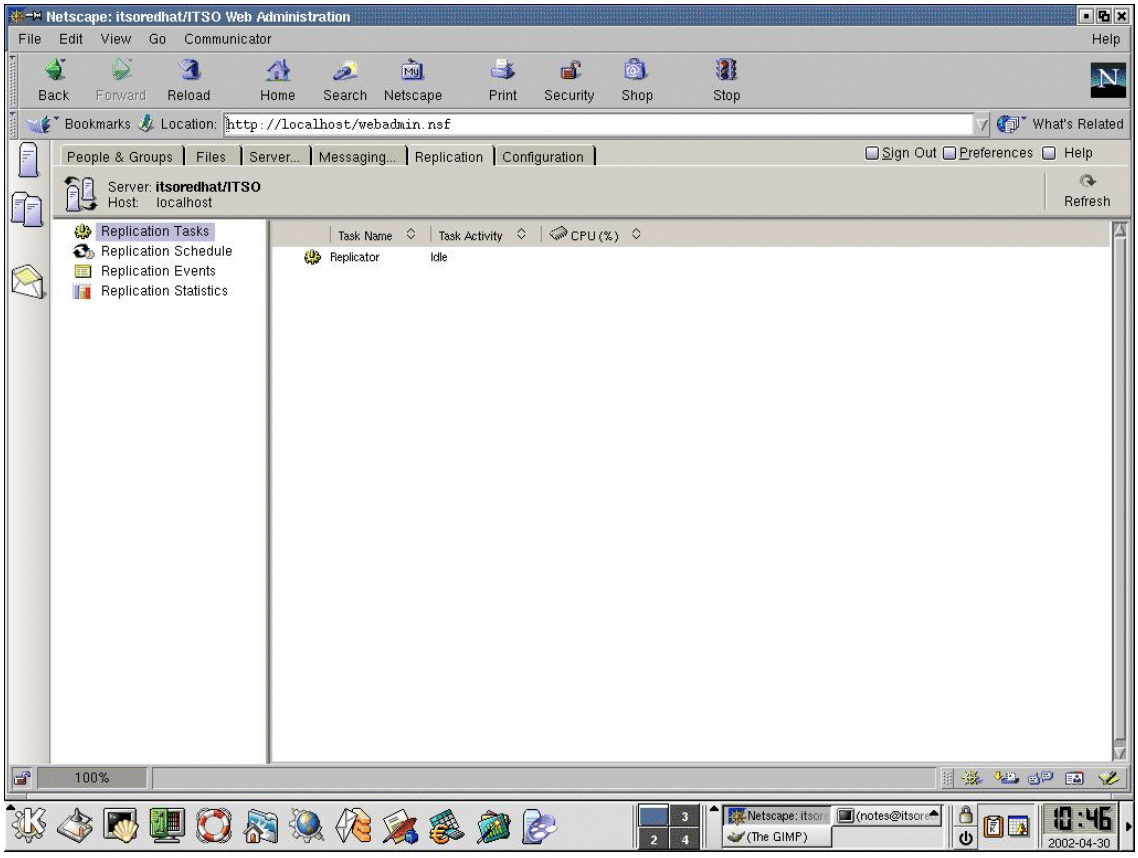


Figure 6-21 Domino Web Administrator: Replication view

Configuration

The Domino Web Administrator provides the ability to control and modify several Domino server configuration options. The following configurations are available:

- Server documents, configurations, and connections
- Directory functions
- Web configuration
- Server monitoring
- Cluster management
- Miscellaneous

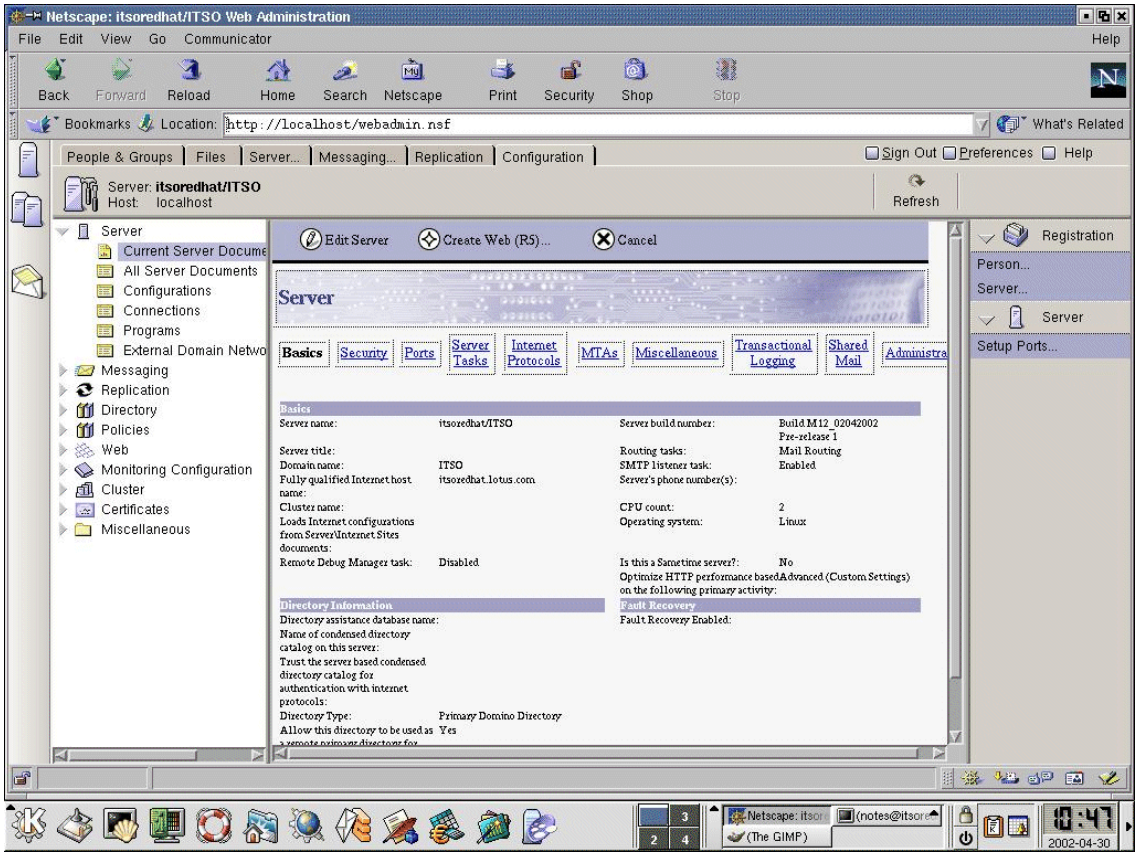


Figure 6-22 Domino Web Administrator: Configuration view

One of the views available through the Configuration tab is the Current Server Document, which is shown in Figure 6-22. It provides access to your Domino server document, which contains many of the settings that define how your server operates. These settings include:

- Basic information, such as the server name and the host name of your server

- Security settings
- Internet protocols such as settings for the HTTP task and Domino Web Engine
- Mail routing
- Transaction logging

6.5.3 Domino Java Console

The Domino Console provides real-time interaction with the Domino Server and is often the fastest way to see what is happening with a server.

The advantage of the Domino Console feature is that, unlike the Windows version of Administration client, you can connect to the server Domino is installed on, even when the Domino server is not responding.

To launch the Domino console, do the following:

- On a Linux system running X-Windows, issue **`jconsole`** from a shell command prompt. If you have not added the Domino executable path to your PATH environment variable, you must specify the full location, which is /opt/lotus/bin by default.
- On a Windows machine with the Administration client installed, launch **`jconsole.exe`**. This executable is located in the Lotus Notes Client program directory.

After the Domino Console launches, you can connect to a new server by **File** → **Connect Controller** (Ctrl-O). You can connect to any Domino 6.x server that has been the Domino Server Controller running. If you have previously connected to a server with this console, you can click the multiple server icon and select it from the list. In the prompt box, enter your Notes name (or shortname) as your username and your Domino HTTP password in the password field. For a new server, type the name in the server; otherwise, select the server from the pull-down list.

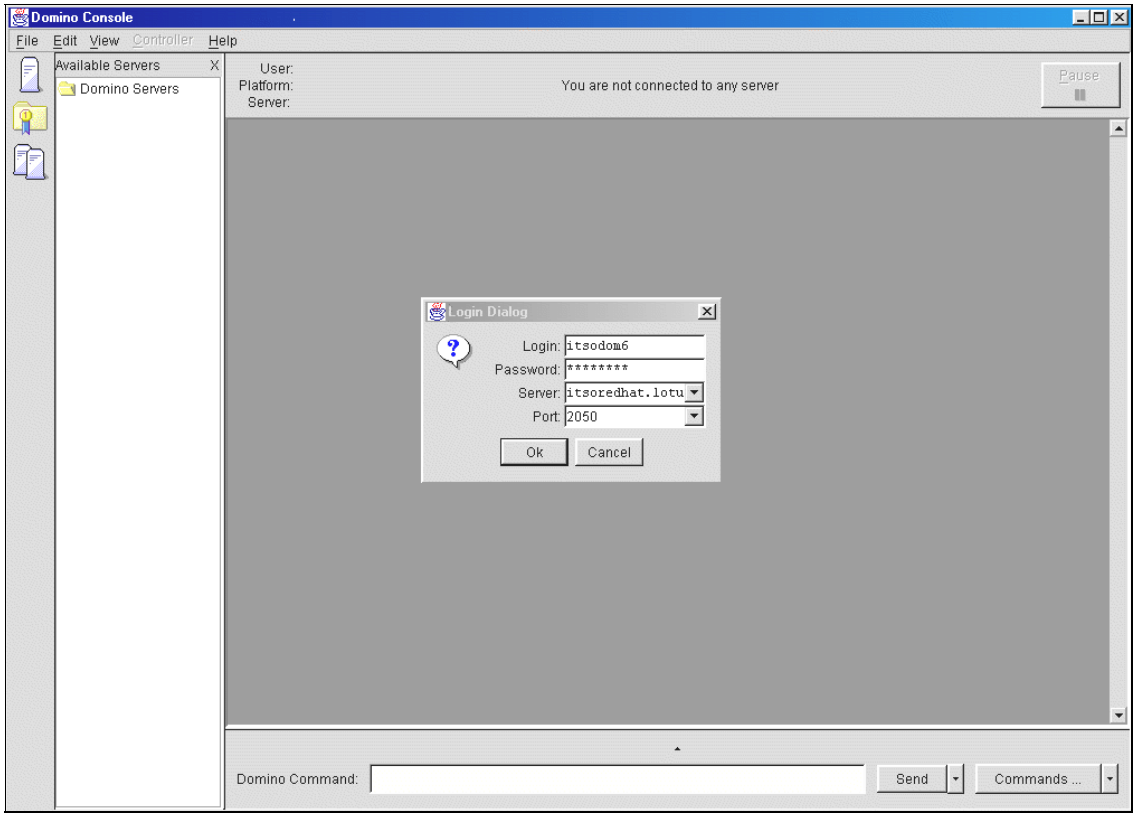


Figure 6-23 Domino Console: Connecting to a server

Table 6-3 identifies some of the common commands you can use from the console; these commands also work from the Web admin quick console.

Table 6-3 Common Domino Console commands

Domino Console command (abbreviation)	Description of the command results
show users (sh us)	Shows the users connected to the Domino server.
show tasks (sh ta)	Shows the tasks currently running.
show cluster (sh cl)	Shows how the cluster is performing and current connectivity to cluster members.
show config servertasks	Shows the current value of the servertasks notes.ini entry. You can use show config to display any notes.ini entry.

Domino Console command (abbreviation)	Description of the command results
`set config servertasks=`	Replaces the existing server tasks notes.ini entry with the values you specify after the equal sign. The values you specify replace the existing ones (they are not appended).
`load replica`	Loads an instance of the replicator that remains until you reboot the server. Any load command without options loads another permanent instance of the task while a load command with options (see the next example) runs, then quits.
`replicate itsoredhat/ITSO names.nsf` (`rep itsoredhat/ITSO names`)	This causes the current server, itsosuse/ITSO in our case, to replicate the specified database, names.nsf, with the specified server, itsoredhat/ITSO. You must use the full hierarchical name of the server. When replication finishes, the replicator will quit.
`show stat server.users`	Displays the specified Domino statistic. There are hundreds of statistics; consult the event4.nsf database for a description of each statistic.
`restart server` (`res s`)	This restarts the Domino server. If issued from the Web admin quick console, you will not be able to view the restart. If issued from a client connected via the new controller, you can monitor the restart process.

Commands are entered into the Domino Command area at the bottom of the Domino console. For frequently used commands, you can click the **Command** button and select from a pre-defined list. Optionally, you can click the arrow to the right of the **Command** button and create a customize command list.

To record a customized command:

1. Click the arrow to the right of the Command button and select **Customize**.
2. In the Make a Custom Command dialog box, enter the desired command.
3. Click **Add** to add the command to your list.
4. Repeat Steps 2 and 3 until you have entered the commands for your list.
5. If you make a mistake or want to remove a command, highlight the command in the Make a Custom Command display and click **Remove**.

6. Click **Save** to save and exit the dialog box.

In addition to Domino commands, you can also send Shell commands if you have the appropriate access. Refer to **Help** → **Help Topics** available with the Domino Console, or the Lotus Domino Administrator help, for more information.

6.6 Converting mail files to Domino Web Access 6.5

Use the Domino Administrator Console and the mail convert utility to convert mail files to the new Domino Web Access 6.5 design.

Syntax: load `convert [-r] [-u]filename OldDesignName NewTemplateName`

- The -r switch indicates that the change should be done recursively in subdirectories.
- The -u switch upgrades the custom folder design of all mail databases in the subdirectory of the Notes data directory to the Inbox design.
- `StdR60Mail` represents the old design name. This example replaces all mail files in the data\mail directory that have the earlier design called STDR60Mail with the new design that is contained in iNotes6.ntf.

Another example shows us how to migrate all users in the mail/ directory:

```
load convert mail/*.nsf * iNotes6.ntf
```

Attention: Be sure to type the name as it is shown, because it is case sensitive.

This example replaces the design of all files in the data\mail directory with the design in iNotes6.ntf. The name of the previous design does not matter. When you are finished converting mail, send users an upgrade notification message.

Important: When you use a wildcard character, such as an asterisk (*), to specify which files to upgrade to the Notes 6 mail template, be sure that all databases in the directory (and, if specified, subdirectories) are mail files. When you use a wildcard character, Lotus Domino replaces the design of all databases specified by the wildcard character with the specified template, such as the Notes 6.5 mail template. If you replace the design of a non-mail database with the Notes 6.5 mail template by mistake, you can use the mail conversion utility by to restore the original design and then specify the correct template.

Finally, we recommend that you compact and archive all mail databases before you start converting your users. After you have converted your users to Domino Web Access 6.5, rebuild all views to make sure they are up to date. Table 6-4 shows the server console commands you can use to perform these operations.

Table 6-4 Commands related to compacting and converting mail files

Command	Description
`load compact -a mail/*`	Compact and archive databases in the mail directory.
`load convert mail/* * iNotes6`	Convert all databases in the mail directory to the iNotes6 template.
`load updall`	Rebuild views in all the databases on this server.

7

Configuration and tuning

This chapter discusses some ways to configure and tune Domino Web Access 6.5. We begin with some Linux OS considerations and follow with ways to modify the behavior and performance of Domino Web Access itself.

Many existing references are available that cover overall Linux OS tuning, so we only focus on a few of the most relevant parameters for tuning Linux. We also discuss items that are necessary for the proper operation of Domino and Domino Web Access.

Some good resources for more detailed information on Linux OS tuning are available through each of the following sites:

- Linux Documentation Project Web site

  `http://www.tldp.org/`

- Linux Performance Tuning Web site

  `http://linuxperf.nl.linux.org/`

There are also a number of comprehensive articles about Domino configuration on the Lotus Developer Domain Web site at:

`http://www.lotus.com/ldd/today.nsf`

Within the Lotus Developer Domain site, you will find particularly relevant articles in the *Performance Perspectives* section.

Important: OS and application tuning is a very environment-specific art form. What works best in one environment may not work as well in another. What we cover here should be used primarily for guidelines and for awareness purposes. Any extensive tailoring of a site-specific configuration has to be done based on that site's specific needs. We recommend some Best Practices here, and also provide some insight into how the various tuning items may affect the operation of Domino Web Access 6.5. This is to enable administrators to make their own informed decisions about how best to configure their servers.

7.1 Configuring Linux tunable parameters for DWA 6.5

This section outlines changes you can make to your Linux kernel parameters to customize it for proper operation of a Domino Web Access 6.5 server. Refer to the redbook *Lotus Domino 6 for Linux*, SG24-6835, for more detailed coverage of performance tuning of the Linux OS and Domino 6.

Red Hat Advanced Server 2.1 and UnitedLinux 1.0 are both enterprise-level operating systems and, as such, have many tunable parameters increased to levels that work for most operating environments. Domino 6.5 (and thus Domino Web Access 6.5) is mainly concerned with the number of file descriptors available to a process, the overall number of threads and processes that a user can execute, and the stack size of a process. Some of the shared memory and semaphore kernel settings can be modified as well, but the default settings are usually acceptable in most environments.

7.1.1 Modifying file descriptor and thread limits

To begin tuning, determine the current levels for the tunables we are concerned with.

1. First, run:

   ```
   cat /proc/sys/fs/file-max
   ```

   This shows the default maximum number of file descriptors that a process is allowed to open. A file descriptor is a handle to a file that is used to do I/O operations. On our Red Hat server within our test environment, the default was 8192. On our UnitedLinux server, the default was 117963. The limit on the SUSE server was quite sufficient (bordering on absurd for our purposes), so we left that alone. The Red Hat server, however, we felt was low. On a busy Domino Web Access server, you can potentially use a significant amount of file descriptors. A file descriptor is consumed not only for each open regular file, but other non-obvious, special files, such as network sockets and I/O devices. A server running in a constrained file descriptor environment may get `Too many open files` errors on the console.

   To increase the limit of file descriptors on Red Hat Advanced Server, log in as the root user and modify the file /etc/sysctl.conf (using a text editor), and add a line:

   ```
   fs.file-max = 65536
   ```

   For UnitedLinux, you can modify the limit directly in the /proc hierarchy by issuing the following command while logged in as the root user:

   ```
   echo "65536" > /proc/sys/fs/file-max
   ```

In this case, we chose 65536 somewhat arbitrarily. It is a sufficiently large number so that we should not run out of file descriptors, but can also be stored in an unsigned integer.

2. Next, check the limit on the number of threads allowed across the system:

   ```
   cat /proc/sys/kernel/threads-max
   ```

   We advise having *at least* 8192 as the thread limit. On the Linux platforms, threads are implemented as Light Weight Processes (LWPs) and, as such, each thread under our various tasks consumes a process. So, with 60-80 threads for the server process, 128 threads for HTTP, 25-50 threads for router, and so on, and including any other applications, OS processes, and the like, it is clear that the number of threads/processes across the system can be consumed rather easily if not planned for.

   In our lab environment for this book, both servers had values greater than 8192, so we did not modify this limit. If you determine that you do need a greater thread limit, on Red Hat Advanced Server, you can add another line to sysctl.conf:

   ```
   kernel.threads-max = 8192
   ```

   On UnitedLinux, you can issue the following command:

   ```
   echo "8192" > /proc/sys/kernel/threads-max
   ```

3. Next, in order to take advantage of the new kernel settings, modify the default limits in the user space by modifying the file /etc/security/limits.conf. To do so, log in again as the root user and, using a text editor, add lines to the file that follow this convention:

   ```
   <user>softnofile65536
   <user>hardnofile65536
   <user>softnproc8192
   <user>hardnproc8192
   ```

   For this convention, <user> is the user who will run the Domino server. (In our case, <user> was dwalinux.) This increases the limit for the Domino user for the number of open files it can handle and the number of processes it can consume.

   To see the results of these changes, reboot the OS so the kernel modifications are loaded, then issue the following command while logged in as the user substituted for the <user> value above.

   ```
   ulimit -a
   ```

4. Edit the file /etc/fstab and add the noatime parameter to the options of the file system (or systems) on which your Domino data directories reside. In this example we use the /local file system. This disables tracking of the access time, which is a value that Domino never uses, and increases performance.

   ```
   /dev/sda6    /local    ext3      defaults,noatime   1     2
   ```

In this example, we added a command and the noatime parameter after the existing `defaults` parameter.

5. In order for the changes to take effect, you must reboot the OS.

Note: Any number of other OS parameters could be tuned to optimize performance for a Domino Web Access server, in particular file I/O buffers, additional memory parameters, and TCP/IP buffers. Unfortunately, in our environment we were unable to perform comprehensive benchmark testing in order to isolate parameters that would give us the greatest impact. The Domino Performance Team in Westford, Mass., under the IBM Software Group Messaging and Collaboration development arm, is continuing work on benchmarking performance results and intends to publish these in the LDD Today "Performance Perspectives" section of the Lotus Developer Domain (LDD). LDD Today is available at:

`http://www.lotus.com/ldd/today.nsf`

7.2 Domino Web Access configuration and tuning

Domino Web Access has many of the same configuration considerations, with regard to performance tuning, as a standard Domino mail server. By this we mean that in most environments Transaction Logging should be enabled, multiple mailboxes can be beneficial, non-essential server tasks should be disabled, and so on. There is a wealth of information available on overall Domino server performance tuning in other redbooks (for example, redbook *Lotus Domino 6 for Linux*, SG24-6835), and in articles on the Lotus Developers Domain in the *Performance Perspectives* section at `http://www.lotus.com/ldd`.

As mentioned in the introduction to this chapter, we do not focus significantly on overall Domino server performance tuning. Instead, we emphasize configuration issues and settings particular to Domino Web Access 6.5.

7.2.1 Domino HTTP configuration

One of the main differences between Domino Web Access and a standard Domino mail server is the fact that all Domino Web Access traffic is handled through the HTTP stack. Accordingly, specific tuning for the Domino HTTP server can be helpful in boosting DWA performance. Although the redbook team was unable to perform extensive benchmarking tests to determine what settings have the most impact on Domino Web Access on Linux, we want to discuss a few particular configuration changes that may be worth exploring if performance issues are seen.

HTTP threads

By default our HTTP stack uses non-persistent connections for all browser sessions. An HTTP thread receives a connection request from a browser, handles the request, completes whatever was asked of it, then moves on to whomever next needs service. This model is perfect for the type of traffic that Domino Web Access generates. We allocate 40 HTTP service threads in standard environments but allow administrators to modify this as needed. If users are having difficulty establishing connections at peak times, the server may benefit by increasing the number of service threads available to HTTP.

To increase the number of available threads, edit the Server document for the DWA server. Select the **Internet Protocols** → **HTTP** tab, and under the Basics section, increase the number of threads in the Number of active threads field. We recommend modifying the value in increments of 10-20 threads to see how the behavior is. Allocating additional threads increases the overall CPU consumption of the task, especially at peak times. As the thread count gets higher, there will be a diminishing return, such that your connection rates and response times will not improve significantly, but you will still see an increase in the CPU busy rate. HTTP service threads can usually handle a substantial number of requests per second, and so a relatively small thread count can handle a fairly large number of users. In most environments the thread count should not have to be increased beyond 100 to 128 threads, while often much fewer suffice.

HTTP memory caches

Domino Web Access users pull their design elements from essentially two locations: Forms5.nsf and Forms6.nsf in the iNotes subdirectory of the Domino data directory. Design elements are cached by the Web server in order to improve performance. We cache 128 elements by default, and this should be sufficient for most purposes but can be increased if necessary. Monitor the Domino.Cache.Design.Count, Domino.Cache.Design.MaxSize and Domino.Cache.Design.DisplaceRate statistics, which can be seen by issuing this command from the Domino server console:

```
show stat domino
```

If the Count grows close to the MaxSize, or the DisplaceRate grows, increase the size of the design cache by editing the Server document and changing the value in the Maximum cached designs field on the **Internet Protocols** → **Domino Web Engine** tab.

The other memory cache to focus on is the User cache. Monitor the Domino.Cache.User.Count, Domino.Cache.User.MaxSize, and Domino.Cache.User.DisplaceRate statistics as seen by issuing the **`show stat domino`** command.

If the Count value nears the MaxSize value, the DisplaceRate grows, or both, the administrator should increase the size of the user cache by editing the server document and modifying the Maximum cached users field on the **Internet Protocols** → **Domino Web Engine** tab.

7.2.2 GZIP network compression

Domino Web Access 6.5 introduces GZIP network compression as a technology to reduce the overall network bandwidth and improve performance of Domino Web Access sessions. This compression is enabled by default, though it can be disabled either through a setting in the server document or through a notes.ini setting.

The improvements gained through this compression are particularly noticeable for dial-up connections or any type of slow network. There are a few notes.ini parameters that govern how GZIP compression operates in your server environment, including what data types to include or exclude from going through compression.

Notes.ini parameters relevant to GZIP compression

- iNotes_WA_GZIP_Disable

  This parameter governs whether GZIP compression will be used. By default it is enabled (set to 0). To turn off GZIP compression for all sessions, add the following line to the notes.ini and restart HTTP:

  ```
  iNotes_WA_GZIP_Disable=1
  ```

  Note: This can also be controlled within the server configuration document, via the Compress HTTP response data field under the Other Settings section of the Domino Web Access tab. By default, the box will be selected. To disable, uncheck the box, save the configuration document, and restart HTTP. (See Figure 7-1 on page 252.)

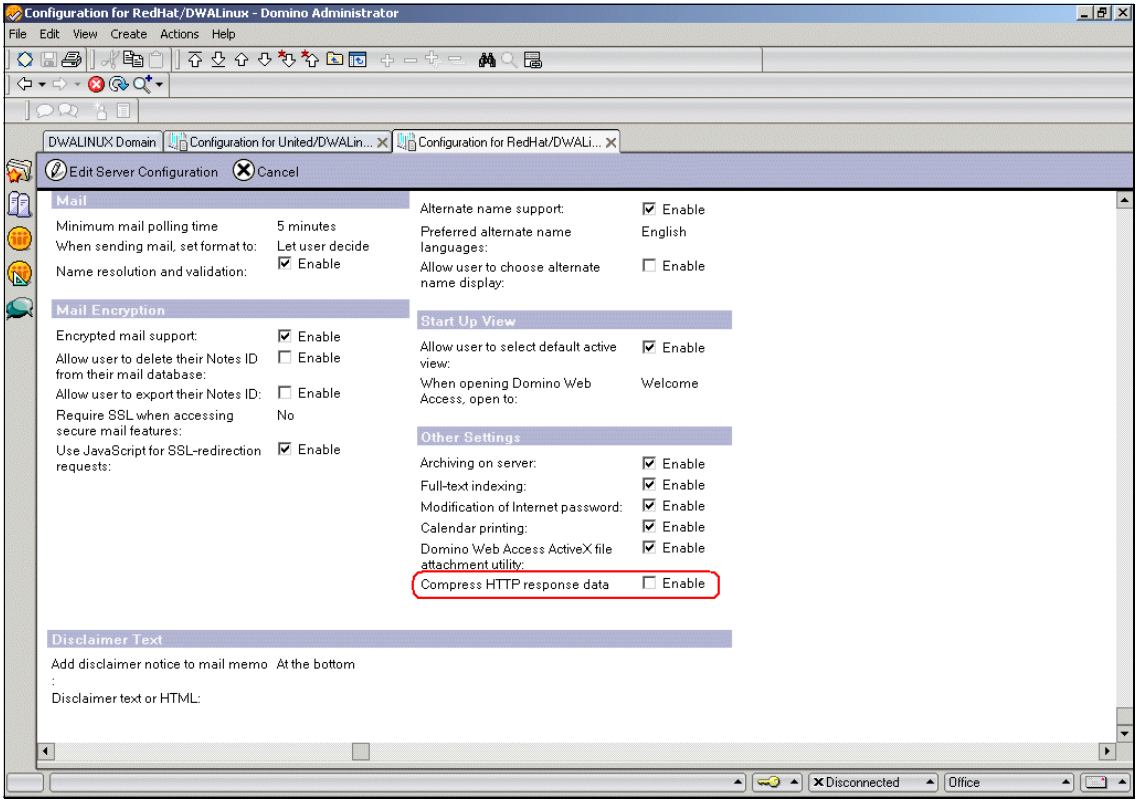


Figure 7-1 Compress HTTP response data field

- iNotes_WA_GZIP_Content_Types_Included

  This parameter enables the administrator to specify elements of what particular Content Types are compressed. By default, we compress all elements with a Content Type of text/* and application/*. To modify what types are compressed, add a line to the notes.ini:

  ```
  iNotes_WA_GZIP_Content_Types_Included=”image/gif;text/*;application/*”
  ```

  This adds the image/gif type to the list of Content Types that get compressed.

  Note: Domino Web Access compresses only those types that are listed in the iNotes_WA_GZIP_Content_Types_Included parameter, assuming that it is set. If you set this parameter to be one type, such as image/gif, only GIFs will be compressed. This overrides the default of text/*;application/*. This also applies to the iNotes_WA_GZIP_Content_Types_Excluded parameter described below. The notes.ini parameter will override the default values.

- iNotes_WA_GZIP_Content_Types_Excluded

  This parameter enables the administrator to explicitly control what elements are *not* compressed. By default, we do not compress elements with image/* and application/pdf Content Types. To modify the list of Content Types to exclude, add a line to the notes.ini:

  ```
  iNotes_WA_GZIP_Content_Types_Excluded=”text/xml;image/*;application/pdf”
  ```

  This example prevents elements of type text/xml from being compressed, in addition to the default excluded Content Types.

Important: An important point to note is the precedence order of the Included and Excluded parameters above. Domino Web Access checks for a match in this order:

1. Exact Match in the Included parameter
2. Exact Match in the Excluded parameter
3. Wildcard Match in the Included parameter
4. Wildcard Match in the Excluded parameter

When a match is found, DWA stops checking and either compresses or not, depending on where the match was found. Thus, explicit Content Types (for example, application/pdf) take precedence over anything non-specific, such as application/*.

7.2.3 Other Domino Web Access configuration settings

The Domino Web Access tab on the server Configuration document has a number of settings that can affect the overall performance and behavior of the server. We highlight a number of them here and describe some notes.ini parameters that affect Domino Web Access behavior.

Alarms

The first area on the Domino Web Access tab that can affect server performance is the Alarm section (see Figure 7-2 on page 254). The options in this section enable the administrator to customize whether DWA users can choose to be notified when a meeting, appointment, or other calendar entry is impending. The default poll time is 5 minutes. You can either turn off the feature entirely or increase the default length of time the DWA session polls to see if an alarm is due. A slight performance gain can be seen if the default polling time is increased. Turning the feature off entirely shows a larger gain, especially in environments with a large number of DWA users, as it can reduce session traffic.

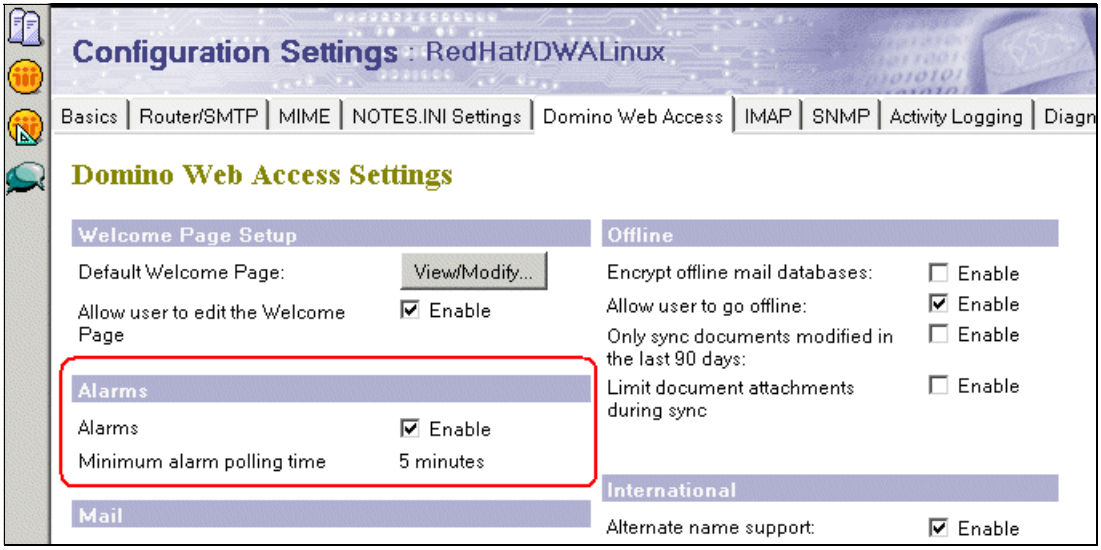


Figure 7-2 Alarms section of server Configuration Settings document

Mail

The next section that can affect server performance is the Mail section. (See Figure 7-3.) By default, DWA sessions poll the server to see whether there is new mail in the user's Inbox every 5 minutes. By increasing the interval for this poll, the Administrator can decrease session traffic and see a slight gain in performance overall on the server.

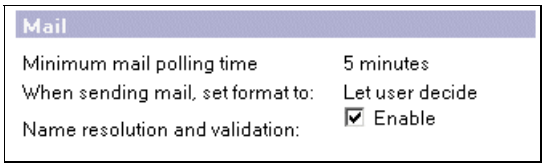


Figure 7-3 Mail section of server Configuration Settings document

In addition to the mail polling interval, this section enables the administrator to either force users to send mail in plain text format, or allow them to choose plain text or a rich text version (HTML). This setting on the Configuration document corresponds to the notes.ini parameter iNotes_WA_MessageFormat.

Setting this parameter to 1 forces the use of plain text. The default is 0.

Finally, this section also enables the administrator to specify whether users can do ambiguous name resolution, which is essentially the same as type-ahead in a Notes client. The main distinction is that in a Domino Web Access session, the

name does not auto-complete as it can in the Notes client. The user has to either press F9 or click the Check Name(s) icon that appears when you have typed characters in one of the recipient fields (To:, CC:, BCC:).

There is also a notes.ini parameter, iNotes_WA_NameLookupMaxNumMatch, that affects the behavior of this option, but it does not have a corresponding field on this tab. This parameter is used to limit the number of names that will be returned when a user attempts to validate a name. By default, we allow 200 matches to be returned, but this parameter can be used to change the value.

Other Settings

The final settings that can have a noticeable impact on server performance are included in the Other Settings section, as shown in Figure 7-4.

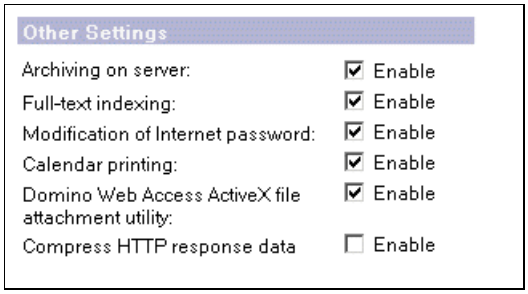


Figure 7-4 Other Settings section of server Configuration Settings document

These settings include:

- Full-text indexing

  This field can be used to allow or prevent users from creating server-side full-text indexes of their mail files. It is enabled by default, but an administrator can save disk space and improve server performance by disabling this ability.

- Archiving on server

  Archiving is also enabled by default. It enables users to create server-side archive copies of their mail file, which can consume disk space and processing power.

- Calendar printing

  This functionality uses an Adobe PDF API on the server to convert calendar entries to PostScript format and returns it to the browser in order to print the entries. This is a fairly lightweight operation for single calendar entries, but users can request for multiple entries, or entire calendar views, to be printed. This can add load to the server if it is heavily utilized.

- Compress HTTP response data

  For a description of the Compress HTTP response data field and its ramifications, see 7.2.2, “GZIP network compression” on page 251.

7.2.4 Additional notes.ini parameters for Domino Web Access

This final discussion addresses remaining notes.ini parameters that can be set to further tune Domino Web Access 6.5

Limiting shared memory

If you have more than 2 GB of physical memory, you should limit shared memory to 1 GB in order to leave enough memory for other tasks. To constrain shared memory, add these two notes.ini variables to your Domino server:

- ConstrainedSHM=1
- ConstrainedSHMSizeMB=1024

When your server is running well, you can consider increasing the size of shared memory to 2048 or 3072. As the amount of addressable memory for 32-bit operating systems is 4 GB, you should not set it higher than 3072 in order to make certain to leave enough memory for other tasks. A single Domino partition should never consume all of your system’s memory under normal circumstances. However, if you begin seeing errors on the Domino console indicating that your system may be running low on memory, these settings may help. For additional information about this issue, we recommend that you review tech note #1095911, which can be found on the IBM support site at:

http://www.ibm.com/support

Session Check parameter

One final tunable parameter that is appropriate to cover in this chapter is yet another parameter that can increase session traffic to the server. By setting the notes.ini setting iNotes_WA_SessionCheck=1, each POST operation from the browser will cause an additional request to be made to the server in order to ensure that a connection is present. This is an option to help prevent data loss in cases where a user is editing a DWA object but the connection to the server is no longer there when the browser attempts to POST the change. So the session traffic is increased in the name of data preservation.

There are a number of other parameters specific to Domino Web Access that are covered in other chapters. For parameters that apply to Sametime integration under Domino Web Access see 9.4, “Notes.ini parameters for Sametime integration” on page 336. For notes.ini parameters that affect Domino Web Access Administration, see 6.3.3, “Notes.ini settings for Domino administration” on page 218.

7.3 Performance comparison: Linux and Windows

The following results are from a recent performance study conducted by Razeyah Stephen and James Powers of the Domino Performance Testing Team in Westord, Mass., and presented at Lotusphere 2004. This performance test represents a comparison between Windows 2000 and Linux on identical systems, and illustrates two key performance advantages of using DWA 6.5 on Linux:

- DWA 6.5 on Linux provided a better response time for a greater number of users.
- DWA 6.5 on Linux allows for a greater number of users, with less CPU utilization per user.

7.3.1 Specifications of test machines

Each of the machines used in this test represents an identical system running the R6iNotes workload tool.

Configuration:

System	COMPAQ Proliant DL580
O/S	SuSE SLES 8 and Win2K Advanced Server
CPU	(4) Xeon MP 1.4GHz
Memory	4Gb
Disk	RAID (3) IBM EXP 300

7.3.2 Overview of results

Figure 7-5 on page 258 illustrates the response time in milliseconds per user with DWA 6.5 on idenitcal systems running Windows 2000 and Linux. As you can see from the results, it was possible to have a better response time on the Linux system, even after adding an additional 1000 users.

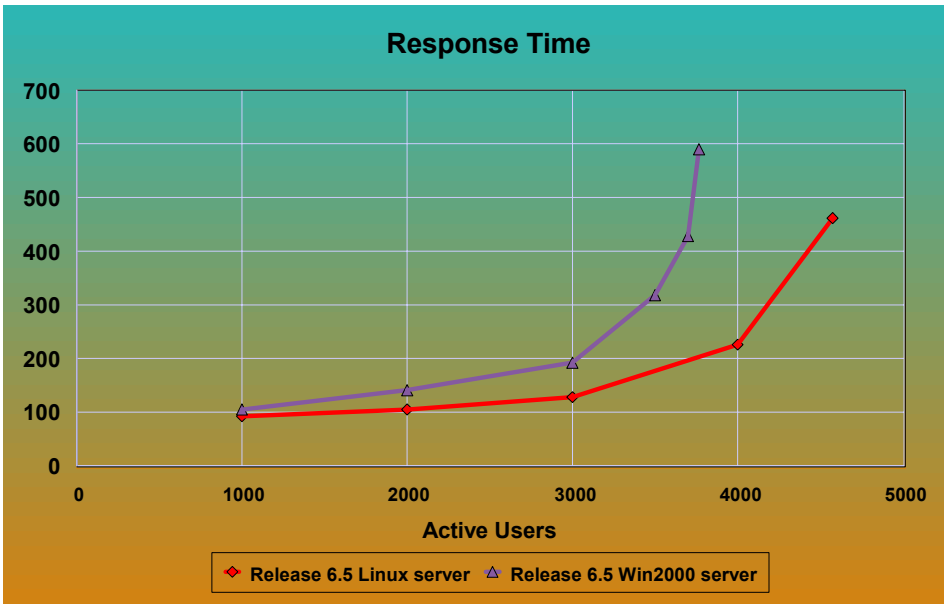


Figure 7-5 Response time in milliseconds

Figure 7-6 on page 259 shows the CPU utilization per user on each of the test systems. The key message here is that Linux used less CPU per user than Windows 2000, which ultimately allows for more users on the system with a given CPU. For this test, CPU utilization reached 90% at approximately 3700 for Windows 2000, versus at 4600 for Linux. This illustrates a significant benefit to using Linux, because the CPU represents a primary hardware constraint.

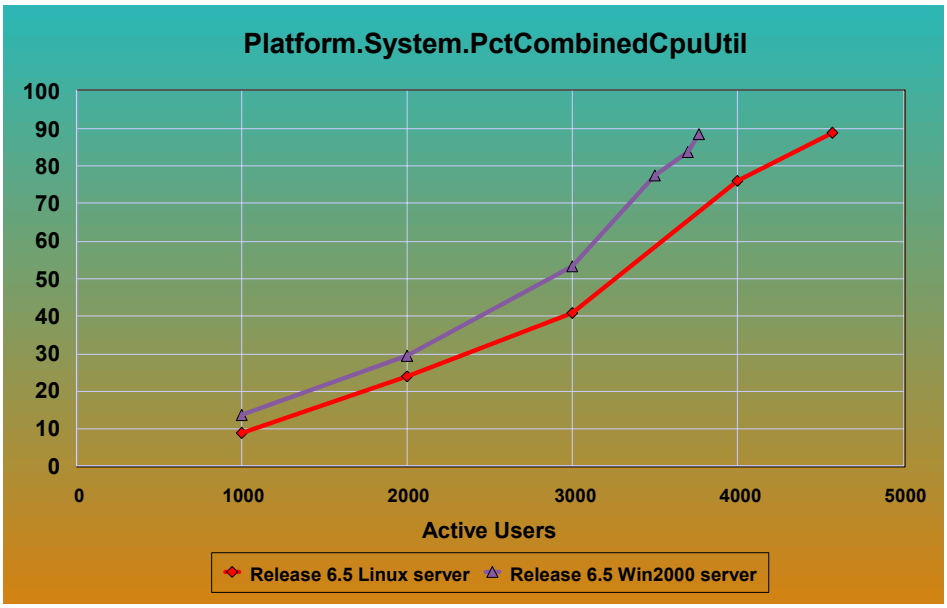


Figure 7-6 CPU utilization per user: Windows 2000 versus Linux

Part 3

Clients for Domino Web Access

8

Linux Clients for DWA 6.5

This chapter provides an overview of supported browsers for Domino Web Access 6.5 and the DOLS (Domino Offline Services) client for Linux. In addition to discussing Mozilla as a browser online, we provide a detailed approach to installing and configuring the DOLS offline client on the Linux system. The DOLS component is discussed in terms of both configuration and administrative requirements on the server. Finally, we provide an overview of our results of working with Mozilla 1.3.1 and offline DOLS configurations on several Linux distributions.

It is important to note that Domino Web Access 6.5 is the first version of Domino that provides offline services on the Linux platform. This is significant as it addresses the strong demand within the IBM/Lotus Community to provide a full-fidelity, Linux-based client solution for synchronizing and using your mail file offline.

8.1 Mozilla

Mozilla is one of the most popular browsers within the Open Source Community. One of its strongest advantages is its broad range of cross-platform support. The Mozilla browser is available for the following operating systems:

- Linux
- Mac OS X
- Windows
- AIX®
- HP UX
- IRIX
- OpenVMS
- OS/2
- Solaris
- True64 UNIX

To better understand the benefits of Mozilla, we recommend that you review an article on the Mozilla Web site called “Why Use Mozilla” at:

http://mozilla.org/why/

This provides an in-depth review of Mozilla features and advantages on different platforms. For this book, we focus on the Linux platform with Mozilla V1.3.1.

For Domino Web Access 6.5, there are some dependencies to consider. The supported Mozilla browser version for this release is 1.3.1. Support for this version is because of the Mozilla Plug-In for Domino Offline Services, a new feature in DWA 6.5 which has been compiled especially for Mozilla 1.3.1.

Attention: While the officially supported browser version for using Domino Web Access 6.5 is Mozilla 1.3.1, we also conducted some tests within our testing environment set up for this book. Results of testing with Mozilla Versions 1.4 through 1.5 (even Firebird 0.6.1 and 0.7) did not reveal any problems using the latest code for Mozilla when working *online* with Domino Web Access 6.5. Keep in mind however, that these browser versions are not officially supported by IBM/Lotus at the time of this publishing. Accordingly, you will not get any support from Lotus if you have problems with these versions. IBM does plan to provide support for additional browser versions with Domino Web Access 6.5.1.

Using the *offline* capabilities of DOLS requires Mozilla 1.3.1. As our testing verified, DOLS does not work with any other versions of Mozilla.

8.1.1 Mozilla installation steps

This section describes the steps to install the Mozilla browser.

After you have verified that the OS is ready, you can install the Mozilla program files, then configure and set up the Mozilla browser.

Attention: If you install into the default directory (which is usually /usr/local/mozilla), or any other directory where only the root user normally has write access, you must first start Mozilla as *root* before other users can start the program. Launching the application initially as the root user generates a set of files required for later use by other users.

To install Mozilla by downloading the Mozilla installer, follow these steps:

1. Create a temporary directory, such as mozilla, using **`mkdir mozilla.`**
2. Click the link on the site from which you are downloading the Mozilla installer file (mozilla-i686-pc-linux-gnu-1.3.1-sea.tar.gz):

   `http://ftp.mozilla.org/pub/mozilla.org/mozilla/releases/mozilla1.3.1/`
   `http://www.mozilla.org/releases/old-releases-1.1-1.4rc3.html#1.3.1`
   `http://www.mozilla.org/releases/`
3. Switch to the temporary directory (in this case, the mozilla directory using **`cd mozilla`**), and decompress the archive with the following command:

   ```
   tar zxvf mozilla-i686-pc-linux-gnu-1.3.1-sea.tar.gz
   ```
4. The installer is now located in a subdirectory of Mozilla named mozilla-installer. Change to the mozilla-installer directory:

   ```
   cd mozilla-installer
   ```

   Run the installer with the **`./mozilla-installer`** command.
5. Follow the instructions in the install wizard for installing Mozilla. (Refer to the next series of screen shots, beginning with Figure 8-1 on page 266.)
6. When the Mozilla installation program launches, you will see the Read me window.

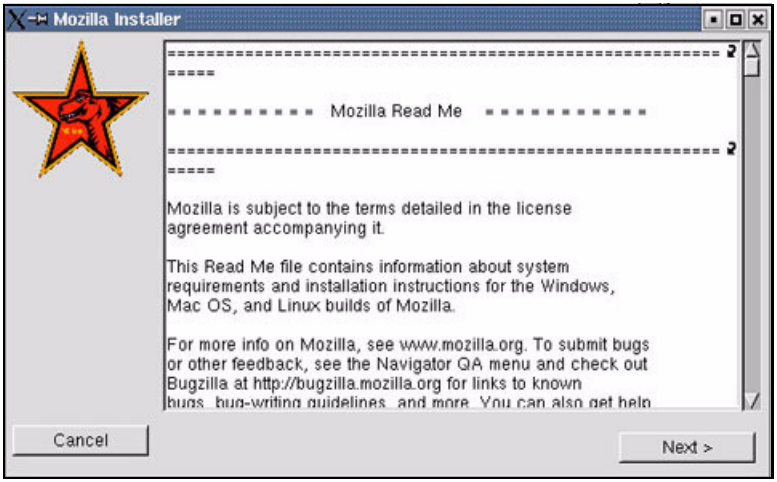


Figure 8-1 Mozilla Read Me

7. Click **Next** to begin the Mozilla installation.
8. After you have read and accepted the license shown in Figure 6-2, click **Accept**.

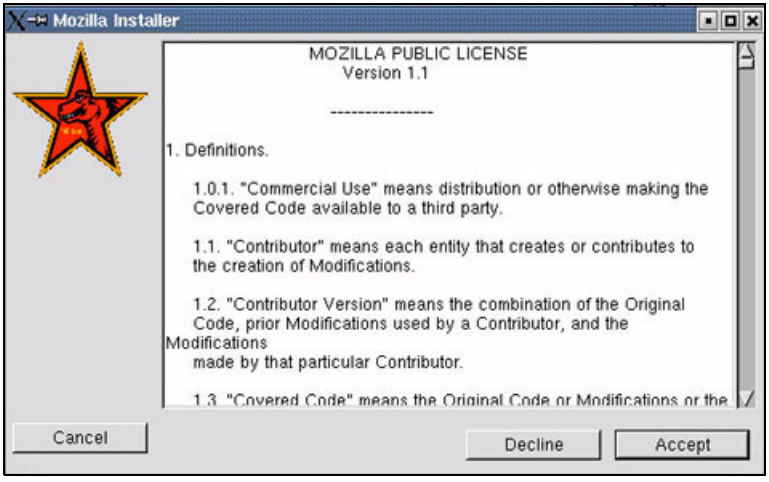


Figure 8-2 Mozilla Public License

9. Select the components of Mozilla that you wish to install from among the setup types: Typical, Complete, Navigator, or Custom (Figure 8-3). We selected Typical, and we accepted the default directory, Keep in mind that it is not necessary to install the program files to the directory /usr/local/mozilla. Click **Next** to continue the installation.

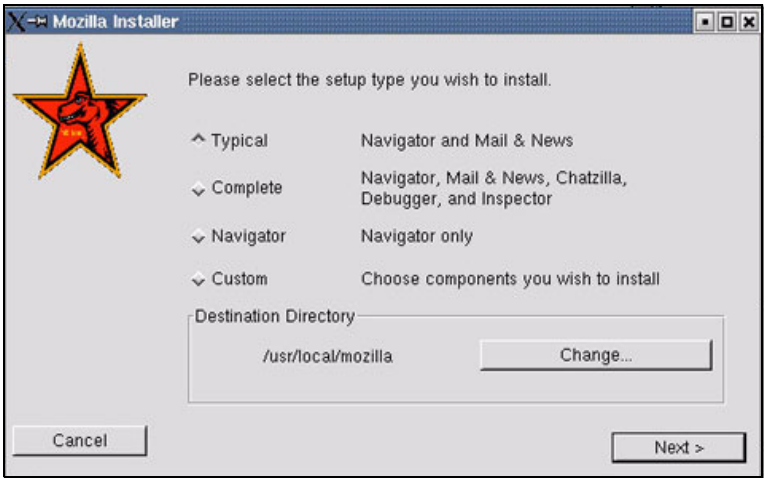


Figure 8-3 Setup type and Destination Directory

10. Click **Yes** to accept and create the default directory shown in Figure 8-4.

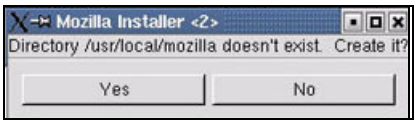


Figure 8-4 Create the program files directory

11. Click **Install** if you are satisfied with the configuration. If you have entered something incorrectly, click **Back** to correct it.

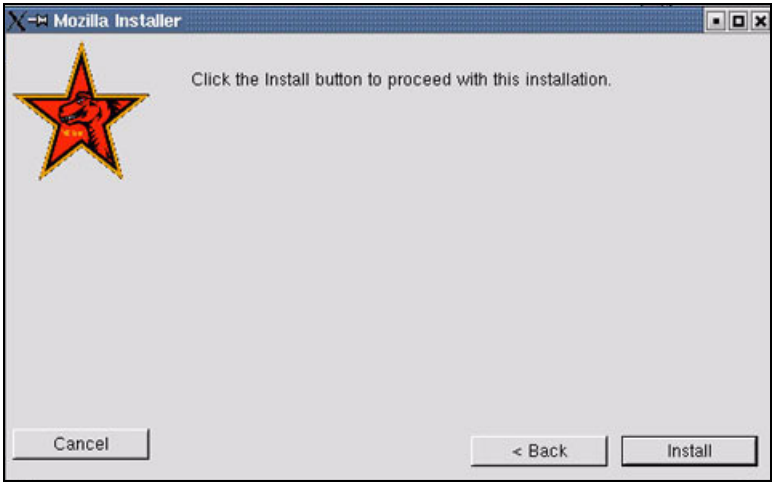


Figure 8-5 Proceed with installation

Important: If you have a slower machine, be aware that the installation may take some time. In this case, the installation progress may appear to hang indefinitely, even though the installation is *still in process*.

12. When the window shown in Figure 8-6 is displayed, the installation of Mozilla is complete. Click **OK**.

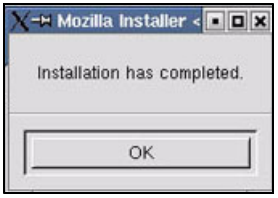


Figure 8-6 Installation complete

Linking the Mozilla icon to the KDE Panel

To link the Mozilla application and icon to the KDE Panel, follow these steps:

1. Click the KDE main menu button and open **Panel** → **Add to Panel** → **Launcher**.
2. Right-click the Mozilla icon on the panel and enter this command:

```
directory_name/mozilla
```

In 8.6.4, “Mozilla does not start after launching DOLS” on page 314, we describe how to install DOLS when Mozilla is not installed in the user’s home directory, as it requires some specific steps.

The directory_name is the path in which Mozilla was installed. For example, the default directory that Mozilla suggests is /usr/local/mozilla.

3. Type in a name for the icon, and type in a comment if you wish.
4. Click the icon button and for the icon’s location, type in `<directory_name>/icons/mozicon50.xpm` where <directory name> is the directory in which you installed Mozilla. For example, the default directory is `/usr/local/mozilla/icons/mozicon50.xpm`.

8.2 Offline usage and Domino Offline Services for Linux

In this section we discuss some of the factors that you should consider when deploying DOLS for Domino Web Access 6.5 on your Domino server infrastructure, especially for the Linux platform. There are many possible variations of Domino architecture, each of which has some unique characteristics to consider. For example, when migrating users to Domino Web Access 6.5, many organizations may want to take a gradual approach. Organizations may continue leveraging their prior investments with Notes clients and Domino servers for some period while migrating their users, until the majority are using Domino Web Access. Other organizations may want to keep users accessing their Notes clients in the office, while using Domino Web Access 6.5 to access their mail files from home or from an Internet café.

This next sections about Domino Offline Services for DWA 6.5 cover the following topics:

- Domino Offline Services functionality
- Setting up DOLS on a Linux server
- Administration of DOLS
- Domino 6.5 server configuration document and DOLS
- DOLS client deployment for online users
- Requirements of the local DOLS configuration for Linux
- Uninstalling DWA 6.5 Offline Services

8.2.1 Overview of DOLS

Domino Offline Services (DOLS) provides a way for users to take IBM Lotus Domino Release 6.x Web applications offline, work in them, and synchronize the changes with an online replica on the Domino server. Users are not required to have IBM Lotus Notes Release 6.5 client, because the applications are accessed with a browser. DOLS enables users to work offline, disconnected from the

network, and provides some replication features that Notes users expect when working in the Notes client.

Nearly all Notes functionality is retained when a DOLS-enabled application (called a subscription) is taken offline. Users can compose, edit, delete, sort, and categorize Notes documents, and perform full-text searches. DOLS subscriptions can make full use of Java applets, agent execution, and workflow. DOLS also supports full data replication, retains application logic, and supports the full Notes security model.

To DOLS-enable an application, the developer and administrator must set up and configure a DOLS subscription for offline use.

The developer copies a number of elements into the subscription, makes design changes if necessary, and configures the subscription in the Offline Subscription Configuration Profile document.

The administrator makes sure DOLS is installed properly on the server, sets security for the subscription, sets up agents, makes changes to the Offline Subscription Configuration Profile document if necessary, and helps users install the subscription.

After the subscription is enabled, users can access it on the server using a browser. The user clicks in a new frame on the subscription's main page to open a JavaScript menu. Choosing **install** from the menu installs the subscription on the computer.

For users with the Windows OS also installed on their computer, the Lotus Domino Sync Manager (previously the iNotes Sync Manager), is the utility for managing DOLS subscriptions. Users can open subscriptions online or offline, synchronize, and set subscription properties with the Sync manager.

Note: DWA 6.5 represents the first IBM Lotus solution for a Linux Desktop that enables you to replicate the mail file using Domino Web Access offline. Currently only mail is supported for DOLS under Linux.

To provide Domino Web Access users with the ability to work offline, you must enable DOLS when you set up the server. (The manual configuration of DOLS is discussed in "Configure DOLS manually" on page 273.) When a Domino Administrator is planning a Domino Web Access 6.5 deployment, DOLS can be turned on or off. If you are not planning to have offline users, Domino Web Access 6.5 offers a simple deployment model with no-touch desktop installation.

Users require a Notes ID to be imported and configured within their Domino Web Access DOLS client, so that DOLS can synchronize the offline mail file with the

server. The default DOLS configuration prompts the user for a Notes ID the first time they go offline with Domino Web Access.

Restriction: In our test configuration, this requirement for the Notes ID to be installed locally was not clear. Initially, without the Notes ID installed, it appeared that DOLS was not working as expected. When we attached the ID file in the mail file, DOLS worked successully.

When DOLS is enabled, users can maintain full fidelity of the Domino Web Access 6.5 environment on the local desktop. A local installation of DOLS is required on the client side.

8.2.2 Functionality

DOLS is a subset of the Domino HTTP and the Replicator tasks, which are modified to run locally in a different configuration. In Domino Web Access 6.5, the Linux user has the ability to synchronize the personal mail file to perform the following tasks offline:

- Reading encrypted mail
- Writing encrypted mail
- Creating calendar entries
- Creating tasks
- Deleting documents in the mail file
- Creating documents in the notebook page
- Reading and writing personal contacts

8.3 DOLS Setup on a Linux server

The following section describes important aspects of setting up and configuring DOLS on the server.

Domino Offline Services (DOLS) must be configured on the Domino server for users to be able to take applications offline and use only a browser to work with them. The Domino Web Access template (iNotes6.NTF) is enabled for DOLS and supported on Linux by default.

The topics to covered in this section are:

- 8.3.6, “DOLS, agents, and subscription considerations” on page 282
- 8.3.7, “Server configuration” on page 284
- 8.4, “Installing and configuring the DOLS client” on page 286

8.3.1 Configure DOLS during Domino Server setup

This section describes the steps that should be taken during the Domino Server setup procedure to enable DOLS. If you do not enable DOLS during the actual setup process, 8.3.2, “Configure DOLS manually” on page 273 describes an alternate approach to configuring DOLS.

During the setup and configuration of your Domino server, follow these steps:

1. Under **Setup Internet services for**, select **Web Browsers (HTTP services)**, and then click **Customize**.
2. As shown in Figure 8-7 on page 272, in the Domino tasks list, check **DOLS Domino Off Line Services**. Click **OK**.

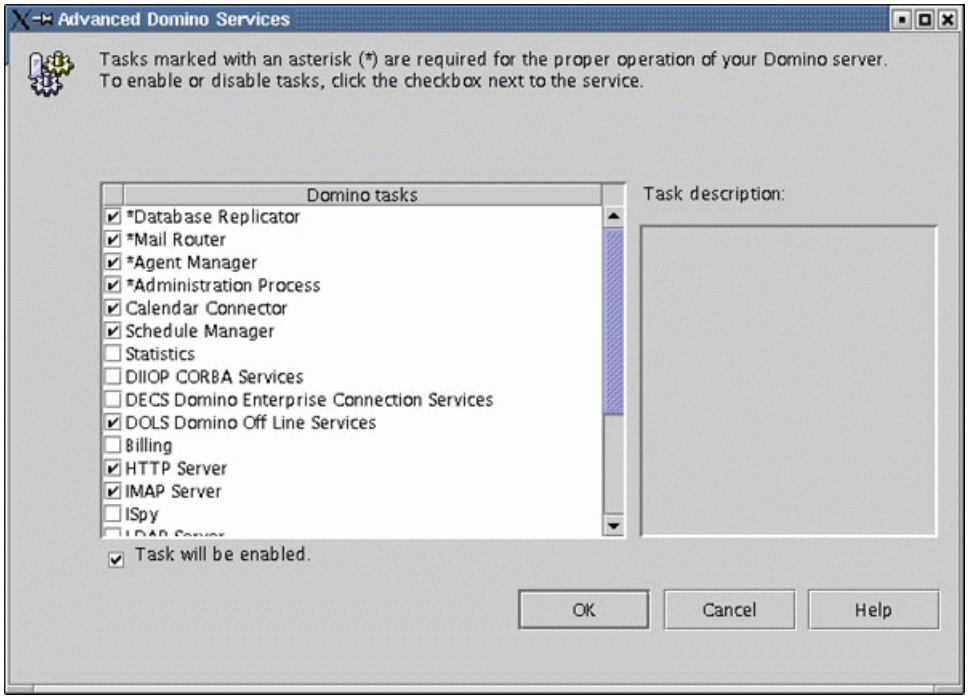


Figure 8-7 Installation screen with choice of Domino Offline Services

3. At the end of setup, when you have the option to create an access control list entry, add the group **LocalDomainAdmins** to all databases and templates.

4. Accept the default option **Prohibit access to all databases and templates**. If you deselect this option, you must open the ACL for each DOLS application and assign No Access to Anonymous.
5. Make sure that the host name of the Linux server is identical to the fully qualified host name in the server document.

8.3.2 Configure DOLS manually

If you do not configure DOLS during Domino Server Setup, you can configure it manually by editing the Server document.

1. Open the Server document.
2. Click **Internet Protocols - HTTP**.
3. In the DSAPI filter file names field (Figure 8-8), enter the name of the DSAPI filter that corresponds to the operating system the server is running on. For example, on our Linux servers, we use `dolextn`. After clicking **Save & Close**, you must restart either the Domino server or the HTTP task.

> **Note:** There is no need to use the lib prefix from the library libdolextn. The name dolextn is working in our scenario as expected (see Figure 8-8). If you load more than one DSAPI library, however (for example, SSO extension), we recommend that you write the full name of the library.

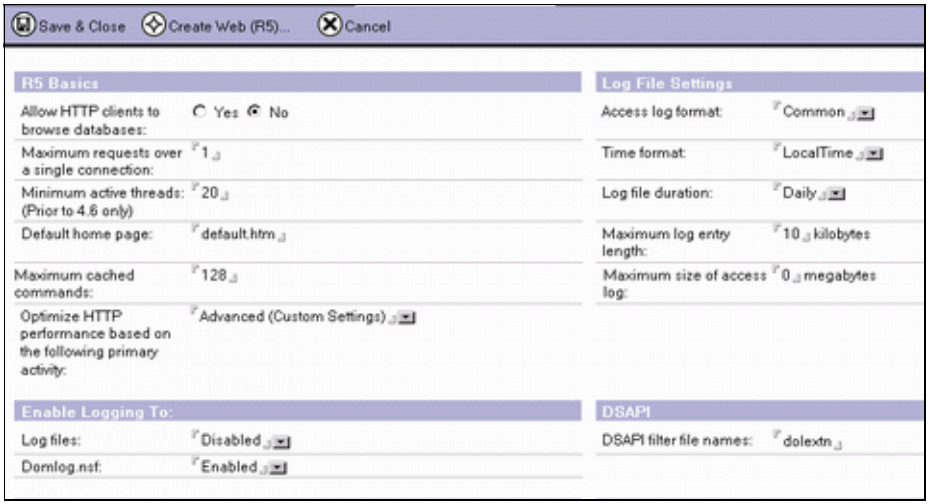


Figure 8-8 DSAPI filter section showing the DOLS extension

4. (Optional) Open the Server document and click the **HTTP** tab. In the Timeouts section, change the Output timeout to 300 seconds (Figure 8-9) to allow enough time for downloads to a LAN.

> **Tip:** If you must support users connecting with less bandwidth (such as GPRS or ISDN connections). we recommend that you increase this value to 600 seconds. Just for DOLS, a Linux user is required to download 65 MB of install components, not including the mail file.

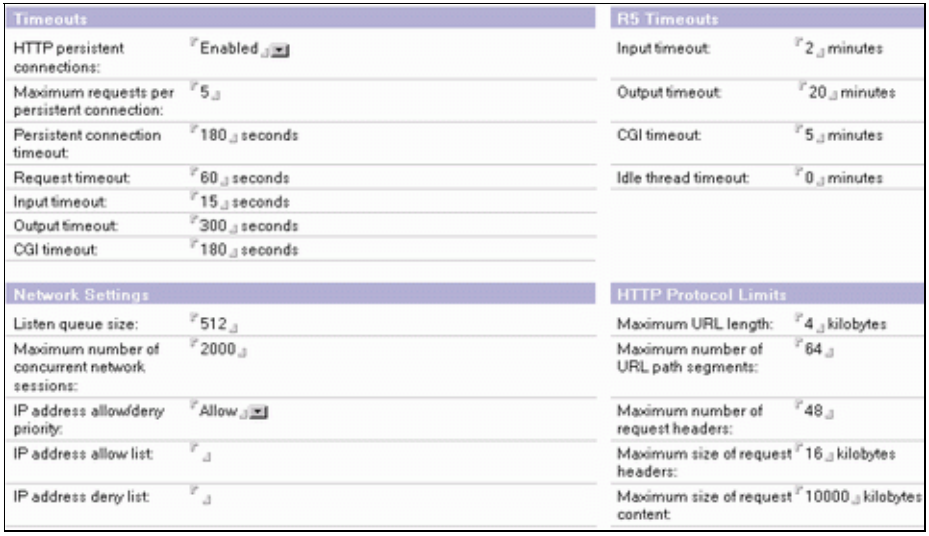


Figure 8-9 Output timeout field on Server document

Attention: Ensure that Anonymous is set to **No Access** in all of the Mail files; otherwise you will not see all documents included in the DWA Mail file. Alternatively, you can disable the Anonymous users for the HTTP server that serves DOLS in **Ports** → **Internetports**, as seen in Figure 8-10.

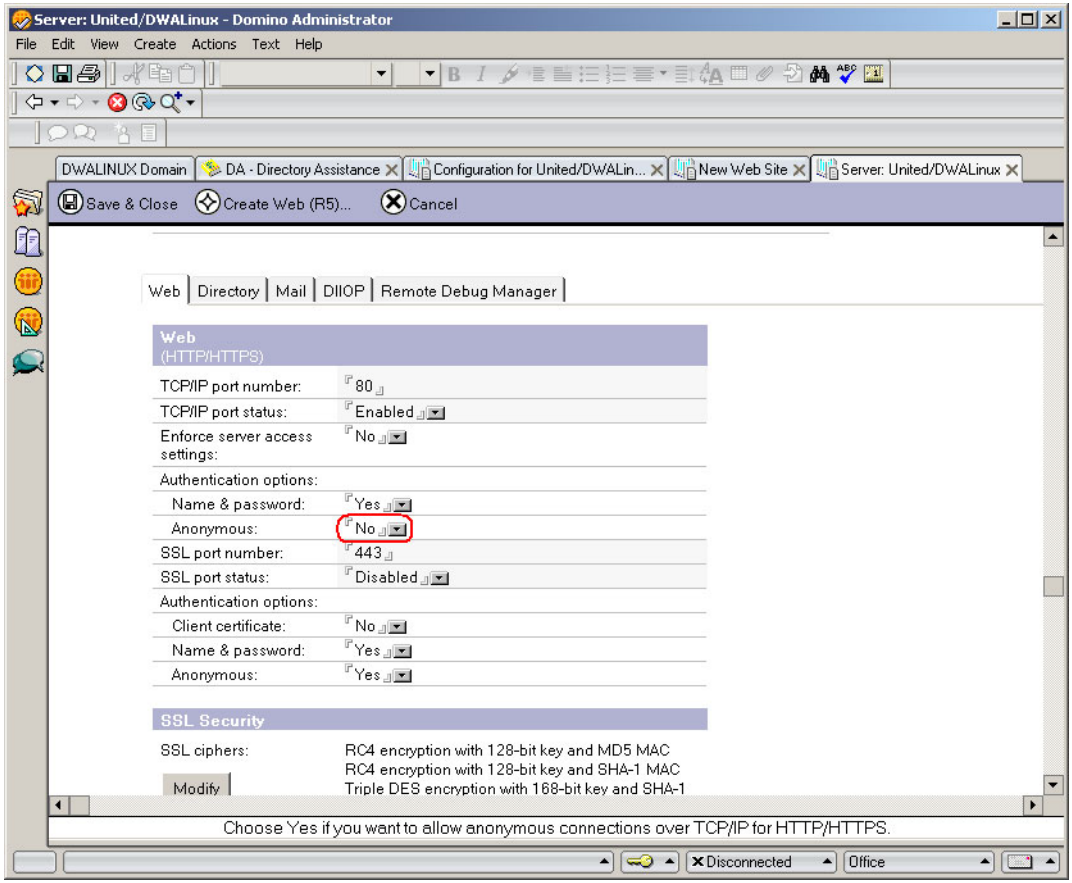


Figure 8-10 Restricting the anonymous access on your DOLS server

Important: For loading the DSAPI filter, the HTTP task must be restarted by typing the following command: `tell http restart`

At server startup, you should see the following console message: `Domino Offline Services HTTP extension <Release version> loaded.` If you see this, the DSAPI file filter extension field is populated correctly.

8.3.3 DOLS Administration

This section provides an overview of DOLS Administration.

Creating the Offline Services administration database

Create and initialize the Offline Services (administration) database by performing the following steps:

1. Open the Notes client.
2. Select **File** → **Database** → **New** to open the New Database window (Figure 8-11).
3. Type `doladmin.nsf` (for DOLS security policy) as a file name.

> **Attention:** Domino expects the specific filename *doladmin.nsf*. If you use another filename, you will not be able to see the tab for Offline Services in the Domino Administration client.

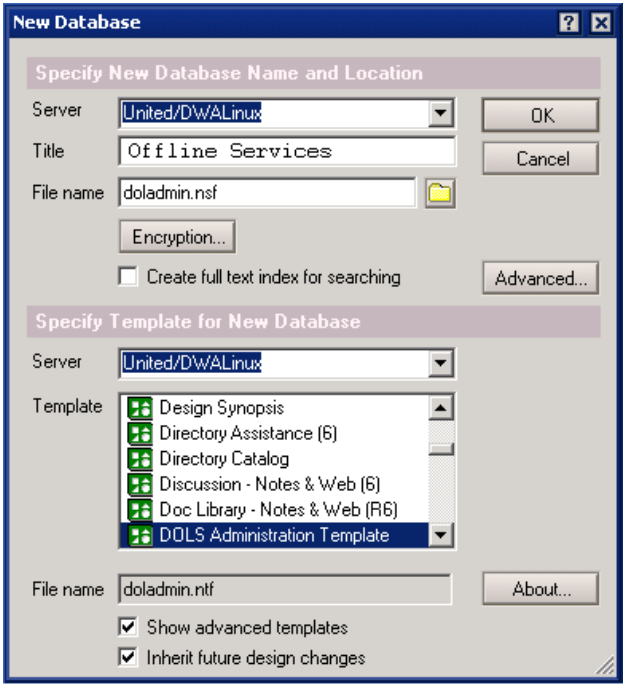


Figure 8-11 Creating a new DOLS administration database

4. Type `Offline Services` for the Title and choose the DOLS Administration Template 1.0.

Note: You must check the box for Show advanced templates in order to see the DOLS Administration Template.

5. Specify the target Domino server where DOLS is to be enabled as the name of the server and template server for the new database.
6. Click **OK** to create the database.

After the database is created, restart the Domino Administrator and click the **Configuration** tab. The name of the Offline services is an option in the Navigation pane, as you can see in Figure 8-12.

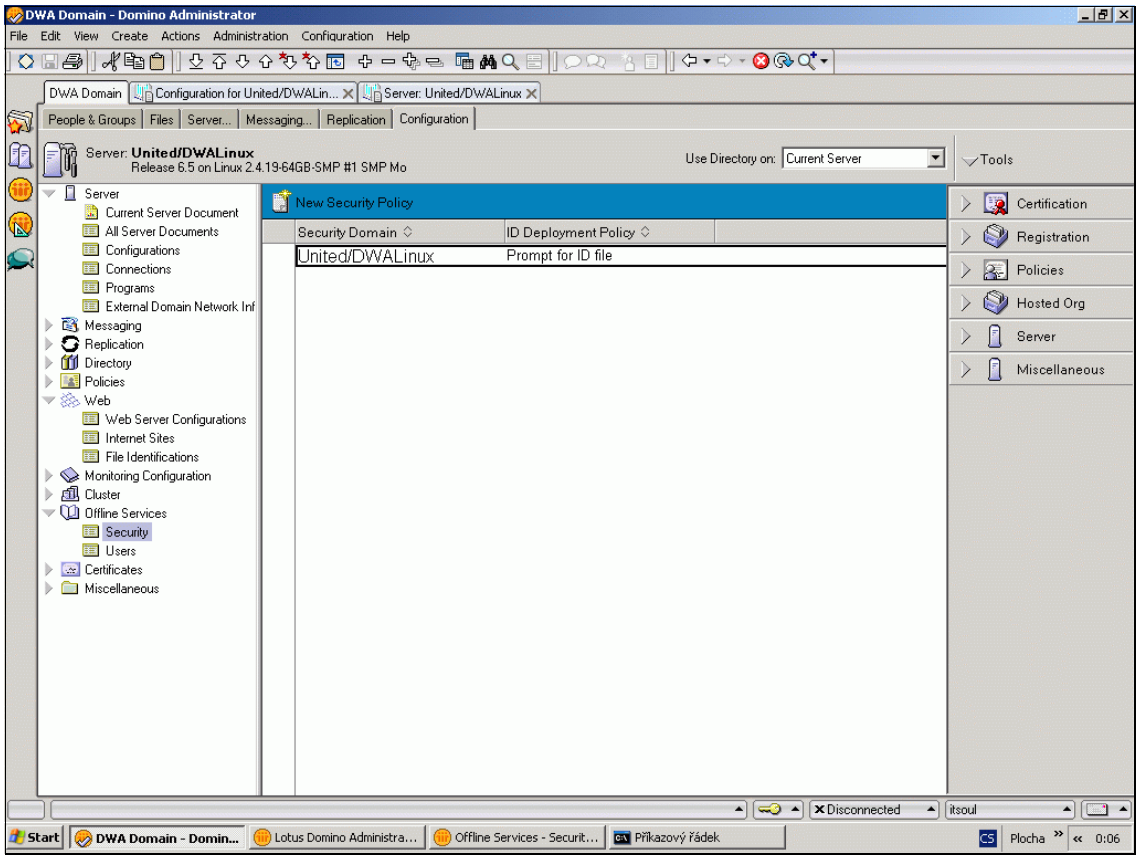


Figure 8-12 Domino Offline Services in Domino Administrator client

Modifying the DOLS configuration for security policies

To modify the DOLS configuration, open the Domino Administrator. Choose the **Configuration** Tab and select **Offline Services**.

1. Select the **New Security Policy** option to create one or more DOLS security policies for the target server. Assuming that you do not specify a Security Policy, the default behavior is to prompt end-users to provide ID files when going offline. You can explicitly control and override that default for given security domains by setting this to **Automatically generate user IDs** or **Use Domino Directory for ID lookup**.

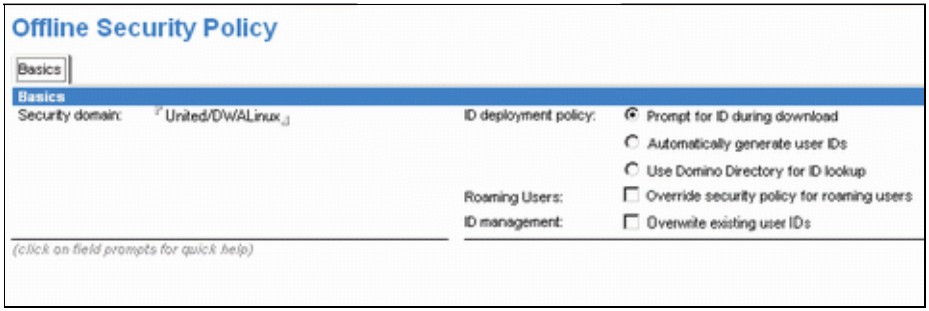


Figure 8-13 New DOLS Security Policy

2. Exit the Notes client. Shut down and restart the target server. DOLS is now available on the server.

You should now be able to go offline on a Red Hat 7.2 Linux client without the Notes ID imported if you have completed the following criteria:

- You have created a valid Offline Security Policy in the dolamin.nsf database on the server
- The Offline Security Policy is set up for the user organization (/organization /countrycode or, if no country code is being used, just /Organization),
- You have configured the Offline Security Policy to autogenerate the user IDs.

This means that you *must* attach the current cert.id for that server domain into the Offline Security Policy document and set the password for that cert.id. If you have tried this and you are still failing when trying to go offline on Linux, try this troubleshooting approach:

- Test whether you can go offline with the same user database from an Internet Explorer 6.x browser on a Windows client, to see whether the Offline Security Policy is working correctly.

Attention: Within our lab environment, we tested using all possible settings but were only successful using Domino 6.5 for DOLS Linux when trying with the first and the second settings: **Prompt for ID during download** and **Automatically generate IDs**.

8.3.4 DOLS in a clustered environment

Before using DOLS on a clustered Domino 6.5 server, make sure of the following:

- The Domino server is either a Domino Utility Server or Domino Enterprise Server.
- All servers in the cluster run the same release of Domino with DOLS.
- Clustered server management is running to handle both failover of replication and HTTP.
- Subscription directories must have the same name on every clustered server. For example, if a subscription is under \data\Webmail user\7CD5957CB669AE2285256BDF00567AD8\, this name cannot be different on another server in the cluster.
- Internet Cluster Manager is running as a task on the servers.

Attention: Internet Cluster Manager (ICM) is an *essential requirement* for providing failover and load balancing for Domino Offline Services. Note that in conjunction with Tivoli Access Manager 4.1 and Webseal, or using other third-party reverse proxies, you must disable the ICM because of the HTTP redirect 302, which is internally managed by Internet Cluster Manager to redirect the user to another domino server. You can use an HTTP sprayer instead of ICM, which is a common way of referring to a load balancer in a situation where multiple servers are run in a cluster that shares the same static resources via a shared file system. Multiple server engines are used concurrently behind a sprayer, which is also called the interactive network dispatcher. An example of this type of configuration can be seen in WebSphere 5 Edge components. This is included as an optional package in WebSphere 5 Enterprise Edition, instead of using the built-in Domino Internet Cluster Manager. See Chapter 3, “Deployment considerations” on page 59 for additional details on this topic.

8.3.5 Using Web Site documents

The Domino 6 server introduces the ability to organize multiple Web sites via Web Site documents within the Domino Administrator client. This allows more flexibility and control than the R5 method of Virtual Sites and Hosts. A Web Site

document is enabled on the basis of the server document, as shown in Figure 8-14.

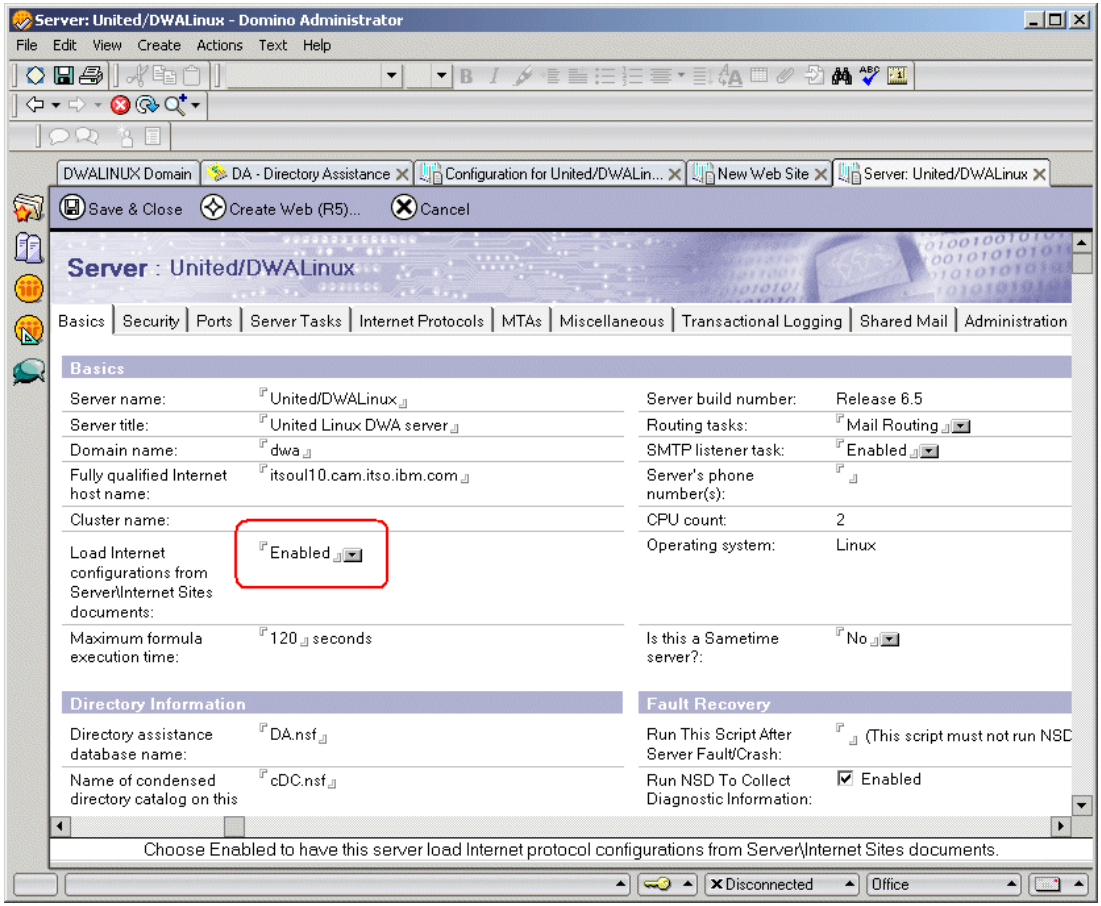


Figure 8-14 Basics tab of the Server document in Domino Administrator

If you create a Web site document (a type of Internet site document - see Figure 8-15 on page 281) on the Domino server, you must add the appropriate DOLS DSAPI filter filename to the DSAPI field of the Web site document for DOLS to be enabled. If there are several Web Site documents, you must add the DSAPI filter filename to each one. To add the DOLS DSAPI filter filename to a Web site document, follow these steps:

1. Open the Web Site document.

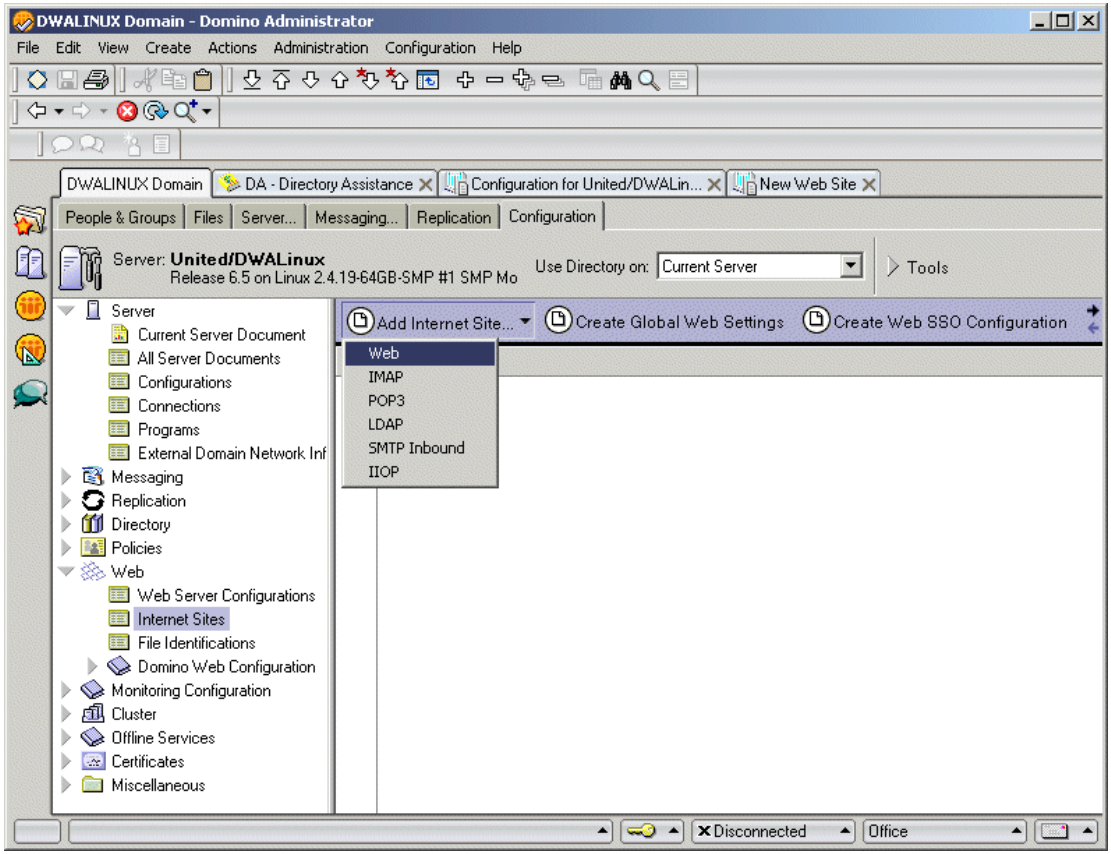


Figure 8-15 Web site in Lotus Domino Administrator 6.5: Create a Web site document

2. Click the **Configuration** tab.
3. In the DSAPI filter field, enter the name of the DSAPI filter that corresponds to the operating system the server is running on. For example, on our Linux servers, we use `dolextn` (Figure 8-16 on page 282).
4. Save the form and restart either the Domino Server or just the HTTP task.

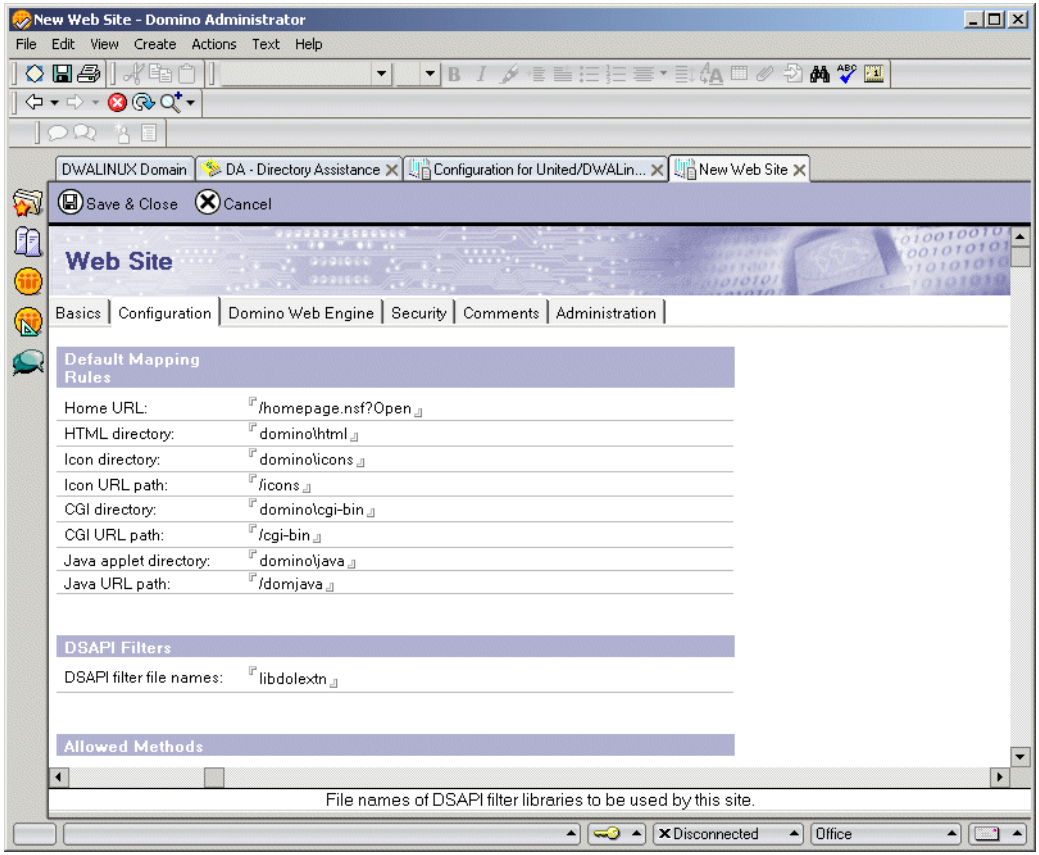


Figure 8-16 Web site document with the configuration tab to enable DOLS

8.3.6 DOLS, agents, and subscription considerations

In this section, we discuss how agents work within subscriptions and what can be done to make these agents work offline.

Agents are small programs that perform actions on a Domino Server. Because they can be powerful tools, they must have permission from the server to work. Agents inherit the permissions of their *signer*. An agent's signer can be the user who created it or a user or organization designated by an administrator. An administrator can also register a *dummy* or security/signing-only user on the server and make it the signer of agents. This provides more control and security, because the dummy user will not do anything that the administrator does not want done.

For an agent to perform actions on a server, an administrator must add its signer, (or a group the signer is in) to the Server document (**Security** → **Agent Restrictions**).

Agents can perform both unrestricted actions and restricted actions. Restricted actions can potentially cause serious damage to the server, so administrators must be careful about the permissions of agents that perform restricted actions.

Important: There are two kinds of agents: triggered and scheduled. Triggered agents are activated by a user action, such as clicking a button or selecting a menu item. Scheduled agents run automatically, on a schedule or when events happen inside a database, such as a new mail document arriving. Only triggered agents work offline because the agent manager is not run.

If a subscription contains triggered agents, do the following to make them work offline:

1. If the subscription contains restricted agents, create a group called DOLS_Restricted_Agents in the Domino Directory.
2. Add the full names of the signers of the restricted agents to the DOLS_Restricted_Agents group.
3. If an agent has been configured to run as a Web user (**Agent Properties** → **Design** tab → **Run as Web user**), use the full name of its signer. Otherwise, use the full name of the signer who modified it last (for example, NewDevelopment/DWALinux).
4. If the subscription uses unrestricted agents, create a group called DOLS_Unrestricted_Agents in the Domino Directory.
5. Add the full names of the signers of the unrestricted agents to the DOLS_Unrestricted_Agents group.
6. If an agent has been configured to run as a Web user (**Agent Properties** → **Design** tab → **Run as Web user**), use the full name of its signer. Otherwise, use the full name of the signer who modified it last (for example, NewDevelopment/DWALINUX).
7. In the Server document, on the Security tab in the Agent Restrictions section, add DOLS_Restricted_Agents to the Run restricted LotusScript/Java agents field. Add DOLS_Unrestricted_Agents to the Run unrestricted LotusScript/Java agents field.
8. Make sure that agent signers have at least Editor access in the ACLs of all databases where the agent runs.
9. Use the DOLCert.id (in the Domino data directory) as the certifier ID to create cross-certificates for each user or organization you specified as being able to

execute agents. DOLCert.id creates cross-certificates issued by O=DOLS. There may already be cross-certificates issued by the Lotus Domino 6 server for these names. You can use the ID file or public key for the agent user and organization to generate cross-certificates.

Important: If a database uses agents, be sure that they are all signed and that the server's CERT.ID is cross-certified with the DOLCERT.ID.

8.3.7 Server configuration

This section describes settings and configurations required for Domino Web Access 6.5, including the Administration for DOLS servers.The configuration document in the Domino 6.5 directory, as shown in Figure 8-17, has a set of features available for Domino Web Access 6.5. By default, most of these features are available to the Domino Web Access client unless you take action to disable them.

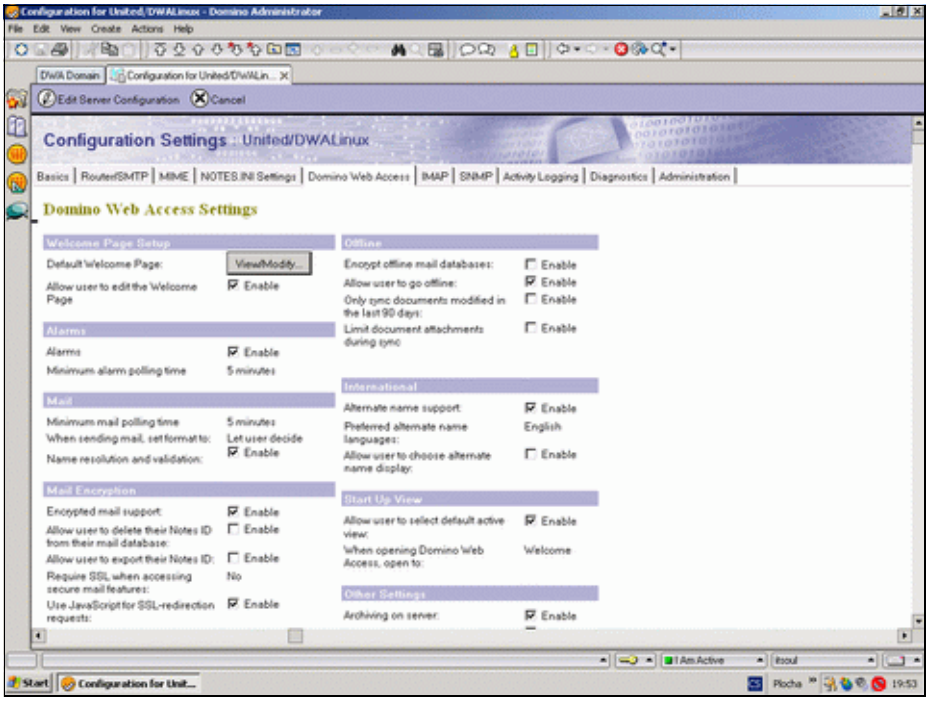


Figure 8-17 Domino Web Access 6.5 Configuration Settings

DOLS configuration options

The configuration settings document in the Domino directory is the right place to define settings, which will then be pushed out to the DOLS clients automatically.

Within this section, we describe the key configuration parameters shown in Figure 8-17 on page 284.

- Encrypt offline mail database

  This option applies to laptop-computer users who sync their mail file with Domino Web Access in an insecure environment. We recommend that the Administrator enable this security feature to help prevent data loss.

  Tip: We recommend that your organization make a formal enterprise policy for your production environment, and that all the functions are thoroughly tested before you plan a mass deployment strategy for the offline clients. Otherwise you should give the end user the right to determine and enable which setting is best for the specific circumstances and environment. For example: If the user has small bandwidth for GPRS or ISDN, a choice can be made in the Offline Client to enable the *Limit document attachments during sync* option. A policy that enables this feature by default would cause problems if users change their bandwidth access or need access to an attachment.

- Allow user to go offline

  We strongly recommend that you enable this function regardless of whether your Domino Web Access 6.5 Linux users go offline. By switching on this option, your users can ultimately decide whether they want to go offline. Keep in mind that an important requirement for anyone planning to use the offline capability is the ability to set up the Linux client (Mozilla browser) as we describe in detail, beginning with 8.4, “Installing and configuring the DOLS client” on page 286.

- Allow user to choose an encryption level

  This setting, when enabled, overrides the administrator-specified encryption level and enables users to choose their own encryption level.

- Only sync documents modified in the last x days

  Enter the number of days to wait before synchronizing offline databases. (The default value is 90.) Users can reset this for each offline subscription file using the Domino Sync Manager.

Attention: The most important setting for running Domino Offline Services within the configuration document is *Allow user to go offline = Enable*.

8.4 Installing and configuring the DOLS client

The remaining sections of this chapter focus on installing and configuring the DOLS offline client on a Linux client.

8.4.1 Overview of supported Linux distributions and DOLS

The Domino Web Access 6.5 release notes state that Red Hat 7.2, SUSE 8.0 and SUSE 8.2 Professional are the only Linux distributions that are supported for both online and offline usage (DOLS). The redbook team did significant testing in this area, however, to verify functionality using additional distributions of Linux, as well as experimenting with the Mozilla Firebird 0.7 browser. Table 8-1 provides a detailed overview of our results. Note that in order for the DOLS client to successfully launch a browser session when running on SUSE 8.0 and 8.2 Professional, it was necessary to modify the browser configuration settings.

Table 8-1 Linux distributions and support for the DOLS client

Linux distribution	DWA 6.5 (Online)	DWA 6.5 DOLS client (offline)	Comments
Red Hat 7.2	► Success using Mozilla 1.3.1 ► Officially supported configuration	► Successful install ► Officially supported configuration	► Installation successful ► Icon displayed as expected
Red Hat 8.0	► Success using Mozilla 1.3.1 ► Officially supported configuration	► Successful install ► *Not* officially supported configuration	► Icon not displayed as expected. (See also 8.6.3, “Case of the missing icons for DOLS” on page 313). ► Set up browser as described in Figure 8-49 on page 321.
Red Hat 9.0	► Success using Mozilla 1.3.1 ► Officially supported configuration	► Unsuccessful install ► *** *Not* officially supported	We do not recommend using this distribution with DWA 6.5.

Linux distribution	DWA 6.5 (Online)	DWA 6.5 DOLS client (offline)	Comments
SUSE 8.0 Professional	► Success using Mozilla 1.3.1 ► Officially supported configuration	► Successful install ► Officially supported configuration	► Icon not displayed as expected. (See also 8.6.3, “Case of the missing icons for DOLS” on page 313.) ► Set up browser as described in Figure 8-49 on page 321.
SUSE 8.2 Professional	► Success using Mozilla 1.3.1 ► Officially supported configuration	► Successful install ► Officially supported configuration	► Icon not displayed as expected ► Set up browser as described in Figure 8-49 on page 321.

Be aware of the following important configuration notes used in determining the testing results above:

- Red Hat 7.2, SUSE 8.0 Professional, and SUSE 8.2 are the only officially supported Linux distributions for working with the DOLS offline client.
- We performed limited testing in our lab environment at the ITSO with Mozilla Firebird 0.7 on Linux and Windows and were pleased to discover that this browser could be an excellent alternative for Mozilla 1.5, *while working in an online environment*. We are aware, however, that Firebird is only a beta version at this time and Domino Offline Services does not work with Firebird.

8.4.2 Deployment and installation of the DOLS client

The installation of the DOLS client uses a Mozilla plug-in that is *only supported by Mozilla 1.3.1*. Many people may be wondering why DWA 6.5 only supports this version of Mozilla at this time. The reason for the restriction is based primarily on the plug-in. The DOLS Mozilla plug-in is only supported and compiled with Mozilla 1.3.1.

Restriction: Mozilla 1.3.1 is the only supported version for IBM Lotus Domino Web Access 6.5 that can run offline.

Considerations for deployment

The following points are important to consider prior to a deployment of DOLS:

- Deployment should only occur after upgrading mail templates to iNotes6.ntf for existing users or creating new mail files using iNotes6.ntf mail template for new users. See 6.6, “Converting mail files to Domino Web Access 6.5” on page 242 for more information about this topic.
- The fully qualified Internet host name (including domain name) of the server must be used to access the mail file. For example, use:

  `http://itsoul10.cam.itso.ibm.com/mail/mailfile.nsf`

  Do not use the common name of the server, such as this:

  `http://itsoul10/mail/mailfile.nsf`
- Make sure that your policy documents have been set up correctly, as described in 8.3.6, “DOLS, agents, and subscription considerations” on page 282. The redbook team discovered that if the user does not already have a Notes ID attached into their browser through the preferences settings (see 6.4.1, “Encrypted mail support” on page 219), and a policy document has not yet been set up correctly, the only error message that will be displayed is an Unsupported Configuration error similar to that shown in Figure 8-18.

Attention: In our configuration we had an issue with the DOLS policy document. If the user had no Notes ID file attached, an Unsupported Configuration error (Figure 8-18) appeared.

Figure 8-18 Error message resulting from going offline with no attached ID file

Attention: If you receive an Unsupported Configuration error, check your DOLS policy document. The DOLS policy document must have the option set to either Prompt for ID File or Create Automatically. For this option, you must also provide the cert.id in the DOLS policy document.

Figure 8-19 illustrates how a user may create a new subscription by selecting **Install Subscription** from the **Go Offline** button on the Welcome page.

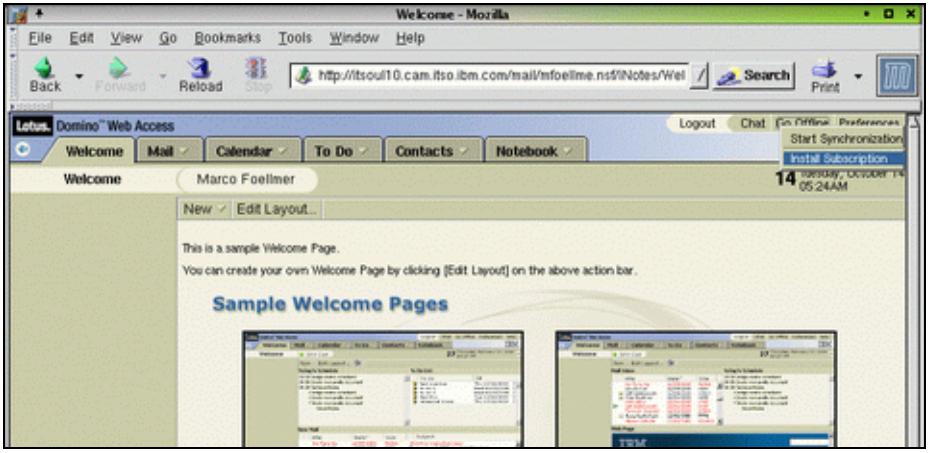


Figure 8-19 Normal DWA 6.5 under Linux with the Go Offline button

- Finally, remind users to use their Internet password because it may be different from their Notes password.

> **Note:** If you change the configuration in the DOLS policy document, be aware that the end user must reinstall the subscription.

8.4.3 Local requirements: checklist for installing DOLS plug-in

This topic provides a checklist for installing the DOLS plug-in, including all permissions the Linux desktop needs to run DOLS for Linux. The commands show how to prepare the Linux OS and specific directories for using DOLS.

> **Restriction:** This DOLS release supports only one Linux user. There is no chance to get multi-user support running.

1. First, you must prepare the permissions of Mozilla directories using the root user. The following directories must have *write access* for the user for installing the DOLS plug-in. The best approach is to use the group of users to set up the permissions.
   - mozilla/plugin
   - /usr/tmp
   - mozilla/components
   - /home/marco

Note: This is the home directory of the user, in this case, Marco.

2. Change to the installation directory of the browser (for example, if Mozilla is the installation director, /opt/mozilla or /usr/lib/mozilla) and perform `chgrp <group>./components` and `chgrp <group>./plugins`, where <group> is a group that has the DWA users (in our case `users`).
3. Change the permissions so that the group has write access:

   `chmod g+w ./plugins and chmod g+w ./components`
4. Now start the browser as the user who wishes to install DOLS.

Attention: Do not install DOLS as a root user. This does not work, because DOLS requires a user home directory by default. You could create a link, but we advise that it is preferable to install as a normal user.

5. Again, ensure that you have installed the right version of the browser (see 8.1.1, “Mozilla installation steps” on page 265), by choosing **Help** → **About Mozilla** from the Mozilla menu bar (Figure 8-20).

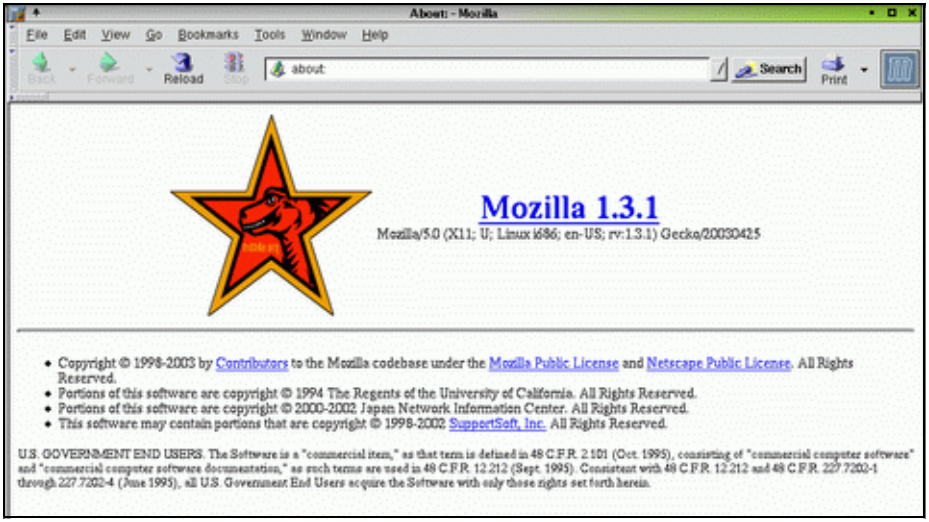


Figure 8-20 Version information for the Mozilla browser

Attention: As we have mentioned, the only supported browser version with DOLS is *Mozilla 1.3.1*. The DOLS plug-in is compiled only for this version. At the time this book was being written, this plug-In does not work on other versions of Mozilla.

6. In this same Help menu, make note of the installed plug-ins by selecting **Help** → **About Plug-Ins** (Figure 8-21).

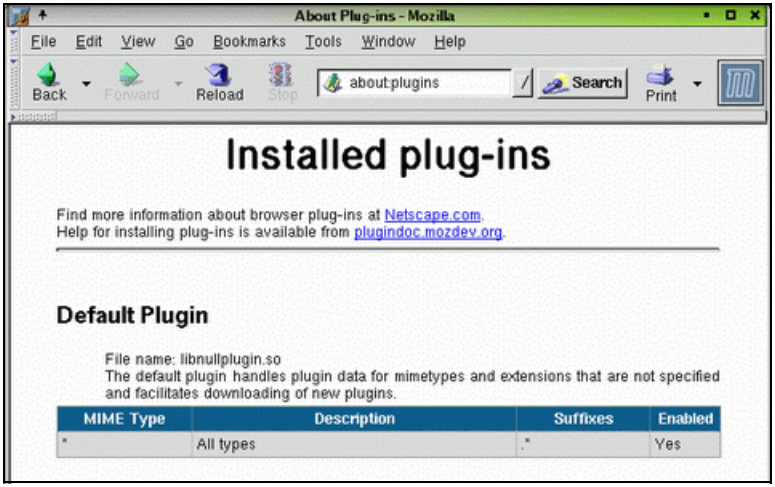


Figure 8-21 No plug-ins: a clean install of Mozilla

7. Next, log on to your mail file by choosing the server URL. In our testing environment, this was http://itsoul10.cam.itso.ibm.com. Type your username and the password.

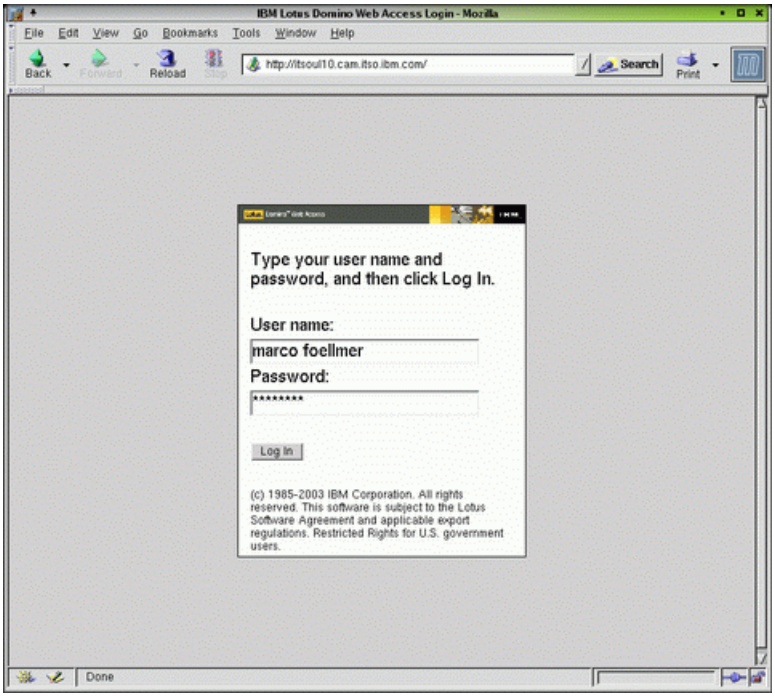


Figure 8-22 A customized DWA login screen

Note: See Chapter 11, “Customizing Domino Web Access” on page 349 for more about customizing login screens, such as Figure 8-22 shows.

8. Assuming that the server has been configured for offline use, click the **`Go Offline`** menu option in the upper-right corner of the screen to begin installing the subscription for the offline components. (See Figure 8-23.)

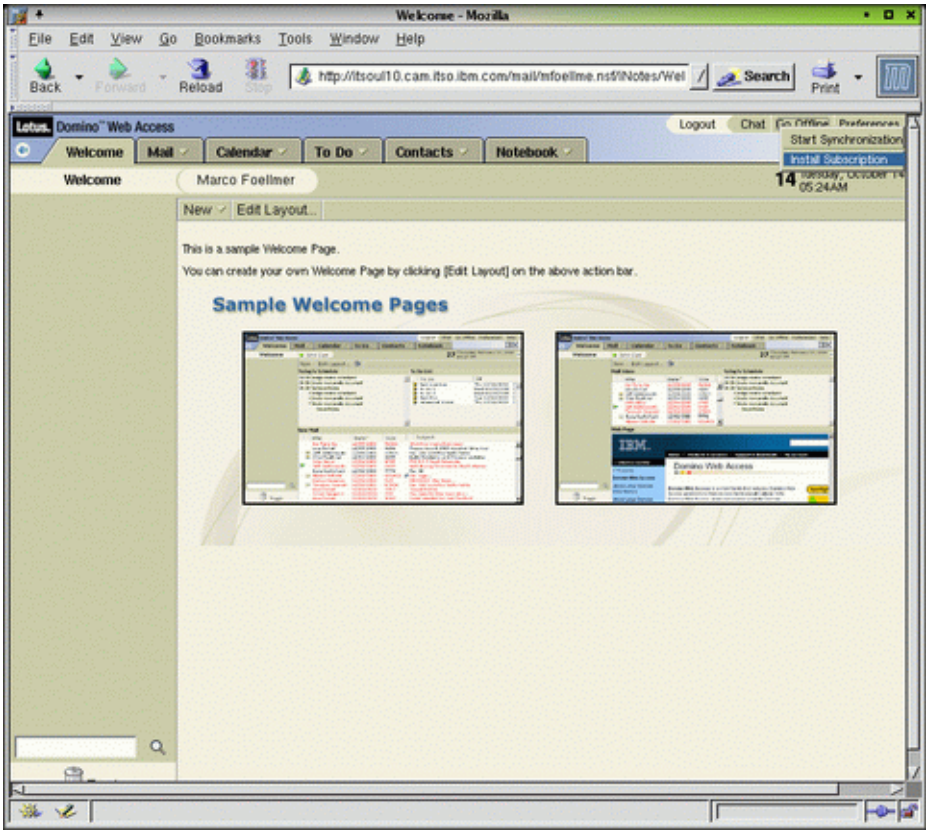


Figure 8-23 The Go Offline button with the Install Synchronization option

9. Several messages appear, including a license agreement (Figure 8-24).

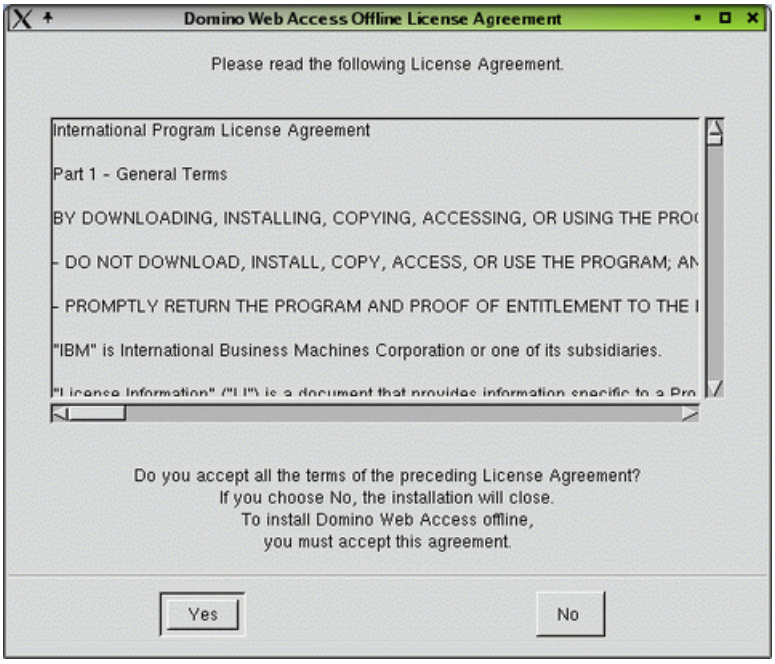


Figure 8-24 DWA Offline License Agreement

10. Figure 8-25 shows the screen about required write permissions on `[mozilla]/components` and `[mozilla]/plugins` for setting up DOLS successfully.

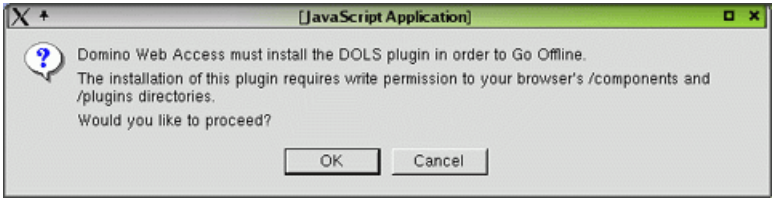


Figure 8-25 First installation screen of DOLS

11. A final warning screen appears just prior to installing the DOLS plug-in. Click **Install** (Figure 8-26).

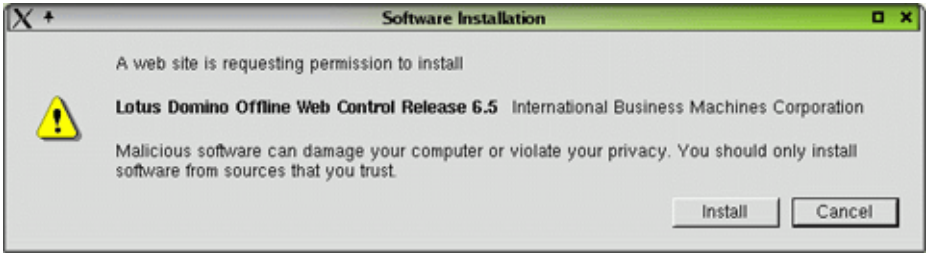


Figure 8-26 Standard warning screen

12. When installation is successful, you see a confirmation screen (Figure 8-27) signalling that you have completed the installation of the DOLS plug-in. Click **OK** and restart the browser.

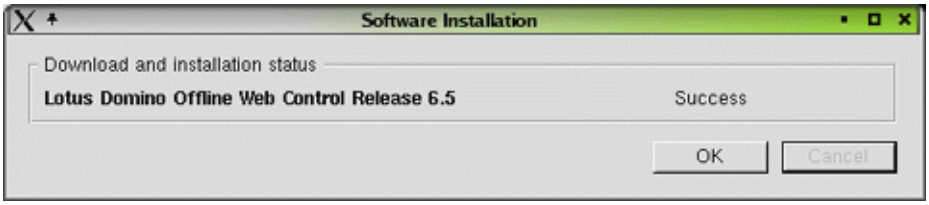


Figure 8-27 Successful installation

Important: After the successful installation of the DOLS plug-in you *must* restart the browser.

13. Finally, confirm that the plug-in is installed correctly. You can verify this by checking that the libnpdolctlm.so plug-in is installed. To do this, type `help/about plugins` or `about:plugins` in the location bar. Figure 8-28 shows that you have successfully installed the DOLS plug-in.

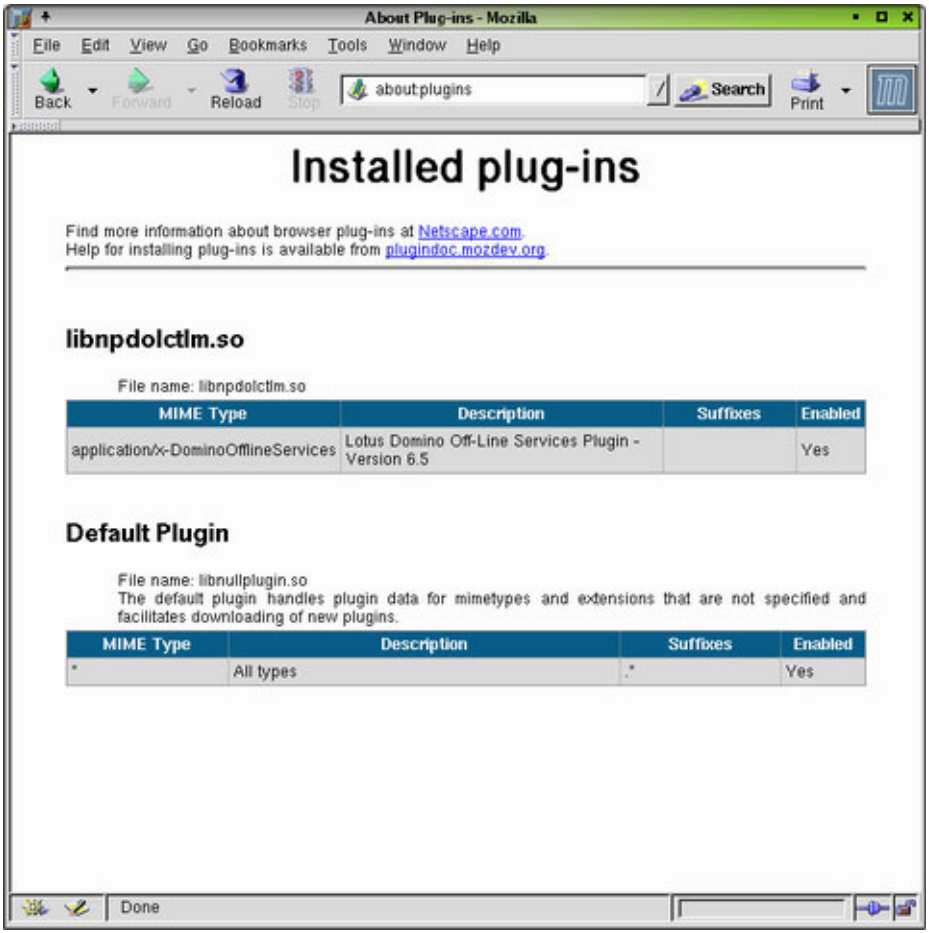


Figure 8-28 Plug-in installed and registered successfully

Install the DOLS synchronization subscription

In this section, we discuss how to install the DOLS subscription, which tells DOLS which database has to be synchronized.

Attention: Be aware that this version supports only the mail file. Accordingly, the replication stub of the mail file has to be installed first and *only one* DOLS user is supported.

1. Go back to the mail file and log on to Domino Web Access 6.5 on the server. After logging on successfully, you will see the sample welcome pages.
2. Click the **`Go Offline`** button in the top-right of the screen (Figure 8-29).

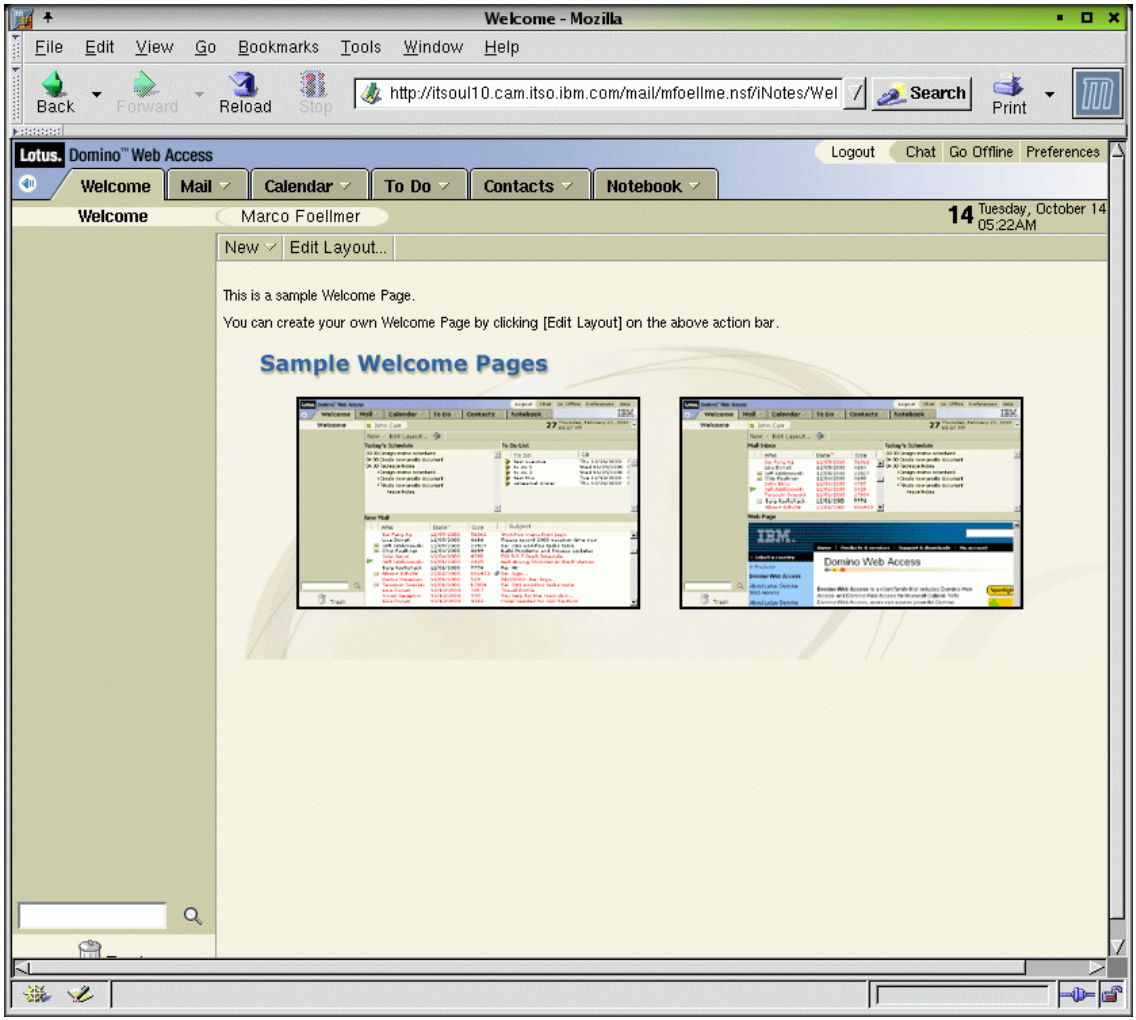


Figure 8-29 The Go Offline button

3. DWA 6.5 first looks for an installed plug-in, then installs the subscription of your mail file. A subscription includes your mail file, help-related databases, and property settings.

4. Finally, we include a series of screens for the correct installation of the subscription.

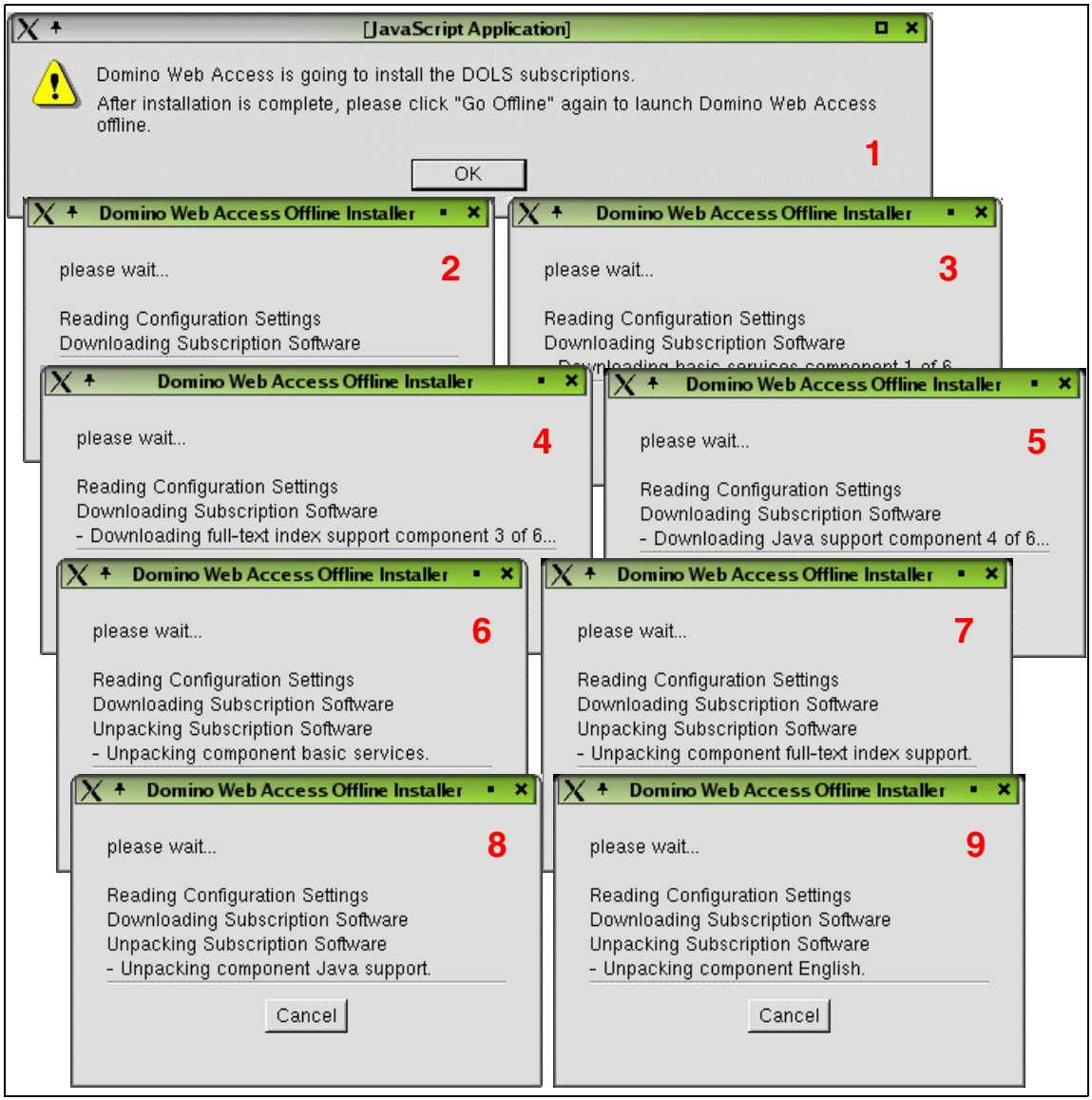


Figure 8-30 Installation screens of DOLS subscription for Linux

5. The Lotus Domino Sync Task prompts for authentication the first time you synchronize. Enter your normal Internet password (Figure 8-31).

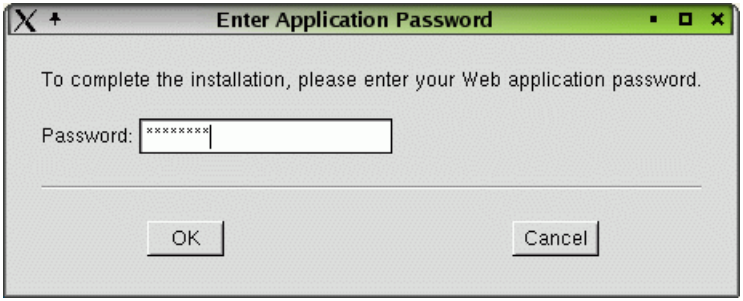


Figure 8-31 Lotus Domino Sync Task password prompt

Restriction: If you type the wrong password here, you will not able to retype the password. Fortunately, a reinstall of the DOLS subscription will solve the problem. To do this, click **Go Offline** → **Install Subscription** again. A subscription will be installed again and you will be prompted to type your correct password.

6. After deploying the subscription, the Lotus Domino Sync Task synchronizes the mail file for the first time, as shown in figure 8-27.

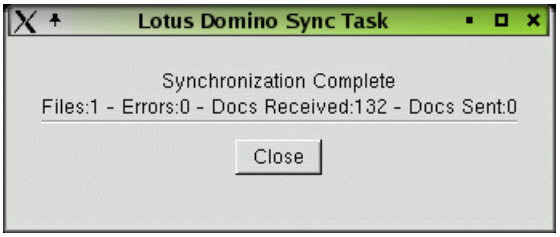


Figure 8-32 Sychronization completed with 132 documents

7. After the installation is complete, a shortcut icon called Offline is installed on the desktop (at least with KDE), as shown in Figure 8-33. This is a link to the directory for the udoloff task, which, when clicked, starts the HTTP server. It is located in /home/<username>/inotes/startup udoloff.

Figure 8-33 DOLS including subscription installation is finished

- Figure 8-34 shows the properties of the Offline application.

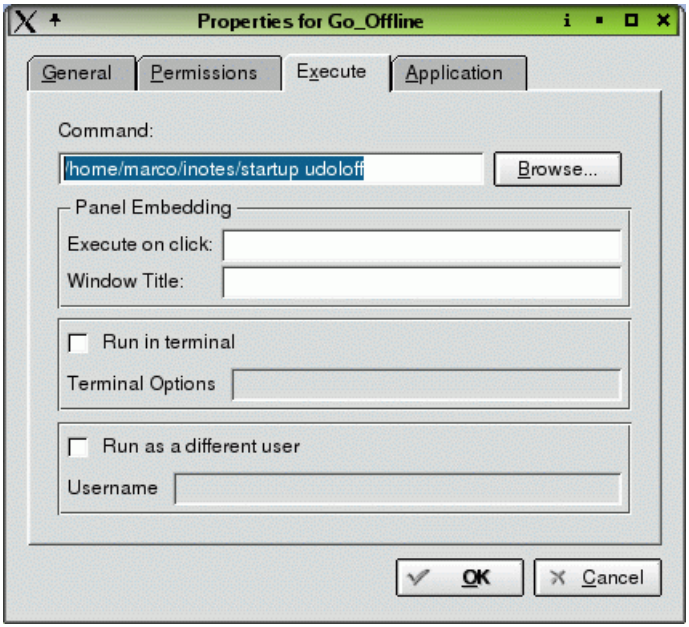


Figure 8-34 Properties settings of the DOLS offline program

8.4.4 Working offline

After the DOLS for Linux installation has finished, working offline enables users to access the information in their mail files while their computers are not connected to a network. While working offline, you can create messages, schedule meetings, respond to e-mail, and do most of the same things you can do when you are online.

Restriction: Online Awareness did not work when online, connected to the network, but working in offline mode.

Going offline

To begin working offline, click **Go Offline** on the Linux desktop. This loads the Lotus Domino Sync task, which is the local HTTP server, and Replicator task. After Domino Offline Services starts the browser and the offline services tasks, you can work offline (Figure 8-35).

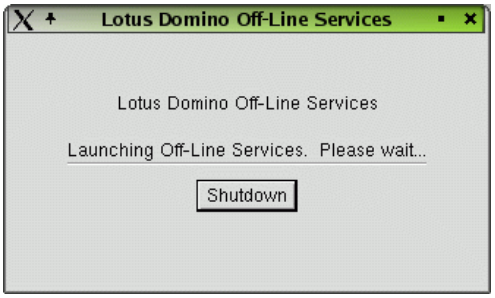


Figure 8-35 Starting Lotus Domino Offline Services on Linux

You will be prompted to enter your password, as shown in Figure 8-36.

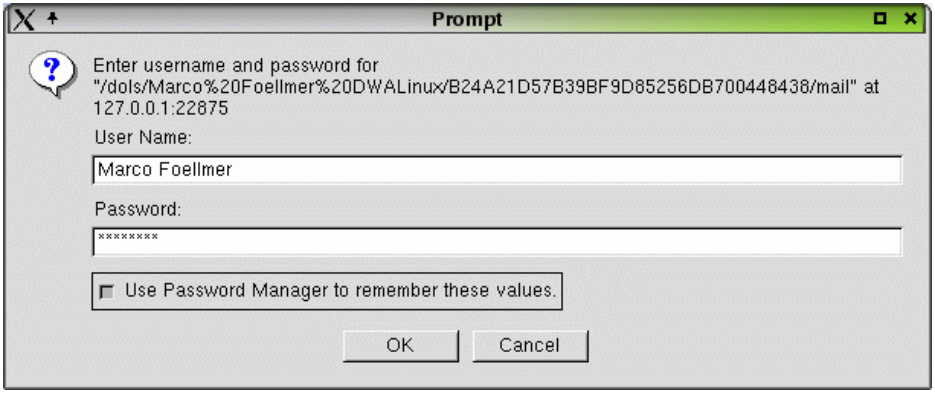


Figure 8-36 DOLS Offline prompt for the Domino user ID and password

This logs you onto the offline client so that you can begin working (Figure 8-37).

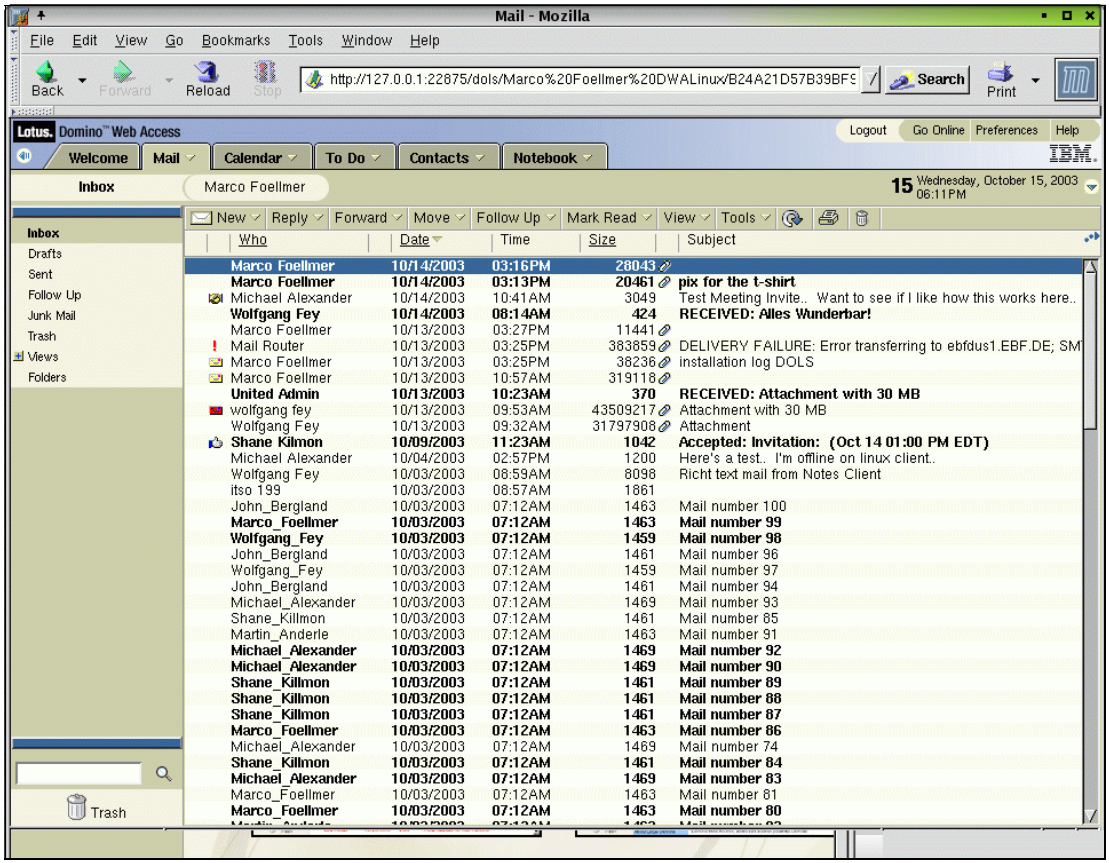


Figure 8-37 Working with DWA 6.5 offline

Notes:

- Single Sign-On with DOLS in offline mode is not supported in this release. The ability to log on Offline and subsequently get authorized on the Domino server when going back online is not supported.
- You can use the HTTP task running on port 22875 for troubleshooting, as described in 8.6, “Troubleshooting DWA 6.5 Offline Services” on page 311.
- The script behind the offline button is /home/<username>/inotes/startup udoloff.

Sync Manager

Lotus Domino Sync Manager is on the Linux desktop, and it lets you manage only one offline subscription. For this specific release of DWA 6.5, just the mail file is allowed to replicate. With Lotus Domino Sync Manager, you can perform the following tasks:

- Open Domino Web Access 6.5 offline, to use it as if it were online and connected to a network server.
- Synchronize the online and offline versions of Domino Web Access 6.5 with each other.

Restriction: If you rename a user, the user must reinstall the DOLS offline subscription in order for the offline mail file to synchronize with the server. After a name change, the user must wait for the old Notes ID and password to stop working, accept the name change using a Notes client, then log on to Domino Web Access with the new Notes ID and password.

Working with messages offline

While working in offline mode, you can read and create any document in your Domino Web Access 6.5 offline. If you create a mail message while working offline, then start to synchronize with DWA, you see the prompt for undelivered mail shown in Figure 8-38.

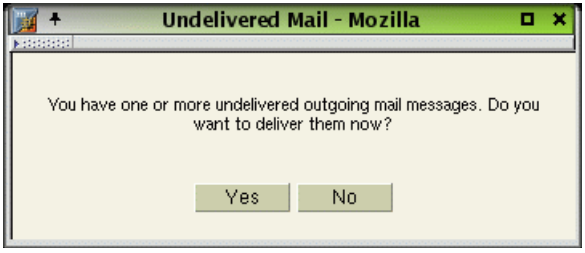


Figure 8-38 Undelivered mail prompt indicating that the user should synchronize

Restriction: Sending encrypted mails and signing mails is not supported in DWA offline mode (Figure 8-39 on page 304).

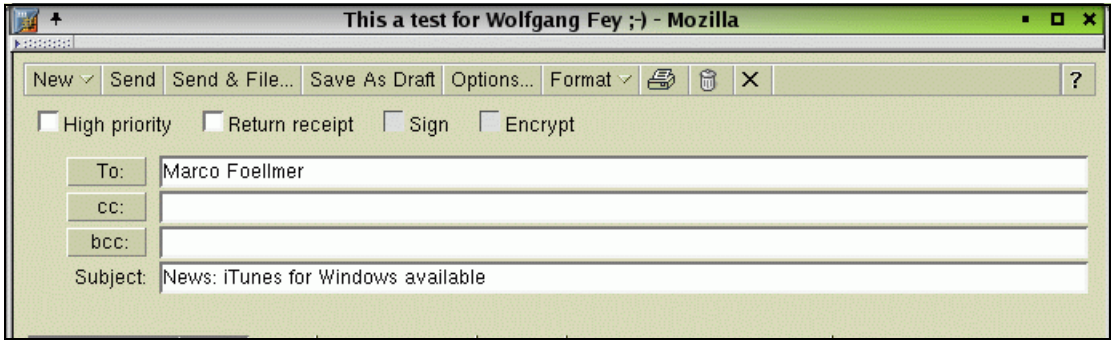


Figure 8-39 Sign and Encrypt checkboxes greyed out when offline

Restriction: When you work offline, you cannot change spelling dictionaries; your spelling dictionary is set by the default language selected on the server.

8.4.5 Preferences for Offline Users

In Domino Web Access 6.5, the user may set specific offline Mail preferences using the Mozilla preferences dialog shown in Figure 8-40. In this section, we describe some scenarios and more specific examples for each preference.

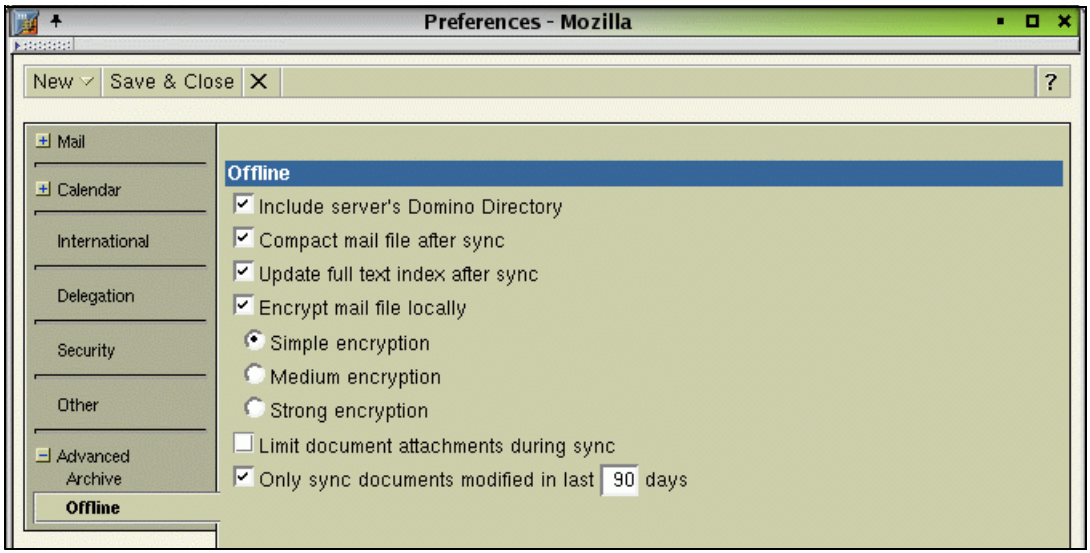


Figure 8-40 Offline Mail preferences dialog

- Include server's Domino directory

  This creates the Directory Catalog locally, enabling you to see it after you reinstall the subscription. This does not replicate the full Domino Directory.

  Attention: The word *catalog* is not seen as expected in the field label in the preferences dialog. This will be fixed in a future version of Domino 6.5. With this option, the Domino Directory will not replicated. Instead, the function of this preference is to replicate the Domino Directory Catalog.

  We reported this issue to the Lotus QA team, which assigned it this SPR number: `MALR5SKPJU`. See 8.5.1, "Mobile or condensed Directory Catalog" on page 307 for more about using the Directory Catalog in offline mode.

- Compact mail file after sync

  This option compresses the mail file after the synchronization is finished.

  Tip: Our recommendation is to enable the COMPACT tasks for offline usage in the Mail Preferences document, for better local performance and disk space reasons.

- Update fulltext after sync

  This is included because the UPDALL task, which runs on the local Linux operating system, is included in the Domino Offline Services. Select this choice to update your views.

  Restriction: The user cannot save any changes in the Preferences while offline. Figure 8-41 shows the warning if an attempt is made to edit preferences offline. Preferences changes can be made only when online.

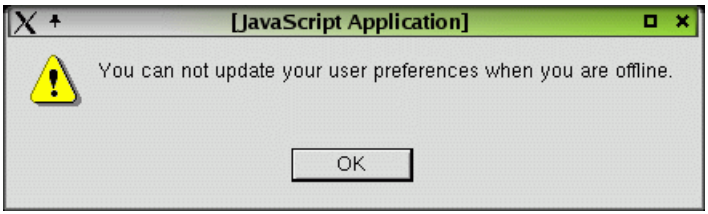


Figure 8-41 Preferences cannot be modified while user is offline

8.5 Uninstalling DWA 6.5 Offline Services

Follow these steps to uninstall Domino Web Access 6.5 on Linux:

1. First, delete your browser cache:
   a. Open your Mozilla 1.3.1 browser.
   b. Select **Edit** → **Preferences** → **Advanced** → **Cache** and click the **Clear Cache** button.
   c. Close the browser.

> **Attention:** Within the ITSO lab here in Cambridge, we ran into several issues by not deleting the cache in our browser. We strongly recommend clearing the cache on a regular basis. Our advice is to delete the cache manually by issuing this command:
>
> ```
> rm -r-f /home/<username>/.mozilla/cache/*
> ```

2. To complete the removal of DOLS, open a terminal session and type the following commands (Figure 8-46 on page 318):

```
rm  -rf /home/<username>/inotes
rm /usr/local/mozilla/plugins/libnpdolctlm.so
rm /usr/local/mozilla/components/npdolctlm.xpt
rm /usr/tmp/*
```

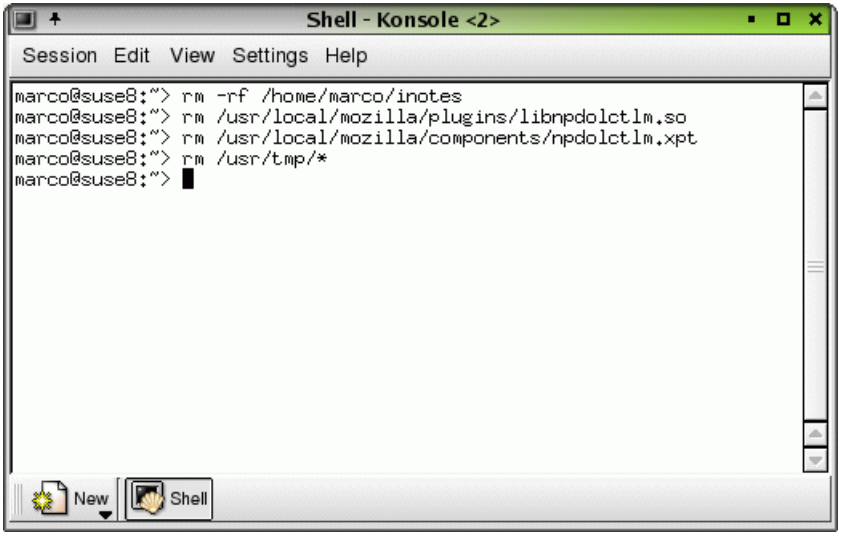


Figure 8-42 Removing DOLS files in Linux

8.5.1 Mobile or condensed Directory Catalog

Domino Web Access 6.5 can use other directories made accessible through configured Directory Assistance while online, or it can use the Mobile Directory Catalog, which is a condensed directory created by the *dircat* server task. You can use this catalog offline, because this directory will be replicated as a subscription setting. Within the Select Addresses dialog box, you can search and find people from all directories defined in Directory Assistance online.

Condensed Directory Catalogs

You create a condensed Directory Catalog from the Directory Catalog template (DIRCAT5.NTF). Condensed Directory Catalogs are designed to be small enough to fit on Notes clients to use for Domino Offline Service. For example, several Domino directories that together contain more than 350,000 users and total 3 GB in size, when aggregated in a condensed Directory Catalog, are likely to be only about 50 MB. In general, each user and group entry is slightly more than 100 bytes. Condensed Directory Catalog are designed primarily for use on Notes clients.

To achieve its small size, a condensed Directory Catalog uses a unique design that combines multiple documents from the Domino Directories into single documents in the Directory Catalog, and that limits the number of sorted views available for lookups.

- Aggregate documents

  One reason a condensed Directory Catalog is small is that it combines many entries from the source Domino Directories into single aggregate documents. A single Directory Catalog aggregate document can contain up to 250 source directory entries, although on average the maximum is about 200. This means that a condensed Directory Catalog needs to use only about 1000 aggregate documents to store information from 200,000 documents in the source Domino Directories.

- Limited number of views

  A condensed Directory Catalog is also small because it contains only a few, small views. By contrast a Domino Directory and an Extended Directory Catalog have multiple, typically large views.

- $Users view

  This is the one view used in a condensed Directory Catalog for name lookups. When you configure the Directory Catalog you choose how to sort this view, either by distinguished name, by last name, or by alternate name. To find names that do not correspond to the selected sort order, a full-text search is done of the Directory Catalog rather than a view lookup.

You should not open the aggregate documents in the $Users view manually. These documents are not intended for viewing, and it can take a considerable amount of time to format them for that purpose.

- $Unid view

  This view contains information needed by the dircat task to replicate the source directory entries into the Directory Catalog. The $Unid view is not created on replicas of the Directory Catalog, which further reduces the Directory Catalog size.

- $PeopleGroupsFlat view

  This view displays directory names when Notes users click the Address button to browse directories.

- Configuration view

  This view shows the Configuration document that contains the Directory Catalog configuration settings.

- Users view

  This is a view that users can open and programs can access to see the names included in the Directory Catalog. This view is not stored on disk but instead is built as needed.

- Design changes

  In general, you should not change the database design of a condensed Directory Catalog. One exception is changing the name of the Users view; you can change the name of this view, as long as you keep the original view name, Users, as an alias.

- Application access

  Notes applications can use these methods to access a condensed Directory Catalog programmatically:

  – NAMELookup calls to the $Users view

  – NAMEGetAddressBooks calls, if you use the NOTES.INI setting Name_Include_Ed=1.

  – NIFFindByKey, NIFReadEntries, and NIFOpenNote calls.* You cannot use NSFNoteOpen to open notes passed back from NIFReadEntries; you must call NIFOpenNote instead.

  LotusScript methods[1]

  – @NameLookup function

  In addition, LDAP applications can search a condensed Directory Catalog used by a server that runs the LDAP service.

[1] Can access the Users view but not the $Users view.

Adding a directory catalog to a DOLS subscription

Adding a directory catalog to a DOLS subscription enables users to take Domino Directory information offline. Note, however, that adding a catalog means more for a user to download. To keep download time reasonable, you may want to create a directory catalog specifically for offline users, which contains only the information they absolutely need.

To add a default catalog, open the NOTES.INI file on the server and add the line `$DOLSDirectoryCatalog=`*`nameofcatalog`*`.nsf` (*nameofcatalog* being the actual name of the catalog).

Note that the Domino Directory Catalog must be listed on the server document Basics tab.

Tips:

- Go to the server console and set the notes.ini variable as follows:

  ```
  set conf $DOLSDirectoryCatalog=nameofcatalog.nsf
  ```

- You can check the notes.ini with the following command:

  ```
  show config $dols* which shows the actual setting in the notes.ini
  ```

- If you are planning to deploy the Mobile Directory Catalog, our advice is to avoid more deployment costs by following this approach:
  - Set up the Directory Catalog first, *before* any user starts to install the subscription.

Figure 8-43 illustrates a Mobile Directory Catalog being accessed through an offline client.

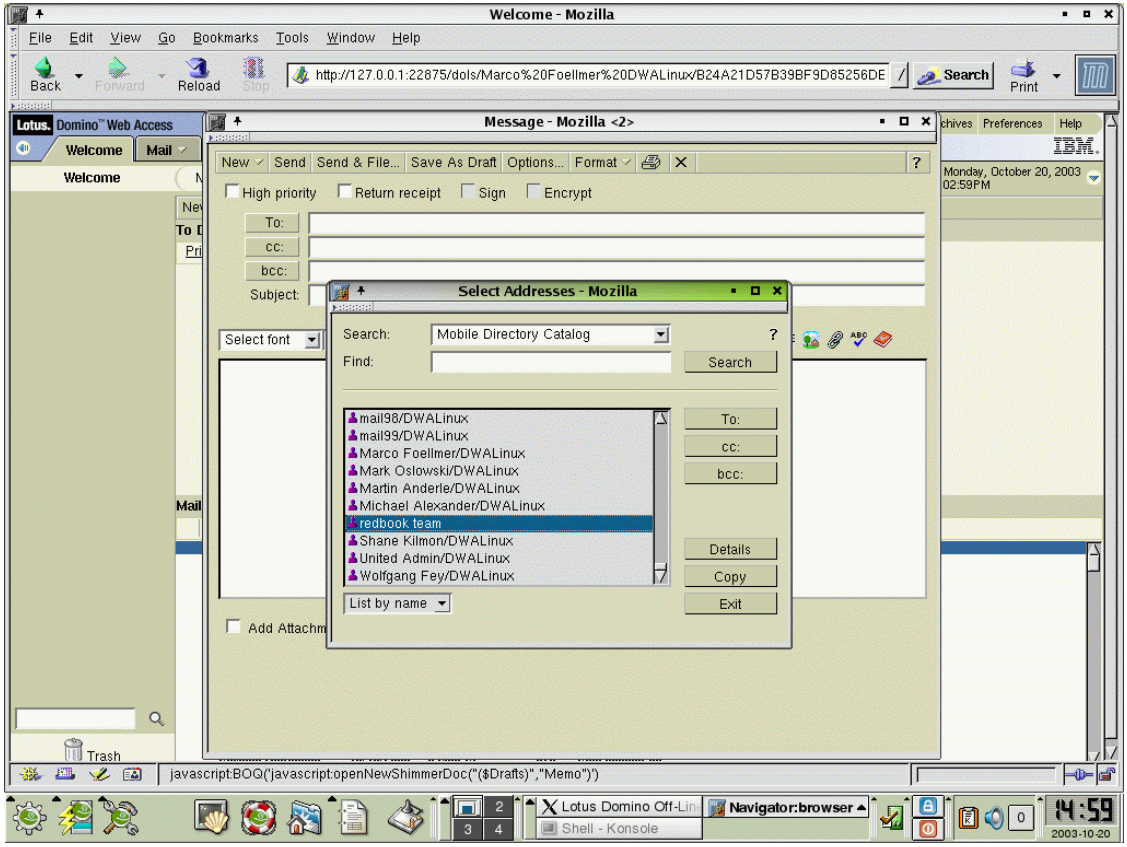


Figure 8-43 Mobile Directory Catalog offline provided through the new installed subscription

From within the Mobile Directory Catalog, a user can search for names quickly by typing in the first few letters of a last name entry. (Figure 8-44).

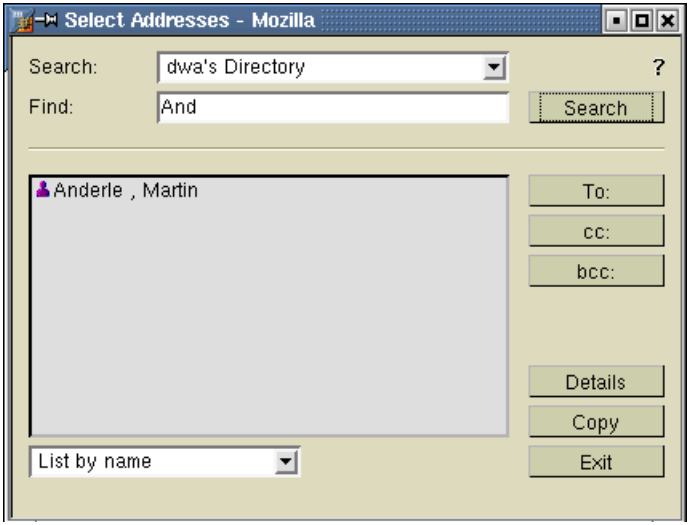


Figure 8-44 Search and Find within Domino directory

For more information about Directory Catalog, and how to configure the Domino server for Directory Assistance, refer to *Domino Administration Help*.

For more information about setting up Domino Web Access, see Chapter 5, “Installation and setup of Domino Web Access 6.5 on Linux” on page 153. For more information about setting up Sametime for Domino Web Access, see Chapter 9, “Integrating Sametime with Domino Web Access 6.5” on page 325.

8.6 Troubleshooting DWA 6.5 Offline Services

In our test environment we experienced only a few significant issues to troubleshoot. As a best practice, it is helpful to understand the directory structure and know which log files to look into if problems occur.

8.6.1 Common error messages with the plug-in

In our test environment we found several issues during plug-in installation that we would like to share with you (Table 8-2 on page 312).

Table 8-2 :Plug-in installation error messages

Error Message	Method to resolve
`invalid configuration -`	Check your DOLS Administration Policy Document.
`this is not a valid package`	The plug-in installation verified the browser version and detected a later version of Mozilla than V1.3.1. You cannot install this plug-in.

8.6.2 Linux directory structure and installed files

In the home directory of the Linux user, /home/<username>/inotes has the directory structure shown in Example 8-1.

Example 8-1 Description of important directories of DOLS for Linux

```
inotes/data/dols/Marco Foellmer DWALinux/B24A21D57B39BF9D85256DB700448438
inotes/data/dols/Marco Foellmer
DWALinux/B24A21D57B39BF9D85256DB700448438/cdc.ft

inotes/data/dols/Marco Foellmer DWALinux/B24A21D57B39BF9D85256DB700448438/mail
inotes/data/dols/Marco Foellmer
DWALinux/B24A21D57B39BF9D85256DB700448438/mail/mfoellme.ft
```

These are the most important files, which DOLS needs as a subscription for Offline usage. These are the key components of the mail file, including subscriptionid and fulltextindex, which is created right after the installation of the subscription and updated after each synchronization job is finished. The tasks UPDALL and COMPACT are also running after each synchronization.

Note: To enable the tasks UPDALL and COMPACT for Offline users check the Server configuration document.

Example 8-2 Important directories for Domino Offline Services for Linux

```
inotes/
inotes/data
inotes/data/IBM_TECHNICAL_SUPPORT
inotes/data/dols

inotes/data/domino
inotes/data/domino/cache
inotes/data/domino/html
inotes/data/domino/icons
```

```
inotes/data/domino/java
inotes/data/domino/java/editctrl

inotes/data/gtrhome
inotes/data/iNotes
inotes/data/iNotes/help65_iwa_en.ft
inotes/dols

inotes/jvm:
inotes/jvm/bin
inotes/jvm/bin/classic
inotes/jvm/lib
inotes/jvm/lib/audio
inotes/jvm/lib/cmm
inotes/jvm/lib/ext
inotes/jvm/lib/fonts
inotes/jvm/lib/images
inotes/jvm/lib/images/cursors:
inotes/jvm/lib/security

inotes/res
inotes/res/C

/usr/tmp
```

8.6.3 Case of the missing icons for DOLS

In our environment, we had only one Linux distribution (Red Hat 7.2), which properly displayed the desktop icon for launching DOLS. As a brief instruction to editing the icon and having it display properly, follow these steps:

1. Open a program to modify PNG files (for example, Kpaint).
2. Open the icon file, for example:
   `/home/marco/inotes/dols/subscriptions.png`
3. Select **File** → **Save**.
4. Go to the File properties and choose this icon again. Click **OK**.
5. Select **File** → **Save**. The icon should now be visible on the desktop.

Restriction: In our scenario, we have seen this icon (shown in Figure 8-33 on page 300) only in Red Hat 7.2. The workaround is to resave the icon to the proper graphic format. By doing this, we could make this icon visible for every distribution. See our overview Table 8-1 on page 286, which covers all the Linux distribution and the redbook team's experience with each distribution.

8.6.4 Mozilla does not start after launching DOLS

Attention: The Redbook team discovered an issue where neither the DOLS Offline icon nor the offline startup script would properly start the Mozilla browser in some environments. With DOLS in 6.5, the icon and startup scripts utilize the udoloff task. Udoloff is an essential part of the offline application and expects the Mozilla binary to be /usr/bin/mozilla.

If the browser has been installed to a different directory than /usr/bin/mozilla (mostly on SUSE distributions), you should prepare your environment by modifying the directory. The detailed steps are described as follows:

Modifying the Mozilla environment to work via udoloff

The following steps illustrate how to modify the Mozilla environment to allow the udoloff task to start Mozilla.

1. As root, type `cd /usr/bin`
2. Create a link in /usr/bin that points to the location of your Mozilla binary:

   ```
   ln -s /usr/local/mozilla/mozilla
   ```

3. Modify the user environment for the user who wishes to run the Offline client. Assuming they are using the Bash shell, set these lines in /home/<user>/.profile:

   ```
   export MOZILLA_HOME=/usr/local/mozilla
   export MOZILLA_FIVE_HOME=/usr/local/mozilla
   ```

4. Have the user log out and log in again to refresh the environment, and the Offline icon and startup script should work properly. Udoloff should correctly start the Mozilla browser.

Note: Upon discovering this issue, the redbook team logged a new SPR with the development team. SPR # SKIN5SDKMQ: **“**`DOLS startup on some LINUX distribution does not start Mozilla`**.”**

Restriction: In DWA 6.5, only one user is supported for the LINUX client to go offline. Mulit-user support is not available as of this writing.

8.6.5 Troubleshooting DOLS from the dol.log and the command line

1. As a first technique, we can look at the dol.log file, which is in /home/<username>/inotes/dol.log. It shows the local activity of Domino Offline Services.

   Here we can see whether a mail message has been dispatched and the client has synchronized the mail file, and find out information about the Lotus Domino Sync task.

Example 8-3 Excerpt from the dols.log

```
[Sat 18 Oct 2003 02:30:39 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Dispatching offline
mail documents to United/DWALinux for CN=Marco Foellmer/O=DWALinux>
[Sat 18 Oct 2003 02:30:39 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: 1 mail documents
dispatched>
[Sat 18 Oct 2003 02:30:39 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: 15% complete>
[Sat 18 Oct 2003 02:30:39 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Synchronizing
application data with United/DWALinux>
[Sat 18 Oct 2003 02:30:39 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Synchronizing group
memberships>
[Sat 18 Oct 2003 02:30:40 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: 15% complete>
[Sat 18 Oct 2003 02:30:40 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Synchronizing agent
permissions>
[Sat 18 Oct 2003 02:30:41 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Applying configured
replication settings>
[Sat 18 Oct 2003 02:30:44 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: 75% complete>
[Sat 18 Oct 2003 02:30:44 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Applying configured
replication settings>
[Sat 18 Oct 2003 02:30:44 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: 90% complete>
[Sat 18 Oct 2003 02:30:44 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: 100% complete>
[Sat 18 Oct 2003 02:30:44 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Ready for use -
compacting in background>
[Sat 18 Oct 2003 02:30:48 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Compaction
Complete.>
[Sat 18 Oct 2003 02:30:48 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Ready for use -
indexing in background>
[Sat 18 Oct 2003 02:30:48 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Indexing
application file: mfoellme.nsf>
[Sat 18 Oct 2003 02:30:49 PM EDT] <Marco Foellmer - Lotus Domino Sync Task: Indexing
application file: cdc.nsf>
```

2. For the second technique, we show the ability to start the Offline Icon with the terminal flag in the icon properties. Select **Execute** → **Run in terminal**.

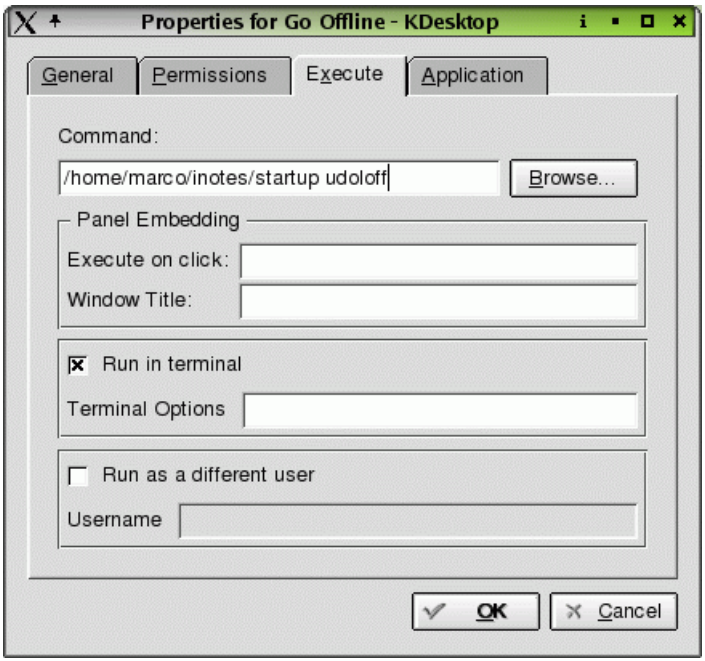


Figure 8-45 Activate the run terminal option for more information about the offline task

By opening the Offline application, we see the DOLS task, which starts the HTTP task as shown in Example 8-4.

Example 8-4 Offline task console gives more information about DOLS activity

```
10/21/2003 09:24:46 AM  HTTP Server: Using Web Configuration View
10/21/2003 09:24:47 AM  JVM: Java Virtual Machine initialized.
10/21/2003 09:24:47 AM  HTTP Server: Java Virtual Machine loaded
10/21/2003 09:24:49 AM  HTTP Server: Started
10/21/2003 09:25:25 AM  Starting replication with server United/DWALinux
10/21/2003 09:25:25 AM  Access control is set in United/DWALinux
mail\mfoellme.nsf to not replicate forms or views from /dols/Marco Foellmer
DWALinux/B24A21D57B
39BF9D85256DB700448438/mail/mfoellme.nsf
10/21/2003 09:25:26 AM  Finished replication with server United/DWALinux
10/21/2003 09:25:27 AM  Starting replication with server United/DWALinux
10/21/2003 09:25:27 AM  Pulling /dols/Marco Foellmer
DWALinux/B24A21D57B39BF9D85256DB700448438/mail/mfoellme.nsf from
United/DWALinux mail\mfoellme.nsf
10/21/2003 09:25:27 AM  Replicator updated 2 document(s) in /dols/Marco
Foellmer
DWALinux/B24A21D57B39BF9D85256DB700448438/mail/mfoellme.nsffromUnited/DWALinu
x mail\mfoellme.nsf
```

```
10/21/2003 09:25:28 AM  Finished replication with server United/DWALinux
10/21/2003 09:25:28 AM  Starting replication with server United/DWALinux
10/21/2003 09:25:28 AM Access control is set in United/DWALinux cDC.nsf to not
allow replication from /data/dols/Marco Foellmer
DWALinux/B24A21D57B39BF9D85256D
B700448438/cdc.nsf
10/21/2003 09:25:28 AM  Finished replication with server United/DWALinux
10/21/2003 09:25:28 AM  Starting replication with server United/DWALinux
10/21/2003 09:25:29 AM Access control is set in United/DWALinux cDC.nsf to not
allow replication from /data/dols/Marco Foellmer
DWALinux/B24A21D57B39BF9D85256D
B700448438/cdc.nsf
10/21/2003 09:25:29 AM  Finished replication with server United/DWALinux
```

Important: Enable this `Run in terminal` option only for troubleshooting. We do not recommend showing this screen to an end user.

3. Third, we can look at the databases shown in Example 8-5, which Domino Offline Services provides by default installation.

Example 8-5 DOLS system databases

```
marco@suse8:~/inotes/data> ls -lisa *.nsf
 105498   256 marco    users      262144 Oct 21 10:30 DOLConfig.nsf
 105460 16656 marco    users    17039360 Oct 21 10:30 dolnames.nsf
 105461  1321 marco    users     1350144 Oct 21 10:30 log.nsf
 105502   384 marco    users      393216 Oct 21 10:30 subscriptions.nsf
```

8.6.6 Using the browser for troubleshooting offline configuration

Within this section, we describe how to use a browser to examine specific databases and better understand the offline configuration.

To access the database, we use only the browser, using the specific URL when the DOLS service is started:

```
http://127.0.0.1:22875/log.nsf
```

Tip: Before using a browser, make sure that you have installed Java to support the Domino applets for view, action buttons, and so on, as described in Chapter 9, “Integrating Sametime with Domino Web Access 6.5” on page 325.

Figure 8-46 illustrates a view into a DOLS log file (more specifically, the replication log document) through a browser.

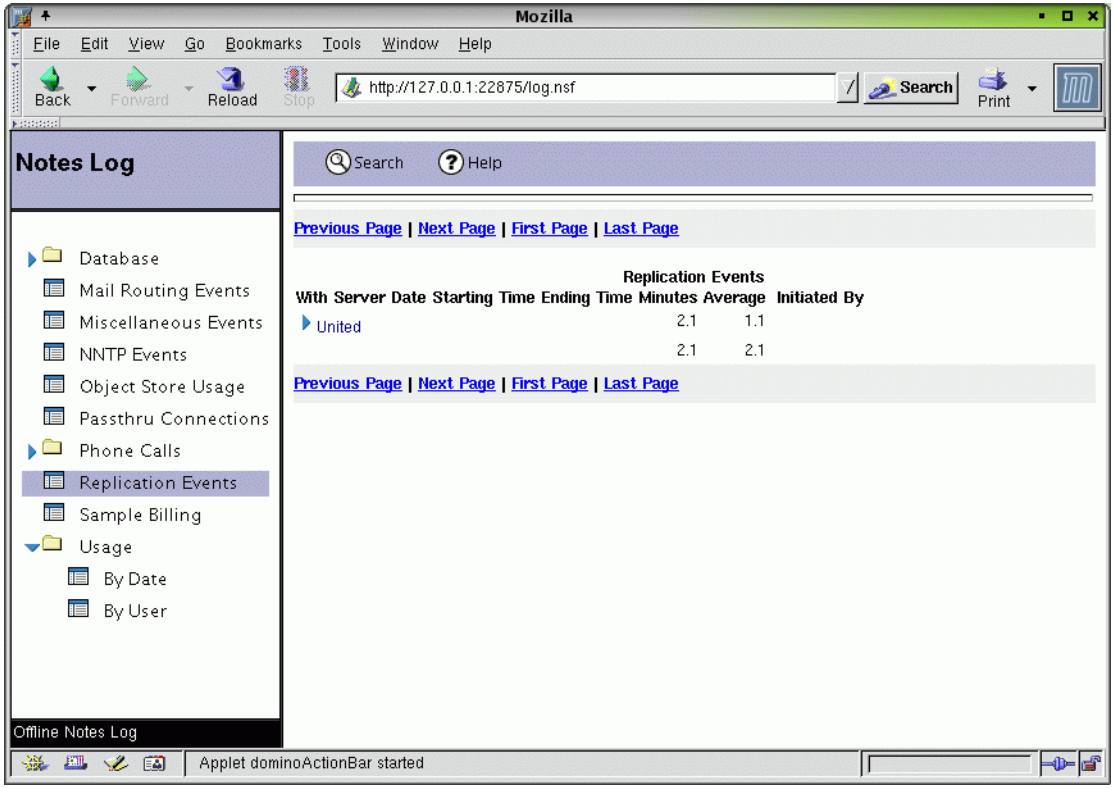


Figure 8-46 DOLS log.nsf working as expected in the browser

Figure 8-47 illustrates the use of databases, which we already know from the Domino Server log file. The condensed Directory Catalog is used on the server and locally, offline.

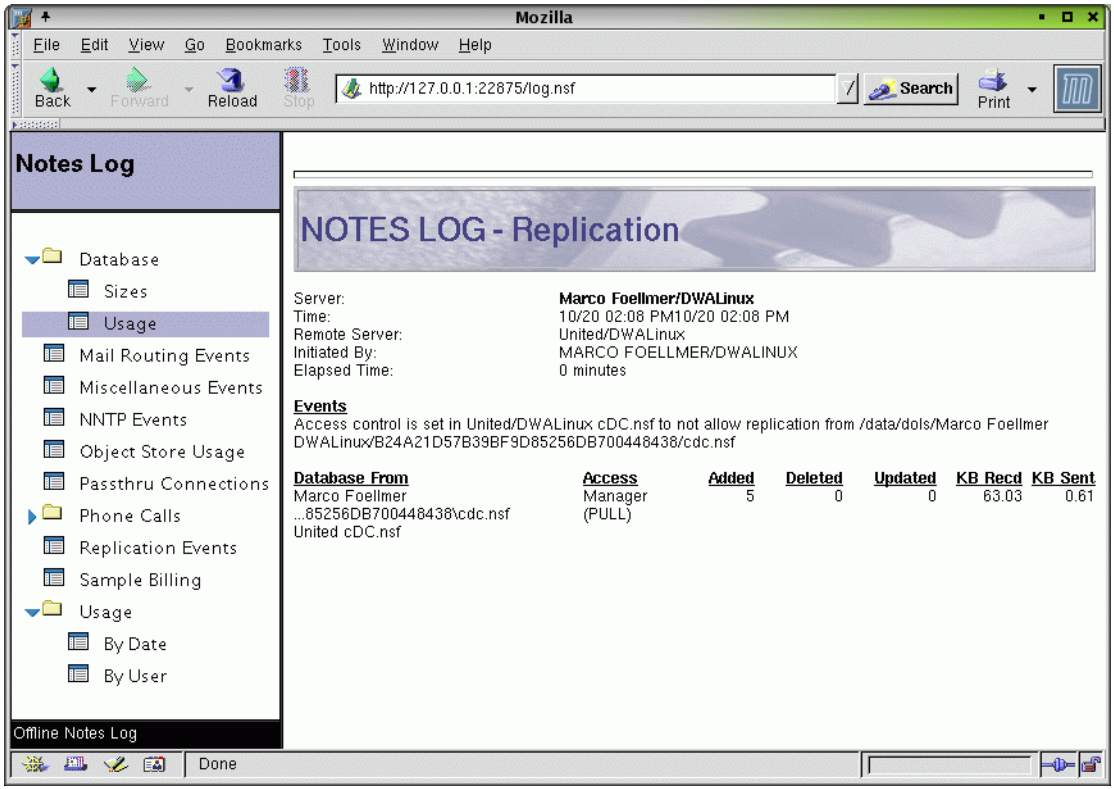


Figure 8-47 Replication log document with more detailed information

In Figure 8-48, the mail file is replicated as expected, and we see the subscribtion ID of the mail file from the user.

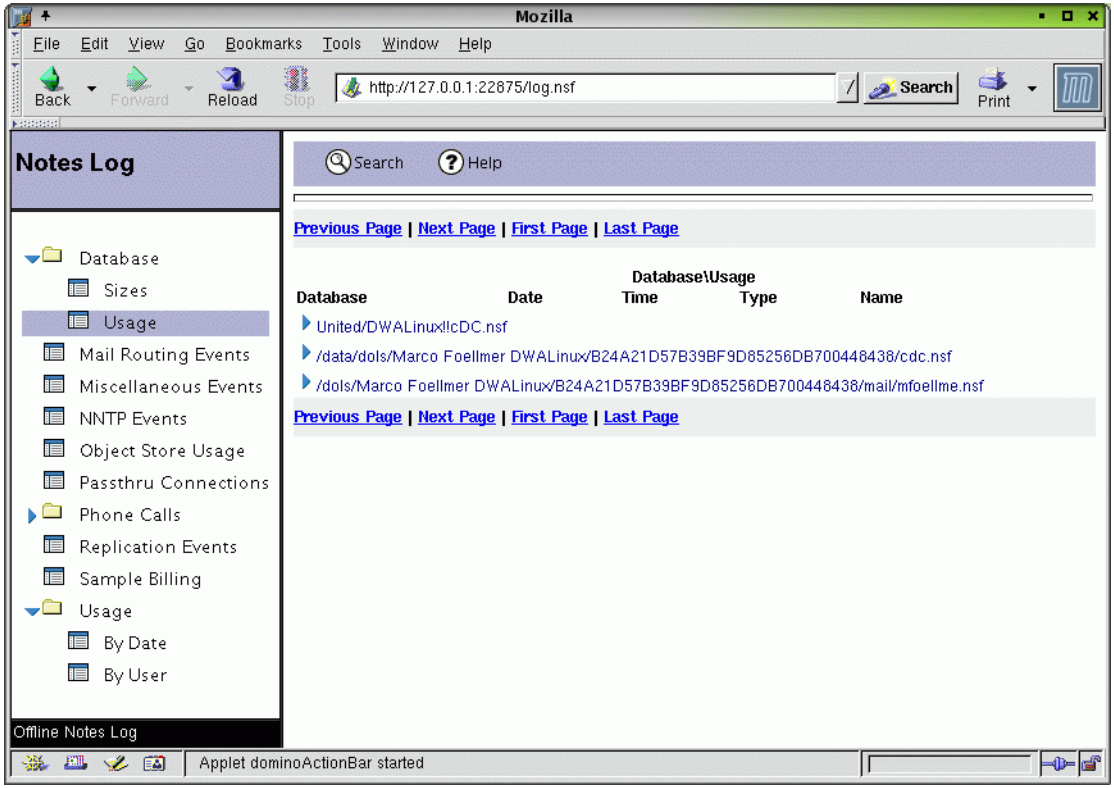


Figure 8-48 DOLS Logfile Usage view

Figure 8-49 illustrates the content of the subscription document, with more detailed information about the user's mail subscription. Here we can see the ID of the subscription, so we can check new subscription settings if they are applied to the users.

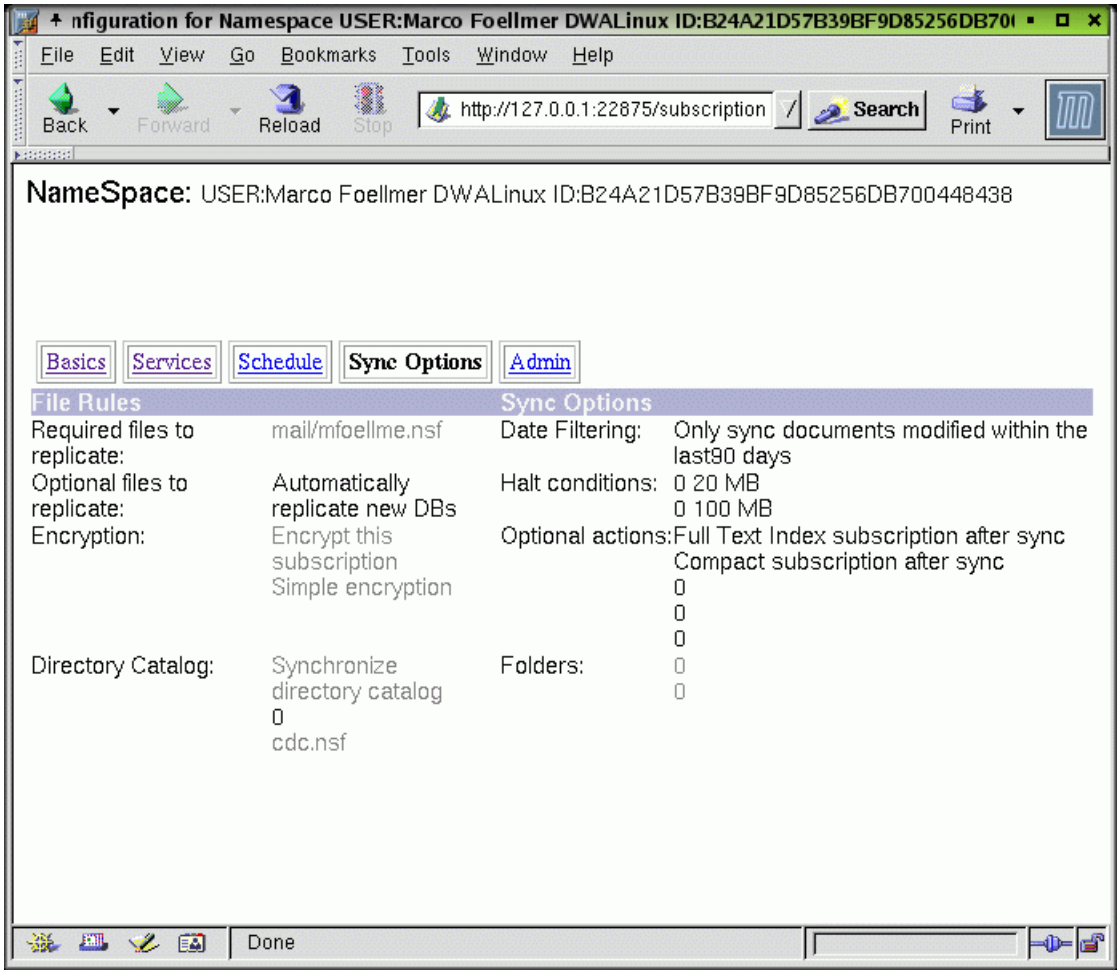


Figure 8-49 Content of the subscription document

Part 4

Customization and integration

9

Integrating Sametime with Domino Web Access 6.5

Domino 6.5 tightly integrates Domino and the IBM Lotus instant messenger (Sametime) capabilities from both the Notes rich client and the browser-based Domino Web Access platform. This chapter discusses how to integrate Sametime 3.1 with Domino Web Access 6.5.

The following aspects of Sametime integration are covered:

- Configuration of the Domino Web Access and Sametime servers
- Configuration of the Mozilla browser on Linux
- Using Chat within Domino Web Access
- Notes.ini parameters that effect Sametime integration

9.1 Configuration of the DWA and Sametime servers

Domino Web Access 6.5 requires a Sametime 3.1 server in order to support chat (instant messaging) using a Mozilla browser. For complete information about installing and configuring a Sametime server, refer to the Sametime product documentation, including the Installation and Administration guides.

Note: When configuring the Sametime server, it must be in the same Domino domain as the Domino Web Access servers you wish to integrate it with.

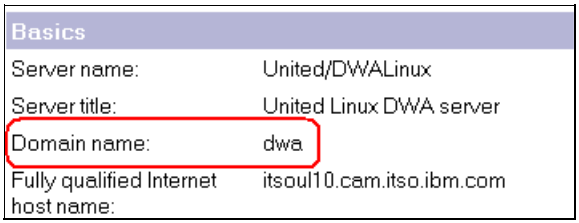


Figure 9-1 Domino Domain in the Server Document

9.1.1 Connection documents

After each server is set up, connection documents must be made for them to communicate properly. From the Domino Administrator client, connect to your administration server (if your practice is to use one server for Directory changes), or the DWA or Sametime server. On the Configuration tab:

1. From the menu bar, click **Server** → **Connections**.
2. Click the **Add Connection** button.
3. Choose **Local Area Network** for the Connection type.
4. Enter the DWA Server name (example: `United/DWALinux`) in the Source server field.
5. Enter the Sametime Server name (example: `STGateway/DWALinux`) in the Destination server field.
6. Make sure both Source domain and Destination domain contain the correct Domino domain (example: `dwa`). Remember, both servers must be in the same Domino domain.
7. Click **Save & Close**.
8. Repeat the steps above to create a connection document with the source server as the Sametime server, and the destination server as the DWA server.

9.1.2 Modify person documents

While you are still connected and editing the Domino Directory, the next step should be to modify each person document to specify the Sametime server:

1. Click the **People & Groups** tab.
2. Select the **People** view under the Domino Directory and <Org> **Directory** pull-down menus, where <Org> is your Domino Organization name.
3. Click the name of a user you wish to have Sametime integration, then click the **Edit Person** button.
4. Enter the name of the Sametime server (example: `STGateway/DWALinux`) in the Sametime server field under the Real-Time Collaboration section of the Basics tab (Figure 9-2).
5. Click **Save & Close**.
6. Repeat steps 3 through 5 for each person you integrate with Sametime.

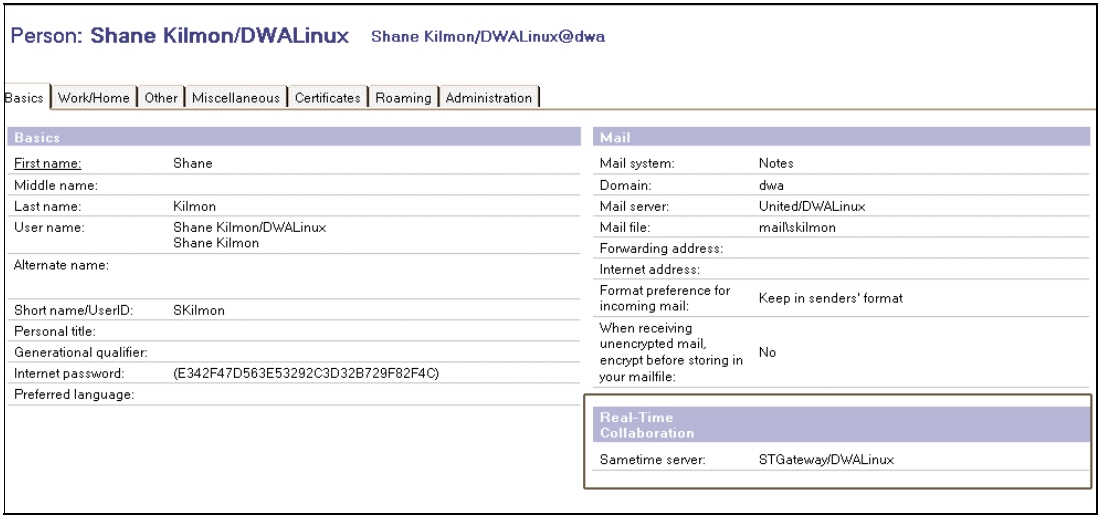


Figure 9-2 Sametime server field in a Person document

9.1.3 Configuring authentication

The Sametime server naturally needs to authenticate any client that requests a connection, including DWA sessions. To do so, it uses Secrets and Tokens databases (STAuthS.nsf and STAuthT.nsf). A copy of these databases must be put on the DWA servers in order for the authentication to succeed:

1. From a Notes client, select the **File** → **Database** → **Open**.
2. Enter the name of the Sametime server in the Server field.

3. When the list of databases is shown, enter `stauths.nsf` in the Filename field and click **Open**.
4. When the database is open, select **File** → **Replication** → **New Replica**.
5. Enter the name of the DWA server in the Server field, and in the File path field, make sure that the database is called `STAuthS.nsf` (note capitalization). Click **OK** to create the new replica.
6. Repeat steps 1 through 5, but use `stautht.nsf` in step 3.

Important: On DWA 6.5 Linux servers, the STAuthS.nsf and STAuthT.nsf MUST have that exact file name, including the capitalization, in order to work. (You would not believe how long it took us to figure that out.)

The next configuration requirement is to give each server access to the Java resources necessary to use both Forms5.nsf-based and Forms6.nsf-based databases. Note that Mozilla clients on Linux will not work with Forms5.nsf-based databases.

- For Forms5.nsf support:
  a. Create a directory on the Sametime server called `SametimeApplet`. This directory name is case-sensitive and must be created in <data directory>\domino\html\:

     ```
     > mkdir <data directory>\domino\html\SametimeApplet
     ```

  b. Copy the contents from the corresponding SametimeApplet directory on the DWA server to the new SametimeApplet directory on the Sametime server.
- For Forms6.nsf support:
  a. On the DWA server, create a `sametime` subdirectory under the <data directory>/domino/html/ directory. This directory is not case-sensitive.
  b. Create a `stlinks` subdirectory in the sametime directory that you created in step 1.
  c. Copy all of the contents of the Sametime server's <data directory>\domino\html\sametime\stlinks\ directory into the newly created stlinks directory on the DWA server.

Note: For Mozilla clients only: if the stlinks.jar file in the stlinks directory is not a signed version, you must replace it with a signed version of stlinks.jar, which can be found in the Toolkit\stlinksignedapplet\ directory on the Sametime installation CD #2.

The final step is to make sure that all Directory changes are replicated to the servers involved. Force replication between the Sametime and DWA servers to ensure that all of the servers have the same information.

Attention: One other potential configuration issue to look out for is how your servers' name resolution is configured. In our test environment, we used Domino server names that did not match the host name of the machine we were installing on (example: RedHat/DWALinux was installed on itsorhas21.cam.itso.ibm.com.) Due to this, we had to make sure that we could resolve the fully qualified name of the Domino server with respect to the DNS domain we were in (in other words, redhat.cam.itso.ibm.com had to be an alias for itsorhas21.cam.itso.ibm.com). This applied to both the Domino Web Access servers and the Sametime gateway server.

9.2 Configuration of the Mozilla browser

Sametime integration in DWA relies heavily on a proper Java environment on the browser side. This requires a Java plug-in to be present on the client system and registered with the browser. To determine whether a recent Java Runtime Environment (JRE) is already installed on the system, check both /usr/java and /usr/lib/ for JRE directories. In /usr/java this will generally look like:

```
j2re<version>
```

In /usr/lib/ you may see a java or java2 symbolic link that points to a version of the Sun JDK environment, which may also contain a JRE plug-in. For DWA 6.5, we require a Java 1.4.2 plug-in for full support of Sametime integration. If JRE 1.4.2_<xx> (where <xx> is a minor revision number, such as 01) is not present, download the latest J2SE 1.4.2 from:

http://java.sun.com

If you download the RPM package for Linux and follow the install instructions, it should put the JRE in /usr/java/j2re1.4.2_<xx>. After the JRE is installed, you can create a link in your Mozilla plug-ins directory that points to the Java plug-in. This can be done either in your personal Mozilla plug-in directory, $HOME/.mozilla/plugin, or preferably, in the global plug-in directory for the browser, so that all users will have the plug-in.

In many environments, the Mozilla installation is under /usr/local/mozilla, so the plug-in directory is generally /usr/local/mozilla/plugin. In either case (local or global), **cd** into the appropriate plug-in directory, and run:

```
ln -s /usr/java/j2re1.4.2_<xx>/plugin/i386/ns610/libjavaplugin_oji.so.
```

Note: If installing to the global plug-in directory, this command most likely should be run as root.

Also note: The instructions provided on the Sun Web site for registering the plug-in with Mozilla on SUSE 8.1 or later indicate that you should link to the libjavaplugin_oji.so that is found in

```
/usr/java/j2re1.4.2_<xx>/plugin/i386/ns610-gcc32/
```

However, our testing using Mozilla 1.3.1 on SUSE 8.1 and 8.2 has shown that the non-gcc32 version of the plug-in is the proper one for our test clients. Your environment may be different, so use the one that works based on your particular installation. To confirm that the plug-in was installed correctly, after restarting the browser, select **Help** → **About Plug-ins** from the menu bar, and look for the Java 1.4.1_<xx> plug-in in the list.

9.2.1 Modify preferences in Mozilla

The final step to fully enable Sametime integration in a user's DWA session is to modify their Preferences to enable Instant Messaging:

1. Start the browser (after registering the Java plug-in).
2. Enter the URL for your DWA mail file. In our test environment, this was:

   ```
   http://itsoul10.cam.itso.ibm.com/mail/joeuser.nsf
   ```

3. After authenticating, and after the Welcome page loads, click the **Preferences** button in the top-right corner.
4. On the **Other** tab, make sure that **Enable Instant Messaging** is selected (Figure 9-3 on page 331).
5. Click **Save & Close**.

This should take you back to the Welcome page, which should refresh automatically. If it does not show a Chat button in the top right, near the Preferences button, or if you do not see the Sametime awareness icons next to the user names in your Inbox, clear the browser cache and reload the page.

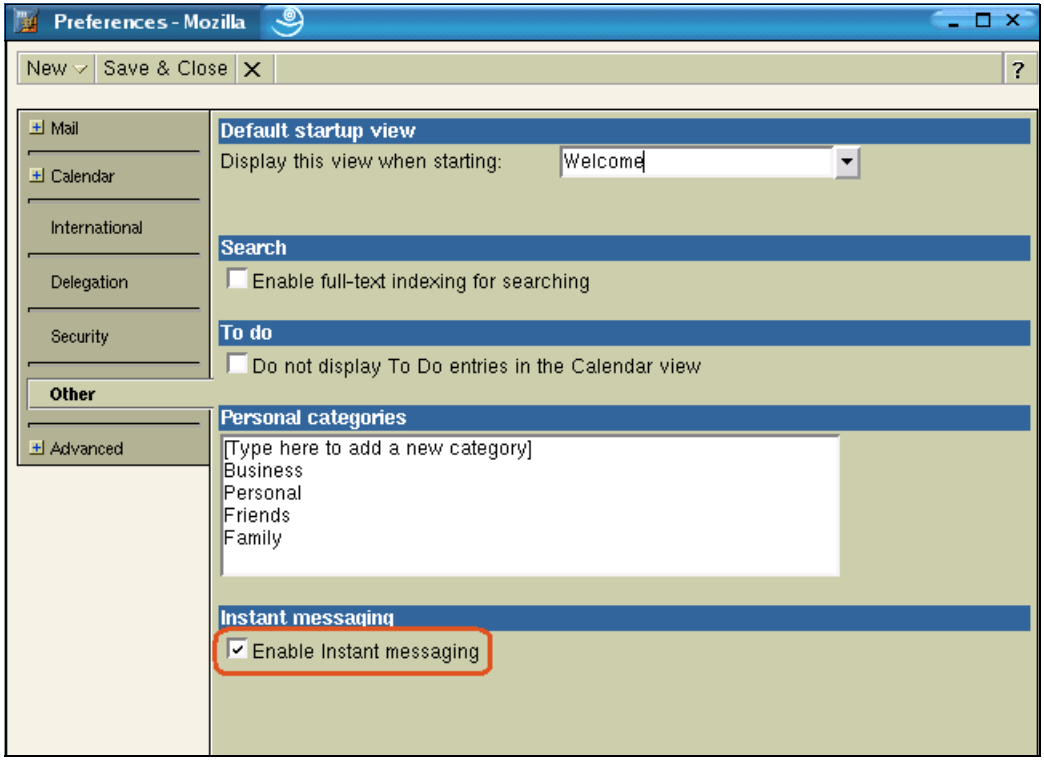


Figure 9-3 User Preferences dialog

9.3 Using chat within Domino Web Access

Integration of Sametime and Domino Web Access is a very powerful tool for increasing user productivity. The first productivity enhancement comes just by logging into DWA. As soon as you start your DWA session, you are also immediately able to use Sametime instant messaging functions. No separate login is required, and no separate client must be executed in order to enable real-time collaboration.

The ability to collaborate instantly with other members of your organization while maintaining the workflow of the task you are performing is a great productivity gain and should increase efficiency in all environments.

9.3.1 Productivity enhancements through presence awareness

While in the DWA session, the most obvious example of the Sametime integration is the online status indicator that precedes each user's name in your Inbox (Figure 9-4). You can tell at a glance whether the person who sent you mail is available for an instant message.

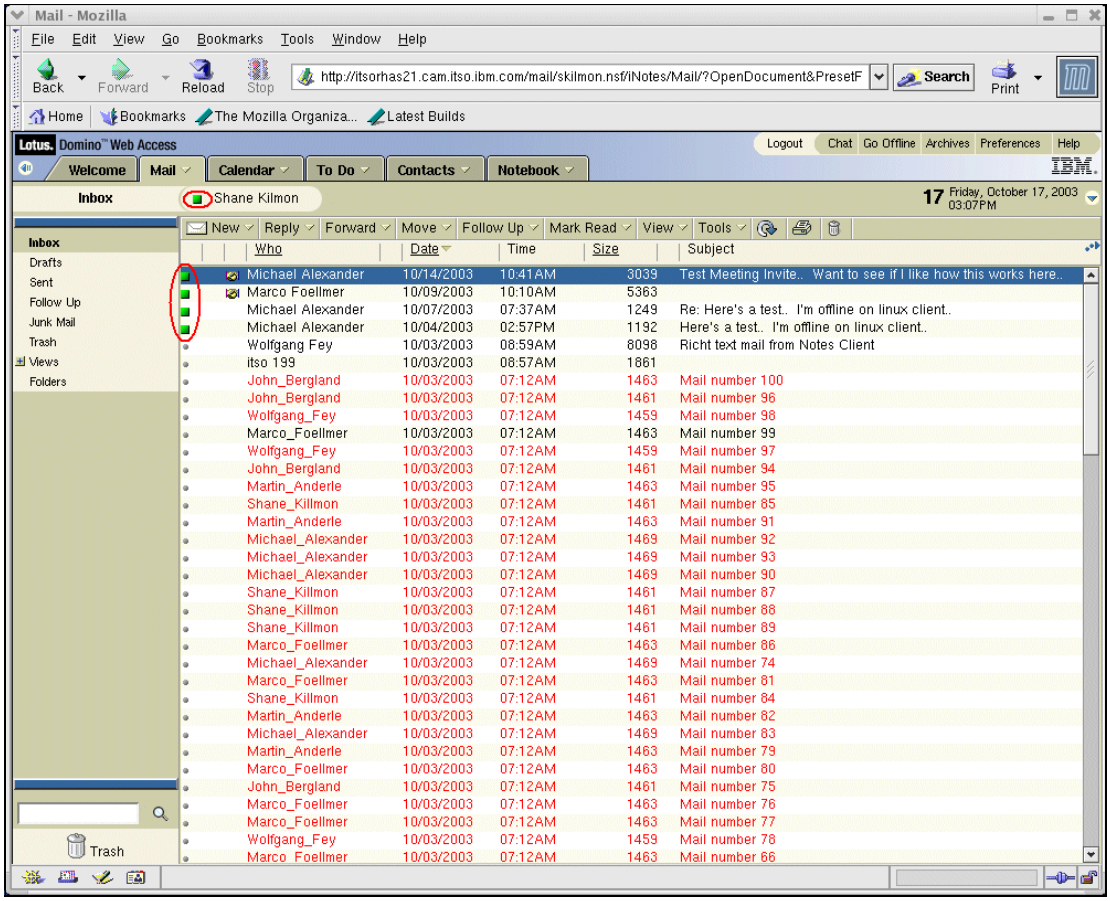


Figure 9-4 Online status indicators in an Inbox

Open the mail message, and each person in the To: and CC: fields also has an online status indicator (Figure 9-5).

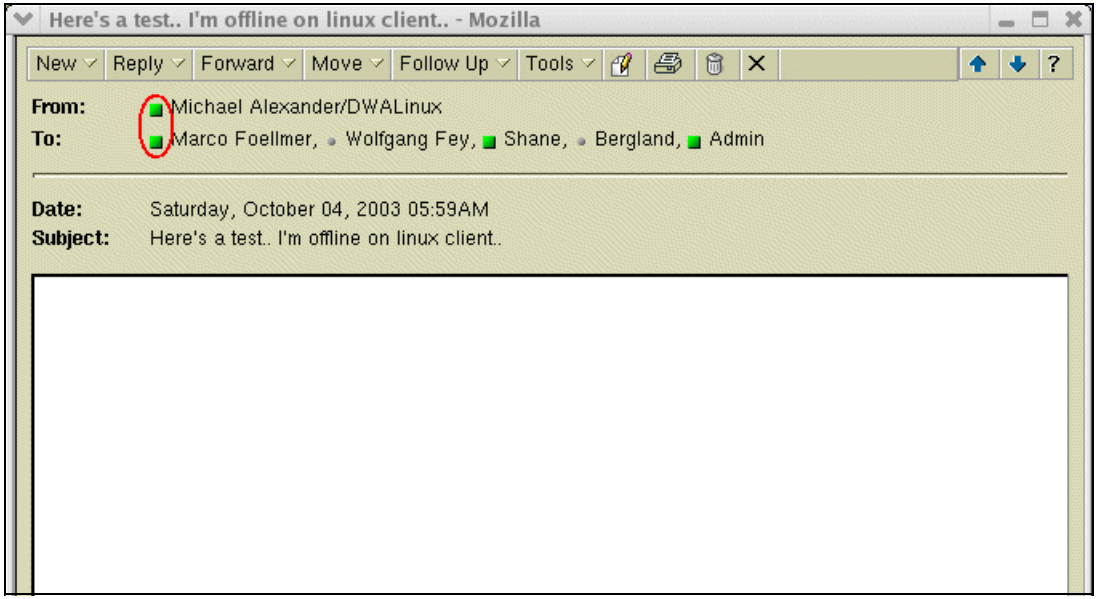


Figure 9-5 Online status indicators within a mail message

To initiate a chat, simply click on the online status indicator for that user (either at the Inbox level or within the message). This opens a chat window, as shown in Figure 9-6.

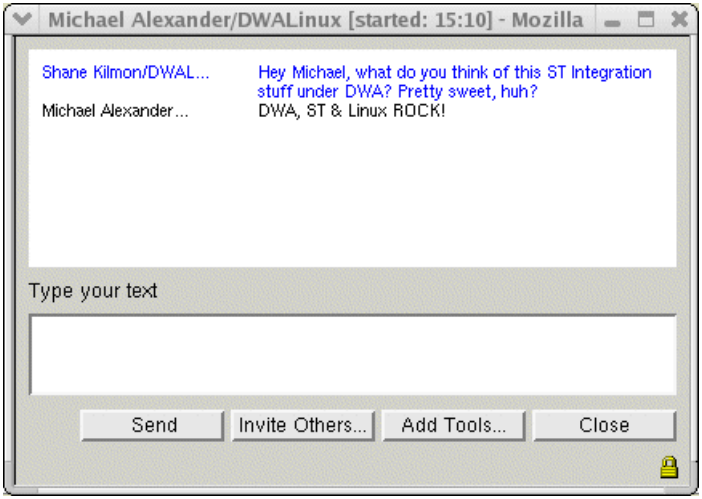


Figure 9-6 Chat window using Mozilla

By selecting your name at the top of your Inbox or Welcome page, you can change your online status to be in Active, Away, or Do Not Disturb mode (Figure 9-7). You can also change the message users see when hovering over your name in their instant messaging contact list, Sametime integrated Domino Web Access, or Notes client.

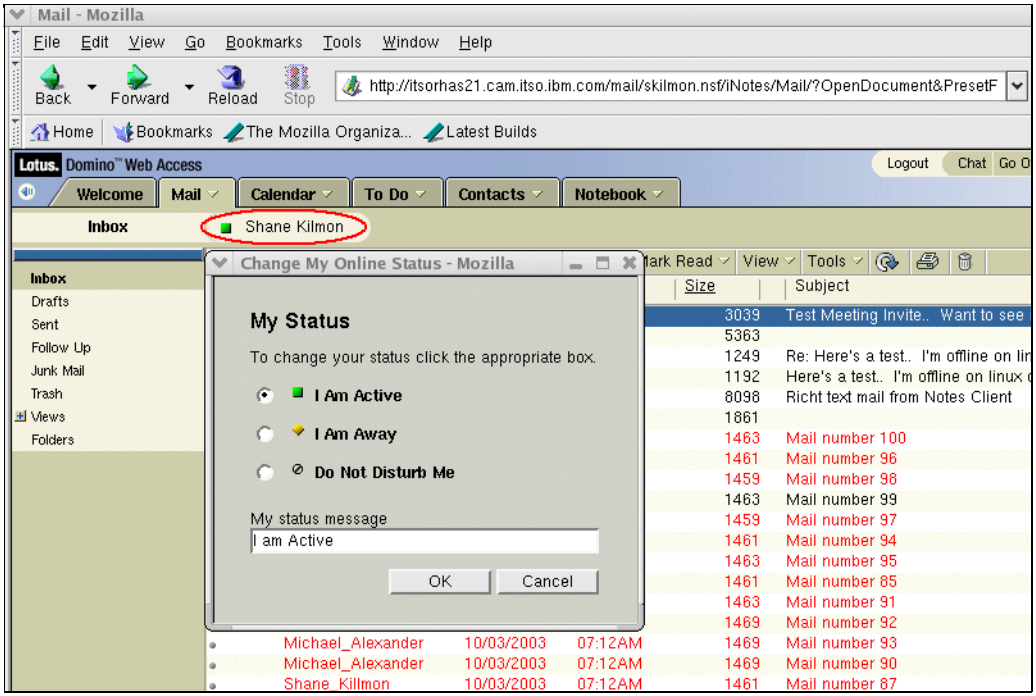


Figure 9-7 Changing online status within Mozilla

To access your instant message contact list (Figure 9-8), click the **Chat** button at the top right of your Domino Web Access session (Figure 9-9). This opens a window in which you can create or modify your contact list, add personal groups, and initiate chat sessions with people on your contact list.

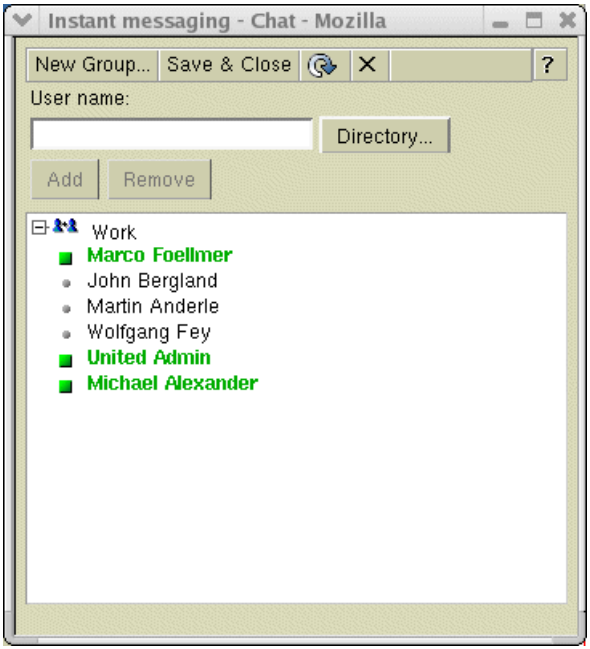


Figure 9-8 Contact list within Mozilla

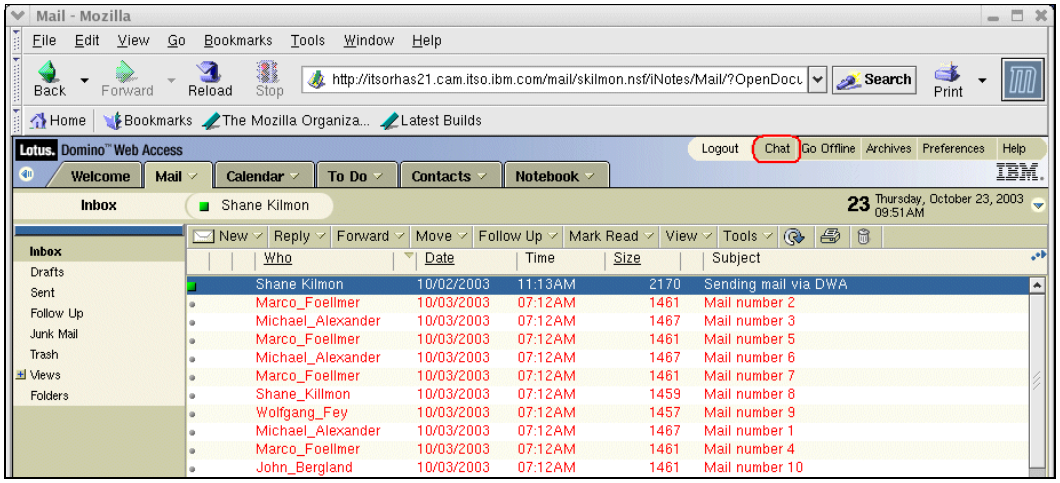


Figure 9-9 Chat button in Domino Web Access session

9.4 Notes.ini parameters for Sametime integration

Now that we have covered how to set up and use Sametime integration, we will discuss the parameters that are available to change its behavior. The following parameters can be accessed and modified through the notes.ini file:

- iNotes_WA_Chat

  Set this parameter to 0 to turn off all chat functionality. With this set, the Chat button in the top-right corner of the browser the online presence indicators will no longer be visible. The user will be unable to initiate chat via the DWA session.

- iNotes_WA_LiveNames

  Set this parameter to 0 to turn off all presence awareness indicators in views and messages. The user can still access the Chat button and the buddy list to initiate chat sessions (See Figure 9-10.)

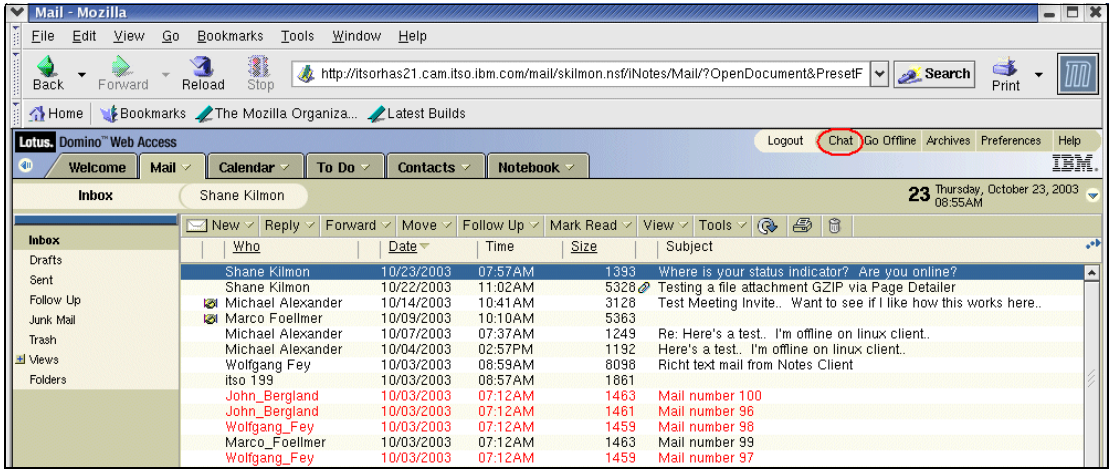


Figure 9-10 $Inbox with iNotes_WA_LiveNames=0 set on the server

- iNotes_WA_SametimeToken

  Set this parameter to 0 to disable the use of the Sametime Token method of authentication (via STAuthS.nsf and STAuthT.nsf), and use standard LTPA tokens if present.

- iNotes_WA_SametimeServer

  Setting this to the fully qualified domain name of a Sametime server (for example, stgateway.cam.itso.ibm.com), will override whatever is set in the Sametime server field in each user's Person document. This can be helpful in environments using Sametime clustering.

- iNotes_WA_STLinksCodebase

  This parameter should be set to the full URL to a valid stlinks directory on the Sametime server; for example:

  ```
  http://proxy.cam.itso.ibm.com/domino/sametime/stlinks
  ```

  The Java code in the stlinks directory is used to facilitate the connection between the Web clients and the Sametime server. This parameter enables the administrator to specify a different URL for the stlinks code, which is generally necessary in cases in which the environment calls for HTTPS connections, or if it requires a reverse-proxy path.

  You can also use this to provide a separate port number for the Sametime server.

- iNotes_WA_SametimeJavaConnect=1

  Adding this parameter setting to the Notes.INI on a DWA server enables an administrator to configure the DWA UI to display the Sametime Connect Client for Browsers UI rather than the native DWA Chat UI. For the change to take effect, the DWA server and the Sametime server must be restarted. This optional parameter is listed as an available option in the Domino Administrator 6.5.x Help, in the topic titled “NOTES.INI Settings for Domino Web Access with Sametime.” Finally, keep in mind the following additional considerations if DWA is configured to use the Sametime Connect Client for Browsers UI in place of the default Chat UI:

  – When the user clicks the Chat for the first time in the current DWA session, instead of seeing the DWA Chat list, the user is prompted to log into the Sametime Connect client for Browsers (unless SSO is enabled).

  – The Sametime Connect client for Browsers then launches the same way it would if the user had launched it from the Sametime server's home page. The user has access to all of the standard Sametime Connect Client functionality (aside from any functionality that has been disabled deliberately by the Sametime Administrator).

  – Because the Sametime Connect client is running in its own browser window, it can be minimized and maximized using the browser's window buttons and the Windows task bar.

  – If the Sametime Client is minimized to the Windows Task bar, clicking the Chat button in the DWA UI has no permanent effect. The DWA window will refresh and the Sametime Connect client will display briefly on the screen, but then it returns to a minimized state.

  In contrast, if the Sametime Connect client is currently displayed, clicking the Chat button will minimize the Connect client to the Windows Task Bar.

– Closing the DWA browser window (and exiting DWA) does not affect the Sametime Connect client. The user must exit the Sametime Connect client separately.

10

WebSphere Portal integration

With IBM Lotus Domino Web Access 6.5, there are several different ways to integrate with IBM WebSphere Portal Server. In IBM WebSphere Portal Server 4.21 and in the current release, IBM WebSphere Portal Server 5.0, there are many different portlets that can be used easily for integration. This chapter covers the integration considerations concerning the relevant portlets for Domino Web Access 6.5.

Additionally, we have provided Appendix A, “WebSphere Portal 5 installation on Linux” on page 387. This describes how to install IBM WebSphere Portal 5.0 and discusses the required configuration for using a Domino Directory–based LDAP server for Single Sign-On.

10.1 Relevant portlets

In this section we describe some of the portlets that are available from IBM, relevant to Domino Web Access. We discuss portlets that are available for both WebSphere Portal Server Versions 4.2.1 and Version 5.0.

Portlets in WebSphere Portal Server 4.2.1

The following two portlets are available from IBM and are relevant to Domino Web Access:

- Clipping: This portlet enables the administrator to clip content, images, tables, forms, table cells, and more from Web sites.
- Lotus iNotes: This portlet opens a user's calendar, address book, e-mail, or to-do list. This is also compatible with Domino Web Access.

Portlets in WebSphere Portal Server 5.0

We see that similar portlets are available for WebSphere 5.0:

- Clipping portlet: This portlet enables the administrator to clip content, images, tables, forms, table cells, and more from Web sites.
- Domino Web Access portlet: This portlet opens a user's calendar, address book, e-mail, or to-do list in the Domino Web Access design.

Notice that the Lotus iNotes portlet has now become the Domino Web Access portlet.

10.1.1 Domino Web Access and iNotes portlets

The Domino Web Access portlet is an iframe wrapper around the existing Domino Web Access GUI. The portlet gives options to wrap specific parts of the GUI such as the Welcome page, Mail, Calendar, To Do, and so on. Other than the iframe technology, these portlets do not add any extra capabilities over the base Domino Web Access.

Note: The Domino Web Access portlets from IBM WebSphere Portal V 4.2.1 and IBM WebSphere Portal V5.0 are supported both on Internet Explorer and with Domino 6.5, as well as on Mozilla 1.3.1 running on Linux.

Environment

The environment used in this scenario is illustrated in Figure 10-1.

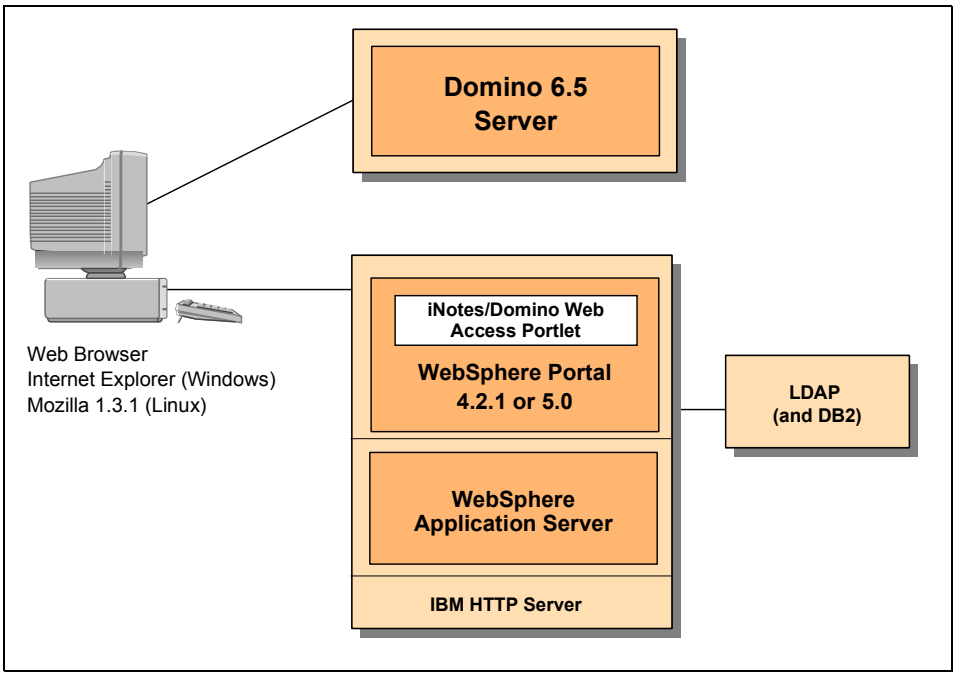


Figure 10-1 Domino Web Access portlet scenario

Tip: Internet Explorer 5.5 or later is recommended because when the portlet containing the iframe in the browser has a connection with the Domino server, with IE 5.5+, WebSphere Portal is not used as a bridge between the user on a workstation and the Domino server. There is direct communication between the iframe and the back-end Domino server, so performance is improved.

10.1.2 iNotes portlet from WebSphere Portal 4.2.1

This section gives an overview of the functionality and configuration for iNotes portlet, which is packaged and delivered with WebSphere Portal Server 4.2.1.

Generic parameters

After the Domino server is configured, each user must provide connection parameters (user name, password, and database name) to use the portlet.

Example 10-2 shows the iNotes portlet, which is deployed automatically during the installation.

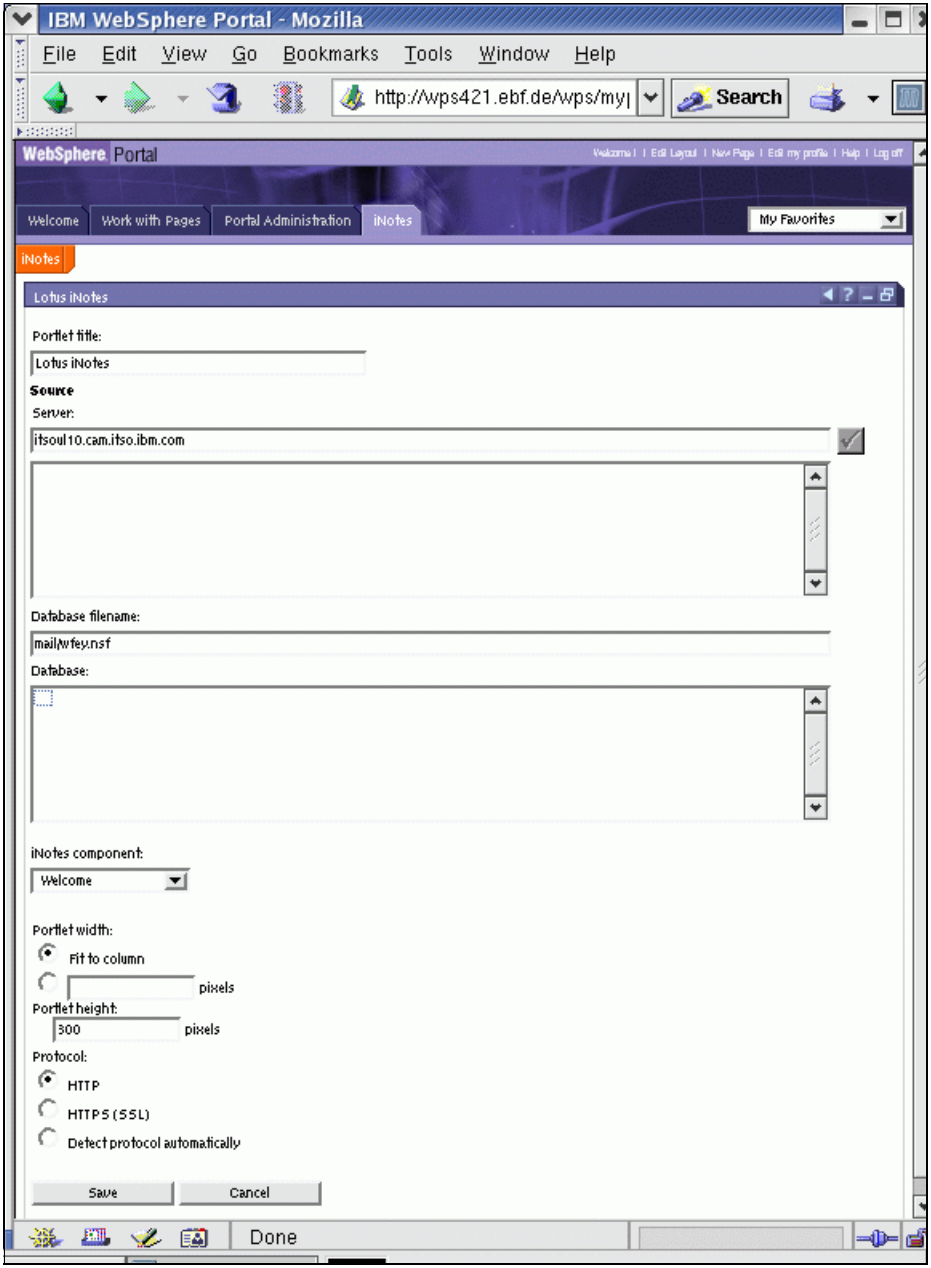


Figure 10-2 iNotes portlet from WPS 4.2.1 parameter form

iNotes portlet

Using this portlet, you can check your Domino Web Access or iNotes–based personal information management on your Domino mail server. If you are familiar with the iNotes or Domino Web Access browser-based environment, you see that is more or less the same thing. In this case, it is just running in a portlet window in the portal.

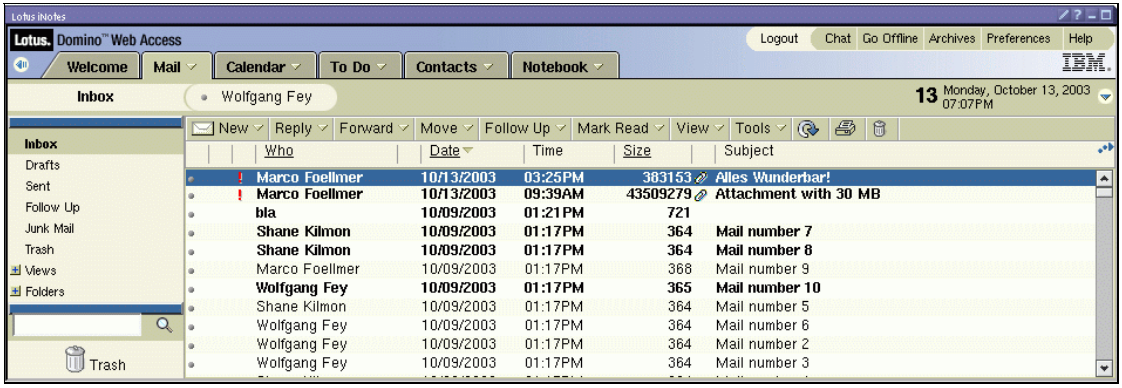


Figure 10-3 iNotes Mail portlet running Domino Web Access

The portlet contains all available Domino Web Access functions. This includes the entire Domino Web Access function set that is available to standard browser clients.

10.1.3 Domino Web Access portlet from WebSphere Portal 5.0

To configure the Domino Web Access portlet from WebSphere Portal 5.0.

1. Step 1: Configuration.

   To configure the Portal server itself you need administrator access to the portal server. Log in as the portal administrator.

2. Step 2: Select a page and enter the edit mode.

   After accessing the Portal server, from the main menu select a page where you want to add the Domino Web Access portlet. To edit the page, click **Edit page** in the menu, and the dialog in Figure 10-4 appears in the browser.

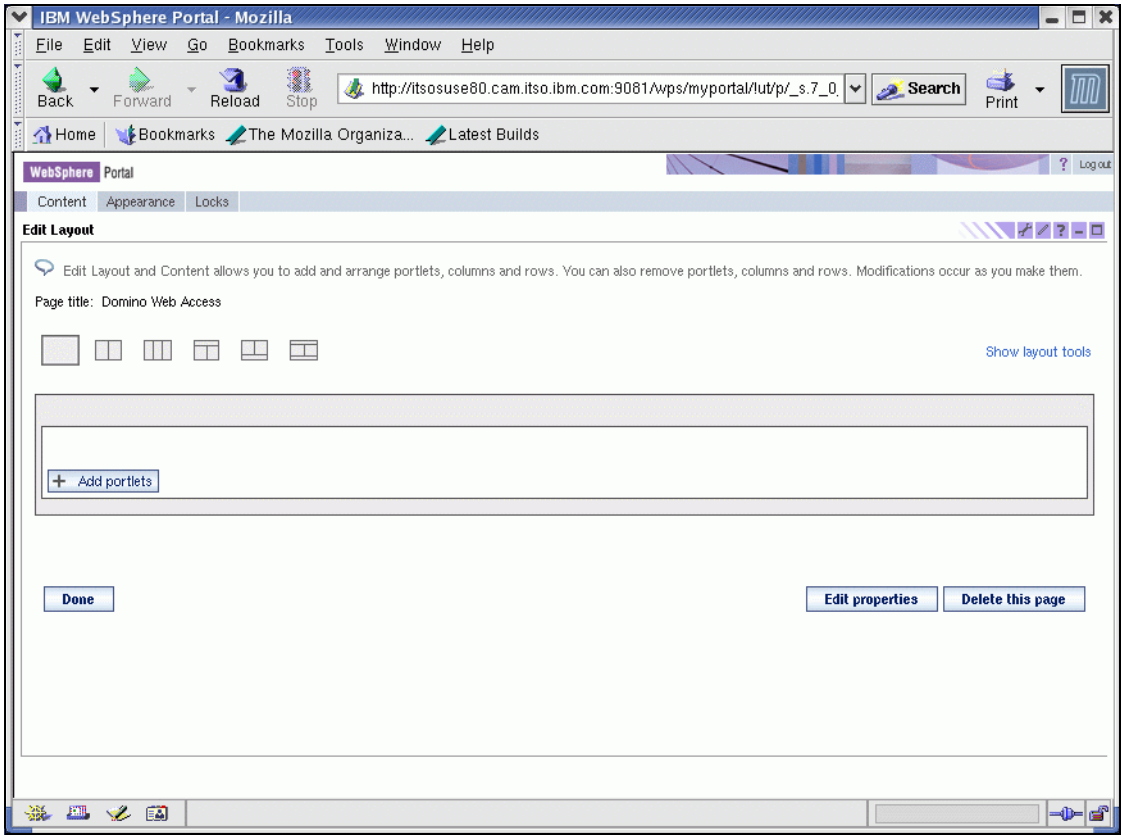


Figure 10-4 Editing the layout of WebSphere Portal page

3. Step 3: Edit the properties of the page.

   Click the **Edit Properties** button to change the settings for the page shown in Figure 10-5. Save the settings with the **OK** button.

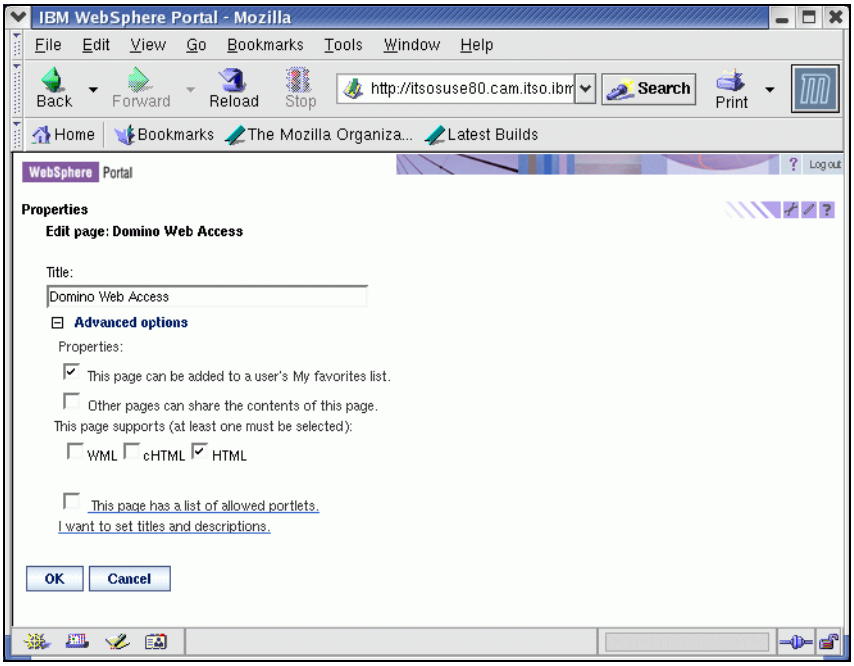


Figure 10-5 Portal page properties

4. Step 4: Add the portlet to the page.

   Click the **Add portlet** button to select a portlet from the list of available (deployed) portlets. Scroll through the list (Figure 10-6) until you reach the Domino Web Access portlet, or search for it with the search function.

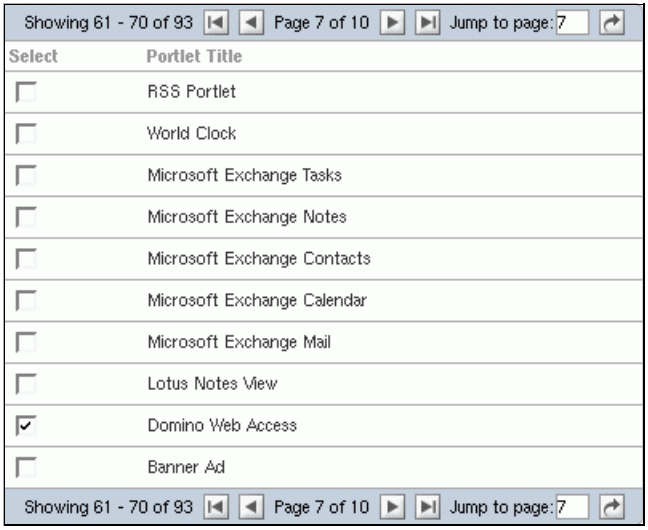


Figure 10-6 Adding the Domino Web Access portlet

   Click **OK** and **DONE** to save the portal page. The portlet is now generally available on the edited page.

Figure 10-7 Portal page save successful

5. Step 5: Set the portlet properties.

   In this step you set the portlet properties. Locate the properties logo on the upper-right corner of the portlet container on the portal page (Figure 10-8 on page 347).

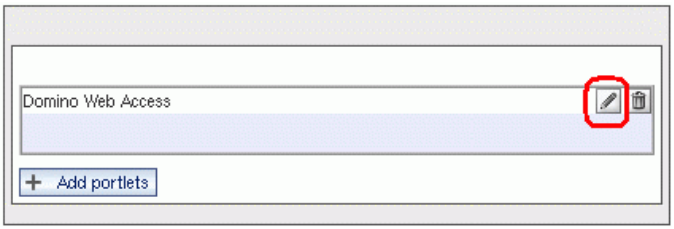


Figure 10-8 Setting the portlet properties

6. Click the properties logo and fill in the properties form (Figure 10-9).

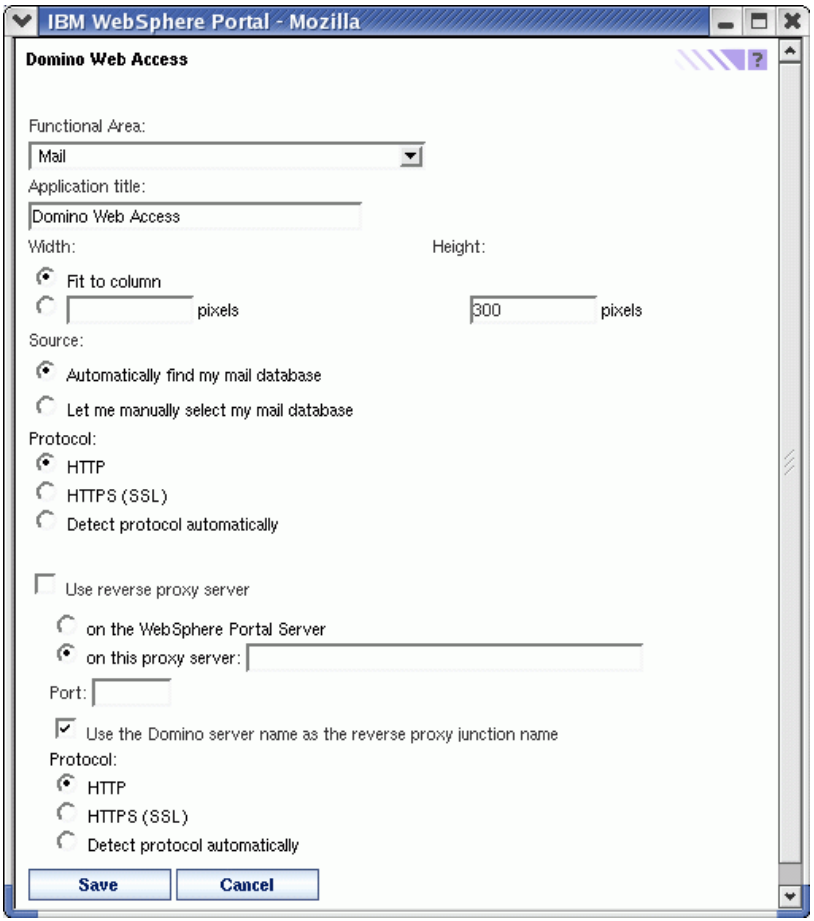


Figure 10-9 Domino Web Access portlet properties

Apply the correct setting for your environment and click **Save** to store these settings in the portal page.

7. Step 6: Portlet applied and page ready to use.

   With Single Sign-On enabled, the Domino Web Access dialog appears in the portlet on the portal page. Otherwise, the sign-on dialog from the Domino server appears in the portlet window.

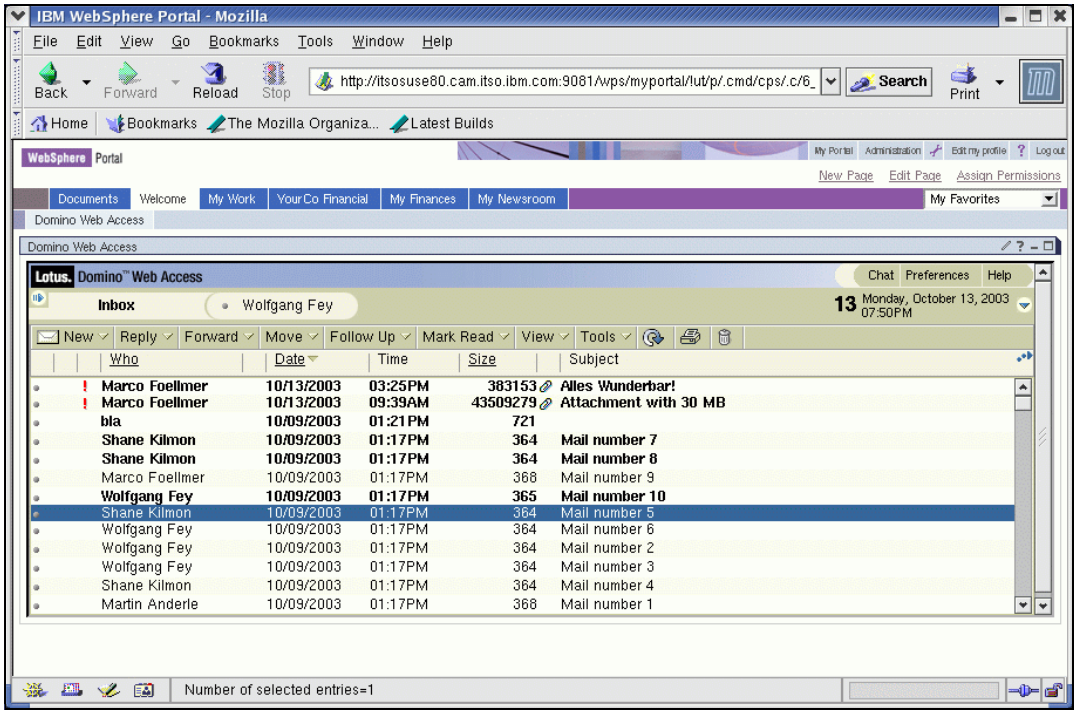


Figure 10-10 Portal page displaying the Domino Web Access portlet

10.2 Conclusion

This chapter has provided an overview of two simple portlets that are available with WebSphere Portal to provide access to Domino Web Access. To learn more about building custom portlets, we recommend reviewing the redbook *Portalizing Domino Applications for WebSphere Portal,* SG24-7004.

11

Customizing Domino Web Access

In this chapter we provide an overview of the Domino Web Access 6.5 template architecture and discuss why it is difficult to customize the design beyond the documented ways. Yet, some parts can be customized, with a reasonable amount of work. Several customization examples are covered in this chapter.

Domino Web Access 6.5 provides a new mechanism for customers and business partners to modify or customize some parts of the design templates. This ability to perform limited customization helps organizations make DWA 6.5 better fit their business needs, or to incorporate their corporate identity in the layout and design of the user interface.

This chapter covers the following topics:

- Customization considerations
- Template architecture
- Inheriting from an alternate template
- Customization samples
- Customizing the forms6.nsf
- Customizing the login screen

11.1 Customization considerations

Customizing Domino database templates, including the Standard R6 Mail template, is common among many customers and business partners. This has led to numerous questions regarding the type of customizations that can be done to the Domino Web Access 6.5 mail template.

Some areas of Domino Web Access were not designed in the Domino Designer. For this reason, the design resists the customization techniques familiar to developers who work with other Lotus products.

There is an extensive amount of JavaScript code used in Domino Web Access. Comments and meaningful text strings are stripped away from the code in order to optimize performance by minimizing the amount of code that has to be passed to the client side. This process is called obfuscation and we mention the translation lists of the JavaScript functions in 11.4.7, “Obfuscated JavaScript code” on page 369. The specific list of function names and their abbreviations can also be downloaded. See Appendix C, “Additional material” on page 443 for specific details about how to download this.

Important Customization Disclaimer: The ability to customize Domino Web Access 6.5 was not one of the design goals for this release. As such, customized templates are neither certified nor supported. Standard practice for Lotus Notes Support for customers who open incidents resulting from a customized template will be to instruct the customer to revert to the stock template to see whether the problem still occurs. If it does, Lotus Notes Support will troubleshoot the problem as it exists in the stock template. (In other words, Lotus support will not troubleshoot the customized template). If the problem does not exist in the stock template, Lotus Notes Support will recommend that the customer remove the modifications and submit an enhancement request of the desired functionality for the next release. This policy includes the forms6.nsf database as well.

11.2 Template architecture

The Domino Web Access template is located in the data directory on your Domino server. It contains the following properties:

Filename inotes6.ntf
Database title Domino Mail and C&S
Template name iNotes6

The Domino Web Access template inherits fully from the Extended Mail template (mail6ex.ntf). This template was designed to enable offline use of Domino mail

with the Web browser. Figure 11-1 shows an overview of this architecture and the inheritance relationship.

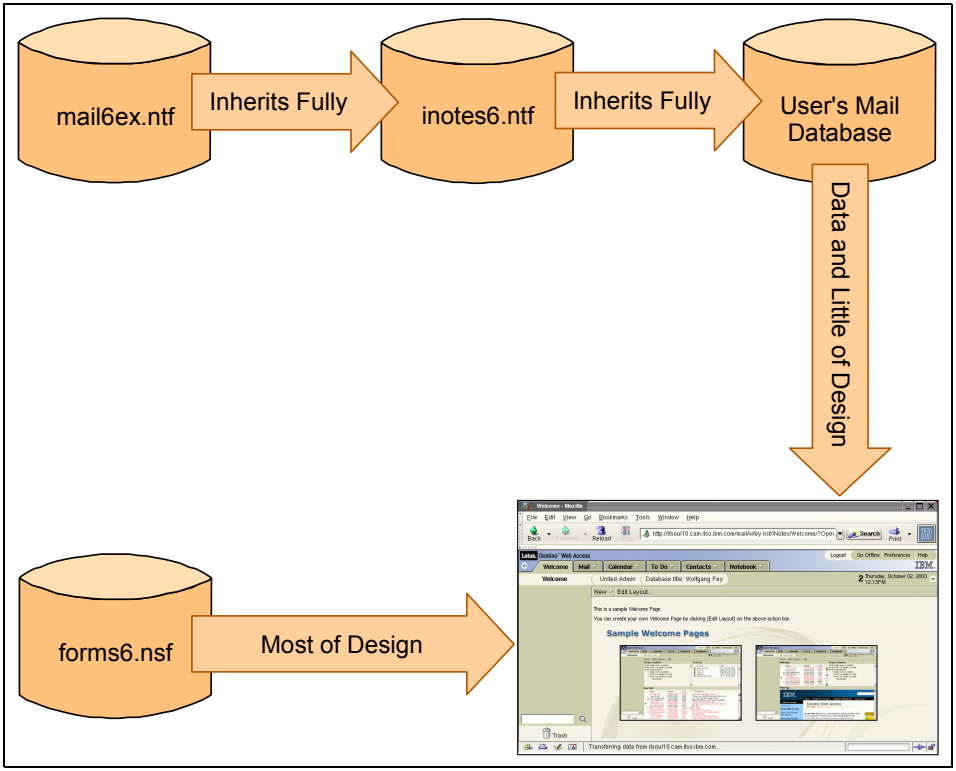


Figure 11-1 Domino Web Access template architecture

11.2.1 Additional design elements within inotes6.ntf

Additional elements in the inotes6.ntf template database include:

- Two Agents to support bidirectional synchronization from the Notes client for the Personal Address Book and Journal to the Domino Web Access Contacts and Notebook areas:
  - Synchronize Address Book
  - Synchronize Journal
- New views explicitly for Domino Web Access:
  - New Tasks view (iNotes_ToDo)
  - View to support Gantt view (Haiku_TasksAll)
  - New Contacts view (iNotes_Contacts)

  - New Notebook view ($Journal)
  - Meeting Notices from calendar (iNotes_Notices)
  - Two views to support the Domino Web Access Table of Contents and Menu (Haiku_TOC, iNotes)
- Additional Outline (iNotesOutline) to show the view and folder structure

11.2.2 The forms6.nsf database

All of the forms, subforms, and most graphics[1] used by Domino Web Access reside in a separate database named forms6.nsf. The database forms6.nsf is located within the <domino data>\iNotes\ subdirectory on the server.

The reason for keeping design elements in a different single database, instead of in individual mail databases, is that they can be cached on the server. All of the Web browsers accessing mail files on a server use the same design elements, which can be loaded from the server cache. Caching the elements on the server results in better performance on the server.

Figure 11-1 on page 351 illustrates the relationships between the databases that are used to comprise the user interface for a Domino Web Access mail file. The data itself is kept on the mail file (in this case, User1.nsf).

11.3 Inheriting from another mail template

If a company is customizing the mail template, the best approach might be to make this customized template be derived from mail6ex.ntf. The inotes6.ntf template can then be modified to inherit fully from this customized template. This would enable the company to continue to experience the customization that has been done to the Notes client or WebMail experience. However, most of the customization will not be viewable or usable with the Domino Web Access client.

Any additional view or folder, which is normally viewable from a browser, will also be displayed in the Domino Web Access outline. If a view or folder is hidden from the Web, then it will also be hidden in Domino Web Access.

11.4 Customizing the forms6.nsf

Despite the disclaimers in the beginning of this chapter cautioning against customization, there are *some* modifications that should not harm the

[1] The only exception to this is that certain images that are used in the mail views are contained either in the Domino icons directory or within the mail template.

functionality of Domino Web Access. As stated in 2.2, “Overview of new features” on page 16, there are several new ways to customize and enhance the design and functionality of Domino Web Access. In this section, we describe several customizations that an administrator and Domino developer can perform.

Several of the forms contained in the forms6.nsf database (in the iNotes directory on the server) enable Domino developers to modify their interfaces through Domino Designer. For example, developers could modify the s_MailMemoEdit subform so that e-mails include the location or department. Developers could write code in the Scene_PreSubmit function (inside the Custom_JS_Extensions form) to validate the new field.

- The Custom_JS_Extensions, Custom_WelcomePage, and Custom_Banner forms are available for modification. In addition, you can modify subforms.

11.4.1 General process for customization

The steps listed here describe the recommended process a developer should follow to modify the Forms6.nsf file:

1. Copy the Forms6.nsf file to a temporary directory.
2. Make changes to the forms as desired.
3. Test the changes to the forms.
4. Stop the HTTP process on the Domino server using the **`tell http quit`** server command.
5. Flush the database cache using the **`dbc f`** server command.
6. Copy the new Forms6 file to the Domino directory under the Domino Data directory.
7. Start the HTTP process using the **`load http`** server command.

Keep in mind that end users are not involved directly with the customization process. They only see the results. This feature is primarily for skilled Domino developers working with administrators who have necessary access rights to the server. All modifications to Forms6.nsf are made using Domino Designer.

11.4.2 Adding functionality to the user interface

The Custom_JS_Extensions form enables developers to write custom action buttons for any view or dialog. The functions will be included in almost every action bar, assuming that you are not parsing for the action that is currently active. Accordingly, be aware of what kind of function to add in this way. We provide some examples here for customizing the action bar.

Modifying the action bar

In this section, we discuss how to add new menu options to the action bar using two examples:

- Add a function for showing a Web page.
- Provide a function to show an alert, dialog box, or both that displays the unid of one or more selected documents.

Figure 11-2 highlights a new function in the Inbox action bar that opens the ITSO IBM Redbook Web page.

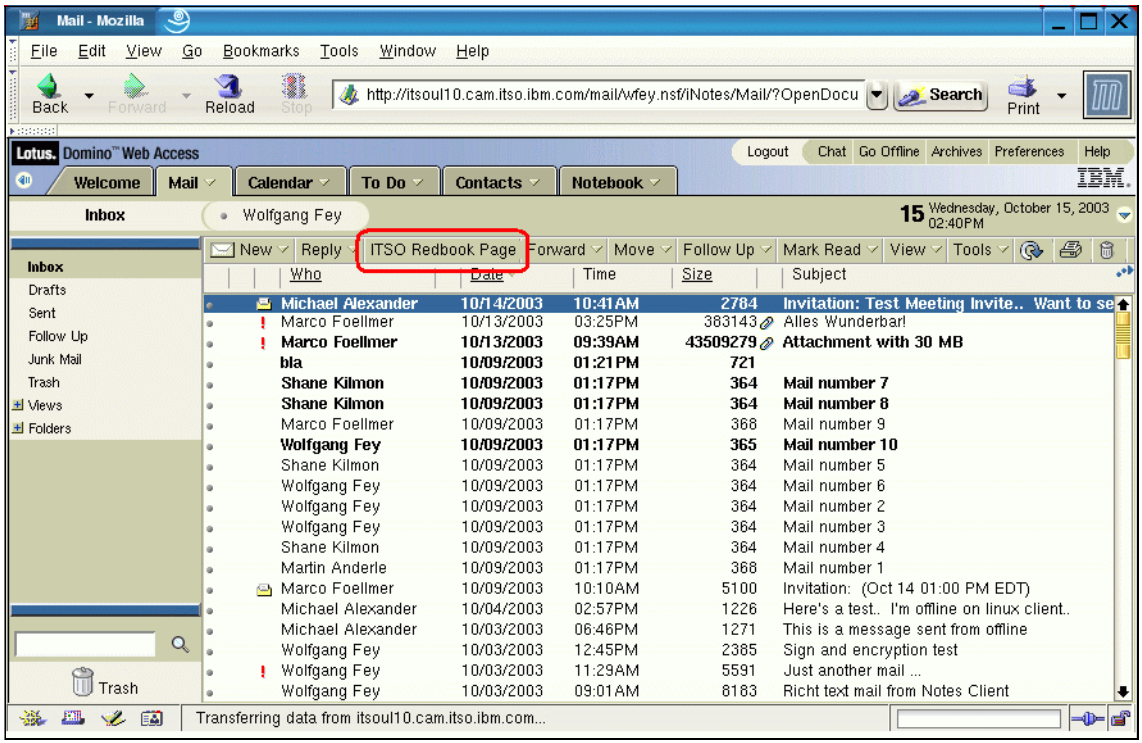


Figure 11-2 Additional menu item action button

This additional action button can be created by editing the Custom_JS form in the forms6.nsf file, as shown in Example 11-1.

Example 11-1 Custom_JS form JavaScript code (excerpt)

```
function Scene_Actions( s_SceneName, o_Window, a_Actions )
{
   a_Actions[a_Actions.length] = {pos:99, title:'Show Unids',
href:'javascript:ShowDocUnids()'};
```

```
   a_Actions[a_Actions.length] = {pos:100, title:'ITSO Redbook Page',
href:'http://www.redbooks.ibm.com'};
}
```

The called JavaScript function in the same form could be similar to Example 11-2.

Example 11-2 Custom JavaScript function code (excerpt)

```
function ShowDocUnids()
{
   //
   // this is a test of the 2 API functions:  D_Custom_GetSelectedDocs and
D_Custom_IsView
   //
   var fp = API_GetSelectedDocs();
   if (fp)
      alert("Selected Documents" + "\n" + fp.join("\n"));
   else
      alert("Please select a document.");
}
```

The result of these modifications are two additional action buttons in the menu bar, which are highlighted in Figure 11-3 on page 356.

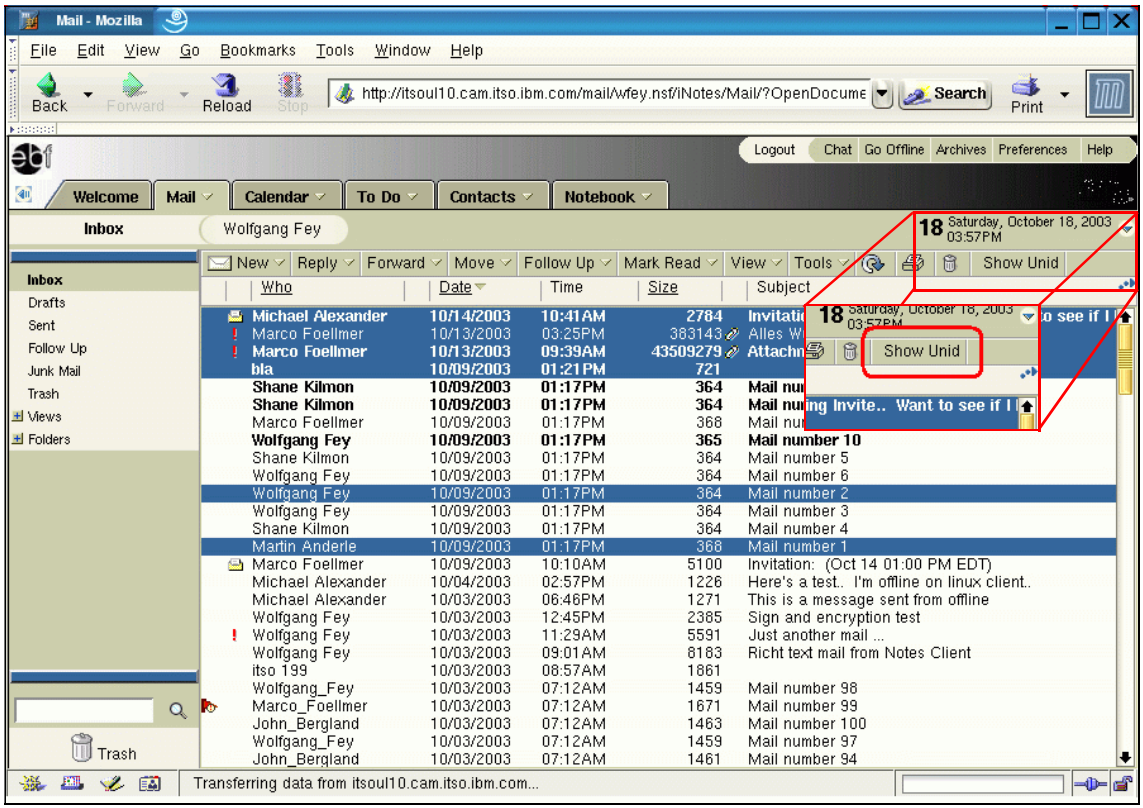


Figure 11-3 Inbox with new Show Unid function and selected documents

After you have selected one or more documents in the Inbox (or any other folder or view), the Show Unid function displays the window shown in Figure 11-4.

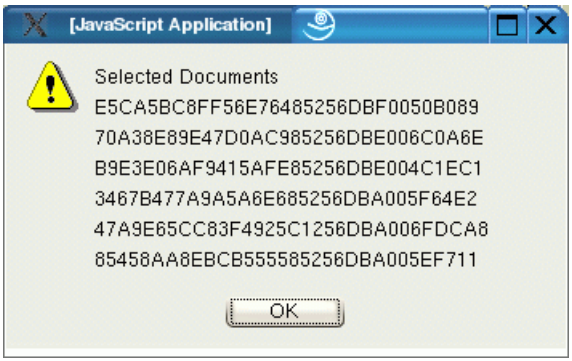


Figure 11-4 Displaying the unique IDs of the selected documents

Adding a subfunction to the Tools menu

The next example (Example 11-3) shows how to implement an additional subfunction for the Tools menu. This is a launch function for creating a new mail memo with a pre-populated subject field. In this example, a Help Request memo is created directly from a menu entry.

Example 11-3 Code for adding a subfunction to the Tools menu

```
function Scene_Actions( s_SceneName, o_Window, a_Actions )
{
   if (s_SceneName.toLowerCase().indexOf("s_") != 0)
   {
      var imax = a_Actions.length;
      for (var i=0; i< imax; i++)
      {
         var s;
         if ("object" == typeof(a_Actions[i].title))
            s = a_Actions[i].title[0];
         else  s = a_Actions[i].title;
         if ("tools" == s.toLowerCase())
         {
            a_Actions[i].href[a_Actions[i].href.length] = "divider";
            a_Actions[i].href[a_Actions[i].href.length] = null;
            a_Actions[i].href[a_Actions[i].href.length] = "Send help request";
            a_Actions[i].href[a_Actions[i].href.length] =
"javascript:SendHelpReq()";
            break;
         }
      }
   }
}
```

Example 11-4 illustrates the JavaScript function that is being called by the new menu entry.

Example 11-4 Code for the JavaScript function

```
function SendHelpReq()
{
   var RecipientList = "onlinehelp@ibm.com";
   var SubjectText   = "Help Request";
   var urlArgs='';
   urlArgs += ',SendTo;'  + RecipientList;
   urlArgs += ',Subject;' + SubjectText;
   openNewShimmerDoc("($Drafts)","Memo",urlArgs);
}
```

After implementing this code change, the new menu item is shown in the Tools menu. This is highlighted in Figure 11-5.

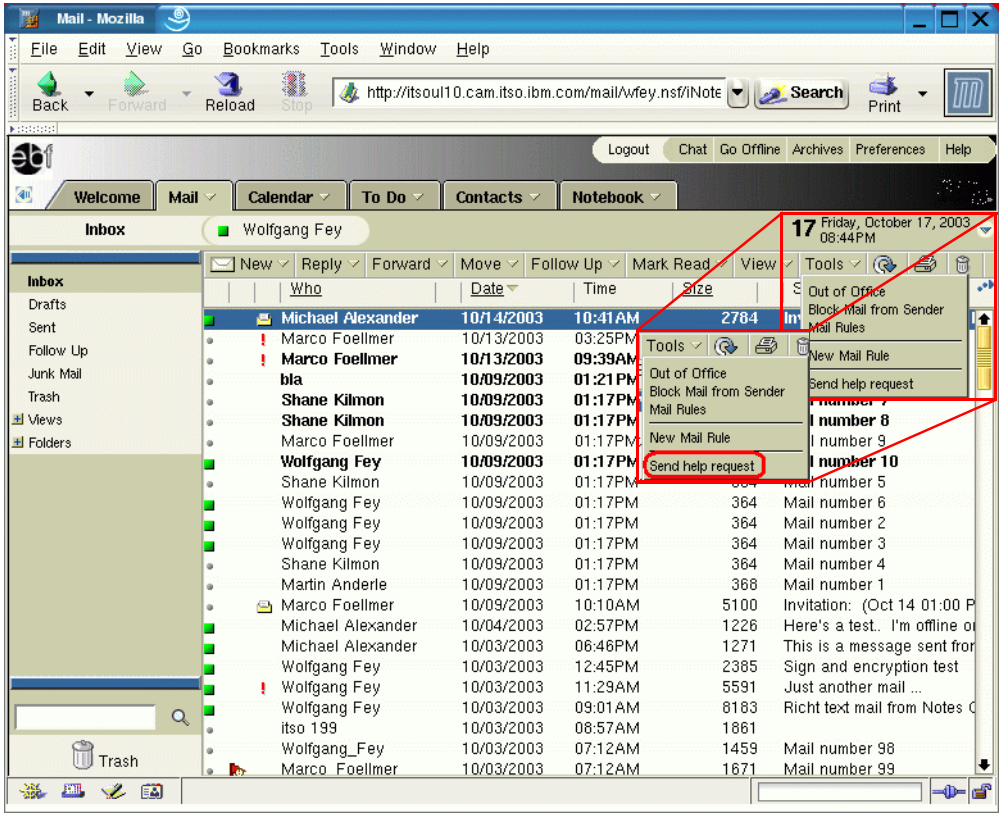


Figure 11-5 New menu entry in the Tools menu

Figure 11-6 shows a memo with the subject line pre-populated by the new function.

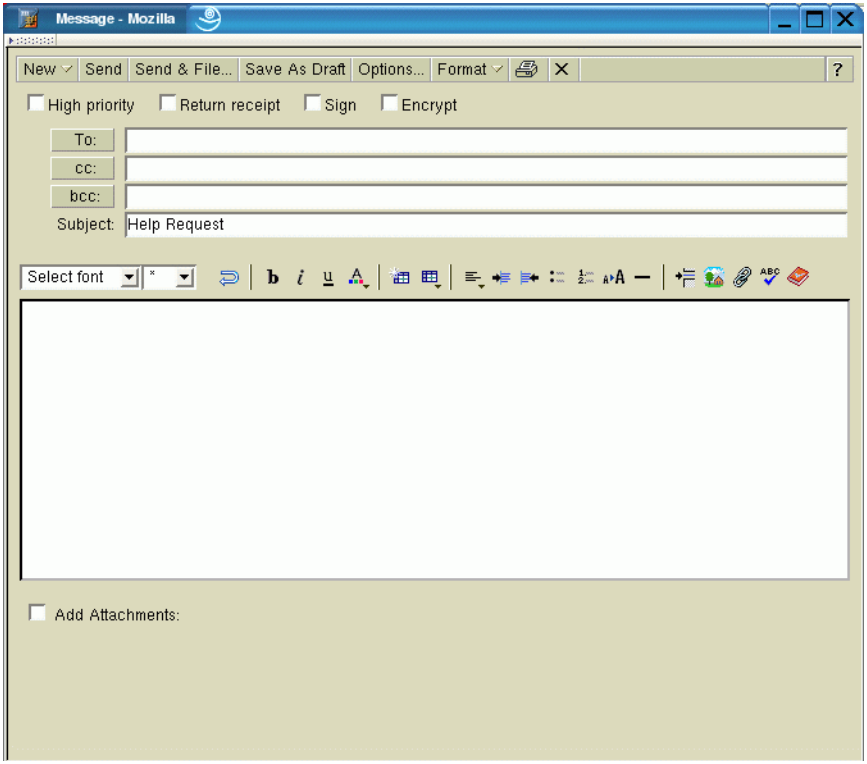


Figure 11-6 New mail with pre-filled field

11.4.3 Customizing the Welcome page

The Custom_WelcomePage form enables developers to add more choices for the end user's Welcome Page. As an example, we demonstrate how to increase the listing of choices that are inserted in the Web site selection control from within the edit dialog of the Welcome page configuration.

Figure 11-7 shows the listing of forms within forms6.nsf, as it would be viewed from within the Domino Designer 6.5.

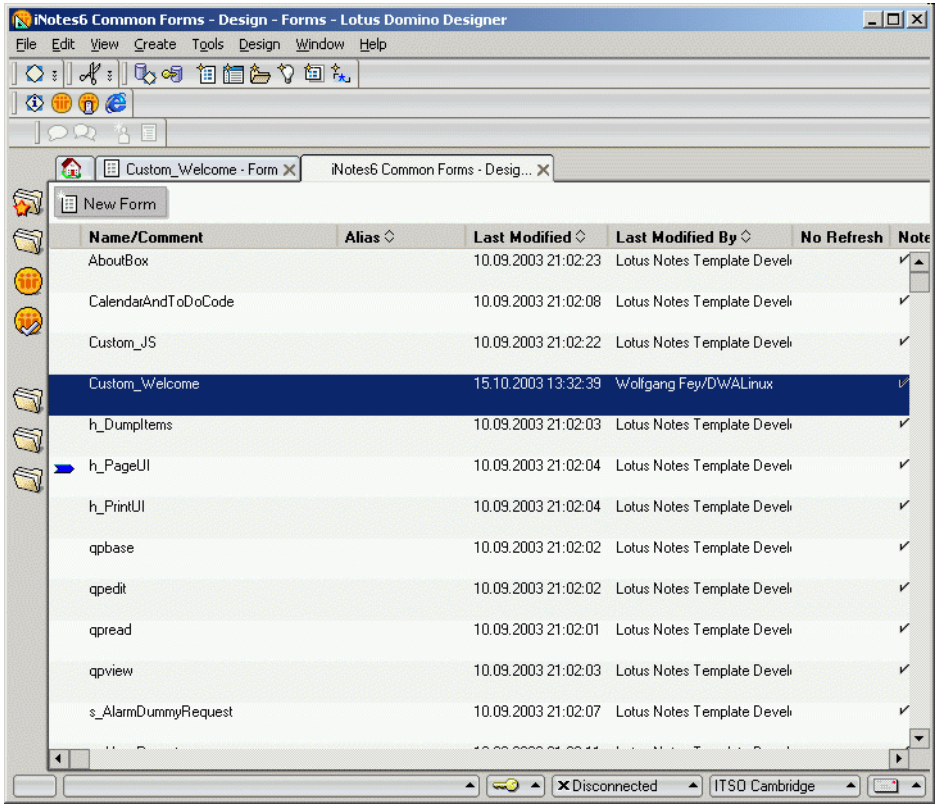


Figure 11-7 Notes 6.5 Designer showing the iNotes6.nsf with the customizing forms

When the Custom_Welcome form is opened, the example code shown in Figure 11-8 illustrates the values for the titles variable. The important part to note is that an additional value of `ITSO` has been added to the titles variable, and the corresponding URL of `http://www.redbooks.ibm.com` has been added as a new value to the URLs variable.

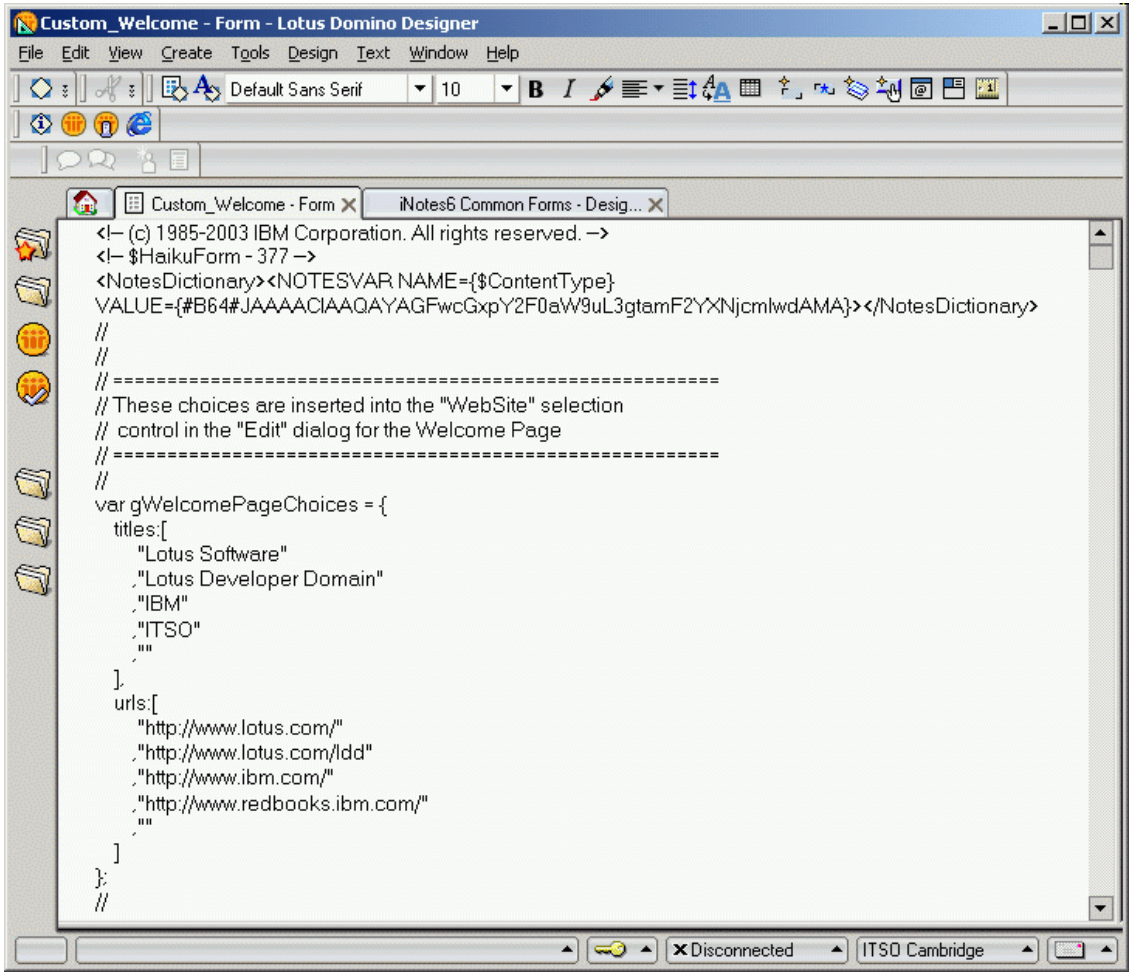


Figure 11-8 Custom_Welcome form in Domino Designer 6.5

After saving this code change within the form and restarting the HTTP server on the Domino server, end users can select the additional entry option of `ITSO`. This is demonstrated in Figure 11-9.

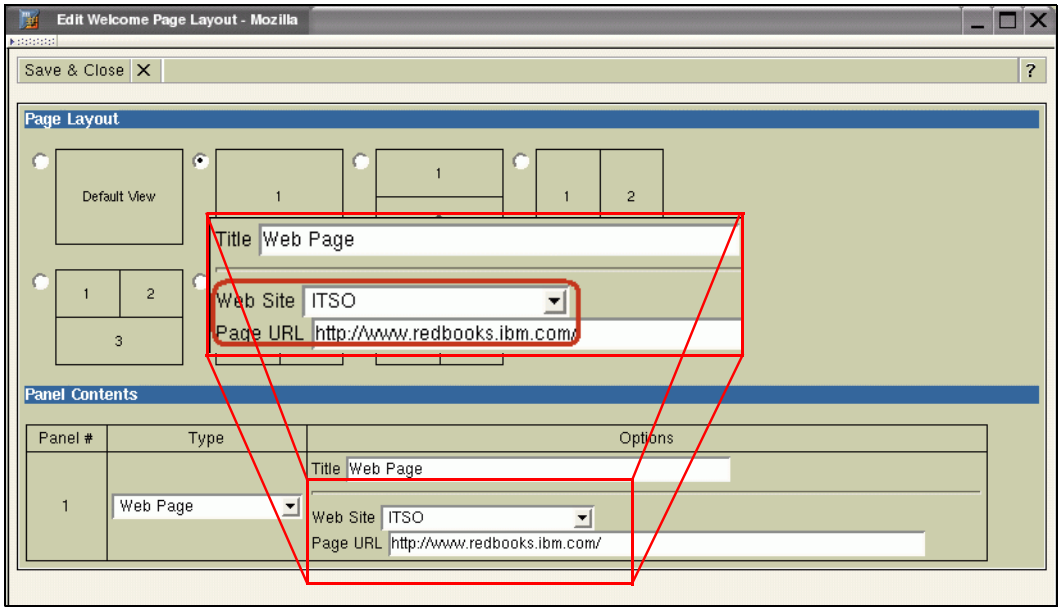


Figure 11-9 Customize Edit Welcome Page Layout dialog

Selecting the new entry shown in Figure 11-9 opens a welcome page similar to the one shown in Figure 11-10.

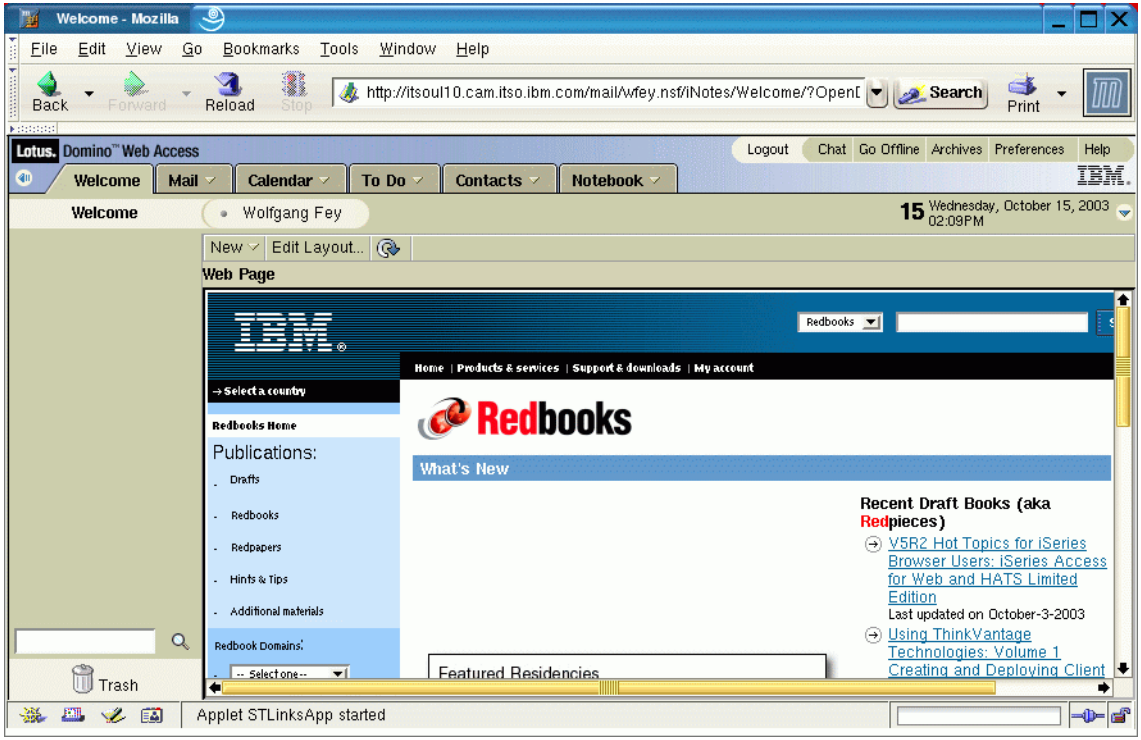


Figure 11-10 Welcome page with the customized Web page loaded

11.4.4 Customizing the banner logo

The Custom_Banner subform enables developers to modify the Domino Web Access logo or to replace the logo with a text string instead of a graphic image. In the following two examples we do both.

Modifying the banner with text

To perform this modification, first open the subform in Domino Designer 6.5 and include a simple text string. Figure 11-11 on page 364 shows how we insert the text string `DWA customization example`.

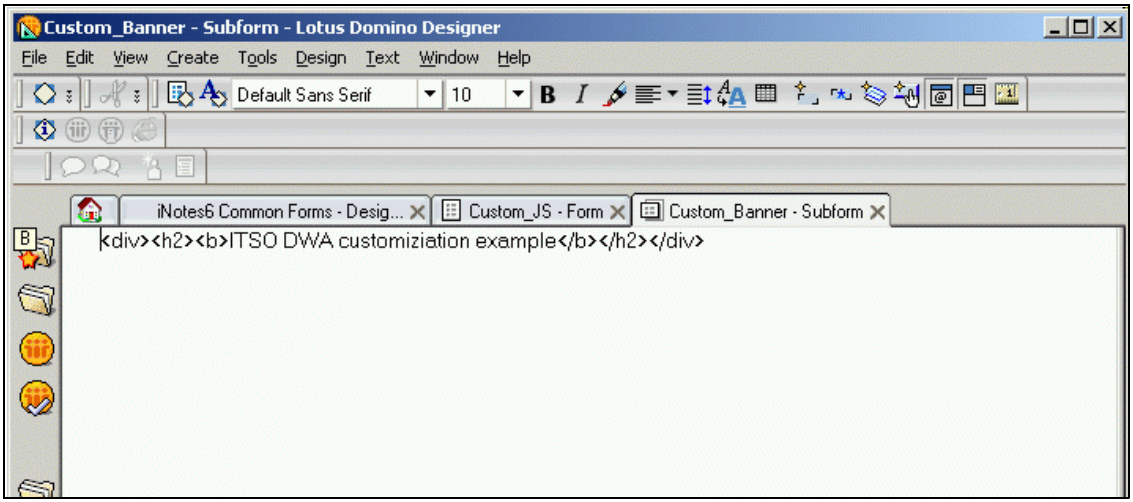


Figure 11-11 Modifying the Custom_Banner subform in Domino Designer 6.5

When the modification is complete and the changes have been saved on the server, the top banner in Domino Web Access appears as shown in Figure 11-12.

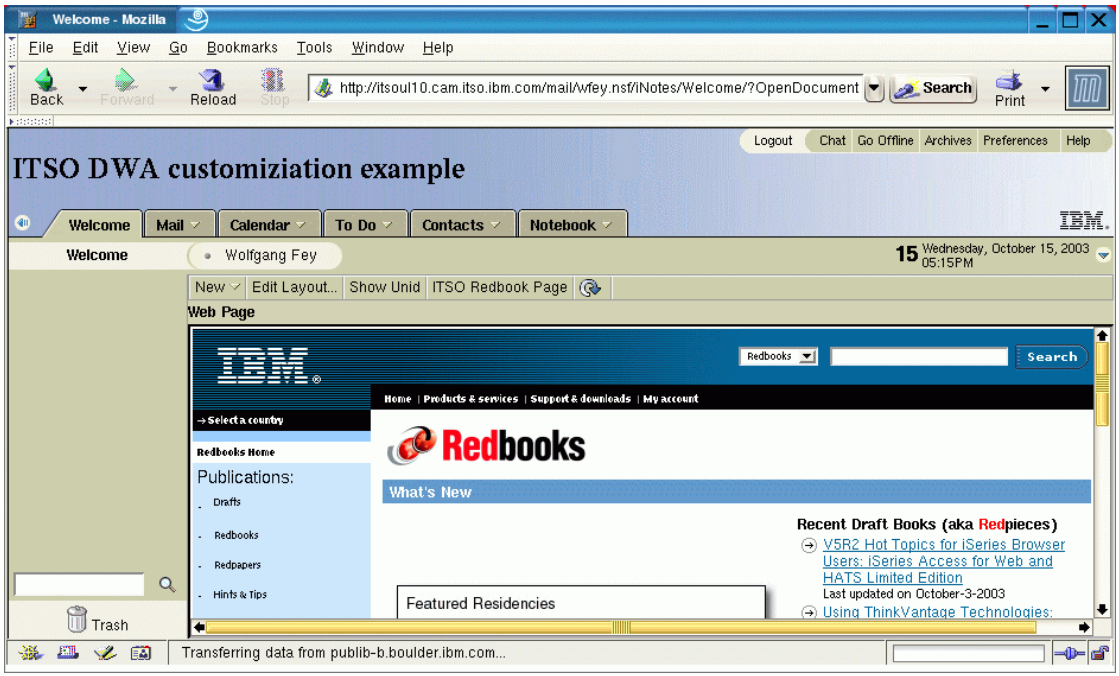


Figure 11-12 Customized Domino Web Access with a simple text string

11.4.5 Modifying the banner with a custom logo

You can modify and set a custom logo for the Domino Web Access screen. For this example, create (or have access to) a new image resource. In our example, the name of the new banner logo iwmage. is ebf.gif.

Next, open up the Custom_Banner subform and reference your image resource in the subform as shown in Figure 11-13.

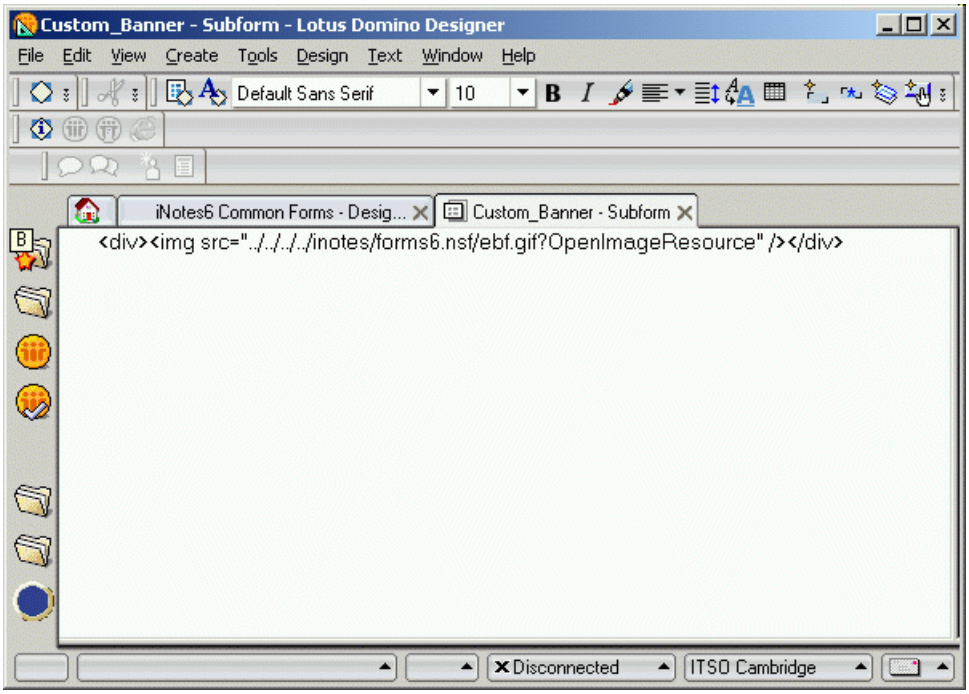


Figure 11-13 Referencing an image resource in the Custom_Banner subform

After saving this modification, the Domino Web Access browser window appears as shown in Figure 11-14.

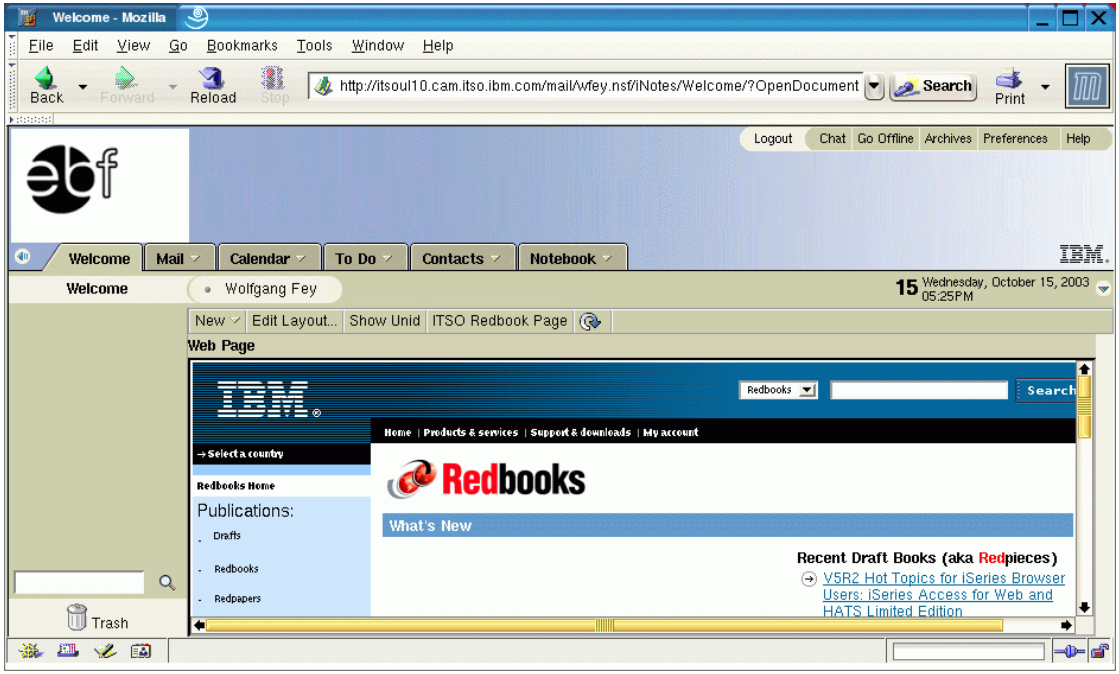


Figure 11-14 Custom logo applied to the Domino Web Access design

11.4.6 Customizing styles

> **Attention:** The modification shown in this section is absolutely unsupported and only advisable if you are totally familiar with the design and architecture of Domino Web Access. Be aware that you will make these modifications at your own risk. We strongly recommend that you thoroughly test all modifications in a test environment prior to introducing these changes to your production environment.

The first example for customizing styles is to change the color gradient on the top banner. We change the existing shading background (from blue to white) and modify this to a gradient with a transition from white to black colors.

The background gradient is taken from an attachment in an image form document called gradblue10.jpg. It is placed in the forms6.nsf in the hRessourcesByName view.

Attention: At this point, you are altering a supported configuration. If you follow this step and then need official support from Lotus, the support team will ask you to switch back to the original forms6.nsf to properly troubleshoot any problems.

The following steps describe how to modify the gradient image that serves as the background for the top banner:

1. To modify the gradient image, create a new form with the form name `Image` and a field called `Body` of type `richtext`.

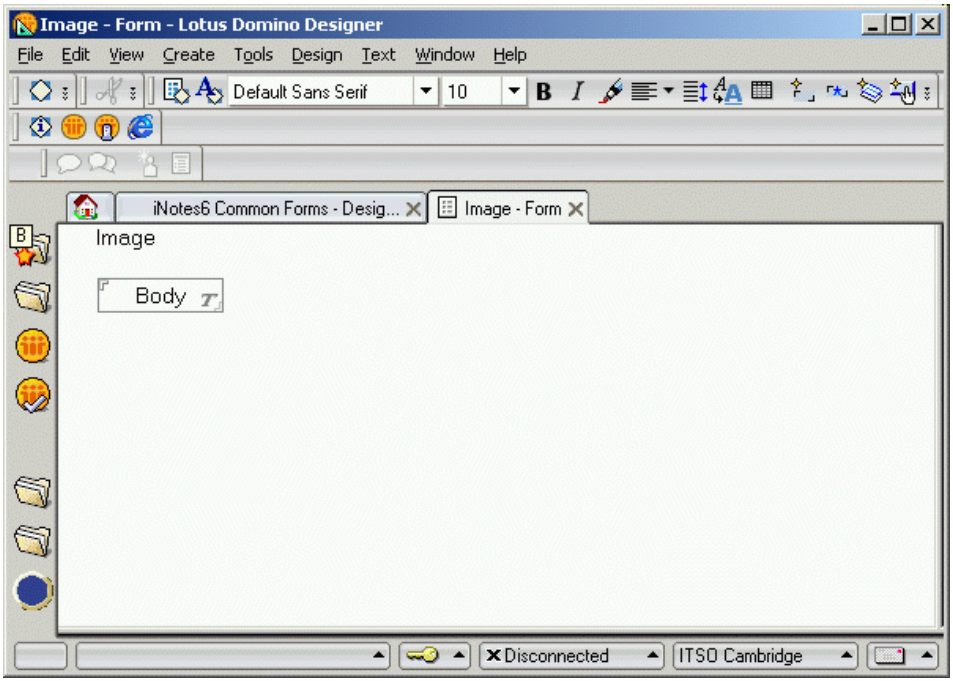


Figure 11-15 New Image form

2. Next, open the hResourcesByName view with the Notes Client.

3. Locate and open the gradblue10.jpg document. Detach the attachment, modify the colors with a graphics editing tool, and reattach the file *without changing the name* and *without changing the size of the image* (Figure 11-16).

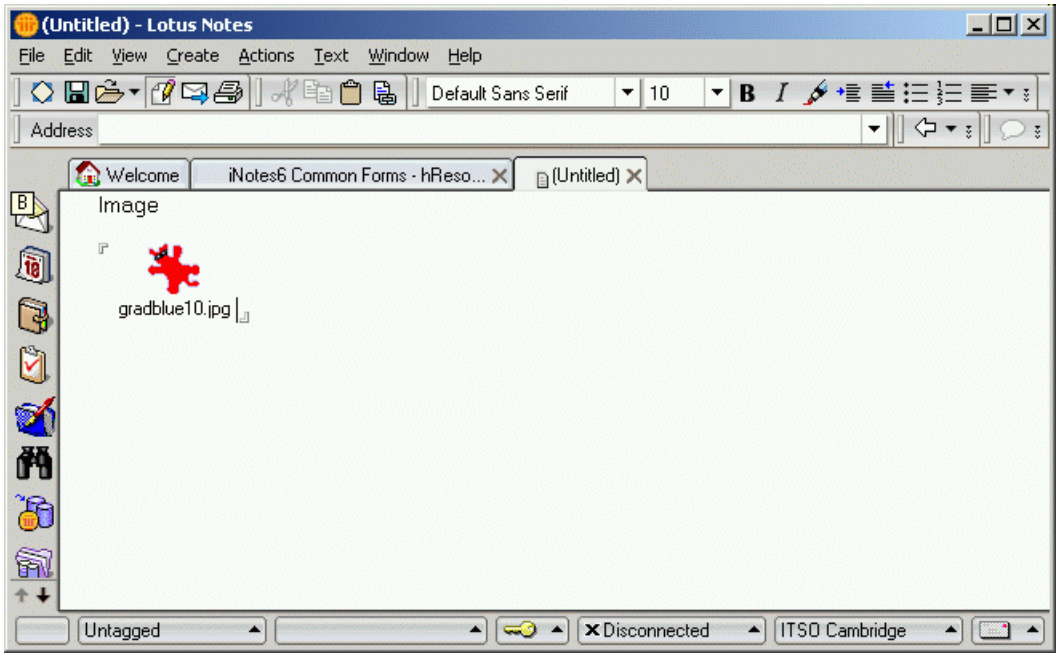


Figure 11-16 Image document gradblue10.jpg after modification

4. Save and close the document. Restart the HTTP server and reload the browser window to view the change. In our example we switched the background image in the banner from a blue to gray gradient. We also switched the gradient direction from left to right. Figure 11-17 on page 369 shows the results.

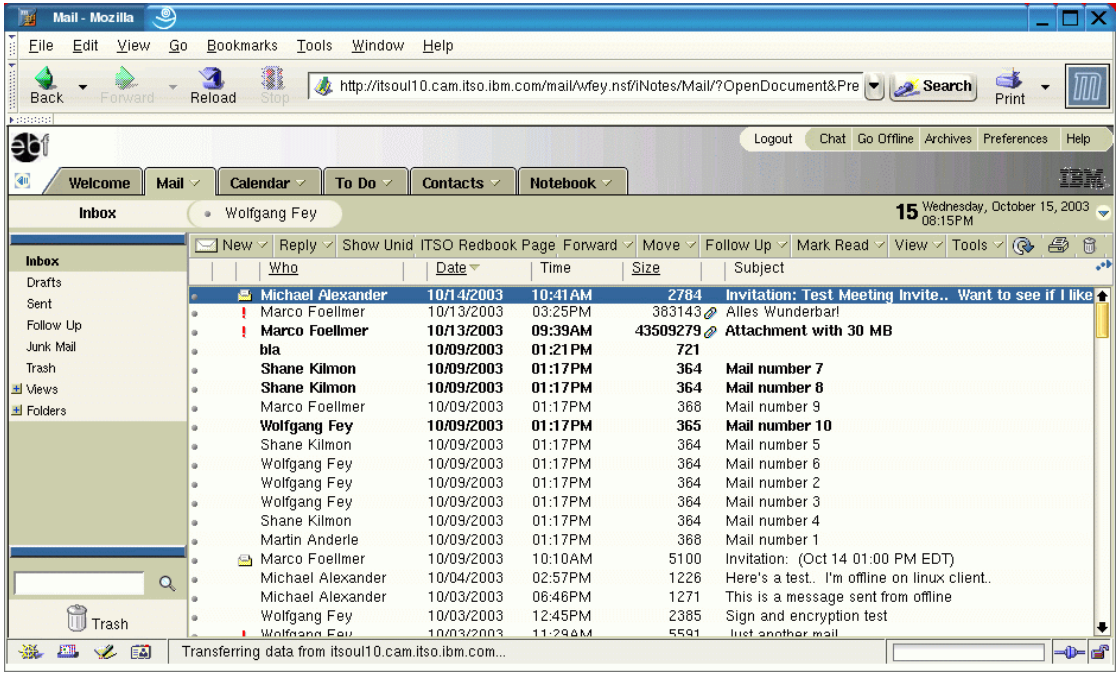


Figure 11-17 Top banner background image after modification

11.4.7 Obfuscated JavaScript code

The Customization_Wordmap.txt file (casually referred to as the Obfuscation List) is a list of JavaScript functions that maps long JavaScript function names to specialized abbreviated names for the same functions.

As you may know, Lotus abbreviates (obfuscates) much of the code within Domino Web Access in order to enhance performance of the product and to make it more difficult for someone to decipher the proprietary code. Fortunately, this list provides a map to translate long function names into short ones. Keep in mind that the browser does not care what a function is called. However, it does care about how many bytes are downloaded. By changing the long function names to short ones, this saves on the number of bytes a user downloads and ultimately enhances the performance of DWA.

Fortunately, this list is available as an additional material to this redbook. Refer to Appendix C, “Additional material” on page 443 to learn how to access this file.

Figure 11-18 on page 370 shows a sample of the entries in this list that map the actual JavaScript function names to the abbreviated, obfuscated names in the

JavaScript code. Access to this list should help developers to better understand the JavaScript code and to modify and debug it in their own ways.

Note: We hoped to print much of this list within the book, but the file contains more than 6,000 entries, so it is much more practical to keep the file online and allow users to download it at their convenience.

```
These strings will replace the following:
=================================================
AA      IWAOfflineCtrl_DoInstall
AB      lenWksInMnth
AC      bEditable
AD      refreshtree
AE      sFormsFile
AF      tableMenu
AG      ScheduleTab_ZoneChangedCB
AH      LastCondArray
AI      GCInfo_getDateHeaderTitle
AJ      iTotal
AK      m_isGecko
AL      sRepeatWeekends
AM      CZoneInfo_addBoundaries
AN      isSaveAction
AO      anAdjusts
AP      getDates
AQ      aoEndDateTime
AR      CCSFormControler_getDocCtx
AS      getControl
AT      oDocCtxOrig
AU      currentMonth
AV      stHour
AW      sUnreadOnly
AX      bShowMissed
AY      CSequentialAsyncAction_doAborted
AZ      isDateOnlyDoc
Aa      RepeatAction
Ab      stDummy
Ac      stIndex
Ad      Initialize
Ae      setHours
Af      thisVsHorz
Ag      FindRepeatAction
Ah      bDeleteAttach
Ai      getInformation
Aj      sAltCopyTo
Ak      div_parent
Al      div_child
Am      getRow
An      posCornerSquare
Ao      CResPickControler_addOnlineMeetingPlaces
Ap      oProposedDates
Aq      minute1
Ar      alertOwnerNotSet
As      minute2
At      sDatesAreaHtml
Au      bBooking
Av      updateDNTime
Aw      compareDate
Ax      CCommonDOMElem_findElem
```

Figure 11-18 Sample entries from the Customization_Wordmap (Obfuscation List) file

11.5 Using Redirect to customize the login screen

In this section, we describe how to customize the login screen using the Domino Web Access Redirect feature. The login form that will be referenced is the DWALogin form. After the Redirect feature has been properly configured and the DWALogin form has been properly referenced, the form may be customized using the Domino Designer.

As a new usability enhancement built into DWA 6.5, Domino Web Access Redirect enables a user to log into a specific server (the redirect server) and be redirected automatically to a different server that has been set up for a specific purpose. This enables end users to access their mail file *without needing to know the name of their mail file or the name of their mail server*. Using Domino authentication methods, Domino Web Access Redirect redirects a browser to a user's mail file based on the user name and password. Users need only know the name of the Domino Web AccessRedirect server.

Any Lotus Domino Designer programmer can code additional functionality into the redirect database. We do not show any examples here, but we could think of an integration into a portal or about using the styles of a corporate identity design. In terms of functionality, it could be a redirect into a special portal database, containing the DWA portal mode content (with &ui=portal at the end of the URL), or it could be a referer to a local news database shown to the user before he enters his own mail file, for example.

The following sections provide an overview for installing and configuring the Domino Web Access redirector. The first step for redirection setup is the creation and setup of the redirector database.

11.5.1 Setting up Domino Web Access redirector database

Before customizing the login screen, set up Domino Web Access Redirect, which is included as a template (IWAREDIR.NTF) in the Domino data directory. The user configures information for each of the following areas:

- Server Settings
- UI Setup
- Application Setup

To set up Domino Web Access Redirect, perform the following steps:

1. Create a database from the IWAREDIR.NTF template.
2. Using the Notes client, open the database that you created.
3. Click **Setup** (as shown in Figure 11-19 on page 372) and follow the prompts to set up Domino Web Access Redirect.

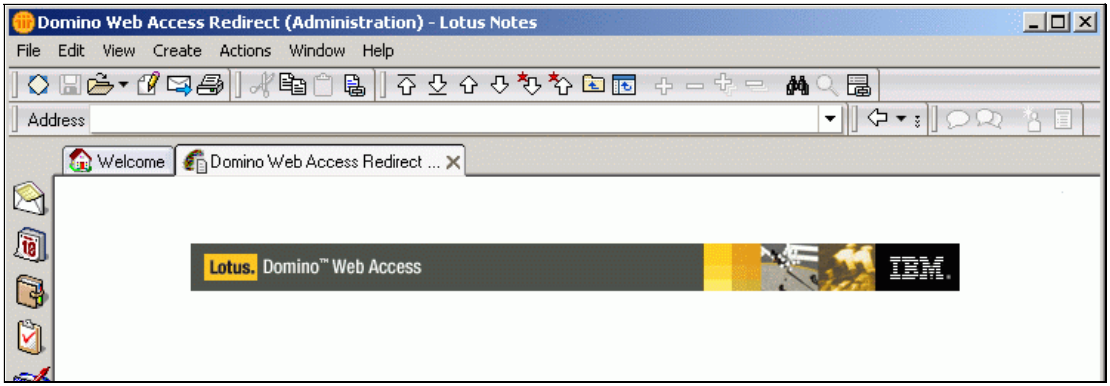


Figure 11-19 Set up Domino Web Access redirector database

4. Select the **Server Settings** option (Figure 11-20).

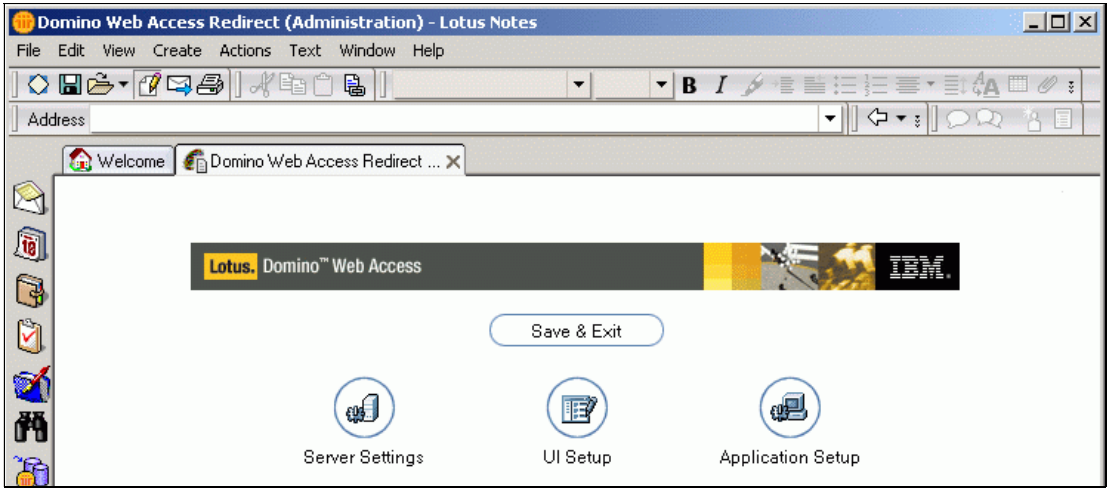


Figure 11-20 Setup option selection

Server Settings

The Server Settings menu, has three options:

Fixed	Binds the redirection to a specific Domino server.
Mailserver	Redirects the user to the home mail server in the person document.
Dynamic	Selects a Domino server from the list of available servers by its common name. This name is added as the target host name to the rest of the full qualified domain name.

Important: Be aware that the common name is not always the same name as the TCP/IP host name. If it is not, the redirection fails with this option selected.

5. Select **Fixed** and enter a fixed server address to redirect users to, as shown in Figure 11-21. (In our case, this is http://itsoul10.cam.itso.ibm.com.)

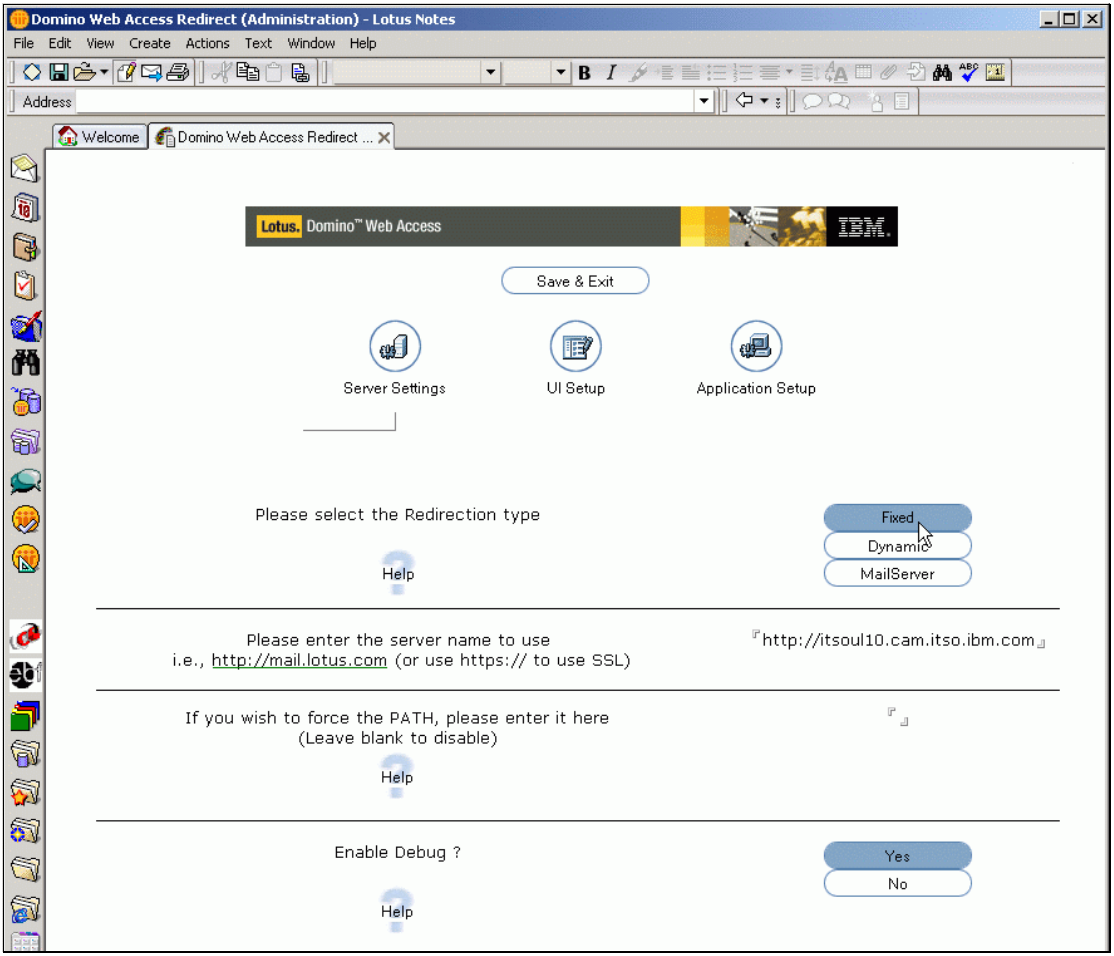


Figure 11-21 Selection of redirection options

By setting the last option, Enable Debug, to **Yes**, the user sees the browser debug options displayed while being redirected. This is very helpful to an administrator when looking at the user's browser window to troubleshoot or resolve redirection or login problems.

Tip: After Domino Web Access redirection is set up correctly and running without any problems in the production environment, this parameter should be switched to **No** for better login and redirection performance.

UI Setup

In the UI Setup dialog, the administrator can set the parameters for the user's browser display. This includes switching colors, adding a custom logo, and including a custom text message (such as `Please be patient`) to the redirection page. Figure 11-22 on page 375 provides an overview of the different options.

This UI Setup screen is just for configuration (not customization) and it is very simple. Only the logo, background color, and redirection text message are configurable. Anything else must be coded in the Designer.

After setting the UI settings, switch to the last option, Application Setup.

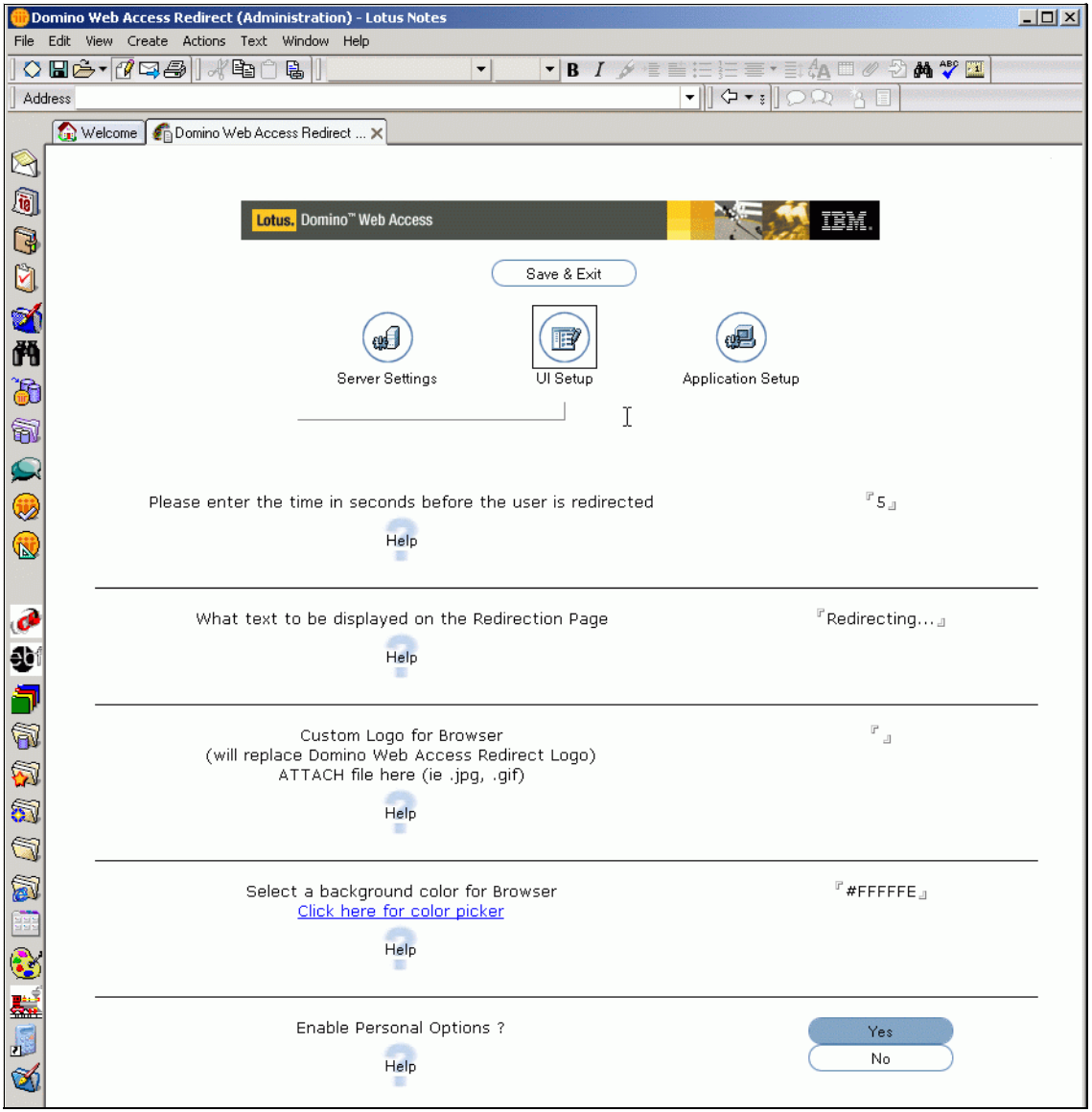


Figure 11-22 UI Setup options

Application Setup

The Application Setup interface (Figure 11-23) gives an administrator the option to set ACL access. It also provides information about the default server setup.

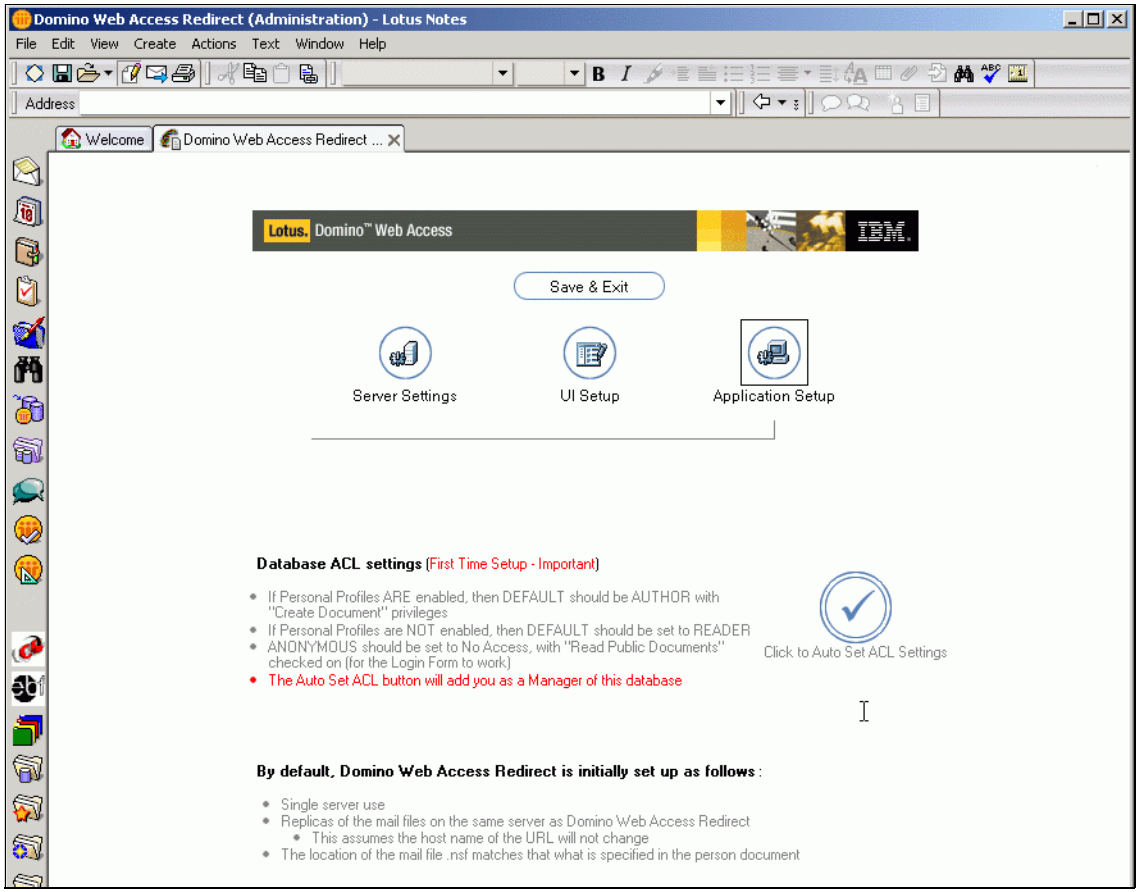


Figure 11-23 ACL setup dialog

In this Application Setup dialog, the administrator can set the ACL to the right levels automatically. Clicking that button opens the message in Figure 11-22 on page 375.

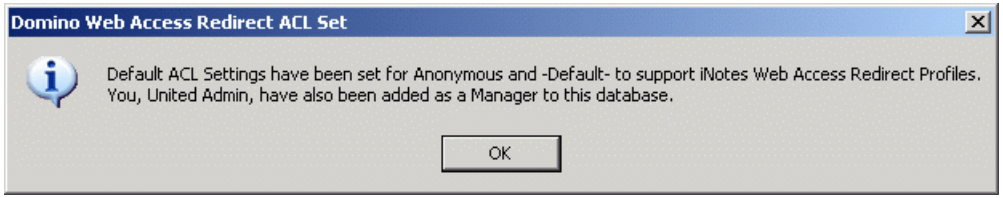


Figure 11-24 ACL Settings message

After you close this dialog, click **Save & Exit**. This completes the setup process for the redirector. The ACL has been set to the levels shown in Figure 11-25.

Access Control List

		Actions								
	Names	CrDoc	DlDoc	PerAg	PerFld	ShrFld	LscAg	RdPub	WrPub	**Type**
Managers:	United/DWALinux	1	1	1	1	1	1	1	1	Admin Server
	United Admin/DW ...	1	1	1	1	1	1	1	1	Person
	LocalDomainAdmins	1	1	1	1	1	1	1	1	Person Group
	LocalDomainServers	1	1	1	1	1	1	1	1	Server Group
Designers:										
Editors:										
Authors:	-Default-	1	0	0	0	0	0	1	0	Person
Readers:										
Depositor:										
No Access:	OtherDomainServers	0	0	0	0	0	0	0	0	Server Group
	Anonymous	0	0	0	0	0	0	1	0	Unspecified

Figure 11-25 Redirection database ACL after automatic setup

11.5.2 Using Domino Web Access Redirect

When the procedures in the previous sections are complete, the redirection database is set up and ready for use.

Referencing the Domino Web Access login form

Using the Domino Web Access redirect database requires the setup and administration of a Domino Web Server Configuration database. This is based on the domcfg5.ntf template on any server running the redirector database, as shown in section 11.5.1, “Setting up Domino Web Access redirector database” on page 371.

In order to use the new Domino Web Access login form as the active default login form for browser-based login, the form must be referenced in the Domino Web Server Configuration database (domcfg.nsf). If the database does not yet exist, the administrator must create it and can use the following steps:

1. Create a new database.

2. Select the **Show advanced templates** option.
3. Give the database the name `domcfg.nsf` in the Notes data directory on the server.
4. Choose the domcfg5.ntf template called **Domino Web Server Configuration**, as shown in Figure 11-26.

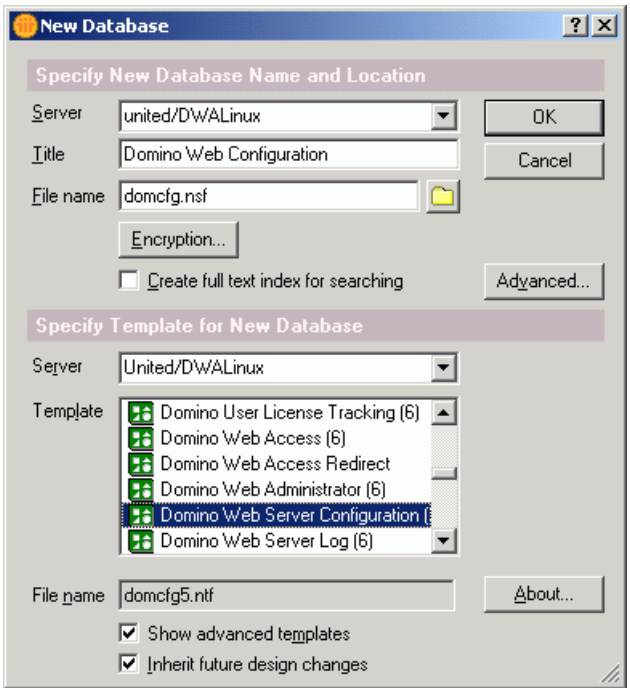


Figure 11-26 Creation of Domino Web Configuration database dialog

5. Open the new Domino Web Server Configuration database (domcfg.nsf).

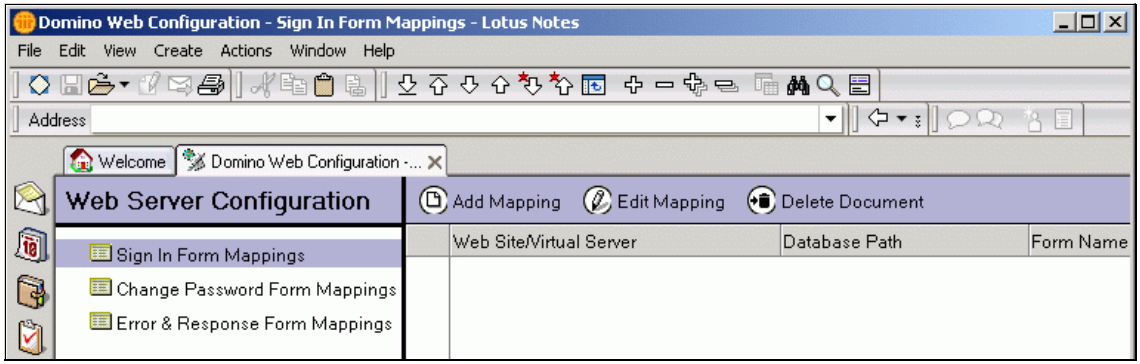


Figure 11-27 Domino Web Server Configuration database

6. On the Domino Web Configuration tab, click **Add Mapping**.
7. In the Sing In Form Mapping window (Figure 11-28), change the Target Database to your Domino Web Access Redirect database.
8. Change the Target Form to `DWALoginForm`.

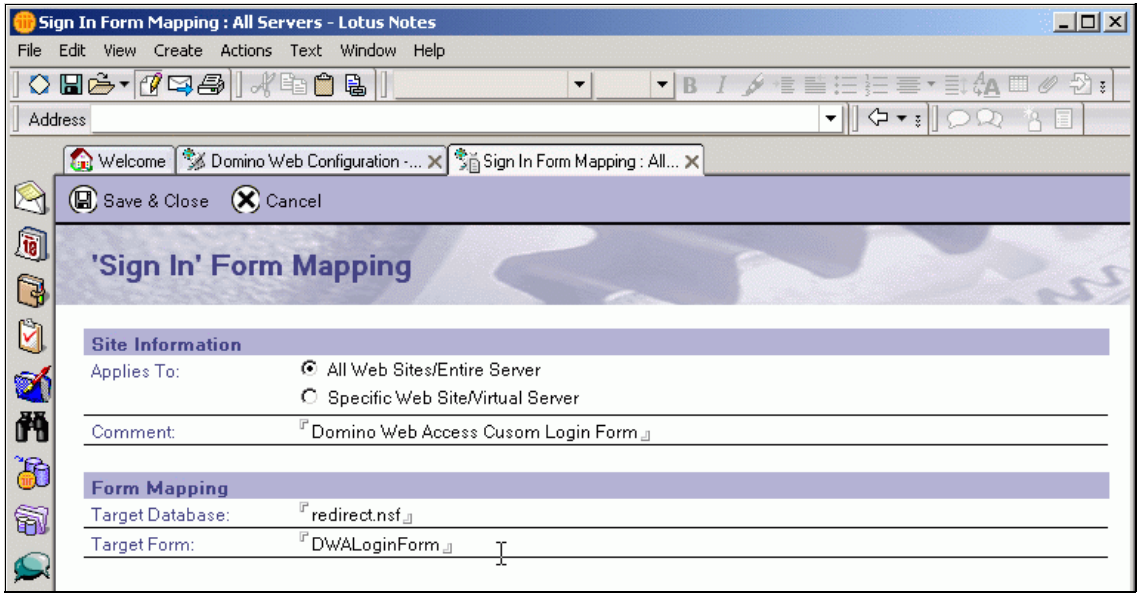


Figure 11-28 New login form mapping

9. Click **Save & Close** to save the changes.

The new DWALoginForm is now ready to use.

Note: In the ITSO testing environment, all changes became active *without* restarting the Domino server or the HTTP task. As a general rule, however, it may be necessary to at least stop and re-start the HTTP task for changes to take effect and be visible through a browser. In other cases, it may be necessary to completely restart the Domino server.

The DWALoginForm can be enhanced in any way the Domino Designer supports modifying Domino forms. Be aware that you should leave the *fields* of the form untouched. Otherwise the login may not function correctly.

To use the Domino Web Access Redirect:

1. Launch the browser.
2. Enter the URL of the Domino Web Access Redirect server. (In our case, `http://itsoul10.cam.itso.ibm.com`).

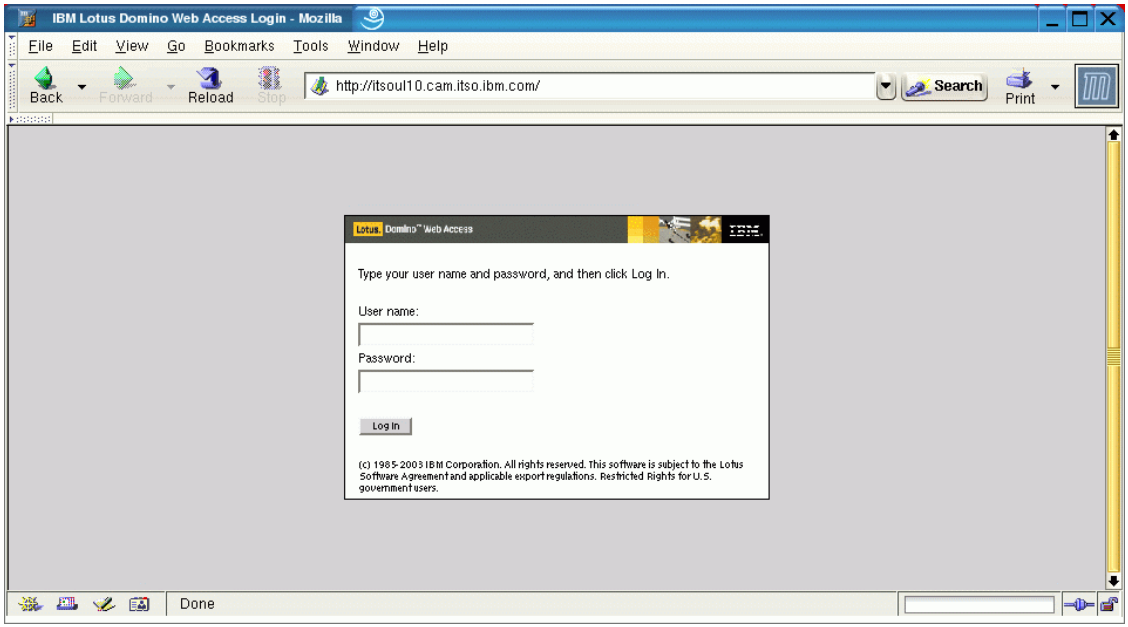


Figure 11-29 Login form in Mozilla browser

3. When prompted, enter your user name and password. Select **Log in**, and the redirection screen is displayed as you are redirected to another server. Note that the debug statements are visible within the form while the debug parameter is switched on (Figure 11-30 on page 381).

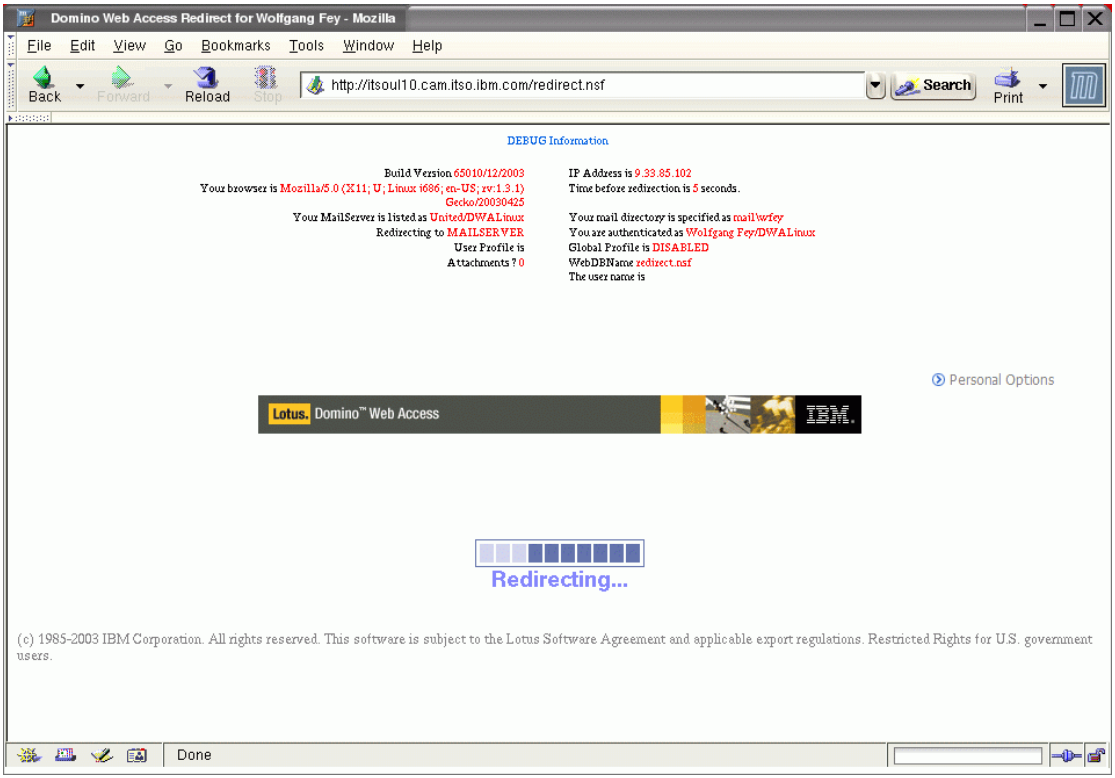


Figure 11-30 Default redirection window

Figure 11-31 on page 382 shows another example with a *customized* redirection form for the ITSO Redbook test environment.

Note: We have illustrated an example of a customized redirect form, but the login form also can be customized. A Notes developer with the proper skills can modify the content of the current DWA login form in the redirection database or directly code his own form. This is not new to Version 6.5, as it has been possible since Version 5 of Notes / Domino.

Figure 11-31 Customized redirection form

11.6 Customizing the server side

This section describes configuration settings that enable you to redirect a user upon logging out of the system.

11.6.1 Redirecting users to a Web page after logout

Use the NOTES.INI variable, iNotes_WA_LogoutRedirect, to specify a URL to redirect users to after logging out from server. The setting provides normal cache clearing with the Domino Web Access control and clearing of browser credentials. This variable enables sites with additional required actions on a logout (such as logging out of a reverse proxy server) to specify a URL to do this additional activity.

You can also use this variable to return people to an initial login page or corporate portal page. For example:

```
iNotes_WA_LogoutRedirect=http://www.ibm.com
```

11.6.2 NOTES.INI settings for Domino Web Access

This section lists some of the specific notes.ini settings for Domino Web Access:

- iNotes_wa_GZIP_Disable

  Use this setting to turn compression on and off. The default is 0 (on). For example, to turn off compression:

  ```
  iNotes_wa_GZIP_Disable=1
  ```

- iNotes_wa_GZIP_Content_Types_Included

  Use this setting to define which types of content you want to compress. The default is:

  ```
  "text/*;application/*"
  ```

  For example, to compress all text:

  ```
  iNotes_wa_GZIP_Content_Types_Included="text/*"
  ```

- iNotes_wa_GZIP_Content_Types_Excluded

  Use this setting to define which types of content you do not want compress. The default is:

  ```
  "image/*;application/pdf"
  ```

  For example, to exclude XML data so that it will not be compressed:

  ```
  iNotes_wa_GZIP_Content_Types_Excluded="image/*;text/xml"
  ```

  Note: You can also disable GZIP compression using the Compress HTTP response data setting on the Domino Web Access tab of the Configuration Settings document.

Additionally, the article “Variables That Affect iNotes Web Access,” which is referenced on the Lotus Developer Domain, is very helpful for better understanding of notes.ini parameters that affect Domino Web Access. Find the article at:

http://www-10.lotus.com/ldd/today.nsf/62f62847467a8f78052568a80055b380/5036a5bc34265e6b85256be6001dc5fa?OpenDocument

Part 5

Appendixes

A

WebSphere Portal 5 installation on Linux

This appendix describes an overview of the installation of the IBM WebSphere Portal 5.0 on Linux. We included this appendix in order to provide you with an end-to-end Linux solution that includes Domino, WebSphere Portal, and the end user client.

Because the primary focus of this book is really Domino Web Access, this is not intended to provide exhaustive details about WebSphere Portal installation and configuration. You may wish to refer to the redbook *IBM WebSphere Portal for Multiplatforms V5 Handbook,* SG24-6098, which is available from the IBM Redbooks site at:

http://www.redbooks.ibm.com

LDAP directory considerations

This chapter covers the integration of IBM WebSphere Application Server and IBM WebSphere Portal Server with an LDAP directory based on IBM Lotus Domino.

We recommend that you use Domino as the LDAP server if no existing directory is already in place or if you intend to make use of Lotus Collaborative Components. If there is already a non-Domino directory server in place, you may want to use the Domino Directory Assistance feature to incorporate the existing directory with Domino. If you intend to use Domino as the LDAP server for WebSphere Portal, you should configure Domino Directory in Domino Administrator or the Notes client before you install WebSphere Portal.

Configure WebSphere Application Server and WebSphere Portal Server for LDAP usage

This is an overview of steps to plan for, install, and configure WebSphere Portal Server with LDAP. This example uses the Domino directory and the Domino LDAP server (Version 5.012 or later for 5.x).

Planning considerations for LDAP use with WebSphere Portal Server

A WebSphere Portal Server can be configured to use an LDAP directory to store user information and to authenticate users. This section discusses the issues to consider when you use an LDAP directory with WebSphere Portal.

Use the questions below to help plan your LDAP implementation:

- Will you install a new LDAP server or use an existing LDAP server? Verify that the server is supported by WebSphere Portal. Refer to Supported hardware and software for information about supported LDAP servers.
- Where will the LDAP directory be installed? You can install the LDAP server on the same machine as WebSphere Portal or on a remote machine. Installing the LDAP server on a remote machine can improve performance.
- Do you want to secure the data flowing between the LDAP server, WebSphere Portal, and WebSphere Application Server? If so, set up LDAP over SSL.
- Will you use WebSphere Portal collaboration features? If so, you may want to use Domino Directory for your LDAP server.

Install WebSphere Portal Server

This section is intended as a high-level guide to help you through the installation of IBM WebSphere Portal Server V5.0 on Linux.

Before installation

First, make sure that you have all CDs ready for installation or have the CDs copied to a filesystem that you can access.

Restriction: The use of mixed CDs from the Experience, Enable, or Extended versions of IBM WebSphere Portal Server is not supported and does not work. If you accidentally mix CDs from different versions, there are no error messages during the install program telling you that the CD set is not consistent. If you see a `No suitable JVM found` error, recheck all CDs.

Step 1: Mount the setup CD and start the install.sh

To begin the installation, mount the first CD from the CD set (cdsetup). From that CD, install.sh must be launched in a shell. This shell script checks the UNIX environment for needed components for the installation process. It also checks for a suitable JVM to start the InstallShield wizard for the GUI-based installation of IBM WebSphere Portal Server. After the required components for installation are verified, this wizard launches to begin the installation.

Note: This step does not check all prerequisites for the WebSphere Portal 5 product itself, but only for the installation process.

Step 2: Select installation language

After launching the wizard, a dialog box appears to select the install wizard language.

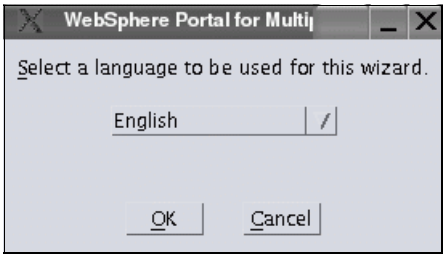


Figure A-1 Install wizard language selection

The next window (Figure A-2) shows a Launch InfoCenter link. The InfoCenter contains the whole product documentation about IBM WebSphere Portal Server and IBM WebSphere Application Server.

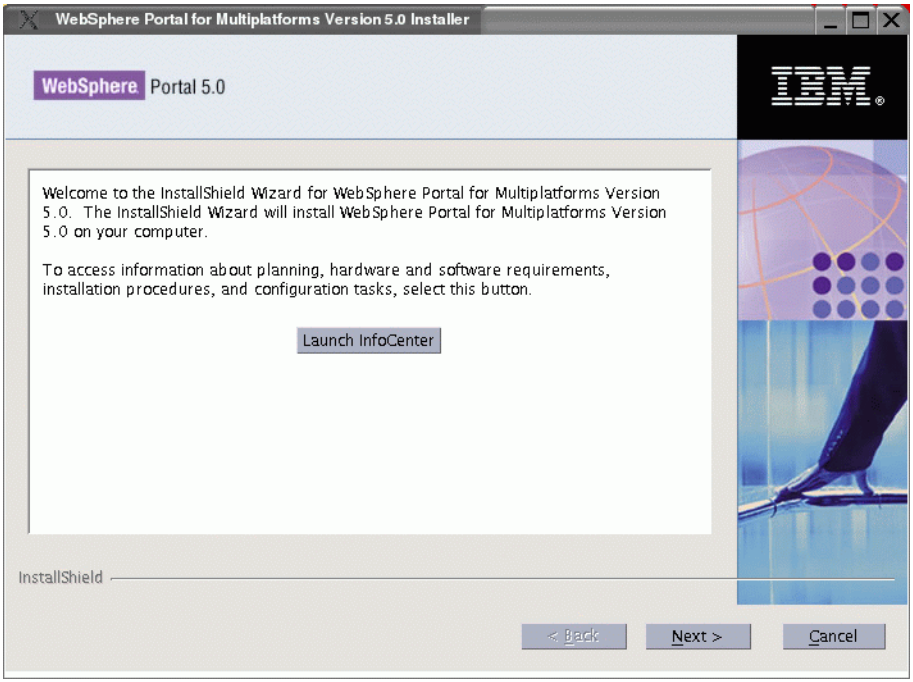


Figure A-2 Welcome to the install wizard

In the InfoCenter, you can review all documented prerequisites and dependencies, as well as the steps for installing all of the components of the two products. Every WebSphere component has its own InfoCenter. The InfoCenter is not installed on the local machine during the regular installation of the products, but it can be launched from the first CD (cdsetup) or from the Web.

The link to the IBM WebSphere Application Server InfoCenter is:

`http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp`

The link to the IBM WebSphere Portal Server InfoCenter is:

`http://publib.boulder.ibm.com/pvc/wp/500/ent/en/InfoCenter/index.html`

Step 3: Accept the license agreement

The next window (Figure A-3) shows the Software License Agreement. The installation cannot continue if this is not accepted.

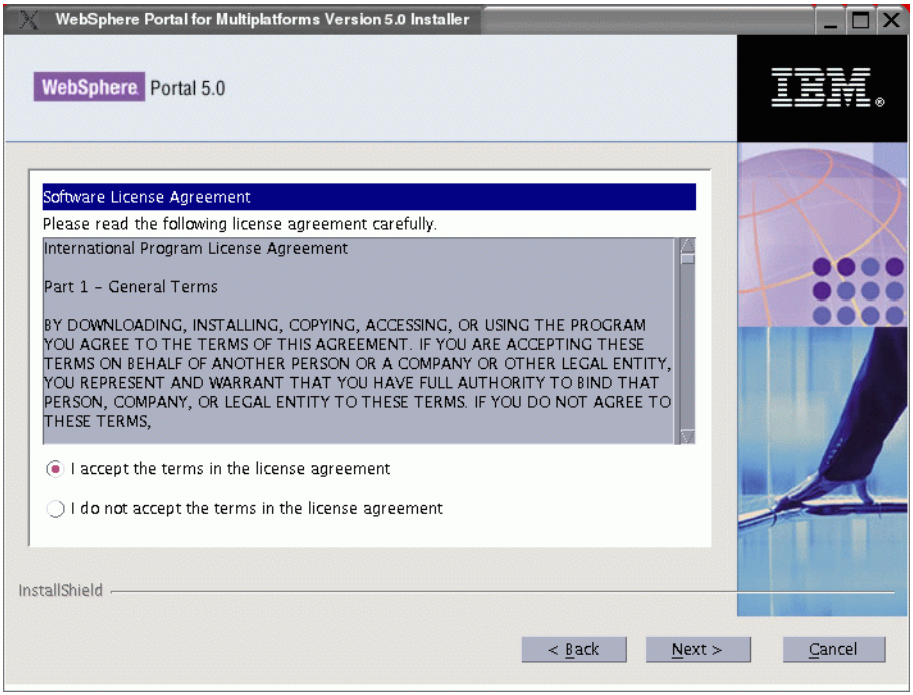


Figure A-3 Software license agreement

Step 4: Checking the prerequisites

The next window shows the Checking for prerequisites screen. In this step the installation program checks filesystem space as well as components.

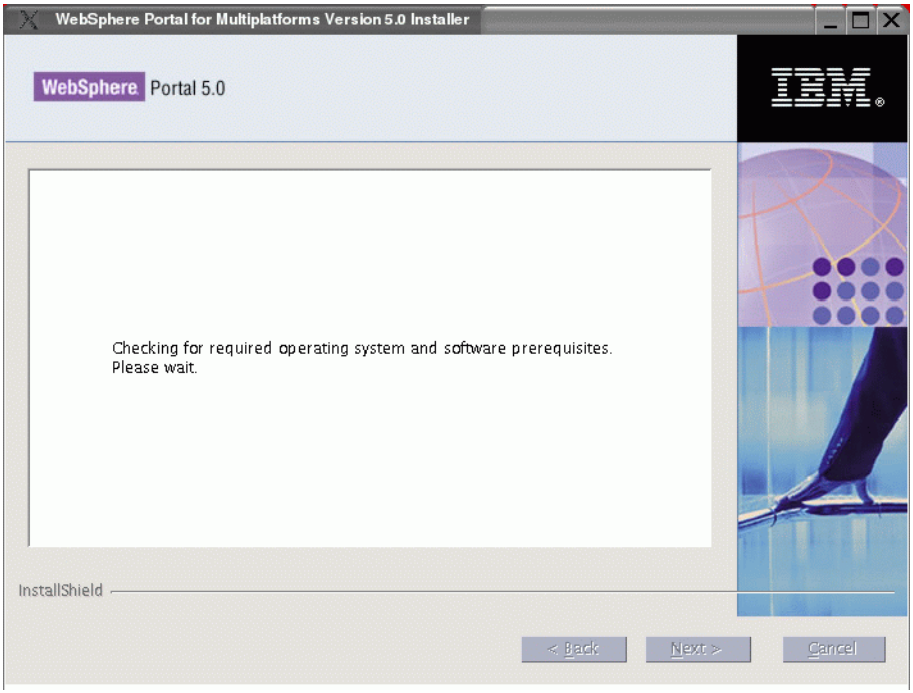


Figure A-4 Checking for prerequisites

Step 5: Choose the installation path

In this step the installation path is chosen. There are two separate ways:

- Full installation
- Custom installation

In our example we have chosen the **Custom** path.

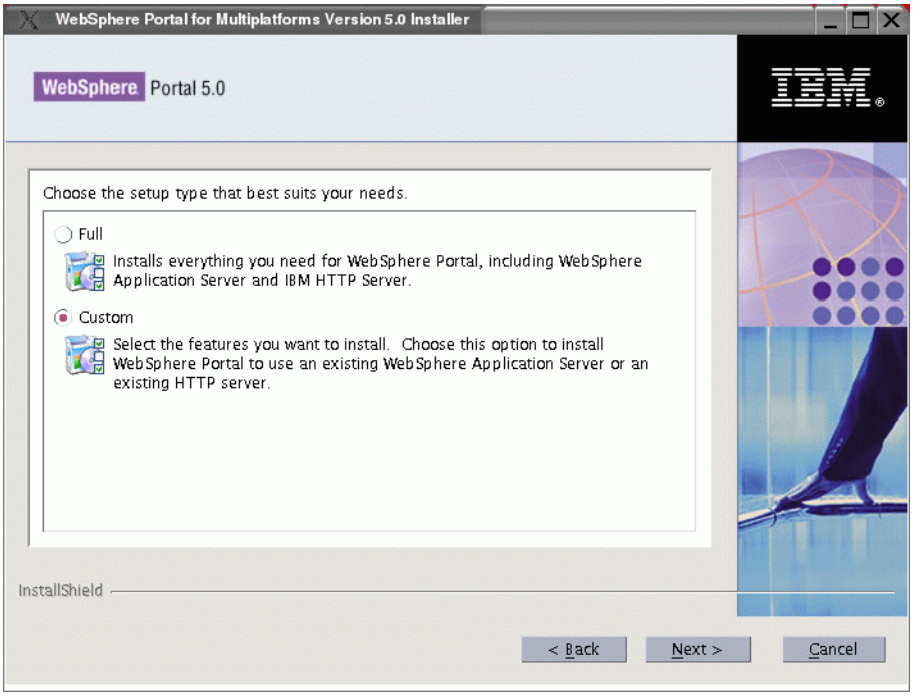


Figure A-5 Selection of installation path

Step 6: Installation options

In this step, specify whether to install a new WebSphere Application Server on the same machine, to use one already installed, or to deploy the Portal on one that runs on a remote system. In Figure A-6, a new IBM WebSphere Application Server is installed on the system to run the IBM WebSphere Portal Server.

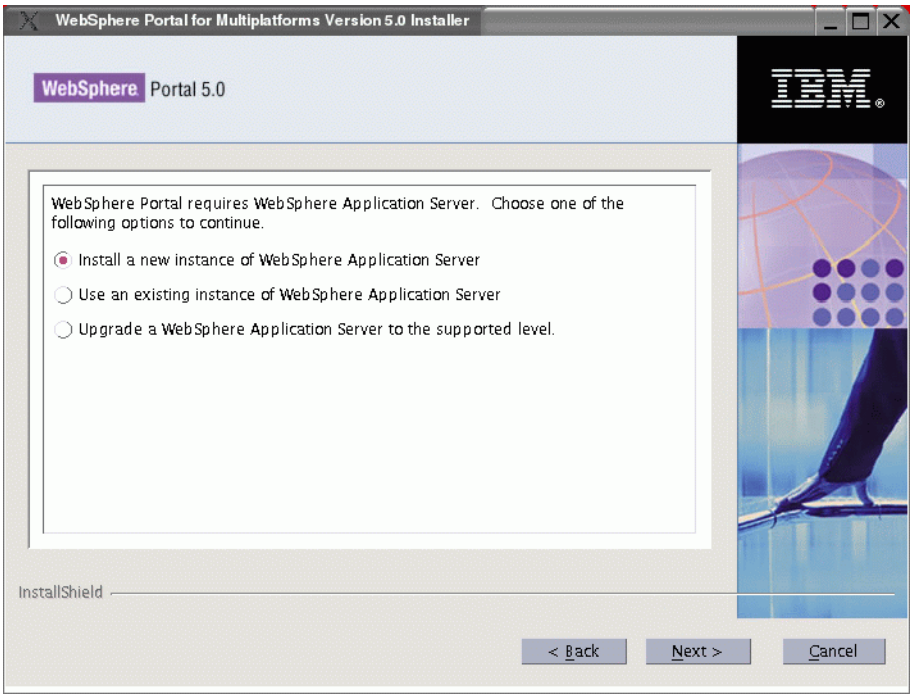


Figure A-6 Installation options for WebSphere Application Server

Step 7: Installation path for WebSphere Application Server

In this step, the installation path for the WebSphere Application Server can be changed. We strongly recommended that you do not change the default installation path.

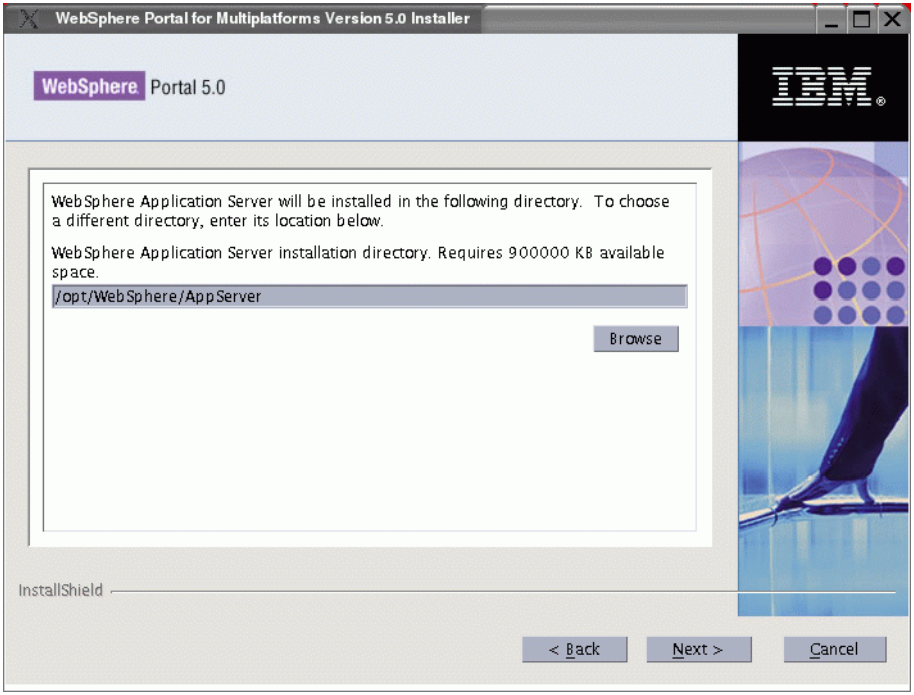


Figure A-7 Installation path

Step 8: Optional installation of the IBM HTTP Server

In this step, you are asked whether to install the IBM HTTP Server product on the same machine, or to install the plug-in for any supported existing HTTP server on the system. In Figure A-8, the IBM HTTP Server will be installed on the system.

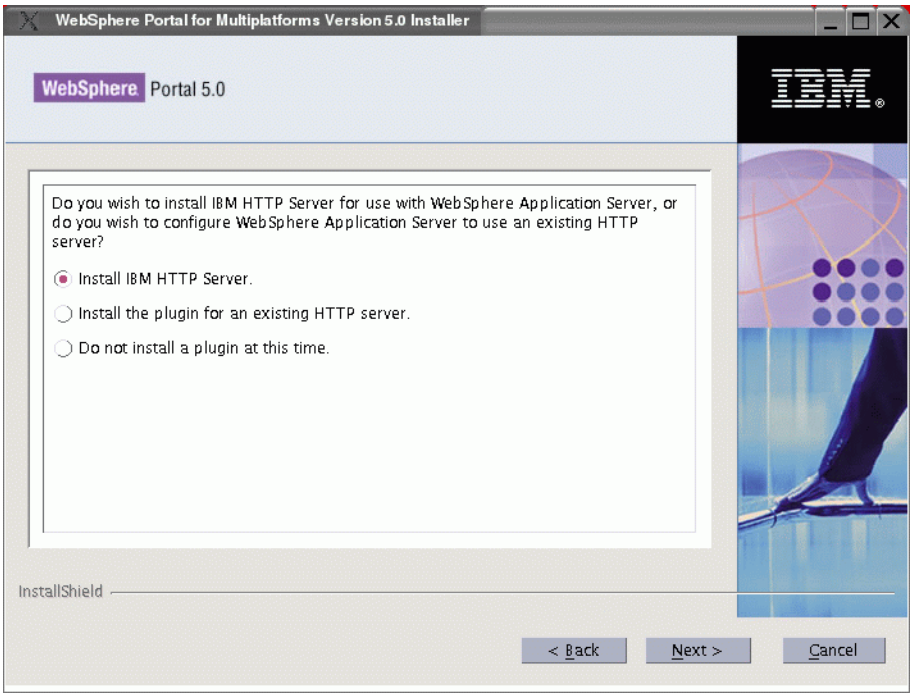


Figure A-8 Installation option of IBM HTTP Server

Step 9: Installation path for the IBM HTTP Server

This dialog provides the installation path for the IBM HTTP Server product. We recommend that you install it into the default path.

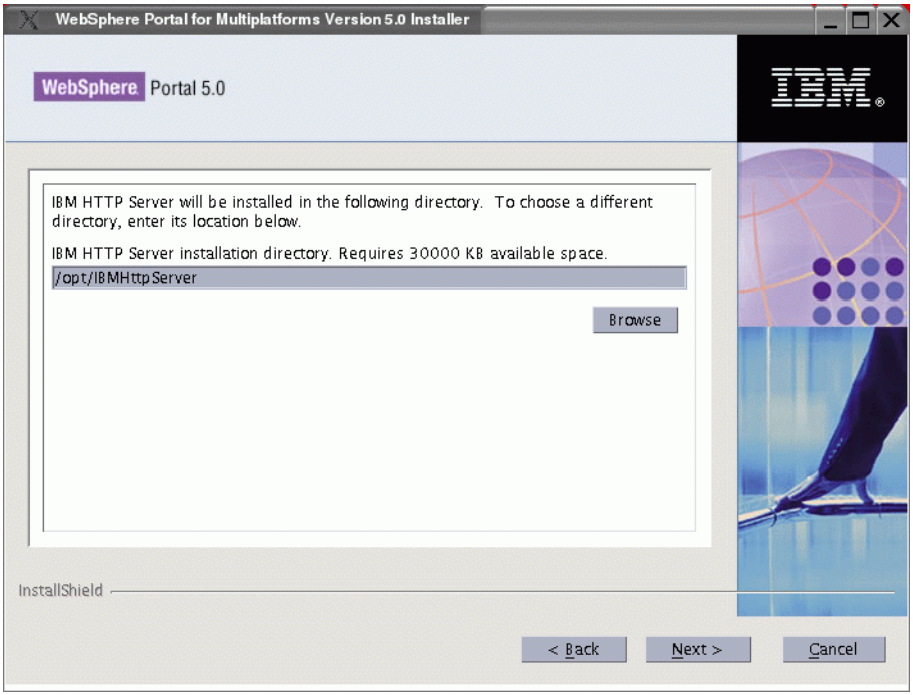


Figure A-9 Installation path for IBM HTTP Server

Step 10: Nodename and host name

The newly installed WebSphere Application server needs an unique node name and also an unique fully qualified host name. *This is a very important step in the installation*. Make sure that the selected host name is fully qualified and that the TCP/IP setup reflects the host name and the domain you enter. To test the proper TCP/IP setup, open a new shell and try to **`ping`** the host name and the fully qualified host name. If both work, go ahead with the installation.

Important: If TCP/IP is not setup properly or name resolution is not working, pause the installation at this step and set up TCP/IP correctly. Otherwise, the installation will definitely fail.

Figure A-10 Node name and application server host name

Step 11: Installation path for WebSphere Portal

This step provides the selection of the installation path for WebSphere Portal. Again, we recommend that you keep the default value.

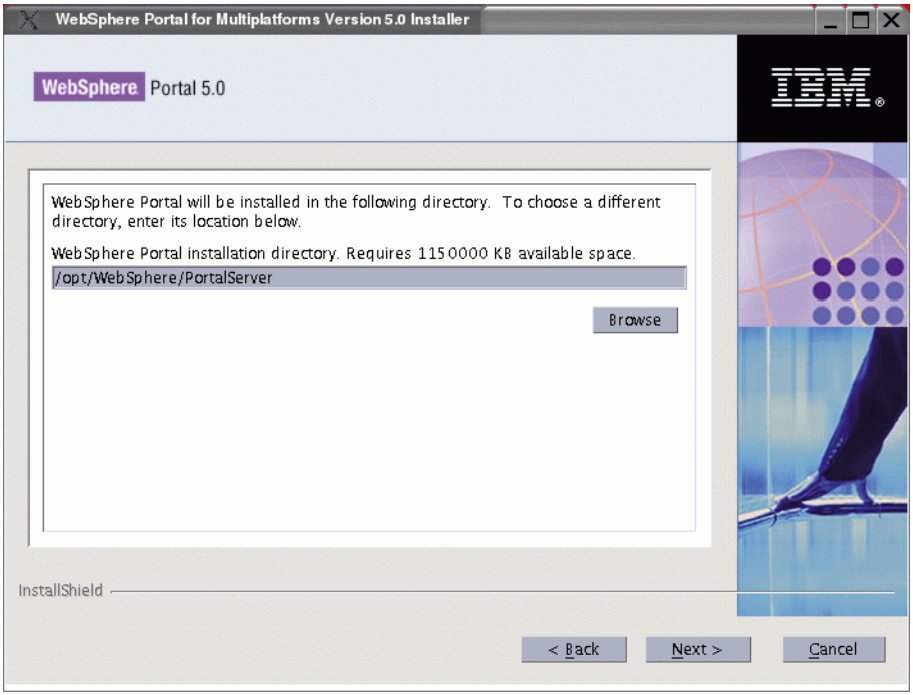


Figure A-11 Installation path for IBM WebSphere Portal Server

Step 12: Portal administrator user

In this step, the installation process creates a user ID for the portal administrator. This is neither a Linux user ID nor an LDAP user ID. See “Configuring WebSphere Portal for Domino Directory” on page 424 for creating a Domino LDAP-based user ID for the portal administrator.

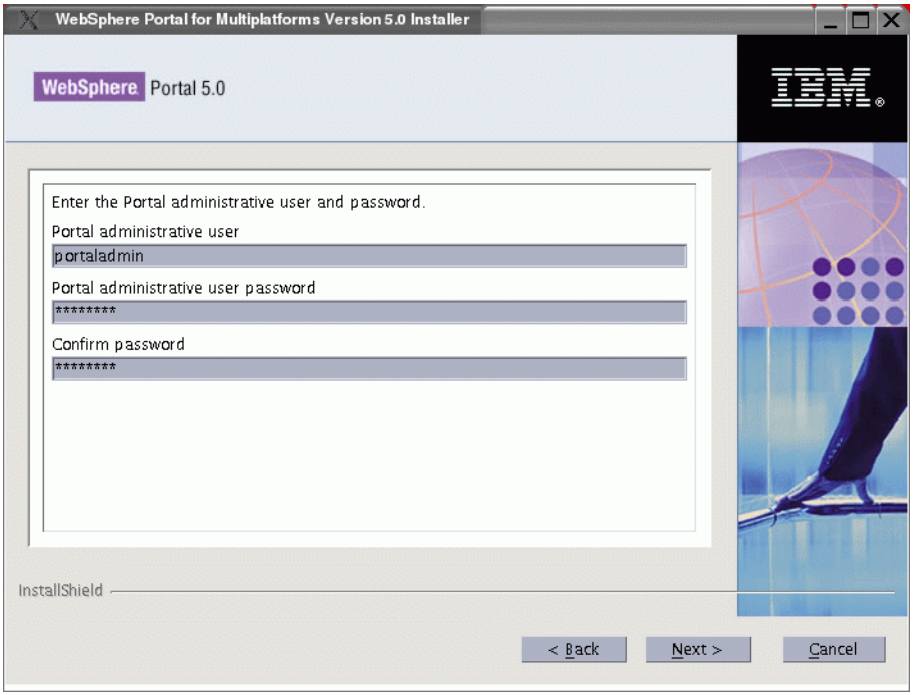


Figure A-12 Portal admin user ID

Step 13: Review installation dialog

This is the last step before the actual installation process begins copying files and writing configurations. This step represents the last chance to review the installation options or to cancel the entire process.

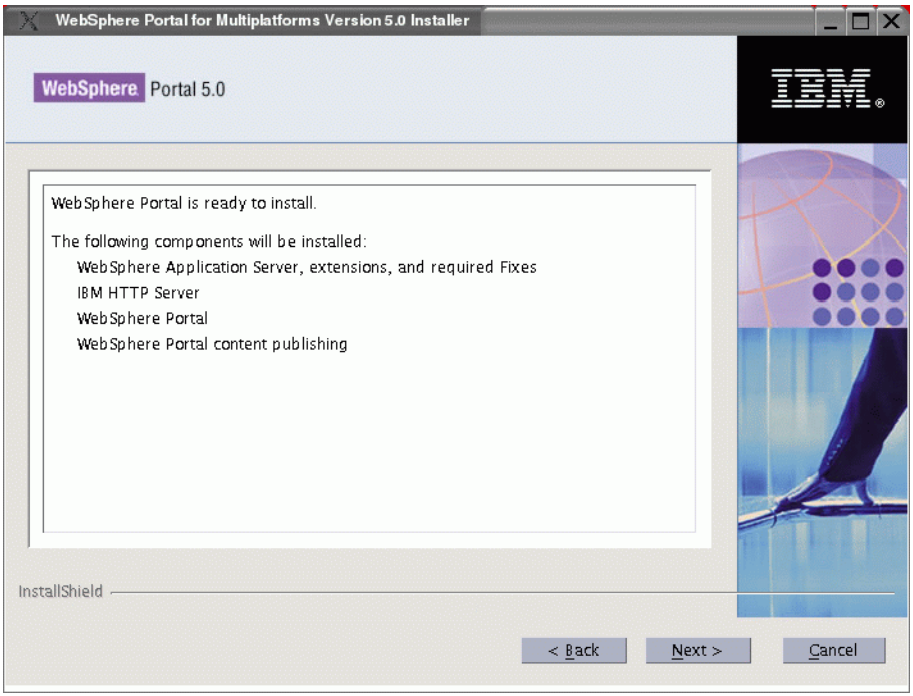


Figure A-13 All options set

Step 14: Installation process running

This is a view-only step with nothing to do except watch the process and note the messages. The process writes a very detailed log to /tmp/wpsinstall.log. The file can be monitored with the **`tail -f`** command from a shell.

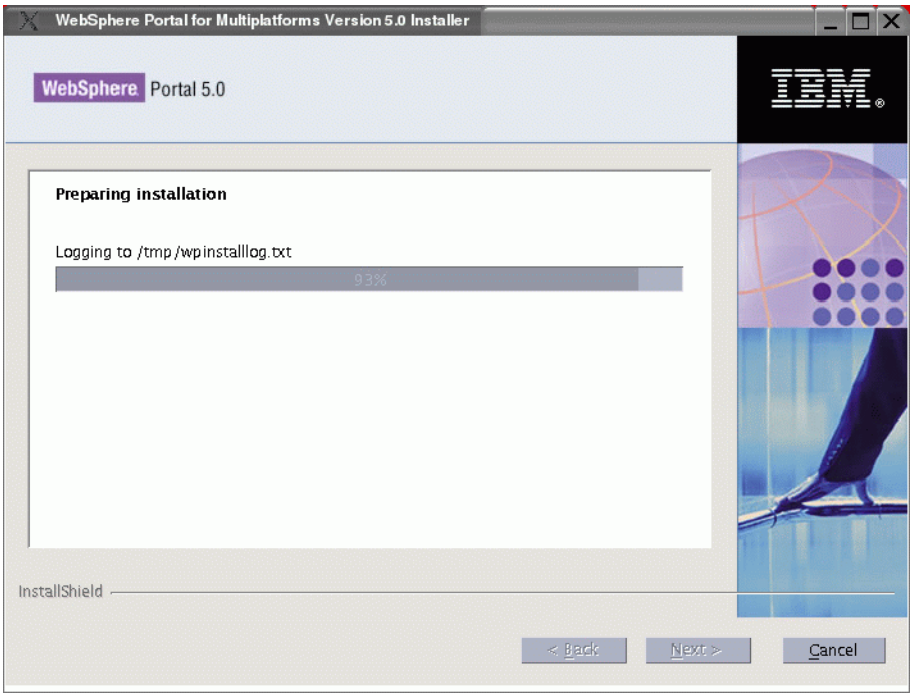


Figure A-14 Preparing installation

The program starts several processes to complete the product installation. From this step on, no further user interaction is necessary until the installation has finished. While installing the components, the installation program creates a lot of log files in the /tmp path. They are moved to the program directories after the installation of each component finishes. If one installation step fails, these log files are a good source to track what happened.

Step 15: Change CDs

If this dialog comes up, then either the proper CD has to be entered into the CD drive or the CD has not been copied correctly to the file system before installation. Insert the right CDs and continue.

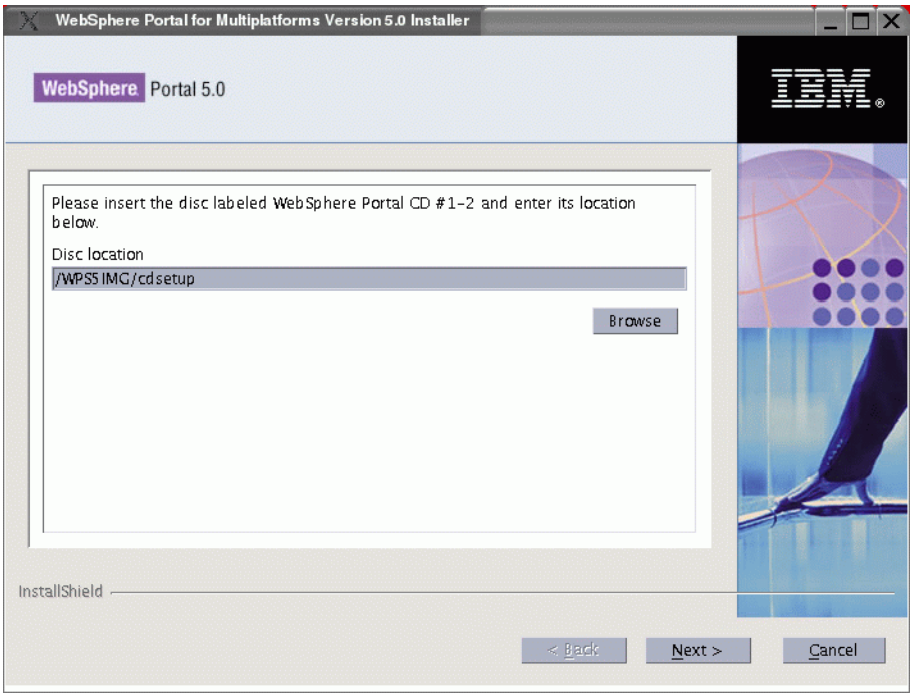


Figure A-15 Change CD dialog

Step 16: WebSphere Application Server install

In this step, the WebSphere Application Server is being installed. Its logfile is written to /tmp/log.txt and can also be monitored with **`tail -f`** from a shell.

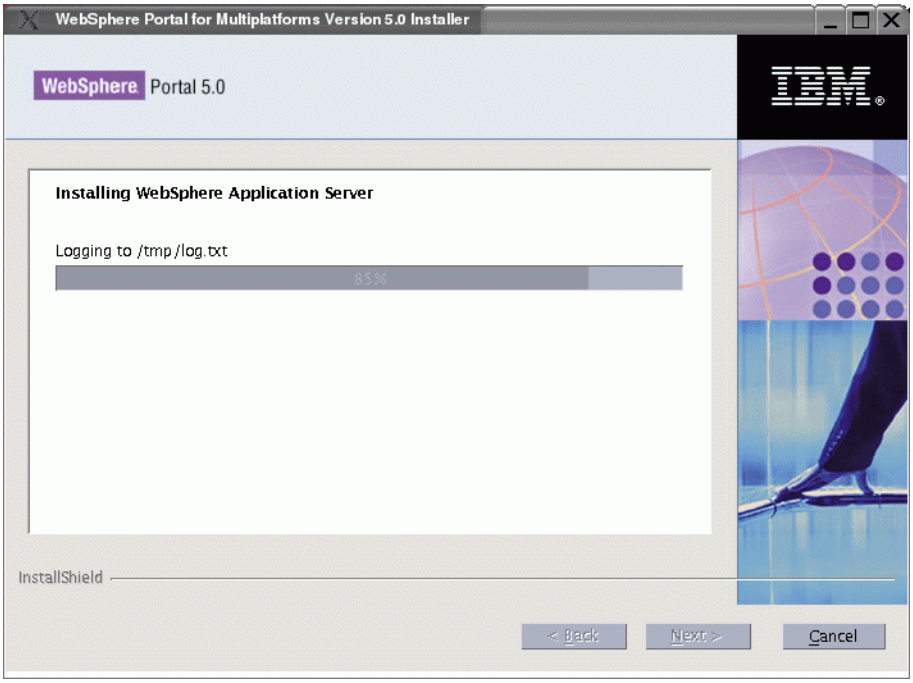


Figure A-16 First component: IBM WebSphere Application Server

Step 17: Installation of the Enterprise Server

This step installs the WebSphere Application Enterprise Server. It writes its logfile to /opt/WebSphere/AppServer/logs/WAS.PME.install.log.

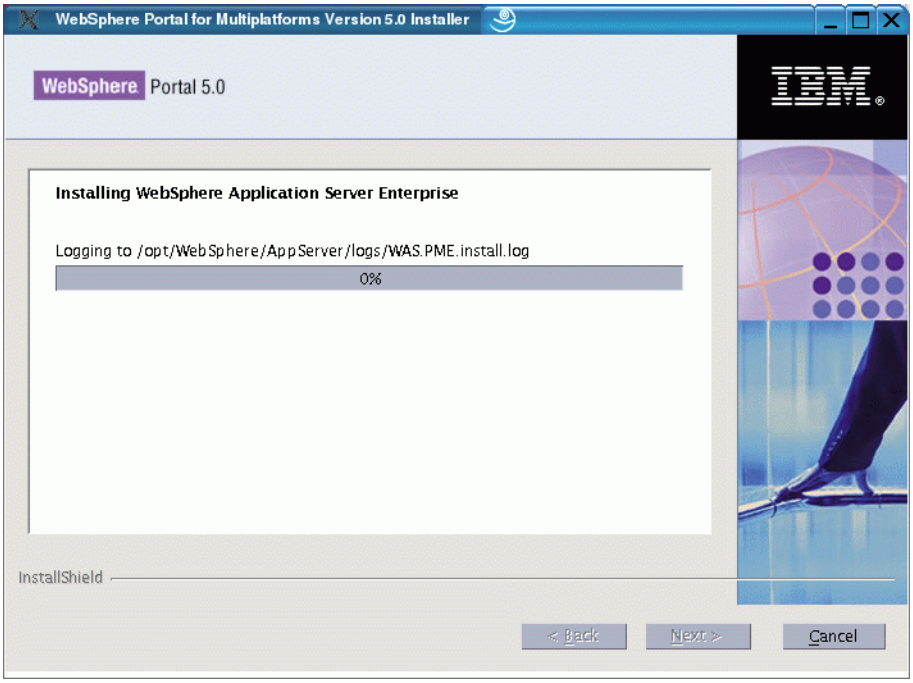


Figure A-17 WebSphere Application Server Enterprise

Step 18: Applying WebSphere Application Server Fix Pack 1

Fix Pack 1 is needed for running the WebSphere Portal Server 5. This step logs to /opt/WebSphere/PortalServer/log/wpwasfp1.txt.

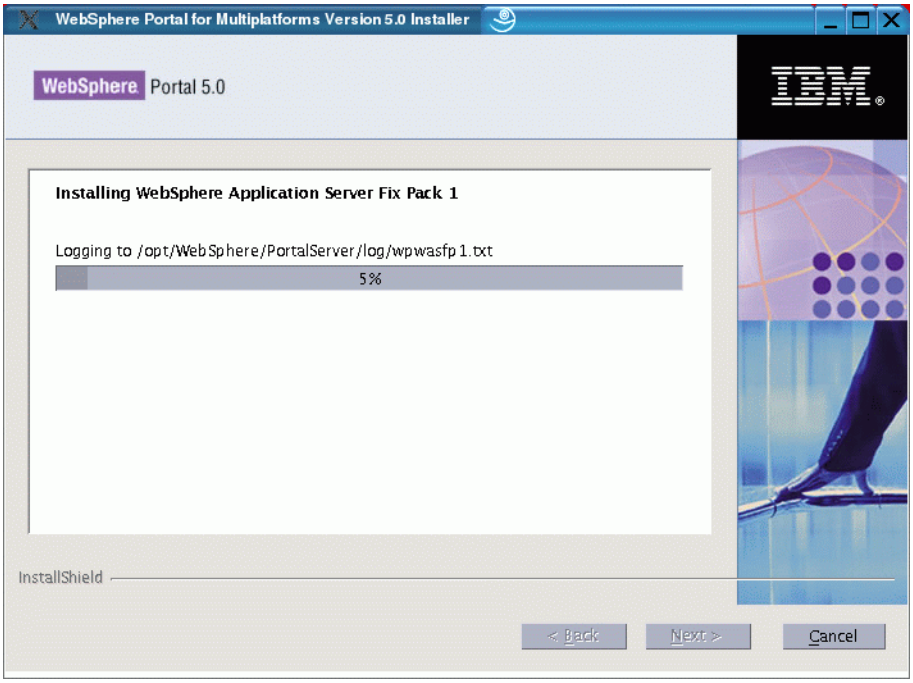


Figure A-18 WebSphere Application Server Fix Pack 1

Step 19: Installing more fixes

This step installs several fixes, not yet packaged in a Fix Pack to the WebSphere Application Server. It logs to /opt/WebSphere/PortalServer/log/wpinstalllog.txt.

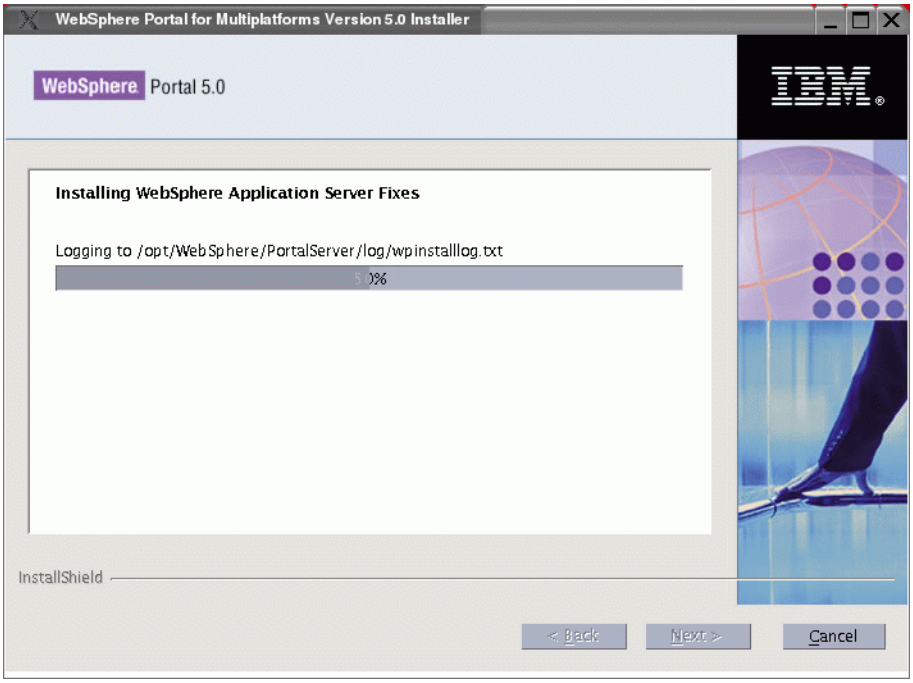


Figure A-19 More fixes to be installed on WebSphere Application Server

Step 20: First server start

The newly installed WebSphere Application Server is now started for the first time. This can take several minutes.

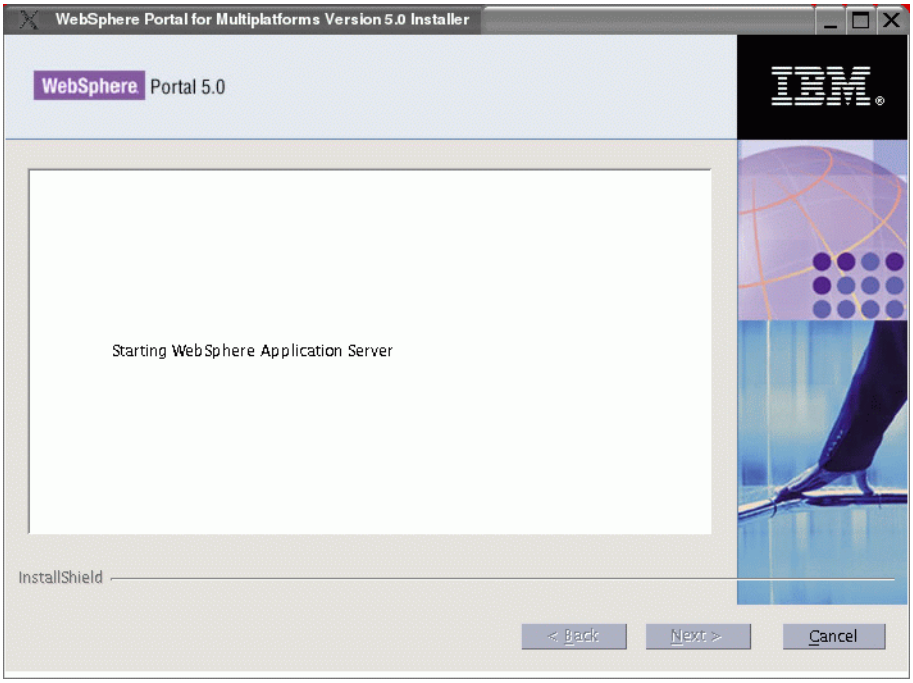


Figure A-20 First server start

Step 21: Installation of WebSphere Portal

Now the portal component is being installed. It logs to /tmp/wpsinstalllog.txt.

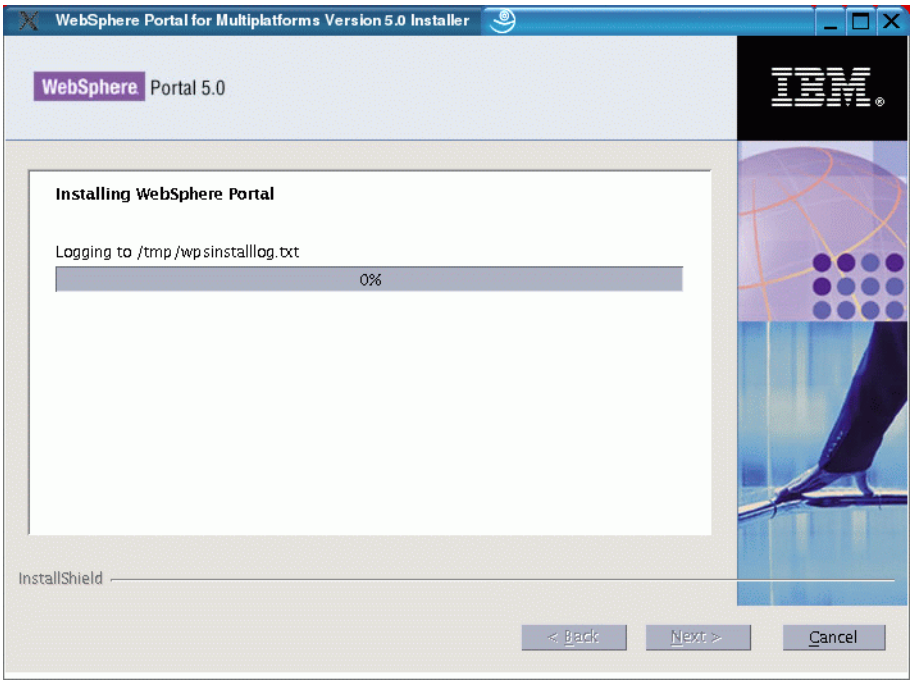


Figure A-21 Installation of IBM WebSphere Portal

Important: The log files and their respective locations in the file system are provided throughout the various steps. Take note of these as they may be very helpful in your troubleshooting efforts.

Step 22: Test the running WebSphere Application Server

To test the installation of IBM WebSphere Application Server, try to connect to http://<nodename>:9080/snoop. Figure A-22 shows the desired output.

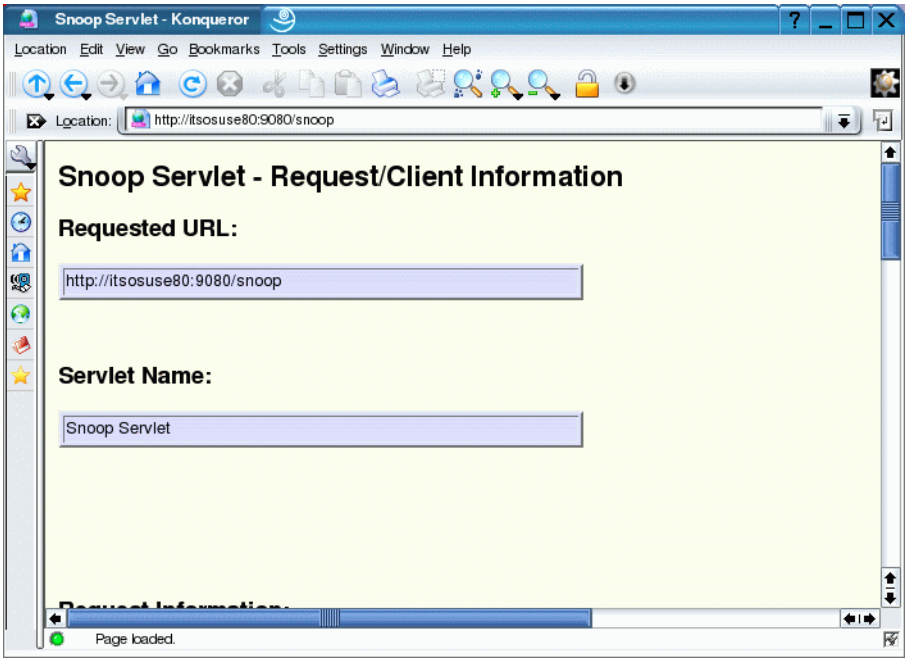


Figure A-22 IBM WebSphere Application Server up and running

Step 23: Installation of the InfoCenter

Now the InfoCenter is installed on the system. There is also an online version of the InfoCenter, which is always on the newest release.

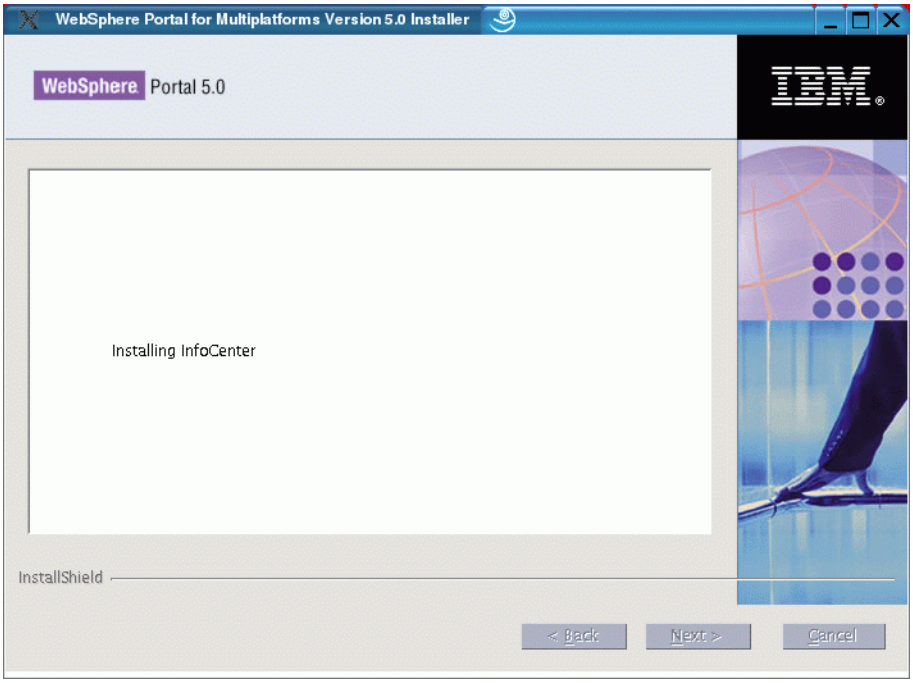


Figure A-23 InfoCenter installation

Step 24: First portal start

In this step, the portal is being started for the first time. Several parameters are set and the configuration is written.

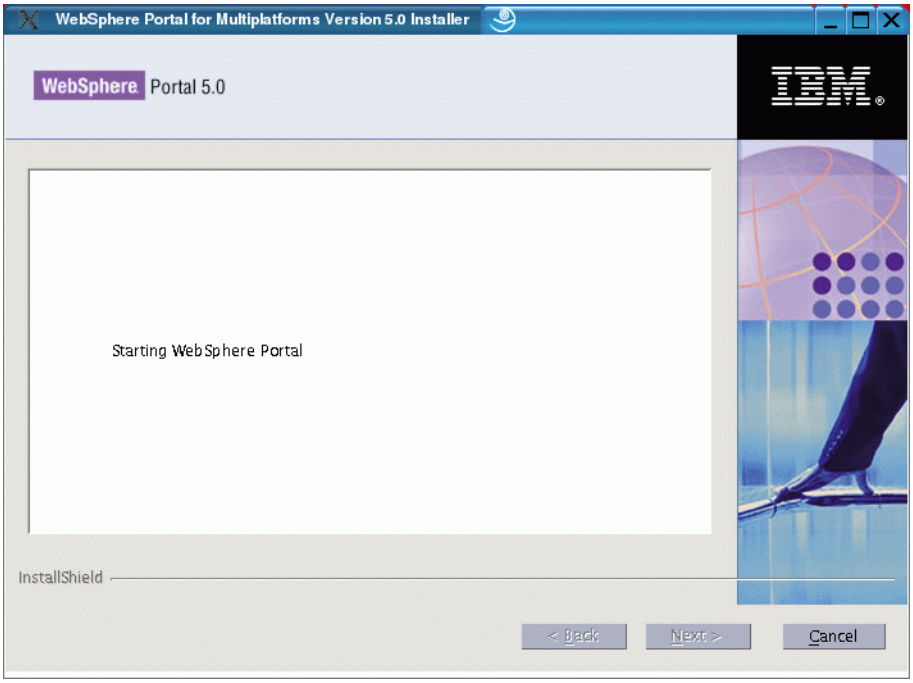


Figure A-24 First WebSphere Portal start

Step 25: Validation of portal installation

The portal installation is validated in this step to confirm that all earlier steps completed successfully.

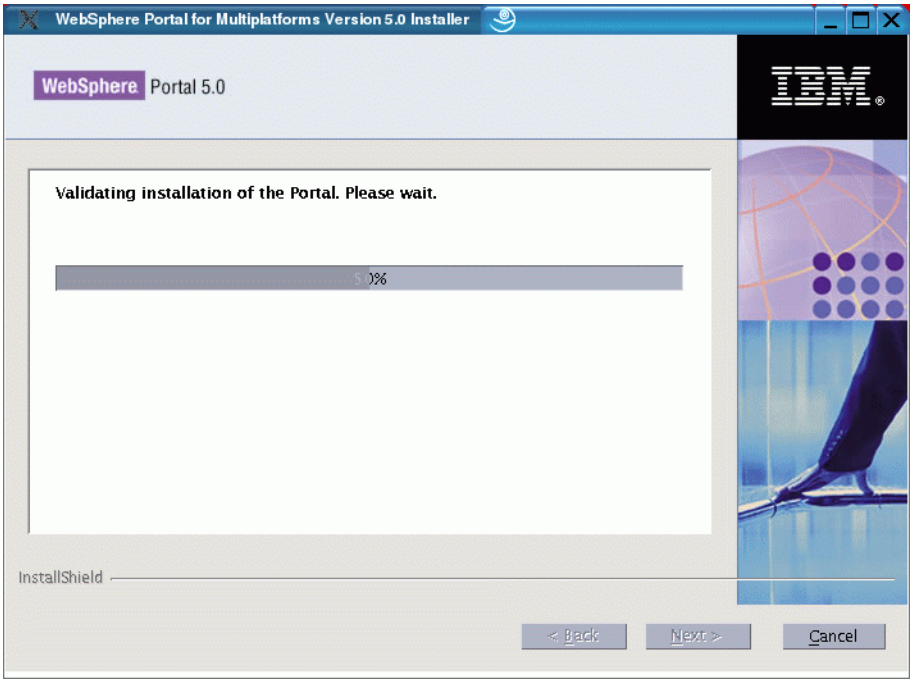


Figure A-25 Validation of portal installation

Step 26: Portlet deployment

After the verification of the portal installation completes successfully, the portlets will be installed. Because of the large quantity of portlets that come with the product CD set, this process can take a long time.

Attention: This installation step may show the 10% completion mark, as in Figure A-26, throughout 90% of the installation time for this step, so be patient.

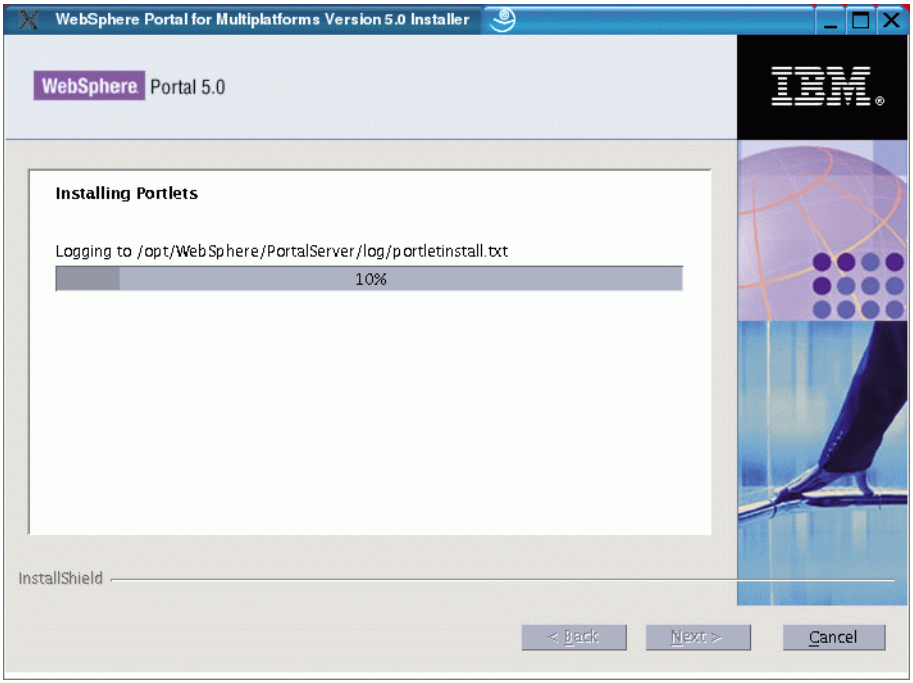


Figure A-26 Portlet installation

Step 27: Installation of WebSphere Portal content publishing

After the portlet deployment, the WebSphere Portal remains started and the last component is being installed. This step logs to /tmp/wpcpinstall.log.

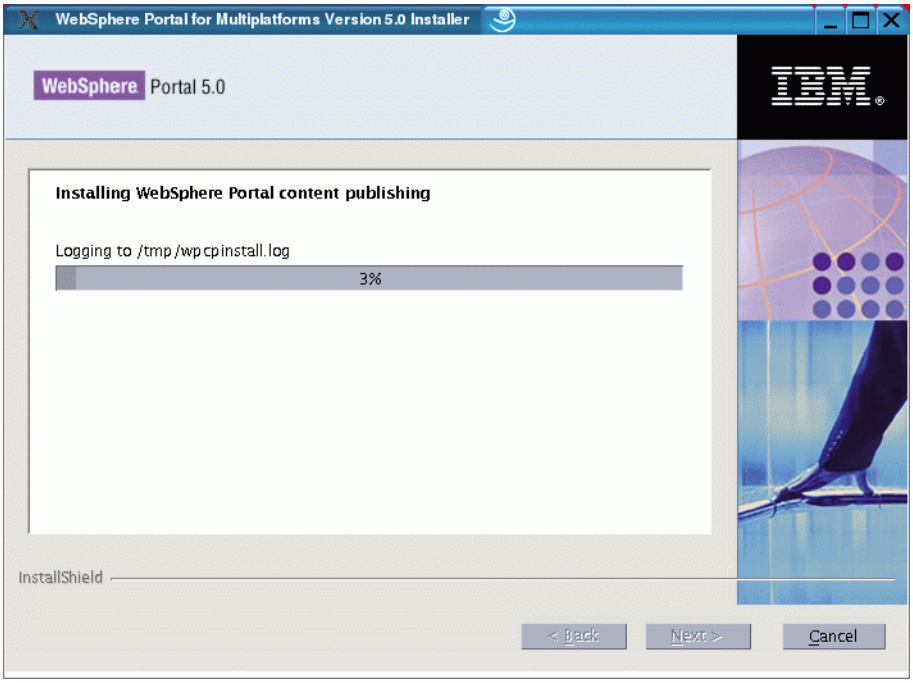


Figure A-27 Installing portlet content publishing

Step 28: Installation finished

When you see the window in Figure A-28, WebSphere Portal v.5 has installed successfully and the IBM WebSphere Portal Server is already running.

Note: This represents essentially a staging environment at this point. Security through LDAP and db2 have not been configured, as they have to be in a production environment.

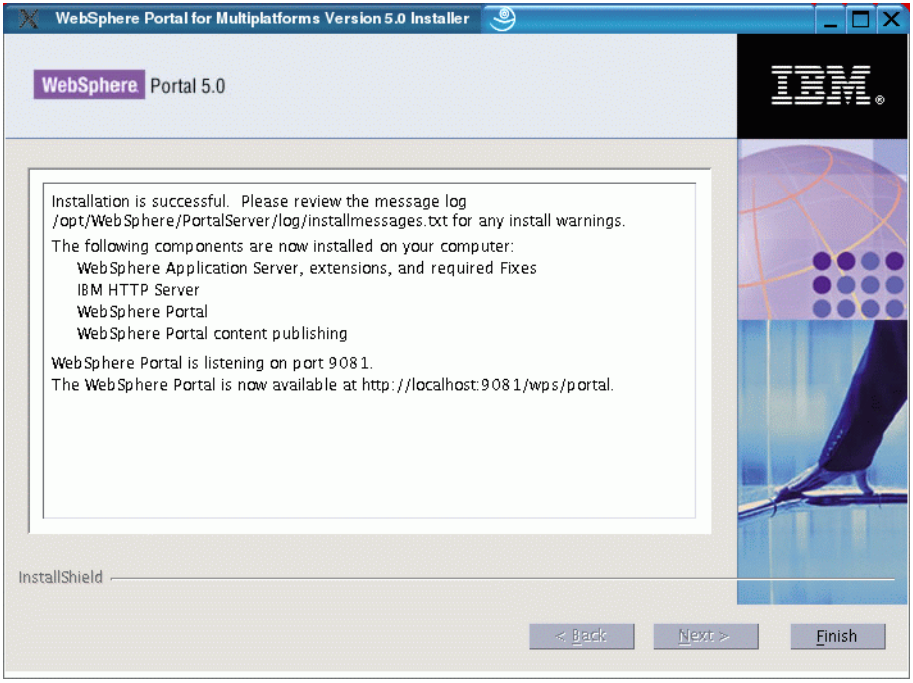


Figure A-28 Installation finished

Start a browser and connect to the Portal at http://<hostname>:9081/wps/portal to see the WebSphere Portal Server default start-up screen (Figure A-29).

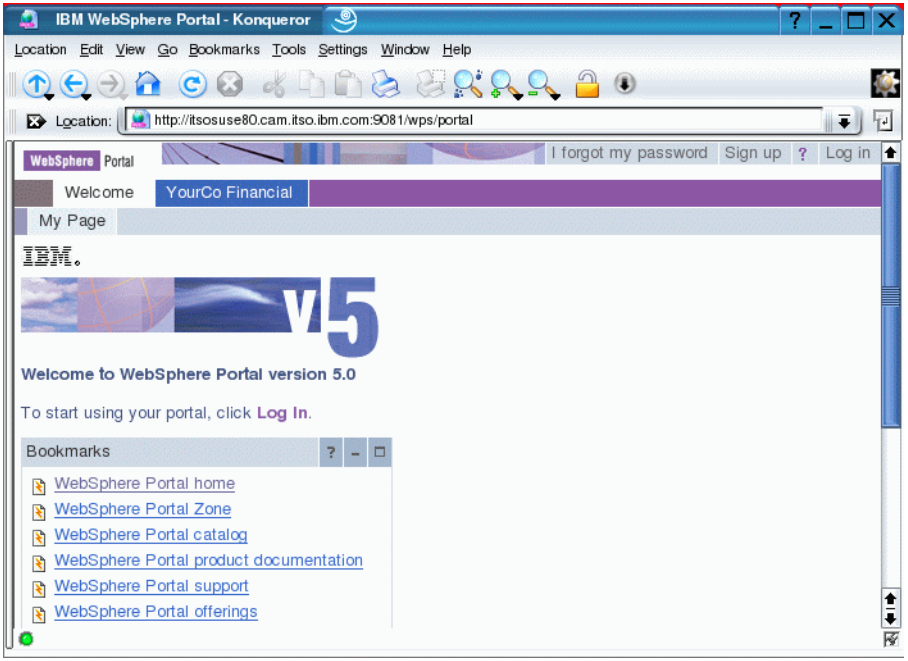


Figure A-29 The new installed and running portal

Step 29: Create desktop icons

The installation process normally fails to install the desktop icons for starting and stopping the IBM WebSphere Application Server and the IBM WebSphere Portal Server, but these can be created easily. Figure A-30 shows the shell scripts and parameters.

Figure A-30 Icons and shell scripts with parameters

To stop just the portal but not the whole Application Server, use this command:

```
/opt/WebSphere/AppServer/bin/stopServer.sh WebSphere_Portal
```

The desktop icons delivered with the product CDs are in *.ico format and are normally not usable for Linux desktop icons. In the ITSO environment they were converted to *.png format, which worked successfully.

Installing LDAP for integration with Domino

The installation of an LDAP server is not part of the default WebSphere Portal installation, so you must install the LDAP server separately. You may install it on the same machine as WebSphere Portal or on another remote machine.

There are several supported LDAP servers for IBM WebSphere Portal Server, but this book covers only the Domino LDAP integration. For the example in this chapter, we used Domino V 5.012. This integration makes the Single Sign-On work between Domino Web Access and IBM WebSphere Portal Server logon requests.

Before you can configure WebSphere Portal to work with the LDAP server, the Domino LDAP directory must have some minimal user and group information already populated. This section describes the procedures necessary to set up the LDAP server to work with WebSphere Portal.

Required groups and users

A minimum of one group and one user is required for WebSphere Portal. Depending on the software you may have deployed and configured already, you may need up to two additional user accounts. These can be existing user accounts that you can use in WebSphere Portal, or you may create new ones.

The required group is wpsadmins or an equivalent. This will be the first administrator group for WebSphere Portal. Members of this group will have administrative authority within WebSphere Portal. It is expected that the first administrator account, WebSphere Portal administrative user ID, will be a member of the group in the directory, but WebSphere Portal does not actually enforce that.

Descriptions of the one *required* and two possibly *needed* user accounts are:

- Required: WebSphere Portal administrative user. This will be the first administrator account for WebSphere Portal. This account should be a member of the wpsadmins group.

- Optional: If you choose to have WebSphere Portal configure IBM WebSphere Application Server security, you must specify a Security Server ID account name and password. This account will be configured into, and will be used to administer, WebSphere Application Server. If this account is different from the following LDAP access accounts, then it needs no special privileges in the LDAP directory.
- Optional: An LDAP access account for WebSphere Application Server and, by extension, WebSphere Portal. This identity will be used by WebSphere Portal to access the LDAP directory. If you keep the default values for the Bind Distinguished Name of WebSphere Application Server in the wpconfig.properties file, wpsbind will be used as the Bind Distinguished Name. The required privileges for this account in the directory are:
  - Write: If you want to allow users or portal administrators to create and modify directory attributes through self-registration and self-care screens or the Manage Users and Groups portlet, the Bind DN (LDAPBindID) user must have permission to read and search the LDAP directory that WebSphere Portal will use or the subtree of that directory rooted at the LDAP suffix.
  - Read: If you will not use any WebSphere Portal facilities to write to the directory, but your directory security policies will not allow anonymous searches of the directory, the Bind DN (LDAPBindID) user must have permission to read and search the LDAP directory that WebSphere Portal will use or the subtree of that directory rooted at the LDAP suffix.

Portal administrator users

You can select an existing LDAP user to act as the portal administrator. If you want to create a new user to administer your portal, you should create the user before continuing.

Note: LDAP Relative Distinguished Name (RDN) prefixes, such as cn=, uid=, or ou=, should be entered in lowercase. Uppercase or mixed-case can cause problems with subsequent case-sensitive queries of the WebSphere Member Management and WebSphere Portal databases.

Example of a Domino Directory server structure

As an example of the Domino Directory server structure, Figure A-31 helps you determine the appropriate values when configuring WebSphere Portal to work with your specific directory layout. The values shown match the default values for this LDAP.

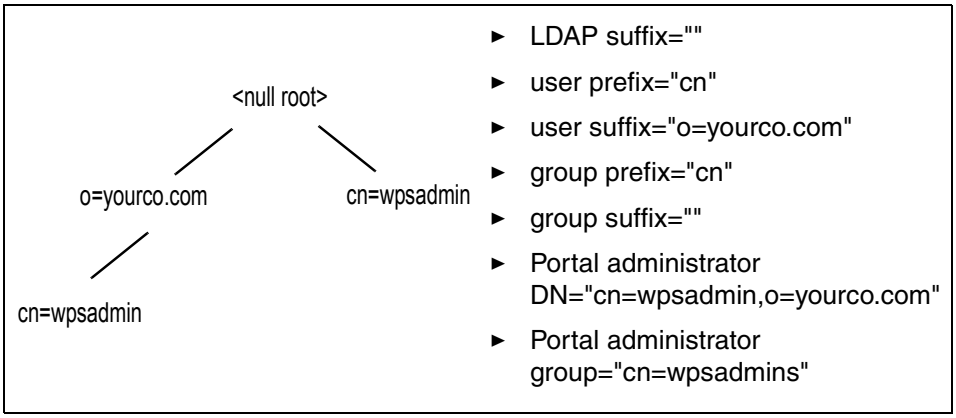


Figure A-31 Example Domino directory structure

Specifying Server configuration settings for LDAP

To specify the configuration settings for Domino Directory, follow these steps:

1. In the Domino Administration or the Notes client, open the server's Domino Directory, names.nsf, and navigate to **Server** → **Configurations**.
2. Open the global configuration Configuration Settings document. If a global configuration document does not exist, click **Add Configuration** to create a new configuration document and display Configuration Settings.
3. On the Basics tab, for the option Use these settings as the default settings for all servers, click **Yes**.

   Note: You must select Yes to cause the LDAP tab to appear for use in the next step.

4. On the LDAP tab, click the **<< >>** button to choose fields that anonymous users can query via LDAP. The LDAP Field List dialog box appears for you to specify the Person and Server fields.
5. From the Form pull-down list, select **Person** and click **Show Fields**.

6. From the Fields in Form, select the following fields to add them to the Person form:
   - MailFile
   - Mail Server
   - SametimeServer
7. From the Form drop-down list, select **Server\Server** and click **Show Fields**.
8. From the Fields in Form, select the following fields to add them to the Server form:
   - HTTP_HostName
   - NetAddresses
9. Click **OK** to close the LDAP Field List dialog box and return to the Configuration Settings document on the LDAP tab.
10. Ensure that Anonymous users can query field shows the following:
    - AltFullName
    - Certificate
    - FirstName
    - FullName
    - HTTP_HostName
    - InternetAddress
    - LastName
    - ListName
    - Location
    - MailAddress
    - MailDomain
    - MailFile
    - MailServer
    - Members
    - NetAddresses
    - PublicKey
    - SametimeServer
    - ShortName
    - userCertificate

11. For the option Allow LDAP users write access, click **Yes**. This setting ensures that portal users can use the self-care and self-registration features of WebSphere Portal.
12. Keep all other default LDAP settings in Configuration Settings.
13. Save and close Configuration Settings.

A.0.1 Adding portal administrators to the Domino Directory

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

1. Navigate to the People view of the Domino Directory and, from the action bar, click **Add Person**.
2. In the New Person form, enter the following values in the fields shown:

Last Name `wpsbind`

User name `wpsbind/<DominoDomain>`
(where DominoDomain is your Domino Domain wpsbind)

`wpsbind`

Short name/UserID `wpsbind`

Internet password `wpsbind`

> **Note:** Make sure that you enter two values in the User name field, where the first value includes the Domino Domain.

   – Save and close the new person record for wpsbind and return to the People view of the Domino Directory.

3. From the action bar, click **Add Person** and complete the New Person form for wpsadmin as follows:

Last name `wpsadmin`, where wpsadmin is the user ID for the portal administrator.

User name `wpsadmin/<DominoDomain>`, where wpsadmin is the user ID for the portal administrator and DominoDomain is your Domino Domain

wpsadmin, where wpsadmin is the user ID for the portal administrator

Short name/UserID wpsadmin, where wpsadmin is the user ID for the portal administrator

Internet password `wpsadmin`, where wpsadmin is the password for the portal administrator

Note: Make sure that you enter two values in the User Name field, where the first value includes the Domino Domain.

4. Save and close the new person record for the new administrative user and return to the People view of the Domino Directory.
5. Navigate to the Groups view of the Domino Directory and, from the action bar, click **Add Group**.
6. In the New Group form, on the Basics tab, enter the following values in the fields shown to create the portal administrators group wpsadmins and add the wpsbind and the portal administrative user. You can add additional users to administer the portal, if desired.

Group name `wpsadmins`

Group type `Multi-purpose`

Members `wpsbind`

`wpsadmin`, where wpsadmin is the user ID for the portal administrator.

7. Save and close the wpsadmins group.

Updating the Access Control List of the Domino Directory

You must ensure that the administrator group, wpsadmins, has the proper permissions and roles in the Domino Directory.

1. In the Domino Administration or in the Lotus Notes client, open the server's Domino Directory (names.nsf), and from the main menu, choose **File** → **Database** → **Access Control** to open names.nsf.
2. In the **Access Control List** → **Basics**, ensure that the portal administrators group wpsadmins has either Author access or Editor access for all roles available.
3. For the wpsadmins group, add and assign the following Role Types:
   - GroupCreator
   - GroupModifier
   - UserCreator
   - UserModifier

4. Click **OK** to save these changes to the Access Control List of the Domino Directory.
5. Select **Exit** in the Domino Administrator or Notes client.

Configuring WebSphere Portal for Domino Directory

Follow the steps below to edit the wpconfig.properties file and run the appropriate configuration tasks so that WebSphere Portal can work with the Domino LDAP server.

Note: These instructions configure WebSphere Portal to work with Domino as an LDAP server only.

A configuration template might exist to support these instructions. Refer to the <wp_root>/config/helpers directory for available configuration templates. Use the configuration template to update the wpconfig.properties file according to the property descriptions and recommended values provided next. If you do not want to use a configuration template, simply follow the instructions as written:

1. Ensure that the LDAP software is installed and that any setup required by WebSphere Portal has been performed.
2. Locate the <wp_root>/config/wpconfig.properties file and create a back-up copy before changing any values.
3. Use a text editor to open the <wp_root>/config/wpconfig.properties file and enter the values appropriate for your environment.
4. Note the following:
   - Do not change any settings other than those specified in these steps. For instructions for working with these files, see “Configuration properties reference” in the Infocenter for a complete properties reference, including default values.
   - Use / instead of \ for all platforms.
   - Some values, shown in *italics* below, may have to be modified to your specific environment.

Table A-1 Values for editing wpconfig.properties file

Section of properties file	Property	Value
Websphere Application Server Properties	WasUserid	Description: The user ID for WebSphere Application Server security authentication. This should be the fully qualified distinguished name. Note: If a value is specified for WasUserid, a value must also be specified for WasPassword. If WasUserid is left blank, WasPassword must also be left blank. Note: For LDAP configuration this value should not contain spaces. Recommended value: *cn=wpsbind,o=yourco.com* Default LDAP value: *uid=wpsbind,cn=users,dc=yourco,dc=com*
	WasPassword	Description: The password for WebSphere Application Server security authentication. Note: If a value is specified for WasPassword, a value must also be specified for WasUserid. If WasPassword is left blank, WasUserid must also be left blank. Recommended value: No recommended value for this property. Default value: <none>
Portal configuration properties	PortalAdminId	Description: The user ID for the WebSphere Portal administrator. This should be the fully qualified distinguished name. Note: For LDAP configuration this value should not contain spaces. Recommended value: *cn=<portaladminid>,o=yourco.com* Default value: <none>
	PortalAdminShort	Description: The short form of the user ID for the WebSphere Portal administrator, as defined in the PortalAdminId property. Recommended value: *<portaladminid>* Default value: <none>
	PortalAdminPwd	Description: The password for the WebSphere Portal administrator, as defined in the PortalAdminId property. Recommended value: No recommended value for this property Default value: <none>
	PortalAdminGroupId	Description: The group ID for the group to which the WebSphere Portal administrator belongs. Recommended value: *cn=wpsadmins* Default value: <none>
	PortalAdminGroupIdShort	Description: The short form of the group ID for the WebSphere Portal administrator, as defined in the PortalAdminGroupId property. Recommended value: *wpsadmins* Default value: <none>

Section of properties file	Property	Value
WebSphere Portal Security LTPA and SSO configuration	LTPAPassword	Description: The password for the LTPA bind. Recommended value: No recommended value for this property. Default value: <none>
	LTPATimeout	Description: Sets the time out for the LTPA bind. Recommended value: 120 Default value: 120
	SSODomainName	Description: Single sign-on domain; for example, SSODomainName=yourcompany.com Recommended value: *SSODomainName* Default value: <none>

Section of properties file	Property	Value
LDAP Properties Configuration	LookAside	Description: The purpose of a Look Aside database is to store attributes which cannot be stored in your LDAP server. You can either install with LDAP only or with LDAP using a Look Aside database. To enable a Look Aside database, set this property to true. If you intend to use a Look Aside database, set this value before configuring security, as it cannot be configured after security is enabled. Note: Using a Look Aside database may slow down performance. Recommended value: false Default value: false
	LDAPHostName	Description: The host information for the LDAP server that WebSphere Portal will use; for example, yourserver.yourcompany.com. Recommended value: *ldapserver_host_name* Default value: *wpsldap.ibm.com*
	LDAPPort	Description: The port number for the LDAP server that WebSphere Portal will use. Recommended value (non-SSL): *389* Recommended value (SSL): *636* Default value: *389; (636 for SSL)*
	LDAPAdminUId	Description: The LDAP administrator id; for example, LDAPAdminUId=cn=root. Recommended value: *LDAP_admin_id* Default value: *cn=root*
	LDAPAdminPwd	Description: The LDAP administrator password. Recommended value: *ldap_admin_password* Default value: <none>
	LDAPServerTyp e	Description: Type of LDAP Server to be used Recommended value: *DOMINO502* Default value: *IBM_DIRECTORY_SERVER*
	LDAPBindID	Description: User ID for LDAP Bind authentication Recommended value: *bind_user* Default value: *uid=wpsbind,cn=users,dc=yourco,dc=com*
	LDAPBindPassw ord	Description: Password for LDAP Bind authentication Recommended value: *bind_password* Default value: <none>

Section of properties file	Property	Value
Advanced LDAP Configuration	LDAPSuffix	Description: LDAP Suffix Recommended value: <none> Default value: *dc=yourco,dc=com*
	LDAPUserPrefix	Description: DN prefix attribute name for user entries. Recommended value: *cn* Default value: *uid*
	LDAPUserSuffix	Description: DN suffix attribute name for user entries. Recommended value: *o=yourco.com* Default value: *cn=users*
	LDAPGroupPrefix	Description: DN prefix attribute name for user entries. Recommended value: *cn* Default value: *cn*
	LDAPGroupSuffix	Description: DN suffix attribute name for group entries. Recommended value: <none> Default value: *cn=groups*
	LDAPUserObjectClass	Description: User object class corresponding to your directory. Recommended value: *inetOrgPerson* Default value: *inetOrgPerson*
	LDAPGroupObjectClass	Description: Group object class corresponding to your directory. Recommended value: *groupOfNames* Default value: *groupOfUniqueNames*
	LDAPGroupMember	Description: Specifies the attribute name of the membership attribute of your group objectclass. Recommended value: *member* Default value: *uniqueMember*
	LDAPsslEnabled	Description: Specifies whether secure socket communications is enabled to the LDAP server. Recommended value (non-SSL): *false* Recommended value (SSL): *true* Default value: *false*

Important: Do not change any other settings in this file. Always use forward slashes (/) instead of back slashes (\) to separate elements in a path, even in a Windows environment.

If WebSphere Application Server is installed as part of the WebSphere Portal installation and it is planned to use WebSphere Application Server Single

Sign-On, ensure that the following properties in the wpconfig.properties file have the values listed below.

Table A-2 Values for editing wpconfig.properties WAS installed as part of Portal

Section of properties file	Property	Value
WebSphere Portal Security LTPA and SSO configuration	SSOEnabled	Description: Specifies that the single signon function is enabled. Recommended value: *true* Default value: *true*
	SSORequiresSSL	Description: Specifies that single signon is enabled only when requests are over HTTPS Secure Sockets Layer (SSL) connections. Choose False unless SSL is already enabled for WebSphere Portal. In most cases, SSL for WebSphere Portal will not yet be in place. After SSL for WebSphere Portal is set up, change this value using the WebSphere Application Server administrative console. Recommended value: *False or True depending on your environment.* Default value: *false*
	SSODomainName	Description: Specifies the domain name for all single signon hosts. Enter the part of the domain that is common to all servers that participate in single signon. For example, if WebSphere Portal has the domain portal.us.ibm.com and another server has the domain another_server.ibm.com, enter ibm.com. See the WebSphere Application Server documentation for further details about this setting. Recommended value: *domain_identifier* Default value: *ibm.com*

Important: It is very important that you use the same LTPA values that are already configured in your environment.

Table A-3 LTPA values for the wpsconfig.properties file

Section of properties file	Property	Value
WebSphere Portal Security LTPA and SSO configuration	LTPAPassword	Description: The password for the LTPA bind. Recommended value: *password* Default value: <none>
	LTPATimeout	Description: The property that sets the time out for the LTPA bind. Recommended value: *<none>* Default value: *120*

5. Save the file.
6. Open a command prompt and change to directory <was_root>/bin. Enter the following commands:
   - `startServer server1`
   - `stopServer WebSphere_Portal`
7. Change to the directory <wp_root>/config. Enter the following command to run the appropriate configuration task for your specific operating system:
   - UNIX: `./WPSconfig.sh validate-ldap`
   - Windows: `WPSconfig.bat validate-ldap`

   Note: If the configuration task fails, validate the values in the wpconfig.properties file.

8. Enter the appropriate command to run the configuration task for your specific operating system:
   - UNIX: `./WPSconfig.sh enable-security-ldap`
   - Windows: `WPSconfig.bat enable-security-ldap`

   Note: Check the output for any error messages before proceeding with any additional tasks. If the configuration task fails, verify the values in the wpconfig.properties file. Before running the task again, be sure to stop the WebSphere Portal application server by entering the following command from the <was_root>/bin directory and specify the WebSphere Application Server user ID and password (as defined by the WasUserid and WasPassword properties):

   ```
   stopServer WebSphere_Portal -user was_admin_userid -password
   was_admin_password
   ```

9. Perform this step only if you are using LDAP over SSL:
   - If not already configured, configure WebSphere Application Server to use LDAP over SSL using the WebSphere Application Server Administrative Console. WebSphere Portal should be stopped before doing this. Consult the WebSphere Application Server documentation to configure the SSL settings dialog. If possible, verify that the settings are correct by restarting the Administrative Console again and confirming that no LDAP traffic is sent to port 389 on the LDAP directory server. All necessary certificate setup should have be done when setting up LDAP over SSL.

- Configure WebSphere Portal to use LDAP over SSL by modifying <wp_root>/shared/app/wmm/wmm.xml:
  - Change the LDAP port from 389 to the port on which your LDAP server is listening for LDAP over SSL traffic. By default, this value is 636. In the <ldapRepository...> stanza of the wmm.xml file, change the port number as desired:

    ```
    ldapPort="636"
    ```
- In the <ldapRepository...> stanza of the wmm.xml file, add the following key/value pairs: `java.naming.security.protocol="ssl"`
- Restart WebSphere Portal.

At this point when using Domino, users cannot log in to WebSphere Portal using a shortname. Users must use a full first and last name to log in. To allow users to log in with a shortname, you must reconfigure a filter in WebSphere Application Server. Use the following steps as a guide to configure a filter.

10. In the WebSphere Application Server console, select **Security User Registries LDAP Advanced LDAP Settings**.
11. Adapt the user filter as follows:
    - Change the user filter from (&(cn=%v)(objectclass=inetOrgPerson)) to `(&(uid=%v)(objectclass=inetOrgPerson))`
    - If inetOrgPerson is not your user object class, replace it with the appropriate value for your environment.
12. Change to directory <was_root>/bin, and enter the following commands:
    - **stopServer server1**
    - **startServer server1**
    - **startServer WebSphere_Portal**
    - If you are running with security enabled on WebSphere Application Server, you must specify a user ID and password for security authentication when entering the commands:
      - st**opServer server1 -user was_admin_userid -password was_admin_password**
      - **startServer server1**
      - **startServer WebSphere_Portal**

13. Perform this step only if you installed WebSphere Portal into a pre-existing SSO environment. Because you will not be given the option to import your existing token file, you must perform the following steps:
    - To import your SSO Token:
        - In the WebSphere Application Server Administrative Console, select **Security Authentication Mechanisms LTPA**.
        - Enter the LTPA token password in the Password field.
        - Enter the password again in the Confirm password field.
        - In the Key File Name field, enter the LTPA token file.
        - Click **Import Keys**.
        - Click **Save**.
        - Click **Save**.
    - To set your SSO Domain:
        - In the WebSphere Application Server Administrative Console, select **Security Authentication Mechanisms LTPA**.
        - Click **Single Signon** in Additional Properties.
        - Enter the domain name in the Domain Name field.
    - Click **OK**.
14. Use http://<hostname.yourco.com>:<port_number>/wps/portal to access WebSphere Portal and verify that you can log in.

Note: Configuring WebSphere Portal to work with an LDAP directory automatically enables WebSphere Application Server Global Security. After security is enabled, you must type the fully qualified host name when accessing WebSphere Portal and the WebSphere Application Server Administrative Console.

Security is enabled

After you have enabled security with your LDAP directory, you must provide the user ID and password required for security authentication on WebSphere Application Server when you perform certain administrative tasks with WebSphere Application Server. For example, to stop the WebSphere Portal application server, you would issue the following command:

```
stopServer WebSphere_Portal -user was_admin_userid -password was_admin_password
```

Verifying LDAP

After setting security with LDAP, use the following steps to verify that your LDAP server for WebSphere Portal has been properly configured:

1. Go to WebSphere Portal and create a new user by clicking **Sign-up** in the upper-right corner.
2. Log on to WebSphere Portal as the user you have just created.

If the logon is successful, your LDAP server should be working correctly.

Note: The content resulting from logon may vary according to user role. If you do not receive an error message, you can assume that the LDAP server is functioning properly.

WebSphere Portal Server hardware requirements for Linux Intel systems

Refer to the following list for hardware requirements for Linux Intel systems:

- Processor: CPU speeds of late model, mid-range to high-end servers are recommended. Pentium 800MHz or equivalent at a minimum. Production environments should consider the Pentium 4 processor at 1.4GHz or higher.
- Physical memory: 1024 MB or more per processor
- Disk space: See Table A-4 for required disk space if you use the installation program to install WebSphere Application Server, extensions, fixes, IBM HTTP Server, and WebSphere Portal.

Note: You can perform a custom installation of the components.

Table A-4 Disk space requirements by component

Component	/opt	/tmp
WebSphere Portal	1124 MB	50 MB
WebSphere Application Server, extensions (includes Embedded Messaging), and fixes	968 MB	245 MB
IBM HTTP Server	30 MB	n/a
Total	2413 MB	295 MB minimum

- Virtual memory/swap space: It is recommended that this be equal to double your physical memory. At minimum this should be at least equal to your physical memory.
- File system size: If for any reason you need to change the file system size, the Linux ext3 file system (which is used by default) does not allow you to change it. Therefore, you should carefully plan in advance for the size of your file system in order to avoid related problems. The following disk space is required for each directory:
  - /: 1.5 GB or more (root directory)
  - /opt: 2.5 GB or more. The default directory to install WebSphere Portal on Linux is /opt, which you could change to any directory you like later. By default, /opt is under / file system in default. If you choose to install WebSphere Portal under /usr, 3.5 GB or more is recommended.
  - /home: 500 MB or more (home directory)
- Network connectivity: To use a portal across a network, the following is required for the portal machine:
  - Network adapter and connection to a physical network that can carry IP packets. For example, Ethernet, Token Ring, ATM, and so on.
  - Static IP address
  - Configured fully qualified host name. The portal system must be able to resolve an IP address from its fully qualified host name. To ensure that this is configured correctly, you can issue the **`ping`** command from a command line. An example command is: **`ping`** `hostname.yourco.com`, where hostname.yourco.com is the fully qualified host name.

B

Configuring Internet Cluster Manager

The following appendix describes how to configure the Internet Cluster Manager (ICM). Much of this information has already been included in *iNotes Web Access: Deployment and Administration*, SG24-6518. The information contained here has been updated to reflect Domino Web Access 6.5.

Internet Cluster Manager

The Internet Cluster Manager (ICM) enables you to use Domino clusters to provide failover and workload balancing to HTTP clients (Internet browsers) when they access Domino Web servers. This makes your iNotes Web Access servers highly available to clients. You can run the ICM on any server that is using the Domino Release 5 Enterprise Server license. Install and configure Domino clusters as you normally would, and then configure the ICM. The ICM supports the HTTP and HTTPS protocols.

The ICM acts as an intermediary between HTTP clients and the Domino Web servers in a cluster. When Domino Web servers are running in a cluster, they generate URLs that direct HTTP client requests to the ICM. The ICM maintains information about the availability of servers and databases in the cluster. When the ICM receives a client request, it redirects the client to the most available server that contains a replica of the requested database.

The ICM sends periodic probes to the Web servers in the cluster to determine their status and availability. When the ICM receives a client request, it looks at the information in the Cluster Database Directory to find a server that contains the requested database. The ICM determines the most available server that contains the requested database, and then redirects the client to that server. This results in the client closing the session with the ICM and opening a new session with the selected server. The user may see this as a change in the host name in the URL. The user may also see the path to the database change in the URL because the database may have a different path on the target server.

Configuring the ICM

Configure the ICM by making entries in the Internet Cluster Manager section of the Server document. You can also set up a separate IP address for the ICM (see “Setting up a separate IP address for the ICM” on page 439). You can then start the ICM.

You can configure the ICM settings on one server and have more than one ICM access these settings. This lets ICMs on different servers share a common configuration. You should include the ICM configuration information on every Web server in the cluster, not just the server on which you run the ICM, because each Web server uses its own Server document to determine how to generate URLs that refer to the ICM. The Web server obtains the host name of the ICM from the Server document. The Web server then uses that host name to generate URLs that reference the ICM.

Use the following steps to configure the ICM:

1. From the Domino Administrator, click the **Configuration** tab.

2. Expand **Server** and click **All Server Documents**.
3. In the **Results** pane, select the Server document for the server on which you want to run the ICM; then click **Edit Server**.
4. Click **Server Tasks** → **Internet Cluster Manager** tab as shown in Figure B-1.

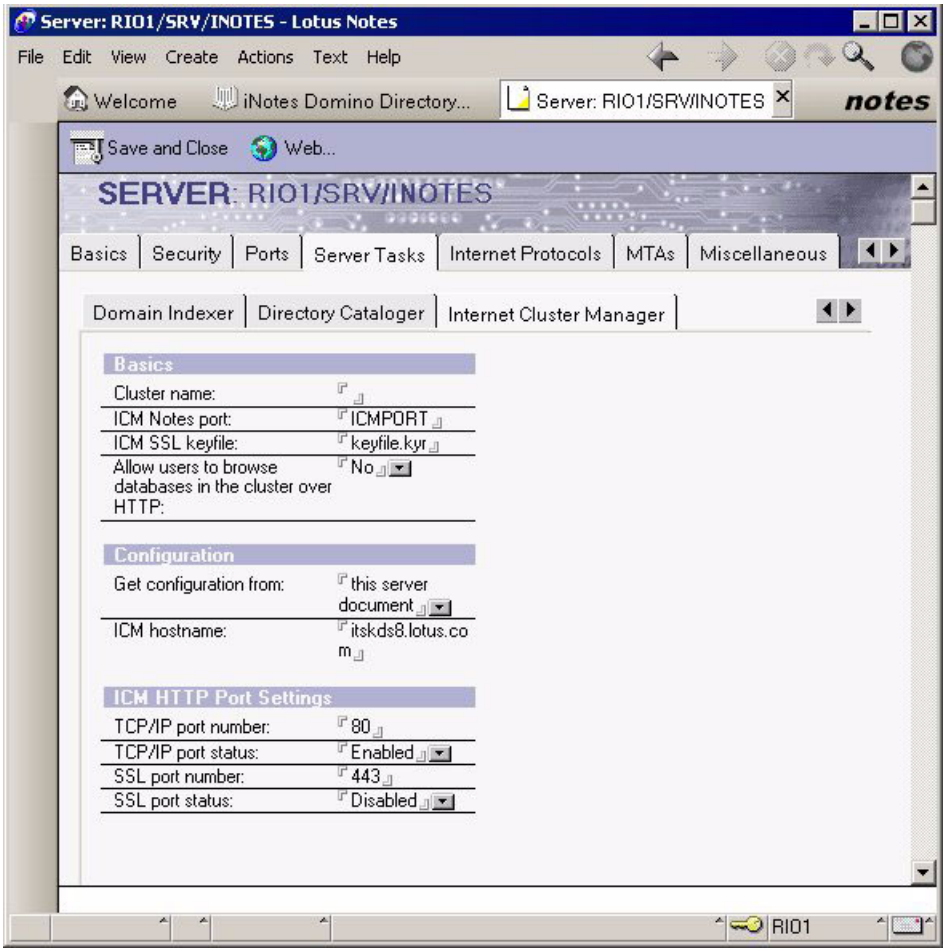


Figure B-1 Internet Cluster Manager tab on Server document

5. Complete the fields identified in Table B-1 on page 438.

Table B-1 Internet Cluster Manager fields on Server document

Field name	Description
Cluster name	The name of the cluster the ICM will service. If this field is blank, Domino uses the name of the cluster that contains this server.
ICM Notes port	The name of the Notes port the ICM will use to communicate with HTTP clients. If you leave this field blank, which is the default, the ICM can use any Notes port to communicate with HTTP clients. Enter a port name only if you want to restrict ICM communication to one specific port.
ICM SSL keyfile	The name of the SSL key file that contains certificates to identify the ICM when communicating with HTTP clients.
Allow users to browse databases in the cluster over HTTP	Lets HTTP clients view a list of the databases in a cluster. When you enable this field, users can enter `http://icmhostname/?OpenServer` as the URL to access. Entering this URL displays a list of databases on the servers in the cluster associated with the ICM named in icmhostname.
Get configuration from	Lets you specify a different Server document to get configuration information from. This field lets multiple ICMs share the same configuration.
Obtain ICM configuration from	This field appears when you select **another server document** in the field Get configuration from. Enter the name of the server whose Server document contains the configuration you want to use.
ICM hostname	The fully qualified name of the host that clients should use to communicate with the ICM. This can be the registered DNS name or the IP address. The Domino Web server uses this field to create URLs that reference the ICM. If this field is blank, the Web server will not be able to generate URLs that refer to the ICM.
TCP/IP port number	Enter the port number for the ICM to use. If you are running the ICM on the same server as the Web server, you must avoid address and port conflicts. If you do not give the ICM its own IP address, be sure that the port number the ICM is using is different from any of the other port numbers you use on the server.
TCP/IP port status	To enable HTTP communication with the ICM, choose Enabled. To disable HTTP communication with the ICM, choose Disabled.

Field name	Description
SSL port status	To enable HTTPS communication with the ICM, choose Enabled. To disable HTTPS communication with the ICM, choose Disabled.
SSL port number	Enter the port number to use for SSL. If you are running the ICM on the same server as the Web server, and you do not give the ICM its own IP address, be sure the SSL port number is different from any of the other port numbers you use on the server.

6. Save and close the Server document.

When the ICM starts, it looks at the Server document on the server on which it is running to find the ICM cluster name and its network address. It then obtains the host name and port settings from the same Server document or from the Server document specified in the field Obtain ICM configuration from.

If you run the ICM on the same system as a Domino Web server, you must avoid IP address conflicts or port number conflicts. The best approach is to assign the ICM its own IP address. You can also have the ICM share an IP address with the Web server if you specify different port numbers for the ICM and the other protocols on the Web server.

Setting up a separate IP address for the ICM

When you run the ICM on a Web server, you can give the ICM its own IP address to avoid conflicts:

1. Use your operating system to make the IP address available.
2. From the Domino Administrator on the server that contains the ICM, set up a port by doing the following:
   a. Choose **Files** → **Preferences** → **User Preferences**.
   b. Click the **Ports** icon, as shown in Figure B-2 on page 440.

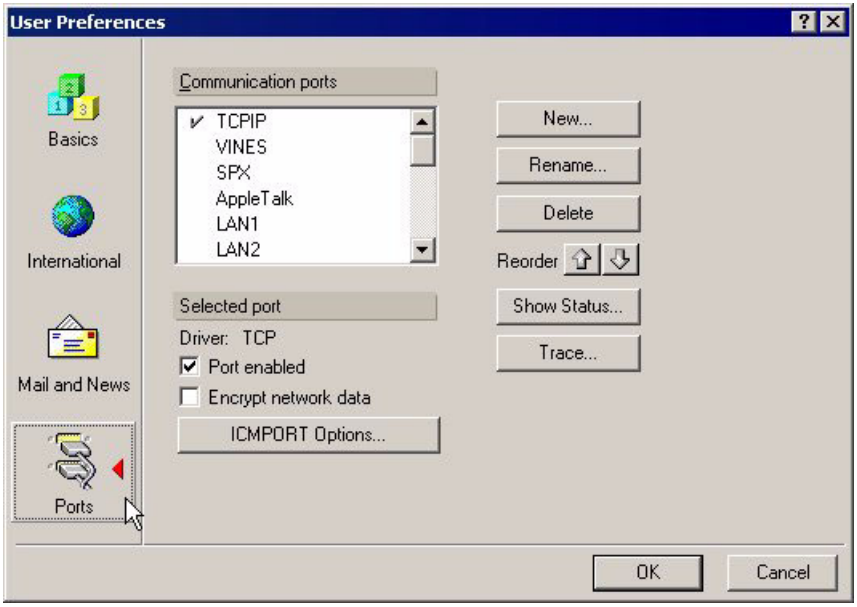


Figure B-2 User Preferences: Ports

c. Click **New**.

d. Specify a name for the new port, such as `ICMPORT` (see Figure B-3) and choose **TCP** as the driver.

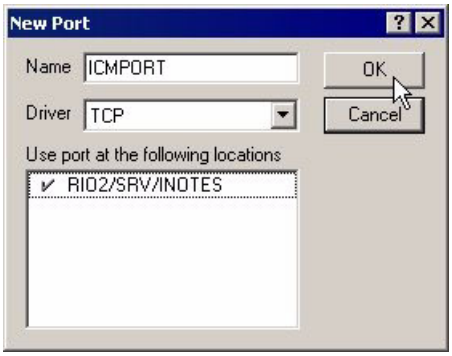


Figure B-3 New ICM port

e. Click **OK** twice.

   If you are not running the Domino Administrator on the server that contains the ICM, do the following to set up the port:

   - Add the following line to the NOTES.INI file:

     ```
     Portname=TCP,adapter number or network number,number of sessions,data buffer size
     ```

     For example: `ICMPORT=TCP,0,15,0`

   - Add the name of the port, such as ICMPORT, to the Ports setting in the NOTES.INI file.

3. Add the following to the NOTES.INI file:

   ```
   Portname_TcpipAddress=0,IPAddress
   ```

   Where portname is the name of the port you configured from the Domino Administrator, such as ICMPORT, and IPAddress is the IP address you are using for the ICM. For example:

   ```
   ICMPORT_TcpIpAddress=0,192.94.222.169
   ```

4. In the field ICM Notes port on the **Server Tasks** → **Internet Cluster Manager** tab in the Server document, enter the name of the port you configured, such as ICMPORT.

5. If you want to use port 80 for both the ICM and the Web server, you must do the following:

   a. In the Server document, click **Internet Protocols** → **HTTP** tab.

   b. In the Host name(s) field, enter the IP address or host name of the Web server.

   c. In the Bind to host name field, select **Enabled**.

C

Additional material

This redbook refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material associated with this redbook is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser to:

ftp://www.redbooks.ibm.com/redbooks/SG247060

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select the **Additional materials** and open the directory that corresponds with the redbook form number, SG247060

Using the Web material

The additional Web material that accompanies this redbook includes the following files:

Table 11-1 Files included as additional material

Filename	Description
Customization_Wordmap.txt	Obfuscation list for abbreviated JavaScript function calls used in DWA 6.5
startserver	Script for starting and rebooting the Domino Server
domino	Script for starting only the domino server.

How to use the Web material

Create a subdirectory (folder) on your workstation, and unzip the contents of the Web material zip file into this folder.

Related publications

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

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 445. Note that some of the documents referenced here may be available in softcopy only.

- *Domino R5 for Sun Solaris 8,* SG24-5969
- *IBM WebSphere Portal for Multiplatforms V5 Handbook,* SG24-6098
- *Lotus Domino 6 for Linux*, SG24-6835
- *Portalizing Domino Applications for WebSphere Portal,* SG24-7004

Online resources

These Web sites are also relevant as further information sources:

- Lotus Developer Domain

  http://www.lotus.com/ldd
- InfoCenter of IBM WebSphere Application Server

  http://publib.boulder.ibm.com/infocenter/wasinfo/index.jsp
- InfoCenter of IBM WebSphere Portal Server

  http://publib.boulder.ibm.com/pvc/wp/500/ent/en/InfoCenter/index.html

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

Domino Web Access 6.5 on Linux

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

Domino Web Access 6.5 on Linux

Installation, configuration, tuning of DWA 6.5 on Red Hat, UnitedLinux

Overview of features and functionality

Basic customization techniques

IBM Lotus Domino Web Access 6.5 (IBM Lotus iNotes Web Access) is a sophisticated Web client that gives end users many of the messaging and collaboration features previously available only with a Lotus Notes client.

Beginning with Domino 6.5, you can access Lotus Domino on a Linux server, while using Domino Web Access on a Linux desktop, giving you a leading-edge, end-to-end collaborative solution for Linux. Browser users will be able to take full advantage of Domino services through an ultra-intuitive, easy-to-use interface, both online and offline, seamlessly. Domino Web Access was architected using the latest Web application development technologies and can be centrally administered, helping organizations to drive down deployment costs and, potentially, reduce Total Cost of Ownership.

This IBM Redbook provides a detailed technical overview of Domino Web Access 6.5 and discusses how to install, configure, and deploy an end-to-end Linux solution for Domino. In addition to setting up DWA 6.5, it also covers how to integrate Lotus Sametime for real-time collaboration and awareness. Finally, we discuss key deployment considerations, integration points between Domino Web Access and IBM WebSphere Portal, and some approaches and techniques to customizing Domino Web Access 6.5.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7060-01 ISBN 0738497770