

Upgrading to Lotus Notes and Domino 6

New features of Notes and Domino 6 described

Details about upgrading servers, clients, and directory

Administering the new environment



Tommi Tulisalo
Edwin Kanis
Jean-Noel Koval
Cynthia Mamacos
Carol Sumner



International Technical Support Organization

Upgrading to Lotus Notes and Domino 6

December 2002

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

First Edition (December 2002)

This edition applies to IBM Lotus Notes 6.0 and IBM Lotus Domino 6.0

© Copyright International Business Machines Corporation 2002. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	xi
Trademarks	xii
Preface	xiii
The team that wrote this redbook	xiii
Become a published author	xv
Comments welcome	xvi
Chapter 1. Introduction	1
1.1 Benefits to upgrading	2
1.2 Best new features	3
Chapter 2. Upgrade considerations	7
2.1 Server and client licensing	8
2.1.1 New Domino Server licensing	8
2.1.2 Client licensing	9
2.2 Interoperability issues	9
2.2.1 Client/mail template interoperability	10
2.2.2 Calendar & Scheduling interoperability: R4 and Notes 6	11
2.2.3 Client interoperability	13
2.2.4 Mail interoperability	14
2.2.5 Administrator client	14
2.2.6 Template interoperability	14
Chapter 3. Upgrade considerations for Notes clients	17
3.1 Training	18
3.2 Workstation requirements	18
3.3 Calendaring and scheduling considerations	19
3.4 Upgrading the client before upgrading the server	19
3.5 A Word about On Disk Structure	20
3.6 Mail files	21
3.6.1 Mail file replicas (non-clustered)	21
3.6.2 Mixed-release cluster and mail file replicas	23
3.6.3 Customized mail templates	23
3.6.4 Using seamless mail upgrade to upgrade mail files	23
3.7 Notes 6 client with R4.6 and R5 applications	24
3.8 Policy-based administration	25
3.8.1 From R5 user profiles to Notes/Domino 6 policies	25

3.8.2	New possibilities with dynamic configuration	26
3.9	Client upgrade options	26
3.9.1	Upgrade by mail	26
3.9.2	Smart upgrade	27
3.9.3	Manual upgrade	28
3.9.4	Third-party deployment options	28
Chapter 4.	Upgrade considerations for Domino servers	29
4.1	Server requirements	30
4.2	Restructuring your environment	30
4.3	Upgrade sequence	31
4.4	Install and configure new Domino 6 features	32
4.5	Server upgrade options	32
4.6	Directory and ODS upgrade	33
4.6.1	ODS upgrade	33
4.6.2	Domino Directory design upgrade	33
4.7	Coexistence or interoperability	34
4.7.1	Lotus companion products	35
4.7.2	Third party products	35
Chapter 5.	Domino Directory upgrade	37
5.1	Introduction to the new design	38
5.1.1	The Domino Directory user interface	38
5.1.2	Server form	39
5.1.3	Configuration form	44
5.2	Administration delegation possibilities	48
5.3	Fault recovery	51
5.4	UNK table in a mixed environment	52
5.5	Controlling and managing the distribution	54
5.5.1	Using a custom design template for the Domino Directory	56
5.5.2	Retaining R5 Domino Directory design on certain servers	59
5.6	Secondary directories	60
5.6.1	Extended Directory Catalog	60
5.6.2	Condensed Directory Catalog	61
5.6.3	Directory Assistance	61
5.6.4	Cascading Domino Directories	61
5.6.5	LDAP Schema changes	62
5.7	Upgrading your Domino Directory to the new design	63
5.7.1	Upgrading your Domino Directory first	64
5.7.2	Server and Directory design upgrade at the same time	65
5.8	Introduction to the new On-Disk Structure (ODS)	68
5.8.1	Upgrading to the new ODS level	71
5.8.2	Demystifying some ODS legends	72

Chapter 6. Domino Server upgrade	75
6.1 Upgrade sequence	77
6.2 Disabling and deleting unused program documents	77
6.3 Make a full backup of your servers	79
6.4 Upgrade checklist and pre-upgrade tasks	80
6.5 Upgrade the server code	85
6.6 Before restarting the server: Post upgrade tasks	103
6.7 Start your Domino Server (now running Domino 6)	112
6.8 Post-upgrade tasks	112
6.9 ODS conversion	114
Chapter 7. Lotus Notes client upgrades	117
7.1 Preparation: Know your environment	118
7.1.1 Determine the hardware and OS level of each machine	118
7.1.2 Physical location of the machine	119
7.1.3 Administrative rights to the workstation	119
7.1.4 Current Lotus Notes clients	119
7.1.5 Notes applications already being used	120
7.1.6 Mail and calendar delegation situation	120
7.1.7 Upgrade restrictions	121
7.1.8 Comfort level with new technologies	121
7.2 Prepare to install the client	121
7.2.1 Hardware and OS	121
7.2.2 Back up the following essential files	121
7.3 Install the Notes 6 client	122
7.3.1 Client options	122
7.3.2 Detailed instructions for installing the client	122
7.3.3 Setting up the Personal Address Book preferences	128
7.3.4 Configuring Upgrade-by-mail	130
7.3.5 Changes to the Notes client	134
7.3.6 Rolling back to R4 or R5	135
7.4 Upgrading the mail file design	136
7.4.1 Use the convert utility on the server	137
7.4.2 Manually upgrade the design of the mail file	139
7.4.3 Seamless mail upgrade	141
7.5 Upgrading the client in the future	145
7.6 Standard templates/files installed with Notes 6	145
7.7 Help and documentation	146
Chapter 8. Monitoring your infrastructure	149
8.1 Monitoring configuration and results databases	150
8.1.1 Creating your monitoring infrastructure	154
8.1.2 Monitoring Configuration database (Events4.nsf)	156

8.2 New analysis capabilities	180
8.2.1 New log search capabilities	180
8.2.2 Console properties: Event filter and color coding	188
8.3 Activity logging	198
8.3.1 Enabling activity logging	199
8.3.2 Reporting Activity Logging data	203
Chapter 9. New messaging administration options	209
9.1 Router controls	210
9.1.1 System mail rules	210
9.1.2 Mail journaling	218
9.1.3 Using the router for quota management	223
9.2 Controlling automatic forwarding	227
9.3 SMTP settings	229
9.3.1 SMTP inbound controls	231
9.4 Automatic mail archiving	245
9.4.1 Client-side archiving	246
9.4.2 Server-side archiving	255
9.5 Single copy object store (Shared mail)	273
9.5.1 Set up shared mail with the server document	274
9.5.2 Guidelines for configuring shared mail	276
9.6 IMAP improvements	276
9.7 Configuring mail files for IMAP access	277
9.7.1 Automatic conversion of mail files	278
9.7.2 Manual conversion of mail files (R5 and Domino 6)	279
9.7.3 Conversion of R4 mail files	281
9.7.4 Checklist for IMAP accounts	282
9.8 Server configuration for IMAP	283
9.8.1 Starting the IMAP service	283
9.8.2 IMAP port configuration	284
9.8.3 IMAP service configuration	285
9.9 Making use of the NAMESPACE extension	291
9.9.1 Sharing mail files	292
9.9.2 Public databases (mail-in databases)	295
9.10 IMAP activity logging	298
9.10.1 How to configure IMAP activity logging	298
9.10.2 View the logging data	300
Chapter 10. Security	303
10.1 Domino server security configuration	304
10.1.1 Administrators	304
10.1.2 Security settings	313
10.1.3 Server access	314

10.1.4	Programmability restrictions	318
10.1.5	Internet access	322
10.1.6	Passthru use	322
10.2	Workstation security	323
10.2.1	General guidelines to create secure ECLs	324
10.2.2	Security settings documents for ECLs	325
10.2.3	Check the security settings on the workstation	328
10.2.4	Notes Client security - automatic logout	333
10.2.5	Forcing encryption of local replicas	335
10.2.6	Notes browser security	337
10.3	Web security	340
10.3.1	Protecting your Web server at the connection level	342
10.3.2	Protecting your Web server at the validation level	346
10.3.3	Protecting your Web server at the authentication level	347
10.3.4	Protecting your Web server at the authorization level	354
Chapter 11.	Certificate Authority (CA) process	357
11.1	Certificate Authority concepts	358
11.2	Domino 6 server-based CA for Notes IDs	360
11.2.1	Steps to set up the CA process	360
11.2.2	Table of ca console commands	370
11.2.3	Registration Authority administrative tasks	372
11.2.4	Certificate Authority administrative tasks	375
Chapter 12.	Internet Site architecture	385
12.1	Domino R5 and Domino 6 documents - differences	386
12.2	Internet Site configurations	387
12.2.1	Internet Site documents	387
12.2.2	Global Web Settings document	392
12.2.3	Internet Site Rule document	392
12.3	Additional new features related to Domino 6	396
12.3.1	Language differentiation	396
12.3.2	Third-party HTTP server integration	397
12.3.3	WebDAV	403
12.3.4	Session-based name-and-password authentication	404
12.3.5	Other changes to the Domino HTTP task	405
12.4	Upgrading to Domino 6 Internet Site architecture	405
12.4.1	Upgrading steps	406
Chapter 13.	Domino hosting features	407
13.1	Hosted organizations	408
13.1.1	Addressing models	408
13.1.2	Multiple organization Domino Directory	409

13.2 Differences between Domino and xSP Domino	409
13.3 Planning for the hosted organization model	411
13.3.1 Scalability and reliability	411
13.3.2 Protocol support	411
13.3.3 Billing	412
13.3.4 Database management in a hosted organization setup	413
13.4 Setting up the xSP Domino environment	413
13.4.1 Registering hosted organizations	413
13.4.2 Steps for setting up the environment	415
13.4.3 Installing the server	415
13.4.4 Setting up the Domino Certificate Authority	421
13.4.5 Setting up policy documents	422
13.4.6 Binding the IP addresses to the xSP server	423
13.4.7 Creating loopback addresses	424
13.4.8 Configuring Global Web Settings and Internet Site documents ..	425
13.4.9 Using Global Web Settings documents	425
13.4.10 Configuring activity logging for billing	426
13.4.11 Setting up additional security	428
13.5 Additional information	429
Chapter 14. Extended ACL	431
14.1 Usage and benefits	432
14.1.1 Planning and considerations	432
14.2 Implementing and administering the xACL	433
14.2.1 Enabling the xACL	434
14.3 Extended administration server	444
14.4 Considerations for xACL implementation	446
Chapter 15. Policy-based administration	449
15.1 Policies	450
15.1.1 Policies in Domino	450
15.1.2 Administrative areas	451
15.1.3 Available policy types	452
15.1.4 Policies versus setup profiles	453
15.2 Administering policies	453
15.2.1 Parent and child	453
15.2.2 Inheritance	453
15.2.3 Policies in the Administration client	454
15.2.4 Creating and explaining policy and settings documents	456
15.2.5 Policy synopsis	460
15.3 Planning your policy model	462
15.3.1 Example of using policies	464

Chapter 16. Administering the Notes 6 client	469
16.1 Client installations	470
16.1.1 Shared network installation	470
16.1.2 Multi-user workstations	472
16.1.3 Customizing client installations with transform files	476
16.1.4 Silent install	484
16.1.5 Smart Upgrade	484
16.2 Making use of policies	493
16.3 Corporate welcome pages	494
16.3.1 Create the new welcome page	494
16.3.2 Configure the desktop settings document	502
16.3.3 Apply the policy	503
16.4 Other user interface features	505
16.4.1 Notes ID files	505
16.5 License tracking	517
Appendix A. Consolidation	523
Benefits of consolidation	524
Consolidation and Domino 6	526
Planning for consolidation	528
Service level requirements	528
Logical environment considerations	528
Physical environment considerations	529
Planning your consolidation path	529
Appendix B. Monitoring and troubleshooting	531
Monitoring your Domino server	532
Operating systems statistics	532
Domino statistics	536
Tools for monitoring Domino	537
Troubleshooting	540
Defining the problem	540
Looking for the cause	541
Finding possible solutions	542
Implementing the solution	543
Tools and utilities to monitor your infrastructure	543
Related publications	545
IBM Redbooks	545
Referenced Web sites	545
How to get IBM Redbooks	546
IBM Redbooks collections	546
Index	547

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:

IBM®

IBM eServer™

Redbooks (logo)™ 

AIX®

OS/400®

Perform™

Redbooks™

S/390®

SP™

Tivoli®

WebSphere®

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

Lotus®

Word Pro

Domino Designer®

Domino™

iNotes™

Lotus Notes®

Notes®

QuickPlace™

Sametime®

The following terms are trademarks of other companies:

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

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

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

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

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

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

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

Preface

IBM released another major version of IBM Lotus Notes and Domino in October 2002. Notes and Domino 6 contain a lot of new, interesting, and powerful features.

Many of the features are aimed at making administration easier, while others have a dramatic effect on performance (for example, the new network compression functionality, which will in most cases substantially decrease the amount of network traffic).

In this IBM Redbook, we show how to upgrade existing Lotus Notes and Domino installations to IBM Lotus Notes and Domino version 6. The chapters have been structured as a series of logical steps that you can follow when upgrading your environment.

First, we introduce the new features of Lotus Notes and Domino 6, and discuss overall upgrading considerations, coexistence issues, and interoperability. Next, we examine upgrading considerations specifically related to clients and servers. Then we guide readers through the actual steps needed to upgrade the Domino Directory, the Domino Server, and Lotus Notes Clients.

New functionality of the Domino 6 environment is presented, along with topics related to administering the new environment, including server monitoring, messaging, security, administering clients, policy-based administration, and more. Information on troubleshooting is also provided.

This redbook is written for Lotus Domino R5 administrators who need to upgrade to Notes and Domino 6. Working knowledge of Domino infrastructures and Domino servers is assumed.

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 Center.

Tommi Tulisalo is a project leader for the International Technical Support Organization at Cambridge, Massachusetts. He manages projects whose objective is to produce redbooks on all areas of Lotus Software products. Before joining the ITSO in 2001, he was an IT Architect for IBM Global Services in Finland, designing solutions for customers, often based on Lotus software.

Edwin Kanis is a Senior Consultant with Spherion Business Solutions in The Netherlands. He works as a groupware consultant, specializing in Notes/Domino infrastructure, deployment, and migration projects. Over the past six years, he has gained extensive experience in handling projects for small, medium, and large customer accounts. Edwin can be reached at edwinkanis@spherion.nl.

Jean-Noel Koval works as a Senior IT Systems Specialist for the IBM Software group in Paris, France. He joined Lotus six years ago and has been leading IBM's internal early deployment of Notes and Domino 6 for the EMEA region. He has worked with early deployment of Notes and Domino 6 since 2000, and was involved in the early deployment of Domino R5 for Lotus EMEA. His areas of expertise include Domino administration and infrastructure implementation and optimization, with a focus on performance-related issues on various platforms. He has also been an early adopter for Domino for Linux. Jean-Noel can be reached at jnk@fr.ibm.com.

Cynthia Mamacos is a Development Relations Manager in the Product Introduction organization. Her primary responsibility is the early deployment of Notes/Domino 6 for the IBM/Lotus account. She joined Lotus in 1991 and worked in many parts of the organization, ranging from Desktop Support to Domino Product Management, before joining the newly formed Development Relations team.

Carol Sumner is an Advisory IT Specialist working for IBM Software Services for Lotus. She has 11 years of IT experience, including six years of specialization in messaging systems implementation, administration, and migrations. She received a B.A. from the University of Iowa, and holds a Master of Divinity degree from Texas Christian University.

Special thanks to the following people for their contributions to the redbook:

Mary LaRoche is a Consulting I/T Architect for IBM Software Services for Lotus (ISSL) in Bethesda, Maryland. An infrastructure and security architect, Mary designs and leads the implementation of technical solutions for the varied business needs of customers, ranging from bio-technology and legal firms to major banks and US Government agencies. Mary contributed to the chapter describing the security features in Domino 6.

Varada Manavalan is a Consultant with IBM Global Services and Research, Albany, New York. He has been part of the IBM Lotus Notes and Domino technical team for AIX and S/390 since 1997. He has six years of experience in Lotus Notes and Domino, including three years on AIX UNIX. He holds a Master's degree in Computer Information Systems from Marist College. His areas of expertise include architecture, customization, quality assurance, deployment, performance tuning, troubleshooting, relational databases, and

front-end tool development. Varada contributed especially to the chapters describing Domino server and Directory upgrade.

Benjamin Morris is an I/T Specialist with IBM Global Services. He has supported Notes and related products within IBM for over two years, and has been involved in the Notes 6 project for much of that time. He can be contacted at morrisb@us.ibm.com. Ben contributed to the chapter describing client upgrading, specifically on how to use the InstallShield Tuner for Lotus Notes.

Special thanks also to **Lateef Junaid**, IBM Global Services in Atlanta and **Gregory Rick Chadbourne**, Lotus Software in Westford, for reviewing the redbook and making comments and suggestions.

We would like thank to the following people, who provided support and guidance:

Lori Davidson, Jim Lund, Peter Mierswa, Moses Peabody, Paul Raymond, Ray Sambrano, Katherine Spanbauer, Raz Stephen, Carol Zimmet - IBM Westford Lab

Gary Devendorf, James Grigsby, Jill Jones, Greg Kelleher, Alan Lepofsky, Ted Niblett, Andrea Russell - Lotus software

Amy Smith and the whole GPD UA team

Ken Xu, John Justin - IBM Global Services

Ruud van Eijken, Bas Noij - Spherion

Adam Missner, The Coca-Cola Company

Ella Buslovich, Alison Chandler, Terry Barthel, Alfred Schwab - ITSO, Poughkeepsie Center

William Tworek, ITSO, Cambridge Center

Become a published author

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

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

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our 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 Internet note to:

redbook@us.ibm.com

- Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. TQH, Mail Station P009
2455 South Road
Poughkeepsie, NY 12601-5400



Introduction

This chapter describes the new and enhanced features in Notes and Domino 6. In addition, it identifies the benefits—from both administrator and user viewpoints—of upgrading to Notes and Domino 6.

1.1 Benefits to upgrading

There are several compelling reasons your organization will want to upgrade to IBM Lotus Notes and Domino 6. Domino 6 will enable you to harness more value from your infrastructure, manage more users, increase network efficiency, while at the same time controlling or reducing total cost of ownership. The improvements made in the new version let administrators and end users do more with less. Lower costs, fewer resources required, reduced time and effort—all of these benefits can be achieved by putting Lotus Notes and Domino 6 to work in your organization.

Since the focus of this redbook is upgrading, we do not try to enumerate all the features of Notes and Domino, concentrating instead on new and enhanced features introduced in Domino 6.

Some of the hottest enhancements are:

- ▶ Streamlined deployment and administration with centralized tools that enable policy-based management. These tools allow the administrator to dynamically configure clients and servers from a central location.
- ▶ Heightened performance with enhanced cluster support and optimized server start-up.
- ▶ Advances in end-user productivity, such as improved customer dialog boxes and dual time-zone support.
- ▶ Mobility enhancements like selective, scheduled, and streaming replication.

For a technical overview on all the features that IBM Lotus Notes and Domino 6 have to offer, consult *LDD Today* on the Lotus Web site, especially the following articles:

“Notes 6 Technical Overview”

“Domino 6 Technical Overview”

Other good resources are the files that come with the new system, in particular:

- “What’s new” section of the release notes
- The online help databases (help6_admin.nsf, help6_client.nsf, help6_designer.nsf)

1.2 Best new features

As soon as Notes and Domino 6 were introduced, we started getting favorable comments from administrators and users. The best new features of Domino 6—according to our customers—are the following:

Domino server improvements

Many new features at the server level will make your life easier, including:

- ▶ Streaming replication - Improves replication across all servers, especially mail server performance. Additionally, when using the Notes client, you no longer have to wait until the replication is over before seeing replicated documents in the folder. This means you can begin working before the replication is done.
- ▶ Network compression - Reduces the number of bytes sent during transactions by up to 50%. Just enabling network compression on all the servers can save you significant bandwidth. If you also enable clients to use network compression (easily done with a policy), you will see even more improvements and customer satisfaction.
- ▶ Tivoli predictive server health monitoring - Helps guide you with both short-term and long-term recommendations for improving server performance.
- ▶ Automatic server fault recovery - Available on Windows NT and UNIX, it shuts down and restarts the server without administrator intervention. You can configure the number of times it will do this, and also automate actions it takes with scripts.
- ▶ Multi-lingual server support - Enables more than one language per server.
- ▶ Advanced transactional logging (view logging) - Decreases the amount of time the server takes to restart since the critical views will not have to be reindexed.
- ▶ DNS Blacklists (DNSBLs) - Mail from servers found on a DNS Blacklist can be tagged or rejected, giving you more control over mail from hosts that may be sending or relaying potential spam.
- ▶ Server-based mail rules - Let you specify message criteria and action to be taken for all messages processed on the server.
- ▶ Automatic archiving - Enables you to archive mail for your users, thereby relieving them of the burden of setting up and running archive.
- ▶ Web Admin 6 - Do virtually anything from the Web, instead of launching the administrator client—handy when you're not sitting at your desk!

Client improvements from an administrator's perspective

Administering the Notes client environment has been improved through the use of policies and tighter integration with the operating system. You have more control over the client environment if you want it. The user interface for certain features has been improved so your users may be able to navigate through certain client options on their own. Specific enhancements in Domino 6 include:

- ▶ MSI Support - Create customized installations with the same look and feel as other Windows installations. Create different installation packages for different kinds of users.
- ▶ Corporate welcome pages - You have the ability to push out corporate welcome pages, or even departmental welcome pages, if that is desirable in your organization.
- ▶ Multi-user workstations - In combination with the Windows operating systems, you can easily set up separate Lotus Notes environments for several users on one workstation.
- ▶ Smart upgrade - Automatically upgrade clients when new maintenance releases become available.
- ▶ Seamless mail upgrade - Automatically upgrade mail file designs as the clients are upgraded.
- ▶ Policy-based management - Goes beyond Domino R5 setup profiles and simplifies administration. Clients can be reconfigured through a *policy*, configuration is no longer tied to the setup of the client.
- ▶ Workstation security - Dynamically reconfigure workstation security, including ECLs; create different security settings for different groups of users.
- ▶ User security interface - All of the security settings have been consolidated into one path: Password changes, certificate management, data encryption, automatic logout, and smartcard configuration take place through the File -> Security -> User Security menu path. The user is given help with changing their password (and password strength requirements are demonstrated for them).

All of the server and client administration features are explained in great detail in this redbook.

Client improvements from a user perspective

Your users will enjoy these new features. We don't provide details about these features here since the focus of this book is upgrading your system. However, you may want to investigate them on behalf of your users.

- ▶ Welcome page - Redesigned to increase ease of use and make more of the features accessible to users.

- ▶ Bookmarks - Now include two new folders: a startup folder and a history folder.
- ▶ Inbox customizations:
 - Color coding of mail messages based on client mail rules configured.
 - Sort order is now a sticky switch.
 - Unread document count in folders.
 - Attachment handling enables users to edit attachments in place. Never send the wrong version of an attachment again!
- ▶ Drag/Drop from the desktop or operating system.
- ▶ Swiftfile:
 - Intelligent assistant to help file messages from the inbox.
 - Install from the /Apps directory on the CD.
- ▶ Replication:
 - Streaming replication - When using the Notes client, you no longer have to wait until the replication is over before seeing replicated documents in the database; you can begin working before the replication is done.
 - Drag/drop to replicate selected documents, a view or a database. Just drag to the replicator page.
 - Selective replication form - In the Notes 6 mail template users can create a replica based on sender, sent mail, draft mail, calendar entries, and so on.
- ▶ Increased user productivity; support for multi-tasking in the client:
 - Poll for new mail
 - Detaching files
 - Replication
 - Printing
 - Monitoring Alarms
 - Subscriptions
 - Processing
 - Agents
 - Replacing database designs
 - Copying databases
- ▶ More general client features:
 - Customized logout screen appears when your user ID is locked.
 - Dynamic toolbars for quick access to features, options, and commands.
 - Status bar customization.
 - Window tab repositioning.

- Copy view as table.
- Type-ahead support in dialog boxes.
- Resizable dialog boxes.
- Document locking.

Notes 6 calendar and scheduling improvements

- ▶ Enhanced calendar user interface
- ▶ Summarized view has an easy-to-read columnar format
- ▶ New intuitive meeting form with time zone support
- ▶ Embedded scheduler
 - Shows who can and cannot attend a meeting
 - Displays appointment details
 - Provides access to other users' calendars and appointments
 - Provides suggested meeting times
- ▶ New preferences: Delegation wizard, colors, and time zones
- ▶ Enterprise calendar management:
 - Streamlined method to manage calendars
 - Menu shortcuts to open executives' calendars
 - E-mail notification to assistant when executive receives invitation
 - E-mail notification for accepts and declines when the executive is the chairperson
 - Notifications include doclinks to allow quick access to the invitation, acceptance, and so forth
- ▶ Better calendar printing options
- ▶ Resource reservations
 - New resource type
 - Improved overall messages
 - Individual room/resource calendars
- ▶ To Do's
 - In-view adding and editing
 - Customizable view
 - Categories: allows you to define your own categories
 - Display calendar based on user preferences



Upgrade considerations

This chapter discusses some of the areas administrators should consider before starting an upgrading project. The topics covered are:

- ▶ Server and client licensing
- ▶ Interoperability issues
- ▶ Coexistence issues

2.1 Server and client licensing

This section provides a comparison of the new Lotus Domino 6 Server license offerings in reference to the Domino R5 offerings you are already familiar with, and also provides a little more detail about each of the new offerings.

2.1.1 New Domino Server licensing

Table 2-1 Domino Server offerings

Lotus Domino R5 server offerings	Lotus Domino 6 server offerings
Domino Mail Server	Domino Messaging Server
Domino Application Server	No longer exists for Domino 6; replaced by Enterprise Server
Domino Enterprise Server	Domino Enterprise Server
Domino Enterprise Advanced Server	No longer exists for Domino 6; replaced by Utility Server
Domino Extranet Server	Domino Utility Server

Following is a brief overview of the Lotus Domino 6 server offerings:

► **Domino Messaging Server**

This is the Domino server that provides messaging services. It allows access to the messaging and calendar functions of Domino. This option includes the partitioning feature that allows customers to have multiple instances of Domino servers on the same machine. Note that it does not include support for application services or Domino clusters.

Use this server for e-mail, calendar and scheduling, and if you do not need clustered servers.

► **Domino Enterprise Server**

The Domino server that provides both messaging and application services, with support for Domino clusters. It provides access to full collaborative functions of Domino as well as the messaging and calendaring features of the Domino Messaging server.

Use this server for applications and messaging and if you need clustered servers.

► **Domino Utility Server**

The Domino server that provides access to application services only, with support for Domino clusters. Note that it does not include support for

messaging services. The Domino Utility Server is a new installation type for Lotus Domino 6 that removes client access license requirements. See full licensing text in the release notes for details.

Use this server for applications where mail is not required.

2.1.2 Client licensing

There are no changes to the types of IBM Lotus Notes Client licenses that are available.

2.2 Interoperability issues

When upgrading your environment to a newer version of Domino, you will have a situation—at least for a while—when the environment has different versions of servers, clients, and applications. This section describes some of the known interoperability issues that you need to be aware of. This information will help you to plan and conduct your upgrade while still maintaining the successful functioning of your environment.

To upgrade to Lotus Notes/Domino 6, your Notes/Domino system should be running Domino 4.6 or later. Upgrade a Domino 4.6 system to the latest Maintenance Release (MR) 4.6.7a *before* upgrading to Lotus Notes/Domino 6.

Some of the key interoperability issues you need to consider are:

- ▶ Client/Template
- ▶ Calendar & Scheduling between R4 and Notes 6
 - Repeating meetings
 - Recommendations that will improve the calendar experience until all client and mail templates can be upgraded to Notes 6
- ▶ Client interoperability
- ▶ Mail interoperability
- ▶ Administrator client Interoperability
- ▶ Template interoperability

The following tables list known interoperability issues when using mixed versions of Domino servers, Notes clients, and mail files.

2.2.1 Client/mail template interoperability

This section provides information about which features of the different mail template versions are available when using the template with Notes R4, Notes R5 and Notes 6 clients.

Table 2-2 Client/mail template interoperability issues

Client	Reading R4.5/R4.6 Mail Template	Reading R5 Mail Template	Reading Notes 6 Mail Template
R4.5/R4.6 clients	Full functionality	<ul style="list-style-type: none">•Calendar View: Can only view 30 day view.•Clients <4.64 may see 4 errors upon opening the mail database using R5 mail template, and 2 errors upon closing the mail database.•Lotus Notes 4.6.4 is the minimum Notes client release for compatibility.	<ul style="list-style-type: none">•Calendar view: Can only view 30 day view.•Clients <4.64 may see 4 errors upon opening the mail database using R5 mail template, and 2 errors upon closing the mail database.•Lotus Notes 4.6.4 is the minimum Notes client release for compatibility.
R5 Notes client	Full functionality	Full functionality	<p>Mail View</p> <ul style="list-style-type: none">•Can do anything that you could do in mail in R5.•Do not have any of the new Notes 6 functionality because you don't have the Notes 6 binaries to support it. <p>Calendar view</p> <ul style="list-style-type: none">•Can read calendar entries, but cannot act on them or delete them.•Can see all R5 calendar views, but not new Notes 6 views (work week, two work week view, work month view).•No soft deletes.•Cannot access preferences form. <p>To Do View</p> <ul style="list-style-type: none">•Same as Calendar view.
Notes 6 client	Full functionality	Full functionality	Full functionality

2.2.2 Calendar & Scheduling interoperability: R4 and Notes 6

This section describes Calendar & Scheduling interoperability issues when using R4 and Notes 6 clients. Tables outlining the calendar and scheduling features available for this combination of clients are provided.

Repeating meetings

Here are some general rules about reschedule notices for repeating meetings when an R4 chair/participant is involved:

1. You must add the invitation to your calendar before processing any reschedules.
2. Reschedules must be processed in the order received because a reschedule adjusts each calendar entry by an offset, not an absolute value (also known as the Delta Shift Model). Applying them out of order may cause undesirable results.
3. Reschedules are keyed off of a particular repeat instance. This instance must appear on the Calendar in order for the reschedule to be applied.

To determine the instance in question:

- The reschedule's Start Date Time and End Date Time fields should match the repeat instance's Start Date Time and End Date Time fields.
- In addition, the repeat instance will have a Form field with the value of Appointment and the Calendar Date Time field should be the same as Start Date Time field. The Form field differentiates the document from a workflow notice. The presence of a Calendar Date Time field causes the document to display in the Calendar views.
- The reschedule will either be a child document of the repeat instance, or a child of the same parent as the repeat instance (the reschedule and repeat instance are sibling documents).

Note: Organizations that want to use the repeating meetings feature in the Notes/Domino 6 mail template should upgrade their Notes 4.6 clients and mail templates to Notes 4.6.3 or later for repeating meetings to work properly in a mixed-release environment. You do not need to upgrade servers, but you must upgrade the mail templates for those clients that want to use repeating meetings.

Using R4 mail files on Domino 6 servers

Upgrade your servers to Domino 6, regardless of when the clients and mail files are being upgraded. Notes R4 clients will benefit from this.

Place all replicas for mail files based on the R4 mail template onto Domino 6 servers. There have been a number of improvements made in Domino 6 for calendar and scheduling functions. Moving your R4 template-based users to Domino 6 servers improves their calendar experience until their client and mail templates can be upgraded to Notes 6.

The following tables outline some of the features available to R4 mail clients running on an Domino 6 server.

Table 2-3 Notes 6.0 with Notes R4.6 invitees

Notes 6.0 chair	4.6 Invitee with 4.6 server	4.6 invitee with 6.0 server
Invite and reschedule repeating meetings	Not available	Available unless messages are encrypted.
Add invitee to repeat meeting - All	Not available	Available with the following limitation: On the invitation form in the section entitled "Repeating meeting information", the line beginning with "This meeting repeats" will have missing dates. However, the following line, "Meeting Dates", will be accurate.
Add invitee to repeat meeting - Partial	Not available	When multiple partial invitations are sent by the Chair: <ul style="list-style-type: none"> •Merges the dates into first invitation if it has not been added to the calendar. •Attempts to keep the beginning of the repeat meeting accurate. •Subsequent invitations are always changed into a confirmation. On the invitation form in the section entitled "Repeating meeting information", the line beginning with "This meeting repeats" will have missing dates. However, the following line, "Meeting Dates", will be accurate.
Remove and re-add to a repeat meeting	Not available	Behaves the same way as "Add Invitee to Repeat Meeting - Partial". To work around the case when the invitation was previously added to the calendar, remove all documents related to the meeting before being re-added.
Send updated information	Not available	Changes the update info notice into a confirmation.

Table 2-4 Notes 6.0 invitee with Notes 4.6 chair

6.0 Invitee	4.6 Chair with 4.6 Server	4.6 Chair with 6.0 Server
Autoprocess repeat meetings	Not available	Only support for invitations; reschedules are not processed.

2.2.3 Client interoperability

This section describes some known interoperability issues between different versions of Notes clients.

Local databases and unread marks

When opening a local database with Notes and Domino 6, all unread marks are reset (all documents marked unread) if it is later opened locally with Notes or Domino 5. This is working as designed and is a consequence of upgrading the internal format of the unread table storage. The upgrade happens regardless of the NSF file's ODS version.

When Notes and Domino 6 opens a database locally, it automatically converts the unread mark storage to an improved format. However, if the same database is later opened by R5 Domino or Notes, it won't be able to recognize this new format, and will discard the database, which effectively causes unread marks to reset. This only happens when opening a database locally.

If a Notes 6 or Notes 5 client accesses the database through an R5 server, the internal format is preserved. If a Notes 6 or Notes 5 client accesses the database through a Domino 6 server, the internal format is upgraded, but both versions of the client will still be able to read and set the unread marks appropriately as long as the server version is Domino 6 or later. If the server version is downgraded to R5, the R5 server won't be able to understand the unread mark storage format and will reset the unread marks.

Case and accent sensitivity in view sorting

In R4, the view column properties "Case-sensitive sorting" and "Accent-sensitive sorting" meant if two strings were the same, without regard to case or accent, then the case and accent would be used to try to differentiate them. This meant that most of the time, cas- and accent-sensitive sorting was not used.

In R5 & Notes 6, the two properties mean to sort with regard to case and accent all the time. This is fundamentally different than it was for R4. For this reason, an R4 database converted to an R5 or later database defaults to not having the properties selected.

When the case-sensitive sorting is set to “on” in Domino R5 or Domino 6, the word “dog” sorts before “Cat”, as lower case letters are sorted before uppercase letters. In R4 this would be the opposite, no matter whether the setting is on or off.

When the accent sensitive sorting is set to “on” in Domino R5 or Domino 6, the word “ääni” sorts before “aalto”, as accented letters are sorted before non-accented letters. In R4 this would be the opposite, no matter whether the setting is on or off.

2.2.4 Mail interoperability

If Norton Lotus Notes Virus Protection is configured on a client to hook database open calls, then encrypted S/MIME mail will appear to be unencrypted when it is opened.

2.2.5 Administrator client

Following are interoperability issues relating to using extended ACLs in an environment that includes Release 5 servers and clients.

- ▶ You must use a Notes 6 client to set Extended ACLs, and you must set the Extended ACLs on a directory database on a Domino 6 server.
- ▶ You can use Extended ACLs in a mixed-release environment. To replicate changes from a Domino 5 server to a Domino 6 server, the Domino 6 server must pull the changes from the Domino 5 server.
- ▶ During Domino 6 to Domino 5 replication, the Domino 6 server only replicates to the Domino 5 server the database contents that the Extended ACLs allows the Domino 5 server to access.
- ▶ Lotus Domino 5 servers and earlier releases do not enforce Extended ACL rules.
- ▶ R4.x, R5.x and Lotus Notes 6 clients respect extended ACL restrictions set on directory replicas on a Lotus Domino 6 server.

2.2.6 Template interoperability

This section describes some known interoperability issues when migrating databases created with a TeamRoom template.

- ▶ Migrating TeamRoom 4.1 to TeamRoom(R6) must go through TeamRoom(R5)

If you have a TeamRoom database that is based upon the TeamRoom 4.1 template, you need to replace the design with TeamRoom(R5) and run the conversion utility *before* replacing the design with a TeamRoom(R6) design.

► TeamRoomR6 alternate name support when migrating from TeamRoom(R5)

TeamRoom(R6) supports the use of Alternate Names. However, when a TeamRoom(R5) is updated to the Notes/Domino 6 design, the existing documents do not automatically generate alternate names (because the information was not saved when the document was created). Therefore, existing documents need to be opened and resaved by the author before alternate name information can be displayed for the document. Any new documents created after the design update will automatically contain the alternate name information where available and appropriate. If you have a large number of documents, consider writing an agent which automates the task.



Upgrade considerations for Notes clients

Rolling out the client for a product is usually the most time consuming and expensive part of an upgrade. In this chapter we describe the issues which should be considered prior to beginning a rollout. This will help you avoid some pitfalls and unnecessary crises. We also describe the ways in which the new Notes/Domino 6 environment can reduce the time and expense of this part of the upgrade.

This chapter deals with planning; the actual steps for performing the client upgrades are in Chapter 7, “Lotus Notes client upgrades” on page 117.

3.1 Training

One of the goals of the Notes 6 client design was to reduce the amount of training needed by end users after the upgrade. Users of the R5 client should have very little difficulty making the transition to the Notes 6 client. The help desk will not be overwhelmed by calls from users new to the Notes 6 client.

The easiest way to inform your users about new features is to have a central database with tips in it. Using the new policy-based administration you can push out a bookmark to this database to make access easier for your users. A Web site may also work well in this scenario. Companies that have already deployed the Notes 6 client have discovered that they can avoid the costs of distributing training materials by using these centralized online methods.

If you have Sametime in your environment, consider setting up Sametime Meetings for training purposes. Your users can attend the meetings from their own PCs so you avoid many of the costs associated with classroom teaching (for example, travel).

We strongly recommend that users who are moving from an R4 environment to Notes 6 be given training on the new client because the client and most of its functions went through a major redesign with R5 and this has been further refined with Notes 6. If you are upgrading from R4, a training plan for your users should be included in the upgrade plan.

3.2 Workstation requirements

Always check the recommendations for hardware and OS levels in the release notes of the version you are installing. Notes 6 has space requirements that are very similar to the ones R5 had. Generally speaking, the hardware that is sufficient for running the R5 client should be able to run the Notes 6 client.

Note: If the user has a local mail file, upgrading it to the Mail 6 design will increase the size of it by about 10 MB.

The workstation requirements are listed in 7.1.1, “Determine the hardware and OS level of each machine” on page 118.

3.3 Calendaring and scheduling considerations

Notes users who have delegated their calendar or mail to another individual should be upgraded at the same time as that individual. We have seen this most frequently in the case of an executive who has delegated his or her calendar to an executive assistant. If it is absolutely necessary to upgrade them at different times, be sure to upgrade the assistant first so that they will always be able to access the executive's mail file (a Notes 6 client can access R5 and R4 mail files). In the case of a group of users who are sharing their calendars through delegation an effort should also be made to upgrade them simultaneously.

For more detailed information refer to 2.2.1, "Client/mail template interoperability" on page 10. That section describes what functionality is available with different versions of clients and mail files.

3.4 Upgrading the client before upgrading the server

We recommend upgrading the servers before the clients because the interoperability options are stronger with that route, and you can start taking advantage of the many improvements available in Domino 6 server. That said, it is entirely possible to upgrade clients before servers. Users can take advantage of the benefits of the Notes 6 client right away, particularly if they have local replicas of their mail files (see 3.6.1, "Mail file replicas (non-clustered)" on page 21 for the correct way to configure this).

Table 3-1 Client/Server functionality matrix: R5 and Notes & Domino 6

Client/Server	R5 Domino Server	Domino 6 Server
R5 Client with R5 mail template	works	works
Notes 6 Client with R5 mail template	works	works
Notes 6 Client with Notes 6 mail template	not supported*	works
R5 Client with Notes 6 mail template	not supported*	Mail functions work, C&S is limited. No new features are available, including preferences

A more detailed interoperability table is available in the "Lotus Notes 6 mail file template interoperability" section of the Lotus Domino 6 Administrator Help database.

***Note:** In our experience, you can put a Notes 6 mail file on an R5 server and have basic mail functionality, although some advanced features are not available with this configuration. However, this configuration is not recommended, has not been tested, and is not supported by Lotus.

3.5 A Word about On Disk Structure

One thing that you should be aware of is that the Domino 6 server and Notes 6 client use a different On Disk Structure (ODS), or database format, than previous releases. You can determine the ODS of a database by looking at the information tab of its properties:

- ODS 20 = Release 4.6
- ODS 41 = Release 5.x
- ODS 43 = Notes/Domino 6

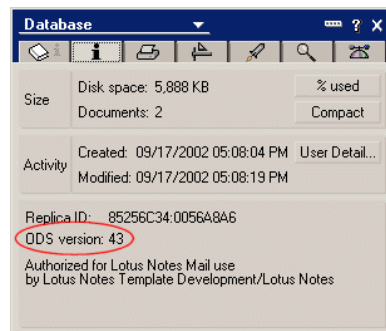


Figure 3-1 ODS version

You can also use the Domino Administrator client to look at the files on the server:

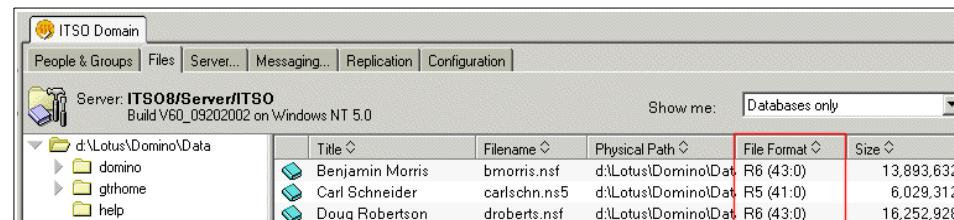


Figure 3-2 Finding a database's ODS with the Administrator client

ODS is basically a transparent feature. Different ODS levels do not cause any problem because ODS has to do with the way in which the server or the client writes the information to the physical disk. It does not affect the interaction between the server and the client. An R4, R5, or Notes 6 client can access the same database on a server, no matter what ODS level the database has. ODS only has to do with the way in which the server or client interacts with its own hard drive. ODS does not replicate either.

The ODS is also unrelated to the design of a database. A database will receive design updates from a template even if they have different ODS levels. Two database replicas on different servers (with different ODSs) replicate with no problem.

The only time ODS may cause a problem is if you copy a database with a higher level ODS at the operating system level (not recommended, but we know people do it) and then attempt to access it with an earlier release of the client or server. Even then you can work around this problem by creating a new replica of the database (using a Notes 6 client) and naming it with an ns4 (for R4.6) or ns5 (for R5) extension, which will give it the desired database format.

Some Notes/Domino 6 design features require ODS 43. For example, the ability for quota management based on the amount of data in a mail file instead of the total file size can only be implemented if the server is Domino 6 and the mail file has the new design and ODS.

For further information about ODS and how to upgrade the ODS level as well as how to revert back to earlier versions, see 5.8, "Introduction to the new On-Disk Structure (ODS)" on page 68.

3.6 Mail files

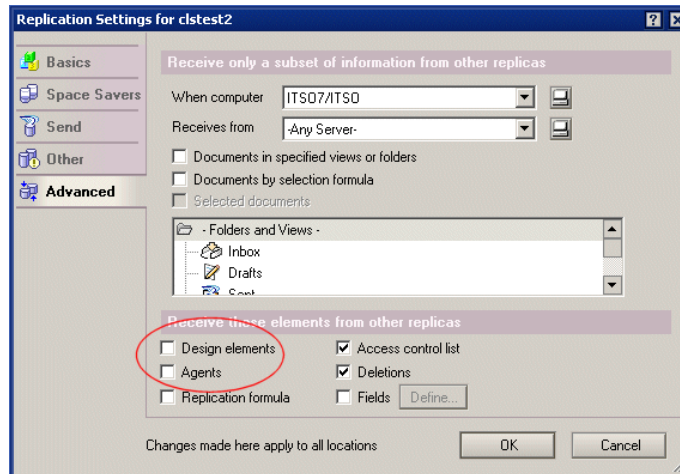
The following sections refer to R4.6 mail files, R5 mail files and Notes 6 mail files. By that we are indicating the mail file template used to create the mail file. A 4.6 mail file is based on the standard R4.6 mail template. An R5 mail file is a mail file based on the design of the mail50.ntf template, and a Notes 6 mail file is a mail file based on the design of the mail6.ntf template.

3.6.1 Mail file replicas (non-clustered)

A Notes 6 mail file does not work properly on a Domino 4.6 or Domino 5 server. You also want to ensure that the older Notes 4.6 design does not overwrite the design of the Notes 6 mail file on the Domino 6 server. To prevent the designs of the two replicas from replicating, do the following *for each mail file*:

Disable design replication on server replicas

1. In the Administrator client navigate to the mail file in the Files.
2. From the menu select File -> Replication -> Settings.
3. Click the Advanced tab.
4. Under “Receive these elements from other replicas” clear the “Design elements” and “Agents” check boxes.



5. Click OK.
6. Repeat Steps 1 to 5 for *each replica* of the mail files. Because disabling replication is a database property, it is not replicated.

Disable design replication on local replicas

1. Open the mail file with the Notes 6 client.
2. From the menu select File -> Replication -> Settings.
3. Click the Advanced tab.
4. Under “Receive these elements from other replicas” clear the “Design elements” and “Agents” check boxes.

Note: This procedure does not work for clustered servers and databases because cluster replication ignores selective replication.

3.6.2 Mixed-release cluster and mail file replicas

In a mixed-release cluster, users cannot have a Notes/Domino 6 mail file on Domino 4.6 or Domino 5 servers—the Notes/Domino 6 mail template does not work properly on these releases. If you have a mixed-release cluster with mail files, either:

- ▶ Use the Notes/Domino 4.6 or Notes/Domino 5 design for mail files.
- ▶ Place users' mail files with Domino 4.6 design only on Domino 4.6 servers; those with Domino 5 design on Domino 5 servers only; and those with the Domino 6 design on Domino 6 servers only.

Do not mix mail file templates. Because cluster replication ignores selective replication formulas, you cannot rely on it to preserve the design of mail files.

3.6.3 Customized mail templates

Many organizations have made modifications to the R5 mail template. A list of these changes should be compared to the standard Notes 6 mail template. It is quite possible that many of the modifications made to the R5 mail template by an organization have been incorporated into the new Notes 6 mail template. Once the developers have compared the customized R5 mail template to the new Notes 6 mail template they should implement any required modifications to the standard Notes 6 mail template. This is a good time for the organization to review the need for mail template modifications. Lotus does not recommend that organizations modify the mail template.

3.6.4 Using seamless mail upgrade to upgrade mail files

You can use a new feature in Notes/Domino 6 called “seamless mail upgrade” to automatically upgrade the mail files of your users when their clients get upgraded. In order to do this you must do the following *before* you start upgrading their clients:

- ▶ Upgrade the Domino Directory and their mail server to Domino 6. See Chapter 5, “Domino Directory upgrade” on page 37 and Chapter 6, “Domino Server upgrade” on page 75 for details.
- ▶ Remove setup profile settings from your users' person documents in the Domino directory.
- ▶ Create a desktop settings document specifying the appropriate client level and mail file templates.
- ▶ Create a policy specifying the desktop settings document created for this.
- ▶ Apply the policy to your users. See Chapter 15, “Policy-based administration” on page 449 for detailed information about policies and how to use them.

- Start upgrading clients.

The client notifies the server of the client upgrade at the time of the upgrade. If you set this up after the client has been upgraded, the notification will not occur and the mail file will not be upgraded automatically. For detailed instructions concerning seamless mail upgrade, refer to 7.4.3, “Seamless mail upgrade” on page 141.

Note: If your mail servers are in a clustered environment and you want to use seamless mail upgrade, be sure to upgrade all the members of the cluster before upgrading the clients.

3.7 Notes 6 client with R4.6 and R5 applications

Lotus Notes/Domino 4.6 and Notes/Domino 5 applications should function unchanged under Lotus Notes/Domino 6. However, it is essential that you test important applications in a lab environment before upgrading mission-critical production applications to Lotus Notes/Domino 6 in a production setting. Sophisticated applications require careful testing because potential issues may be subtle or not easily evaluated.

Create a list of the key features and functions in your applications and evaluate their functionality under Lotus Notes/Domino 6. Apply any Notes/Domino 6 templates and the Notes/Domino 6 format to applications. Be careful to document and test the following:

- Custom changes you have made to standard templates. Notes/Domino 6 templates may incorporate the functionality you added, making custom changes unnecessary, or may have changed how the feature you are using works.
- Reuse of template code. If you duplicated standard template code (such as LotusScript or @commands) in your applications, be aware that changes in how this code functions in templates will also be reflected in how your application works.
- Use of undocumented features or settings. You may have used features, commands, or items in Notes that are undocumented and unsupported. While these items may have worked in earlier releases, they might not in Lotus Notes/Domino 6.
- Creative workarounds. You may have implemented coding or design changes to overcome a limitation in earlier releases. These workarounds may no longer be necessary in Lotus Notes/Domino 6, or functionality changes could change how the workarounds operate.

Be certain to test your applications thoroughly under conditions that mirror production use of the applications.

3.8 Policy-based administration

It is easier to support a Notes environment that has standards for client configuration. Notes and Domino 6 help you achieve such standardization through policies which can control the Notes client desktop, security, setup, and archiving. These policies can be applied with a great deal of granularity so that you can address the variety of situations in your organization. Prior to upgrading clients it is wise to think about how you intend to administer the client environment in the future.

See Chapter 15, “Policy-based administration” on page 449 for detailed information about policies, how the policies work, and how to use them.

3.8.1 From R5 user profiles to Notes/Domino 6 policies

In previous releases of Lotus Notes/Domino, you configured “Setup Profiles” to set workstation defaults. Notes/Domino 6 has greatly improved on the idea of setup profiles by implementing policy-based administration. Lotus Notes/Domino 6 continues to support setup profiles for backwards compatibility. However, if you choose to implement policies, be aware of the following:

- ▶ Setup profiles in a Person document override policies. In order to implement policies you will need to disable setup profiles in the Domino directory's person documents. A simple agent which clears the contents of the setup profiles field in the person documents will do the trick.
- ▶ The setup, desktop, and security settings documents are supported only by Lotus Notes 6 clients.
- ▶ Registration settings documents have virtually no effect on Lotus Notes 5 and earlier clients. For example, you can have an organization-wide policy that standardizes password strength, internet password setup, mail file owner access, create file in background, internet domain, ID file location upon creation, certificate expiration date, and database quotas. The R5 Administrator client will not recognize any of those settings from a registration settings document and instead will apply the settings from its own domadmin.nsf which is configured individually on every R5 Domino Administrator client. More registration settings can be pre-configured through a Notes 6 policy than was possible with R5 registration preferences. Plan to use the Domino 6 Administrator client for creating new users as soon as you have upgraded your Domino directory.

3.8.2 New possibilities with dynamic configuration

The Notes 6 client is dynamically configured. Each time it authenticates with its home server it checks for updates to policies which have been applied to the account which is logging in. The next time the client authenticates with the server the new policies are enforced.

- ▶ **Workstation security - ECLs:** Before upgrading Notes, the domain administrator may want to set the Administration Execution Control List (ECL) in the Domino Directory. The Administration ECL sets the default security on the Notes client when users start Notes for the first time after they upgrade. Workstation security defines which group's applications can execute on a Notes client. If a group is not specified in the ECL for a client, Notes warns the user when an application created by the group attempts to run on that client. For more information about workstation security, see 10.2, "Workstation security" on page 323.
- ▶ **Welcome page administration:** You can control the look of the Lotus Notes client by configuring a customized welcome page for the organization as a whole, or for smaller groupings of people in the organization (for example, by OU or by group). Welcome pages can be configured and controlled centrally instead of by the local client. You do this through the desktop settings in the policy-based administration. By customizing the welcome page you may be able to ease the transition to the Lotus Notes 6 client. For example, you could push out a bookmark to a discussion database or a Web site with tips on using the new client. For more information about distributing corporate welcome pages, see 16.3, "Corporate welcome pages" on page 494.

3.9 Client upgrade options

This section introduces the different Notes client upgrade options.

3.9.1 Upgrade by mail

Upgrade by mail is an e-mail notification system that notifies users to upgrade their Notes clients and mail file templates to the Notes/Domino 6 design. Upgrade by mail requires that you copy all installation files to a network file server or a shared directory that users can access. In the upgrade notification, you specify the path to SETUP.EXE. The notification message includes buttons that users click to launch the Lotus Notes 6 installation program and to replace the design of their Notes mail file. Use Upgrade by mail to upgrade Notes 4.6 and Notes 5 users to Lotus Notes 6.

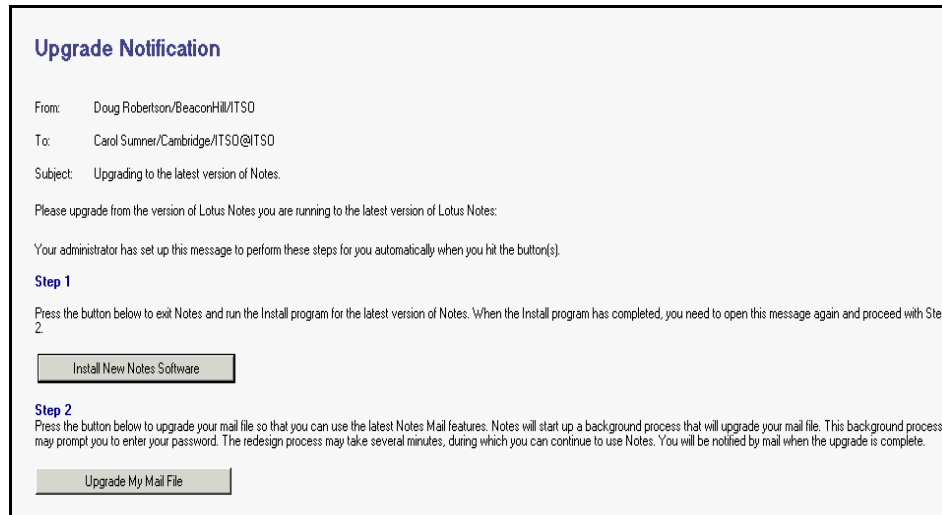


Figure 3-3 Sample upgrade by mail message to end user

The advantage to this system is that users can determine an opportune time for these upgrades. The disadvantage is that administrators cannot control when the client upgrades or mail file design upgrades will occur, although they can configure the upgrade notification system to notify them when a user has completed the steps. Administrators can also look in the Domino Directory to determine who has or has not been upgraded

For step-by-step instructions on configuring upgrade by mail see chapter Chapter 7.3.4, “Configuring Upgrade-by-mail” on page 130.

3.9.2 Smart upgrade

Lotus Notes Smart Upgrade is a system for updating the Notes client code automatically. *It only works with the Notes 6 client*, for example, to upgrade from Notes 6.0 to Notes 6.01. It is not applicable for R4.6 or R5 to Notes 6 upgrades, nor within R5 codestream, for example from 5.0.11 to 5.0.12.

After Smart Upgrade has been configured, the user is notified when their client needs to be updated. The administrator can set a grace period for the user to allow the upgrade, after which time the client will be upgraded no matter how the user responds to the prompt.

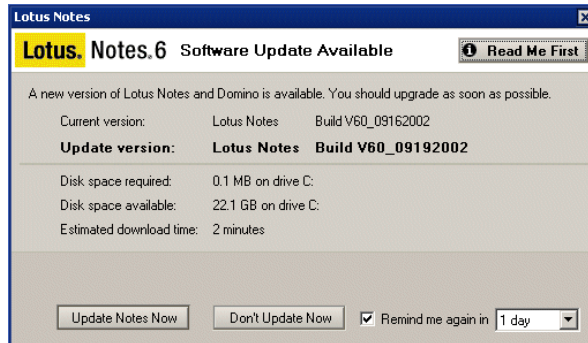


Figure 3-4 Client update notification

3.9.3 Manual upgrade

You can upgrade a client on a workstation by simply installing the code from the CD or a network location. Section 7.3, “Install the Notes 6 client” on page 122 gives detailed instructions concerning the client upgrade. Even with manual upgrades you may want to smooth the process by standardizing the installations through the use of Windows Installer Technology. Detailed instructions for creating transform files is available in 16.1.3, “Customizing client installations with transform files” on page 476.

3.9.4 Third-party deployment options

Application management tools provide methods of pushing client code to a workstation. Network operating system providers like Microsoft (Systems Management Server) and Novell (Zenworks) have their own products for this. In addition there are companies that specialize in application deployment solutions. A simple search on the Web for “application deployment” will give you a number of options. Wolcott’s Application Deployment Toolkit (ADT) specializes in Lotus Notes deployments. You can find more information about this toolkit at

<http://www.wolcottgroup.com>

In combination with the ability to customize installations through Windows Installer Technology and the seamless mail upgrade, it is possible to upgrade your Notes client environment with very little “hands on” intervention.



Upgrade considerations for Domino servers

This chapter covers many important factors you should consider when planning a Domino R5 to Domino 6 upgrade of your Domino server infrastructure.

It concentrates on topics related to planning, and considerations that affect most Domino architectures, independent of size, hardware, or operating system used. We also describe the ways in which the new Notes/Domino 6 environment can reduce the time and expense of this part of the upgrade.

4.1 Server requirements

Always check the recommendations for hardware and OS levels in the release notes of the version of the Domino server you are installing. In general, hardware that is running the R5 servers properly should be able to run the Domino 6 servers.

IBM early deployment, the Lotus Developer Domain, and the early deployment customers have experienced better performance results with Domino 6 on the same hardware that was used for Domino R5. The individual results depend on the hardware you use for your environment.

The Domino 6 server licensing program has changed; make sure you have purchased the correct licenses before installing the servers. To learn more about new Domino server licensing programs, refer to 2.1, “Server and client licensing” on page 8.

4.2 Restructuring your environment

While you are preparing for a Domino infrastructure upgrade, it is a good idea to take the opportunity to consider rearchitecting your environment. New, advanced Domino capabilities might help you to design and built an even more structured and secure environment.

Also plan to clean up your Domino environment, since a clean and structured environment will help you to perform the migration more easily and results in a better performing Domino 6 environment.

See Chapter 16, “Administering the Notes 6 client” on page 469 for detailed information on Domino 6 features and capabilities, and how to administer them.

Consolidation or centralization of your Domino environment is one of the possibilities that might be appropriate since this can lower your total costs and administration efforts. Domino 6 now includes network compression, and features like fault tolerance, transactional logging, fault recovery, clustering and partitioning have been improved to make a scalable consolidation more viable.

See Appendix A, “Consolidation” on page 523 for a general discussion of how Domino 6 can help you consolidate your environment.

4.3 Upgrade sequence

Upgrading a Domino system in an organized process will minimize work and avoid disrupting users. Therefore, thorough planning and preparation for the upgrade process is highly recommended.

The following upgrade sequence, recommended by Lotus/IBM, has been used in IBM's internal early deployment and for many early adopter customers. These steps apply for most Domino environments, for upgrading both small and large Domino R4 and R5 environments into Notes and Domino 6.

Recommended upgrade path

1. Upgrade the Administration server and Administrator clients.
2. Upgrade the Domino Directory.
3. Upgrade Hub servers.
4. Upgrade Mail servers.
5. Upgrade Application servers.
6. Upgrade Notes clients.
7. Upgrade applications and databases.
8. Upgrade to the new ODS.
9. Steady state (performance tuning and optimizing your environment).
10. Utilization of new features.

The upgrade steps are discussed in detail in later chapters of this book. Refer to the individual chapters for more information.

Note: By upgrading servers before clients, and servers and clients before applications, you minimize disruption to users and to business activities.

Users do not see Lotus Notes/Domino 6 features until their clients can utilize them; conversely, users don't attempt to take advantage of Lotus Notes/Domino 6 features until their servers can handle them. Yet you as an administrator, as well as your Domino infrastructure, benefit from Domino 6 server upgrades before client upgrades.

4.4 Install and configure new Domino 6 features

Before starting the upgrade process, you need to decide if you want to implement new Domino 6 features, and then determine which of the features are to be implemented. We think that implementing new Domino 6 features can improve your Domino infrastructure, but you can only take advantage of these features by planning your changes thoroughly.

When you have to guarantee a highly available Domino infrastructure, you may consider first upgrading the environment to Domino 6, and then implementing newly introduced features. Consider establishing a “steady state” after the upgrade process, meaning that you make sure your environment is stable, before you start planning the implementation of new features.

Some options will help you to perform the upgrade; consider implementing them during or right after the upgrade process. Plan to implement the following features early so that you take advantage of them during the upgrade:

- ▶ Policies model for registering new users, desktop management, and security additions. See Chapter 15, “Policy-based administration” on page 449 for details.
- ▶ Seamless mail upgrade, which is actually part of the Policies model, helps you upgrade your Notes clients. See 7.4.3, “Seamless mail upgrade” on page 141 for details.
- ▶ Monitoring and performance measuring features. Chapter 8, “Monitoring your infrastructure” on page 149 discusses these in detail.

4.5 Server upgrade options

You do not need to be at a specific release level to upgrade to Notes and Domino, but the upgrade path will be easier when you are running all servers on Domino R4.6.7a. Nevertheless, the upgrade path from R4.x servers is supported by Lotus.

Note: We advise you to upgrade all current R4.x servers to release 4.6.7a before upgrading to Domino 6.

See Chapter 6, “Domino Server upgrade” on page 75 for instructions and discussion about upgrading the server.

4.6 Directory and ODS upgrade

The upgrade of the Domino directory and the upgrade of the on-disk structure is an important step during the upgrade process. Whereas in R4 to R5 upgrades this process was very critical, you will find the Domino 6 directory more compatible with your R4 and R5 servers. Nevertheless, make sure that you know exactly what happens during the Directory upgrade and that you control the process.

The detailed steps for upgrading the Domino Directory to version 6 are in Chapter 5, “Domino Directory upgrade” on page 37.

4.6.1 ODS upgrade

Significant architectural changes were made to the database on-disk structure in Domino 6. The new ODS enables you to use new features like attachment LZ1 compression, view logging, the Single Copy template, and many more options.

Upgrading the ODS of your databases is an important step in the Notes and Domino 6 upgrade plan, and may even be a time consuming factor since you upgrade with the Domino Compact server task.

The following upgrade paths can be used to upgrade to the new ODS:

- ▶ Compacting the complete server during your upgrade process
- ▶ Compacting only your system databases during the upgrade process, and running an off-line compact command later for the remaining database
- ▶ Scheduling a program document which will trigger a compact during off-hours

We recommend that you upgrade to the new ODS after all servers have been upgraded to prevent data and functionality losses that are visible by your users.

Note: The ODS does not replicate with your database, and ODS level is completely unrelated to the database design.

The ODS and the ODS upgrade process is described in detail in 5.8, “Introduction to the new On-Disk Structure (ODS)” on page 68.

4.6.2 Domino Directory design upgrade

In a Lotus Domino infrastructure, the Lotus Domino Directory is the most important database. Therefore, it's very important to give attention to your upgrade process for this database and be sure that you are using the appropriate methodology.

The new Domino Directory version 6 design contains a lot of changes and improvements that introduce some new capabilities, but it is still backward compatible. This allows you to approach the upgrading of the design of the Domino directory at any time in this process, as long as you make sure that this is a controlled process. Chapter 5, “Domino Directory upgrade” on page 37 discusses all the details of the Directory upgrade, including how to upgrade the Domino Directory design.

You should use, at minimum, Lotus Domino R4.6.7a release level servers in your environment to avoid any UNK table issue when you try to replicate your Lotus Domino Directory freshly upgraded to the 6 design. More details about this issue are in 5.4, “UNK table in a mixed environment” on page 52.

Organizations that use a customized Domino directory should review the design changes in the current template and see if their customizations are still needed in the Domino 6 design. If so, create the necessary design changes in the new Domino directory template. Customizing the Domino Directory design, like any template designs that ship with Domino 6, is generally not a good idea, nor is it recommended or supported by Lotus. Try to avoid this if you can.

Also, when you use more directories, like Extended catalog, Condensed Directory catalog, Secondary directory or Cascaded directories, you should consider using the new features that Domino 6 provides. See 5.6, “Secondary directories” on page 60 for details.

4.7 Coexistence or interoperability

Lotus Domino 6 servers can coexist in a mixed environment with Domino R5 and Domino R4 servers and are fully backwards compatible for mail and applications. Databases that exist on these Domino server levels can replicate and interact, but with the caveat that on-disk structure levels do not replicate.

Since Domino 6 design elements cannot be read by the Domino R4 and R5 server, it is recommended that a Domino 6-designed database should reside on a Domino 6 server so users can take advantage of the new design features.

Important: Lotus supports mixed environments, but strongly advises customers to use only Notes and Domino R4.6.x releases; R4.6.7a is preferred.

4.7.1 Lotus companion products

Before you upgrade a Domino server on which you run one of the companion products, like Lotus Sametime or Lotus QuickPlace, make sure that the other Lotus product supports Lotus Domino 6.

If you use any Lotus companion product in your environment that shares the same Domino Directory (namely, Sametime or Quickplace) and you want to retain an R5 design for these servers, you could prevent any design changes by changing the replication setting for the replica of the Domino Directory which is on these targeted servers. This is described in detail in the next chapter.

Check the Release Notes of specific companion products for information on interoperability with Domino 6.

4.7.2 Third party products

Upgrading to Domino 6 requires that the third party products you are using are compatible. Take a look at the following list and try to identify if you have third party solutions in your infrastructure that need to be compatible with Domino 6 to ensure a properly working environment:

- Anti-virus software
- Fax software
- Custom, in-house, or business partner built applications
- Specific backup and restore agents and software
- Specific messaging and calendaring applications
- Specific monitoring and system management applications
- User management and archiving applications

See the documentation and the Web sites for respective third party vendors to determine whether their products support Domino 6.

Depending on the size and complexity of your environment, this list might not be complete. Section 7.1, “Preparation: Know your environment” on page 118 describes how to audit your environment to define all the third party products and Lotus companion products.

Note: Do not upgrade your environment before you have a compatibility confirmation from your third party software vendor or ISV.



Domino Directory upgrade

In a Lotus Domino infrastructure, the Lotus Domino Directory is the most important database. From this database Lotus Domino can build its mail routing table, get information for scheduling replications, provide information about groups and registered people, provide authentication, just to mention a few of its important uses. Therefore, it is crucial to give your best attention to the upgrade of this database and be sure that you are using the appropriate methods.

There are some added features and some changes in the new release of Domino Directory template. The user interface of the directory has also been enhanced, and framesets have been introduced to provide better end-user and administrator usability.

In this chapter we introduce the new functionality of the Domino Directory 6 and we describe the methods you can use to get your Lotus Domino Directory upgraded smoothly, without causing damage for your infrastructure.

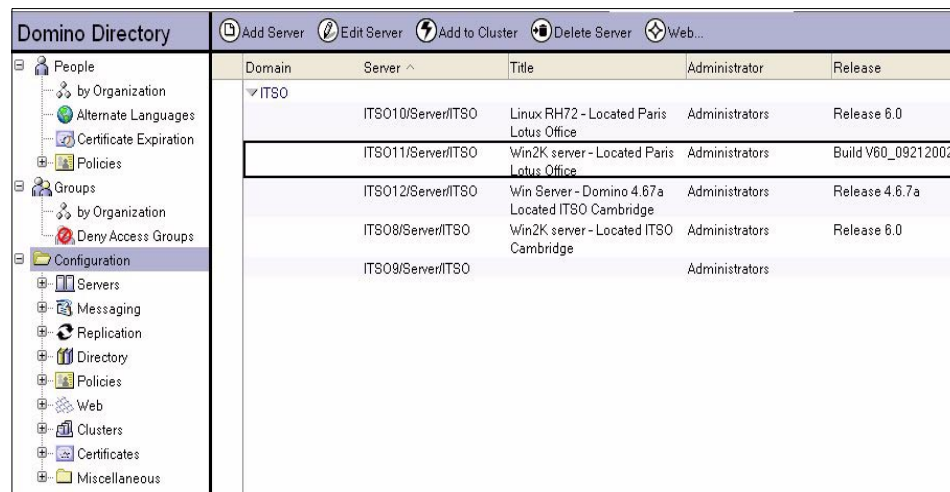
5.1 Introduction to the new design

Domino Directory in Lotus Domino 6 contains a lot of improvements brought about by changes to some existing functions, and the introduction of some new capabilities. For a detailed description of the new features and changes see the document “New Domino server and Domino Administrator client features” in the Domino Administrator 6 Help database. You can also refer to Chapter 14, “Extended ACL” on page 431 for detailed discussion about the new Extend ACL functionality.

In this section we focus on some key areas in the new design, which can have an impact during your upgrade process. The Domino Directory has been redesigned to allow more control over your infrastructure and better delegation of administration privileges. In particular, many changes have been made to the Server and Configuration form of the Domino Directory, so we discuss these items in detail.

5.1.1 The Domino Directory user interface

The Domino Directory user interface has been redesigned to resemble the look and feel of the Domino Administrator 6 client; the same framesets, icons, and color themes were used for a consistent look and feel, and ease of use. See Figure 5-1.



The screenshot shows the Domino Directory application window. On the left is a navigation pane with a tree view containing categories like People, Groups, Configuration, and Miscellaneous. The 'Configuration' category is selected, and 'Servers' is highlighted. The main area displays a table of servers. The table has columns for Domain, Server, Title, Administrator, and Release. The data is organized under an expanded 'ITSO' domain.

Domain	Server	Title	Administrator	Release
ITSO	ITS010/Server/ITSO	Linux RH72 - Located Paris Lotus Office	Administrators	Release 6.0
	ITS011/Server/ITSO	Win2K server - Located Paris Lotus Office	Administrators	Build V60_09212002
	ITS012/Server/ITSO	Win Server - Domino 4.67a Located ITSO Cambridge	Administrators	Release 4.6.7a
	ITS08/Server/ITSO	Win2K server - Located ITSO Cambridge	Administrators	Release 6.0
	ITS09/Server/ITSO		Administrators	

Figure 5-1 New outline view from Domino Directory

5.1.2 Server form

The server form contains some new features, which are distributed across the different tabs.

Basic tab

You can now define whether your server is a Primary Domino Directory or a Configuration Domino Directory.

Directory Information	
Directory assistance database name:	
Name of condensed directory catalog on this server:	
Trust the server based condensed directory catalog for authentication with internet protocols:	<input type="checkbox"/> Yes
Directory Type:	Primary Domino Directory
Allow this directory to be used as a remote primary directory for other servers:	<input checked="" type="checkbox"/> Yes

Figure 5-2 Primary / configuration Domino directory

Fault recovery settings can be defined directly at this level.

Fault Recovery	
Fault Recovery:	<input checked="" type="checkbox"/> Enabled
Cleanup Script Name:	/opt/lotus/notes/latest/linux/nsd.sh -batch
Cleanup Script Maximum Execution Time:	300 seconds
Maximum Fault Limits:	3 faults within 5 minutes
Mail Fault Notification to:	Administrators

Figure 5-3 Fault recovery settings

Security tab

This tab provides new Administration delegation settings.

Administrators	
Full Access administrators:	<input type="checkbox"/> SuperAdmin
Administrators:	<input type="checkbox"/> Administrators
Database Administrators:	<input type="checkbox"/> DatabaseAdmins
Full Remote Console Administrators:	<input type="checkbox"/> RemoteAdmins
View-only Administrators:	<input type="checkbox"/> ViewOnlyAdmins
System Administrator:	<input type="checkbox"/> SystemAdmins
Restricted System Administrator:	<input type="checkbox"/> RestrictedSysAdmins
Restricted System Commands:	<input type="checkbox"/>
Administer the server from a browser (pre-Notes 6 servers only):	<input type="checkbox"/>

Figure 5-4 Administration delegation

New programmability choices were introduced by the new Agent Manager behavior.

Programmability Restrictions	Who can -
Run unrestricted methods and operations:	
Sign agents to run on behalf of someone else:	
Sign agents to run on behalf of the invoker of the agent:	
Run restricted LotusScript/Java agents:	
Run Simple and Formula agents:	
Sign script libraries to run on behalf of someone else:	
Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.	
Run restricted Java/Javascript/COM:	
Run unrestricted Java/Javascript/COM:	

Figure 5-5 Programmability settings

From the server access menu, you can now specify who can create new templates and who can create master templates, and define a list of trusted servers which will be used to allow remote agents to work against trusted servers.

Server Access	Who can -
Access server:	All users can access this server
Not access server:	
Create databases & templates:	
Create new replicas:	
Create master templates:	
Allowed to use monitors:	*
Not allowed to use monitors:	
Trusted servers:	

Figure 5-6 Accessibility options

Ports tab

- There is a new feature called Remote Debug Manager, which allows a developer to remotely debug agents that he has created (for more detail, refer to *Domino Designer 6: A Developer's Handbook*, SG-24-6854).

Basics	Security	Ports	Server Tasks	Internet Protocols
Notes Network Ports				
Internet Ports				
Proxies				
SSL settings				
SSL key file name:		keyfile.kyr		
SSL protocol version (for use with all protocols except HTTP):		Negotiated		
Accept SSL site certificates:		<input type="radio"/> Yes <input checked="" type="radio"/> No		
Accept expired SSL certificates:		<input checked="" type="radio"/> Yes <input type="radio"/> No		
Web				
Directory				
Mail				
DIIOP				
Remote Debug Manager				
Remote Debug Manager				
TCP/IP port number:		60000		
TCP/IP port status:		Enabled		
Enforce server access settings:		No		
SSL port number:		60001		
SSL port status:		Disabled		

Figure 5-7 Defining Remote Debug Manager ports

Server tasks tab

If you have defined Remote Debug Manager's port in the previous section, you now have to decide whether to enable it or not from the following configuration table, which can be found under the server tasks tab.

Basics	Security	Ports	Server Tasks	Internet Protocols	MTAs	Miscellaneous	Transactional Logging	Shared Mail	Administration
Administration Process									
Agent Manager									
Domain Catalog									
Directory Cataloger									
Internet Cluster Manager									
Web Retriever									
Remote Debug Manager									
Basics									
Allow remote debugging on this server:		Enabled							
Turnoff Server Debug after:		24 hours of inactivity							
Agent Wait at StartTime:		0 seconds							

Figure 5-8 Configuration menu for Remote Debug Manager

Transactional logging tab

There is a new style for Transactional logging called *Linear*, which allows you to define your own amount of disk space used to create the transaction log. This extends the 4 Gigabytes limit for circular. Linear transactional logging works on a circular mode.

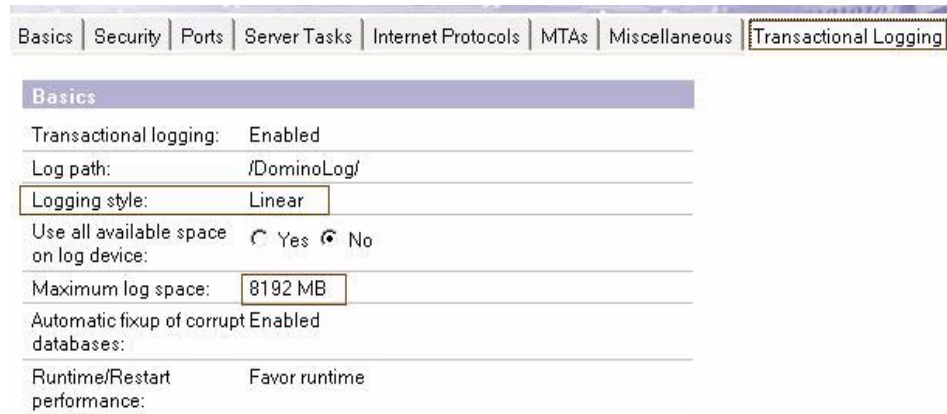


Figure 5-9 Linear mode for Transactional logging

Quota enforcement methods can be selected from the Transactional Logging tab; they work with the router quota delivery option.

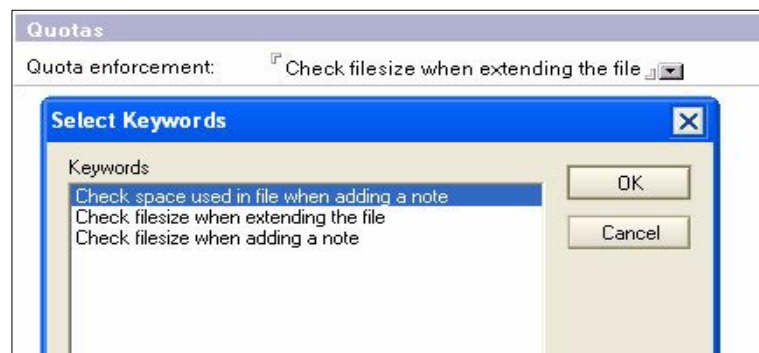


Figure 5-10 Three new quota enforcement methods

Shared Mail tab

In Domino 6, you can have up to ten active shared mail databases on the same server, compared to only one in Domino R5. You can specify the appropriate path for each in order to spread I/O disk operations across all your disk subsystems if you have deployed it.

Basics	Security	Ports	Server Tasks	Internet Protocols	MTAs	Miscellaneous	Transactional Logging	Shared Mail	Administration
Shared Mail									
Shared Mail: Transfer and Delivery									
Directory	Number of Files	Maximum Directory Size	Delivery Status	Availability					
/Domino1/mail1	50	4096 megabytes	Open	Online					
/Domino1/mail2	45	3072 megabytes	Closed	Online					
/Domino2/mail1	50	8192 megabytes	Open	Online					
		megabytes							
		megabytes							
		megabytes							
		megabytes							
		megabyte							
		megabytes							
		megabytes							

Figure 5-11 Single Copy Object Store table

5.1.3 Configuration form

The Configuration form is used by Domino server to define settings in the following areas:

1. Basics
2. Router & SMTP (Simple Mail Transfer Protocol)
3. MIME (Multipurpose Internet Mail Extensions)
4. NOTES.INI
5. iNotes Web Access
6. IMAP
7. SNMP (Simple Network Management Protocol)
8. Activity Logging

Figure 5-13 shows the main difference between the Domino R5 and Domino 6 configuration documents. Notice the highlighted tabs in the Domino 6 document.

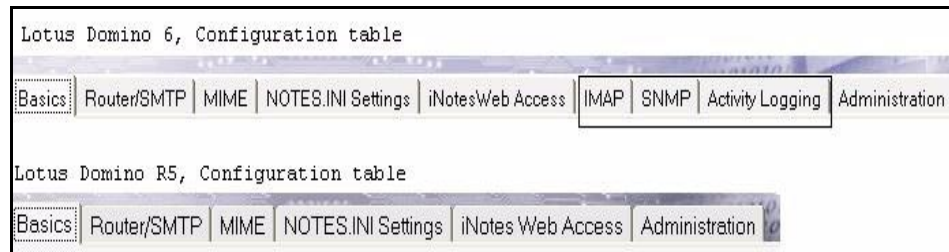


Figure 5-12 Configuration menu in Domino 6 and Domino R5

Some tables within various tabs now include more options to provide a better configuration capabilities. Some of these areas are identified in the next sections.

Basics tab

On the Basics tab you can now include:

- ▶ Specification of the Smart Upgrade database
- ▶ Minimum/Maximum of client level allowed to connect
- ▶ License tracking


Basics Router/SMTP MIME NOTES.INI Settings iNotesWeb Access	
Basics	
Use these settings as the default settings for all servers: <input type="checkbox"/> Yes	
OR	
Group or Server name:	ITSO Servers
Type-ahead:	Enabled
International MIME Settings for this document:	<input type="checkbox"/> Enabled
IMAP server returns exact size of message:	Enabled
POP3 server returns exact size of message:	Disabled
Smart Upgrade Database link:	
License Tracking:	Enabled
Minimum Client Level:	4.6
Maximum Client Level:	6.0.1
Comments:	

Figure 5-13 Basics tab from the Configuration form

Router/SMTP tab

Server-based mail rules can be specified. (See 9.1.1, “System mail rules” on page 210 for details.)

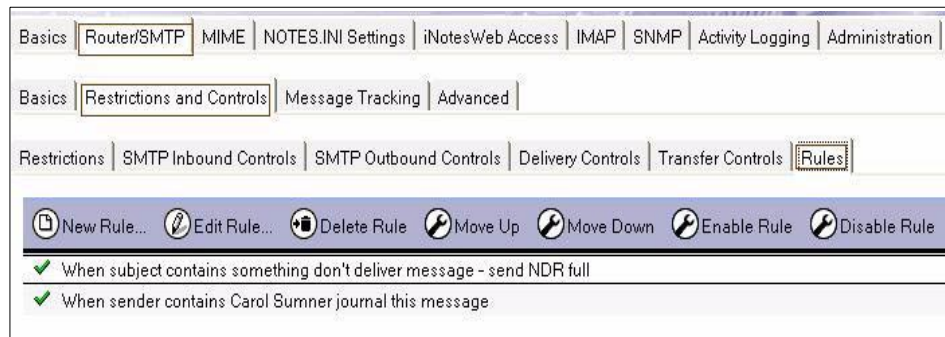


Figure 5-14 Server based mail rules configuration menu

You can control and customize the notification failure message.

Failure Messages	
Failure messages for the <input checked="" type="radio"/> Text file <input type="radio"/> Text conditions below are specified by:	
Transfer failure:	d:\data\message\tranfert.txt
Delivery failure:	d:\data\message\delivery.txt
Message expiration:	d:\data\message\expire.txt
Domain failure:	d:\data\message\domain.txt
Server failure:	d:\data\message\server.txt
Username failure:	d:\data\message\username.txt
Size failure:	d:\data\message\size.txt
Restriction failure:	d:\data\message\restriction.txt
Delay notification:	d:\data\message\delay.txt
Quota warning notification:	d:\data\message\quotawarning.txt
Quota error notification:	d:\data\message\quotaerror.txt

Figure 5-15 Customizable failure messages

Mail Journaling makes it possible for the Domino administrator to store a copy of messages that go through its Mail.box. (See 9.1.1, “System mail rules” on page 210 for details.)

Basics	Router/SMTP	MIME	NOTES.INI Settings	iNotes/Web Access	IMAP	SNMP
--------	-------------	------	--------------------	-------------------	------	------

Basics	Restrictions and Controls	Message Tracking	Advanced
--------	---------------------------	------------------	----------

Journaling	Commands and Extensions	Controls
------------	-------------------------	----------

Basics	
Journaling:	Enabled
Field encryption exclusion list:	Form; From; Principal; PostedDate
Method:	Copy to local database
Database Name:	mailjrn.nsf
Encrypt on behalf of user:	Marcia Robertson/BeaconHill/ITSO
Database Management	
Method:	Periodic Rollover
Periodicity:	1 days

***Reminder: A journaling mail rule is needed to properly enable message journaling.

Figure 5-16 Mail Journaling configuration

Activity Logging tab

Activity Logging is a new tab, which collects information about the activity in your Domino system for IMAP, Notes session, Notes Database, Notes passthru, POP3, and SMTP.

Basics	Router/SMTP	MIME	NOTES.INI Settings	iNotes/Web Access	IMAP	SNMP	Activity Logging
--------	-------------	------	--------------------	-------------------	------	------	------------------

Activity Logging	Activity Trends
------------------	-----------------

Activity logging is enabled: ☒ Yes

Server Activity Logging Configuration	
Enabled logging types:	<input checked="" type="checkbox"/> Domino.Notes.Database <input checked="" type="checkbox"/> Domino.Notes.Passthru <input checked="" type="checkbox"/> Domino.Notes.Session <input checked="" type="checkbox"/> Domino.REPLICA <input checked="" type="checkbox"/> Domino.MAIL
Checkpoint interval:	15 minutes
Log checkpoint at midnight:	<input checked="" type="checkbox"/> Yes
Log checkpoints for prime shift:	<input checked="" type="checkbox"/> Yes
Prime shift interval:	9 AM - 6 PM

Figure 5-17 Configuration of Activity Logging

Activity Trends records and reports statistics about database activity on a server. It is a part of IBM Tivoli Analyzer for Lotus Domino, which is a separate product offering from IBM.

Basics Router/SMTP MIME NOTES.INI Settings iNotesWeb Access IMAP SNMP Activity Logging

Activity Logging Activity Trends

Basics Retention Proxy Data

Activity Trends Basic Configuration

Enable activity trends collector: ☒ Yes

Activity trends collector database path: activity.nsf

Time of day to run activity trends collector: 03:25 AM

Days of the week to collect observations: ☒ Monday ☒ Friday
☒ Tuesday ☒ Saturday
☒ Wednesday ☒ Sunday
☒ Thursday

Activity Trends Data Profile Options

☒ Use defaults

Figure 5-18 Configuration of Activity Trends

Important: Even if you can use the Domino Directory with the new design on a Domino R5 server, you will not be able to use all the new features that can be activated from the new design if the server where you want to use the features is not running Domino version 6. Domino R5 will simply ignore those features.

5.2 Administration delegation possibilities

The Domino Directory design of Lotus Domino 6 gives you the capability to delegate some administrative tasks and allows you more granularity to distribute them among your team. It introduces a new feature called “Full Access Administrators”; all group and people listed in this field will be granted full administrative privileges on all the databases hosted on this server regardless of their ACL rights.

These new settings are located on the server document, Security tab, in the Administrators section. An overview of administrator privileges is presented in Table 5-1 on page 49; for a detailed description and discussion about delegating administrative tasks, and the various administrator levels, see 10.1.1, “Administrators” on page 304.










Basics	Security	Ports	Server Tasks	Internet Protocols
Administrators				
Full Access administrators:		SuperAdmin 		
Administrators:		Administrators 		
Database Administrators:		DatabaseAdmins 		
Full Remote Console Administrators:		RemoteAdmins 		
View-only Administrators:		ViewOnlyAdmins 		
System Administrator:		SystemAdmins 		
Restricted System Administrator:		RestrictedSysAdmins 		
Restricted System Commands:				
Administer the server from a browser (pre-Notes 6 servers only):				

Figure 5-19 Administrators delegation from server form

Table 5-1 Level of administration delegation

Field name	Purpose
Full Access Administrator	These people get the same rights as Administrators, and manager access to <i>all</i> databases on this server regardless of the ACL. They have all roles enabled. This level should only be given to trustworthy and skilled people.
Administrators	Same behavior as in R5. People listed in this field can do the following using Domino Administrator client: <ul style="list-style-type: none"> • Issue remote console command • Compact and delete databases • Create, update, and delete full-text indexes, directories, and links • Create databases, replicas, and master templates • Get and set certain databases options • Use Message Tracking • Use console to remotely administer UNIX server by example
Database Administrators	Database Administrators have the same access to the server databases as Administrators, with the exception of WebAdmin.nsf (not allowed to use a browser to administer the server). They are not allowed to issue any remote console commands.

Field name	Purpose
Full Remote Console Administrators	These people are allowed to issue any remote console command.
View-Only Administrator	These people are only allowed to issue a subset of remote console commands, such as Show tasks, Show server, and so on. Commands that affect server operation are not allowed.
System Administrator	These people are allowed to issue Operating System Command on the server.
Restricted System Administrator	These people are allowed to issue only the Operating System commands that are listed in the Restricted System Commands.
Restricted System Commands	Lists the subset of operating system commands that Restricted System Administrators can issue.
Administer the server from a browser	Lists people who should be allowed to use the Web Administrator to administer the server. This field is ignored by Domino 6 server. Access to this application is controlled by the ACL to WebAdmin.nsf.

Table 5-2 indicates which tasks are available for which group of people. “Full” represents Full Access Administrators, “Database” is Database administrators, and so on.

Table 5-2 Task availability by group

	Enter select system commands	Full operating system access	R5 admin tasks	Manage databases	Use a remote console	Use some console commands
Full	X	X	X	X	X	X
Administrator			X	X	X	X
Database				X		
Full Remote Console					X	X
View Only						X
System	X	X				
Restricted System	X					

When you upgrade your Domino Directory design from R5 to Domino 6, note that the field “Full Access Administrators” will remain empty and people listed as Administrators in the R5 design will remain listed as Administrators in the Domino Directory 6 design. You will have to enter names into the Full Access Administrators field manually, after you have upgraded the Domino Directory design. Do not copy the list from the Administrators field into the Full Access Administrators field without reviewing and rethinking your organization’s administration privileges and policies.

This field is ignored by any R5 servers.

5.3 Fault recovery

You can set up fault recovery to automatically handle server crashes. When the server becomes unavailable (after an internal error or exception), it shuts itself down, terminates each Domino process, and releases all associated resources. The server then restarts without any physical intervention from Domino Administrators. If you are using multiple partitions, only the partition which has the error is terminated and restarted.

For a UNIX Domino administrator, fault recovery is not really a new concept since it has been available for a long time. With Domino 6, fault recovery can be enabled on any platform, including the Win32 platform. You don’t have to edit any NOTES.INI parameters to get it enabled; everything can be done directly from the server document itself. This setting is found under the Basics tab - Fault Recovery section of the server document. The Domino R5 server ignores this section, and if you have already configured Fault Recovery on any UNIX system, you will have the ability to retain your settings in the NOTES.INI files.

Fault Recovery	
Fault Recovery:	<input checked="" type="checkbox"/> Enabled
Cleanup Script Name:	/opt/lotus/notes/latest/linux/nsd.sh -batch
Cleanup Script Maximum Execution Time:	300 seconds
Maximum Fault Limits:	3 faults within 5 minutes
Mail Fault Notification to:	Administrators

Figure 5-20 Fault recovery section from Server document

Table 5-3 Fault recovery field

Settings	Description
Fault Recovery	Enable or disable Fault Recovery.
Cleanup Script Name	Name of the program which will be executed after a crash.
Cleanup Script Maximum Execution Time	Cleanup Script must complete within this time, otherwise it is terminated (maximum is 1800 seconds).
Maximum Crash limit	Number of crashes allowed during a specific time period. When this number of crashes is reached within the specified time, the server will not be restarted automatically. The default is 3 faults in 5 minutes, as shown in Figure 5-20 on page 51; however, we would recommend 3 in 15 minutes or even 3 in 30 minutes. This way NSD has enough time to execute.
Mail Crash Notification to	Users or Groups to whom an email notification is sent.

5.4 UNK table in a mixed environment

If you run any R4.6x servers in your infrastructure, they must be at least on Lotus Domino R4.6.7a release level. This is to avoid any UNK table issues when you try to replicate your upgraded Domino Directory into a R4 server.

Note: What is an UNK table? The UNK (Unique Name Key) table is a table of unique field names stored in the database. The UNK table is used for many things, including full-text search highlighting, searching by form, and populating the field list in the Design pane of the Domino Designer.

UNK tables grow when any document containing a new fieldname is added to the database.

Be sure that the database property “Allow more fields in database” is correctly checked for all your replicas of your Domino Directory. There are two ways to enable this database setting:

1. Issue a server remote console command:

```
>load compact names.nsf -K
```

This must be done on each replica.

2. Use a Domino 6 Administration client to open each replica of your Domino Directory and check the advanced properties with the following steps:

- Select a server and click the File tab to display all databases hosted on this server; select the Domino Directory line.
- In the right pane Tools, select Advanced Properties to display the properties dialog box.
- In the Advanced Database Properties dialog box select the Allow more fields in the database check box as shown in the Figure 5-21.

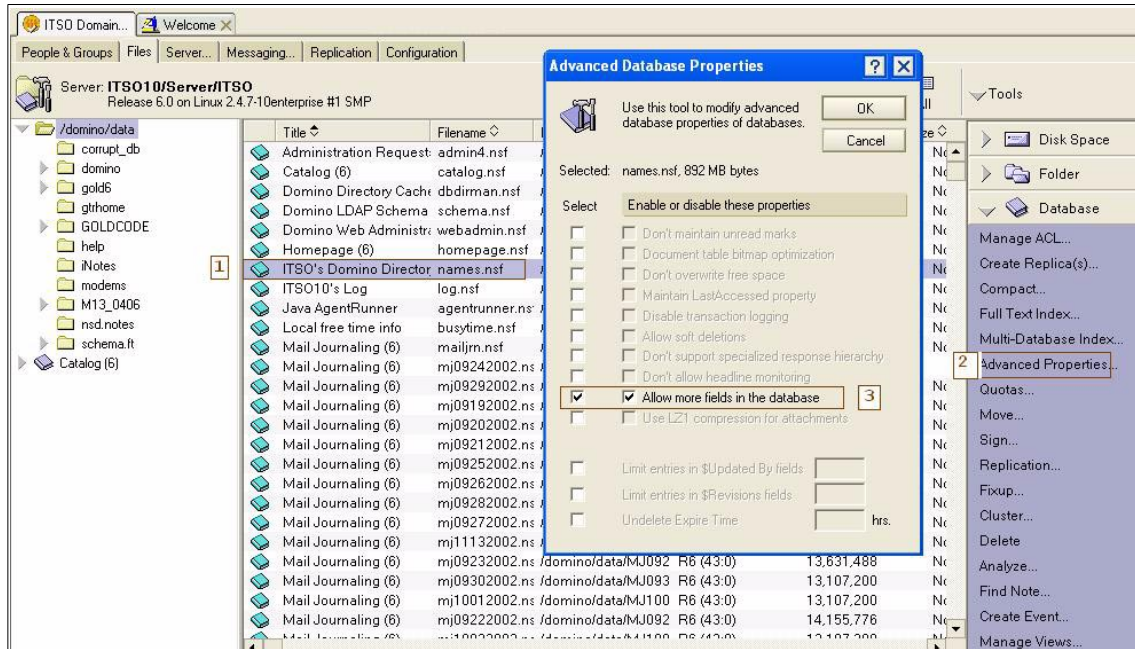


Figure 5-21 Allowing more field on Domino Directory database

This property was introduced in Domino R5.0.1 to increase the number of fields stored in the UNK Table, which was limited to 3000 entries before that, and now can contain around 23000 fields per database. When you create a field in a form stored in a database (from your Domino Designer client) this field is added to the UNK Table for reference.

a

Attention: Even if some database properties are already set, the dialog box, shown in Figure 5-21 on page 53, will not display existing settings. You have to select which parameter you want to turn on.

This flag should be set on each replica of your Lotus Domino Directory regardless of the release of your Domino server—database settings are not replicated.

For Domino R5 servers (this is not supported on R4.6 servers), you can set some additional properties at the same time in your Domino Directory. (These parameters are supported in Domino 6, but for servers that are still running Domino R5, this will improve server performance.) The parameters are:

- ▶ Don't maintain unread marks
`>load compact names.nsf -U`
- ▶ Document table bitmap optimization
`>load compact names.nsf - F`

For R5 servers and higher, all these parameters can be set from the server remote console with a single command:

```
>load compact names.nsf -U -F -k
```

5.5 Controlling and managing the distribution

It is important to ensure that the design of your Domino Directory is still up to date and to prevent any unwanted changes to both its design and contents. The best way to protect your design and contents is to pay special attention to your ACL for the Domino Directory, and to allow only a small number of people and servers to have manager access.

Table 5-4 Example of a recommended ACL for your Domino Directory

ACL rights	Who	Roles
No Access	Default, Anonymous and terminations	No
Depositor	No	No
Reader	Trusted other domain (users and servers)	No
Author	<ul style="list-style-type: none"> • End-users (deselect the Create documents check box) • Local Administrators 	No [groupCreator] [GroupModifier] [UserModifier]

ACL rights	Who	Roles
Editor	<ul style="list-style-type: none"> • Servers (other then Hub) • Regional Admins 	No Same as Local administrator, plus [ServerModifier] [NetCreator] [NetModifier]
Designer	No	No
Manager	Administration server Hub Servers Global Admins	No No All roles

If you have a large domain across several locations, you can consider enabling “Enforce a consistent Access Control List across all replicas” and setting “Maximum internet and password” to Reader, unless you want to grant more access to people accessing to your Domino Directory with a browser.

To change these settings, select your Domino Directory database and select File -> Database -> Access Control, and go the Advanced tab.

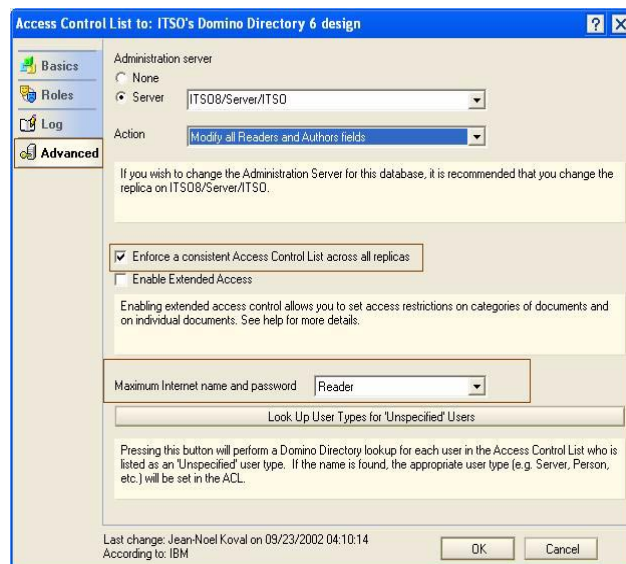


Figure 5-22 Changing ACL settings on the Domino Directory database

You should consider the table and figures as a baseline for determining your ACL strategy. It is really an infrastructure decision and it is closely related to your design and how you want to manage your domain.

Still, to ensure that your design will remain in an appropriate state, you have to consider disabling any inheritance of design for your Domino Directory. (See Figure 5-23.)

By default, each night at 1:00 AM, a design task runs on any Domino Server and will refresh any database's design hosted on your servers which have template inheritance set.

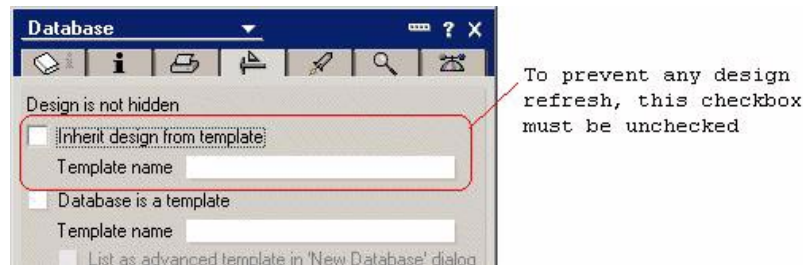


Figure 5-23 Preventing design refresh on a database

Extended ACL should also be executed to help reduce the number of Administrators who have access to certain sensitive documents. Furthermore, using extended ACL will allow your organization to set access to documents and fields easily and globally at one source, rather than requiring you to control access through features such as multiple Readers and Authors fields. For detailed information about extended ACL, see Chapter 14, "Extended ACL" on page 431.

5.5.1 Using a custom design template for the Domino Directory

Many organizations customize their Domino Directory to enhance functionality or to support third party applications (for example mobile, fax, and enterprise directory). This customization might be as simple as a hidden view or an additional field in a form, or as complex as several scripts or agents.

If you have customized your previous R5 Domino Directory, consider whether you still need these customizations; some of them might be implemented in the standard Domino Directory template.

If these customizations are still needed, reproduce them in the new Domino Directory design. Do *not* use your customized R5 Domino directory and try to add the Domino 6 directory elements manually.

Upgrade your new Domino Directory design on a test machine (part of your pilot phase). Do not go into production without doing some intensive testing first.

To propagate all changes, let the design of the Domino Directory 6 replicate throughout your domain.

Important: For any changes needed by third-party software, like fax software or CTI, check with the vendor for Domino 6 compatibility.

Keep in mind that any customization to any existing \$views are unsupported and can have a negative impact on the behavior of your Domino infrastructure.

If you want to keep inheritance enabled, but avoid trouble if an unwanted design is applied by mistake, follow these steps:

1. Since pubnames.ntf has had the same replica ID since R4, create your own copy (it gets a new replica ID), prevent any replication between previous Domino Directory template (from R5 or R4.6) and give it another name with an .ntf extension (for example, CompanyDirectory.ntf)

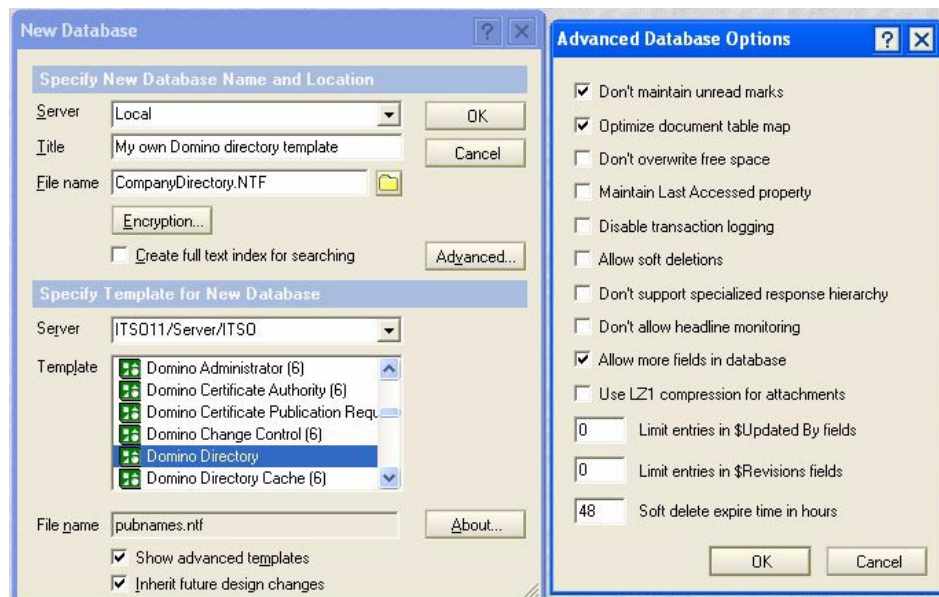


Figure 5-24 Creating a new copy of pubnames.ntf

2. Give the template a Template Name and set your Domino Directory database to inherit from this template.

- a. Select your Domino Directory template (in this example CompanyDirectory.ntf).
- b. Open Database properties and click the Design tab.
- c. Check the box "Database is a template."
- d. Enter a name in the field "Template name" (for example MyDominoDirectoryTemplate) and close the properties box.
- e. Select your Domino Directory database and display database properties.
- f. Go to the Design tab, check the box "Inherit design from template" and in the field "Template name" enter the same name that you defined previously (MyDominoDirectoryTemplate in this example).

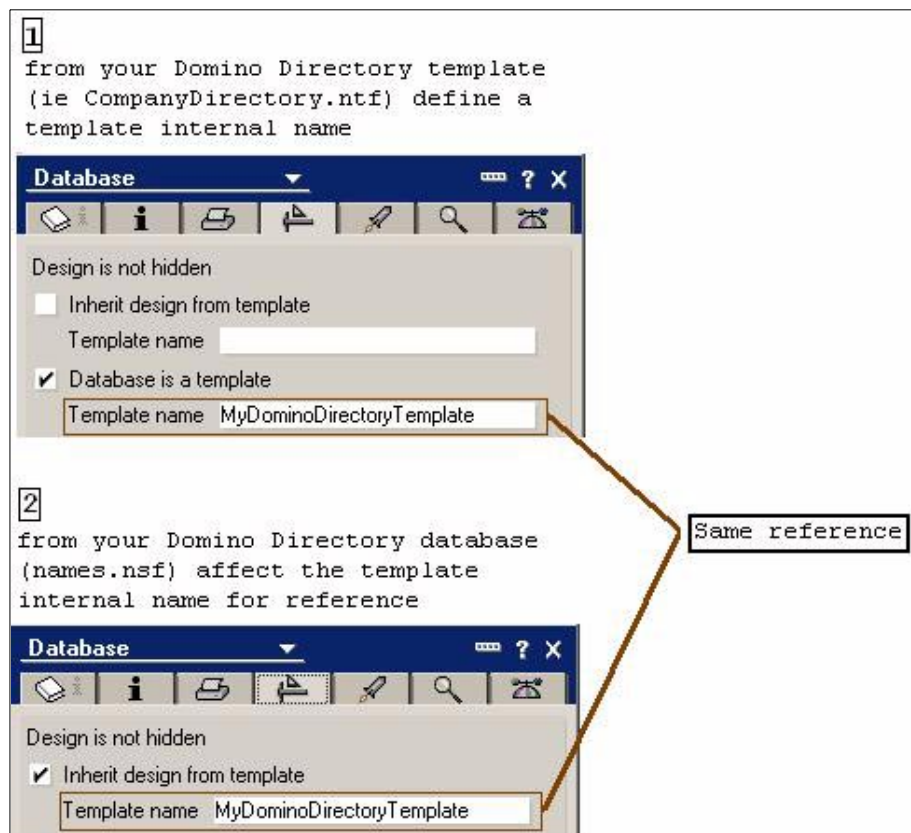


Figure 5-25 Template inheritance in Domino Directory database

3. Modify the ACL to prevent any unwanted changes.
4. Deploy this template (DominoDirectory.ntf) to all your servers, remove any previous Pubnames.ntf that you have on your servers already, and delete the

Pubnames.ntf file which will be installed after a server upgrade or code installation.

Tip: If you enable “Allow more fields in database” for your Domino Directory database, we suggest that you perform the same steps for your template database. If you have set a design inheritance, advanced database properties will be applied from template to database. To maintaining your database properties, make certain that your settings are not overwritten when a design task runs.

This also applies to other properties, such as:

- ▶ Don't maintain unread marks
- ▶ Optimize document table map

5.5.2 Retaining R5 Domino Directory design on certain servers

If you use any Lotus companion products in your environment (for example Lotus Sametime or QuickPlace), and they share the same Domino Directory and you want to retain an R5 design for these servers, you can prevent any design changes by changing the replication setting for the replica of the Domino Directory which is on these targeted servers. From Notes client or Domino Administrator client, select the appropriate replica of Domino Directory and select File -> Replication -> Settings from the actions menu.

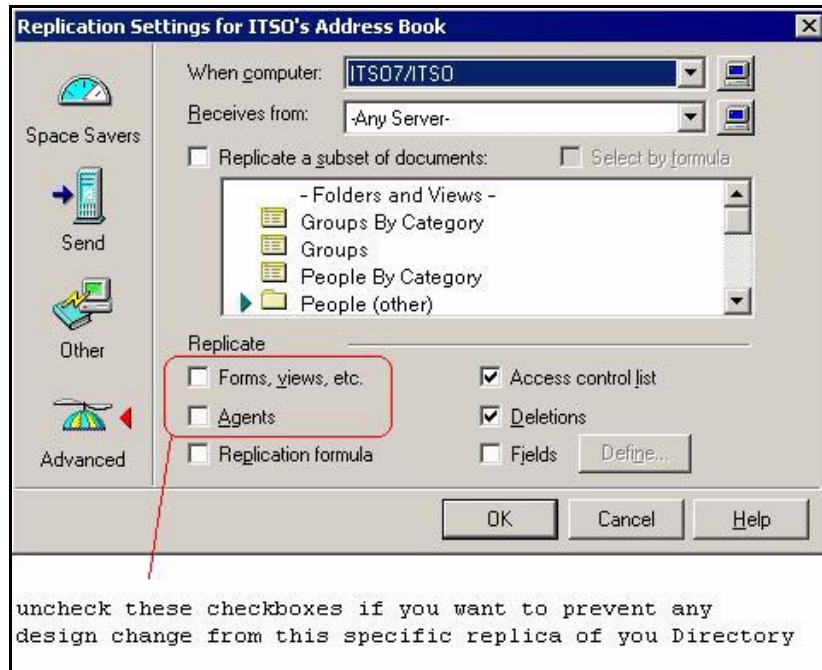


Figure 5-26 Preventing design changes for a specific Domino Directory replica

Unselect the check boxes “Forms, views, etc.” and “Agents” to prevent replication of the design elements.

5.6 Secondary directories

While you are thinking about your Domino Directory (names.nsf) upgrade, you should also take into consideration any secondary directories that you have on your infrastructure, such as a replica from a different domain, Extended Directory Catalog, or Directory Assistance.

5.6.1 Extended Directory Catalog

Extended Directory Catalog (EDC) was introduced in Lotus Domino R5.0.5 and it works with Directory Assistance (DA). EDC is based on pubnames.ntf and can aggregate several directories as Condensed Directory Catalog does. Instead of using full-text searches to resolve any names lookup, EDC uses view lookup, which provides faster results and uses less CPU cycles to achieve its search. This doesn't apply if you want to use it for LDAP searches.

Since EDC is based on pubnames.ntf, the same template as for Lotus Domino Directory, you can use the same upgrade approach as for Domino Directory. You can upgrade it at the same time, while you are still running Domino R5, or you can upgrade EDC later, after you have upgraded the server to Domino version 6.

If you share your directory (either Domino Directory or Extended Directory Catalog) with an external domain, inside or outside your company, you will have to check whether you can push the new design or if you have to retain R5 design for these external databases.

5.6.2 Condensed Directory Catalog

Condensed Directory Catalog uses a design based on the DIRCAT5.NTF template that enables it to be very small. A Condensed Directory Catalog can be both on the server and on a client; in that case it is also known as a Mobile Directory Catalog.

Unlike EDC, Condensed Directory Catalog uses Full-Text indexes to return any searches.

There are no specific changes included in DIRCAT5.NTF which is shipped with Lotus Domino 6 server. However, due to a change of GTR engine (used for view and full-text indexes), after you have upgraded any of your servers to Lotus Domino 6 server, you will have to force a full rebuild of your Condensed Directory Catalog. You can do that by issuing the following command:

```
>load updall <condensed directory catalog name>.nsf -X
```

5.6.3 Directory Assistance

If you use Directory Assistance on an R5 server you don't need to upgrade any design.

Attention: Domino 4.6 administrators must upgrade their directory assistance database with DIRCAT5.NTF after upgrading to Domino Directory 6 design.

5.6.4 Cascading Domino Directories

In R4, information lookup from secondary Domino directories was done by cascading several Domino Directories using the NAMES= line. Cascading Domino Directories is still supported for backward compatibility in Domino 6; however, you should move to a Directory Assistance design. Using Directory Assistance provides more options and functionality, as well as better availability and scalability, than using the old method used prior to Domino 4.5.

Table 5-5 compares Directory Assistance to Cascading Domino Directories.

Table 5-5 Directory assistance and cascading Domino directories

Feature	Directory Assistance	Cascading
Do lookups in secondary Domino Directories on behalf of Notes user for mail addressing.	Yes	Yes
Fail over to an alternate replica of a directory.	Yes	No
Use naming rules to efficiently search secondary Domino Directories.	Yes	No
Support for "Recipient name Type-Ahead" addressing.	Yes	Yes
Support for an unlimited number of secondary directories.	Yes	No ¹
Do lookups in LDAP directories on behalf of Notes Users for mail addressing.	Yes	No
Do lookups in secondary directories on behalf of LDAP clients.	Yes	Yes
Refer LDAP clients to LDAP directories.	Yes	No
Authenticate Internet client registered in LDAP directories.	Yes	No
Authenticate Internet client registered in secondary Domino Directories.	Yes	No

¹ The NAMES= setting has a 256 character limit.

For more information about how to implement Directory Assistance refer to Lotus Domino Administration 6 help.

5.6.5 LDAP Schema changes

This section describes changes to the Domino LDAP Schema in Lotus Domino 6.

There is a new Domino LDAP Schema database created from the template SCHEMA.NTF. This database replaces the Domino 5 LDAP Schema database created from the template SCHEMA50.NTF. A new process called the schema daemon, spawned by the LDAP service, creates the new Schema database on the administration server for the Domino Directory. The schema daemon replicates the databases to all Lotus Domino 6 servers in a domain that run the LDAP service, ensuring a consistent schema throughout a domain. In this release, the Schema database is also a tool you can use to extend the schema.

If you upgrade a Domino 5 server that runs the LDAP service to Lotus Domino 6, the installation program deletes the Domino 5 SCHEMA50.NTF template, and the LDAP service deletes the Domino 5 SCHEMA50.NSF database. To retain these files, rename them before you upgrade.

The first time Domino loads the LDAP service on the administration server of the Domino domain, Domino creates a new Domino LDAP Schema database. While Domino creates the schema documents and builds the views in this database, certain schema elements such as object classes, attribute types, or syntaxes may be unavailable. To avoid potential problems, allow at least 15 minutes after the LDAP service starts for Domino to finish creating all default schema documents before you extend the schema.

Note: The delay that occurs while Domino creates the schema documents and builds the database views occurs only once when Domino loads the LDAP service for the first time.

In Lotus Domino 5, the LDAP service converted a search base of country ("c=xx") to root ("") by default. This conversion accommodates releases of Microsoft Outlook Express earlier than 5.5, which supply a default country search base when users do not specify a search base. In Lotus Domino 5, you can use the NOTES.INI setting LDAP_CountryCheck=1 to prevent the LDAP service from making this conversion.

By default, the Domino 6 LDAP service does not convert a search base of country to root. Use the NOTES.INI setting LDAPPre55Outlook=1 to revert to the Domino 5 LDAP service behavior of converting a search base of country to root to accommodate releases of Microsoft Outlook Express earlier than 5.5. The LDAP_CountryCheck setting is obsolete in Lotus Domino 6.

5.7 Upgrading your Domino Directory to the new design

Domino Directory with version 6 design is fully backward compatible with R5.x and R4.6.7a servers. Upgrade your Domino Directory with either of the following methods:

- ▶ Upgrade the design of your Domino Directory on your current infrastructure before upgrading to Lotus Domino 6.
- ▶ Upgrade the Domino Directory while you are upgrading your Administration server (which must be the first server upgraded in your domain).

In each of the two cases you should identify and detail all steps clearly and make a roll-back plan. Use the upgrade plan and steps in your pilot environment as well.

5.7.1 Upgrading your Domino Directory first

The following list describes the steps needed to upgrade your Domino Directory to Domino 6 design before upgrading any server to Lotus Domino 6.

1. If your Domino Directory is full-text indexed, be sure to delete it before starting your upgrade using your client. Otherwise your UNK table will not be rebuilt by compact -c command, which is issued later in the process. Compact will check specific database header information, so deleting full-text indexes at the OS level will not work.
2. Ensure that your Lotus Domino Directory is correctly configured to support all design changes across your domain (ACL and Design).
3. If needed, add your own customizations.
4. Create your own Master Template and use an explicit name for the template file (for example MydirectoryTemplate.ntf).
5. Replicate this new template on all targeted server if you still want to run design task against your directory
6. Do a backup of your Domino Directory database and ensure that you have disabled replication for this database.
7. From your Notes Client, select the server-based replica of your Domino Directory (be sure to select your Administration server).
 - a. Choose File -> Database -> Replace Design.
 - b. Click the Template Server button.
 - c. Select the server that has the new Domino Directory template and click OK.
 - d. When prompted to replace the template, click Yes.
 - e. If you use an R5 client you will have to wait until replace design is done. If you use a Notes 6 client, replace design will be done in the background and a progress bar will be displayed at the bottom of your client.
 - f. After replacing the design, your server will start to rebuild all views and, depending on the size and complexity of the view, this can be time-consuming. During this time you may have some difficulty accessing this server. You can check the progress of view rebuild by issuing a **show tasks** command at the server console and looking at Directory indexer task. When the view rebuild is complete, this thread will not be displayed before the next schedule. Using the notes.ini variable Log_Update=2 will

print out the view rebuild status to the console and makes it easier to watch.

- g. Alternatively, you can bring down your server to issue a full **upda11** against your Domino Directory from a DOS dialog box:

```
>\data directory\nupda11 -R names.nsf (for win32 platform)
<notes@unix>data directory\upda11 -R names.nsf (for UNIX Platform)
```

Restart you server.

8. Check that your server is working properly by accessing it with your client.
9. Turn on replication for your Domino Directory database to push design changes across your domain.
10. During the next hours or days, watch for any design replication, connectivity, or mail routing issues across your domain. On some occasions you might experience mail routing problems even between servers in the same domain. You might need to force a rebuild of Domino Directory views to solve the problems. This is explained in “Run FIXUP program on Key System databases” on page 104.
11. If you use any secondary directory refer to 5.6, “Secondary directories” on page 60.

5.7.2 Server and Directory design upgrade at the same time

This section describes the steps needed to upgrade your Domino directory and your Administration Server at the same time. (The first six steps are the same as those given in the previous section until step 6; they are repeated here for your convenience.)

Important: In this section we have been mainly focused on the Domino Directory design upgrade. The same approach must be taken to upgrade your Administration Requests database (ADMIN4.NSF). Upgrading the Domino Directory while you upgrade your Administration server will cause ADMIN4.NSF to be upgraded to the new design (version 6), unless you have moved admin4.ntf from the Domino data directory to prevent any design refresh.

We recommend that you upgrade the design of your ADMIN4.NSF database at the same time you upgrade your Administration server.

1. If your Domino Directory is full-text indexed, be sure to delete it before starting your upgrade using your client. Otherwise your UNK table will not be rebuilt by **compact -c** command, which is issued later in the process. Compact will

check specific database header information, so deleting full-text indexes at the OS level will not work.

2. Ensure that your Lotus Domino Directory is correctly configured to support all design changes across your domain (ACL and Design).
3. If needed, add your own customizations.
4. Create your own Master Template and use an explicit name for the template file (for example MydirectoryTemplate.ntf).
5. Replicate this new template on all targeted server if you still want to run design task against your directory
6. Do a backup of your Domino Directory database and ensure that you have disabled replication for this database.
7. Bring you server down and install the Lotus Domino 6 code (all the steps will be described in the next section)

Important: During the upgrade process you are asked to run several maintenance tools (fixup, compact, and updll). When you upgrade your Administration server, you will have to perform compact and updll twice against some databases at two different steps. This is necessary; do not skip these steps.

8. Before you restart your server, rename your new Domino Directory template, at the OS level, to Pubnames.ntf; the server upgrade script will look at that name to upgrade the design.

Table 5-6 provides a list of all templates that will be applied to databases during the upgrade, if you have databases that inherit from these templates.

Table 5-6 Templates applied during server upgrade

Database Title	File name
Administration Requests	ADMIN4.NTF
Agent Log	ALOG4.NTF
Archive Log	ARCHLG50.NTF
Billing	BILLING.NTF
Bookmarks	BOOKMARK.NTF
Catalog	CATALOG.NTF
Certification Log	CERTLOG.NTF
Cluster Directory	CLDBDIR4.NTF

Database Title	File name
Database Analysis	DBA4.NTF
DOLS Resource Template	DOLRES.NTF
DOLS Offline Services	DOLADMIN.NTF
Domino Configuration	DOMCFG.NTF
Domino Web Server Log	DOMLOG.NTF
Local Free Time Info	BUSYTIME.NTF
Server MailBox	MAIL.BOX
Mail Router MailBox	MAILBOX.NTF
Master Address Box	MAB.NTF (& DA50.NTF)
Monitoring Configuration	EVENTS4.NTF
Notes Log Analysis	LOGA4.NTF
Notes Log	LOG.NTF
NT/Migration Users' Password	NTSYNC45.NTF
Domino Directory (or PAB)	PUBNAMES.NTF
Server Web Navigator	PUBWEB45.NTF (&PUBWEB50.NTF)

9. After renaming the appropriate template (Pubnames.ntf, Admin4.ntf, etc.) start the Domino Server.
10. From the Domino server console, when Domino asks if you want to upgrade the Domino Directory design to your new design, enter Y.
11. While the server upgrades Domino Directory and all databases listed in the table, watch for any errors that are displayed. When the server is ready to accept any connections, the message "Database server started" is shown on the server console. Type `Quit` (or simply `Q`) at the Domino server console to bring the server down again.
12. When the server is down, from an operating system command line issue the commands listed in Table 5-7.

Table 5-7 Commands to run after the server upgrade

Win32	UNIX	Description
ncompact -c	compact -c names	Does a compact using copy-style behavior and gets rid off any UNK table issues by rebuilding the UNK table. Converts the database ODS to version 43.
nupdall - names.nsf -t “(\$ServerAccess)” -r	updall - names.nsf -t /(\$ServerAccess) -r	Rebuilds \$ServerAccess view on names.nsf
nupdall -names.nsf -t “(\$Users)” -r	updall -names.nsf -t /(\$Users) -r	Rebuilds \$Users view on names.nsf

In the Domino 6 directory, the (\$ServerAccess) and (\$Users) views are designated for transaction logging. If you enable transaction logging for the Domino Directory, future restarts after a server failure will be faster.

13. At the OS level, rename back to their originals all NTF files that you changed earlier.
14. Restart your Domino server and check for any problems (connectivity, replication, and so forth). If you have disabled replication of your Domino Directory, remember to enable it again.
15. During the next hours or days, watch for any design replication, connectivity, or mail routing problems across your domain.
16. i If you use any secondary directory, refer to 5.6, “Secondary directories” on page 60.

5.8 Introduction to the new On-Disk Structure (ODS)

On-Disk Structure is the way data is written to the disk storage. Every major release of Notes/Domino has included significant architectural changes to the database structure. These changes to the ODS provide a lot of benefits and new features with very low risk. Upgrading the ODS of your database is an important step in a Notes/Domino 6 upgrade plan.

You can view the On-Disk Structure level of a database by using a Notes 6 client and selecting the Information tab of the Database Properties box.

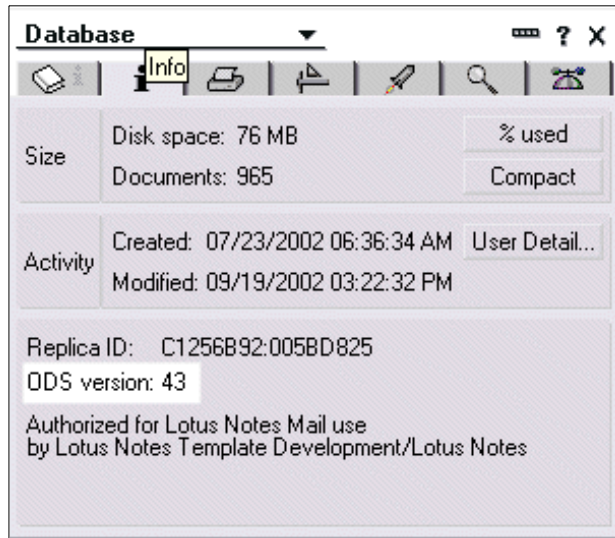


Figure 5-27 Local Database ODS level

Note: A notes R4.6 client doesn't show the ODS version because the ability to display this settings wasn't introduced until the R5 release.

You can also display the level of the ODS using the Domino 6 administration client. Select the server that you want to check database versions on, select the Files tab and look at the File Format column (see Figure 5-28).

Title	Filename	File Format
Java AgentRunner	agentrunner.nsf	R5 (41:0)
Local free time info	busytime.nsf	R6 (43:0)
Server Certificate Admin	certsrv.nsf	R6 (43:0)
Domino Directory Cache (6)	dbdirman.nsf	R6 (43:0)
Catalog (6)	catalog.nsf	R6 (43:0)
Mail Journaling (6)	mj09192002.nsf	R6 (43:0)
Domino Web Administrator (6)	webadmin.nsf	R6 (43:0)
Mail Journaling (6)	mailjrn.nsf	R6 (43:0)
Administration Requests (R5)	admin4.nsf	R6 (43:0)
Homepage (6)	homepage.nsf	R6 (43:0)
ITSO10's Log	log.nsf	R6 (43:0)
Reports for ITSO10/Server/ITSO	reports.nsf	R6 (43:0)
Offline Services	doladmin.nsf	R6 (43:0)
Statistics & Events	events4.nsf	R6 (43:0)
ITSO's Address Book	names.nsf	R6 (43:0)

Figure 5-28 ODS level of databases hosted on a server

Tip: You can also check the ODS level directly at the console level (or using a Domino remote console) of your server when you issue this command:

```
show directory
```

DbName	Version	Logged	---Modified Time---
/domino/data/mailjrn.nsf	V6	N/A	09/19/2002 02:02:50 AM
/domino/data/MJ09192002.nsf	V6	N/A	09/19/2002 01:02:29 AM
/domino/data/catalog.nsf	V6	N/A	09/19/2002 01:01:28 AM
/domino/data/webadmin.nsf	V6	N/A	09/18/2002 11:21:05 PM
/domino/data/busytime.nsf	V6	N/A	09/19/2002 02:01:07 AM
/domino/data/dbdirman.nsf	V6	N/A	09/19/2002 08:48:39 PM
/domino/data/mail.box	V6	N/A	09/19/2002 05:00:56 AM
/domino/data/certsrv.nsf	V6	N/A	09/19/2002 02:01:06 AM
/domino/data/doladmin.nsf	V6	N/A	09/19/2002 02:01:05 AM
/domino/data/reports.nsf	V6	N/A	09/19/2002 01:02:37 AM
/domino/data/names.nsf	V6	N/A	09/19/2002 07:00:18 PM
/domino/data/events4.nsf	V6	N/A	09/19/2002 01:02:36 AM
/domino/data/admin4.nsf	V6	N/A	09/19/2002 07:00:19 PM
/domino/data/log.nsf	V6	N/A	09/19/2002 08:58:07 PM

If you use the remote console of the Domino administrator 6 client, you can copy and paste the output of this command.

Table 5-8 shows details about ODS levels on different Notes/Domino releases.

Table 5-8 ODS level information

Domino release level	On-Disk Structure level	Server output version
Notes R3.x	17	V3
Notes/Domino R4.x	20	V4
Notes/Domino R5.x	41	V5
Notes/Domino 6	43	V6

5.8.1 Upgrading to the new ODS level

Upgrading the ODS level of your database provides new features and enhancement, such as:

- ▶ LZ1 compression for attachment (both Server and Client need to run Notes/Domino 6)
- ▶ View logging
- ▶ Single copy template

You can upgrade your databases to the new ODS level from your server using any one of the following methods:

- ▶ During your upgrade process, run a full compact against your whole directory.
- ▶ Compact only your system databases during the upgrade process, and run an off-line compact command later for the remaining database.
- ▶ Schedule a program document which will trigger a compact during off-hours.
- ▶ Run compact online by using the new .IND file, in which you can specify several databases that need to be compacted. This will also allow you to compact databases by directories, or by compacting individual databases by order of importance.

Attention: When your server is upgraded to Domino 6, each time you create a new replica, a new database copy, or a new database, you will use the new ODS level by default.

If you want to retain the previous ODS level, you have to do one of the following:

- ▶ Specify the following file database extension:
databasename.ns5
(Renaming the file at the OS level doesn't revert the ODS level.)
- ▶ Run the following command at the server console:
`load compact path/database -r`
- ▶ Schedule a program document to have a `compact -r` running against either some databases or directories that you would like to retain in R5 ODS format (ODS 41).

To upgrade your database to the new ODS level from your client, click the compact button for each database that you want to upgrade. The compact button is found on the Information tab of the Database Properties box.

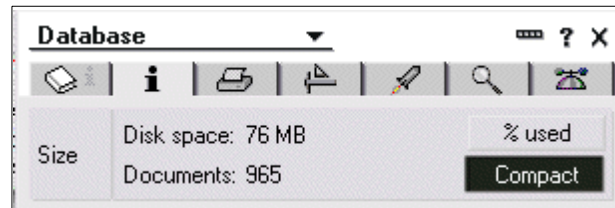


Figure 5-29 Compacting your local database

As for the server, each time you create a new replica, a new database, or a new database copy, by default you will use the new ODS 43, unless you specify .NS5 as the database file extension.

5.8.2 Demystifying some ODS legends

In this section we try to clear up some common misconceptions about ODS.

- ▶ The ODS doesn't replicate. There is complete support for having several ODS levels of several replicas of the same database:
 - One replica with Domino 6 ODS (43) on a Domino 6 server
 - One replica with Domino 5 ODS (41) on a R5 server

- One replica with Domino 5 ODS (41) on a Domino 6 server using .NS5 extension
- ODS level version is completely unrelated to the database design, so:
 - Upgrading the ODS level *will not* affect the design of your database.
 - Changing the design of your database (that is, applying a specific Notes/Domino 6 design) will not affect the ODS.
 - Even if you retain the R5 ODS (41) you can still set a design inheritance from a Notes/Domino 6 template.
 - Having a database replica with a .NS5 extension hosted on a Domino 6 server will not prevent design changes when your database is replicated with another server.

The following table lists the ODS versions that result when working between R5 and Notes/Domino 6 systems (Clients or servers).

Table 5-9 ODS results from various Notes/Domino releases and actions

Scenario	ODS level on the target database
From an R5 client, through the user interface, you run a database copy or replica on a Domino 6 server.	ODS 43 (Notes/Domino 6)
Create a database replica or copy from a Domino 6 server locally on a client R5.	ODS 41 (Notes/Domino 5)
R5 client creates a database on a Domino 6 server.	ODS 43 (Notes/Domino 6)
R5 client creates a database locally.	ODS 41 (Notes/Domino 5)
R5 client creates a database replica or copy on a Domino 6 server using the .NS5 extension.	ODS 41 (Notes/Domino 5) and compact will not convert the database format.
Notes 6 client compacts locally a database which was on R5 ODS.	ODS 43 (Notes/Domino 6)



Domino Server upgrade

In this chapter we describe the steps for upgrading existing Domino R5 servers to Lotus Domino 6, on either a UNIX or Win32 platform.

We include an upgrade checklist that you can use as a reminder or baseline. Any upgrade plan must be tailored to your specific infrastructure design, but most of the information provided in this chapter is generic enough to apply to any organization.

Complete details of the following steps are discussed:

- ▶ Planning the upgrade
- ▶ Pre-upgrade tasks
- ▶ Putting the right code on your server
- ▶ Post-upgrade tasks
- ▶ Conversion of your ODS level

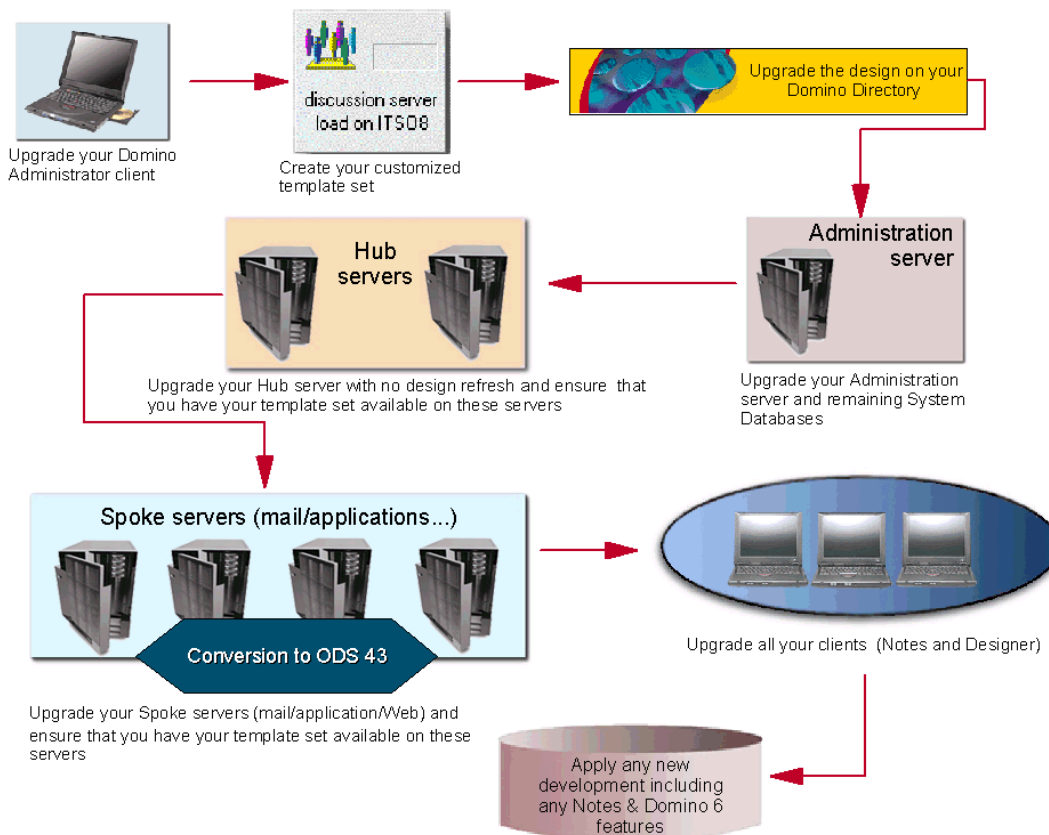


Figure 6-1 Domino 6 upgrade plan diagram

Figure 6-1 illustrates the Domino 6 upgrade process. The diagram gives you a high-level overview of the entire upgrade process.

6.1 Upgrade sequence

We begin this chapter by reviewing the upgrade sequence presented in Chapter 4.

The upgrade of any Domino server needs to be organized task. You should have a checklist for the upgrade and a predefined upgrade sequence. We strongly recommend that you follow the upgrade sequence listed here unless you have a compelling reason to change it.

At a high level, the recommended upgrade sequence is:

1. Domino Administration Client for all your administrators involved in the upgrading project
2. Domino Directory design
3. Domino Administration servers
4. Hubs servers
5. Spoke servers
 - a. Mail servers
 - b. Application servers
 - c. Web servers
6. Notes Clients
7. Mail template and application designs

By upgrading servers before clients, and clients before applications, you minimize disruption to users and business activities. With this approach, users will not see any Notes/Domino 6 features until their clients can utilize them; and conversely, users will not attempt to take advantage of Notes/Domino 6 features until their servers can handle them. However, your infrastructure, as well as your administrators, are able to take advantage of the Domino 6 features and functionality.

6.2 Disabling and deleting unused program documents

While you are planning your upgrade, check all your program documents to determine if they will still be required in your environment after the Domino 6 upgrade. The new features in Domino 6 may make some of them obsolete.

Furthermore, to avoid possible confusion during your server upgrade, disable any program documents running compact, since they might convert the

databases prematurely. The ODS conversion is done later during the upgrade process.

If you need to retain disk space you can run **compact -r** against your application or mail directory (more details about how to use the compact program are provided later in this section).

Disable any replication connection documents to prevent any replication workload during your post-upgrade validation phase, when you will check the server stability. You can enable replication tasks shortly after the end of your upgrade, once you have determined that the upgrade process has been successful and there are no issues with the server.

Attention: Some administrators use the NOTES.INI file to run their daily scheduled programs. If you are not sure which tasks are scheduled and run on your server, check the NOTES.INI file of the server for lines that begin with ServertasksATXX. xx is the time on 24 hours format.

Comment out the lines that you want to disable by adding an apostrophe (') at the begin of the line. For example:

'ServerTasksAt1=Catalog,Design

To prevent the Domino server re-enabling some of the tasks automatically during the server startup, add the following parameter line to the NOTES.INI file:

SetupLeaveServerTasks=1

All program documents can be found in your Domino Directory from the Configuration\Servers\Programs view (see Figure 6-2).



Domino Directory			
Add Program Edit Program Delete Program			
On Server	Run Program	Command Line	Schedule
ITS11/Server/ITSO	compact	directorytoconvert	04:00 AM
ITS011/Server/ITSO	Updall	mail -R -X	04:00 AM
ITS08/Server/ITSO	Updall	-R names.nsf	02:00 AM
	compact	-B	04:00 AM

Figure 6-2 Location of Program documents in Domino Directory

Connection documents can be found on the Configuration tab, Server\Connections view. Use your Domino Administrator 6 client to open the view as show in Figure 6-3.

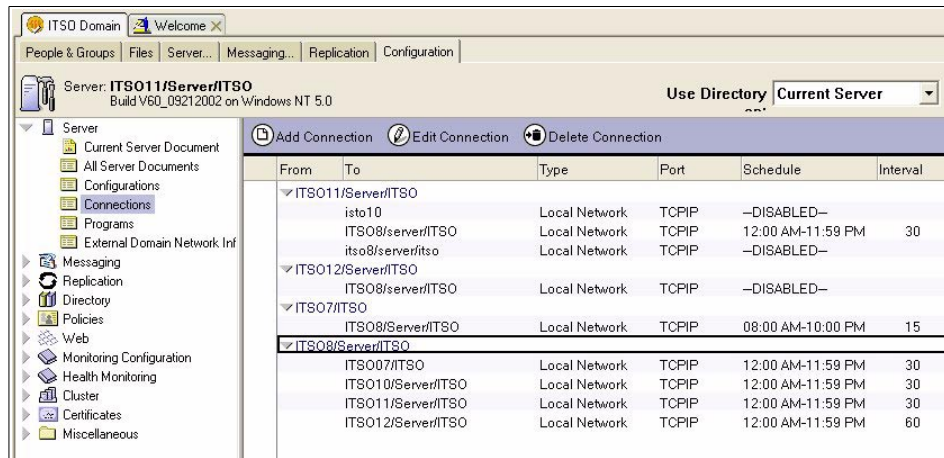


Figure 6-3 Displaying Connection document from Domino Administrator 6 client

Tip: If you use the same Notes Named Network (NNN) across your organization you don't need to specify any connection documents for mail routing between your different mail servers. However if you have a separate NNN and you use Mail Hub servers, you can use dedicated connection documents for mail routing, and for replication. In this case it will be easier to turn off replication without affecting your mail routing infrastructure.

6.3 Make a full backup of your servers

Run a full backup of your Domino server before any upgrade. You can keep the backup for the unlikely event you need to implement the roll-back recovery plan. If you don't have the ability to run a full backup on each server, ensure that you have at least saved the following files:

- ▶ Server ID and all other *.IDs present
- ▶ NOTES.INI (configuration file for the Domino server)
- ▶ Names.nsf (Lotus Domino Directory)
- ▶ Mailxx.box (Server's mail.box; if you use multiple mail.boxes, do a backup of each)
- ▶ Log.nsf (to have a trace of previous activities)
- ▶ Directory assistance database and all secondary directories (EDC, or Directory catalogs)

► **Tip:** If you use any directory (or folder) link, be sure that you are backing up the contents of the directory and not only the link file.

- Any templates that you have customized
- Any extension manager or specific API that you run on this server

6.4 Upgrade checklist and pre-upgrade tasks

You should have a detailed checklist for the upgrade tasks. We have included an upgrade check-list that you may want to use during the Domino 6 upgrade process. Use the list as a basis for preparing your own list. Every environment is unique, so you will need to add/delete/modify tasks that are required in your infrastructure. Most of the tasks listed in the upgrade checklist are detailed in this redbook.

Table 6-1 Upgrade checklist (All steps required unless noted otherwise)

Upgrade task	Win32 platform	UNIX platform
Full backup of your server.	X	X
Ensure that you have the appropriate Domino Directory design replicated on your server.	X	X
Purge all administrative requests in ADMIN4.NSF.	X	X
Ensure all mail has been routed.	X	X
Turn off all unused program documents and compact documents you don't want converted to ODS43 shortly after the upgrade.	X	X
Turn off replication documents and disable replication of Lotus Domino Directory for the current server which is being upgraded.	X	X
If you use LDAP, ensure that you deleted any FT indexes in your directory databases.	X	X
Stop the Domino server.	X	X
Turn off Domino server as a Win32 service.	X	Not applicable
Install Domino 6 code.	X	X
Replace standard template with your own template set if necessary.	Optional	Optional
Remove older NOTES.INI settings.	X	X

Upgrade task	Win32 platform	UNIX platform
Run fixup, compact, and updall against Names.nsf and Admin4.nsf.	X	X
Run updall against your whole directory to have rebuild view and full-text indexes.	Optional	Optional
Delete busytime.nsf (or clubusy.nsf if you are in a clustered environment).	X	X
Move out of your data directory Log.nsf, Catalog.nsf, and Mailxx.box; server will create new ones at startup.	Optional	Optional
Restart your Domino server.	X	X
Test your Domino server, re-enable replication documents (including names.nsf) and third-party software; perform a full backup if you use archive setting for transactional logging; if you use LDAP services, recreate your FT indexes for the relevant directories.	X	X

Purge all administration requests

Before starting your Domino upgrade, ensure that all administration requests have been processed. You can issue the **tell adminp process all** command at the server console (or from the remote server console). It will check and process all admin requests and result in the following:

```
tell adminp process all
23/09/2002 21:52:57 Admin Process: Checking for all requests to perform
```

Figure 6-4 Output for server command 'tell adminp process all'

Full-text indexes and LDAP services

If you use LDAP services, be sure that you have deleted any full-text indexes created for your Domino Directory (if this database can be reached by LDAP searches) or any secondary Domino Directory present on your servers which are "LDAP enabled."

To delete full-text indexes, open your Domino Directory, select Database Properties, and click the Full Text tab. If your Domino Directory is indexed, click the Delete Index button to delete the full-text index.

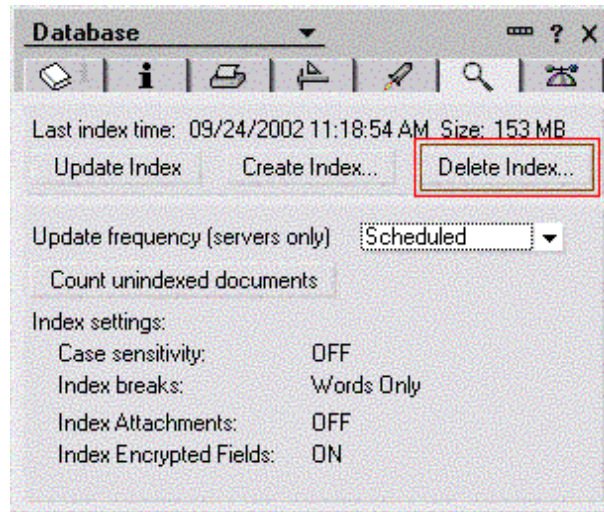


Figure 6-5 Deletion of Full-text on Domino Directory database

Alternatively, you can use your Domino Administrator 6 client to delete the index. Select the File tab, highlight your Domino Directory file, and right-click it to display properties. Select Full-Text Index to open the Full-text index dialog. Select Delete and click OK to delete the index.

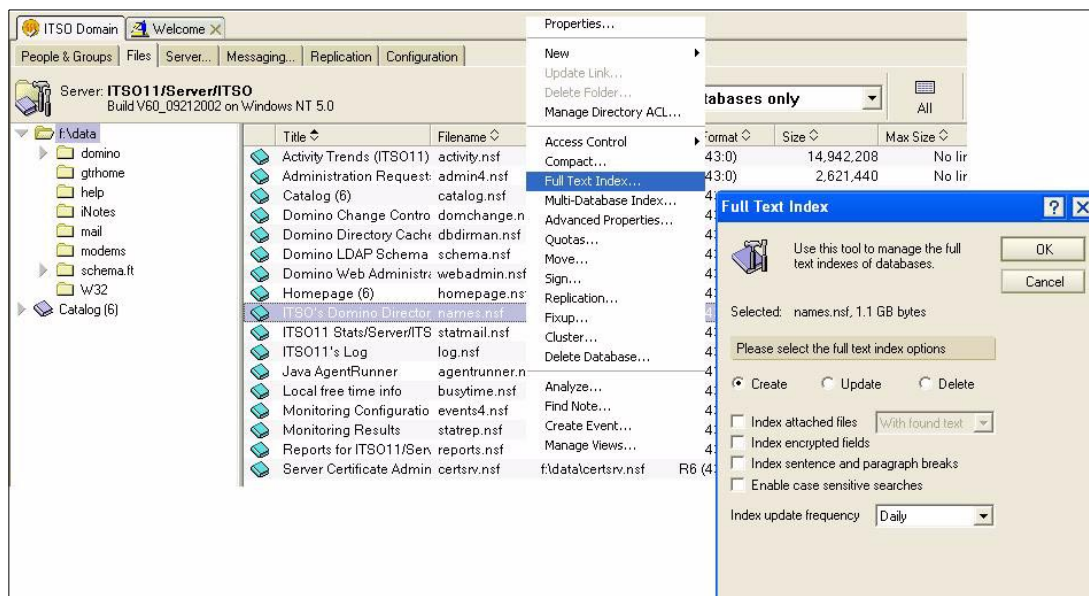


Figure 6-6 removing Full-Text indexing from Domino Administrator 6 client

Make your server unavailable for your users

Before shutting down your server you need to check certain settings because the Mail.box queue requires that you have no users connected to this server. Since you will have the server ties up for a while, at the server console, enter the following commands:

```
>set conf server_restricted=1 <-- prevents any users to connect
>drop all <---terminates any existing user sessions
```

The setting `server_restricted=1` will be reset to 0 at the next startup.

You might want to prevent users from connecting after upgrading your server until you have had time to check availability and ensure server functionality. To prevent access, type:

```
>set conf server_restricted=2
```

Later, to re-enable user connections, type:

```
>set conf server_restricted=0
```

Tip: Once your server is upgraded to Domino 6, you will be able to use your remote server console from your Domino Administrator Client, even if you denied user connections. The `Server_Restricted` setting doesn't apply to users listed as Administrators or Full access administrators of the server. In Domino R5, this setting was applied to all users with no exceptions.

Note that using the `server_restricted` command doesn't prevent any scheduled replication or mail routing operation between servers. You need to take care of disabling those separately.

Ensure that all mail has been delivered or routed

Open all Mail.box files on your server and ensure that there is no mail pending for delivery. At the console level check for any pending mail:

```
tell router show queues

Msgs State   Via  Destination

Transfer Threads: Max = 8; Total = 0; Inactive = 0; Max Concurrent = 4
Delivery Threads: Max = 8; Total = 0; Inactive = 0
```

Figure 6-7 Result of 'tell router show queues' command

The output of this command must show that there are no active router threads which are delivering mails. You can see in Figure 6-7 that the total number is zero for both transfer and delivery threads.

Tip: In Domino 6 you will be able to check mail.box status by issuing the following server command:

```
tell router list main
Mbx Note      ID          State      Size Count From
  2 000008FA 007285DB Pending    1389      1 Jean-Noel Koval/Cambridge/ITSO
```

This example shows you that there actually is mail pending for delivery.

Remove R5.x specific NOTES.INI settings

As with each new release of Domino, some NOTES.INI variables that were used in previous versions are now obsolete, and they can and should be removed. Lotus Notes/Domino 6 will ignore these settings; however, removing or commenting out obsolete settings is recommended.

The following R5.x NOTES.INI settings are no longer required:

- ▶ adminPInterval
- ▶ AdminPModifyPersonDocumentAt
- ▶ Config_DB (replaced by Report_DB)
- ▶ FT_LIBNAME=ftgt34 (not shipped anymore in Lotus Domino 6)
- ▶ LDAP_CountryCheck
- ▶ LDAP_Enforce_Schema
- ▶ LDAP_Strict_RFC_Adherence
- ▶ LDAP_UTF8results
- ▶ KillProcess (Fault Recovery now performs the function)
- ▶ MailClusterFailover (Configured by Lotus Domino 6)
- ▶ New_DNParse
- ▶ NNTPAddress (Not supported)
- ▶ NNTP_Delete_Days (Not supported)
- ▶ NNTP_Initial_Feed_All (Not supported)
- ▶ NNTP_Previous_X_Servername (Not supported)
- ▶ NNTP_Prohibite_NEWSNEWS_command (Not supported)
- ▶ Platform_Statistics_Enabled (Started automatically (not available on Linux); to disable it use Platform_Statistics_Disabled=1)
- ▶ Server_Name_Lookup_Noudapde (Configured by Lotus Domino 6)
- ▶ WebAuth_AD_Group
- ▶ WebAdmin_Disable_Force_GUI

From the ServerTasks line of your NOTES.INI file, you can remove the following tasks that are not used anymore by Domino 7:

Apple Talk, CLREPL, CLDBDIR, NNTP, Report, SMTP MTA, Object Collect
mailobj.nsf

Stop the Domino server

At the console level you can either enter **exit** or **quit** (or **q** if you are really hurried) and wait for the server to complete its shutdown. When ready, the server console is closed (on win32).

```
quit
23/09/2002 23:41:06 SMTP Server: Waiting for all tasks to complete
23/09/2002 23:41:06 Calendar Connector shutdown
23/09/2002 23:41:06 Index update process shutdown
23/09/2002 23:41:07 Schedule Manager shutdown complete
23/09/2002 23:41:07 Administration Process shutdown
23/09/2002 23:41:07 Router: Shutdown is in progress
23/09/2002 23:41:07 Mail Router shutdown
23/09/2002 23:41:07 Event Monitor shutdown
23/09/2002 23:41:07 Change Manager Robotic Administrator: Termination complete
23/09/2002 23:41:07 AMgr: Executive '1' shutting down
23/09/2002 23:41:07 AMgr: Executive '2' shutting down
23/09/2002 23:41:08 LDAP Server: Waiting for all tasks to complete
23/09/2002 23:41:08 RDEBUG Server: Waiting for all tasks to complete
23/09/2002 23:41:08 Change Manager Interface Monitor: Termination complete
23/09/2002 23:41:08 Change Manager Plan Control: Termination complete
23/09/2002 23:41:08 Change Manager Executive: Termination complete
23/09/2002 23:41:08 RunJava: Finalized lotus/notes/addins/changeman/ChangeMan Java task.
23/09/2002 23:41:08 RunJava shutdown.
23/09/2002 23:41:08 Agent Manager shutdown complete
23/09/2002 23:41:10 Database Replicator shutdown
23/09/2002 23:41:10 HTTP Server: Shutdown
23/09/2002 23:41:13 LDAP Server: All tasks have completed
23/09/2002 23:41:13 LDAP Server: Shutdown
23/09/2002 23:41:18 SMTP Server: All tasks have completed
23/09/2002 23:41:18 SMTP Server: Shutdown
23/09/2002 23:41:19 RDEBUG Server: All tasks have completed
23/09/2002 23:41:19 RDEBUG Server: Shutdown
23/09/2002 23:41:20 Stats agent shutdown
23/09/2002 23:41:30 Server shutdown complete
```

Figure 6-8 Shutting down the Domino server

6.5 Upgrade the server code

Before you start the actual Domino server upgrade, you should be aware of some changes in the server licensing. As described in detail in 2.1.1, “New Domino

Server licensing” on page 8, there are three different Domino server types available at installation time.

In this section, we cover server code upgrade steps for both UNIX and Win32.

For the UNIX platform

Important: This redbook is not an introduction to Domino for UNIX. You should be already accustomed to working with the UNIX operating system and running Domino on a UNIX server. If you need more details about running Domino on UNIX systems, refer to “Related publications” on page 545 for a list of recommended IBM Redbooks.

Lotus Domino 6 provides four new UNIX installation options:

- ▶ Add Data directory only, add additional directories to an existing Domino server.
- ▶ Installation of template files (possibility to overwrite existing templates or not to install any templates).
- ▶ Create /opt/Lotus soft link during installation (available only for installation of a single Domino Server).
- ▶ Install of Application Service Provider (ASP), option available after choosing to install a Domino enterprise server only.

Steps to upgrade a standalone UNIX Domino server

In this section we have detailed the upgrade steps for a standalone Domino server for Linux, but the instructions are applicable for all supported UNIX platforms.

For the purpose of this example, the Linux user that is used to run Domino is *notes* and the Domino server name is *DominoUnix*. When we start we are logged on as *notes*—not as *root*.

1. Ensure that your R5 server is not running. At the operating system level, issue the following command:

```
[notes@DominoUnix data]$ ipcs | grep 0xf81f
```

If your server is down, no output must be displayed, otherwise clean-up all semaphore and memory segments by running:

```
[notes@DominoUnix data]$ nsd -kill
```

2. Change to *root* user at an OS command prompt and go to your directory where you **untar** your install file.
3. Execute **./install** file and press Enter to validate.

4. A welcome screen will be displayed as shown in Figure 6-9, use the Tab key to validate.

Attention: Be sure that you are *root* user,—not *notes*—to install the Lotus Domino code. You can easily check this from the command prompt, since the prompt contains *root* instead of *notes*.

```
[root@DominoUnix data]#
```

```
=====
                        Domino Server Installation
=====

Welcome to the Domino Server Install Program.

Type h for help on how to use this program.
Press TAB to begin the installation.

-----
Type h for help
Type e to exit installation
Press TAB to continue to the next screen.
=====
```

Figure 6-9 Domino Welcome screen

5. Press the Tab key to continue.

```
=====
                        Domino Server Installation
=====

A lot of new features have been added to the Domino 6 Server.
In order to install your server correctly, please read the Domino
Server release notes first, then run your installation. Otherwise,
you may experience problems when using the new features.

-----
Type e to exit the Install program.
Press ESC to return to the previous screen
Press TAB to continue to the next screen.
=====
```

Figure 6-10 Domino Welcome screen with New Feature Alert

6. You'll see a couple of Licence Agreement screens next. The next screen (Figure 6-11 on page 88) asks you to read the full licence agreement. Press the Tab key to display the License agreement, then scroll down by using any key.

```

=====
Domino Server Installation
=====

In order to proceed with the installation of the Domino Server,
you must read and agree with the terms and conditions of the
Lotus Domino/Notes Software Agreement.

Press TAB to read the Lotus Domino/Notes Software Agreement.

-----

Type e to exit the Install program.
Press ESC to return to the previous screen
Press TAB to continue to the next screen.
=====

```

Figure 6-11 Licence Agreement screen

At the end of these screens, press Tab to validate your agreement or use Esc to go back to the previous screen.

```

EXCLUDED COMPONENTS: Notwithstanding the terms and conditions of any other
agreement you may have with IBM or any of its related or affiliated companies
(collectively "IBM"), the following terms and conditions apply to all
"Excluded Components" identified in this License Information document: (a) all
Excluded Components are provided on an "AS IS" basis; (b) IBM DISCLAIMS ANY
AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS INCLUDING, BUT NOT
LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED
WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE; (c) IBM will not be liable to you or indemnify you for any claims
related to the Excluded Components; and (d) IBM will not be liable for any
direct, indirect, incidental, special exemplary, punitive or consequential
damages with respect to the Excluded Components.

The following components in the Program are Excluded Components: (a) all third
party components, including third party components included or embedded in the
Program and components referenced in any LICENSE.TXT file included with the
Program or a fixpack or update to the Program, and (b) all source code
included with the Program.
Press the Escape key to go back to the previous screen
or
Press the Tab key to continue...

```

Figure 6-12 Licence Agreement validation

```

=====
Domino Server Installation
=====

You may proceed with the installation only if you agree to the
terms and conditions of the Lotus Domino/Notes Software Agreement.

-----

Type e to exit the Install program.
Press ESC to return to the previous screen.
Press the Spacebar to change the setting until you get the one you want.
Press TAB to accept a setting and continue to the next screen.

-----

>>> Do you agree to the terms of the license agreement ? [Yes]_

```

Figure 6-13 Last screen for licence agreement validation

Select Yes to accept the License agreement and to continue with the installation.

7. Installation of Data Directories only.

You have to select Yes if you want to add only new data directories to an existing Domino server. By default the answer is No; if you select Yes, be aware that no Domino code will be installed. If you are upgrading your Domino server, you don't need to change the default settings, just press Tab to continue.

```
The existing Program directory must be specified in order for
new Server Partitions to be created. However, existing Data
directories do not need to be listed. Any existing Data
directories that are listed will be installed to, and old templates
in those Partitions will be overwritten.

If you wish to add more than one Partition to your existing
Domino server, select "Yes" when asked if you want to run
multiple server partitions on this system. Otherwise you will
only be able to upgrade or install one Data directory.

Warning:
If you do not have an existing Domino Server on your system,
please select "No" for the option to add data directories only.

-----
Type e to exit the Install program.
Press ESC to return to the previous screen.
Press the Spacebar to change the setting until you get the one you want.
Press TAB to accept a setting and continue to the next screen.
-----

>>>Do you want to install data directories only? [No ]
```

Figure 6-14 Installation of Data Directories only

8. Select the type of Domino Server to install.

As mentioned earlier, you have to select between the three new types when installing the Domino server. The default selection is Domino Messaging; to select another type, use the spacebar and press Tab when your selection is identified. In our scenario, we selected Domino Enterprise server.

```
Domino Server Installation
=====

Select the type of installation you want.

-----
Type h for help.
Type e to exit the Install program.
Press ESC to return to the previous screen.
Press the Spacebar to change the setting until you get the one you want.
Press TAB to accept a setting and continue to the next screen.
-----

>>> Select Setup type : [Domino Enterprise Server]
```

Figure 6-15 Type of Domino Server to install screen

9. Install template files.

You can choose whether to install template files that are shipped with Domino server. This additional option is intended for administrators who are installing over a previous version of the Domino 6 server and wish to keep all the existing template files. In our case, since this is not an installation over an existing Domino 6 server, all the templates have to be installed. If needed, templates can be replaced by customized templates at the end of installation.

```
Domino Server Installation
=====

The optional installation feature for template files is designed for
users who are installing over a previous version of the Domino Server
and wish to keep all previous template files. If this is not an
installation over an existing Domino Server, all template files must
be installed.

Warning:
To ensure proper operation of your Domino Server, we highly
recommend installing all template files. Only select [No] if you are
an advanced user and you know that this server already has the latest
template files. The Domino Server will not run properly without the
latest templates.

Type e to exit the Install program.
Press ESC to return to the previous screen.
Press the Spacebar to change the setting until you get the one you want.
Press TAB to accept a setting and continue to the next screen.

>>>Do you want to install all template files for this Domino Server? [Yes]_
```

Figure 6-16 Installation of template files screen

10. Install an Application Service Provider kit (ASP).

This option allows you to configure a server as an Application Service Provider server. This type of server can only be configured after an Enterprise Server installation. The default selection is No.

```
Domino Server Installation
=====

The option to setup an ASP server refers to the configuration of an
Application Service Provider server. This type of server can only be
configured after an Enterprise Server installation.
Selecting "Yes" below will cause the Domino Setup program to configure
the server appropriately for ASP functionality. This will add security
features not present in a normal configuration, so do not select "Yes"
unless an ASP configuration is specifically required for this server.

The default value is "No", which is recommended for performing server
upgrades and/or non-ASP installations.

Type e to exit the Install program.
Press ESC to return to the previous screen.
Press the Spacebar to change the setting until you get the one you want.
Press TAB to accept a setting and continue to the next screen.

>>>Do you want to configure this server with ASP functionality? [No ]_
```

Figure 6-17 Configuration of Application Service Provider server screen

11. Select the directory location for the Domino binaries.

The default directory is /opt/lotus, and we accepted this for our installation.

```
=====
                        Domino Server Installation
=====

The program directory is the path where the Install program
installs the Domino program files. The Install program
automatically adds "lotus" to the path.

-----

Type h for help.
Type e to exit the Install program.
Press ESC to return to the previous screen.
Press ENTER to edit a setting.
Press TAB to accept a setting and continue to the next screen.

-----

Current program directory setting : /opt/lotus
_
```

Figure 6-18 Directory location for Domino binaries

With R5, you did not have to install the program files to /opt/lotus, but the server required an /opt/lotus symbolic link to function properly. Domino 6 no longer requires the /opt/lotus link, and so Domino 6 can coexist with R5 (still using /opt/lotus) or with other installations of Domino 6.

Table 6-2 Example of multiple installations

Version of Domino	Program file installation path
Domino R5	/opt/lotus
Domino 6.0	/opt/dom6a/lotus
Domino 6.0.1	/opt/dom6b/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 to that directory. Doing so will overwrite the symbolic link and the R5 install will no longer function properly.

You can change the location of your Domino binaries. To do this, press Enter, type your new directory path, and validate by pressing Enter again. The install program will append “lotus” to the end of your new directory path automatically.

For our single server, we chose to install only one version of Domino 6, so we pressed Tab to accept the default path.

12. Setup for partitioned Domino servers.

The next two screens concern the setup for a partitioned server on the machine. The default answer is No. For this example, we chose not to partition it and just pressed Tab to continue.

```
=====
Domino Server Installation
=====

You will now be prompted for information on how to install one or
more Domino Data Directories.

Please note that the UNIX user and group names asked for will own
all of the data directories specified.

The system will own the program files.

-----
Type e to exit the Install program.
Press ESC to return to the previous screen
Press TAB to continue to the next screen.
-----
```

Figure 6-19 Entering into the Partitioned installation screen

While Domino 6 gives you the ability to run different versions of Domino on a single server, you still have the option to partition a server. 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 feature that allows multiple installs requires *separate* program files, as well as *separate* data directories, for every instance, and so requires more disk space than partitioning.

```
=====
Domino Server Installation
=====

You can run more than one Domino Server on a single computer
at a time based on this installation. This feature is called
Domino Partitioned Servers, and requires separate Data Directories
for each Domino Server to be run.

-----
Type h for help.
Type e to exit the Install program.
Press ESC to return to the previous screen.
Press the Spacebar to change the setting until you get the one you want.
Press TAB to accept a setting and continue to the next screen.
-----

>>>Do you want to run more than one server based on this installation? [No ]
```

Figure 6-20 Domino partition option screen

13. Select your data directory

You are now prompted to indicate where your Domino data directory is located. By default the path is /local/notesdata. You can edit this path by pressing Enter, entering the path, and validating the new path by pressing

Enter. Press Tab to proceed to the next screen. On our server the data directory is /domino/data.

Domino Server Installation
The data directory is the path where the Install program installs the Domino data files.
Type h for help. Type e to exit the Install program. Press ESC to return to the previous screen. Press ENTER to edit a setting. Press TAB to accept a setting and continue to the next screen.
Current data directory setting : /domino/data

Figure 6-21 Selection of your data directory path

14. Select the UNIX user who will run the Domino server.

The default user is “notes.” If you want to change it, press Enter, edit your user’s name, press Enter again to validate, and then press Tab.

Domino Server Installation
Please enter the Domino UNIX user name. This UNIX user will own the Domino data files, and be used to run the Domino Server.
NOTE for the upgrade installer: The Domino UNIX user name/account name you specify here must be the same as the owner of the existing installed data files for proper operation of Domino.
Type h for help. Type e to exit the Install program. Press ESC to return to the previous screen. Press ENTER to edit a setting. Press TAB to accept a setting and continue to the next screen.
Current UNIX user setting : notes

Figure 6-22 Unix User selection

15. Select the UNIX group.

Select the appropriate UNIX group containing the UNIX users that will run the Domino server. By default the selection is “notes.” To edit this selection, press Enter, enter the appropriate group name, validate by pressing Enter, and press Tab to continue to the next screen.

```

=====
Domino Server Installation
=====

Please enter the Domino UNIX group. This UNIX group will own the
Domino data files. The Domino UNIX user must be a member
of this group.

NOTE for the upgrade installer:
Domino UNIX group/account group you specify here must be the same as
the owner of the existing installed data files for proper operation
of Domino.

-----

Type h for help.
Type e to exit the Install program.
Press ESC to return to the previous screen.
Press ENTER to edit a setting.
Press TAB to accept a setting and continue to the next screen.
-----

Current UNIX group setting : notes

```

Figure 6-23 UNIX group selection

16. Configuration review.

The following screen displays all settings that you have selected. If you agree with these choices press Tab to start the installation, otherwise press the Esc key to reconfigure, if needed.

```

=====
Domino Server Installation
=====
Installation settings:

  Installation type      : Domino Enterprise Server
  Install template files : Yes
  Configure to ASP Server: No

  Program directory     : /opt/lotus
  Data directory        : /domino/data
  UNIX user             : notes
  UNIX group            : notes

Press the Escape key to re-configure the settings
or
Press the Tab key to perform the installation...
-

```

Figure 6-24 Configuration review for final validation

17. Code installation.

After validating this last screen, the perl script checks whether your system runs the appropriate patches or APARs. If everything is correct no list will be displayed. However, if any patches or APARs are missing, the installation will proceed anyway, but you will not be able to launch your Domino server until you have applied the requested missing files.

```
Validating...

For the latest patch DB please go to http://www.lotus.com/ldd/checkos

This will check the Operating System level and tell you what is missing. Note, n
o patch list if all patches are present


The OS appears to have the correct patches .
Installing Domino Server kits ...

The installation completed successfully.

Please be sure to login as the appropriate UNIX user
before running Domino - Do not run as root.
```

Figure 6-25 Domino installation complete

Tip: If you want to ensure that you have all patches and APARS installed before upgrading any UNIX servers, you can download Check OS tool from:

<http://www.lotus.com/ldd/checkos>

This is the same script that is run during the installation.

For Win32 platform

1. Ensure that your Domino server is down. One way to do this is to open the Windows Task Manager to see if you have any Domino server processes running. The names of these processes usually start with the letter *n*.
 - a. Turn off the Domino service (no need to remove the service).
 - b. If you run a Domino R4.6.7a, remove the NT service by issuing the following code from a DOS prompt, in your Domino program directory:

```
>ntsvinst -D
```
 - c. Restart your Win32 server to clear off all memory segments.
2. After your Win32 restart has completed, run the setup program by selecting SETUP.EXE from your server install directory (either from a CD or a local drive); click Next for the next screen.



Figure 6-26 Domino Win32 Welcome screen

3. Licence Agreement screen

Use the Page Down key to read the complete licence agreement. If you agree click Yes, which is selected by default.

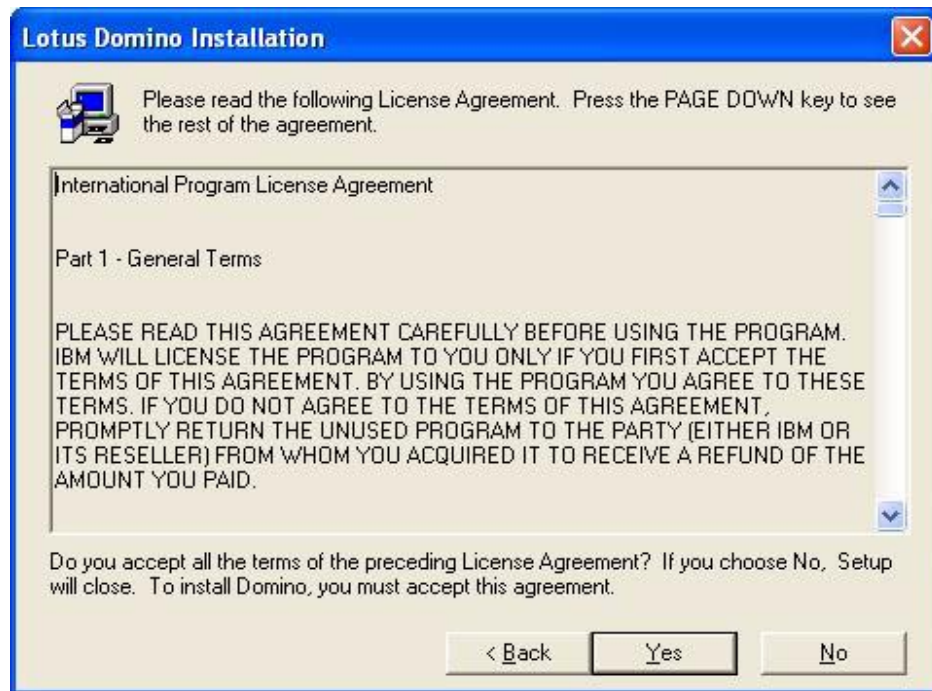


Figure 6-27 Licence Agreement screen

4. Specify your registration information, such as your name and your company's name, and click Next to continue.

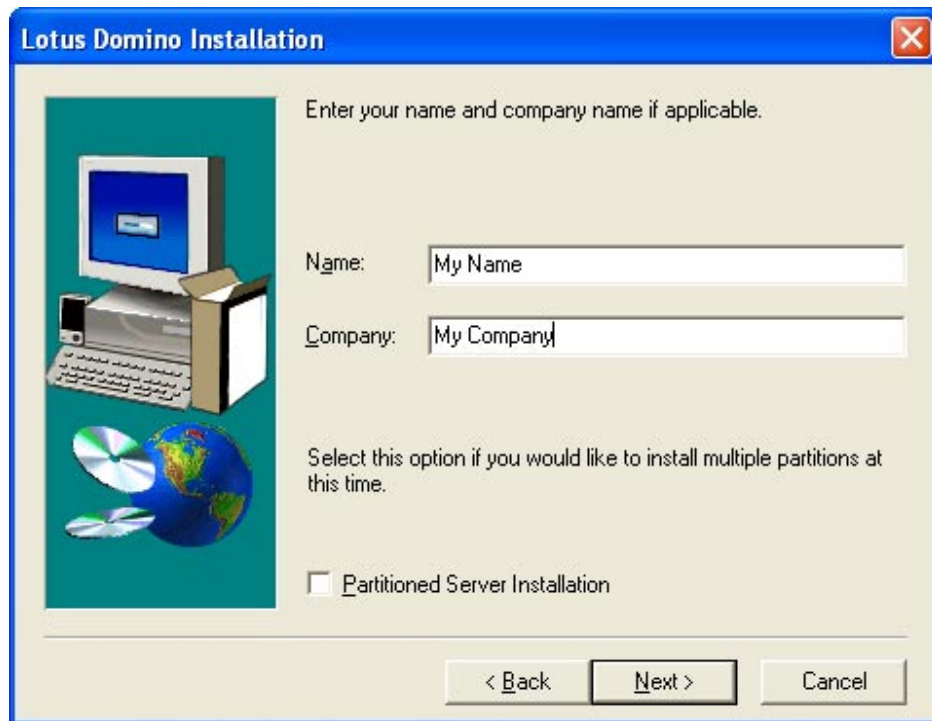


Figure 6-28 Company information

5. Select the type of Domino server to install.

Choose among the three displayed server installation types. The default setting is Domino Messaging Server; in our case we selected the Domino Enterprise Server.

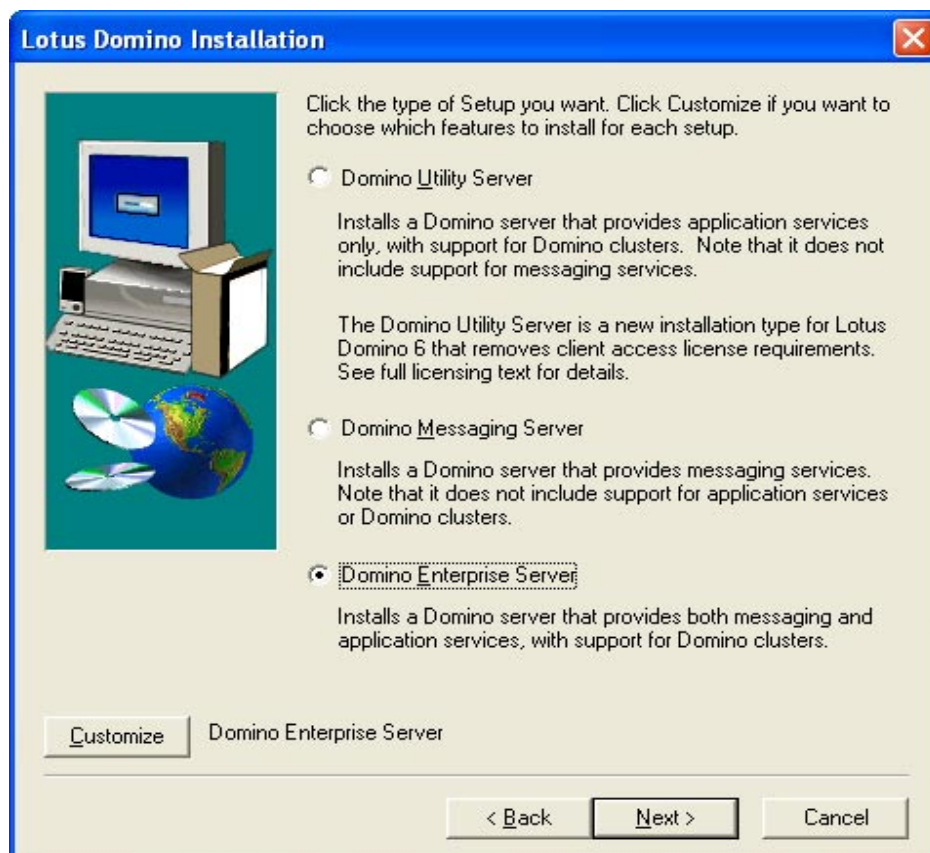


Figure 6-29 Type of Domino Server to install

Select the installation directory for both your program directory and your data directory.

By default, the installation will display the location where you have already installed your Domino R5 server. To upgrade the existing Domino R5 server, use the suggested, existing directories. Click Next to continue.

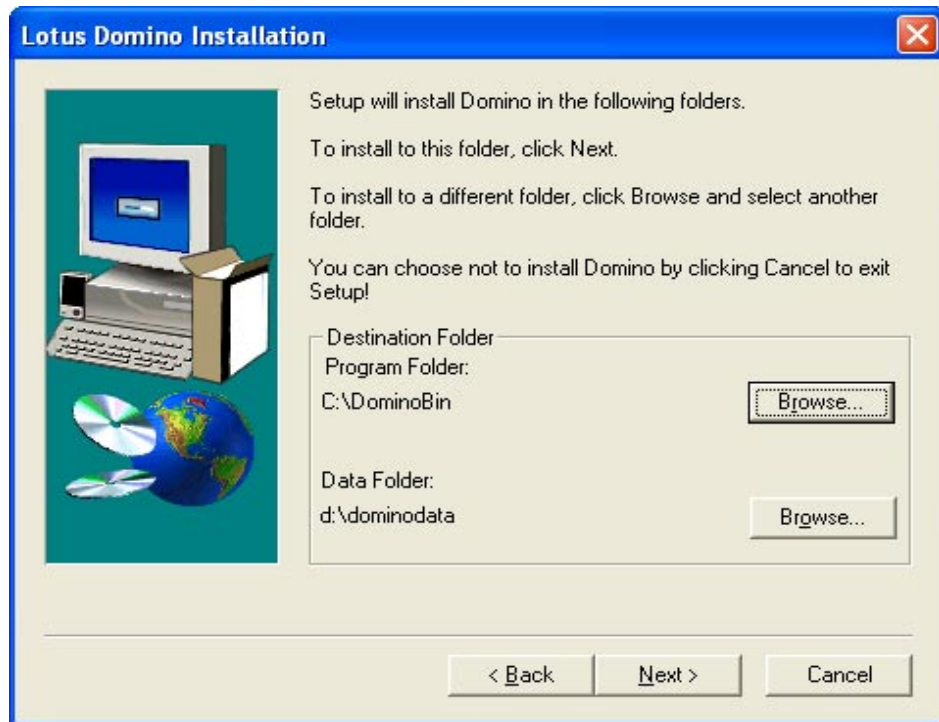


Figure 6-30 Directory location for Program and Data files

6. Select the components to install.

Select the components to be installed from the list by checking the necessary components. Under each component, you can click the button Change to display a list of more detailed of components to install (or not to install), when you have completed your selection, click on "Next" to continue.

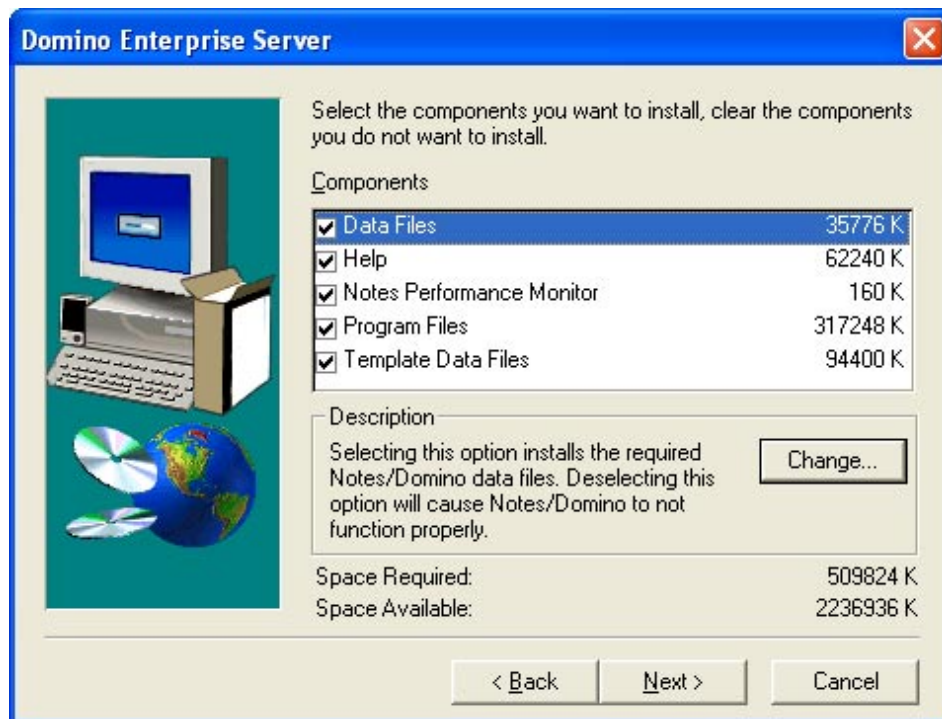


Figure 6-31 Selecting components to install

7. End of Domino installation.

The Domino install process is ready to install code. You can specify a Program group where you can launch your Domino server later if you don't want to start it as a service. By default the selection is Lotus Applications. Click Next to complete the installation process.



Figure 6-32 Program Group folder location

8. After the progress bar reaches 100%, the Congratulations screen is displayed. Click Finish to exit the installation.



Figure 6-33 Congratulation screen: Your server is now upgraded to Domino 6

6.6 Before restarting the server: Post upgrade tasks

Your server code has been successfully upgraded to Lotus Domino 6, but before you restart your server, some tasks need to be performed while the server is still down.

Replace standard templates with your customized templates

If you have created any customized templates, copy them back to the Domino data directory. Domino will automatically upgrade many system databases to Domino 6 design when you bring up the server for the first time.

Important: If you are upgrading your administration server and the design of your Domino Directory at the same time, follow these extra steps (only for your Administration server):

1. If you have changed the replica ID and the file name of Pubnames.ntf as suggested previously, rename it back to pubnames.ntf at OS level. Perform the same operation if you have done the same for admin4.ntf.
2. From an OS command line, go to your data directory and run the following command. The design task will update the design of the specified databases (in this case Domino directory and AdminP databases):

- For win32

```
>\data directory\c:\lotus\domino\ndesign -f names.nsf  
>\data direction\c:\lotus\domino\ndesign -f admin4.ntf
```

- For UNIX (using the user who will run the Domino server)

```
$notes@DominoUnix Data>/opt/lotus/bin/design -f names.nsf  
$notes@DominoUnix data>/opt/lotus/bin/design -f admin4.nsf
```

When done, rename both Pubnames.ntf and admin4.ntf back to the previous names that you have used in your customized template kit.

Run FIXUP program on Key System databases

While you still have your server down, run the following command from an OS command line to run a fixup on your key system databases.

1. for Win32 server

```
>\data directory\c:\lotus\domino\nfixup names.nsf -f -j -v -l  
>\data directory\c:\lotus\domino\nfixup admin4.nsf -f -j -v -l
```

2. for UNIX server

```
$notes@DominoUnix Data>/opt/lotus/bin/fixup names.nsf -f -j -v -l  
$notes@DominoUnix Data>/opt/lotus/bin/fixup admin4.nsf -f -j -v -l
```

Table 6-3 Explanation of FIXUP switches used

Switch parameter	Explanation
-f	Exhaustive fixup, all documents are checked.
-j	Include transaction logged databases. Without this option, fixup doesn't check logged databases.
-v	Exclude database views (faster) for all views that will be rebuilt by updall later, no need to check view at this moment.
-l	Log all processed databases (optional).

In general, you will not need to run FIXUP against your whole data directory, only on the key databases such as Domino Directory (names.nsf) or Administration Requests (admin4.nsf). You can also consider running this tool against your business-critical databases as well, but it's not mandatory, especially if you haven't encountered any database corruption before with these databases.

Tip: What does FIXUP do? FIXUP reads each item in a database and ensures that it is consistent with an expected state for that type of item (data notes, design notes, view indexes). If the item is inconsistent, it is either repaired when possible, or purged from the database. Views are also verified, and when FIXUP finds an inconsistent view, it marks it for rebuild. However, FIXUP does not rebuild any view—you have to use UPDALL to rebuild view.s

Run COMPACT program on Key System databases

After running FIXUP, and still from an OS command line, execute the following commands:

- For a Win32 server

```
>\data directory\c:\lotus\domino\ncompact names.nsf -c -i -K -F
>\data directory\c:\lotus\domino\ncompact admin4.nsf -c -i -K -F
```
- For a UNIX server

```
$notes@DominoUnix Data>/opt/lotus/bin/compact names.nsf -c -i -K -F
$notes@DominoUnix Data>/opt/lotus/bin/compact admin4.nsf -c -i -K -F
```

Table 6-4 Compact switches used

Compact switch	Explanation
-c	Use copy-style compaction (R4 mode) and recover unused white space.
-i	Ignore errors and allow compact to run anyway (only for copy-style).
-F	Enable “Document table bitmap optimization” from your database properties.
-K	Enable large UNK table (>64KB) use to prevent any interoperability problems.

Since you are in the process of upgrading your Domino server to Domino 6, you don't need to use -D switch (discard views). All the views and full-text indexes will be rebuilt anyway due to the change of the Global Text Retrieval (GTR) engine.

Tip: What does COMPACT do? COMPACT eliminates the white space (which results in file size reduction) or marks this white space available for use (no file size reduction). There is two styles of compact:

- Copy-style (R4 style) compact creates a temporary file, copies all the items from the old file to this new file, then deletes the old file and renames the temporary file with the old file name. To run copy style you need to have the same amount of available disk-space that the older file uses. If you run compact using copy-style against a 1 gigabyte database, you need to have an extra 1 gigabyte available on your Domino data directory.

A copy-style compact for your database checks the integrity of documents and creates a fresh new file.

During a compact using copy-style, the database is unavailable for users (including servers).

- In-place style (Default behavior of R5 and Domino6) does the compact in place and doesn't require a duplicate amount of disk space.

If you don't use transactional logging, the default compact in-place style will reduce the file size (compact -B).

If you use transactional logging, the default compact in-place style will only recover white space without reducing the file sizing (compact -b).

If a database cannot be compacted by a compact -B, then a copy-style is automatically tried by the server.

During a compact using in-place style, database can be opened by users

Run UPDALL program on Key System databases

After compact, and as you are in the process of upgrading your Domino server, rebuild views of your Domino Directory (names.nsf) and, alternatively, of your Administration requests (admin4.nsf) databases.

- For Win32 server

```
>\data directory\c:\lotus\domino\nupdall names.nsf -R
>\data directory\c:\lotus\domino\nupdall admin4.nsf -R
```

- For UNIX server

```
$notes@DominoUnix Data>/opt/lotus/bin/updall names.nsf -R
$notes@DominoUnix Data>/opt/lotus/bin/updall admin4.nsf -R
```

Table 6-5 Updall switch used

UPDALL switch	Explanation
-R (or -r)	Rebuild all used views.

Tip: What does UPDALL do? It rebuilds view indexes.

Convert the ODS for all databases

Upgrading the ODS level (from ODS41 to ODS43) for databases is a procedure you should consider doing early in the upgrade process, since you then will be able to take advantage of all the new database features after the conversion. You now have the choice of either running compact right away to convert to ODS43, or waiting for a steady state and converting your databases at a later time (in one or two weeks, for example).

From our own experience in an early deployment project at IBM/Lotus software, we can recommend that you upgrade the ODS when your server has reached a steady state, not only because it will take time to convert, but having a phased approach will provide more flexibility if you have to revert to R5 for any reason.

Converting your databases to the new ODS can be done easily by running a simple compact program from an OS command line (as you did to compact names.nsf and admin4.nsf). To enable large UNK tables (greater than 64KB) on each database), use the following command:

```
>compact -K
```

Tip: Compact can run on a subdirectory. For instance, if you want to run compact only for the databases located in the directory applications, issue the following command:

- For Win32 server:

```
>\data directory\c:\lotus\domino\ncompact applications\ -K
```

- For UNIX server:

```
$notes@DominoUnix Data>/opt/lotus/bin/compact applications/ -K
```

COMPACT, FIXUP and UPDALL support indirect files. This means that if you want to run these programs against several databases located on your server directory, you can create a file which contains the relative path to your Domino directly for your targeted database and save it with an *.ind extension, copy it on your Domino data directory, and launch it from the server console as follows:

```
> load compact myindirectfile.ind
```

You can run it offline as well as from an OS command line, by creating your own batch file.

Upgrading all views and full-text indexes

The Global Text Retrieval (GTR) engine used to build and maintain views and full-text indexes has been upgraded, so that all your views and full-text indexes will be rebuilt automatically when your server is restarted after the code upgrade. However, because this task is CPU- and disk-access-intensive, we advise you to run this program before restarting your server. This way you avoid any user complaints or delays when they try to open their mail files or applications for the first time after the upgrade.

From an OS command prompt type:

- For Win32 server:

```
>\data directory\c:\lotus\domino\nupdall -RX
```

- For a UNIX server:

```
$notes@DominoUnix Data>/opt/lotus/bin/updall -RX
```

The switches -RX will force a rebuild of view and full-text indexes. You can use several instances of UPDALL against different subdirectories at the same time if you have a multi-processor server. Do not specify more than the number of CPUs available on your machine, less one, instances. So, if you have a 4-way system, you can use 3 instances of UPDALL.

- For Win32 server:

```
>\data directory\c:\lotus\domino\nupdall applications1\ -RX  
data directory\c:\lotus\domino\nupdall applications2\ -RX  
data directory\c:\lotus\domino\nupdall applications3\ -RX
```

- For a UNIX server:

```
$notes@DominoUnix Data>/opt/lotus/bin/updall applications1/ -RX  
$notes@DominoUnix Data>/opt/lotus/bin/updall applications2/ -RX  
$notes@DominoUnix Data>/opt/lotus/bin/updall applications3/ -RX
```

Again, be aware that running updall on your whole Domino Directory will take quite some time. It is not easy to estimate the time, as this depends on the number of your databases, view complexity, number of full-text indexes to rebuild, CPU power and number, disk performance, and so forth.

Important: If you decide to not rebuild views and full-text indexes off-line, then at least run Updall -RX against your Condensed Directory Catalog (Dircat) if you use it. See the previous section about Directory upgrade for details about it.

New Global Text Retrieval version

Some major changes have been included in the new release, 4.1, of the search engine. The version of GTR that R5 had was 3.4. In addition, Domino uses the NSF buffer manager for memory services, which improves caching and balances memory between NSF and FT. Furthermore, a new search processor results in closer integration of text retrieval and significantly faster Boolean processing.

Some of the benefits of the new GTR engine are the following:

- ▶ Performance gains
 - Better handling of booleans
 - FTSearch Limit used by engine
 - Caching of result data (GTR uses the UBM now)
- ▶ Resource utilization improvements
 - Lower indexing memory footprint (6 MB per document limit is gone), GTR memory use improved, now using Notes Memory Services
- ▶ Capacity
 - Up to 16 terabytes per index (versus 2 gigabytes before)

Delete BUSYTIME.NSF

In Domino 6, BUSYTIME.NSF has been upgraded, and its design will be automatically upgraded to the new design at the first server startup.

However, if you want start from a clean database, you can remove your previous BUSYTIME.NSF (at OS level) before restarting the server. When the server loads the Schedule task (SCHED) it will repopulate this database, with the appropriate information for the users who have this server configured as their home mail server. For any clustered servers, before you restart your upgraded server, refer to the discussion about free time on a clustered environment.

General comments before you restart your server

In this section we detail some general comments and instructions related to Log.nsf, Catalog.nsf, mail.box, and Transaction logging that should be considered before restarting the server.

Log.nsf

You can run the commands Fixup, Compact, and Updall against the log.nsf database. However, we suggest that you move your previous log.nsf database away from the Domino data directory and let the server create a new one at startup. In this case you will benefit from the new design, and the database will already have the new ODS version. You will not need to run fixup, compact, and updall on this database, so you will save time because usually this database is

quite large. For general performance considerations, we advise you to keep this database as small as possible and to use logging only when needed. Do not enable a logging option if you don't need it. The size of your log.nsf can be adjusted by the following NOTES.INI parameter:

LOG=Logfilename, log_option, not_used,days,size

Table 6-6 Log options

Parameter	Description
logfilename	Name of the log file, usually Log.nsf. You can also specify another location outside of the Domino data directory.
log_option	1 = Log to the console 2 = Force database fixup when opening the log file 4 = Full document scan
not_used	Always set to 0 (zero); not currently used.
days	The number of days to retain log documents.
size	The size in bytes of each document.

Consider leaving the default settings, especially for the parameters log_option, days, and size (log=log.nsf,1,0,7,20000).

Catalog.nsf and Mail.box

If you use a catalog database on your server, you can remove the previous database from your Domino data directory, and let the server create a new one with the new template. As for log.nsf, this new database will be created using the new ODS and will be populated with the last information available when the Catalog task was run.

The same approach can be used for your server mail.box (or mail1.box, mail2.box and so forth, if you use several mail.box files): you can move these files (do not delete them immediately, keep them as a back-up) and let the server create new ones at start-up.

Transactional logging

You now have the ability to have some view updates logged into your Transaction log file, and then have a faster restart in case of server failure. Since the server will just have to do an incremental update from the transaction log, instead of having to rebuild inconsistent views, this will save a huge amount of time. This is particularly true for views in Domino Directory, which is why, your Domino Directory is set to use Transaction logging and has been updated to ODS43. Both \$Users and \$ServerAccess views will be logged, unless you have disabled this option in your pubnames.ntf template for these two views.

To verify if these views are “logged,” open your Domino Directory with Domino Designer 6, expand the view panel, select a view that you want to check, select Display view properties, and select the 5th tab from left (see Figure 6-34).

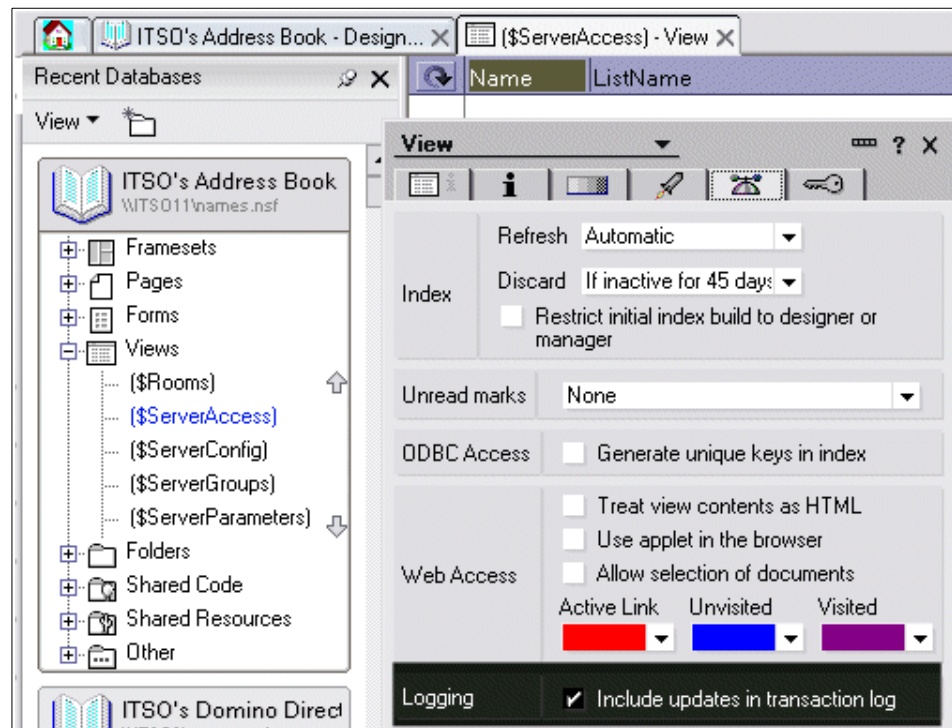


Figure 6-34 View Logging option in Domino Designer 6

This feature will be explained in more depth in later chapters.

Tip: If you want to know all the switches available for FIXUP, COMPACT, UPDALL, DESIGN, etc., at the server console (or using a remote server console) prompt, type:

```
>load compact -?
>load fixup -?
>load http -?
...
```

to display all available parameters.

Do not use FIXUP, COMPACT, or UPDALL unless you are sure of what you are doing. If in any doubt, do not hesitate to contact support. An incorrect use of these programs can have bad outcomes.

6.7 Start your Domino Server (now running Domino 6)

When the server restarts, it will upgrade some system databases and will prompt you to indicate if you want to upgrade the design of your Domino Directory. Be sure to reply *No* by pressing N at the server console level. You have already upgraded the design, either when running on R5, or just after the code upgrade (described earlier in this chapter).

However, if by mistake you reply Y (yes), your Domino Directory design still will not be upgraded since you changed the filename of pubnames.ntf and the template name. The Design task will not be able to locate the design and will skip the upgrade.

When the message “Database Server Started” is displayed at the console level, the server is running and can accept any user’s connection.

Attention: With Lotus Domino 6, by default your Administration server will run the LDAP task, even if you have removed this task from your NOTES.INI:

```
Servertasks=
```

You can use the TELL LDAP QUIT command on the server console to stop LDAP running, if needed.

If you decide to not run LDAP service for your Domino Directory, use the NOTES.INI variable:

```
DisableLDAPOnAdmin=1
```

and ensure that LDAP is not set in the Servertasks line of the NOTES.INI file.

6.8 Post-upgrade tasks

Before you are finished with the upgrade of your server, some post-upgrade tasks remain to be performed:

- ▶ Re-enable Domino as a Win32 service.
- ▶ If you have set the **server_restricted** parameter to 2, reset it to 0 to allow users to connect to this server. (This also allows you to perform some tests). Do this by entering:

```
set conf server_restricted=0
```
- ▶ If you use this server for LDAP services, recreate full-text indexes on the appropriate directory.

- ▶ Test your server to make sure that:
 - Clients can connect to the server
 - You can open any database on the server
 - Send/receive any mail from the server is working
 - Send/receive any mail from Internet is working
 - Name look-up is working
 - You can stop and restart your server
 - Server loads scheduled tasks, such as Design, Catalog, Statlog
- ▶ Re-enable replication of your Domino Directory
- ▶ Add new notes.ini variables for ND 6 to improve server performance.
- ▶ Make sure transaction logging is disabled on mail.boxes to prevent mailbox problems if a corrupted message causes repetitive server crash.
- ▶ If you use the Archiving settings for Transactional Logging, perform a full backup because some DBIID have changed (for all databases you have compacted using copy-style switch or fixup with -j switch).
- ▶ If you have decided to wait for any ODS conversion, but you want to recover the unused space on your databases, you can create a program document to run **compact -r** against your application or mail directories. Do not run **compact** at your root directory level, otherwise you will revert your Domino Directory, Administration Requests databases, and so forth to the previous ODS!

Attention: As explained previously regarding Directory upgrade, all new databases that you create (copy, replica) on this server will be created using ODS43, and reverted to ODS41 when **compact -r** is run.

If you create a database with the file extension *.NS5, this database *will not be* converted to ODS43, unless you manually change the file extension to *.NSF and run **compact** on it. Changing the file extension from *.NSF to *.NS5 at the OS level does not downgrade your ODS level if this database is already at ODS43.

6.9 ODS conversion

Attention: Upgrading your application design is different from upgrading your ODS level on your server. As discussed in the previous chapter, upgrading your ODS will not impact your application design.

Do not start to modify any application structure (design) with Lotus Domino Designer 6 until you complete your upgrade process, or unless you have fully tested that any modification done with Lotus Domino Designer 6 will work in a mixed environment.

A good example of application design change is the new template for Team Room (teamrm6.ntf), which is not supported for R5 clients.

If you didn't convert all your databases to the new ODS during your upgrade process (for instance, because you wanted to wait a few weeks to achieve a steady state), you have two options to bring up your database at the new ODS level 43:

- ▶ Run **compact** off-line (that is, with the server down, at an OS command line).

- For Win32 server:

```
>\data directory\c:\lotus\domino\ncompact directorytoconvert\
```

- For a UNIX server:

```
$notes@DominoUnix Data>/opt/lotus/bin/compact directorytoconvert/
```

- ▶ Use a scheduled program document.

From your Domino Administrator 6 client, select the server where you want to enable a program document, select the configuration tab, expand the Server section in the left frame, select Programs, then click Add Program or Edit Program. (See Figure 6-35 and Figure 6-36.)

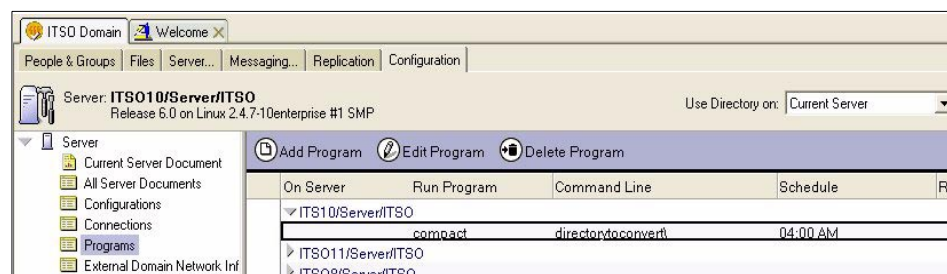


Figure 6-35 Location of Programs view into the Domino Directory

Edit Server Program
 Cancel

Program: compact

Basics Administration

Basics		Schedule	
Program name:	compact	Enabled/disabled:	Enabled
Command line:	directorytoconvert\	Run at times:	04:00 AM each day
Server to run on:	ITS10/Server/ITS0	Repeat interval of:	0 minutes
Comments:	upgrade to new ODS43	Days of week:	Sat

Figure 6-36 Example of scheduled program document for ODS conversion

Tip: If you have used a program document to run **COMPACT directory \ -r** you just have to remove the **-r** switch and schedule it to run Saturday at 4:00 AM.

Finally, regardless of the method that you choose to perform your ODS conversion, you will not need to rebuild any view or full-text indexes because they are not related to the ODS format.



Lotus Notes client upgrades

This chapter provides detailed instructions for upgrading the Notes 6 clients.

It describes the preparation that should be done prior to installation, the actual step-by-step upgrade procedure, and the setup options available.

7.1 Preparation: Know your environment

This section discusses the information that you should have at your disposal when beginning the client upgrades. Upgrading the clients is the most visible part of the upgrade to the user community. How this is handled will determine the success of the upgrade from the user's point of view.

7.1.1 Determine the hardware and OS level of each machine

Table 7-1 gives the requirements for the hardware and OS for the Lotus Notes 6 client.

Table 7-1 Client hardware and OS requirements

Platform	Windows 95 Windows 98	Windows 2000 Windows XP	Macintosh	Windows NT
Supported operating system versions	Windows 95 2nd edition installer minimum) Windows 98	Windows 2000 Windows XP Professional	Macintosh OS_9 Macintosh OS_X	Windows NT4
Service Pack Requirements		W2K - service pack 2		Service pack 6a
Processors	Intel Pentium	Intel Pentium	Power PC	Intel Pentium
RAM Minimum Suggested	64 MB 128 MB or more	128 MB 256 MB or more	128 MB 256 MB or more	64 MB 128 MB or more
Disk space required ¹	275 MB	275 MB	OS 9: 175 MB OS X: 250 MB	275 MB
Monitors	Color monitor	Color monitor	Color monitor 256 colors or greater	Color monitor

¹ More may be required if databases are replicated or copied locally.

Before you install the client, be sure to double check the hardware requirements for the release of Lotus Notes that is being deployed by looking in the Release Notes.

The system drive of the workstation also needs some space to perform the installation. The minimum disk space requirement for client installation is 36 MB of free space on the C:\ drive to run the installation program. If the user's temporary folders are located on a drive other than drive C:\, the minimum disk space requirement is 32 MB of free space.

7.1.2 Physical location of the machine

Whether you are upgrading the clients individually or through an automated process, you should have a current inventory of the physical locations of the workstations. This information will help you plan the order in which to perform the upgrades. For example, you may decide to upgrade all users on the 4th floor or in one office. Your support team will be able to respond more quickly to issues that result from the upgrade if they know where the users are. For larger implementations, some organizations decide to assign an on-site support person to the floor/area/office which was upgraded the day before. A physical inventory of the workstations makes planning for this possible.

7.1.3 Administrative rights to the workstation

To successfully install, upgrade, and use Lotus Notes 6, users must be allowed both Write and Modify permissions to the Program directory, Data directory, and all associated subdirectories.

If you are upgrading Lotus Notes on a Windows NT, 2000, or XP computer, you must have administrator rights to the system. On a Windows NT 4.0 computer, log in as an administrator or set administrator-level privileges for All Users. This can be done from the command line.

Windows NT, 2000, and XP users should log onto their computers with administrative rights to install Lotus Notes 6. For cases in which administrative rights are not available, enable the setting "Always install with elevated privileges." Refer to the Release Notes for the most current information on permissions required when installing as a non-administrator.

Options for installing the Lotus Notes client on Restricted or Standard/Power User computers are described in the Microsoft Windows 2000, Windows XP, and Windows Installer documentation.

7.1.4 Current Lotus Notes clients

Be aware of the client versions that are in your environment. It is especially important to know that all of the R4 and R5 clients have been upgraded *before* you start upgrading the designs of custom databases. To plan an efficient and complete upgrade, track the client levels that are accessing your servers.

Fortunately, once you upgrade the servers to Domino 6 there is an easy way to keep track of who has upgraded their client to Notes 6. Domino 6 servers track client information on the Administration tab of the person documents. This information is recorded when the Notes 6 client initiates dynamic client configuration (ndycng.exe) at start up. Because it is part of the Notes 6 client

code that reports to the server, you will not be able to determine whether a user is on R4 or R5 from the directory, but you will be able to determine that they are not using a Notes 6 client.

Client Information	
Notes client license:	Lotus Notes
Notes client machine:	ITSO-WP3
Notes client platform:	Windows/NT 5.0 Intel Pentium
Notes client build:	Build V60_09242002NP
Network account name:	
Change request:	None

Figure 7-1 Client information is recorded in person documents

Check the Lotus Notes Developer Domain for utilities that can analyze your server logs for client levels (<http://www.lotus.com/ldd>). Also, if you enable license tracking, you can create a private view in the license tracking database, which will tell you the basic levels of clients which are accessing your servers (R4, R5, N6). See 16.5, “License tracking” on page 517 for more information.

7.1.5 Notes applications already being used

Determine which Notes applications users are accessing. If any of them are mission-critical, test their functionality thoroughly with the Notes 6 client prior to upgrading users who are dependent on those applications.

7.1.6 Mail and calendar delegation situation

Notes users who have delegated their calendar or mail to another individual should be upgraded at the same time as that individual. We have seen this most frequently in the case of an executive who has delegated his or her calendar to an executive assistant. If it is absolutely necessary to upgrade them at different times, be sure to upgrade the assistant first so that they will always be able to access the executive’s mail file (Notes 6 client can access R5 and R4 mail files). In the case of a group of users who share their calendars through delegation or use the busy time feature to check each other’s schedules, an effort should also be made to upgrade them simultaneously.

If you have a large organization you will need to create a mechanism for tracking which users have access to other users’ mail files so that they are upgraded in the proper order. Only a detailed analysis of how your users are working together can give you this information.

7.1.7 Upgrade restrictions

People and departments have very different pressure points in their schedules. It would be foolish to add to their difficulties by scheduling an upgrade for one of those times. Interview managers in departments to determine optimal upgrade windows.

7.1.8 Comfort level with new technologies

Try to gauge how much support a particular user or department may need. For departments which typically require more support it may be wise to slow down the rollout so that your staff has time to address the questions. Because of the similarities between R5 and the Notes 6 client, the questions should be minimal. Plan ahead for questions by creating a FAQ Web site or a discussion database.

7.2 Prepare to install the client

This section describes how to prepare a workstation for installation of the Lotus Notes 6 client.

7.2.1 Hardware and OS

1. Verify that the workstation's hardware and OS meet the requirements for the Lotus Notes client. Check the release notes for any changes to these requirements.
2. Verify that you have administrative access to the OS.
3. Temporarily disable any screen savers and turn off any virus-detection software.
4. Make sure that all applications, including Notes, are closed to avoid losing data or corrupting shared files. You may be forced to restart the machine if the Windows Installer software has to be installed.

7.2.2 Back up the following essential files

Back up the files identified in Table 7-2 so that you can reinstall R5/R4.6 clients if absolutely necessary. Keep these files in a safe place until you have determined that there will not be a reason to roll back to an earlier version of Notes.

Note: Because Notes 6 uses a different ODS, you will not be able to use the files with an R4 or R5 client once Notes 6 has upgraded them.

Table 7-2 Critical files to be saved prior to upgrade

File	Default location
notes.ini (notes preferences on the Mac)	For Lotus Notes 4.6 clients, System Directory (for example, c:\winnt) For Lotus Notes 5.x clients, Notes Program directory (for example, c:\lotus\notes)
desktop.dsk (notes 4.6) desktop5.dsk (notes 5.x)	Notes data directory
names.nsf	Notes data directory
user id file	Notes data directory
bookmark.nsf	Notes data directory
local databases (*.nsf)	Notes data directory and subdirectories
local database directory links (DIR)	Notes data directory
customized notes database templates (*.ntf)	Notes data directory and subdirectories
user.dic (personal dictionary entries for spelling checker)	Notes data directory

7.3 Install the Notes 6 client

This section describes in detail how to install Notes 6 clients.

7.3.1 Client options

The Notes client, Designer client, and Administration client are bundled together on the installation CD. During installation the user has the option to install any one, two, or all three of the clients. If you want to limit the options available to your users, use a transform file to customize the installation. See the details about creating these files in 16.1.3, “Customizing client installations with transform files” on page 476.

7.3.2 Detailed instructions for installing the client

If you know that the Windows Installer software has been installed with the operating system, you can use **msiexec.exe** on the command line, or **setup.exe** to initiate the installation. Table 7-3 shows sample command lines for installing Lotus Notes.

Table 7-3 Sample installation commands

Type of install	Command lines
Transform install	<pre>msiexec /i "Lotus Notes 6.msi" TRANSFORMS="custom.mst"</pre> Use this if you have a transform file for customizing the installation.
Transform silent install	<pre>msiexec /i "Lotus Notes 6.msi" /qn TRANSFORMS="custom.mst"</pre> Use this if you have a transform file for customizing the installation and you don't want the end user to see any of the installation screens.
Silent install with fail/success prompt	<pre>msiexec /i "Lotus Notes 6.msi" /qn+</pre> Use this command if you don't want the end user to see any of the installation screens, but you do want them to be notified when the installation is complete.
Silent install	<pre>setup.exe /s /v"/qn"</pre> Use this command if you don't want the end user to see any of the installation screens.
Verbose logging	<pre>setup.exe /v"/L*v c:\temp\install.log</pre> Use this command if you want a log file created to help track the installation (either for troubleshooting or just confirmation).

Run **setup.exe** from the installation CD to start the Notes 6 install program. Setup.exe checks for the existence of the Windows Installer system and installs it if necessary. If this happens, the installation will appear to be very quick, and you will have to reboot the machine.

After the machine is rebooted, the Notes installation starts. You will see the following series of dialog boxes:

- ▶ Welcome to the Installation Wizard for Lotus Notes 6 - Click Next.
- ▶ License Agreement - Click "Yes, I accept."
- ▶ Customer Information - Notes will gather this information from the currently installed client. You can modify it, if appropriate.
- ▶ Installation Path selections - The current Notes installation paths will be shown. The user can change the paths if desired.

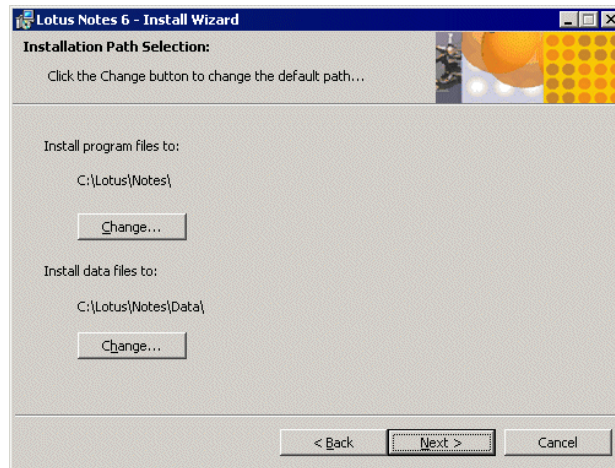


Figure 7-2 Installation path

- ▶ Custom Setup - Uses the standard Windows Installer interface to customize the installation:
 - It defaults to a Notes Client only installation (no Designer or Administration)
 - Without Client Single Logon feature
 - Without Migration Tools
 - Allows changes to what is going to be installed. You can choose to install only one or all three of the clients (Notes, Admin, Designer) and make more specific customizations by expanding each of the sections.

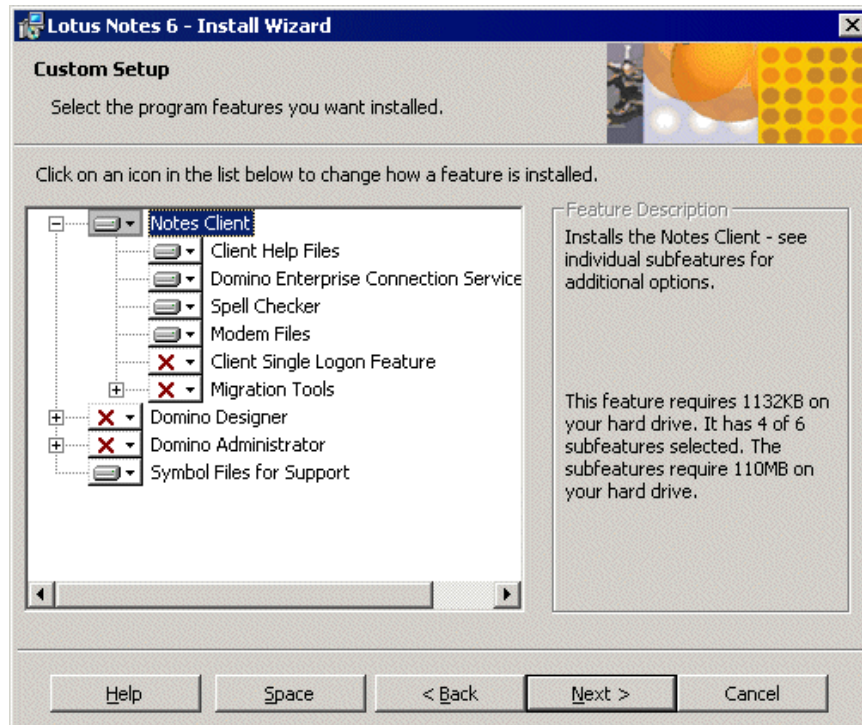


Figure 7-3 Customizing the setup

- Ready to Install the Program -This is the last chance to change the installation options or opt out of the installation. Click Back to return to the previous screens. Click Install to continue the installation.

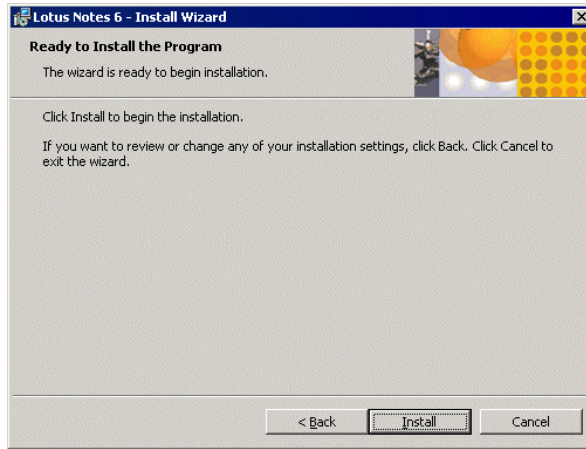


Figure 7-4 Last chance to change installation options

- ▶ While the Notes clients are being installed, a progress bar is displayed.
- ▶ Figure 7-5 shows the message you will receive when the wizard is finished.

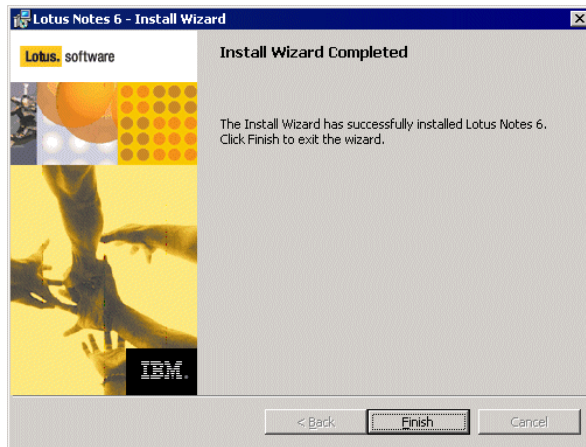


Figure 7-5 Wizard complete

Start the client from the Notes icon which has been placed on the desktop. You will see a message about compacting the databases. Once the compaction has finished the status bar will indicate that several databases are being upgraded to the Lotus Notes 6 design.

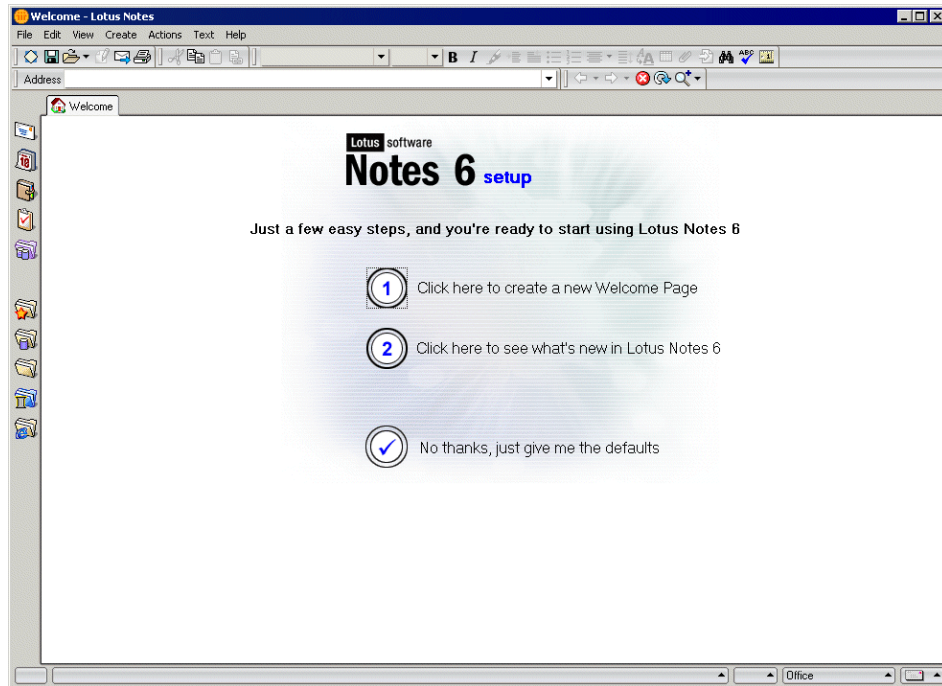


Figure 7-6 Initial Welcome Page of the Notes client

An initial welcome page gives the user the option to:

- ▶ Create a new welcome page.
- ▶ Click on a link to view new features in Lotus Notes 6. This directs the user to the help file that is installed with the client and is an excellent source of information.
- ▶ Start working in Notes with a default welcome page, which has links to:
 - Mail
 - Calendar
 - Contacts (Personal Address Book)
 - To Do List
 - Personal Journal - A personal journal is not created by default when the client is installed. If a user clicks this icon they are given the options to specify the location of their personal journal or to create a new one.
 - Tip of the day

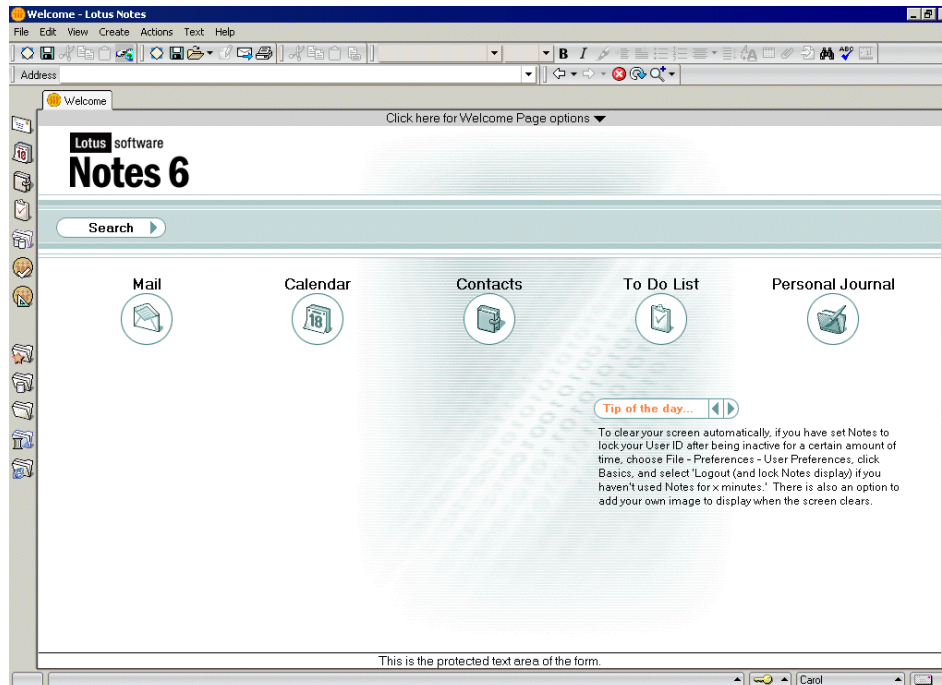


Figure 7-7 Default Welcome page

Only the personal address book is upgraded to the Notes 6 design automatically. The mail file (which also contains the calendar and to do items) is not upgraded automatically, unless the server administrator has configured seamless mail upgrade.

7.3.3 Setting up the Personal Address Book preferences

When you upgrade to Lotus Notes 6, Notes automatically upgrades the design of your Personal Address Book. The first time you open your Personal Address Book after upgrading, Notes should open your Personal Address Book profile and ask you to set up your preferences. If it doesn't, you should open your personal address book and select Tools -> Preferences from the action bar to open the profile.

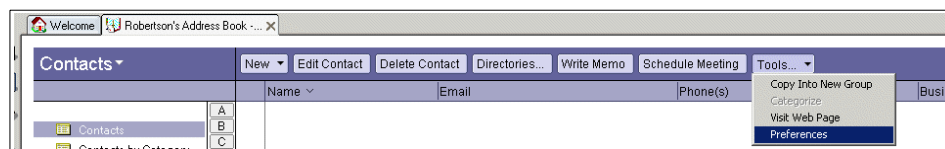


Figure 7-8 Navigating to Personal Address Book Preferences

To customize the address book, fill out the preferences form:

- ▶ Select an Address Book owner. Generally this is the person whose Notes client has been upgraded and who is the primary user of the address book.
- ▶ Select whether to sort alphabetically new groups that you create.
- ▶ Select whether to allow LDAP queries of the address book to elicit detailed information. This option lets you search your address book by categories such as country or phone number when looking up users during mail addressing.
- ▶ Choose whether to format your contacts “Firstname Lastname” or “Lastname Firstname.” You can also update all the current entries so that all previous and future entries will be formatted in the same way.
- ▶ Choose a style for the Business Cards in your address book. You can scroll through the styles by clicking the right and left arrow buttons.

Save & Close

Preferences

Address Book owner: Doug Robertson/BeaconHill/ITSO

☐ Sort all new groups by default

☒ Allow detailed LDAP queries of this address book

Newly created Contacts should have names formatted as:

☐ Firstname Lastname

☒ Lastname Firstname

Update all entries

Default address format for all contacts:

Format 1

Format 1

First Last
Company
Street Address
City, State/Prov. Zip/Postal
Country/Region

Used in:
Australia, Canada, United States

Figure 7-9 Sample Preferences document for a Personal Address Book

- ▶ Click Save and Close.
- ▶ You may be informed that the address book needs to be indexed. If so:
 - Click OK to close the dialog box.

- Go to the Database Properties -> Index tab.

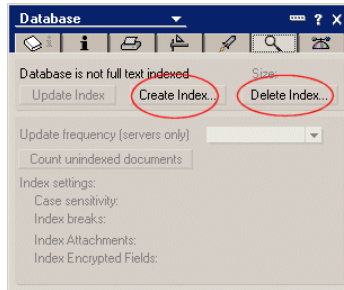


Figure 7-10 Creating an index

- Delete the current index by clicking the Delete button.
- Create a new index by clicking the Create button.
- The Notes client will create a new index.

7.3.4 Configuring Upgrade-by-mail

Upgrade-by-mail is a feature that sends an e-mail notification to specified users to upgrade their Notes clients and optionally, their mail file designs. It is intended for upgrading clients from previous versions of Notes (R4.x to R5.x, R5.x to Notes 6.x). It can be configured to upgrade the client from one version of Notes 6 to another version of Notes 6; however, you should consider Smart Upgrade for doing that.

The upgrade notification contains two buttons that users click to upgrade their clients and mail files. Figure 3-3 on page 27 shows an example of the mail the user receives.

- ▶ The Install Notes button launches a Notes client installation program from a directory on a network drive to which users have access.
- ▶ The Upgrade Mail File button replaces the user's current mail template with a locally stored Notes/Domino 6 mail template or another specified template, like a customized mail template. Users must upgrade their Notes clients to install the Notes/Domino 6 mail file template locally, before they upgrade their mail files.

Important: To use Upgrade-by-mail to upgrade mail file designs, users must have at least Designer access to their mail databases. If users do not have this level of access, use the mail conversion utility (see 7.4.1, “Use the convert utility on the server” on page 137) or seamless mail upgrade (see 7.4.3, “Seamless mail upgrade” on page 141) to update mail file designs.

Detailed settings/instructions

1. Create an installation directory on a file server to which all users have network access, then copy all Notes installation directories and files to this folder.
2. Address the Notification Message.
 - a. In the Domino Administrator, open the server on which your users' mail files reside.
 - b. Click the Messaging tab.
 - c. Open the Mail Users view. Select the recipients of the message and then click Send Upgrade Notifications. If you are going to use a group to address the message, just select one user and then add the group after the upgrade notification document opens.

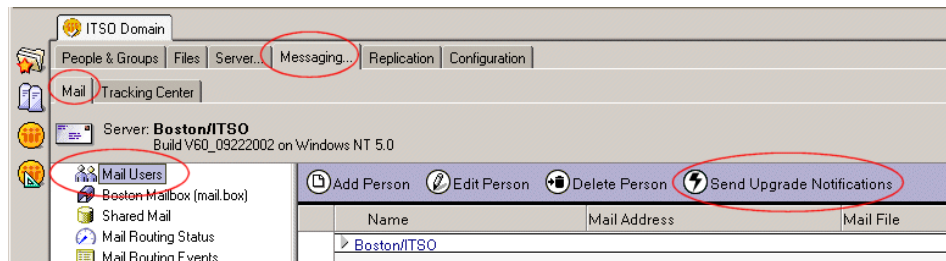


Figure 7-11 Send Upgrade Notifications button

- d. In the Upgrade Message document, complete the To field.

Tip: Create a mail group and address the upgrade notification message to the group. This will allow you to keep track of the recipients more easily. You can notify your help desk that the people listed in that group have been sent the message. This will help them be more prepared for questions about the message.

Tip: You can also send upgrade notifications from the Domino Directory without opening the Domino Administrator client.

3. Configure the client upgrade information section.
 - a. On the Basics tab you have 3 choices for type of upgrade notification:
 - i. Upgrade Notes Client and Mail Template to Notes 6 or higher. Use this for Notes 4.x, 5.x, or 6.x clients that are upgrading to a new version of Notes 6.

- ii. Upgrade Notes Client and Mail Template to pre Notes 6 versions. Use this for Notes 4.x or 5.x clients that are upgrading to a new version of Notes 4.x or 5.x.
 - iii. Convert local cc:Mail, MS Mail/MS Exchange data to Notes. Use this to migrate the local data of other mail systems. This is usually a one-time procedure done as part of a mail migration.
- b. Click the Yes radio button in the “Notify me when users complete mail conversion” section if you want to be notified.
 - c. Add information in the additional information section. This information will be sent in the e-mail to the recipients of the upgrade notification.

Address... Send

Upgrade Notification

From: Admin ITSO/ITSO

To: Marcia Robertson/ITSO

Subject: Upgrading to the latest version of Notes.

Basics | Client Versions | Software Distribution

Select the type of upgrade notification to send out:

- ☒ Upgrade Notes Client & Mail Template to Notes 6 or higher
- ☐ Upgrade Notes Client & Mail Template to pre Notes 6 versions
- ☐ Convert local cc:Mail/MS Mail/MS Exchange data to Notes

Notify me when users complete mail conversion:

- ☒ Yes
- ☐ No

Include additional information in notification:

Your administrator has set up this message to perform these steps for you automatically when you hit the button(s).

Remember to click on the Install New Notes Software button first!!!

Figure 7-12 Basics tab of the Upgrade Notification form

- d. On the Client Versions tab, enter a build number to prevent upgrades of Notes clients running the specified build or a later build. When the user clicks on the upgrade client software button, it will query the client to determine its build. If your users are already on Build Number 171 (all 6.x clients will show up as Build Number 171) enter something higher than 171. This will force the client software to be re-installed.

Subject: Upgrading to the latest version of Notes.

Basics | Client Versions | Software Distribution |

Select which versions to upgrade:	Client Version / Build number matching table:	
Do not upgrade Notes if the workstation uses build 300 or later.	Build Number	Lotus Notes Version
	171	6.0x
	166	5.0x
	147	4.6x
	145	4.5x
	138	4.1x
	136	4.0x
	114	3.0x

Fill in the build number that you are upgrading the end-user to. If the end-user is already using the build you specify or later, they will only be asked to perform the mail template update.

Figure 7-13 Client Versions tab of the Upgrade Notification form

- e. Move to the Software Distribution tab.
- f. In the Notes Install Kit Paths section, enter the directory path in the "Root path for Install kits" field using the following format:

\\server_name\shared_drive_name\installation_folder_name\

You can also use a drive mapping if your users all have the same drive mapping to the location of the installation files:

f:\upgrades\

Tip: You must have a "\ " at the end of the line.

- g. In the "Path for Windows 95, 98, NT, 2000" and "Path for Macintosh PPC" fields, enter the file path to the installation file following the format above, but include SETUP.EXE in the path.

\\server_name\shared_drive_name\installation_folder_name\setup.exe

You can also use a drive mapping if your users all have the same drive mapping to the location of the installation files:

f:\upgrades\setup.exe

You can also use a relative path in this field (relative to the path you set in step f).

\setup.exe

4. Complete the mail template information section (optional).
 - a. Enter the template name of the existing mail files. This is the name found on the design tab of the mail file's database properties and will be

something like StdR50Mail. The default field value is a wildcard character (*), which means that the user's mail file will be updated no matter what design it is based on.

Tip: If you want to make sure that your users do not update the design of their mail files, enter a bogus template name in this field. The code in the button will not execute if the mail file does not have a matching template name in its database properties.

- b. Verify that the mail template filename is correct. Notes will fill this field in for you with the default Notes 6 template filename (mail6.ntf). You will only need to change this if you have created a mail template with a different filename and distributed it with the software.

Important: The new mail template must be in each user's data directory to enable the Upgrade Mail File button sent in the upgrade notification message. Therefore, it is important that your users click the Upgrade Mail File button *after* they click the Install Notes button.

- c. By default the "Ignore 200 category limit" check box is selected. This option overrides a default that limits the creation of folders in a database to 200. If you want no more than 200 folders created, unselect the check box.
- d. If you are upgrading IMAP clients, select the "Mail file to be used by IMAP mail clients" check box.
- e. (Optional) If you want to upgrade custom folders to the Inbox design automatically, select the "Upgrade custom folders" check box.
- f. (Optional) To prompt the user before upgrading custom folders, select the "Prompt before upgrading custom folders" check box.
- g. (Optional) If you want to provide additional information to your users, complete the Additional Information field.
- h. (Optional) Select whether or not to be notified after users have upgraded their mail file designs.

Click Send to send the Upgrade by Mail notification message.

7.3.5 Changes to the Notes client

Notes no longer uses the desktop file to rebuild the bookmarks, as was the case with R5. The desktop file still exists, as desktop6.ndk, but it is used only to configure the Notes workspace. When you upgrade from R5 to Notes 6 the desktop5.nsf is renamed to desktop6.ndk. Bookmarks are kept in bookmark.nsf.

Bookmarks and the workspace have been completely separated. In R5 the ECL was housed in the desktop5.dsk. In Notes 6 it has been moved to the personal address book.

7.3.6 Rolling back to R4 or R5

Only in a very rare situation would you ever need to roll a client back to R4 or R5. More than likely the reasons will be personal or political, rather than technical.

If you ever do encounter this situation, use the following steps to roll back to a previous client:

1. Move the user's ID file to a safe location.
2. Uninstall Notes 6 by using the Add/Remove Software utility in the Control Panel.
3. Delete the Lotus Notes Data directory structure to remove all Notes 6 files. (If you don't, the resulting personal address book and welcome page will have the Notes 6 design). Double check for personal databases the user might have created and keep a copy of those in a separate place.
4. Install the required Notes client version.
5. Copy the notes.ini file, saved prior to the upgrade, into the appropriate directory (R5 - Lotus Notes directory, R4.6 - c:\winnt).
6. Copy the remaining files, saved prior to the upgrade, into the appropriate directory (default = c:\lotus\notes\data.....). You can check the notes.ini file to determine where the data directory was for the previous installation. The second line of the notes.ini file defines the data directory:

Directory=c:\lotus\notes\data

7. Start Notes.

Worst case scenario: You don't have pre-upgrade copies of the files

Because Notes automatically upgrades the personal address book, it has the Notes 6 On Disk Structure and Notes 6 design. If you have to revert to an earlier version of the client, it is easiest to use a copy of the personal address book which was saved before you upgraded to Notes 6. If you don't have a copy there is a way to downgrade the personal address book:

1. Prior to removing the Notes 6 client and data files, use the Notes 6 client to make a copy or replica of the personal address book. When prompted for the location and name of the resulting file use the *.ns5 extension (for example names2.ns5). This will create a copy with the R5 ODS. It is a good idea to create this copy of the personal address book somewhere other than the default Notes data directory (to avoid confusion).

2. Move the user's ID file and downgraded personal address book to a safe location.
3. Uninstall Notes 6 by using the Add/Remove Software utility in the Control Panel.
4. Delete the Lotus Notes Data directory structure to remove all Notes 6 files. (If you don't, the resulting personal address book and welcome page will have the Notes 6 design). Double check for personal databases the user might have created and keep a copy of those in a separate place.
5. Install the required Notes client version.
6. With a Notes 5 client, open the file you just named and replace the design with the R5 personal address book template. You will need to use the ID file of the person who created this name and address book to open it and replace the design.
7. Rename the downgraded file to names.nsf. Put it in the data directory prior to setting up the R5 client.

This method will get the user up and running on Notes 5 again. However, without the recommended backup files they will lose any customizations they had made to their workspace, their bookmarks, their dictionary, and so forth. The personal journal is not upgraded automatically to the Domino 6 ODS or the version 6 personal journal design. Unless you have compacted the database with the Notes 6 client or applied the new design to it, it should function when put back into the R5 environment. If it does have the Domino 6 ODS (43), use the Notes 6 client to create a copy of the personal journal and use a file name with the *.ns5 extension (as in step 1).

7.4 Upgrading the mail file design

When you upgrade users' mail files to the Notes 6 mail template, you can upgrade one file at a time, use the mail conversion utility to automate upgrading the design, or use seamless mail upgrade. Be sure that you have already upgraded the Domino server that hosts the mail files and the Notes clients that access them to Domino 6, or users will not be able to use the features in the new design. Upgrade mail files at a time when users won't be accessing them—for example, early in the morning or over a weekend. Notify users that their mail files will be unavailable during the upgrade.

7.4.1 Use the convert utility on the server

Important: Before executing the convert utility on the server it is best to turn the mail router off by issuing:

```
tell router quit
```

Be sure to turn it back on when you are done using the convert utility.

This is a very powerful and easy way to upgrade the mail files. You must take care that you only upgrade the mail files that you intend to upgrade. It is fairly easy to unintentionally upgrade someone's mail file. *For a complete list of switches and functionality see the Lotus Domino 6 Administrator Help database.*

1. The convert utility is used at the console of the server and has the following basic syntax:

```
load convert path\filename existingtemplatename newtemplatefilename
```

Note: The syntax does not seem to be consistent. The utility wants the *template* name of the existing template (usually StdR50Mail), but it wants the *file* name of the new template (usually mail6.ntf). The name of the template being used now can be found in the Database Properties of the mail file on the Design tab.

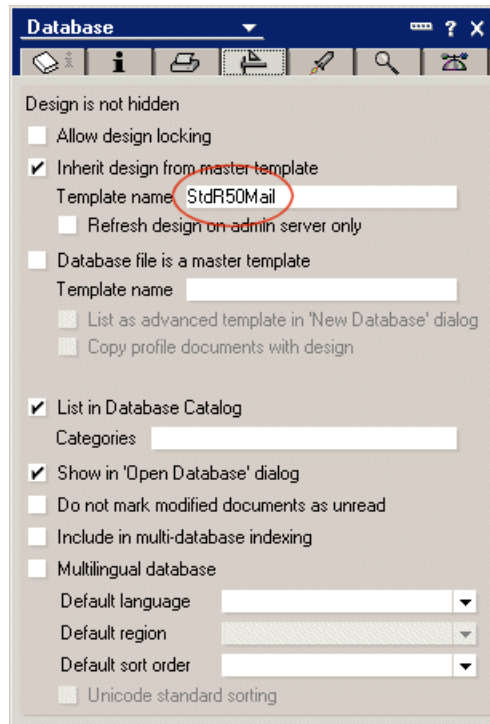


Figure 7-14 How to find the template name of the current template

A simple convert command is:

```
load convert mail\jsmith StdR50mail mail6.ntf
```

2. This tool becomes very powerful when you add switches and wildcards. For example you could convert every database in a directory (no matter what design it is currently using).

```
load convert mail\* * mail6.ntf
```

3. Use a text file to tell the convert utility which files to act on. Create the text file with a simple editor, like notepad, and save it to a directory on the server. The textfile should have 1 line for each mail file you want to upgrade:

```
mail\jsmith
mail\cjones
```

The command line to use the convert utility with a text file for input is:

```
load convert -f c:\temp\maillist.txt * mail6.ntf
```

You can also use the convert utility to create a list of the mail files in a directory. This is the easiest way to get the correct format for the text file:


```
load convert -L c:\temp\maillist.text mail\*
```

This will result in a file with a listing of all the users in the mail directory:

```
mail\jsmith  
mail\cjones  
mail\stomas  
mail\bmorris
```

4. You can add the -u switch to the convert command to automatically upgrade the design of the users' folders to the Notes 6 mail design. If any of your users' mail files are currently on the 4.6 design do not use this switch.

```
load convert -u mail\bjones StdR50mail mail6.ntf
```

Users can update their own folders through a built-in agent in their client. The agent is found by selecting: Actions -> Upgrade Folder Design. By using the convert utility with the -u switch, this is done for them.

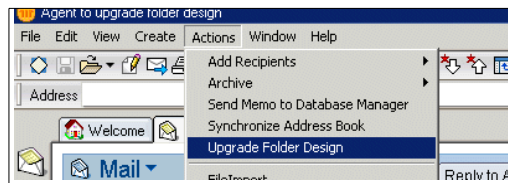


Figure 7-15 Built-in agent to upgrade folders

7.4.2 Manually upgrade the design of the mail file

This is not a scalable solution, but occasionally every administrator has to do this.

1. Open the mail file of the user with a Notes 6 client (the ID file used to open the mail file must have at least designer access to the database).
2. Click File -> Database -> Replace Design.

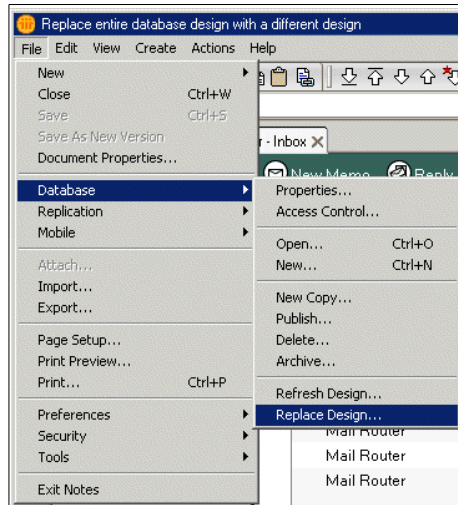


Figure 7-16 Replace design manually

3. Select your server in the Template server field. Always use the template from the user's mail server so that you get the most up-to-date design elements.

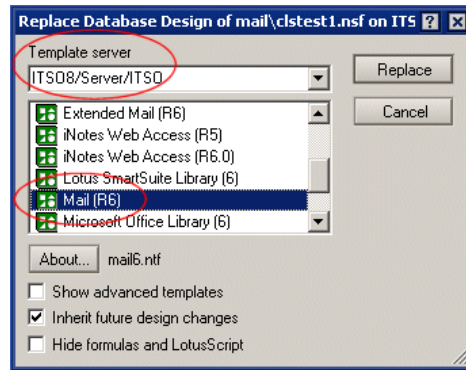


Figure 7-17 Template Server and Template Choices

4. Select the Mail (R6) template from the list of templates.
5. Click Replace. Click Yes when asked whether you really want to replace the database design. The mail file will be upgraded. The progress of the design upgrade is shown in the status bar.



6. Close the mail file and open it again to see the full effect.

7.4.3 Seamless mail upgrade

A very easy way to upgrade users' mail files at the same time as their clients are upgraded, is to use seamless mail upgrade, which is a new feature in Notes and Domino 6. This feature is most useful for large upgrade efforts since it will allow mail file upgrades to occur automatically and virtually in the background. A little forethought can save administrators a lot of work.

Before making use of the Seamless Mail Upgrade feature, your Directory and mail server should already have been upgraded to Domino 6. Delete references to setup profiles in the person documents in the directory because they will override policies.

1. Create a desktop settings document specifying the appropriate client level and mail file templates:
 - a. In the Administrator client click the People & Groups tab.
 - b. Click Settings in the navigation panel.
 - c. In the action bar click Add Settings and select Desktop.

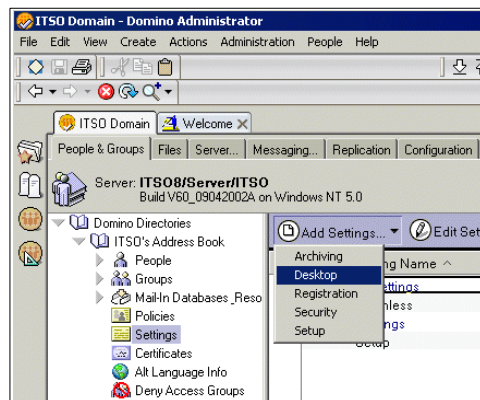


Figure 7-18 Navigate to Desktop Settings

- d. On the Basics tab of the Desktop Settings document go to the Mail Template Information Section. Input the information about the mail template your users are currently using, the mail template you want them to use, and the client level that will trigger the automatic upgrade.

Mail Template Information		Inherit from parent policy:	Enforce in child policies:
Prompt user before upgrading mail file: (If user's have multiple machines or custom folders that they don't want the design replaced on)	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes
Old design template name for your mail files:	<input type="text"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
If Running This Version Of Notes:	Use This Mail Template:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Ignore 200 category limit:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Mail file to be used by IMAP mail clients:	<input type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Upgrade the design of custom folders:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Prompt before upgrading folder design:	<input type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Notify these administrators of mail upgrade status:	<input type="text"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Figure 7-19 Mail Template Information - unconfigured

- e. You will need to decide whether to prompt the user with the option to cancel the upgrade of their mail file. Unless your users have multiple machines on which they run the Notes client, we recommend that you not give them the option. In our experience it will cause some confusion and if they are unsure about it they will click Cancel. They will not be prompted to allow the upgrade the next time they log in and the opportunity for the seamless upgrade will be lost.

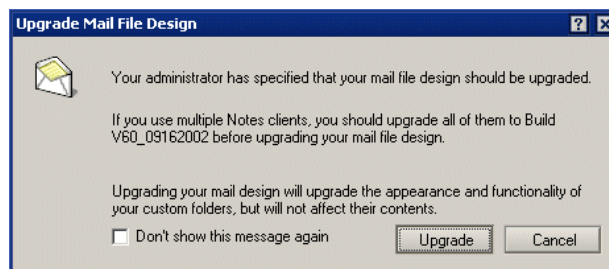


Figure 7-20 Dialog box the user sees during seamless upgrade

- f. Fill in the field "Old design template name for your mail files." Use the template name of the template—not the file name of the template. In most cases this will be StdR50Mail, unless you are using a customized mail template and have changed the name. The name of the design that is being used can be found on the Design tab of the Database Properties.
- g. Fill in the Client version section. Put in the Build number of the client that is being installed on your users' workstations. Here you need to use the syntax for the Build number for the client. This can be found on the splash

screen that comes up when you click on Help -> About Notes in the menu:

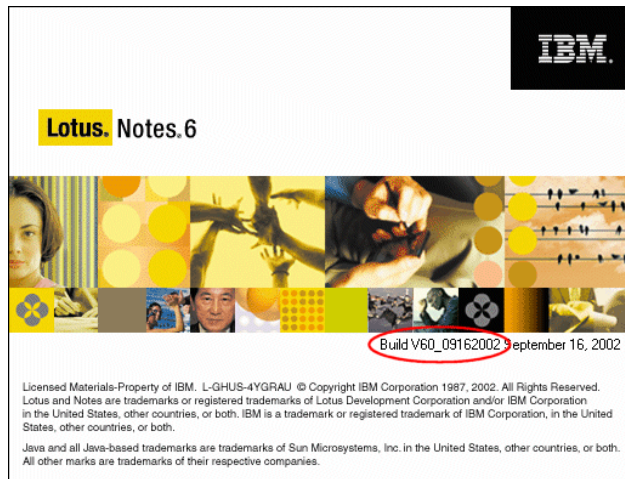


Figure 7-21 Finding the build number of the Notes client

- h. Fill out the field for the mail template that should be applied to the mail files. Put in the *file name* for the new mail template, for example mail6.ntf.
- i. There are several other options which you can choose:
 - Ignore 200 category limit - Select this option to override the default that limits the creation of folders in a database to 200.
 - Mail file to be used by IMAP mail clients.
 - Upgrade the design of custom folders - all folders will be upgraded to the design of the \$Inbox folder. This will give a more consistent look and feel to the mail file.
 - Prompt before upgrading folder design - users will be given the option to defer the folder upgrade.
 - Notify these administrators of mail upgrade status.

Mail Template Information		Inherit from parent policy:	Enforce in child policies:
Prompt user before upgrading mail file: (If user's have multiple machines or custom folders that they don't want the design replaced on)	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes
Old design template name for your mail files:	StdR50Mail	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
If Running This Version Of Notes:	Use This Mail Template:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Build V60_09162002	mail6.ntf	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Ignore 200 category limit:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Mail file to be used by IMAP mail clients:	<input type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Upgrade the design of custom folders:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Prompt before upgrading folder design:	<input type="checkbox"/> Yes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Notify these administrators of mail upgrade status:	Carol Sumner/Cambridge/TSO	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Figure 7-22 Completed Desktop Settings - Seamless Upgrade document

- j. Create a policy specifying the desktop settings document you just created or edit a policy and add this desktop settings document to it.
- k. Apply the policy to the users, if it has not been done already.
- l. Test to make sure that the seamless upgrade is working properly.

When a user's client is upgraded it will notify the server of the upgrade. The server checks the policy statements to see if it needs to take any action because of the upgrade. If it finds a desktop settings document with seamless mail upgrade configured in a policy that has been applied to this user, it will upgrade the mail file immediately. This is a one-time call. Once the client has been successfully upgraded it will not make another upgrade notification call to the server.

Tip: You can recreate an upgrade notification from the client to the server by deleting all but the first 3 lines of a notes.ini file and restarting the client. This could be helpful in a distributed administrative environment where neither the end user nor the local administrator has enough rights to upgrade the mail file manually (you must have designer access). By making the client "think" it is setting up for the first time, it will send the upgrade call to the server and the upgrade will be performed by the server. If any special configuration settings were in the notes.ini file they must be re-entered after using this tip.

7.5 Upgrading the client in the future

Once you have upgraded your users to Notes 6 you will be able to make use of another new feature, Smart Upgrade. Smart Upgrade notifies users to update their Notes 6 clients to later releases. Lotus Notes Smart Upgrade uses policies and settings documents to help manage updates. See 16.1.5, “Smart Upgrade” on page 484.

7.6 Standard templates/files installed with Notes 6

Table 7-4 is a partial list of the standard templates installed with Notes 6, and their functions.

Table 7-4 Standard templates and files installed with Notes 6

Template/File	Function	Comment
pernames.ntf	Creates personal address book	Necessary at first startup
cache.ntf	Creates the cache.ndk	Necessary at first startup
log.ntf	Creates the client's log file	Necessary at first startup
bookmark.ntf	Creates the bookmarks	Necessary at first startup
headline.ntf	Creates headlines	Necessary at first startup
pernames.ntf	Creates/upgrades personal address book	Necessary at first startup
desktop6.ndk	Holds settings for the workspace	Gets upgraded from desktop5.dsk or created new at first startup
mail6.ntf	Standard notes mail template	Can be used to upgrade local mail file
mailbox.ntf	Creates outgoing mailbox for users who are disconnected from the network	Needed when in Island mode
journal6.ntf	Creates the personal journal	Nice to have - some personal welcome pages use this to set up a journal for the user, otherwise it can be created manually
archlog.ntf	Creates archive logging db	Needed if archive logging is turned on

Template/File	Function	Comment
doclbms6.ntf	Creates a document library for MS Office documents	Nice to have, has to be created manually
doclbs6.ntf	Creates a document library for Smartsuite documents	Nice to have, has to be created manually
doclbw6.ntf	Creates a generic document library	Nice to have, has to be created manually
discsw6.ntf	Creates a discussion database	Nice to have, has to be created manually
Help\help6_client.nsf	Help file	This is what comes up when the user presses F1
Help\readme.nsf	Release Notes for this client code	Contains last minute information about this release

7.7 Help and documentation

The Lotus Notes 6 client comes with a very extensive help file for end user-type of questions. Users can access it by pressing the F1 key from anywhere within their client. The help is context-sensitive. For example, if a user is in the calendar and presses the F1 key, the page about Calendar and Scheduling is displayed in the right pane when the help file is opened. The help file opens in its own window so that you can simply press the Esc key or click the x in the upper right hand corner to close it.

Some administrators put a bookmark to the help file on the bookmark bar to make it more easily accessible for their users. See Chapter 15, “Policy-based administration” on page 449 to learn how to do this for all of your users at one time.

If you are looking for a good introduction to the new features of the Lotus Notes client you should also look in the help file. Click the Contents button in the upper left-hand corner to see the Table of Contents structure for the help file. The first item on the list is “What’s new in IBM Lotus Notes 6.” This is an excellent resource for end users as well as technical support people.

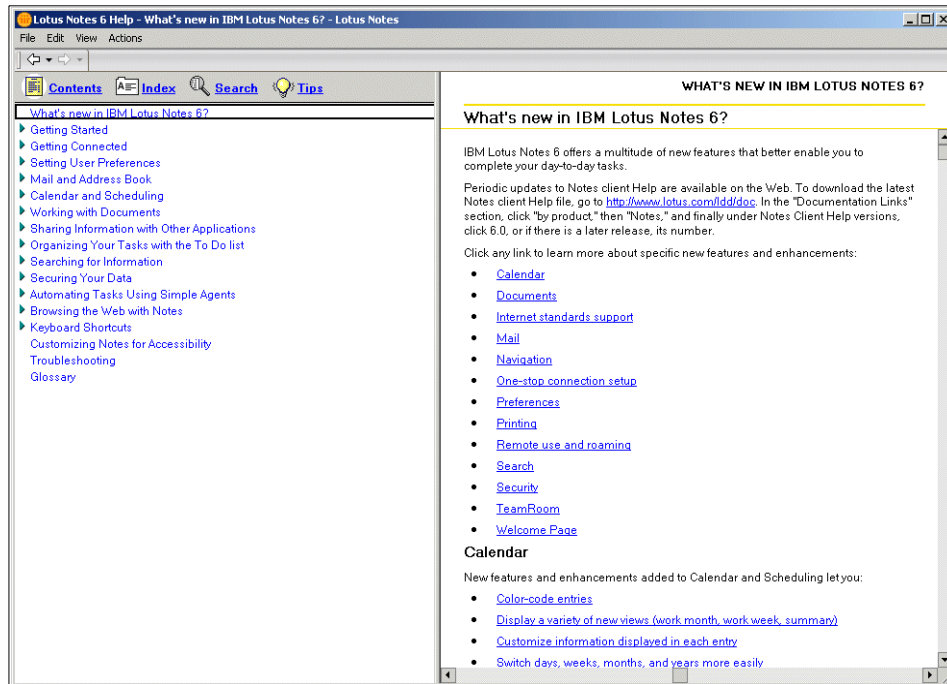


Figure 7-23 What's New in Notes 6



Monitoring your infrastructure

This chapter gives you an overview of the tools built into your Domino Administration client to track server activity. Monitoring an infrastructure includes performing a variety of actions, which can be summarized as follows:

- ▶ Monitoring your Domino infrastructure at the application level
- ▶ Monitoring your infrastructure to determine if your Domino servers are using available system resources efficiently
- ▶ Analyzing data collected with your monitoring tools
- ▶ Defining system application baselines and assessment which denote that you are on track
- ▶ Determining trends and making observations for future capacity planning and better use of your existing resources (hardware and software)

Domino Administrator 6 provides tools to help you perform these tasks, ensure that your environment runs in an appropriate manner, and assist you when some corrective action is necessary.

8.1 Monitoring configuration and results databases

Everything that happens on the Domino system is an “event.” Every message that appears in the server console has been generated by an event task. Domino generates events all the time. To monitor your system, you have to decide which events you want to know about, based on what type of information is important to you.

To configure an event, you have to determine three types of information:

- ▶ What type of events you want to know about?
- ▶ What is the security level of this event?
- ▶ How do you want the event to be handled?

You configure events using an “event generator,” which describes the condition that must be reached for an event to be generated. After that, you define an “event handler,” which is created for this specific event generator to describe what happens when the event occurs.

Note: You can create an event generator without any event handler to handle it. In this case your event generator will not be logged/recorded anywhere, except for server or add-in task events, which are stored in the log.nsf of the server where they occur.

Therefore, if you want to know about an event, you must have at least one event handler associated with it. You can define several event handlers for the same event generator. You might do this, for example, if you want to use several methods of notification.

This concept of monitoring is not new to an experienced Domino administrator, but in Domino 6 both events4.nsf and statrep.nsf databases have new names: the Statistics & Events database (events4.nsf) now is known as Monitoring Configuration, and the Statistics Reports database (statrep.nsf) has become Monitoring Results. In addition to new names, there are some other changes related to how you set up Statistics & Events for your Domino infrastructure.

Another important change is the new name for collecting events or generating an alert, introduced previously as Event Generator and Event Handler.

Table 8-1 summarizes the main differences between Domino R5 and Domino 6 with respect to how events are generated and handled.

Table 8-1 Comparison of monitoring features in R5 and Domino 6

Description	Domino R5	Domino 6
Configuration database	Statistics & Events (events4.nsf)	Monitoring Configuration (events4.nsf)
Log Database	Statistics Reports (statrep.nsf)	Monitoring Results (statrep.nsf)
Event dispatcher	Event task	Event task
Data collection	Collect task	Collect task
Parameter of event	Monitor: - ACL changes - Files - Replication - Statistics Probe: - Domino servers - Mail - TCP server	Event generator: - Database - Domino Server - TCP server - Mail routing - Statistics - Task status
Method of notification	Event notification - Mail - Log to a database - Relay on other server - Log to NT event viewer - Pager - Run a program - Log to UNIX system log - SNMP trap - Broadcast	Event handler: - Mail - Log to a database - Relay on other server - Log to NT event viewer - Pager - Run a program - Log to UNIX system log - SNMP trap - Broadcast - Sound

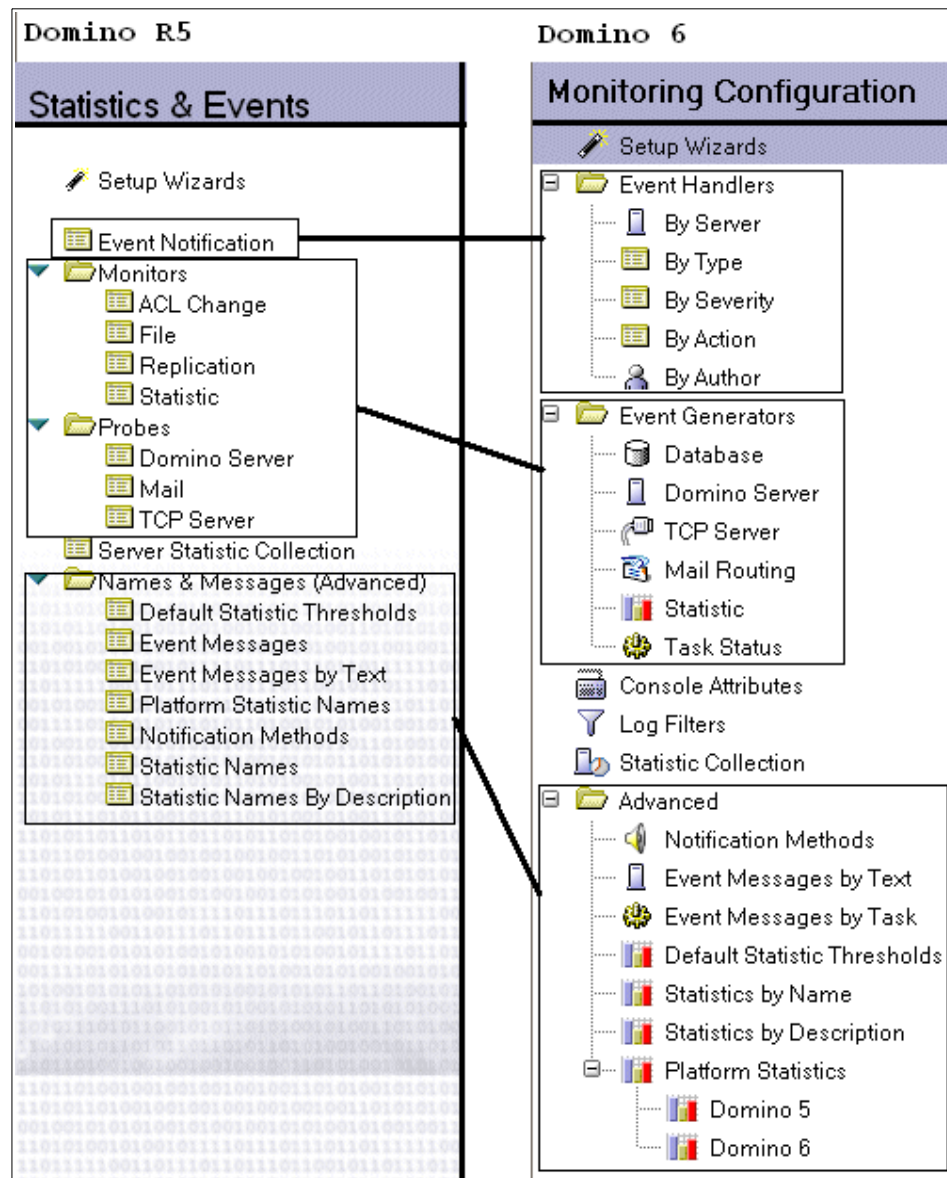


Figure 8-1 Comparison of events4.nsf design between Domino R5 and Domino 6

Table 8-2 Event generator and handler descriptions

Event type	Description
Event generator	<p>There are six types of event generator documents. An event generator document specifies a threshold or condition, which, when met, causes events to be generated.</p> <ul style="list-style-type: none">- Database event generator- Domino server response event generator- Mail routing event generator- Statistic event generator- Task status event generator- TCP server event generator
Event handler	<p>An event handler defines the action that Domino takes when a specific event occurs. An event handler can do the following:</p> <ul style="list-style-type: none">- Log the event to a specified database- Notify you that the event occurred and specify the method of notification- Forward the event to another program for additional processing- Prevent any processing for the event

The Monitor Configuration database (Events4.nsf) includes default event handlers for server tasks. However, you can also create your own or customize existing ones.

Figure 8-2 on page 154 illustrates how the events are handled and the relationships between various components included in event generation and handling.

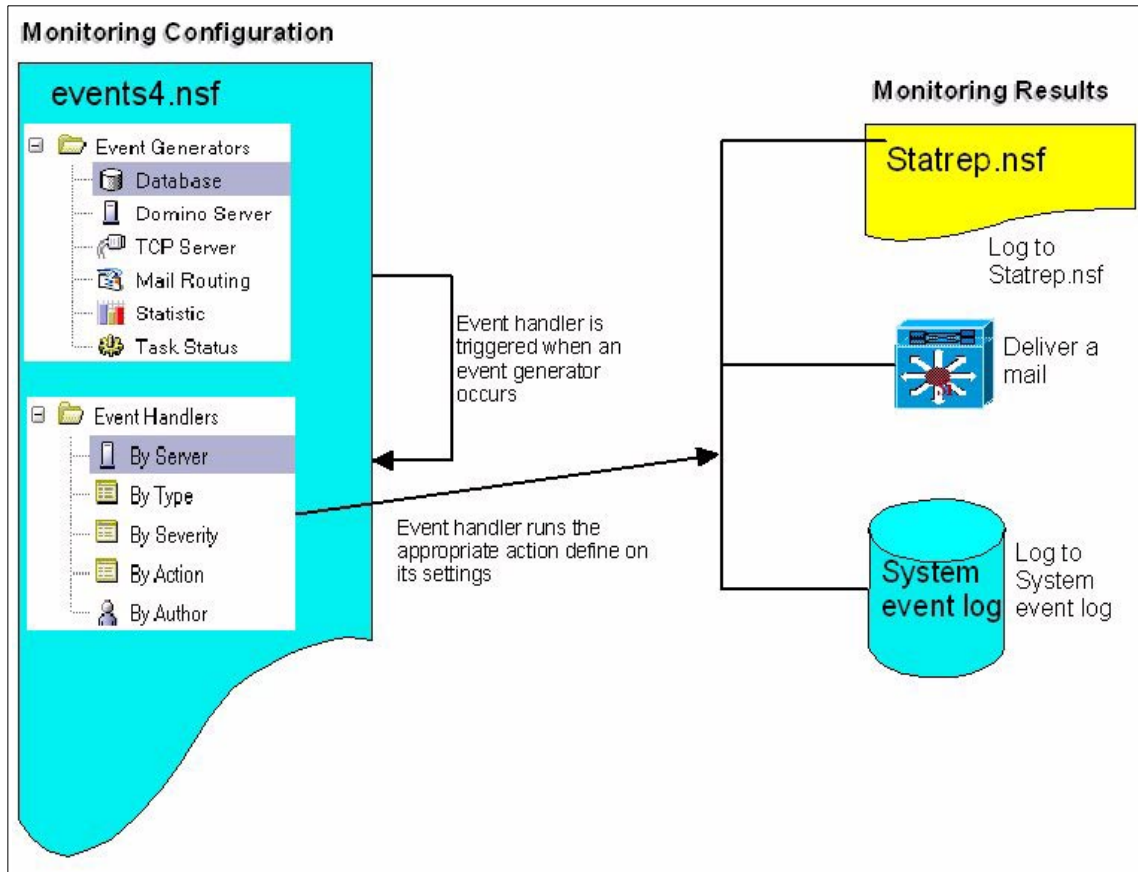


Figure 8-2 How the events are handled

8.1.1 Creating your monitoring infrastructure

When you create a monitoring infrastructure, you have two options available, *centralized* or *distributed*. An overview of each option follows.

► Centralized monitoring

This is the best solution to collect information in one place instead of having to open several servers to gather information. By default, when an event task is loaded at server start-up, it will create a new replica of an existing database from your Administration server if this database doesn't exist yet.

You need to dedicate a server to hold all information for the monitored server in a central Monitoring Results database (statrep.nsf). Using a centralized approach enables you to configure all your infrastructure from one place.

Only the server that hosts the Monitoring configuration database needs to run both collect and event tasks. Other servers need to run only event tasks (loaded by default).

► **Distributed monitoring**

Each Domino server has a copy of the Monitoring Configuration database (events4.nsf) and the Monitoring Results database (statrep.nsf). Each server runs both event and collect tasks to gather information. If you want to make any changes to monitoring, you have to open the correct Monitoring configuration database on the correct server, and then repeat this operation for each server that you want to make changes to.

In a large infrastructure with several locations, you may want to consider an intermediate solution between centralized and distributed. You can dedicate one server per location to collect regional statistics and replicate all the information to a centralized server, where administrators will get global information for the whole infrastructure. Figure 8-3 shows an example of such an organization. The diagram shows that you can monitor both R5 and Domino 6 servers during your upgrade process.

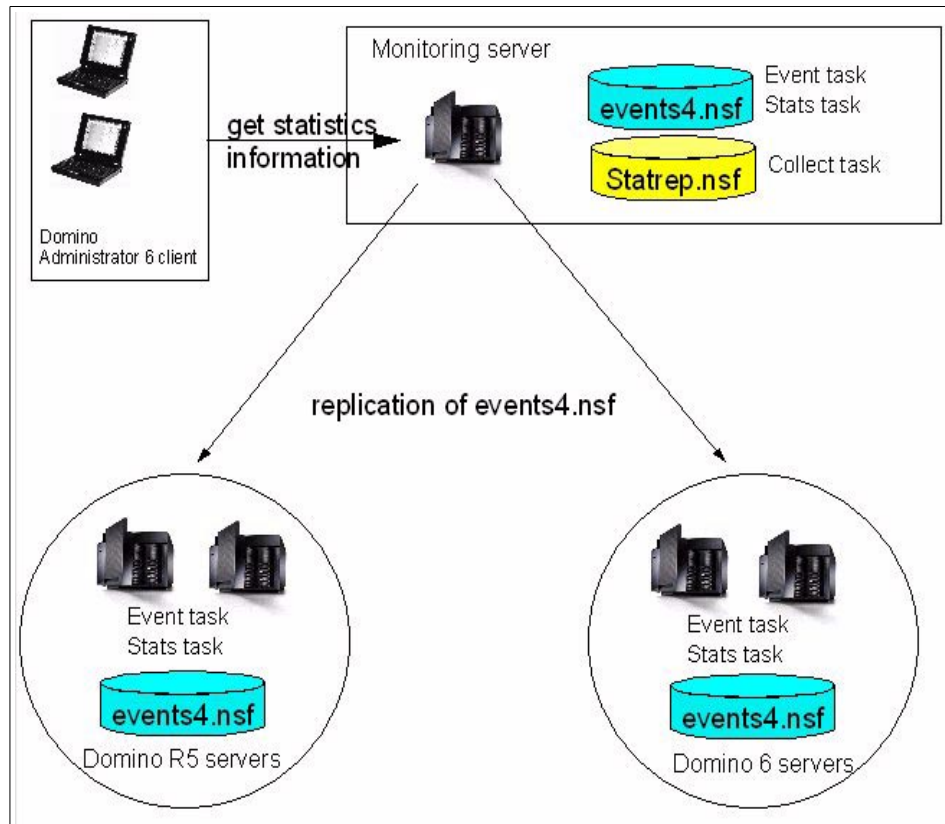


Figure 8-3 Example of centralized infrastructure

8.1.2 Monitoring Configuration database (Events4.nsf)

The Monitoring Configuration database is the container which will allow you to define and create event generators and event handlers. Event generators and event handlers can be created in different places using the Domino Administrator 6 client, but the Monitoring Configuration database is the central repository database for all the event information.

Event generator

Event generators collect information by monitoring a task or statistic, or even by probing a server for access or connectivity reports. Each of these event generators has a specified threshold or condition which triggers its creation. When an event generator is created, the event monitor task checks if there is one or more event handlers associated with the event.

To create an event generator you can use the Domino Administrator 6 client (shown in Figure 8-4) or you can directly open the Monitoring Configuration database on the appropriate server with your Lotus Notes client (Figure 8-5 on page 158). Which method to use is determined by whether you are using a centralized or a distributed monitoring configuration.

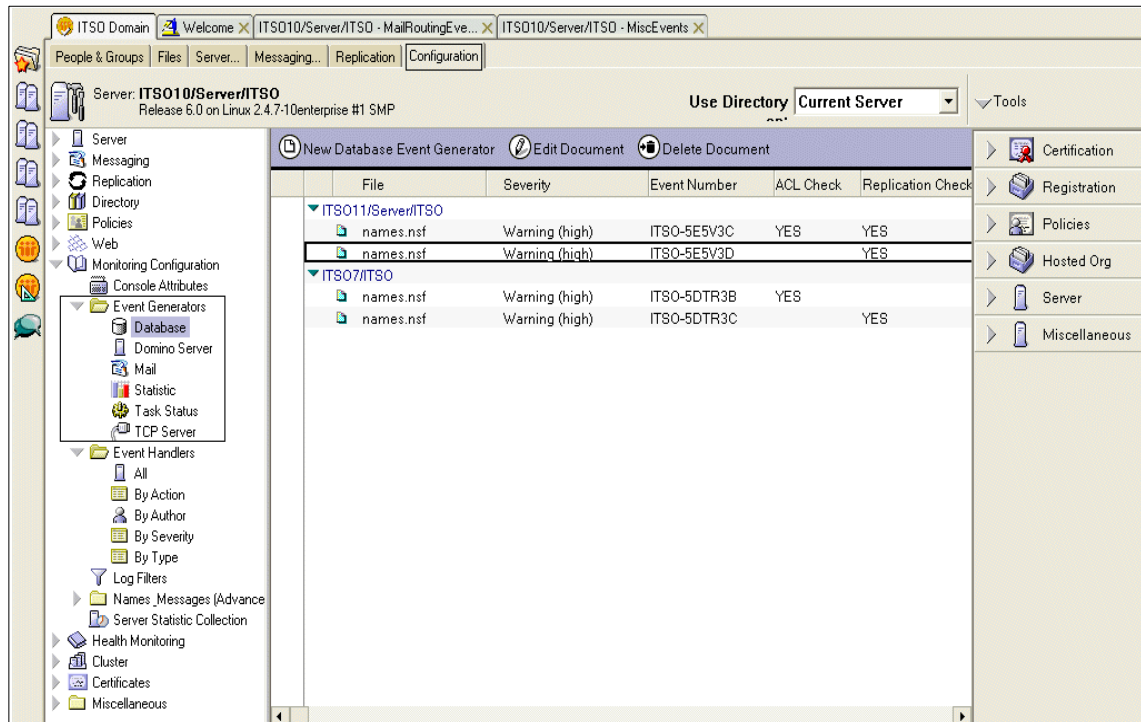


Figure 8-4 Creating Event Generator from Domino Administrator 6 client

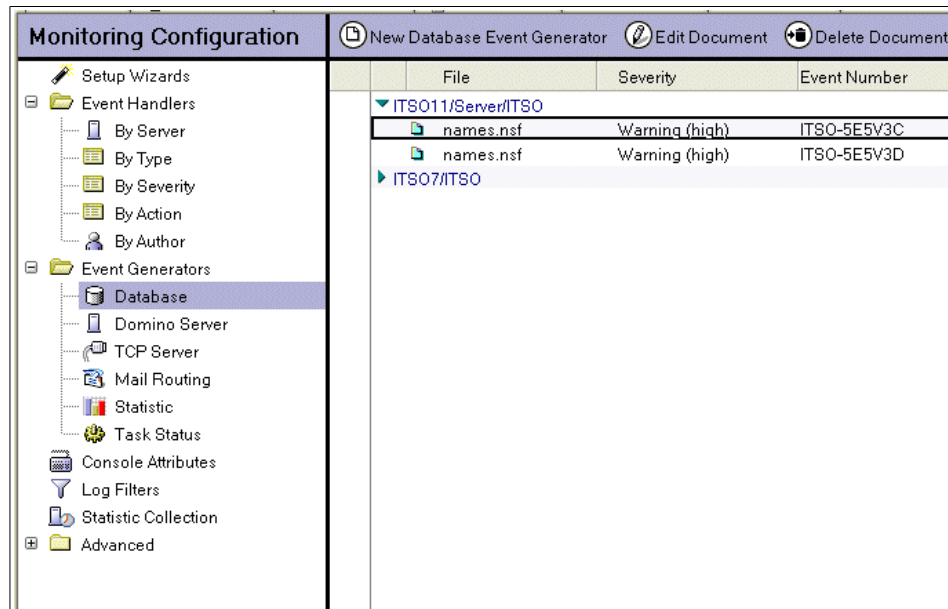


Figure 8-5 Events4.nsf database opened on Lotus Notes client

An alternate, and often much easier, way to create event generators is to use the “Setup Wizard” in the Monitoring Configuration database, as shown in Figure 8-6.

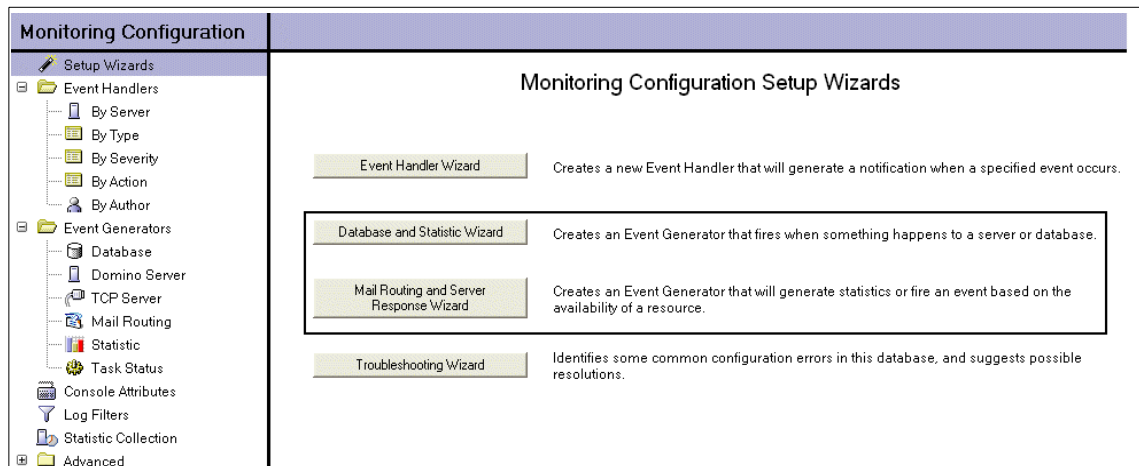


Figure 8-6 Setup Event Wizard from Monitoring Configuration database

Database event generator

A database event generator is used to monitor database usage and ACL changes. There are four types of database event generators:

- ▶ ACL Changes: Monitors all ACL changes, including those made by replication.
- ▶ Replication: Monitors the frequency and success of database replication.
- ▶ Unused space: Monitors the amount of white space (free space) in one or more selected databases on a server, and eventually compacts the database if the amount of white space is over the defined threshold.
- ▶ User inactivity: Monitors database activity and determines which databases are not being used. Activity can be selected for a daily, weekly, or monthly schedule, with a minimum sessions threshold for each.

Use the following steps to create a database event generator:

1. From your Domino Administrator 6, select the server that you want to use the monitoring configuration database.
2. Go to the Configuration tab. In the navigation pane, expand Monitoring Configuration, and select Event Generators -> Database.
3. Click New Database Event Generator.

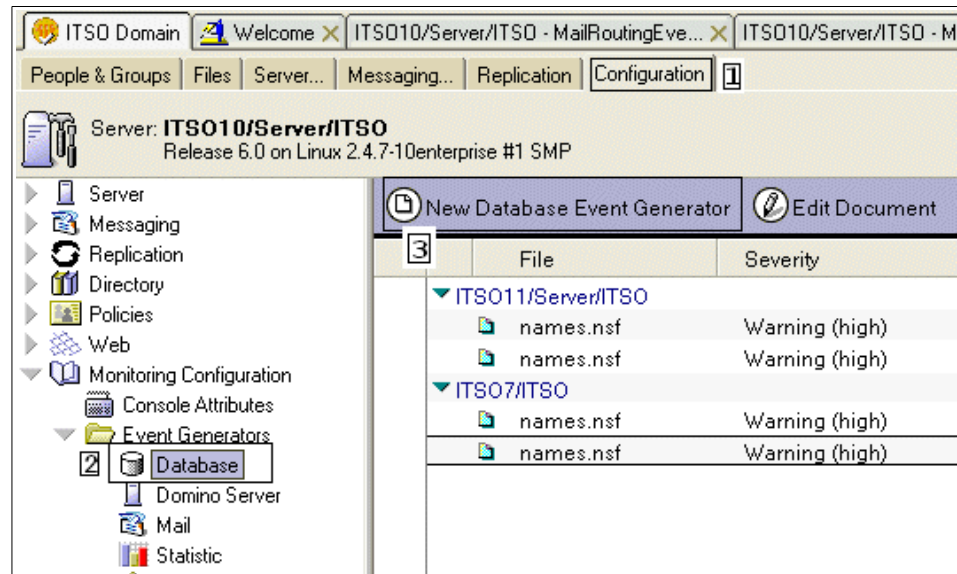


Figure 8-7 Creating a Database Event Generator

4. A new Database Event Generator configuration document is now displayed (Figure 8-8). Specify exactly what you want to monitor.

Save & Close Cancel

Database Event Generator

Event Number: JNKL-5GBTWK event number automatically created for further reference

Basics | Replication | Unused Space | User Inactivity | Other

Database to monitor

File name: Admin.nsf Give the name of the database that you want to monitor

Server(s):
☐ All in the domain
☒ Only the following:
ITSO10/Server/ITSO Select on which server you want to monitor the database

What to monitor

☒ Monitor ACL Changes:
☒ Monitor replication:
☒ Monitor unused space:
☒ Monitor for user inactivity: select which activity you want to know

Figure 8-8 Definition of your Database Event Generator

5. You have to define a threshold for each type of activity to be monitored. The only exception to this is monitoring ACL changes: *any* change to the ACL triggers the event. Define thresholds for:
- Replication (Figure 8-9)
 - Unused space (Figure 8-10)
 - User inactivity (Figure 8-11)

Basics | Replication | Unused Space | User Inactivity | Other

Server(s) with which the database must replicate

☐ All in the domain
☒ Only the following:

ITS010/Server/ITS0

Replication timeout

Timeout: 24 hours

server(s) with which the database must replicate

time-out value after what the event will be generated

Figure 8-9 Replication monitor

Basics | Replication | Unused Space | User Inactivity | Other

Unused space

Trigger the event when unused space exceeds: 10%

☒ Automatically compact the database when the above condition is met

Figure 8-10 Unused space monitor

Basics | Replication | Unused Space | User Inactivity | Other

User Inactivity

What periods do you want to monitor, and what are the minimum number of sessions that must be met or an event is triggered?

Time Periods to Monitor	Minimum Sessions
<input checked="" type="checkbox"/> Daily:	10
<input checked="" type="checkbox"/> Weekly:	50
<input checked="" type="checkbox"/> Monthly:	300

Define your period of observation and the minimum of sessions expected of the selected database

Figure 8-11 User Inactivity monitor

- The last tab is where you can create associated event handlers and define the severity of your event generator.

Basics | Replication | Unused Space | User Inactivity | Other

Event

Generate a Database event of severity:

Create a new event handler for this event.

Warning (high)
Fatal
Failure
Warning (high)
Warning (low)
Normal

Determine the severity level of your events

Enablement

☐ Disable this event generator

Create associated Event Handler to process this Event Generator

Figure 8-12 Definition of severity for your database generator

- When configuration is done, save it by clicking the Save and Close button at the top of the document.

Now your Database Event Generator appears in the Database Event Generator view, as shown in Figure 8-13.

ITSO Domain | Welcome | Database Event Generator ... | Monitoring Configuration

People & Groups | Files | Server... | Messaging... | Replication | Configuration

Server: ITS010/Server/ITS0
Release 6.0 on Linux 2.4.7-10Enterprise #1 SMP

Use Directory: Current Server

Tools

New Database Event Generator | Edit Document | Delete Document

File	Severity	Event Number	ACL Check	Replication Check	Size Check	Usage Check
ITS010/Server/ITS0						
Admin.nsf	Warning (high)	JNKL-5GBTWK	YES	YES	YES	YES
ITS011/Server/ITS0						
ITS07/ITS0						

Figure 8-13 Database Event Generator created

Database event generator is often used to ensure that your critical databases, such as Domino Directory and Administration Requests, are successfully replicated and the ACL is not changed by mistake. You can use this kind of event to monitor database usage and remove any unused application.

Domino server event generator

This event is used to check connectivity and port status for a specified server in your network periodically (for example, every 15 minutes). A Domino server event generator can check:

- The ability to access a destination server
- The ability to access a destination server and open a specific database

To create a Domino server event generator, follow the same steps used to create a database event generator, but in the last step, select Monitoring Configurations -> Event Generators -> Domino Server in the navigation pane from under the Event Generators, again this is found on Monitoring Configurations database on the navigation pane. Finally, click New Domino Server Event Generator.

Fill out the Basics table, specifying which servers to probe and from where. Determine the connectivity test that you want to measure, and specify the interval of time (in minutes) that you want to send the probe. The default is three; however, we suggest increasing this to at least 15 minutes.

Domino Server Event Generator

Event Number: JNKL-5GBV5S

Basics | Probe | Other

Target server(s)

Server(s): ITS011/Server/ITS0, ITS012/Server/ITS0, ITS08/Server/ITS0 v

Select one or several servers that you want to measure access time

Probing server (source)

Server: ITS010/Server/ITS0 v

select the server which will generate the probe

Access

Interval: 3 Minutes

☐ Check just the ability to access the destination server

☒ Check the ability to access the destination server and open this database:

File name: NAMES.NSF

select interval (by default 3 minutes and the type of event)

Figure 8-14 Global setting for the Domino Server Event Generator

On the Probe tab, specify which port to use for probing (any available one or a specific one) and the amount of time allowed to open the database or access the server (the default is 1000 milliseconds).

Domino Server Event Generator

Event Number: JNKL-5GBV5S

Basics | **Probe** | Other

Ports

☒ Perform probe using any available port

Ports to use:
TCPIP

Select which port the probing server will use either any available from Server document or a specific one

Time

Timeout threshold: 1000 Msecs

Amount of time after the event will be generated if the connection is not establish

Resulting statistic

SERVER.<Probing Server>.<Destination Server>

Figure 8-15 Parameters of your Domino Server probe

On the Other tab, define the severity level and create event handlers. Finally, save the document.

The Domino server event generator is useful for determining the availability of a server (and even a database) and to ensure that connections operate at a specific service agreement level, since you can define several probing servers close to your user to test your network response time.

TCP server event generator

The TCP (Transfer Control Protocol) server event generator allows you to verify the availability of the services on Internet ports from one to multiple servers. This TCP probe generates statistics that indicate the amount of time needed to respond on the targeted Internet port. If a probe is unsuccessful, the corresponding statistics get a value to -1. The result statistic is:

QOS.TCPservice.ServerName.MonitorId.ResponseTime=<value>

```
sh stat QOS.*
QOS.HTTP.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = 2750
QOS.HTTP.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = 96
QOS.IMAP.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = -1
QOS.IMAP.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = -1
QOS.LDAP.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = -1
QOS.LDAP.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = -1
QOS.NNTPSSL.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = -1
QOS.NNTPSSL.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = -1
QOS.NNTP.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = -1
QOS.NNTP.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = -1
QOS.POP3.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = -1
QOS.POP3.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = -1
QOS.SMTP.ITSO11/Server/ITSO.ITSO-5E5V3E.ResponseTime = -1
QOS.SMTP.ITSO11/Server/ITSO.JNKL-5GC2F4.ResponseTime = -1
14 statistics found
```

Figure 8-16 Statistics result from a TCP Server Event Generator at the server console

The configuration of such an event generator is comparable to the configuration of the database and server event generators described previously.

1. Define the servers that you want to monitor and from which source. If you select all, servers will probe themselves according to the ports configured in their server documents.

TCP Server Event Generator

Event Number: JNKL-5GC2N6

☐ All Domino servers in the domain will probe their own configured ports

Target Server(s)

☐ All in the domain
☒ Only the following:

Select the servers that you want to probe

Probing server(s) (source)

Define your probing server

Figure 8-17 definition of source and target servers

- Define the internet ports that you want to probe (either all, or select from a list).

TCP Server Event Generator

Event Number: JNKL-5GC2N6

Times

Probe interval: minutes
 Service timeout threshold: seconds

Determine the number of minutes between probes and the timeout threshold

Services

☐ Probe all configured TCP services
☒ Probe these services:

define which TCP probe you want to test

☐ DNS
 ☐ HTTP
 ☐ LDAP
 ☐ POP3
 ☐ HTTPSSL
 ☐ LDAPSSL
 ☐ POP3SSL
☐ FTP
 ☐ IMAP
 ☐ NNTP
 ☐ SMTP
 ☐ IMAPSSL
 ☐ NNTPSSL
 ☐ SMTPSSL

Figure 8-18 Internet ports to probe

3. For HTTP *only*, you can specify a URL to test. This URL must be defined relative to the server to probe (do not include the server in the URL address).

Basics | Probe | DNS | HTTP | IMAP | LDAP | NNTP | POP3 | SMTP | Other

Resulting statistic: QOS.HTTP.<Destination Server>.[JNKL-5GC2N6].ResponseTime

Resulting statistic: QOS.HTTPSSL.<Destination Server>.[JNKL-5GC2N6].ResponseTime

☐ Probe just the port

☒ Fetch this URL

http://<ServerAddress>/

For HTTP service you can either just probe the port or a specific server URL (which could reside on the target server)

A timeout failure when probing this port will generate an event of type Web (HTTP/HTTPS).

Figure 8-19 Specific option to probe HTTP internet port

4. As for HTTP, you can define a specific action for NNTP probe other than just checking the port availability.

Event Number: JNKL-5GC2N6

Basics | Probe | DNS | HTTP | IMAP | LDAP | NNTP | POP3 | SMTP | Other

Resulting statistic: QOS.NNTP.<Destination Server>.[JNKL-5GC2N6].ResponseTime

Resulting statistic: QOS.NNTPSSL.<Destination Server>.[JNKL-5GC2N6].ResponseTime

☐ Probe just the port

☒ Send this command

for NNTP ports, you can either probe the port or send a specific command to the server (which has to run Domino R5 as NNTP is not supported on Domino 6)

Command: ARTICLE

Parameters:

A timeout failure when probing this port will generate an event of type News (NNTP).

Figure 8-20 Specific option to probe NNTP internet port

Important: NNTP support has been removed from Domino 6; therefore, you can only probe NNTP on Domino R5 server.

5. When TCP server event generator configuration is done and you have determined the appropriate event handler, save the document.

Note: To monitor TCP server and mail routing event generator, your probing server must run the ISpy task. To start this task you can either edit the ServerTask setting in the NOTES.INI file to include RunJava ISpy or enter the following command at the server console:

```
>load runjava ISpy
```

The ISpy task is case sensitive; be sure to enter it as shown.

Mail routing event generator

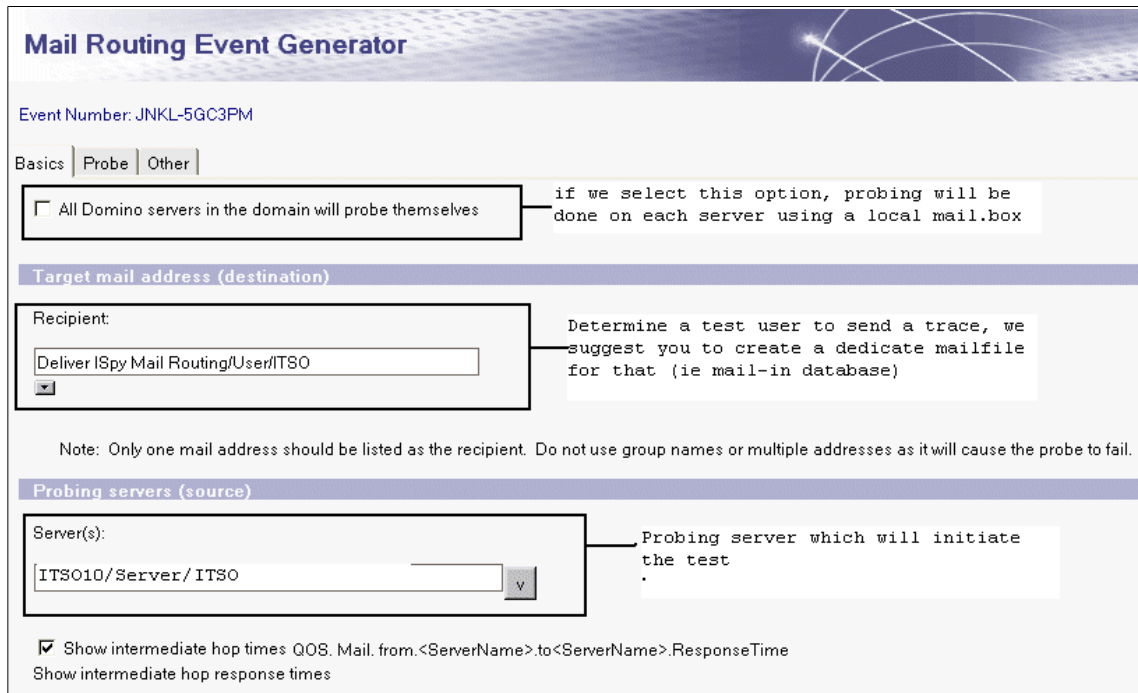
Mail routing event generator is used to test and gather statistics on mail routing. To accomplish this function, the ISpy task sends a mail-trace to the specified user's mail server.

As for the TCP Server, this event generator creates a statistic that indicates the amount of time needed to deliver its test message. If the task fails, the statistic will return a value to -1, and the format of this statistic is as follow:

QOS.Mail.RecipientName.ResponseTime=<value>

Additionally, if you run the statistic Collector task (collect) the result of this statistic will be recorded in the Monitoring Result database of the server which runs the collect task.

1. To create a Mail Routing Event Generator, from the Domino Administrator, click the configuration tab and open the Monitoring Configuration view.
2. Select Event Generators -> Mail, click New Mail Routing Event Generator, and complete the displayed form.



Mail Routing Event Generator

Event Number: JNKL-5GC3PM

Basics | **Probe** | Other

☐ All Domino servers in the domain will probe themselves

if we select this option, probing will be done on each server using a local mail.box

Target mail address (destination)

Recipient:

Deliver ISpy Mail Routing/User/ITSO

Determine a test user to send a trace, we suggest you to create a dedicate mailfile for that (ie mail-in database)

Note: Only one mail address should be listed as the recipient. Do not use group names or multiple addresses as it will cause the probe to fail.

Probing servers (source)

Server(s):

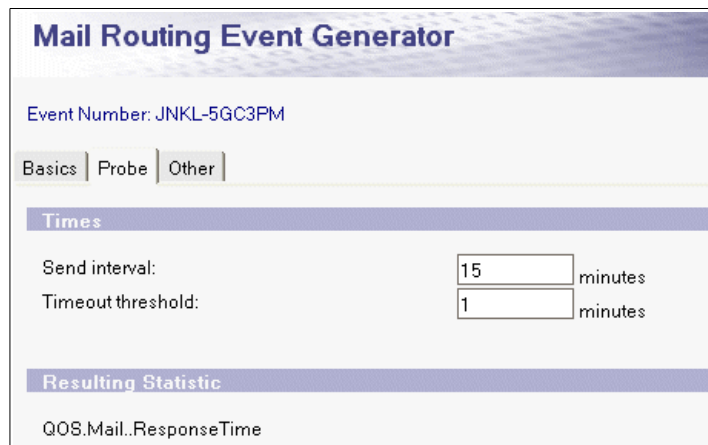
ITS010/Server/ITSO

Probing server which will initiate the test

☒ Show intermediate hop times QOS.Mail.from.<ServerName>.to.<ServerName>.ResponseTime
Show intermediate hop response times

Figure 8-21 Definition of your mail routing test path

- On the Probe tab, define the send interval (by default it's 15 minutes) and the time-out threshold (in minutes) that the probing server waits for a response from the ISpy task before logging a failure.



Mail Routing Event Generator

Event Number: JNKL-5GC3PM

Basics | **Probe** | Other

Times

Send interval: 15 minutes

Timeout threshold: 1 minutes

Resulting Statistic

QOS.Mail..ResponseTime

Figure 8-22 Probe configuration for Mail Routing Event Generator

4. When mail routing event generator configuration is done and you have determine the appropriate event handler, save it by clicking Save and Close at the top of the document.

Tip: You can use this event generator in conjunction with the mail tracking collector to ensure that your mail infrastructure meets your service level agreement (SLA). Furthermore, the mail tracking collector can provide some additional statistics about your users' patterns of use, such as:

- ▶ Top 25 senders by count or size
- ▶ Top 25 receivers by count or size
- ▶ Top 25 most popular "next" or "previous hops"
- ▶ Top 25 largest messages
- ▶ Message volume summary

Task Status Monitor

The Task Status Monitor is used to determine whether specific Domino tasks are running as expected or are stopped or even stalled. The possible condition for each task is:

- Task is down
- Task is up
- Task is stalled
- Task is unstalled

Only a subset of all tasks can be monitored with this tool; they are identified in Table 8-3.

Table 8-3 Tasks that can be monitored with Task Status Monitor

Task name	Domino process
Admin Process	AdminP
Agent Manager	Amgr
Billing (removed in Domino 6)	Billing
Calendar Connector	Calconn
DIIOP server	DIIOP
Event Monitor	Event
Indexer	Update

Task name	Domino process
Maps extractor	Maps
NNTP server (for Pre-Domino 6)	Nntp
Replicator	Replica
Router	Router
Schedule Manager	Sched
Statistics Collector	Collect
Statistics	Stats
Web Retriever	Web

Tip: If you want to monitor a server task that is not listed, create an event generator to probe a port associated with a service (such as Http or LDAP), or create an event handler that looks for a specific text string or event severity. (For more information, open any Monitoring Configuration database -events4.nsf- and go to Advanced\Event Message by task.)

Use the following steps to create a Task Status Monitor.

1. From your Domino Administrator 6 client, click Configuration tab, select the Monitoring configuration -> Event Generators -> Task status view. Click New Task Monitor.
 - On the Basics tab, select the task or tasks you want to monitor. All available server-based tasks are listed in a scrollable window; check all tasks in which you are interested.

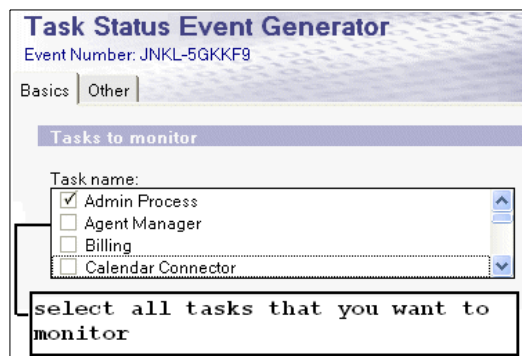


Figure 8-23 Selection of tasks to monitor

- Specify whether you want to apply this task selection to all servers in the domain or only to some of them.

Tip: You can select all tasks; however, we recommend creating one document per server (with the appropriate tasks), or one document per task (with a list of all servers to be monitored).

- Define the state of the task that you want to monitor.

The screenshot shows a dialog box titled "What to monitor". Inside, there is a list of four items, each with a checkbox:

- ☒ Monitor task down
- ☐ Monitor task up
- ☒ Monitor task stalled
- ☒ Monitor task uninstalled

 A rectangular callout box with a pointer to the checked items contains the text: "select the state of the task to monitor".

Figure 8-24 Task status

- On the Other tab, select event severity and the associated Event Handler.
2. Click Save & Close.

Monitoring Domino server tasks should be a key component of the daily Domino administrator job. A task can stop working (or be stalled) without causing the server to crash—but its non-working state can still degrade overall system performance.

Event handler

An event handler describes the action that a Domino server takes when a specific event happens. You can define an event handler to do one or more of the following actions:

- ▶ Log the event to a predefined destination (usually statrep.nsf)
- ▶ Notify you or your team that a specific even occurred and determine the method of notification
- ▶ Prevent the event from being logged to a server console or to a specified destination

There are several default event handlers for server tasks in the Monitoring Configuration database. An event handler can be associated with the following triggers:

- ▶ Any event that matches one of the following criteria:

- Event type (see Table 8-4 on page 173 for a list of events)
 - Event severity (see Table 8-5 on page 174 for a list of severities)
 - Containing specific text in an event message
- A built-in or add-in task event
- A list of all built-in or add-in task events is available for reference from the Monitoring Configuration database, under the Advanced\Event Message by Task view. (See Figure 8-25 on page 174.)
- A custom event generator
- Any event generator that you have created.

Table 8-4 Event types

Event type	Generates
Add-in	Message related to the Add-in task
AdminP	Message related to the AdminP task
Agent	Message related to agents
Client	Message related to the client
Comm/Net	Message related to X.PC
Compiler	Message related to compute and compile functions
Database	Message related to database
Directory (LDAP)	Message related to directory services
Mail	Message related to mail routing
Misc	Miscellaneous message not in another event category
Monitor	Message related to event generated on the Domino Administrator by Server Monitoring
Network	Message related to the LAN communication
Replica	Message related to replication
Resource	Message related to system resources
Router	Message related to mail events
Security	Message related to ID files, server and database access
Server	Message related to condition on a particular server (connect)
Statistic	Message related to statistic alarms

Event type	Generates
Unknown	Message that have an unknown prefix and not listed away
Update	Message related to indexing
Web (HTTP (S))	Message related to the HTTP Task

Table 8-5 Severity levels

Severity	Description
Fatal	Imminent system or task crash
Failure	Severe failure the does not result in system crash
Warning (High)	Loss of function requiring an intervention
Warning (Low)	Performance degradation
Normal	Status message

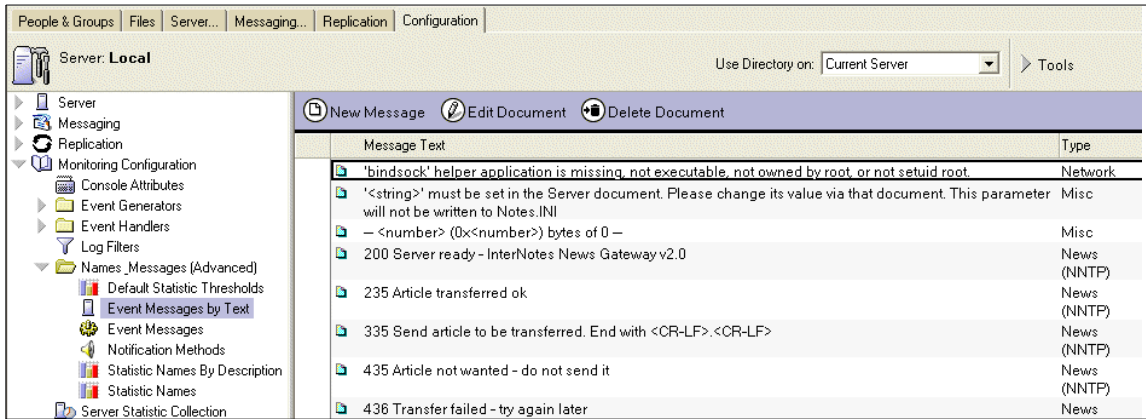


Figure 8-25 List of available built-in or add-in event message

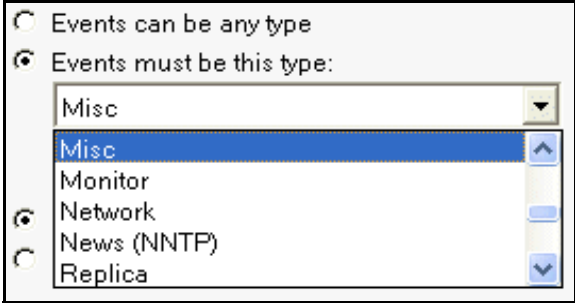
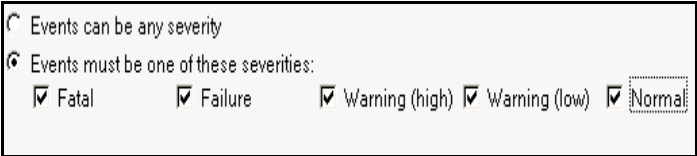
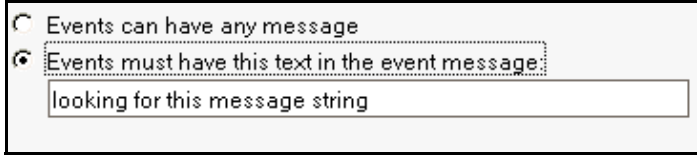
Creating an event handler

You can use either the setup wizard or the Domino Administrator client to create an event handler.

1. From your Domino Administrator, click the Configuration tab and open Monitoring Configuration view.
2. Open the Event Handler\All View and click New Event Handler.
3. On the Basic tab, specify on which server to enable the event handler.
 - a. Notify of the event on any server in the domain.

- b. Notify of the event only on the following servers (you can display a list).
- 4. Under Notification Trigger, choose one:
 - a. Any event that matches a criteria, then complete the fields on the Event tab. (See Table 8-6.)

Table 8-6 Event tab for “any event that matches a criteria” selection

Field	Action
Event Type	<p>Event can be any type, or Event must be this type, and select this from the list</p> 
Event Severity	<p>Event can be any severity, or Event must be one of these severities, and select severity level</p> 
Message Text	<p>Events can have any message, or Events must have this text in the event message (you have to specify your message string)</p> 

- b. A built-in or add-in task event. Go to the event tab to specify the event to handle.
 - i. Click Select Event to view a list of all built-in and add-in tasks available.

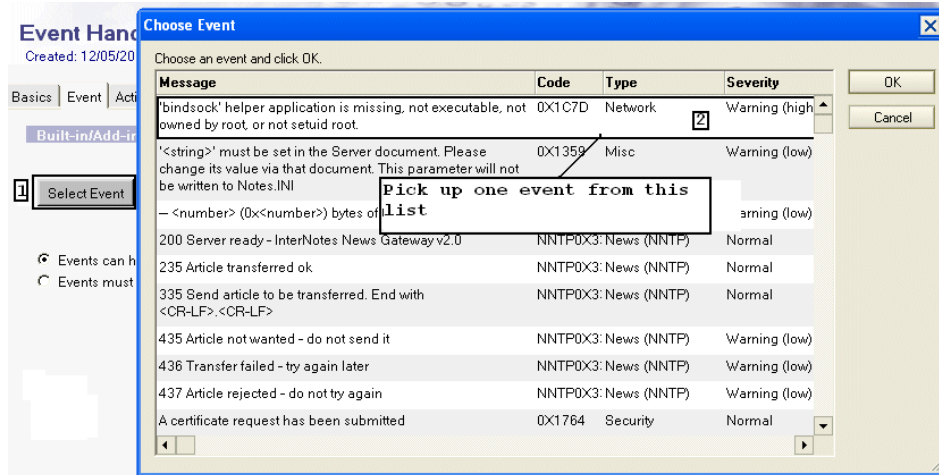


Figure 8-26 Selection of built-in / add-in event task

- ii. If desired, select one of the following conditions:
 - Event can have any message (optional).
 - Event must have this text in the event message (then type the message text in the appropriate field) (optional).
- c. A Custom Event Generator. On the Event tab specify which custom Event Generator you want to handle:
 - i. From the "Select Event" line, you can display all Event Generators that you have created and select those you want to handle.

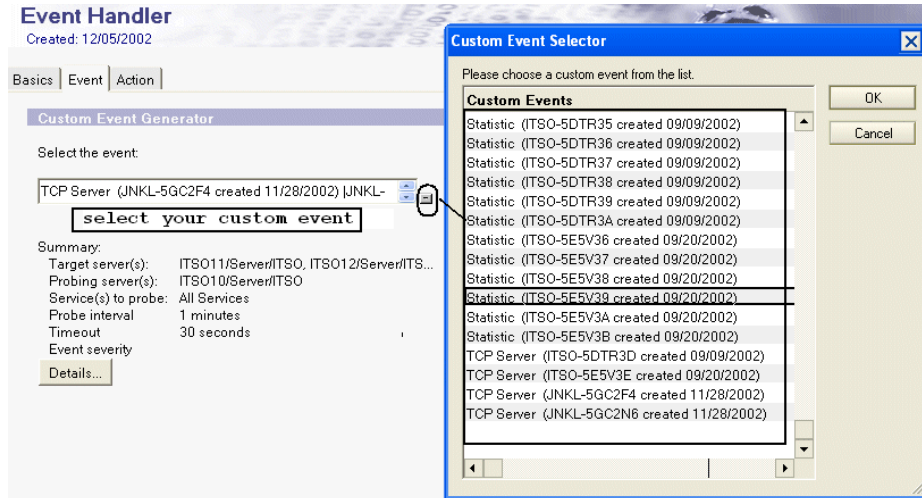


Figure 8-27 Selection of your custom Event Generator

- ii. Click the Details button to view all details about your event generator.
- iii. Alternatively, click the New button to create a specific Event Generator (this is only valid for a Database or Statistics event generator).



Figure 8-28 Event Generator Wizard

5. On the Action tab, specify the desired notification action by clicking it in the drop-down list of available notification methods. The notification methods have the following meanings:

Broadcast	Report event to all users logged onto the server or to a specified group of users.
Log to a database	Log the event to a specified database (usually STATREP.NSF) on a local server.
Mail	Mail a notification of the event to a user, mail-in database (STAMAIL.NSF) or group.
Log to NT Event Viewer	Report the event on the local NT Event viewer if the server runs on Win32.
Pager	Report the event to a mail address of an alphanumeric pager.
Run Program	Run an add-in program or a specified command.
Relay to other server	Relay the event to another server in the same Domino domain to be sent to a specific destination.
Sound	Play a defined sound on the designated server.
SNMP Trap	Send the event as a SNMP trap. (For more information see the Administration Help database help\Help6_admin.nsf, topic SNMP.)
Log to UNIX system log	Report the event to the local UNIX system log if your server runs UNIX.

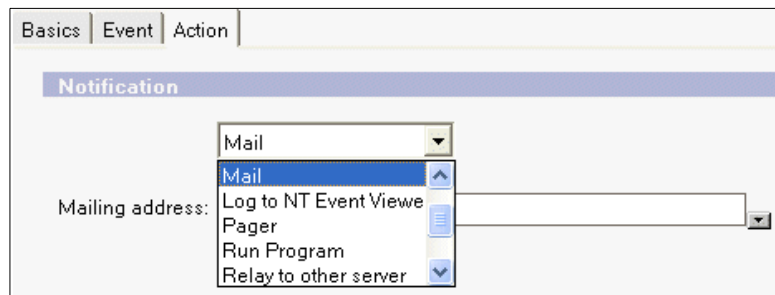


Figure 8-29 Notification method

- d. In the Enablement section, select the appropriate action from the following choices:
- Enable this notification.
 - Disable this notification. (Use this if you want to enable it later or disable an existing Event Handler.)

- Enabled only during these times. (Specify a time range during the day, since typically you don't want to be notified about nightly events.)

Figure 8-30 Enabling notification

6. Save your document to enable your Event Handler. It will appear in your Domino Administrator 6 client, in the Event handler folder as shown in Figure 8-31.

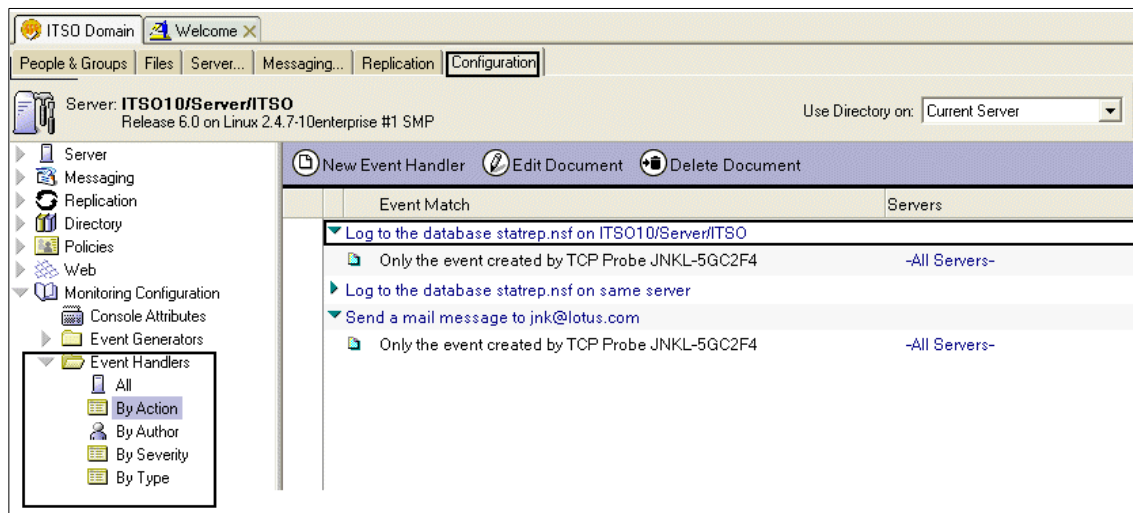


Figure 8-31 Existing Event handlers for a server

8.2 New analysis capabilities

This section describes the new analysis capabilities introduced in Domino 6.

8.2.1 New log search capabilities

Lotus Domino records most of its daily activities into a central database called Log (log.nsf). It is unique for each database, and reports activity for:

- ▶ Mail routing
- ▶ Replications
- ▶ Database usage
- ▶ Phone calls
- ▶ Passthru connections
- ▶ Miscellaneous events

In Lotus Domino 6, the event task starts automatically because all server tasks now use the event task for logging. All documents in Log.nsf are now triggered by the event process, when a condition or a threshold is met:

- ▶ Event status
- ▶ Event type
- ▶ Event severity

This new behavior allows the new log analysis tool included in the Domino Administrator 6 client to be more powerful and provide better search capabilities. You don't have to enable any specific settings to take advantage of this new Log analysis tool; upgrading to Lotus Domino 6 is enough. You have to have a version 6 design for the Log database and use the Domino Administrator 6 client.

Domino Server Log		Help			
		Name	Date	#	Star
<ul style="list-style-type: none"> Miscellaneous Events Mail Routing Events Replication Events Newsgroups Events Passthru Connections Usage Phone Calls 	ITS08/Server/ITS0				
	09/22/2002				
	09/23/2002				
	09/24/2002				
	09/25/2002				
	09/26/2002				
	09/27/2002				
	09/28/2002				
	09/29/2002				
	09/30/2002				

Figure 8-32 New log.nsf design

You will find in this database the same information that you had already in Lotus Domino R5. However, since all events are now recorded by the event task, searches performed using the Lotus Domino Administrator 6 can have more precision and granularity.

To use this new log search interface:

1. Launch your Domino Administrator 6 client.
2. Connect to the server that you want do your log search on.

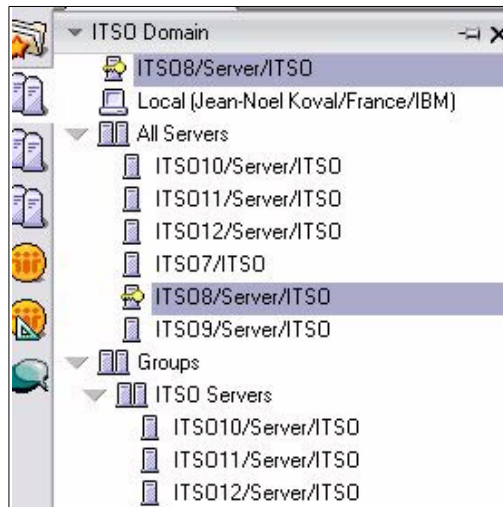


Figure 8-33 Domain Server bookmark in Lotus Domino Administrator 6 client

- Once you have selected your server, go to the Analysis tab (which can be found under the Server tab) and select Analysis -> Log option in the Tools pane, on the right-hand side of the window.



Figure 8-34 Selecting the log from Lotus Domino Administrator 6

- Click Log. A dialog box in which to specify your search is displayed.

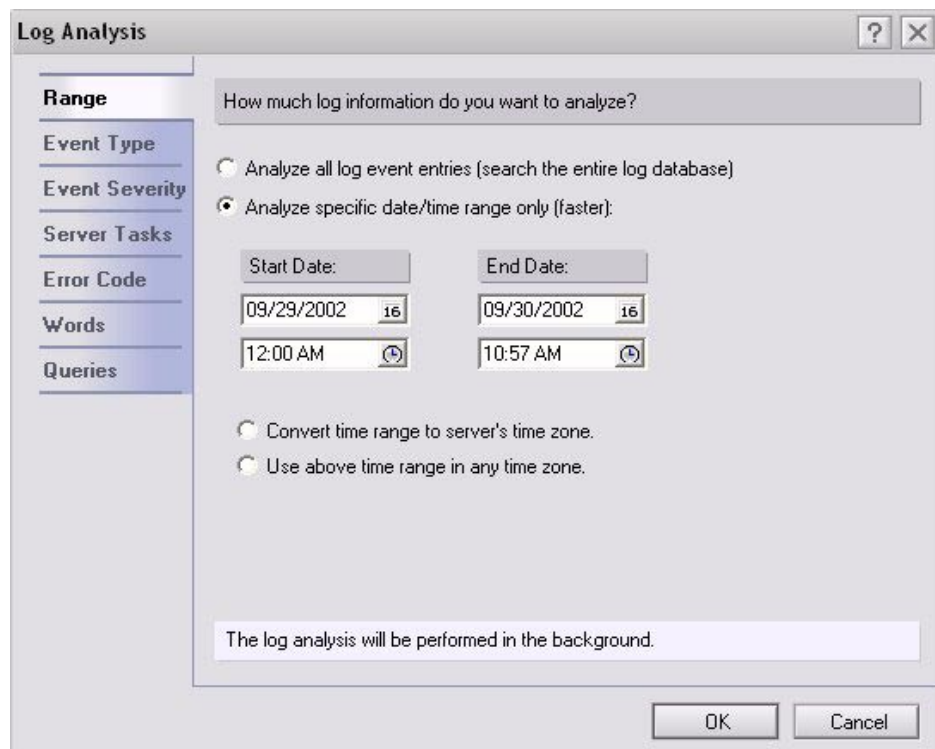


Figure 8-35 Log Analysis definition dialog

5. Define exactly what you are looking for, using the following search options:

– Range

Specify the time range where you want to search. You can also launch a search across the entire log database.

How much log information do you want to analyze?

☐ Analyze all log event entries (search the entire log database)

☒ Analyze specific date/time range only (faster):

Start Date: 09/29/2002 12:00 AM

End Date: 09/30/2002 10:57 AM

☐ Convert time range to server's time zone.

☐ Use above time range in any time zone.

– Event Type

Define the sort of event you are looking for; multiple choices are allowed.

To limit the analysis to certain event types only, select one or more events:

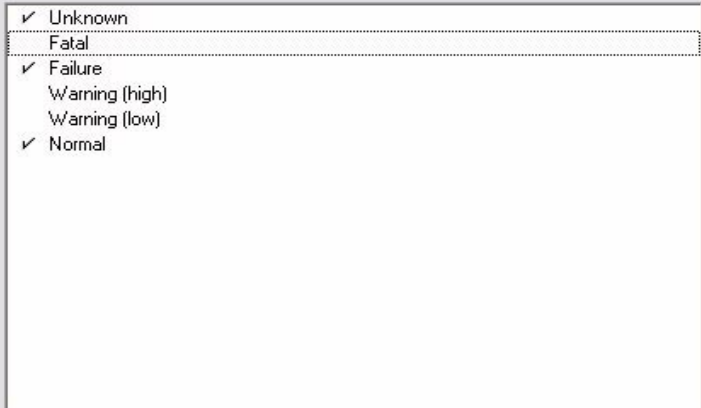
- ✓ Comm
- ✓ Security
- ✓ Mail
- ✓ Replica
- ✓ Resource
- ✓ Misc
- ✓ Server
- ✓ Statistic
- ✓ Update
- ✓ DataBase
- Network
- ✓ Compiler
- Router
- Agent
- Client
- Addin

☒ The results must match one of the these selected event types.

– Event Severity

Select the level of event severity that you want to search; multiple choices are allowed.

To limit the analysis to certain event severities only, select one or more event severities:

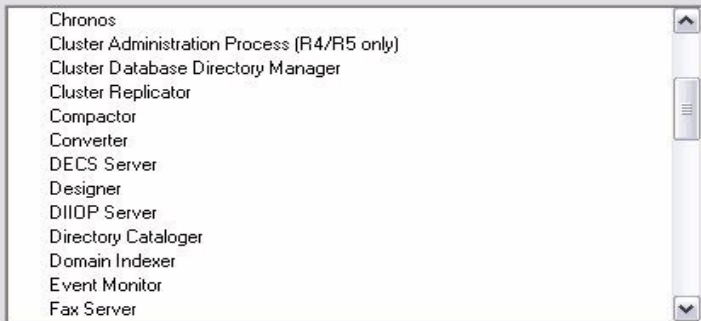


- ✓ Unknown
- ✓ Fatal
- ✓ Failure
 - Warning (high)
 - Warning (low)
- ✓ Normal

– Server tasks

Define the specific tasks that you would like to see returned in your search. If you use custom tasks or add-ins, you can specify them manually. Multiple choices are allowed as well.

To limit the analysis to certain server tasks only, select one or more tasks:



- ✓ Chronos
- ✓ Cluster Administration Process (R4/R5 only)
- ✓ Cluster Database Directory Manager
- ✓ Cluster Replicator
- ✓ Compactor
- ✓ Converter
- ✓ DECS Server
- ✓ Designer
- ✓ DIIOP Server
- ✓ Directory Cataloger
- ✓ Domain Indexer
- ✓ Event Monitor
- ✓ Fax Server

You can also add a custom server task to the list:

– Error Code

List of all error codes that Domino can generate in the log database (0Xxxxx) with a brief description; multiple choices are allowed.

To limit the analysis to certain error codes only, select one or more event errors:

Message	Code
Internal only - delete named table entry.	0X03A4 ▲
Internal only - update named table entry.	0X03A5
Internal software problem. Call Customer Support.	0X093F
Internet address failed with the following error: <error message>	0X1221
Internet Domain information is not available.	0X0E31
Internet mail replicas residing on remote Domino servers not supported.	0X06F1
Internet Messaging Configuration invalid or parts not available.	0X06E1
Internet Messaging Extension error: Cannot create a	0X31E1 ▼

◀ ▶

– Words

In this section you can specify any word (or multiple words) that you want to include or exclude in your search.

To limit the analysis to certain words only, specify the words you are interested in:

Search:

Words:

Word Filters:

Must contain these words:

Must not contain these words:

☒ The results must match the specified words and/or filters.

– Queries

Summarizes all log search options you have specified. You can save your query, like a query profile, if you want to run the same search several times (for example on a daily or weekly basis.) We do not recommend retaining more than 7 seven days of logs in your active log database.

6. When you are done specifying the options, click OK to launch the search. This action will be done in the background (Figure 8-36). Once the search is complete you will be notified by a pop-up dialog like the one shown in Figure 8-37.

Figure 8-36 Search occurs in the background

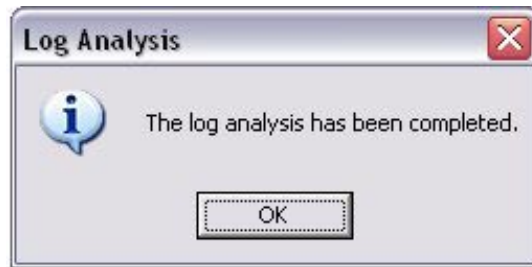


Figure 8-37 The log search has been completed

When the search is over you can go back to the initial window, where you launched your search, to see the results. An example is in Figure 8-38.

Log Analysis Results			
Server: ITS08/Server/ITS0			
Time: 09/29/2002 12:15 AM EDT - 09/30/2002 09:45 AM EDT			
Type	Severity	Time	Event
Unknown	Unknown	09/29/2002 01:00:41 AM	Warning: Cannot locate design note 'DOLS.gif' in 'DOLS Resource Template' template
Unknown	Unknown	09/29/2002 01:00:41 AM	Warning: Cannot locate design note 'iNotes_bnnr.gif' in 'DOLS Resource Template' template
Unknown	Unknown	09/29/2002 01:00:41 AM	Warning: Cannot locate design note 'servers.gif' in 'DOLS Resource Template' template
Misc	Normal	09/29/2002 01:00:41 AM	Updated database SmartUpg.nsf in catalog
Misc	Normal	09/29/2002 01:00:41 AM	Updated database Websitesportal.nsf in catalog
Misc	Normal	09/29/2002 01:00:41 AM	Updated database Websiteslwsmgr.nsf in catalog
Unknown	Unknown	09/29/2002 01:00:42 AM	Warning: Cannot locate design note 'DOLS.gif' in 'DOLS Resource Template' template
Unknown	Unknown	09/29/2002 01:00:42 AM	Warning: Cannot locate design note 'iNotes_bnnr.gif' in 'DOLS Resource Template' template
Unknown	Unknown	09/29/2002 01:00:42 AM	Warning: Cannot locate design note 'servers.gif' in 'DOLS Resource Template' template
Misc	Normal	09/29/2002 01:00:44 AM	Updated database activity.nsf in catalog
Misc	Normal	09/29/2002 01:00:45 AM	Updated database activity.ntf in catalog
Misc	Normal	09/29/2002 01:00:45 AM	Updated database admin4.nsf in catalog
Misc	Normal	09/29/2002 01:00:45 AM	Updated database admin4.ntf in catalog
Misc	Normal	09/29/2002 01:00:45 AM	Updated database alog4.ntf in catalog
Misc	Normal	09/29/2002 01:00:45 AM	Updated database archlg50.ntf in catalog

Figure 8-38 The results of your search

All results of your log queries are saved in a log database, so you can review them at any time. Launch your Domino Administrator 6, select the appropriate server, select Server-Analysis tab, expand the Log entry and select Log Analysis Results in the navigation pane. All the saved log searches are displayed by date. Browse to the results document you want to see.

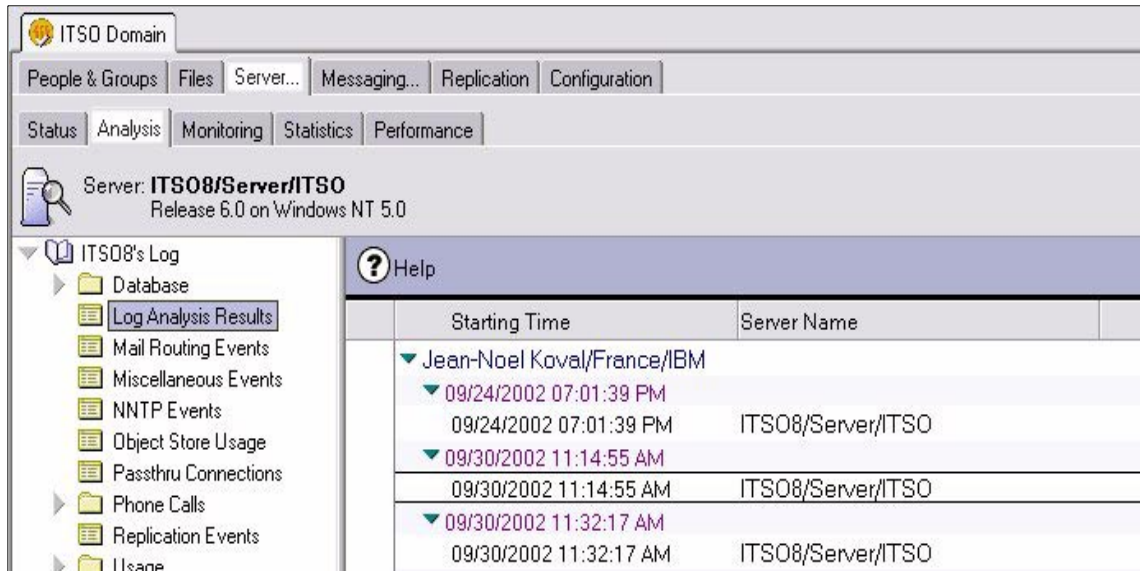


Figure 8-39 All saved Log search result

Using this enhanced Log search, a Domino administrator can easily schedule some profiled daily/weekly searches. While Domino does the searches for you in the background, you can continue any other tasks either with the Domino Administrator 6 client or Lotus Notes 6 client.

8.2.2 Console properties: Event filter and color coding

In addition to using Log search to look for some specific events that have occurred, you can also set your remote server console with some color properties or event filters to display some specific information about events in real time. When you use event filtering or event color coding, you have the ability either to create settings for your session only, or to make selections globally.

Creating settings for your session only means that the settings will apply to all remote server consoles you have open during this session, but when you close your Domino Administrator 6, the settings are reset.

You can define settings globally, which means they will be applied to all your sessions at any time. In this case your profile will be saved in a local database, Monitoring configuration.

Create a temporary session-based filter and color coding for events

From your Domino Administrator 6, open a remote server console on any Domino R5 or 6 server. (Select Server tab -> Status tab -> Server Console in the left pane.)

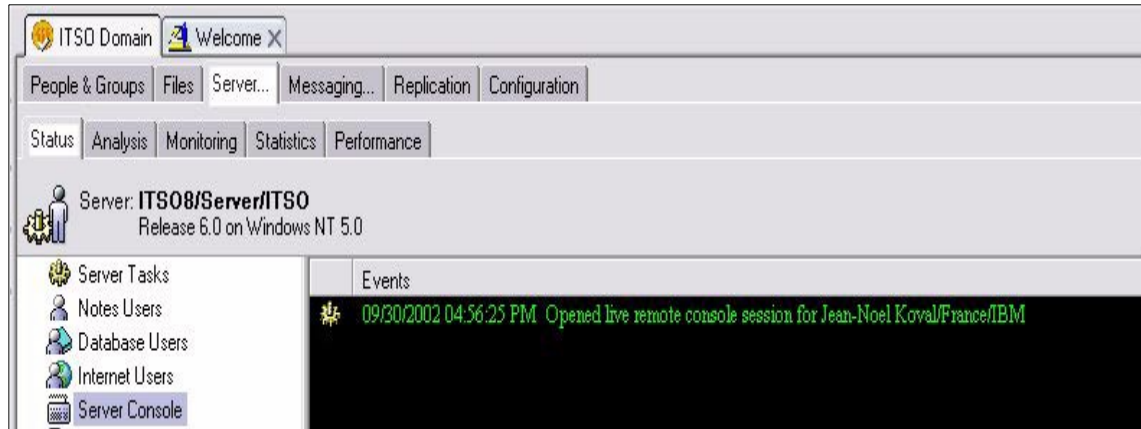


Figure 8-40 Opening a Remote Server Console in Lotus Domino Administrator 6

Now, to set some preferences for displaying and for event filtering, you can either right-click on the Remote Server Console icon, or use the menu action Live Console. In this example we used the first option to open the Console Properties box, and selected Server Console.

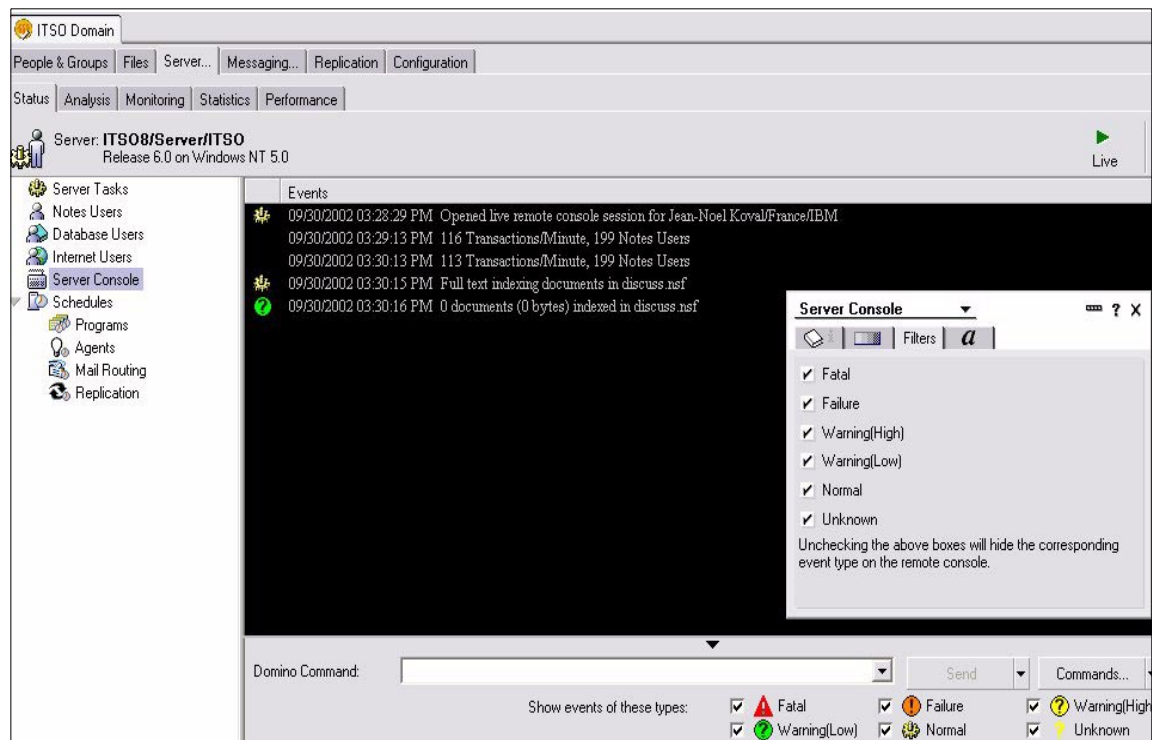


Figure 8-41 Server console properties box

You can now navigate to the different tabs to specify which event levels you want to see displayed at your remote server console, and to define which colors to use for different elements.

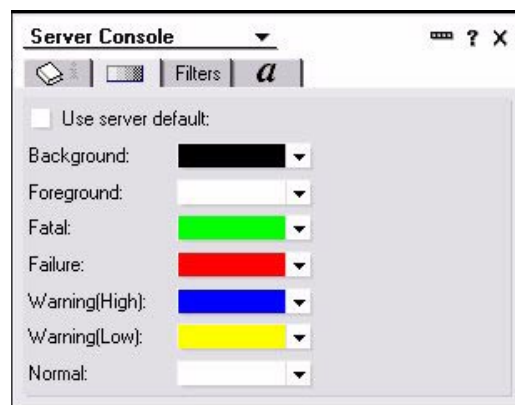


Figure 8-42 Server Console properties

When all your settings are defined, close this dialog box and see the immediate change on the remote console. Figure 8-43 shows an example.

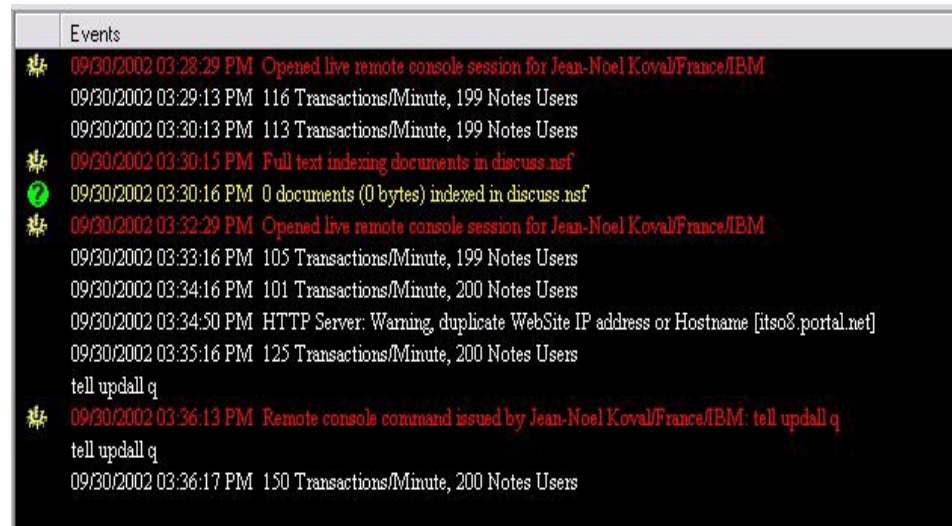


Figure 8-43 Customized remote console settings

At the bottom of your remote server console is a switcher that displays some options to enable you easily to change the level of information displayed on the console.



Figure 8-44 Expanding remote server console properties

All these settings are persistent across all remote server console sessions you open without exiting your Domino administrator client; this works on both R5 and Domino 6 server consoles. (No event or color coding will be displayed when you open a Domino R4.6.7a server.)

Creating persistent settings

If you want to create some persistent console settings that you will be able to retain after each exit of your Domino Administrator 6, open your local Monitoring Configuration database (events4.nsf) and select Console Attributes in the left pane.

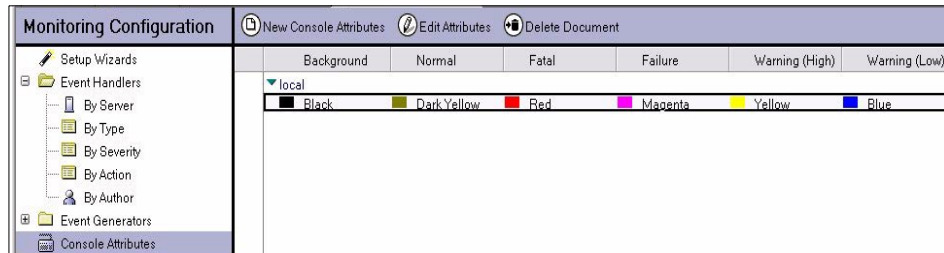


Figure 8-45 Local console attributes

Edit the document that refers to local settings and select the colors you want to use for various elements on your remote server console.

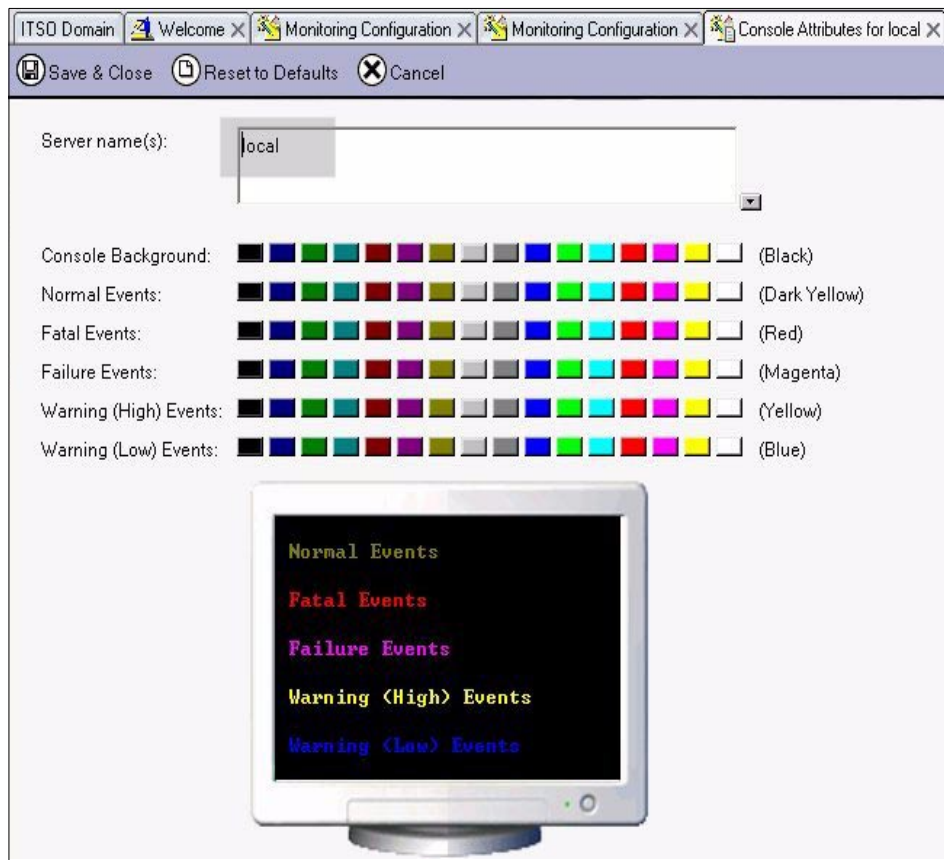


Figure 8-46 Local color attributes for your remote server console

Attention: In the field Server Name(s), be sure that you select Local, so this setting will be applied to your local Client, not the server that you want to monitor.

If you want customize your server console, follow the same procedure on your server-based Monitoring Configuration database.

Using log filters

To select any Log filter, still on your local Monitoring Configuration database, go to Log Filter menu in the left pane and edit your local document.

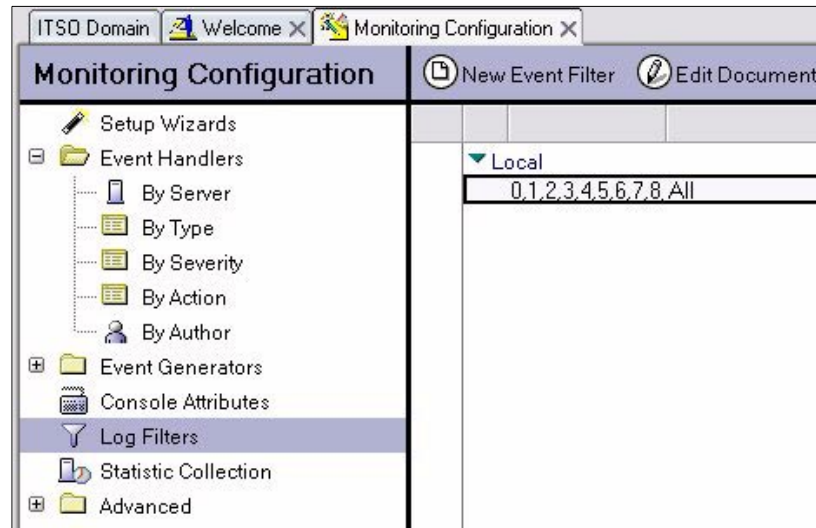


Figure 8-47 Definition of your local settings for your event filter option

After opening your local document, open the Console tab to display console settings. Select which severity levels you want to show up on your remote server console.

Log Filters

Basics | Database | Console

Filters:

Log unknown types/severities? ☒ Yes ☐ No

☒ Log All Types ☐ Select Types

Severities for All Types:

☒ Fatal ☒ Failure ☒ Warning(High) ☒ Warning(Low) ☒ Normal

Figure 8-48 Local filter settings

When done, you can save your document and go back to your server remote console session to see that all changes have been applied. You can override these settings anytime, either by changing your previous selections in your local Events4.nsf database or by re-editing your console preferences, as described.

Console lookup error

When an unknown message displays on your remote server console, you now have the ability to look up the meaning of the message. When you see an unexpected message, (most easily by using event color coding), use the following steps to determine its meaning:

1. Pause your live console and highlight the line with the error message.
2. Right-click to open a pop-up menu.
3. Select Lookup error to get an explanation of the error.

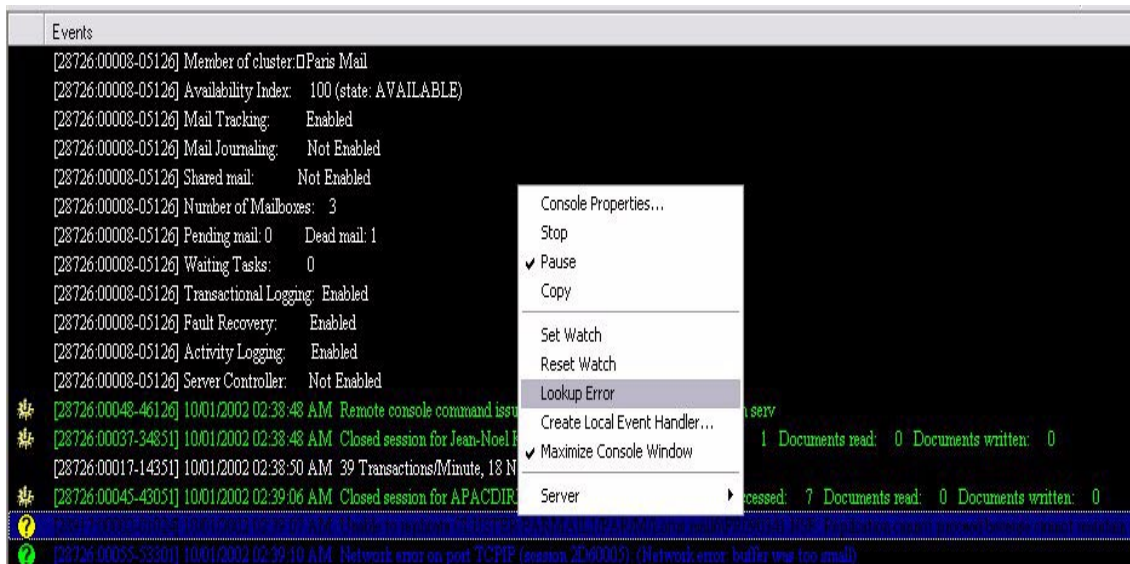


Figure 8-49 Invoking Lookup Error from a remote server console

4. Lookup Error opens a document containing information about the selected message. (An example of the basic information about the error is in Figure 8-50).

Server and Addin Task Event

Basics
Advanced

Original text:

Addin name:

Value:

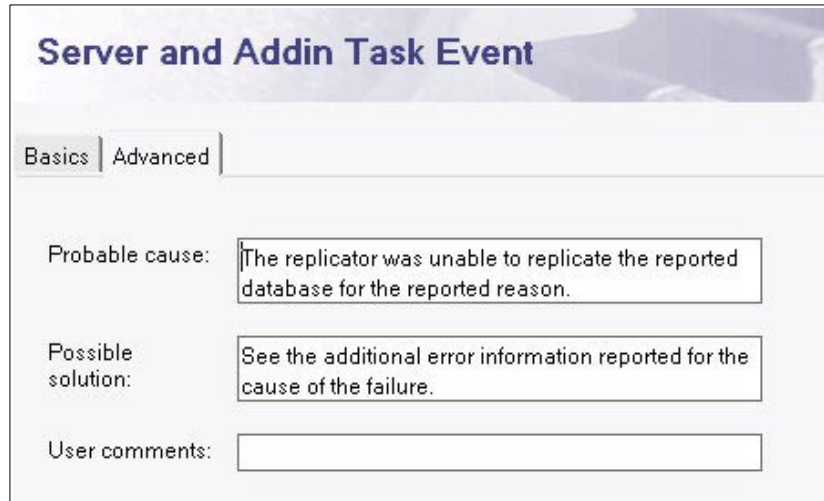
Event type: Replica

Event severity: Warning (high)

Suppression time: minutes

Figure 8-50 Basic information from Lookup Error

5. Click the advanced tab for more advanced information, if any is available for the error message.



The screenshot shows a dialog box titled "Server and Addin Task Event". It has two tabs: "Basics" and "Advanced", with "Advanced" selected. The "Advanced" tab contains three text input fields. The first is labeled "Probable cause:" and contains the text "The replicator was unable to replicate the reported database for the reported reason." The second is labeled "Possible solution:" and contains the text "See the additional error information reported for the cause of the failure." The third is labeled "User comments:" and is empty.

Figure 8-51 Advanced information from Lookup Error

Furthermore, you have the capability of adding your comments in these documents and editing any fields if you want customize the information.

There are more than 4000 definitions available for you by default. If you don't find information for some errors, you can create your own entry and extend this knowledge database.

Attention: All this information are stored on your local events4.nsf. If you customize any information or create your own entries, do not forget to do a local archive of your events4.nsf.

Setting and resetting watches

When you are looking for any additional occurrences of a specific message at the console level, you don't want to monitor the server console by looking at it all the time—especially if you run a busy server where a lot of information is displayed rapidly.

An easier way to keep track of something is to set up a watch, which will bring to your attention specific selected messages, and the next 10 lines.

During a live console session, when you see a message of interest that you want to pay attention to, use these steps to enable a watch:

1. Pause your live session.

2. Highlight the message by right-clicking it, then select Set Watch from the pop-up menu.
3. Now only the next occurrence of this message will be shown at the console, plus the next 10 lines which follow it.

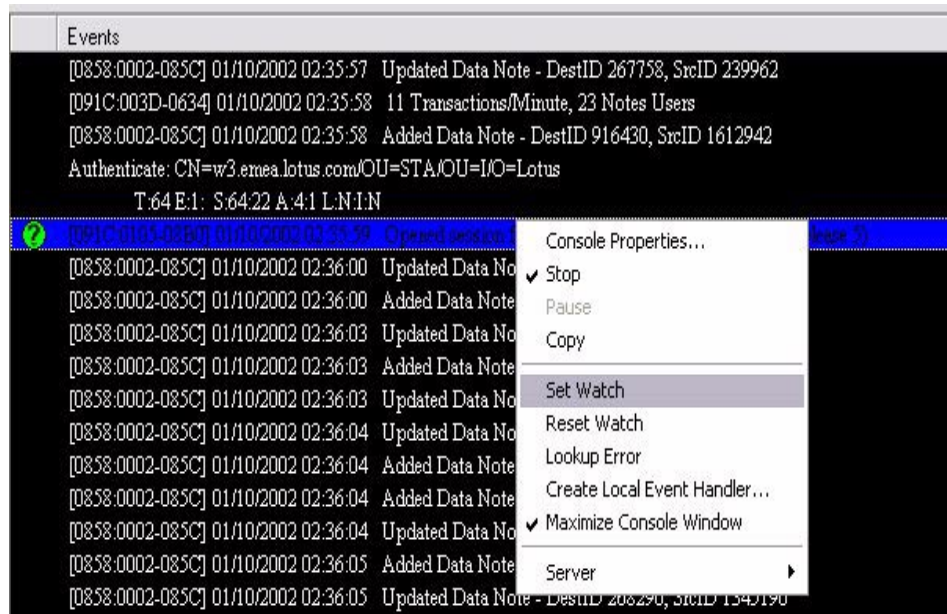


Figure 8-52 Enabling Set Watch

4. When Set Watch is successfully enabled, you will get the confirmation shown in Figure 8-53, and you can turn on your Live session. Your Remote Server Console will pause at the next occurrence of the error message.

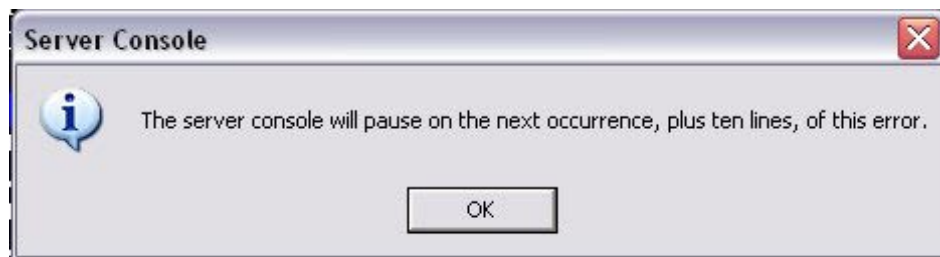


Figure 8-53 Set Watch confirmation dialog box

5. To turn off this setting, return your live console session to pause mode, open the pop-menu by right-clicking, and select Reset Watch.

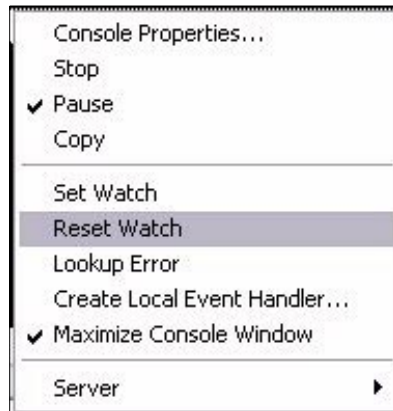


Figure 8-54 *Reset Watch selection*

This will bring up the confirmation message shown in Figure 8-55.



Figure 8-55 *Reset watch successfully disabled*

You can now return to your live remote console, and create a watch if needed.

8.3 Activity logging

Activity logging is a new feature which replaces the Billing task used in previous releases. You can use activity logging to collect and record information about your Domino server activities and determine what kind of activities your Domino server is doing during a period of time.

Activity logging is another piece of Domino monitoring functionality; it can be used to monitor system usage, conduct resource planning, and maybe to determine if clustering will be required.

Furthermore, activity logging can be used to charge users based on their actual use of the Domino services. This is especially useful in Application Service Provider mode, when you need to “bill” each organization that you host based on what they use.

Domino writes the activity logging information in the Domino Log file (log.nsf). This recorded information is not visible in the log file, but it can be displayed by either using the Domino Administrator 6 client or writing a Notes API program to access information in the log file (log.nsf).

Note: For information about writing an API program, see the Lotus C API toolkit for Notes/Domino 6. The toolkit is available for download at:

www.lotus.com/1dd

Activity logging does not require you to run a specific server task; it works with the same process that already exists to record user activity in a database

8.3.1 Enabling activity logging

Activity logging is enabled from a server configuration document using the following steps:

1. From your Domino Administrator 6 client, select the Configuration tab, and select the Server\Configurations view to display all existing configuration documents. You can enable activity logging for all your servers with a global configuration document, for a group of servers, or even server by server.

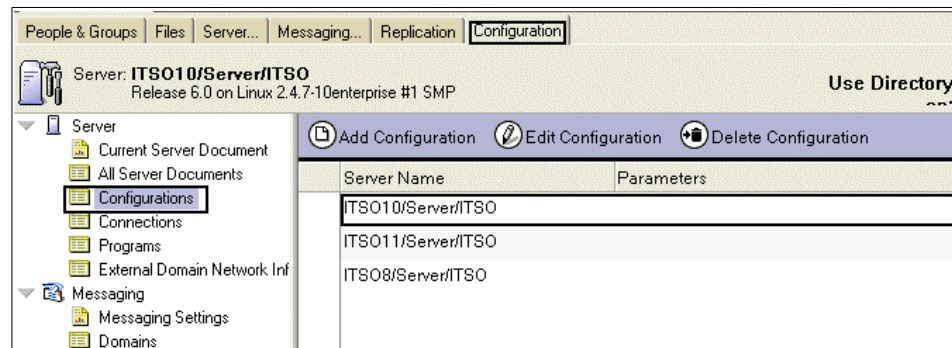


Figure 8-56 Configuration documents

2. Open (or create) the appropriate server configuration document (related to the server or group of servers) that you want enable activity logging for, and click the Activity Logging tab.

Configuration Settings : ITS010/Server/ITS0

Basics | Router/SMTP | MIME | NOTES.INI Settings | iNotes/Web Access | IMAP | SNMP | **Activity Logging**

Activity Logging | Activity Trends

Activity logging is enabled: ☒ Yes

Server Activity Logging Configuration

Enabled logging types:

- ☒ Domino.LDAP
- ☐ Domino.POP3
- ☐ Domino.SMTP.Session
- ☐ Domino.SMTP.Message
- ☐ Domino.Notes.Database

Checkpoint interval: 15 minutes

Log checkpoint at midnight: ☒ Yes

Log checkpoints for prime shift: ☒ Yes

Prime shift interval: 9 AM - 6 PM

Figure 8-57 Configuration of Activity Logging

3. Go to edit mode and check that “Activity Logging is enabled” is set to Yes.
4. In the Server Activity Logging Configuration area, enter or select the appropriate information.
 - a. Enabled logging types:

Agent Records agent activity which runs on the server:

Name of the agent
 Name of the database where agent runs
 Amount of time that the agent ran
 Name of the last agent modifier person

There is no record for an agent that runs from a Web server, or that can run locally on a client or be triggered manually from a client.

HTTP Records Web server requests:

Name of Web server and user requestor
 URL that user clicked
 Number of Bytes returned / result of the request
 Amount of time to process the request
 Time at which the request occurred

IMAP Records IMAP Session activity:

- User name, IP address of the client
- Number of bytes sent and read
- Duration of the session

LDAP Records activity about every LDAP request, but due to the different types of LDAP activities, Domino generates a different record for each type:

- Abandon
- Add
- Bind
- Compare
- Delete
- Extended
- Modify
- ModifyDN
- Search
- Unbind

For each type of activity, you record at least organization name, user name, server name, client IP address, and the specific information related to the request.

Mail Tracks mail that is sent from and received by a server:

- Name of the server that created the record
- Originator and recipients of a message
- Message ID and size
- Mail routing path information (preceding and next hops)

Furthermore, for Mail Activity Logging, there are five types of Activity logging: Deposit, Delivery, Delivery Failure, Transfer, Transfer Failure.

Notes.Database Records database activity during a server session:

- Name of the database
- Name and address of the user
- Number of documents and Bytes read and written
- Total number of transactions executed in the database
- Duration of time that the database was open

Notes.Passthru Tracks passthru activity that is generated by client or a server through a passthru connection:

- Number of bytes sent and received
- Number of documents read and written
- Number of transactions executed
- Duration of the passthru session

Notes.Session Tracks information about network traffic which occurs during a server session with a client or with another server:

- Name and network address of the session user
- Number of document and bytes read written
- Number of transactions executed
- Duration of the session

POP3 Tracks information about a POP3 session:

- User name, IP address of the client
- Number of bytes sent and read from the server
- Number of messages sent to the client
- Number of messages deleted from the client
- Duration of the session

Replica Tracks activity about each database replication that a server initiates; only the initiating server generates activity logging records:

- Name of the source and destination servers
- ReplicaID of the database
- Number of bytes replicated in each direction

When a user initiates replication with a server, Domino records the activity as Session activity. In addition, Cluster Replication does not generate activity logging records for replication.

SMTP Tracks information about your SMTP activities, and can be broken up in two types: Session and Message activity type:

- IP address of the connected client
- Number of message sent by the client to the server
- Number of bytes sent and received
- Number of recipients to who a message is sent
- Duration of SMTP session

- b. Enter a value in minutes for “Checkpoint interval” (by default 15 minutes). For some types of activity, Domino creates multiple records during a session, especially for activity which can be active for a long period of time. Instead of creating an activity record each time, Domino uses a checkpoint record to summarize long duration activities in one record at the end of the session. If an activity record needs to span over a checkpoint interval, the record is logged to ensure that no information will be lost if the server stops functioning before the end of the session. When the session is ended, Domino consolidates all the activity for the entire session. The following types of activity can generate a checkpoint:

- Domino.IMAP
- Domino.Notes.Session
- Domino.Notes.Database

- Domino.Notes.Passthru
- Domino.POP3
- Domino.SMTP (session and message)

Important: To determine the duration of a checkpoint you must balance the following requirements:

1. Need to record information.
2. Need to preserve storage (activity logging is written to log.nsf).
3. Need for performance (activity logging is consuming some resources).

If you create a long checkpoint period interval, you can lose a lot of information if a server failure occurs before information is written into the checkpoint records. On the other hand, if you use a short interval, more disk space will be needed to store this additional checkpoint information. In summary, be sure that you create an activity logging record only for the activity that you really need to track.

- c. Select Log checkpoint at midnight to automatically create Notes session and Notes database checkpoint records every day at midnight (Optional) and have a starting point each day (some activity can span across midnight).
- d. Select “Log checkpoints for prime shift” to automatically create Notes session and Notes database checkpoint records every day at the beginning and end of a specific time period, and then specify the times for the Prime shift interval (Optional). Prime Shift interval is the period of time where you have all your users working, usually 8 AM to 6 PM.

8.3.2 Reporting Activity Logging data

When Activity logging is enabled on your servers, you can retrieve the information using your Domino Administrator 6 client.

Tip: To check if Activity Logging is running on your server, issue the following command at the server console:

```
>show server
```

Look at the last lines to see if activity logging is listed as enabled.

```
Lotus Domino (r) Server (Release 6.0 for UNIX) 12/01/2002 01:58:07 AM
Server name:          ITS010/Server/ITS0 - Linux RH72 - Located Lotus
Paris Lotus
Server directory:     /domino/data
Partition:            .domino.data
Elapsed time:         5 days 20:37:29
Transactions/minute:  Last minute: 12; Last hour: 4; Peak: 1696
Peak # of sessions:   7 at 11/28/2002 08:51:21 PM
Transactions:         12660
Availability Index:    100 (state: AVAILABLE)
Mail Tracking:        Not Enabled
Mail Journaling:      Not Enabled
Shared mail:          Not Enabled
Number of Mailboxes:  1
Pending mail: 0       Dead mail: 0
Waiting Tasks:        0
Transactional Logging: Not Enabled
Fault Recovery:        Not Enabled
Activity Logging:      Enabled
Server Controller:     Not Enabled
```

1. From your Domino Administrator 6 client, select the server that you want to analyze. Click Server\Analysis tab, expand the Tools pane, and select Activity.



Figure 8-58 Select Activity report from your Domino Administrator client

2. After selecting Activity, define which activity you want to report. By default all activity types available on your server are selected.

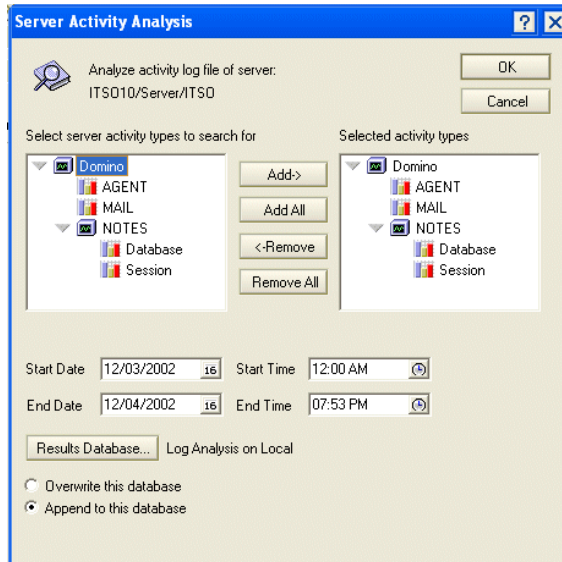


Figure 8-59 Select the activity to analyze

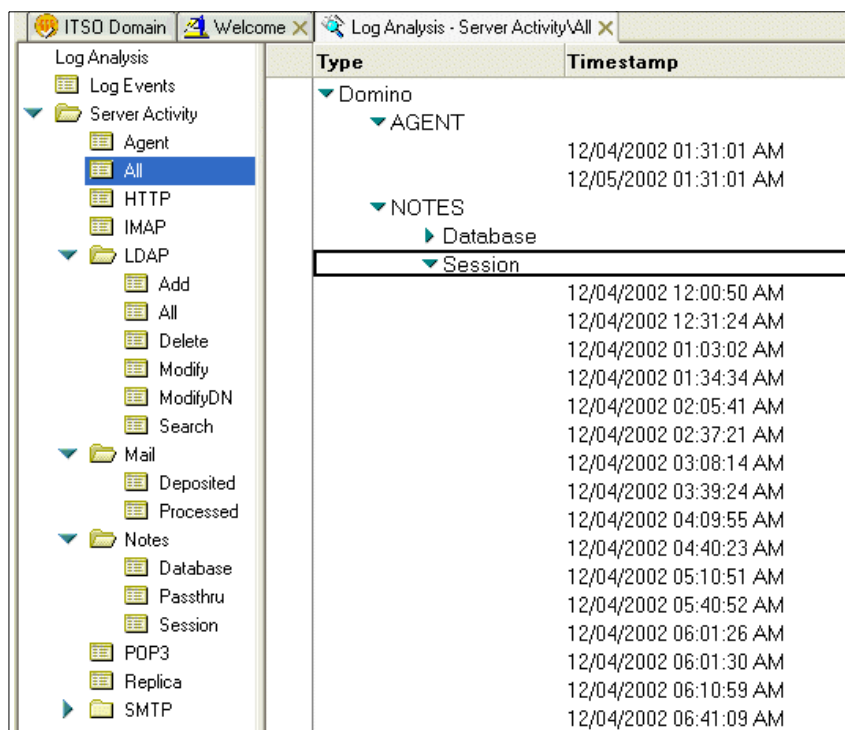
- a. In the right column (selected activity types), highlight any activity type that you don't want to analyze at this time and click the remove button. You can use the Remove All button and then Add activities back one by one, by highlighting available ones from the left column. (Select server activity types to search for.)
- b. Select starting and ending dates and times for the activity that you want to display. Note that the time period is not applied day by day (It's really the precise time that you want to start and end the search.)
- c. Specify a result database by clicking "Result database" to define where you want to store the search result, either locally on your workstation or on a server. Give a title and a file name to your result database (by default the title is Log Analysis and file name is Loga4.nsf). Be aware than even if you choose to create a result database on a server, the process will use LOGA4.NTF (Notes Log Analysis 6) which is located on your workstation. Click OK
- d. Finally, you have to choose if you want to append your result to an existing result database or overwrite an existing one in the case you have selected an existing database in the previous step. Select Yes to append the current search to an existing database. Note that a same database can store several searches coming from differents servers in one central location and be used for futher reference. When all your settings are defined, you click OK to launch the search. As for Log search, this operation occurs in

the background, allowing you to switch back to another operation with your Domino Administrator client. A status bar displays the search progress.

Attention: Since activity Logging uses log.nsf, if you use a purge interval period of 7 days and you don't want to lose any data, you should run your activity search on the same interval (that is, each week).

A good practice is to use a database for each month of activity or a database per server.

When the search is done, the result database is displayed on your Domino Administrator 6 client as shown in Figure 8-60.



Type	Timestamp
Domino	
AGENT	12/04/2002 01:31:01 AM
	12/05/2002 01:31:01 AM
NOTES	
Database	
Session	
	12/04/2002 12:00:50 AM
	12/04/2002 12:31:24 AM
	12/04/2002 01:03:02 AM
	12/04/2002 01:34:34 AM
	12/04/2002 02:05:41 AM
	12/04/2002 02:37:21 AM
	12/04/2002 03:08:14 AM
	12/04/2002 03:39:24 AM
	12/04/2002 04:09:55 AM
	12/04/2002 04:40:23 AM
	12/04/2002 05:10:51 AM
	12/04/2002 05:40:52 AM
	12/04/2002 06:01:26 AM
	12/04/2002 06:01:30 AM
	12/04/2002 06:10:59 AM
	12/04/2002 06:41:09 AM

Figure 8-60 Result database of Activity Logging search

Each type of activity and operation is stored in a document that you can display by clicking on the appropriate document to open it.

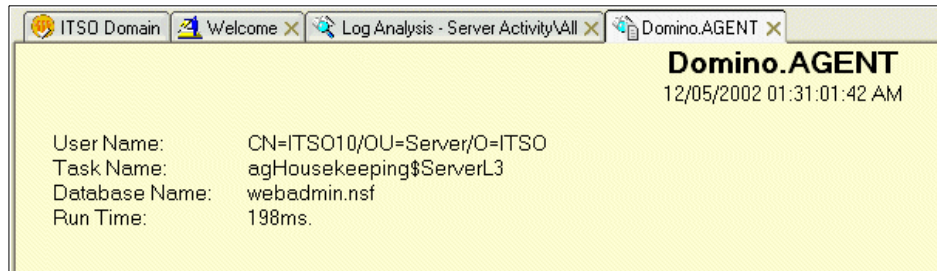


Figure 8-61 Document from activity logging result database

Since all the results are stored in simple documents in a notes database, it's easy for an administrator to display result on a very efficient way. You can easily arrange or display the needed information as you wish, plus now you can rearrange column order just by dragging the headings into the position that you find most useful.

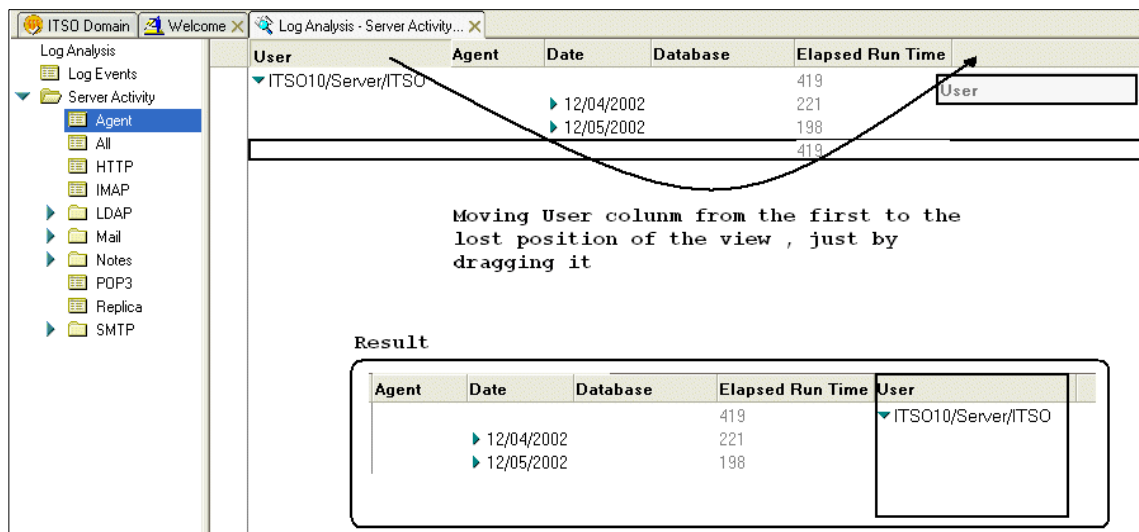


Figure 8-62 Reorganization of a view

Futhermore, when you rearrange a view by using this method, your changes are stored locally and will persistent accross your Notes/ Domino session.

Activity logging can be a very valuable source of information to understand how your system is performing, and who is doing what. This is an open solution that you can customize to meet your specific requirements. But because it is resource-intensive, be sure that you log only needed information for the specific server. Logging everything without really exploiting the information will not really help you.



New messaging administration options

This chapter provides a discussion of the new options available to administrators for controlling the Domino 6 messaging environment. Topics covered include Router controls (System mail rules, Mail journaling, Quota management, and prevention of automatic forwarding), SMTP relay controls (including DNS Blacklists), Automatic archiving, Single copy object store, and IMAP improvements.

9.1 Router controls

The heart of any messaging system is the directory and the message delivery subsystem, that is, the router in Notes. The router controls the flow of messages between users and between servers. Domino 6 expands the configuration possibilities of the router, thereby expanding the control the administrator has over the messaging environment. This section explains how to configure the router with system mail rules, mail journaling, and quota management.

9.1.1 System mail rules

System mail rules act on messages which go through the servers' mail queues (mail.box). They are administered through server configuration documents. Rules can be used to filter out messages from known spam sites, to filter out inappropriate content, or to fulfill specific legal requirements.

Rules can use the message headers, the body of the message, or even the form which a mail message is using, to determine whether to act on them. The combination of conditions and actions is quite large. You can filter out known spam senders with these rules or prevent your own users from sending out a message to a large number of recipients.

However, system mail rules are not intended to serve as an anti-virus mechanism. There are much stronger products which are dynamically updated to keep up with the proliferation of viruses.

Configuration of system mail rules

1. In the Administration client click the Configuration tab and expand the Messaging section.
2. Click Configurations.
3. Select the configuration settings document for the server you want to administer and click Edit Configuration.
4. Click the tabs in the following order: Router/SMTP -> Restrictions and Controls -> Rules

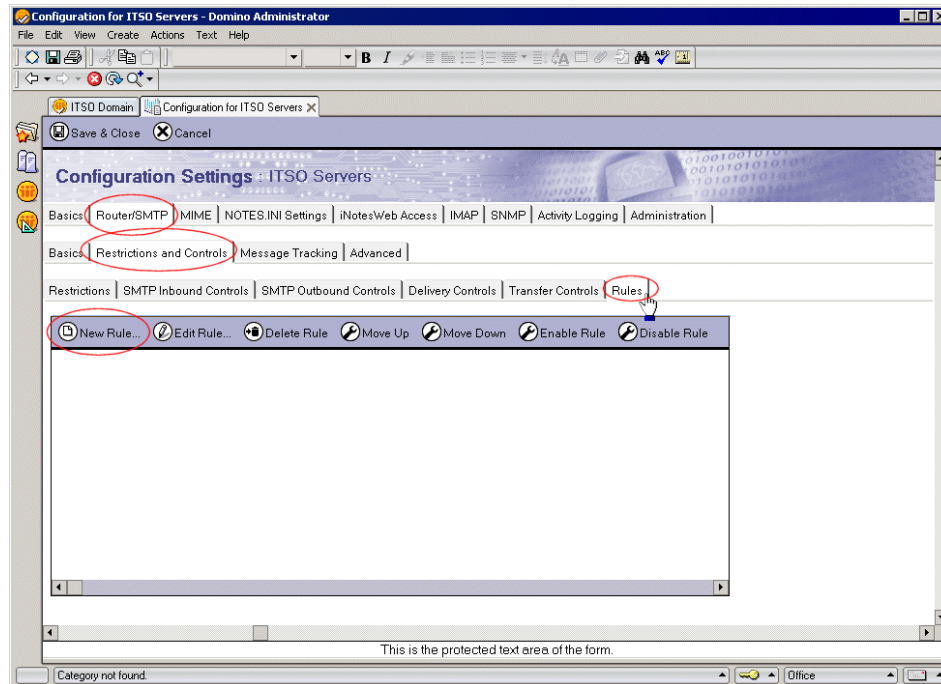


Figure 9-1 Where to set up mail system rules

5. Double click the document or click the Edit Server Configuration button to put the document in edit mode.
6. Click New Rule to create a new rule document.

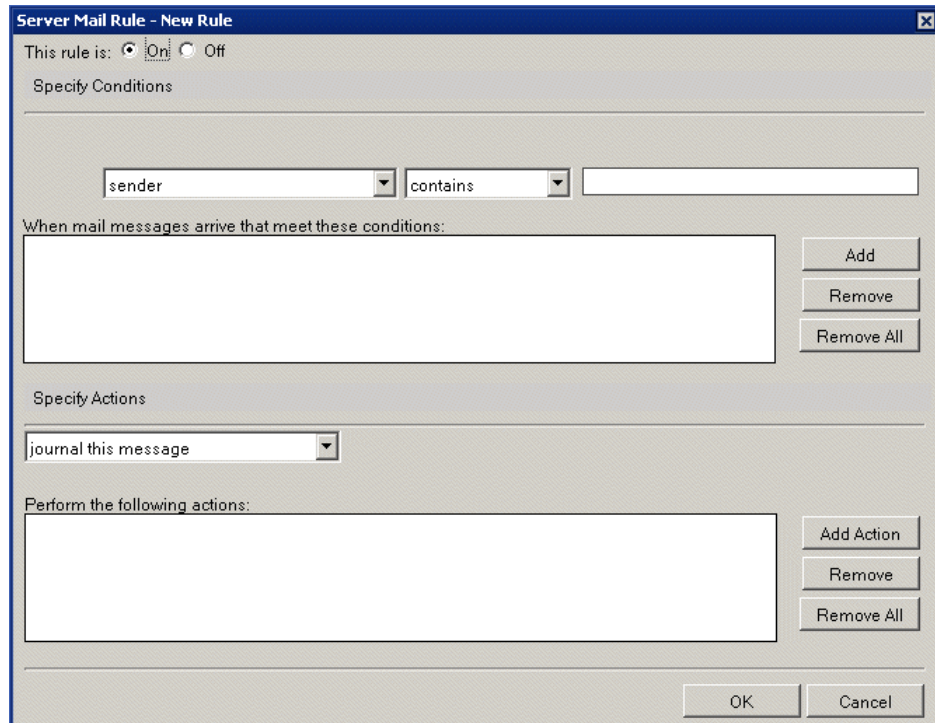


Figure 9-2 New Server Mail Rule

7. Note that the default setting is for this rule to be turned on once you save it.
8. In the Conditions section of the new server mail rule, specify different ways of identifying the mail that you want the rule to act upon.
 - a. First choose a field for the rule to look at:
 - sender
 - subject
 - body
 - importance
 - delivery priority
 - To
 - CC
 - BCC
 - To or CC
 - body or subject
 - internet domain
 - size (in bytes)
 - all documents
 - any attachment name

- number of attachments
- form
- recipient count
- any recipient

This rule is: ☒ On ☐ Off

Specify Conditions

When mail: sender (selected) | conditions: contains (selected) | [Text Input]

Buttons: Add, Remove, Remove All

Figure 9-3 Choose the field to be examined by the rule

- b. Each of the fields can be tested for the following conditions:
- contains / does not contain
 - is / is not

This rule is: ☒ On ☐ Off

Specify Conditions

When mail messages arrive that meet these conditions: sender (selected) | conditions: contains (selected) | [Text Input]

Buttons: Add, Remove, Remove All

Figure 9-4 Specify the criterion for the field

- c. Fields with numeric logic can be tested for the following conditions:
- is less than / is greater than
 - is / is not

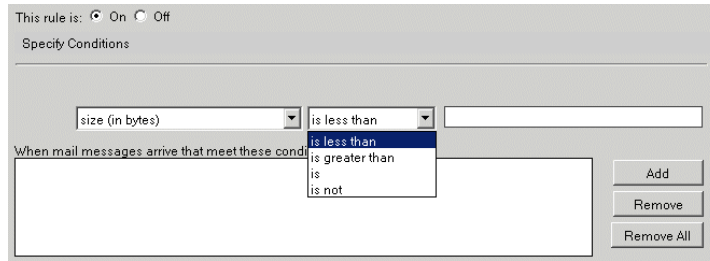


Figure 9-5 Numeric test

9. Click the Add button to enter the condition into the rule. Note that you can add more conditions and that they will be related to the previous condition in one of two ways: and / or.

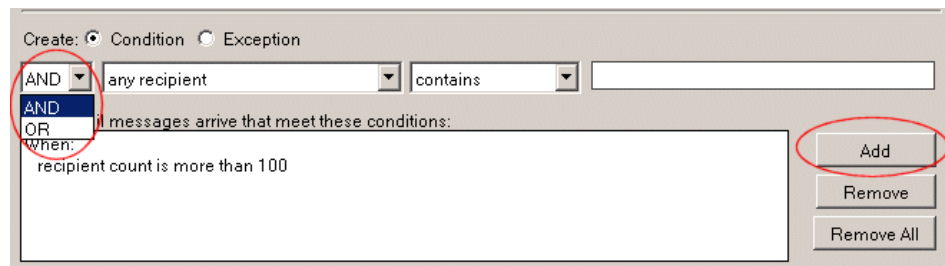


Figure 9-6 Add the condition

10. Move to the Specify Actions section of the Server Mail Rule dialog box. There are five actions available for selection. Only one action per rule can be selected.

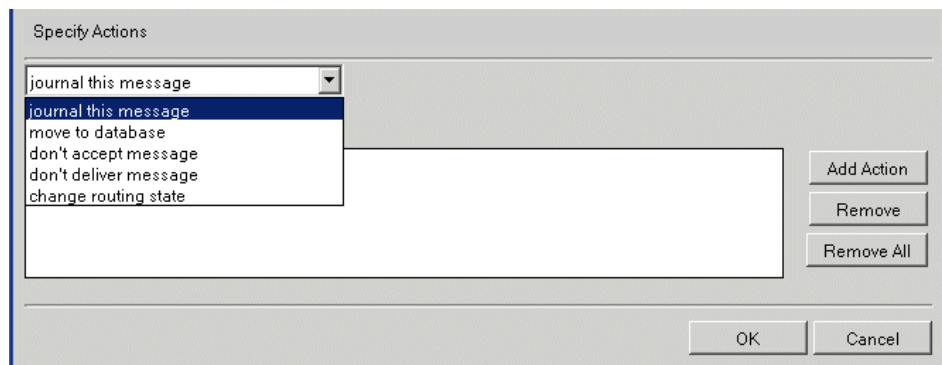


Figure 9-7 Specify action

a. **journal this message**

This is used in conjunction with mail journaling, which is discussed later. See below.

b. **move to database**

You could create a “graveyard” or “quarantine” db for suspicious messages. Be sure to specify the server on which you are creating the rules prior to selecting the database. The router assumes a relative path from the data directory of the server.

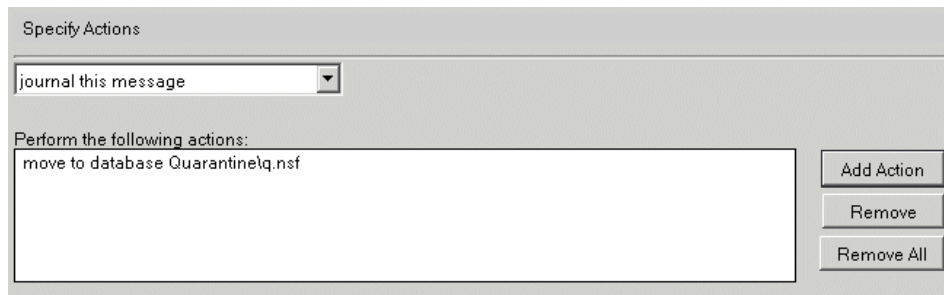


Figure 9-8 Move to database

Tip: Use the normal mail template (mail6.ntf) or the mail journaling template (mailjrn.ntf) to create a quarantine database.

c. **don't accept message**

An internal Notes sender receives an immediate dialog box that the message has been rejected. The message never leaves the user's mail file. For an SMTP message the router informs the connecting SMTP system that it will not accept the message.

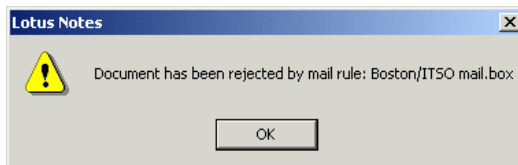


Figure 9-9 Immediate rejection notice

d. don't deliver message

You can configure the system to send a non-delivery report to the sender or to delete the message silently. The non-delivery report states that the message was not delivered because of policy reasons.



Figure 9-10 Non-delivery report

e. change routing state

Domino accepts the message but its routing state in mail.box is changed to “Held.”

11. Once you have finished creating the rule, click OK to close the New Rule dialog box.
12. Click Save & Close to save the Server Configuration Document. The rule will not be recognized until the server configuration document has been saved and the router has recognized the new rules.

Tip: You can force the router to read the new rules by entering this command at the console:

```
set rules
```

The router will respond with the number of system filters it has recognized.

13. You can manage the system rules with the buttons on the Rules tab of the configuration document. You can prioritize, enable, and disable rules.

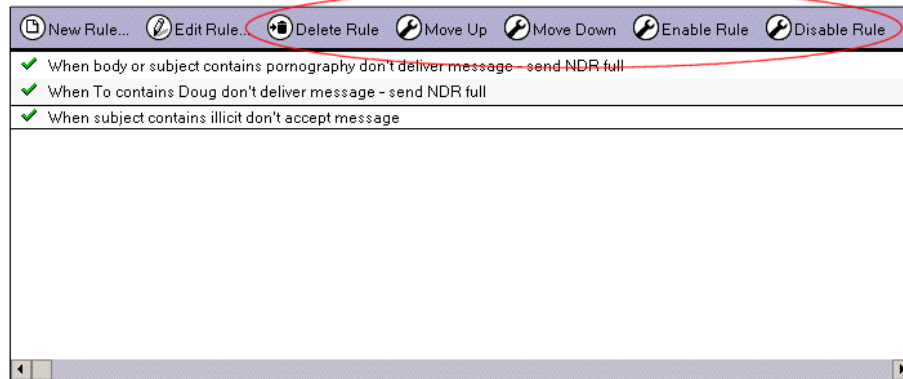


Figure 9-11 Manage system rules

Attention: It is possible to set up a group server configuration document or a global domain document and apply the rules there. However, there are some caveats to doing this:

- ▶ The router reads its own server's configuration document first. If any rules have ever been created in this document it will only read this document to find rules.
- ▶ Once rules are added to a server configuration document, two fields are added to the document. Just the fact that those fields are present in the document causes the router to ignore the system mail rules in other configuration documents.
- ▶ In order to get the router to recognize the rules in a global domain document or a group server configuration document, you can delete the server configuration document and create a new one (which will not have those fields in it) or create an agent with this Lotus script in it:

```
FIELD $FilterFormulaCount:=@DeleteField;
FIELD $FiltersSeqNo:=@DeleteField;
SELECT @All
```

Delete the rules from the server configuration document and save/close it. Select the server configuration document and run the agent. It will strip the fields from the server configuration document. After that the router will be able to register the system mail rules from a higher level configuration document.

9.1.2 Mail journaling

Mail journaling saves a copy of messages that go through one of the system mail queues (mail.box). It can be configured to save all the messages that go through the queue or a subset of them, based on any mail rule. For example, you can configure the system to save all of the messages for a particular subset of users, such as all users in an OU, or just one user. Or it can copy all messages which have a particular word in the subject line or body of the message.

Mail journaling can help an organization meet legal requirements by automatically storing the appropriate messages.

Business reasons for using mail journaling

Suppose a manager suspects that one of his or her employees is using e-mail for completely inappropriate activities, like subscribing to a pornography list. Most companies have explicit policies against such use of their systems. Once the appropriate channels have been followed, the e-mail administrator is asked to investigate. The administrator can use mail journaling to keep a copy of every e-mail a single user sends and receives without the employee having any knowledge of it.

Journaling types

Attention: In order to configure mail journaling, you must have a mail journaling system rule set up.

Mail journaling is configured per server in two different ways:

1. **Local journaling:** Set up a database on the server and configure journaling to put a copy of each message in that database. Since each server has its own mail journaling database, this method does not add to network traffic. If you use local journaling the Domino system automatically maintains the mail journaling database by creating a new mail journaling database when the database reaches a specified size, or on a periodic basis.
2. **Remote journaling:** Set up a mail-in database and configure journaling to send a copy of each message to the mail-in db. With this method it is possible to configure all servers to send the captured messages to one location, instead of having a mail journaling database on every server. This method requires you to set up a mail-in database (and mail-in database document) manually, and to maintain it. Since this method is harder to maintain and adds to network traffic, it is not the preferred method.

Local journaling configuration

1. Create a special ID which will only be used for accessing the mail journaling database.
2. Create a system mail rule to capture the messages you want to be put in the journal (see 9.1.1, “System mail rules” on page 210).
3. Verify that there is a configuration settings document for the server which you want to configure for mail journaling.
4. From the Administrator, open the server on which you want to set up mail journaling.
5. Go to the Configuration tab and click Messaging -> Messaging Settings -> Advanced -> Journaling

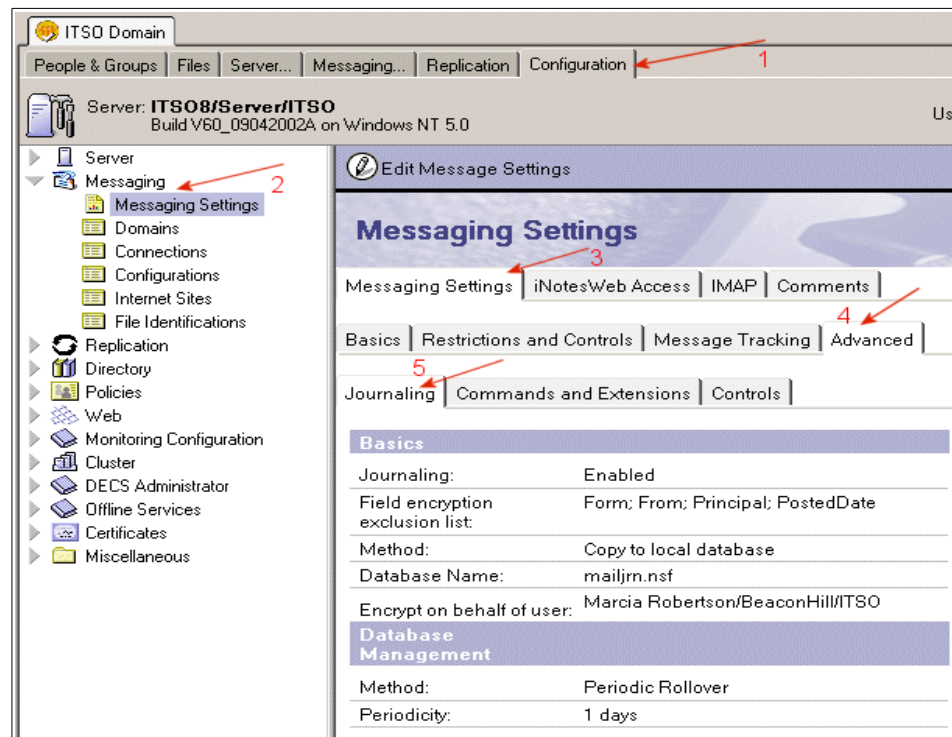


Figure 9-12 Navigating to the Journaling Configuration page

6. Put the Message Settings document in edit mode and click the Journaling tab. Modify the following fields in the Basics section:
 - Journaling: Enabled
 - Method: Copy to local database (default value)
 - Database Name: mailjrn.nsf (default value)

- Encrypt on behalf of user: Select the mail journaling ID created in step 1.
7. In the Database Management section make selections for how the database will be maintained:
 - Choose a periodic rollover to manage the db on a timetable.
 - Choose a size rollover to select the maximum size for the mail journaling database.
 - Choose Purge/Compact to specify a data retention period, after which the database will be purged and white space eliminated.
 - Choose None if you don't want Domino to manage the size of this database.
 8. Use the server console to tell the router to update its configuration:

```
tell router update config
```

Once the router updates its configuration, it creates the mail journaling database, adds all the Server Administrators to the ACL, and starts enforcing the mail system rules for mail journaling. Note: the router automatically updates its configuration approximately every 5 minutes.

Note: In order for the special ID to have access to the mail journaling database, you will have to add it to the ACL of the mail journaling database manually. One extra security measure would be to not add this ID to the ACL of any of the journaling databases (current and rolled-over) until it is necessary for someone to actually read one of the messages

9. Test the configuration:
 - a. Verify that the system mail rule is capturing the correct messages.
 - b. Verify that the router is encrypting the messages with the correct notes certificate.

Remote journaling configuration

1. Create a special ID which will only be used for accessing the mail journaling database.
2. Create a system mail rule to capture the messages you want to be put in the journal.
3. Create a new database based on the mail journaling template (mailjrn.ntf, available on Domino 6 servers -> Advanced templates).
 - Create this database in its own subdirectory to make management of it more intuitive.
 - On the Design tab of the database properties, unselect "Show in 'Open Database' dialog," so that users will not accidentally find it.

- Modify the ACL of this database to match the security requirements of your organization. Be sure to add the special ID created for encrypting the mail journaling database.
4. Configure the database as a mail-in database by creating a mail-in database document:
- Basics Tab: Encrypt incoming mail: Yes
- Use the Get Certificates button on the action bar to select the Notes certificate which will encrypt the incoming messages. Select the ID created in step 1. Encrypting this database with a real person's ID is not recommended.
- Administration Tab: Allow foreign directory synchronization: No

Mail-In Database: Mail Journal	
Basics Other Comments Administration	
Basics	Location
Mail-in name: <input type="text" value="Mail Journal"/>	Domain: <input type="text" value="ITSO"/>
Description: <input type="text" value="Mail Journaling DB"/>	Server: <input type="text" value="ITSO8/Server/ITSO"/>
Internet Address: <input type="text" value=""/>	File name: <input type="text" value="journalmailjrn.nsf"/>
Internet message storage: <input type="text" value="No Preference"/>	
Encrypt incoming mail: <input type="text" value="Yes"/>	

Figure 9-13 Mail-In Database setup for mail journaling

5. Configure mail journaling:
- Verify that there is a configuration settings document for the server which you want to configure for mail journaling.
 - From the Administrator open the server on which you want to set up mail journaling.
 - Go to the Configuration tab and click Messaging -> Messaging Settings -> Advanced -> Journaling.
6. Put the Message Settings document in edit mode and click the Journaling tab. Modify the following fields:
- Journaling: Enabled.
 - Method: Send to mail-in database.
 - Mail Destination: The Mail-in name specified in the mail-in database document (Mail Journal in our example).

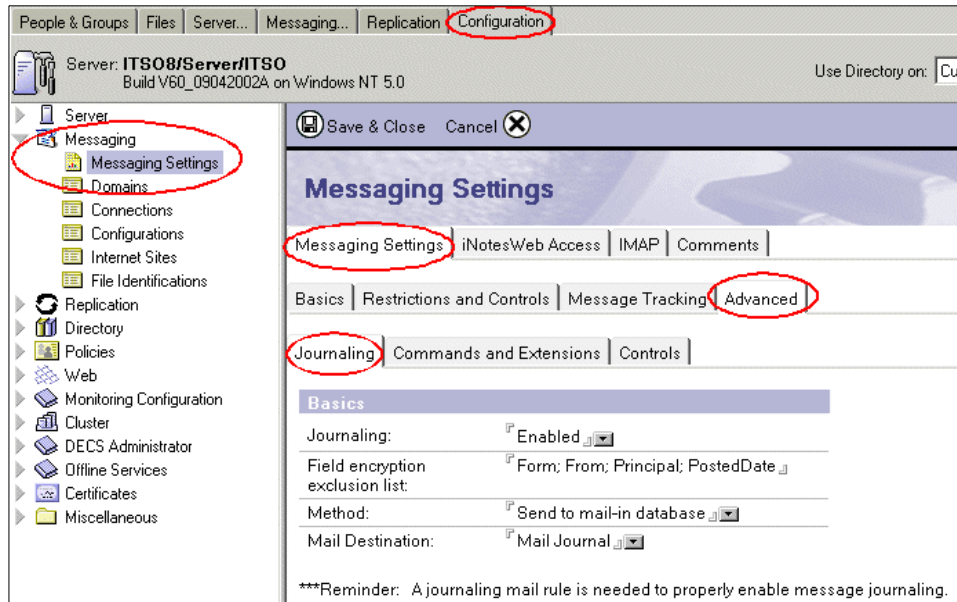


Figure 9-14 Configuration settings for mail journaling

7. From the server console tell the router to update its configuration:

```
tell router update config
```

8. Test the configuration:

- a. Verify that the rule is capturing the correct messages.
- b. Verify that the router is encrypting the messages with the correct notes certificate.

Best practices for mail journaling configuration

Unless there is a legal requirement to save every piece of mail going through your e-mail system, you should use this feature sparingly. You are basically doubling the amount of mail going through your system if you enable this for every user. This is overhead that you probably don't need and it also poses a security risk since someone could conceivably have access to every piece of mail your organization has ever received or produced.

Use a special ID to encrypt the mail journaling database. This can be done with either kind of configuration for mail journaling (local or remote). When you create this ID assign multiple passwords to it so that no one person can read messages in the mail journal database. This ID should not be readily available to users or administrators. Organizational policy should require a high level of management to "unlock" the messages in the mail journaling database.

9.1.3 Using the router for quota management

Users tend to save as much mail as possible, not realizing that this can cause problems. In some cases they don't even realize that they have saved it (for example, sent mail). It is a good idea to limit the size of mail files through quotas.

This section describes how to use the router quota controls to enforce quotas. When a mail file is over the quota you can configure the router to deliver a warning message, deliver the mail anyway but with a warning, hold the mail, or delete the mail and send a non-delivery report to the sender.

You can also configure the router to calculate how much space the messages are consuming instead of only looking at the raw file size. Users will appreciate the fact that once they delete messages there will be room in their mail files immediately for new messages (instead of having to run compact).

There are two kinds of quotas that you can set on a mail file: an absolute quota and a warning threshold. An absolute quota sets the maximum file size for a database. The warning threshold quota is typically set to 5 or 10 MB smaller than the absolute quota. It triggers a warning to the user that they are approaching the absolute quota. The quotas can be set on a mail file at the time of user registration or they can be configured manually at a later time (see Admin help for how to set a quota on a db).

Configure quota management on the router

1. In the Administrator, click the Configuration tab. In the left navigation panel expand the Messaging section and click the Messaging Settings document.
2. Click the Edit Message Settings button to put the Messaging Settings document in edit mode. Navigate through the tabs: Messaging Settings -> Restrictions and Controls -> Delivery Controls -> Quota Controls section.

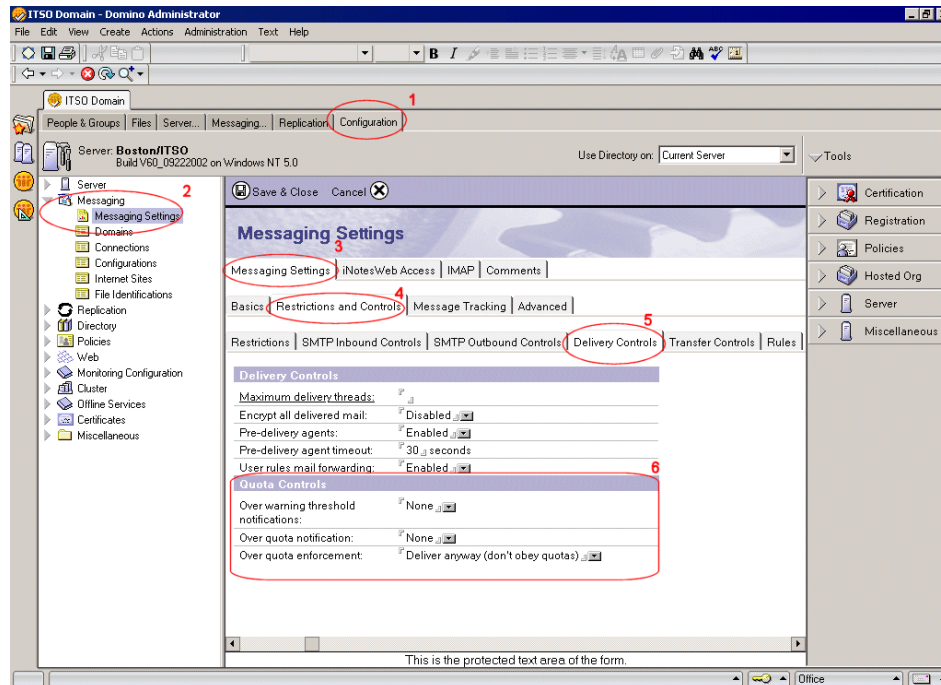


Figure 9-15 Navigate to Quota controls

- There are three fields that you can configure here. “Over warning threshold” and “Over quota notification” have the same options. For each one you can configure the router to not warn the user, warn the user every time it delivers a message, or send a message at a regular time interval. For example, you can configure the system to send the user a warning message every seven days that they are over the warning threshold level, but under the absolute quota level. Then, when they go over the absolute quota level you can configure the system to send them a message every day.

Quota Controls	
Over warning threshold notifications:	<input type="text" value="Per time interval"/>
Warning interval:	<input type="text" value="7"/> Day(s)
Over quota notification:	<input type="text" value="Per time interval"/>
Error interval:	<input type="text" value="1"/> Day(s)
Over quota enforcement:	<input type="text" value="Deliver anyway (don't obey quotas)"/>

Figure 9-16 Quota and Threshold notification options

4. The third field allows you to choose between ignoring the quota, not delivering the message and notifying the sender, or holding the mail and retrying delivery at another time. The default is “Delivery anyway (don’t obey quota).”

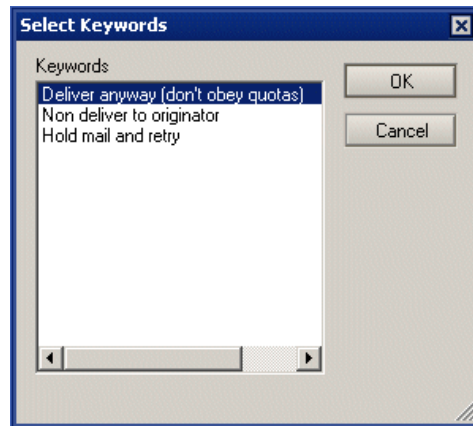


Figure 9-17 Delivery options for over quota mail

5. If you choose to have the router hold the mail and retry delivery, you have other options to configure:

Quota Controls	
Over warning threshold notifications:	<input type="checkbox"/> Per time interval <input type="button" value="v"/>
Warning interval:	<input type="checkbox"/> 7 <input type="button" value="d"/> Day(s) <input type="button" value="v"/>
Over quota notification:	<input type="checkbox"/> Per time interval <input type="button" value="v"/>
Error interval:	<input type="checkbox"/> 1 <input type="button" value="d"/> Day(s) <input type="button" value="v"/>
Over quota enforcement:	<input type="checkbox"/> Hold mail and retry <input type="button" value="v"/>
Attempt delivery of each message:	<input type="checkbox"/> Disabled <input type="button" value="v"/>
Maximum number of messages to hold per user:	<input type="checkbox"/> 500 <input type="button" value="d"/>
Maximum message size to hold:	<input type="checkbox"/> 5000 <input type="button" value="d"/> KB

Figure 9-18 Delivery options for held mail

6. If “Attempt delivery of each message” is enabled, the router will attempt to delivery each message as it arrives. Messages which are small may be delivered if they do not cause the database to exceed its quota.

Note: Enabling the router to deliver smaller messages to databases which are close to their quota limits may cause mail to be delivered out of order.

7. Set the maximum number of messages that the router will leave in mail.box for any one user while it is waiting for the database to conform to the quota.
8. Set the maximum cumulative size of messages the router will leave in mail.box while it is waiting for the database to conform to the quota. Once the messages have gone over that limit non-delivery reports will be sent to the senders of new messages and those messages will not be delivered.

Calculate database size by usage instead of file size

You can enable the router to determine whether a database has exceeded its quota based on the usage instead of the actual file size. The benefit of this is that you do not have to run compact in order for the mail files to remain in compliance with the quota. When a user deletes mail messages they immediately see the effect on their compliance with the quota, rather than having to wait until their mail file is compacted. Because users cannot compact their mail files on a server that is using transactional logging, you should enable quota enforcement with “Check space used in file when adding a note” selected.

Important: Your server and mail files must be at Notes/Domino 6 design levels to take advantage of this setting. It requires both the new design and ODS 43.

1. Navigate to the transactional logging tab of the server document.

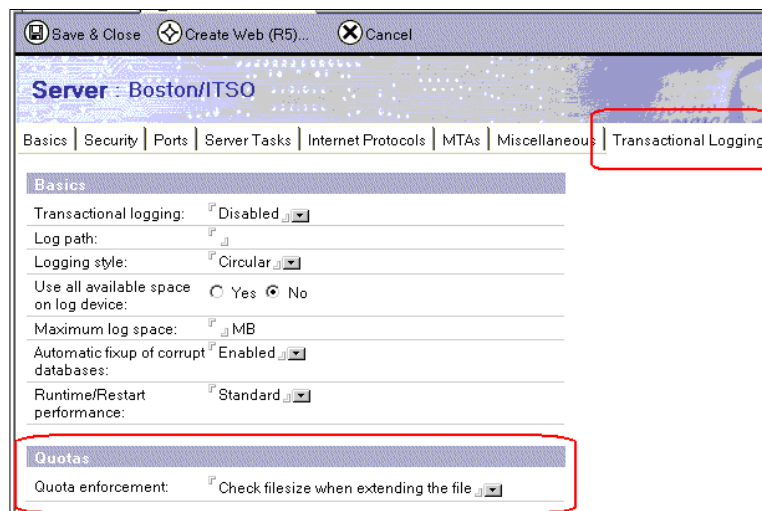


Figure 9-19 Quota enforcement on Transactional Logging tab

2. Select “Check space used in file when adding a note.”

Note: You do not have to have transactional logging turned on for this to work. If you do have transactional logging turned on you should configure the quota enforcement to check the space used in a file when adding a note. If you do not, administrative intervention will be required to get mail files back into compliance with quotas (users cannot compact databases on a server that has transactional logging enabled).

Important: When soft deletions are enabled for a mail file, deleting messages from a mail file doesn't immediately reduce its size. The "deleted" messages are moved to the Trash view until they expire (default setting is 48 hours). To reclaim space immediately, a user must open the Trash view and click Empty Trash or select messages in the view and click Delete.

9.2 Controlling automatic forwarding

Users are now able to set up a mail rule that will automatically forward their e-mail to another individual or an internet address. They do this through the Rule configuration utility in their mail file.

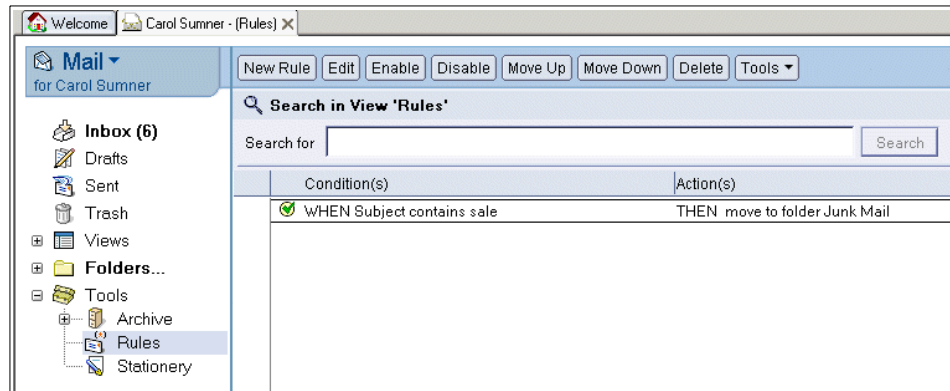


Figure 9-20 Rule utility in the client

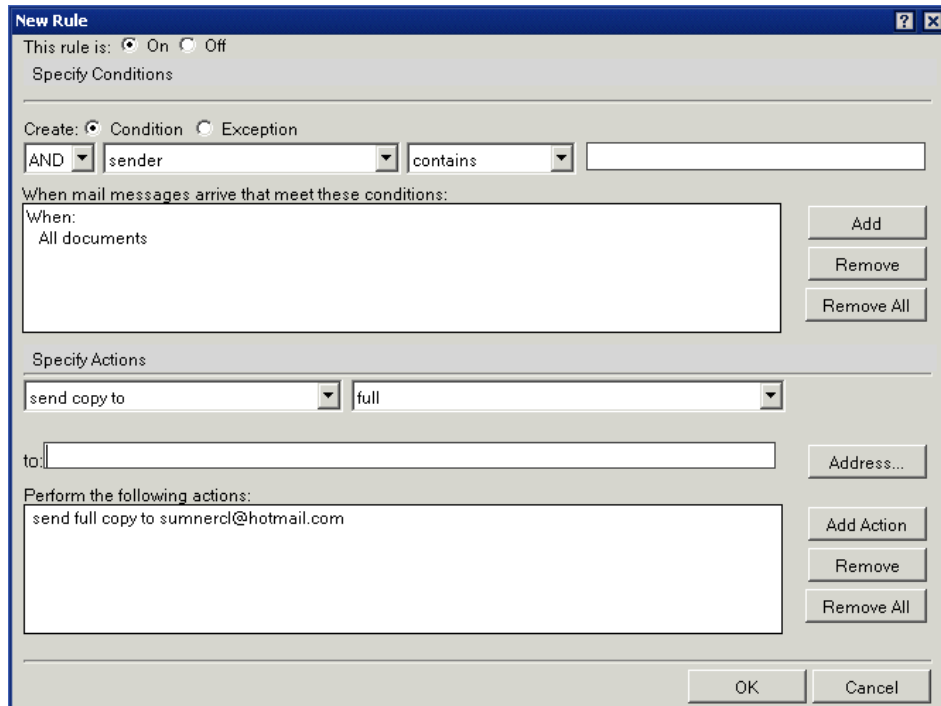


Figure 9-21 Rule that automatically forwards e-mail to an internet account

For security reasons an organization may not want their users to have this capability. An administrator can disable this capability at the server level by configuring the Delivery Controls for the router. By default users are able to run this rule.

1. In Domino Administrator change to the server on which you want to disable the users' capability to forward mail automatically. Click the Configuration tab.
2. In the navigation panel expand the messaging section and click Messaging Settings. This will open the messaging settings document.

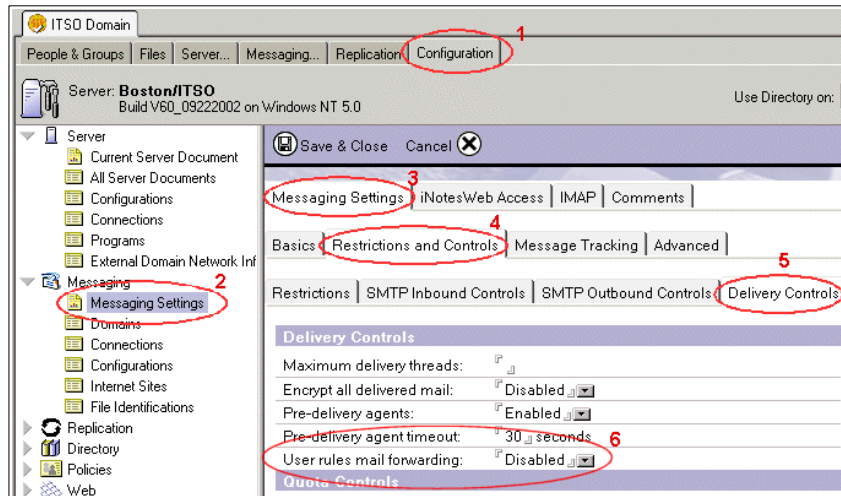


Figure 9-22 Disable automatic forwarding at the server level

3. In the Messaging settings document click the following tabs: Messaging Settings -> Restrictions and Controls -> Delivery Controls.
4. In the Delivery Controls section of the document change the setting for “User rules mail forwarding” from Enabled to Disabled.
5. Click Save & Close. The router will automatically update its configuration within a few minutes. You can also issue the command **te11 router update config** at the server console if you want the setting to take effect immediately.

9.3 SMTP settings

The SMTP settings in Server Configuration Settings documents are your key to a secure and effective Internet mail service. Three new sections have been added in Domino 6. The other fields have not changed between R5 and Domino 6. However, it is always a good idea to check all of the settings in these documents because they are often not well understood or implemented.

Domino servers running the SMTP Listener task need to be properly configured to avoid annoyance to your users and sometimes public embarrassment. A properly configured Domino server will:

- Reject e-mails with spoofed sender addresses. Anyone with a POP3 client can set his return address to any value—for example, `president@whitehouse.gov`. If your server does not limit from which servers it accepts incoming messages, your server can transfer messages that will cause embarrassment.

- ▶ Reject relaying of unsolicited and often offensive e-mail, usually called spam. A new heading on the SMTP Inbound Controls tab, inbound Relay Enforcement, further refines R5 capabilities for preventing relaying.
- ▶ Reject spam mail addressed to your users. Incoming SPAM is restricted by enabling DNS Blacklist support and by configuring the new Rules tab.

The following section, from Administrator 6 Help, explains how the SMTP controls work to protect your server and your users. Only the SMTP Inbound controls are listed because most of your security risk is with messages coming in from the Internet.

Many of the fields are new to Domino 6. The fields that have remained the same as in R5 are also included, because sometimes the wording is a little different. Even when the functionality is the same, the instructions have been rewritten to make them more understandable. We recommend you use the upgrade to Domino 6 as an opportunity to review all of your SMTP settings.

All of these fields are located on the configuration documents for your servers. With the Domino Administrator, click the Configuration tab, expand the Server section, click the Configurations view, select the server you want to configure, and click the Edit Configuration button in the action bar.

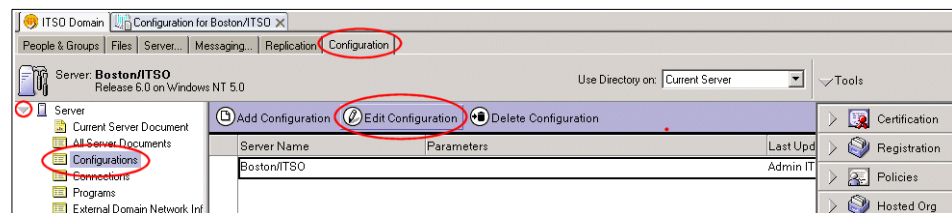


Figure 9-23 Navigate to Configuration document with Domino Administrator

Once the document is open click the Router/SMTP tab, then click the Restrictions and Controls tab. There you will find the tabs named SMTP Inbound Controls and SMTP Outbound Controls.

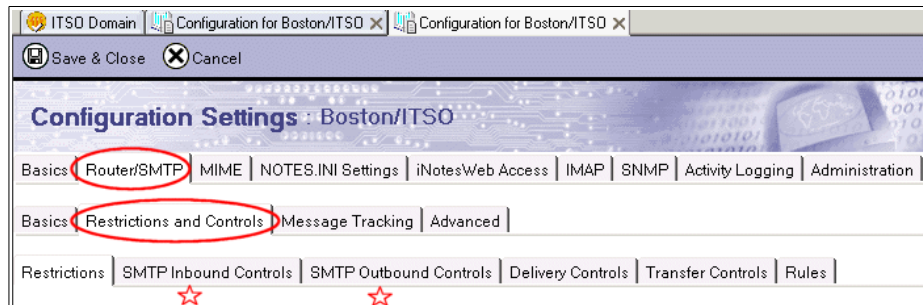


Figure 9-24 SMTP Controls

9.3.1 SMTP inbound controls

The SMTP Inbound Controls tab configures your inbound Internet mail settings. Most of your security risk is with messages coming in from the Internet. If a Domino SMTP server is accessible from the Internet, people outside your organization can relay mail through it to destinations in external Internet domains. This may result not only in one of your servers being burdened with extra traffic, but also in mail appearing to originate in your domain, possibly even spam. To prevent the Domino server from providing an open relay, Lotus Domino 5 introduced relay controls. Using Allow and Deny destination lists, these controls determine the relay destinations to which a server can or cannot send mail and the sources from which the server can and cannot accept relays.

Important: Because you configure the valid relay destinations separately from the valid relay sources, conflicts between the two sets of restrictions can occur. When such conflicts occur, Lotus Domino requires instructions for resolving the conflict. In Lotus Domino 5, Deny entries took precedence over Allow entries; in Lotus Domino 6, Allow entries take precedence over Deny entries.

Inbound relay controls

This section controls how Domino will handle requests to transfer mail from one external internet domain (a source) to another (a destination). This is called mail relay. There are four fields to configure. Two deal with destination domains and two deal with the hosts that make relay requests (sources). It is best to think of these fields as pairs, which together create a configuration:

“Allow messages to be sent only to the following external internet domains”
combines with

“Deny messages to be sent to the following external internet domains”
to create the allowed relay destinations configuration.

“Allow messages only from the following internet hosts to be sent to external internet domains”
 combines with
 “Deny messages from the following internet hosts to be sent to external internet domains”
 to create the allowed relay sources configuration.

Inbound Relay Controls	
Allow messages to be sent only to the following external internet domains:	<input type="checkbox"/>
Deny messages to be sent to the following external internet domains: (* means all)	<input checked="" type="checkbox"/> *
Allow messages only from the following internet hosts to be sent to external internet domains:	<input type="checkbox"/>
Deny messages from the following internet hosts to be sent to external internet domains: (* means all)	<input type="checkbox"/>

Figure 9-25 Default Inbound Relay Controls

Destination restrictions

Valid entries include internet domain names (such as lotus.com) and Domino domains (such as AcmeEast).

Hosts which end in the domain entered here are considered a match. For example, if you enter lotus.com and a destination named abc.lotus.com is requested, it will be subject to all the restrictions for lotus.com.

To name a domain explicitly, prefix an @ sign to the entry. If you enter @lotus.com, destinations like @abc.lotus.com are not considered a match.

Domino domains which can be relay destinations are entered with a percent sign (%) as a prefix.

Sample entries for these two fields:

```
lotus.com
@lotus.com
%AcmeEast
```

- ▶ Allow messages to be sent only to the following external internet domains:
 - Default is to allow transfer to all domains (blank).
 - If you enter a domain in this field, Domino will transfer messages *only* to this domain and to no others.

- ▶ Deny messages to be sent to the following external internet domains (* means all):
 - Default is all (*) - Domino will not allow relay of any messages from any external internet domain to another external internet domain.
 - Domino denies only messages destined for recipient addresses in the specified domains. All other messages may relay.

Note: Because the destination allow and deny lists can result in a conflict, Domino has a built-in rule that the deny restriction will take precedence over the allow restrictions. A destination appearing in both lists will not receive relayed mail through this server.

Tip: If you enter a domain in the Allow field remove the * from the Deny field. If there is a valid entry in the allow field only that domain will have mail relayed to it. All other domains will automatically be denied. If you leave the * in the Deny field no domains can have mail relayed to them, including the one you entered in the Allow field.

Source restrictions

These two fields determine which Internet servers will be allowed to relay mail through this Domino server. Valid entries include IP addresses and Internet domain names (for example lotus.com). IP addresses should be enclosed in brackets and may include * (asterisk) as a wildcard to represent subnets. Sample entries for these two fields:

lotus.com
[123.45.*]

Hosts which end in the domain entered here are considered a match. For example, if you enter lotus.com and a server named abc.lotus.com connects, it will be subject to all the restrictions for lotus.com.

- ▶ Allow messages only from the following internet hosts to be sent to external internet domains:
 - Domino allows only the entries in this field to relay outbound Internet mail.
 - If this field contains valid entries, Domino allows only servers matching these entries to relay. Message relays from other servers are denied.

- ▶ Deny messages from the following internet hosts to be sent to external internet domains (* means all):
 - Domino does not allow the entries in this field to relay outbound Internet mail.
 - If this field contains valid entries, Domino denies message relays from servers matching those entries and *allows* message relays from all other servers.
 - Default is blank, which means that all servers may relay messages.
 - * (asterisk) means do not allow any host to relay messages.

Note: Because the source allow and deny lists can result in a conflict, Domino has a built-in rule that the deny restrictions will take precedence over the allow restrictions. A host appearing in both lists will not be allowed to relay messages through this server.

Tip: If you enter a host name in the Allow field do not enter an * in the Deny field. An entry in the Allow field automatically limits relay to that one host and denies it to all others. If you leave the * all hosts will be denied relay privileges, including the host you entered in the Allow field, because the Deny configuration will take precedence.

Tip: If you enter any host in the Deny from field be sure to enter at least one host in the Allow from field. If you do not, Domino will deny the host entered in the Deny field and allow all others to attempt to relay.

Conflicts between the destination and source restrictions

Domino 6 handles the conflict that can occur between the destination and source fields differently than R5 did. In Lotus Domino 5, Deny entries took precedence over Allow entries; in Lotus Domino 6, Allow entries take precedence over Deny entries.

For example, you allow relays from the following host and deny them to the following domain:

Allow from hosts: 9.95.91.51
Deny to domains: yahoo.com

On a Domino 5 server, because the Deny entry takes precedence, the named host, 9.95.91.51, cannot relay to denied destinations. In the example, the Domino 5 server cannot relay to any address in the yahoo.com domain.

On a Domino 6 server, in the event of a conflict between entries, Allow entries takes precedence. By giving a specific host “Allow” access, you allow that host to relay to any destination. In the example, the host 9.95.91.51 can relay to the yahoo.com domain even though the domain is explicitly denied as a relay destination.

Similarly, the following configuration denies relays from a specified host and allows them to a specified domain:

```
Deny from hosts: myhost.iris.com
Allow to domains: hotmail.com
```

On a Domino 5 server, the Deny entry takes precedence, so that the named host, myhost.iris.com, is not a valid relay source. The named host cannot relay to any domain, even to allowed domains.

On a Domino 6 server, the Allow entry takes precedence. In the preceding example, myhost.iris.com is allowed to relay to hotmail.com, but not to any other destination.

Tip: When you upgrade the Domino 5 SMTP mail server, you have the option to not accept this change if you do not want to reconfigure your upgraded mail servers. Lotus Domino 6 provides the NOTES.INI setting SMTPRelayAllowHostsandDomains to allow the server to follow the Domino 5 behavior. Set this value to 1 to allow the Deny entries to take precedence. The default value for this setting is 0.

```
SMTPRelayAllowHostsandDomains=1
```

Table 9-1 Sample inbound relay configurations

Allow to	Deny to	Allow from	Deny from	Result of inbound relay setting
	*			No hosts will be allowed to relay mail through the Domino server
	*	abc.com		abc.com can relay to any destination. All other hosts will not be allowed to relay any mail
xyz.com			*	All hosts will be allowed to relay messages to xyz.com, but not to any other domain.

Table 9-2 Avoid these inbound relay configurations

Allow to	Deny to	Allow from	Deny from	Result of inbound relay setting
	xyz.com		abc.com	All hosts, except abc.com can relay mail to any destination. abc.com can relay to any destination, except xyz.com.
	xyz.com		*	All hosts can relay mail to any destination except xyz.com
	xyz.com	abc.com		All hosts can relay mail to any destination.
	*		abc.com	All hosts, except abc.com, can relay mail to any destination
xyz.com			abc.com	All hosts, except abc.com, can relay mail to any host. abc.com can relay mail to xyz.com

Inbound relay enforcement

The inbound relay enforcement section of the SMTP Inbound Controls tab configures whether the settings have been enabled, and if so for which connecting hosts.

Inbound Relay Enforcement	
Perform Anti-Relay enforcement for these connecting hosts:	<input checked="" type="checkbox"/> External hosts 
Exclude these connecting hosts from anti-relay checks:	<input type="checkbox"/> 
Exceptions for authenticated users:	<input checked="" type="checkbox"/> Allow all authenticated users to relay 

Figure 9-26 Inbound Relay Enforcement configuration

This section has 3 fields:

- Perform Anti-Relay enforcement for these connecting hosts:
By default the inbound relay controls are enabled for external hosts. If the connecting host's IP address resolves to a name in one of the local Internet domains, the host is considered internal. IP addresses that resolve to host names outside the local Internet domains, or that do not have DNS entries, are considered external. You can change this so that all or no hosts are subject to the inbound relay controls.

- ▶ Exclude these connecting hosts from anti-relay checks:
 - Enter IP addresses or host names of specific servers that should be able to relay messages through this server.
 - IP addresses are entered in brackets. Wildcards can be used to indicate all addresses in one subnet.
 - [156.16.25.1]
 - [156.16.25.*]
 - apps1.lotus.com
 - Set the previous field to “All connecting hosts” and enter IP addresses or host names of internal servers that are allowed to relay in order to prevent unauthorized use of your SMTP servers by internal departments.




Inbound Relay Enforcement	
Perform Anti-Relay enforcement for these connecting hosts:	<input checked="" type="checkbox"/> All connecting hosts 
Exclude these connecting hosts from anti-relay checks:	<input checked="" type="checkbox"/> apps1.lotus.com 
Exceptions for authenticated users:	<input checked="" type="checkbox"/> Allow all authenticated users to relay 

Figure 9-27 Sample relay enforcement configuration

- ▶ Exceptions for authenticated users:

This field provides an exception mechanism so that POP3 and IMAP users will be able to send internet e-mail through this server. Users will have to configure their client to connect to the SMTP server using a name and password. In Outlook Express this is found through the Account Properties tool, on the Servers tab.

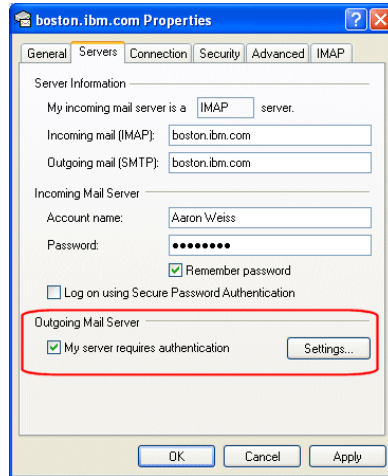


Figure 9-28 Outlook express SMTP configuration

Inbound connection controls

The inbound connection controls let you specify whether Domino checks the names of connecting hosts in DNS and which hosts will be allowed/denied connection.

If you create a separate Configuration Settings document for your internal SMTP servers, you can use the inbound connection controls to ensure that these internal servers accept SMTP connections from specific SMTP hosts only. For example, configure servers to allow SMTP connections only from servers that receive mail from the Internet. Restricting connections in this way prevents users with POP3 or IMAP clients from sending mail through the server, helps you define valid outbound routing paths, and limits the load on the server.

Inbound Connection Controls	
Verify connecting hostname in DNS:	Disabled
Allow connections only from the following SMTP internet hostnames/IP addresses:	
Deny connections from the following SMTP internet hostnames/IP addresses:	

Figure 9-29 Inbound Connection Controls

- Verify connecting hostname in DNS:
 - The default is disabled.

- If enabled, Domino verifies the name of the connecting host by performing a reverse DNS lookup. Domino checks DNS for a PTR record (a reverse pointer record) that matches the IP address of the connecting host to a host name. If Domino cannot determine the name of the remote host because DNS is not available or no PTR record exists, it does not allow the host to transfer mail. Although Domino accepts the initial connection, later in the SMTP transaction it returns an error to the connecting host in response to the MAIL FROM command.

Note: Internet SMTP hosts are not required to have PTR entries in DNS. As a result, when this field is enabled, the SMTP task may reject connections from valid SMTP hosts.

- ▶ Allow connections only from the following SMTP internet hostnames/IP addresses:
 - Default is blank, which means allow all.
 - If you enter host names and/or IP addresses in this field, only servers matching these entries can connect to the SMTP listener; connection requests from all other servers are denied.
 - Enter IP addresses in brackets:
[192.68.10.17]
 - If a host name entry is complete, it specifies a particular server:
mailserver.abc.com
 - If a host name entry is partial, it implies a wildcard and all hosts in that domain will be allowed to connect through SMTP:
abc.com
- ▶ Deny connections from the following SMTP internet hostnames/IP addresses:
 - If you enter host names and/or IP addresses in this field, all servers *except* those matching entries in this field can connect to the SMTP listener; connection requests are denied only for servers matching the entries in this field.
 - Enter IP addresses in brackets:
[192.168.10.17]
 - Enter fully qualified host names:
mailserver.abc.com
 - Enter partial names, indicating that no servers in that domain should be allowed to connect:
.abc.com

Tip: Using name entries may inadvertently block mail from other unrelated domains. For example, in the previous example, entering `abc.com` also prevents connections from `mailhost.xyzabc.com`. To apply restrictions to hosts in a specified domain and its subdomains only, enter a leading dot (`.`) as in the immediately preceding example.

Inbound sender controls

To save system resources, before it accepts a message, the Domino SMTP listener checks the Mail From address specified in the message envelope during the SMTP transaction. If you set the Domino server to deny mail from a particular source, Domino denies it whenever that source is encountered—for example, if users from a denied domain send mail through a relay, Domino denies it based on its origin from that domain. Domino creates an entry in the log file (LOG.NSF) whenever a message is rejected.

Inbound Sender Controls	
Verify sender's domain in DNS:	<input type="checkbox"/> Disabled 
Allow messages only from the following external internet addresses/domains:	<input type="checkbox"/>
Deny messages from the following internet addresses/domains:	<input type="checkbox"/>

Figure 9-30 Inbound Sender Controls

- ▶ Verify sender's domain in DNS:
 - Default is disabled.
 - Enabled - Domino verifies that the sender's domain exists by checking the DNS for an MX, CNAME, or a record that matches the domain part of the address in the MAIL FROM command received from the sending host. If no match is found, Domino rejects inbound mail from the host.
- ▶ Allow messages only from the following external internet addresses/domains:
 - Default is blank, meaning all are allowed.
 - If you enter addresses in this field, only messages with senders matching those addresses can send Internet mail to users in your local Internet domain. Mail from all other addresses is denied. For example, if you enter `lotus.com` in the field, Domino accepts incoming mail only if the address in the MAIL FROM command ends in `lotus.com`. Domino denies messages from all other Internet addresses.

- Deny messages from the following internet addresses/domains:
 - Default is blank, meaning all are allowed.
 - If you enter addresses in this field, all messages except those matching addresses listed in this field can route to your users. Mail is denied only from addresses matching the entries in this field. For example, if you enter lotus.com in the field, Domino accepts messages from all Internet addresses and domains except those ending in lotus.com. Domino denies messages from senders whose addresses end in lotus.com.

Tip: For both the Allow and Deny fields you can create a Notes group containing a list of addresses from which to allow messages and enter the group name in this field. A group entry is valid only if it does not contain a domain part or dot (.). For example, the group with the name group1 is valid, but the groups named iris.com or group2@iris are not.

Inbound intended recipients controls

Inbound Intended Recipients Controls allows you to configure the Domino SMTP listener to check the RCPT TO address specified in the message envelope during the SMTP transaction. If enabled it will match the recipients to the allow and deny fields and take the appropriate action.

Inbound Intended Recipients Controls	
Verify that local domain recipients exist in the Domino Directory:	<input type="checkbox"/> Disabled
Allow messages intended only for the following internet addresses:	<input type="checkbox"/>
Deny messages intended for the following internet addresses:	<input type="checkbox"/>

Figure 9-31 Inbound intended recipients controls

- Verify that local domain recipients exist in the Domino Directory:
 - Default is disabled.
 - When enabled, if the domain part of an address specified in an SMTP RCPT TO command matches one of the configured local Internet domains, the SMTP listener checks all configured directories to determine whether the specified recipient is a valid user. If all lookups complete successfully and no matching username is found, the SMTP server returns a 550 permanent failure response indicating that the user is unknown.

- Enabling this option can help prevent messages sent to nonexistent users (for example, spam messages and messages intended for users who have left the organization) from accumulating in MAIL.BOX as dead mail.

Note: When this setting is enabled, the server cannot relay mail to a smart host, because Domino rejects messages addressed to local domain recipients who are not listed in the Domino Directory.

- ▶ Allow messages intended only for the following internet addresses:
 - If you enter addresses in this field, only those recipients can receive Internet mail. Domino denies mail for all other recipients.
- ▶ Deny messages intended for the following internet addresses:
 - If you enter addresses in this field, all addresses except those listed in this field can receive Internet mail. Domino denies mail for only the addresses in this field.

Tip: If the server supports Local Part name lookups, users whose addresses are listed in the Deny field may still receive mail addressed to alternate Internet addresses. To prevent use of alternate addresses, complete the Internet address field in each user's Person document and allow users to receive inbound mail destined for their fullname addresses only. Refer to "Specifying how Domino looks up users in the Domino Directory" in the Admin Help file for information on restricting name lookups.

DNS Blacklist filters

In R5, to protect your users from receiving unwanted and often offensive e-mail (usually called spam), you had to enter the addresses of known senders. This approach does not work very well because the worst spam sites constantly change their addresses. Domino 6 supports the new DNS Blacklist feature. You can set up Domino to check whether incoming SMTP connections originate from servers listed in one or more DNS Blacklists (DNSBLs). DNSBLs are databases that keep a record of Internet SMTP hosts that are known sources of spam or permit third-party, open relaying.

When DNS Blacklist filters are enabled, for each incoming SMTP connection Domino performs a DNS query against the blacklists at the specified sites. If a connecting host is found on the list, Domino reports the event in a console message and in an entry to the Mail Routing Events view of the Notes Log. Both the console message and log entry provide the host name and IP address of the server, and the name of the site where the server was listed.

In addition to logging the event, you can configure Domino to reject messages from hosts on the blacklist or to add a special Notes item to flag messages accepted from hosts on the list.





DNS Blacklist Filters	
DNS Blacklist filters:	<input checked="" type="checkbox"/> Enabled 
DNS Blacklist sites:	<input type="checkbox"/> 
Desired action when a connecting host is found in a DNS Blacklist:	<input checked="" type="checkbox"/> Log only 
Custom SMTP error response for rejected messages:	<input type="checkbox"/> 

Figure 9-32 DNS Blacklist filter settings

- ▶ DNS Blacklist filters:
 - Default is Disabled. Once you select enabled for the DNS Blacklist filters field the other DNS blacklist settings appear.
- ▶ DNS Blacklist sites:
 - After you enable the DNS Blacklist filters, you can specify the site or sites the SMTP task uses to determine if a connecting host is a “known” open relay or spam source. Specify sites that support IP-based DNS Blacklist queries.
 - If Domino finds a match for a connecting host in one of the Blacklists, it does not continue checking the lists for the other configured sites.
 - Specify sites that support IP-based blacklist queries.

Important: Domino uses IP version 4 (IPv4) addresses when querying DNS blacklist sites to find out if a connecting host is listed. If the connecting host has an IP version 6 (IPv6) address, Domino skips the DNSBL check for that host.

- For performance reasons, it's best to limit the number of sites, because Domino performs a DNS lookup to each site for each connection.

A number of public and subscription services on the Internet maintain DNS Blacklists, and each has its own criteria for adding servers to its list. Blacklist sites use automated tests and other methods to confirm whether a suspected server is sending out spam or acting as an open relay. More restrictive Blacklist sites add servers to their list as soon as they fail the automated tests, and regardless of whether the server is verified as a source of spam. Other less restrictive sites list a server only if its

administrator fails to close the server to third-party relaying after a specified grace period or if the server plays host to known spammers.

► Desired action when a connecting host is found in a DNS blacklist:

– Default is Log only.

– Options are:

- Log only

The server records the following information in the Notes log: the host's IP address and host name (if a reverse DNS lookup can determine this information) and the name of the site that listed the host.

- Log and tag message

In addition to logging as above, Domino adds a special Note item to messages received from hosts found on a blacklist. After Domino determines that a connecting host is on the blacklist, it adds the Note item, `$DNSBLSite`, to each message it accepts from the host before depositing the message in MAIL.BOX.

The value of a `$DNSBLSite` item is the blacklist site in which the host was found. Administrators can use the `$DNSBLSite` note item to provide custom handling of messages received from hosts listed in a blacklist. For example, you can test for the presence of the item through the use of formula language in an agent or view and provide conditional handling of messages that contain the item, such as moving the messages to a special database.

- Log and reject message

The server records the following information in the Notes log: the host's IP address and host name (if a reverse DNS lookup can determine this information) and the name of the site that listed the host. It then rejects the message so that it never enters the messaging environment.

Use restraint when taking action, particularly if you use the blacklist of a more restrictive site. The action you select applies to each of the specified blacklist sites. That is, you cannot configure Domino to deny connections for hosts found on one site's list and log the event only for hosts found on another site's list.

► Custom SMTP error response for rejected messages:

The default error message indicates that the connection was denied for policy reasons. You can customize the message to return more information to the host.

You can use the format specifier "%s" to specify the IP address of the denied host and the DNS blacklist site where Domino found the host listed. For example, if you enter the following:

Your host %s was found in the DNS Blacklist at %s

Domino replaces the first instance of "%s" with the IP address of the host, and the second instance with the DNS blacklist site name. Thus, if you entered the text in the preceding example, a denied host receives an error such as:

Your host 127.0.0.2 was found in the DNS Blacklist at
blackholes.mail-abuse.org

Hosts that are exempt from DNS Blacklist checks

To avoid unnecessary DNS lookups, Domino performs DNS Blacklist checks only on hosts that are subject to relay checks, as specified in the SMTP inbound relay restrictions. Any host that is authorized to relay is exempt from Blacklist checks. For example, by default, Domino enforces the inbound relay restrictions only for external hosts (Router/SMTP -> Restrictions and Controls -> SMTP Inbound Controls -> Perform Anti-Relay enforcement for these connecting hosts). If the default setting is used, internal hosts are not subject to relay controls, and thus are also exempt from Blacklist checks. For more information on configuring relay enforcement, refer to "Inbound relay controls" on page 231.

DNS Blacklist statistics

The SMTP task maintains statistics that track the total number of connecting hosts that were found on the combined DNSBL of all sites combined, as well as how many were found on the DNSBL of each configured site. Since the statistics are maintained by the SMTP task, they are cumulative for the life of the task only and are lost when the task stops.

You can view the statistics from the Domino Administrator or by using the SHOW STAT SMTP command from the server console. You can further expand the statistics to learn the number of times a given IP address is found on one of the configured DNSBLs. To collect the expanded information, set the variable SMTPExpand DNSBLStats in the NOTES.INI file on the server. Because of the large numbers generated by the expanded set of statistics, Domino does not record the expanded statistics by default.

9.4 Automatic mail archiving

With Notes and Domino 6 the administrator has the possibility of setting up centralized server-side archiving or local client-side archiving. Centralized archiving is configured through archiving setting documents and applied through policies. You can also control how much access users have to the archive tool in their own client.

As the administrator you should decide how archiving will be handled in the organization. If you do not create an archiving settings document and apply it

through a policy, you are automatically enabling all end users to archive their mail files on their local workstations. The archive criteria settings are very flexible. You can set up almost any combination of source and destination databases for archiving. Keep in mind that your users will need Database Create rights to a server if you want them to use their workstations to archive their mail to a Domino server. If you configure archiving for the Domino mail server to perform the archiving, it will need database create rights on the destination server.

Table 9-3 User access requirements for archive configurations

Archive performed by	Archive destination	Access required by end user to destination server
Notes client	Local workstation	N/A
Notes client	Domino server (can be mail server or another server)	User must have the right to create databases on the destination server
Domino server	Domino server (can be mail server or another server)	Same as mail server access

9.4.1 Client-side archiving

If the administrator has not restricted access to the archive tool, users can set up archiving on their own workstations. The advantage to this is that they use their own CPUs for the archiving, they can configure the archiving in any way they want, and the user bears responsibility for the archives. The disadvantage is that there is no consistent method of archiving, which makes support more difficult, and there is no way to enforce a company-wide archive policy (for instance for legal reasons).

The archive profile is configured through the archive tool, which has received a face-lift in the Notes 6 client and provides for much more flexibility in its configuration.

Steps to set up client-side archiving

The tool is part of the mail file design. With the mail file open to the inbox, choose Tools from the action bar and then select Archive settings.

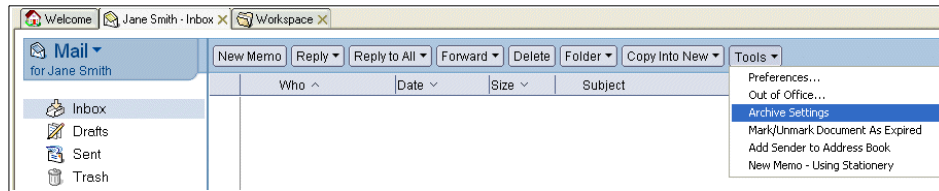


Figure 9-33 Navigate to archive settings in the client

In the archive settings tool there are 3 sections: Basics, Settings, and Advanced.

1. Click the Basics tab of the Archive settings tool. On the basics page you choose whether you want the archiving to be performed by the client or the server and whether the archive database will be located on the local client or on a Domino server.

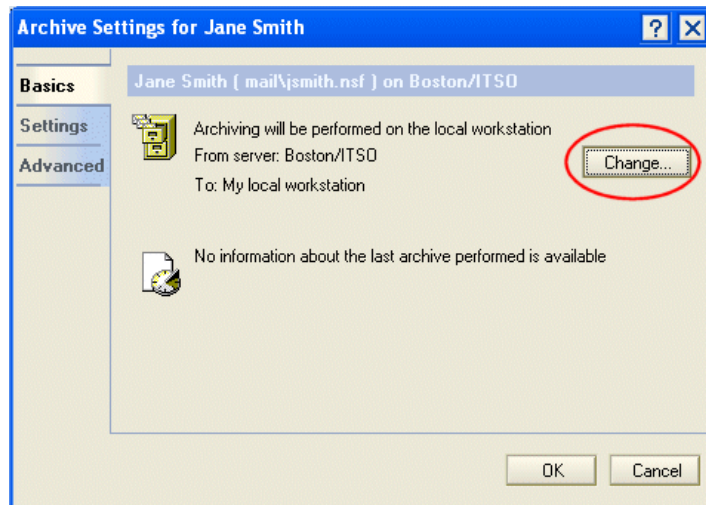


Figure 9-34 Basics default settings for client-side archiving

If your administrator has disabled local archiving you will see a warning on the basics page when you open your archive settings profile and the Change button will be grayed out.

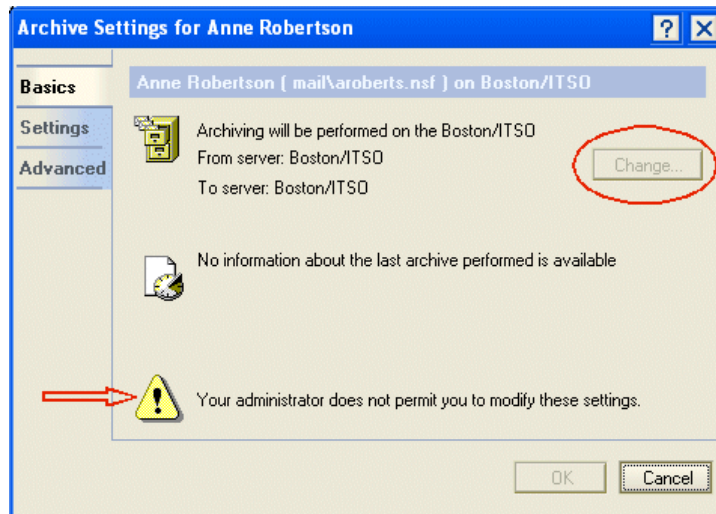


Figure 9-35 Warning on archive profile setting when client-side archiving has been disabled

2. Click the Change button and select the radio button, “On my local Notes client to.” Choose whether the resulting archive database will be on your local workstation or on the server by selecting the down arrow next to this field. Select a server *only* if you know that you have permission to create a database on the server. If you do not have sufficient rights on the server you will receive an error message when you try to archive. Check with your administrator about this. Click OK.

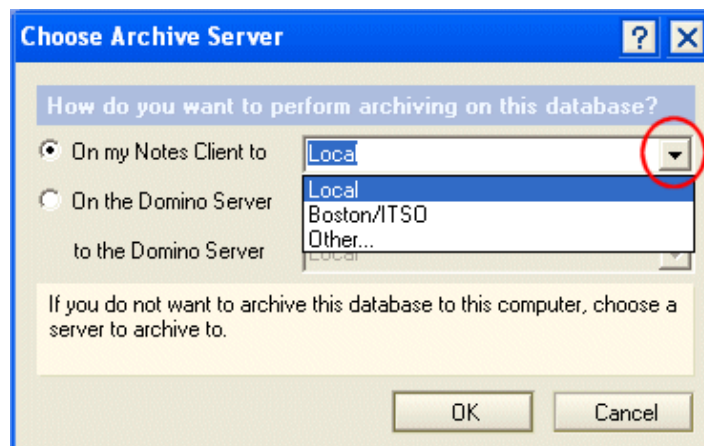


Figure 9-36 Choose Archive Server

Note: Once you configure the archive basics settings they apply to all of the archive criteria settings which you create. All of your archives will be handled in one of three ways:

- ▶ By your local client to your local workstation
- ▶ By your local client to a server
- ▶ By a Domino server to a Domino server

3. Configure the archive criteria:
 - a. Click the Settings tab of the archive settings tool.

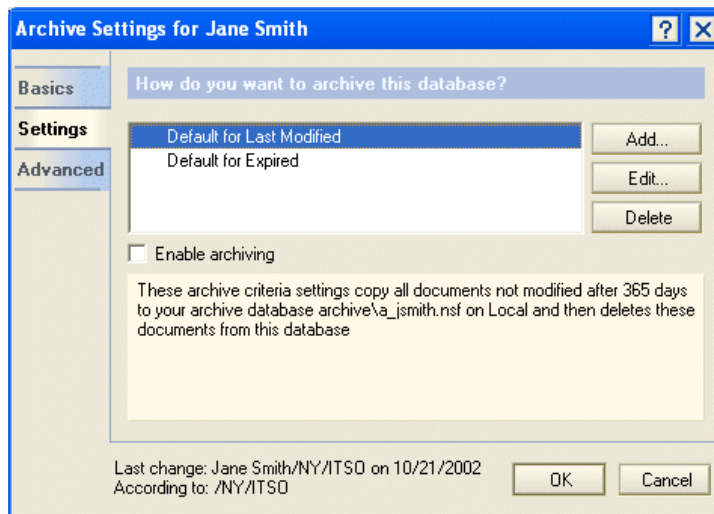


Figure 9-37 Settings tab

This section allows you to configure archive criteria. You can set up different criteria to archive messages into separate archive databases. There are two default pre-configured settings. Neither of these are enabled by default:

- Default for Last Modified -This criterion will archive any documents which have not been modified within the last 365 days.
 - Default for Exired - This criterion will archive any documents which have an expiration date more than 5 days old.
- b. Select the criterion you want to work with and click the Edit button, or create a new set of criteria by clicking the New button.

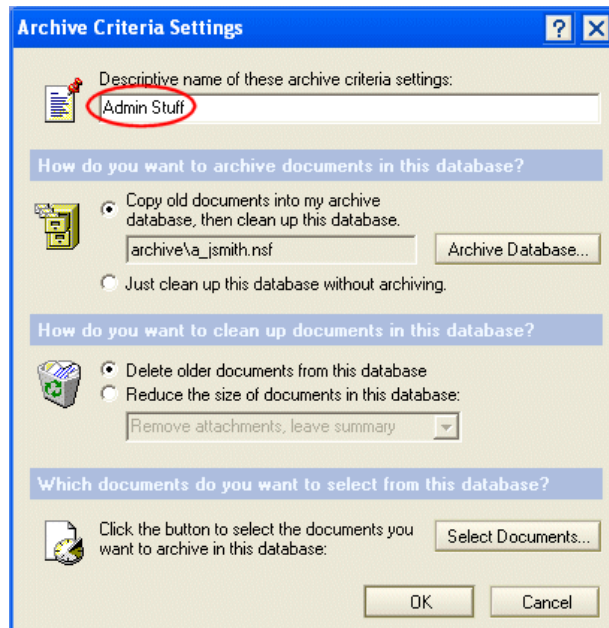


Figure 9-38 Archive criteria settings

- Give a descriptive name to this criteria set if it is new. This is the name which will appear under the Tools section of the navigation pane in the mail file.

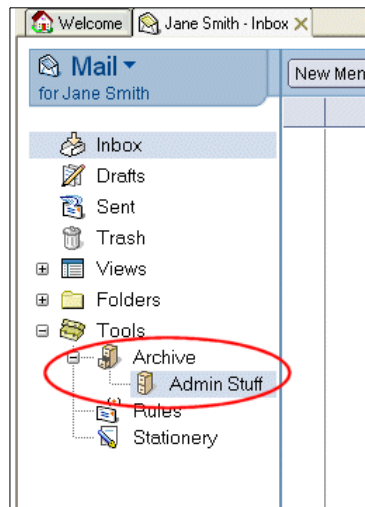


Figure 9-39 Name of archive criterion set as it appears in the mail file

- Choose whether you want to copy old documents into the archive database or just clean up the current database (see later steps for the methods used to clean up a database). If you want to change the archive database for this set of criteria click the Archive Database button.

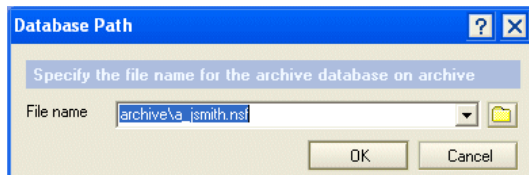


Figure 9-40 Database path for archive database

Tip: To create a new archive database change the file name in the Database Path dialog box to a filename which does not currently exist. The client will create the archive database the next time it uses this criteria set to archive messages from the mail database.

- Choose whether older documents should be deleted or reduced in size.
- Click the Select Documents button to configure which documents this criteria settings profile will affect. Archive settings criteria will affect documents which are marked as expired or have not been modified. Both settings use time stamps to determine document eligibility for archiving. By default the criteria will affect all documents in the mail file.

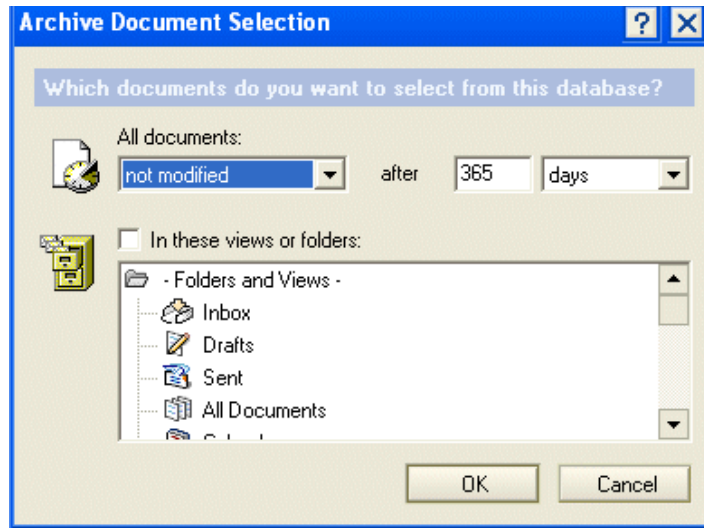


Figure 9-41 Archive document selection

You can narrow down the document selection by clicking the checkbox, “In these views or folders” and selecting one or more items in the list.

- Click OK to close the Archive Criteria Settings dialog box. This will bring you back to the main screen of the archive profile.

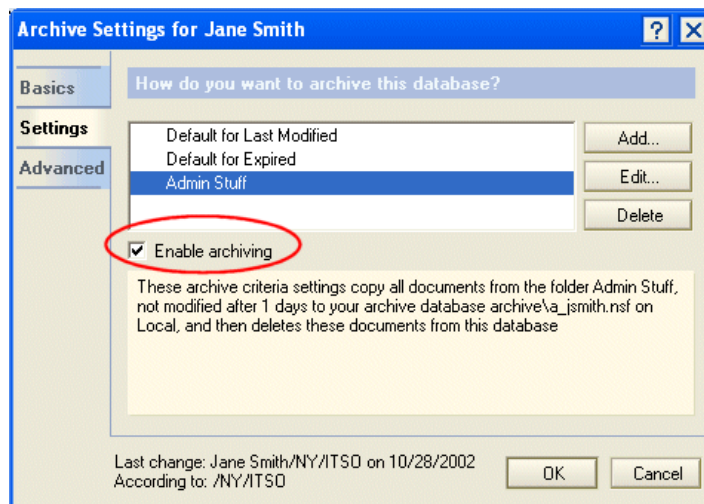


Figure 9-42 Enable archiving

- Select the archive settings which you just configured and then click the checkbox “Enable archiving”. Review the criteria in the box to make

sure that you are archiving the correct documents and using the appropriate method to do so.

4. Click the Advanced tab of the archive settings tool.

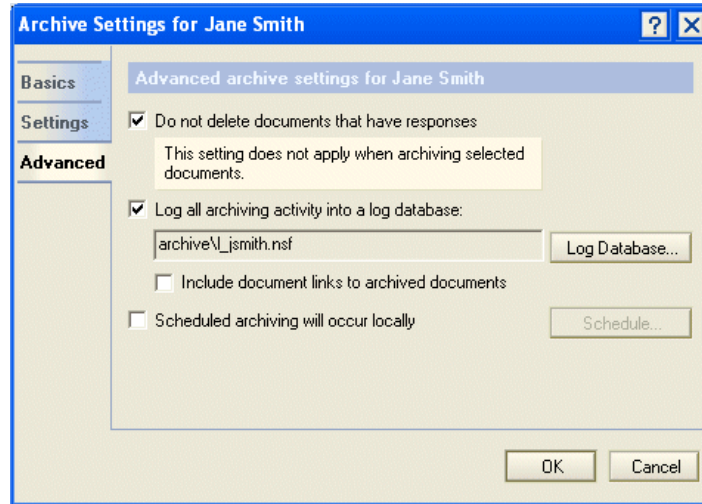


Figure 9-43 Advanced archive settings

- a. Configure whether the client will automatically archive documents whose responses do not meet the archive criteria (for example, a recent response to a message sent out a long time ago). This will help preserve message threads which you may need.
- b. Decide whether you want to log all the archive activity. You can also configure the profile to create a document link to every message which it archives.

Tip: If you're having trouble getting the archive feature to work, try deleting the archive log file. It holds information about the source and destination databases that must be accurate for the archive feature to work.

- c. You can schedule archiving so that it occurs automatically.

Note: The workstation must be on, the Notes 6 client loaded, and the correct person logged in for locally scheduled archiving to work properly.

- Click the Schedule button. Select the time, days, and Notes location that should be active at the time of archiving (default is any location).

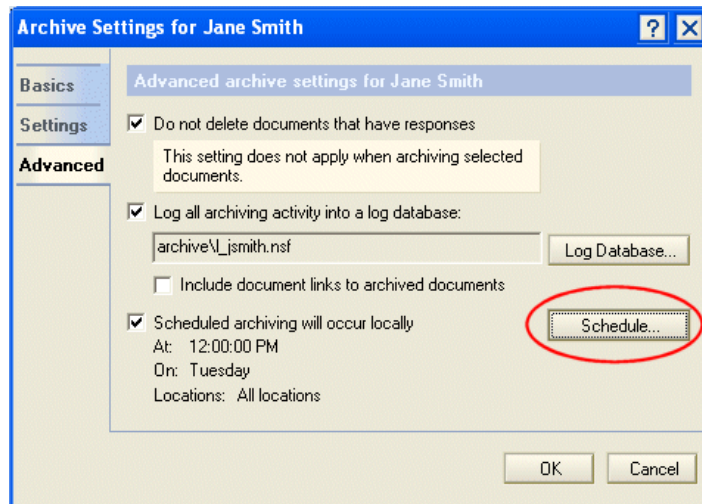


Figure 9-44 Schedule local archiving

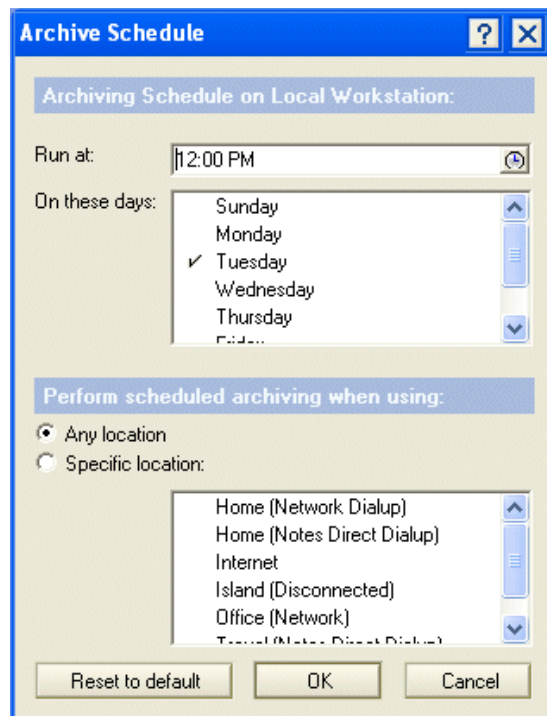


Figure 9-45 Set the archive schedule

9.4.2 Server-side archiving

Server-side archiving provides an easy way for administrators to create and enforce standard archive policies. Mail which is rarely accessed in active mail files can be transferred to dedicated archive servers. The administrator can also configure the utility to simply delete certain messages, for example, those from the Sent view. In this way the resources of the mail servers can be preserved for active mail use and users can still have access to their old mail.

Server-side archiving is configured through archiving settings documents which are applied through policies (see Chapter 15, “Policy-based administration” on page 449 for details on how to apply a policy). The criteria for archiving (which mail messages will be affected by the policy) are configured as a subset of the Archiving Settings document in Archive Criteria Settings documents (found on the Selection Criteria tab). An archiving settings document may contain many archive criteria settings documents.

You will need to think through exactly how the selection criteria will interact to make sure that one is not defeating another. For example, if you need to archive all the messages in a particular folder once they have not been accessed for 60 days, make sure that you don’t have another criterion deleting documents in the all documents view if they have not been accessed for 30 days.

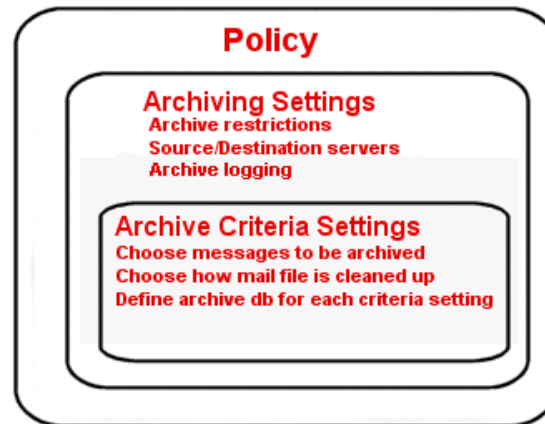


Figure 9-46 Layered control of archiving

Configure archiving setting documents

Make sure that you have Editor access to the Domino Directory and one of these roles:

- ▶ PolicyCreator role to create a settings document.
- ▶ PolicyModifier role to modify a settings document.

1. With the Domino administrator client select the People & Groups tab. Click the Settings view in the navigation panel. Click the Add Settings button and select Archiving from the drop-down list.

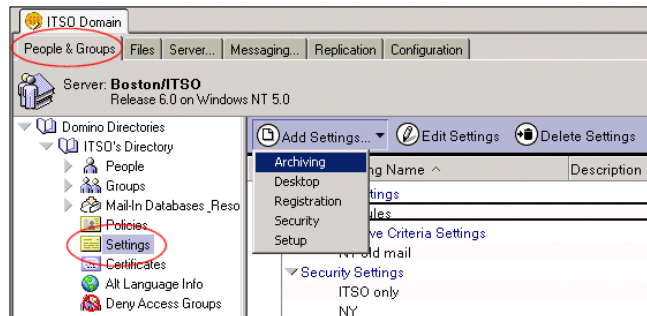


Figure 9-47 Navigate to Archiving settings

2. The Basics tab configures the general parameters for archiving, including user access to the archive tool in their client, the machine to perform the archiving, and the source and destination servers.
 - a. In the Basics section give the setting a name and description. The name should make the settings document easily identifiable, for example, named by OU or department.

ITSD Domain New Archiving Settings X

Save & Close Cancel Inheritance Enforcement

Archiving Settings

Basics | Selection Criteria | Logging | Schedule | Advanced | Comments | Administration

Basics

Name:

Description:

Archiving Options:	Inherit from parent policy:	Enforce in child policies:
<input type="checkbox"/> Prohibit archiving	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="checkbox"/> Prohibit private archiving criteria	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Archiving will be performed on:

☒ User's local workstation ☐ Inherit ☐ Enforce

☐ Server

Archiving source database is on:

Source Server:

☐ Local ☐ Inherit ☐ Enforce

☐ Specific server

☒ Mail server

Destination database is on:

Destination Server:

☒ Local ☐ Inherit ☐ Enforce

☐ Specific server

☐ Mail server

Figure 9-48 Basics tab of Archiving Settings document

b. (Optional) In the Archiving Options section, choose to limit the access your users have to the archiving tool in their client. Default is for the user to have complete access.

- Prohibit archiving - prevents both server-side and client-side archiving of a user's account

Prohibit private archiving criteria - prevents the user from changing the archive criteria. The user will see a warning when they open their archive settings.

If you choose this option and choose for archiving to be performed on the user's workstation, the user will be able to initiate archiving but will be limited to the criteria you configure on the Selection Criteria tab.

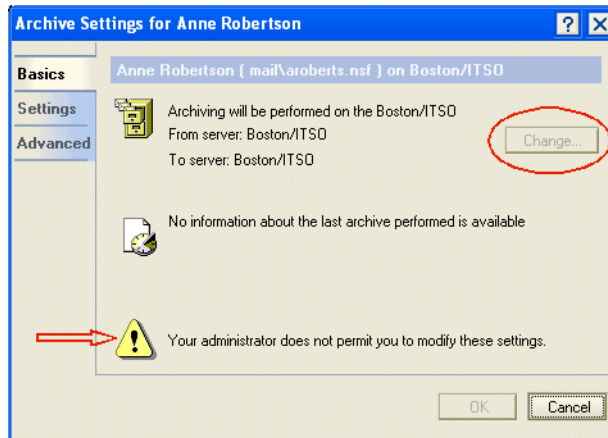


Figure 9-49 What the user sees when locked out of archive tool

- c. In the section, “Archiving will be performed on” configure whether the user’s workstation or a Domino server performs the archiving. The server on which the source database exists will perform the archiving.

Important: If you choose for a server to perform the archiving, you must configure a program document for that server to run compact with the -a switch.

- d. Configure the location of the source database:
 - If you have chosen for the archiving to be performed by a server the option for the source database to be on the local workstation disappears.
 - If you choose that the source database is located on a specific server you must specify a server in the Server information section at the bottom of the Basics tab. That server will then perform the archiving. This might be the case, for example, if you would prefer a cluster server to perform the archiving.
 - If you choose that the source database is located on the mail server the user’s mail server will do the archiving.

Tip: The source server matches the mail file owner name of the source database to names in the NAB and archives documents according to the policy assigned in the person document. If archiving is not working the way you think it should, check to make sure that the mail file owner name is correct in the source mail file.

- e. Configure the location of the destination database. In this section you choose on which server the resulting archive database will be created. It can be the mail server or another server. If you choose a server other than the mail server you must define that server in the Server information section at the bottom of the Basics tab.

Archiving Options:			Inherit from parent policy:	Enforce in child policies:
<input type="checkbox"/> Prohibit archiving	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
<input checked="" type="checkbox"/> Prohibit private archiving criteria	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
Archiving will be performed on:				
<input type="radio"/> User's local workstation	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
<input checked="" type="radio"/> Server				
Archiving source database is on:				
Source Server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
<input checked="" type="radio"/> Specific server				
<input type="radio"/> Mail server				
Destination database is on:				
Destination Server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
<input checked="" type="radio"/> Specific server				
<input type="radio"/> Mail server				
Server information:				
Choose source server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
NewYork/ITSO				
Choose destination server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce		
NewYork/ITSO				

Figure 9-50 Sample server-side settings document

- f. In Figure 9-50 you can see a sample of a server-side settings document. In this sample archiving will not take place on the user's mail server and the destination archive database will also not reside on the user's mail server. These settings have no effect until you create archive criteria settings on the Selection Criteria tab.
3. The Selection Criteria tab configures which documents will be affected when archiving is done and how they will be affected. This tab contains buttons which create or access archive criteria settings documents.

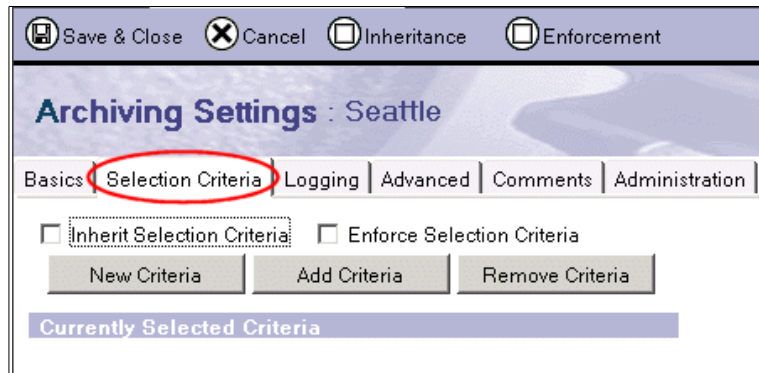


Figure 9-51 Selection criteria tab for archiving

- a. Click the New Criteria button to create a new Archive Criteria Settings document.

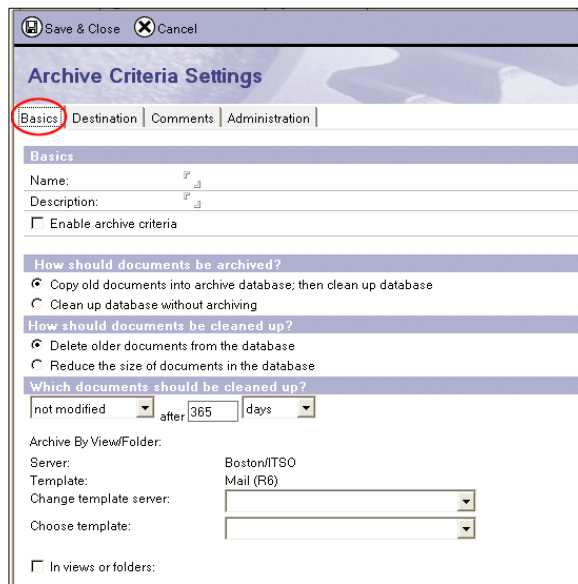


Figure 9-52 Basics tab of Archive Criteria Settings

- b. Make the following entries on the Basics tab:
 - Enter a name and descriptive text about the criteria. Entering descriptive text will make it much easier to reuse this criteria settings document in other archive settings documents.

Note: Archive criteria settings documents are not enabled by default. Don't forget to click the Enable archive criteria checkbox to enable the criteria. Remember that if you use this criteria set in more than one Archive Settings document, it will be enabled for all of them.

- Select whether you want the archive procedure to save copies of the documents or clean up the database without saving them. If you select that it should not save them the Destination tab disappears.
- Select whether the utility should delete the documents or just reduce their size. If you choose to reduce the size you must select whether attachments will be deleted only or attachments deleted and the text reduced to 40k.

Figure 9-53 Clean up configuration

- Configure which documents the archive utility should work on.

Figure 9-54 Choose the documents to be cleaned up

By default the archive utility will work on all the documents in the mail file. If you need to restrict the utility to particular folders or views, click the checkbox, “In views or folders.” Based on the template, the settings document will present all the possible views and folders. By default the views and folders of the mail (R6) template on the current server will be presented. You can choose another server/template combination if needed (for example, if you use a custom template).

Which documents should be cleaned up?

not modified after 60 days

Archive By View/Folder:

Server: Boston/ITSO

Template: Mail (R6)

Change template server:

Choose template:

☒ In views or folders:

☐ To Do ☐ Drafts ☒ Sent

☐ All Documents ☐ Inbox ☐ Trash

☐ Calendar ☐ Meetings

Figure 9-55 Narrow the selection criteria to a particular view or folder

- c. Click the Destination tab. Configure the destination database for this archive criteria set on this tab. Each set can have its own database. The utility will create an archive database using the configuration options on this tab.

Save & Close Cancel

Archive Criteria Settings : Seattle

Basics **Destination** Comments Administration

Path Information

Archive Directory: archive

Archive Prefix: sent

Archive Suffix:

Number of Characters from original filename: 12

[Preview an example:](#)

archive\sent_jsmith.nsf

Figure 9-56 Configure Destination database

- Type in the name of the directory on the destination server into which you want these documents to be archived. A new database for each user will be created in this directory. If the directory does not currently exist it will be created the first time this criteria set is used.
- Configure the prefix for each database. You will want to do this if you are isolating different kinds of messages in different archive databases.

- You can add a suffix to the name of the destination database (for the same reasons you add a prefix).
- Choose how many characters the filename should retain from the original's filename. The default is 6 characters. If you have a lot of mail files on your system you will want to increase this to assure uniqueness.

Tip: While creating the destination database configuration press the F9 key to see a sample of the filename that will be created.

- d. On the Administration tab change the “Owners and administrators” to an administrative group if you want others to be able to edit this criteria settings document.
- e. Click Save & Close to save the document and return to the Archive settings document. You will see the archive criteria settings document appear in the list of Currently Selected Criteria.

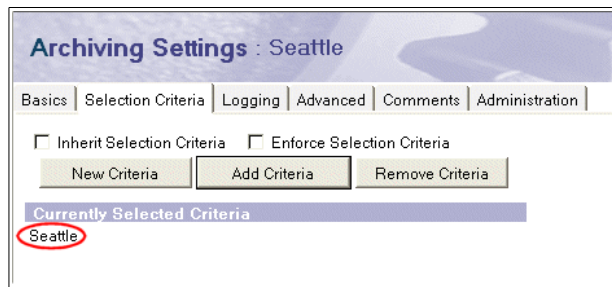


Figure 9-57 Currently selected criteria

- f. If you want to add other criteria settings documents which already exist, click on the Add Criteria button. Select the settings you want to implement.

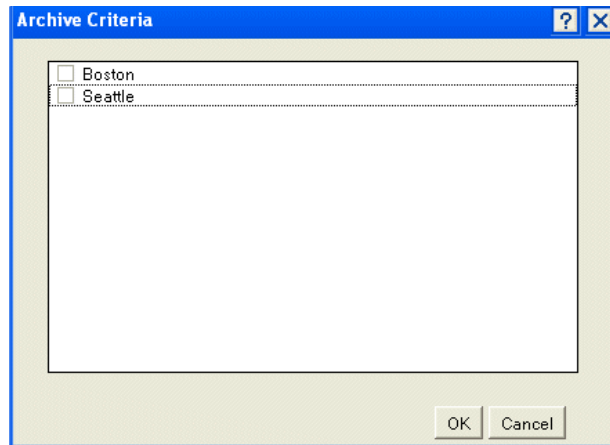


Figure 9-58 List of Archive Criteria

Tip: It is possible to select an archive criteria settings document which is not enabled. Once you decide that you want to include another criteria settings document double check to make sure that it is enabled.

4. Click the Logging tab to configure the logging for archiving. If logging is turned on, each archive instance will log at least two entries in the user's archive log.

Archive Log		Close Database	
Archive Logs		Information	
<ul style="list-style-type: none"> By Archive Date By Archive Database By Source Database Failed Archives 	★	11/05/2002 07:16 PM	Archive Statistics for: Peg Weiss
	★		Peg Weiss (Archive) (archive05la20_pweiss.nsf on boston/itso). Docs copied:3
	★		Peg Weiss (Archive) (archive1a5_pweiss.nsf on boston/itso). Docs copied:8
	★	11/05/2002 07:09 PM	Archive Statistics for: Peg Weiss
	★		Peg Weiss (Archive) (archive05la20_pweiss.nsf on boston/itso). Docs copied:0
	★		Peg Weiss (Archive) (archive1a5_pweiss.nsf on boston/itso). Docs copied:6
	★	11/05/2002 06:59 PM	Archive Statistics for: Peg Weiss
	★		Peg Weiss (Archive) (archive05la20_pweiss.nsf on boston/itso). Docs copied:2

Figure 9-59 Archive log

One entry gives the archive statistics for the archive session (how many documents, where they went, and document links).

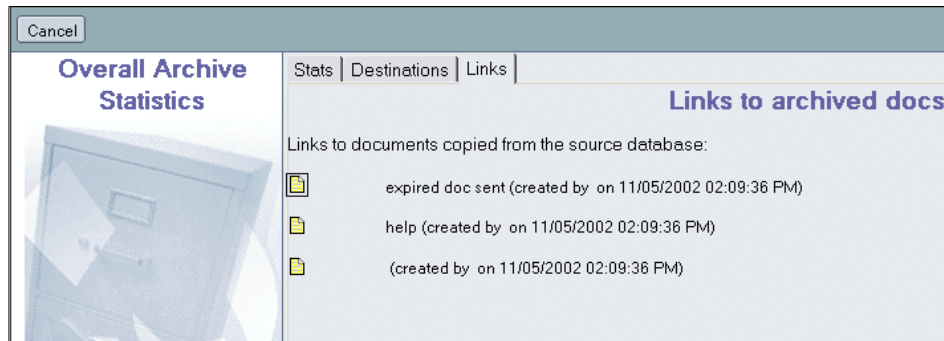


Figure 9-60 Overall Archive Statistics

Other entries are destination logs. There may be more than one of these if the different criteria settings documents are configured to go to separate destination databases.

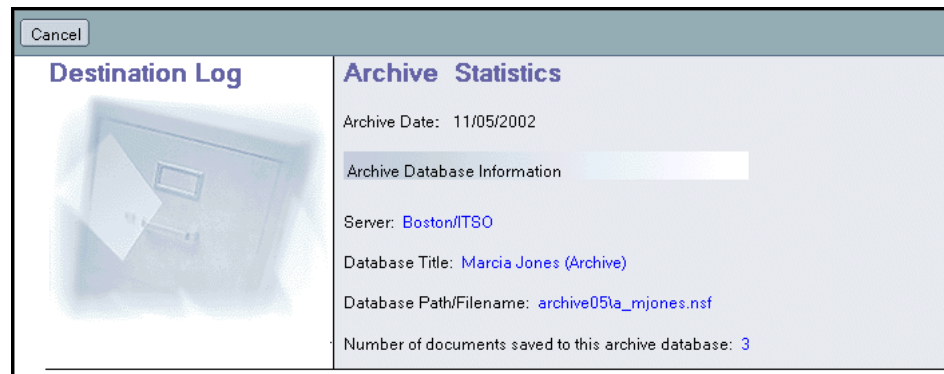


Figure 9-61 Destination log

If you decide not to enable logging, uncheck the box which enables it and proceed to step 5.

Save & Close Cancel Inheritance Enforcement

Archiving Settings : Archive all

Basics | Selection Criteria | **Logging** | Advanced | Comments | Administration

Archive Logging		Inherit from parent policy:	Enforce in child policies:
<input checked="" type="checkbox"/> Log all archiving activity into a log database		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Path Information		Inherit from parent policy:	Enforce in child policies:
Log Directory:	<input type="text" value="archive_"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Log Prefix:	<input type="text" value="I_"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Log Suffix:	<input type="text" value=""/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Number of Characters from original filename:	<input type="text" value="6"/>	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input checked="" type="checkbox"/> Include document links to archived documents		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

[Preview an Example:](#)
archive9U_aitso.nsf

Figure 9-62 Archive logging configuration

By default logging is enabled. You can configure how the logging is done by modifying the following settings:

- a. (Optional) Change the Log directory. If it doesn't exist it will be created on the destination server.
 - b. (Optional) Change the Log prefix. By default "I_" will be used in combination with the mail file's original name. This can help you identify types of log files more quickly at a later time.
 - c. (Optional) Add a Log suffix to the log file name. This can help you identify types of log files more quickly at a later time.
 - d. (Optional) By default Domino will use 6 characters from the mail file's original filename. You can increase this if uniqueness is a concern.
 - e. By default Domino will create a database link to each archived document in the archive log. If you would prefer for it not to do this, uncheck the box "Include document links to archived documents."
 - f. Click Save & Close.
5. Click the Advanced tab. The only option on this tab is whether or not documents with responses should be deleted during the archive process. By default it is set to not delete such documents. This will prevent the account from having replies to e-mails, without having the original e-mail. Once all of the replies and the original e-mail meet the archive criteria they will be archived.

Using compact to archive documents

Server-side archiving is initiated with the compact utility with special switches. It can be done at the console, at a command prompt on Win32 systems, through a program document, through the files utility in the Domino Administrator, or through the Task tool in the Domino Administrator.

No matter how you initiate it, you add a switch to tell the compact utility that it is archiving documents. When you use the -A or the -a switch, compact ignores other switches. If you want to reduce the file size of your mail files run compact twice; once with the -A switch and once with the -B switch.

- ▶ The -A switch simply archives documents and cleans up the source database. It does not compact the database. This is faster than the -a option. Choose this option if you are concerned about the task taking too long to run.
- ▶ The -a switch archives documents, cleans up the source database, and then compacts the source database (using in-place compaction).
- ▶ The -j switch must be used in conjunction with one of the other switches

In most cases you will want to configure a program document to run the archive process on a regular basis during low usage periods.

Important: Running compact on a server may affect the dbiid (database instance ID). If you use transactional logging be aware of the implications of running compact before you set up server-side archiving. If you are only archiving (using compact with only the -a or -A switch) it will not affect the dbiid.

Run compact at the console

Enter the command:

```
load compact mail\filename.nsf -A
```

or

```
load compact mail -A
```

This is a good option if you need to archive a mail file immediately.

Run compact at a command prompt (Win32 systems only)

You can use ncompact at a command prompt whether the server is up or not.

1. Navigate to the program directory for your server. By default this will be c:\lotus\domino
2. Enter the command:

```
ncompact mail\filename.nsf -A
```

or

```
ncompact mail -A
```

If you want to archive all databases on the server and compact them, enter:

```
ncompact -a
```

Configure a program document to run compact at a specified time

1. With the Domino Administrator, click the Configuration tab. Expand the Server section and click the Programs view.

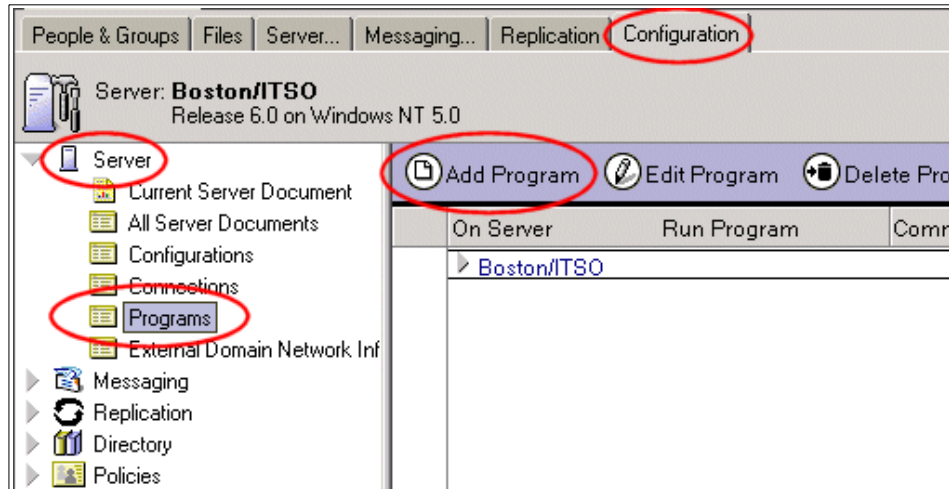


Figure 9-63 Navigate to Program documents in Domino Administrator

2. Click Add Program to create a new program document.

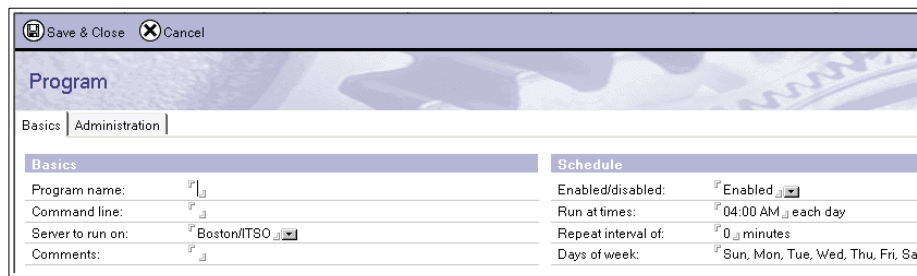


Figure 9-64 Program document

3. With the Program document in edit mode, add entries to the following fields:
 - Program name: compact
 - Command line: -A or -a

If you only want to archive files in a particular directory add the name of that directory in the command line field:

mail -A

- Server to run on: this is the server on which the files to be archived reside. Select the correct server by clicking the down arrow.
- Comments:
- Enabled/disabled: Enabled.
- Run at times: Pick a time when the server is not very busy.
- Repeat interval of: You probably won't use this for archiving.
- Days of week: Pick a day or days as needed.

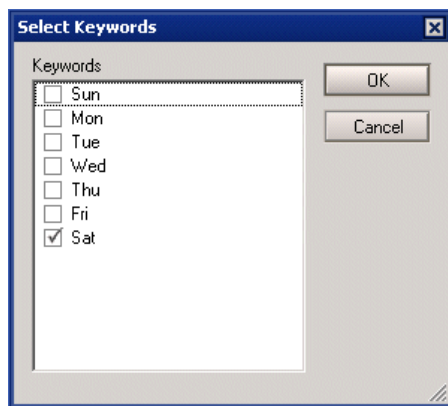


Figure 9-65 Select days on which the program will run

4. Click Save & Close.

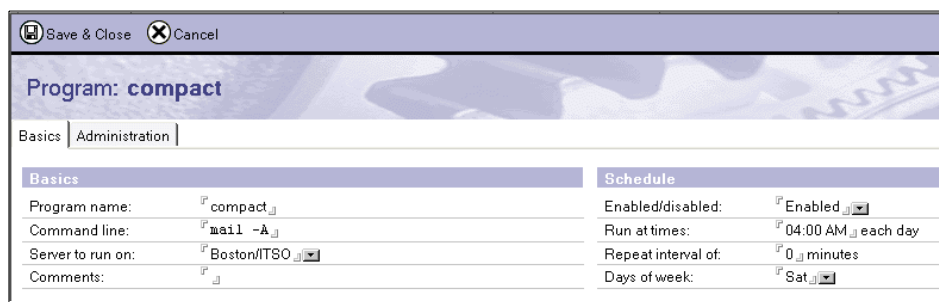


Figure 9-66 Sample Program document

Use the file tools in the Domino Administrator

1. With the Domino Administrator, click the Files tab. Navigate to the directory where the files to be archived are located.
2. Select the file or files you want to archive.
3. In the right-hand panel expand the Tools if they are collapsed, then expand the Database section.

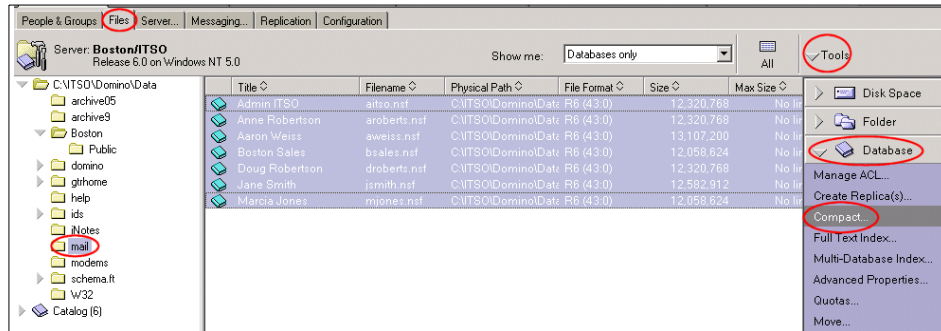


Figure 9-67 Navigate to database tools in Domino Administrator

4. Click Compact to bring up the Compact Database dialog box.

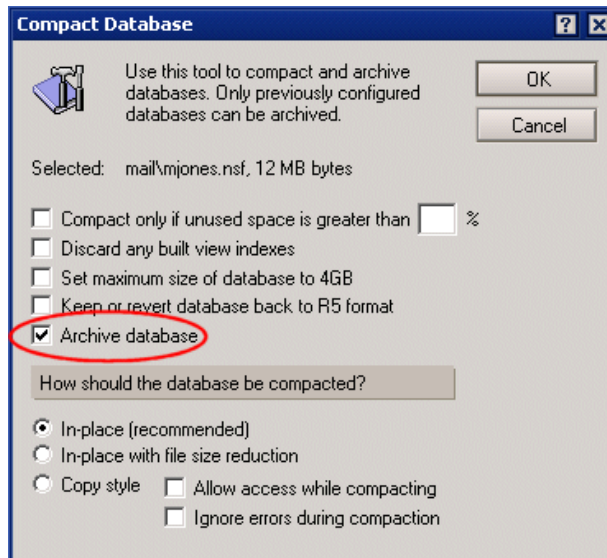


Figure 9-68 Database tool compact utility

5. Click Archive database. This is equivalent to using the -a switch in the program document or on a command line. Compact will archive the

documents, clean up the mail file as specified in the policy, and compact the database.

6. Click OK to process the databases. The server will store this request and process the files as it has time.

Use the Task - Start tool in Domino Administrator

1. Verify that you have remote console access rights to the server. This is basically a GUI interface for a console command.
2. With Domino Administrator:
 - Click the Server tab.
 - Click the Status tab.
 - Click Server Tasks.
 - Expand the Tools pane if necessary.
 - Expand the Task section and click Start.

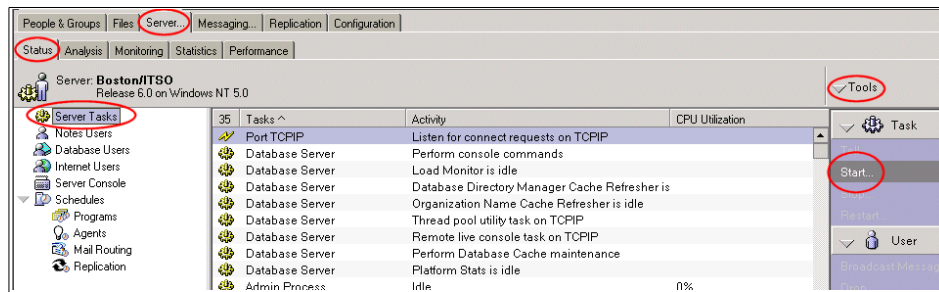


Figure 9-69 Navigate to the Task tool

3. When the Start New Task dialog box appears, scroll down to Compactor and click once to select it. Verify that the checkbox “Select advanced option” is checked. Click the Start Task button.

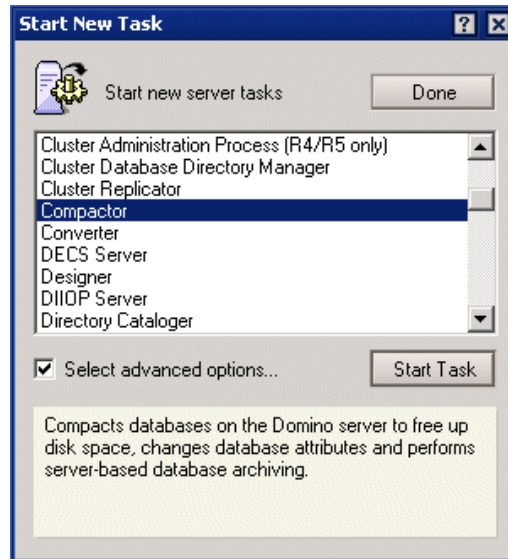


Figure 9-70 Start New Task dialog box

4. Enter a directory on the Basics tab to indicate which files you want to compact. You can enter either a directory or an entire file path (relative to the data directory of the server) if you just want to archive one mail file.

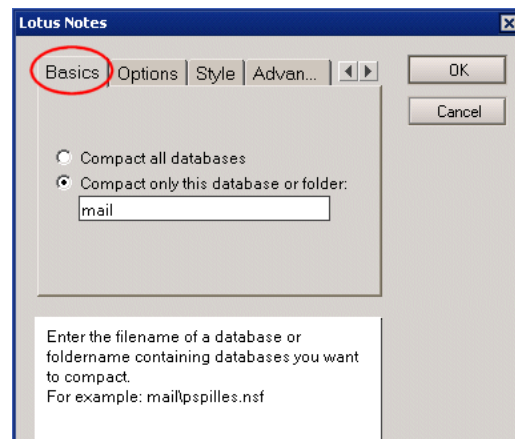


Figure 9-71 Configure a one-time compact run with the Task tool

5. Click the right arrow to the right of all the tabs several times until the Archive tab appears. Click the Archive tab.

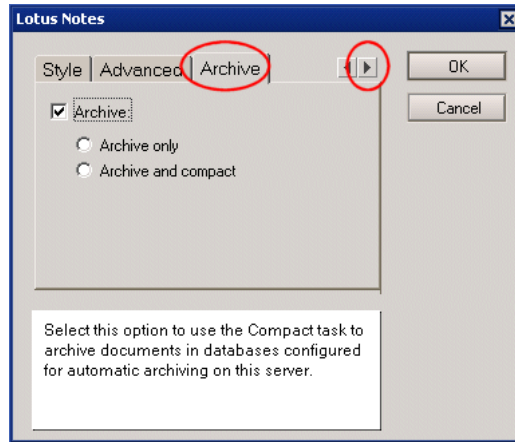


Figure 9-72 Archive choices in the Task tool

6. Click in the checkbox labelled Archive and then choose archive only (equivalent to compact -A) or Archive and compact (equivalent to compact -a).
7. Click OK. The compact task will begin immediately on the server.

9.5 Single copy object store (Shared mail)

Single copy object store (SCOS) is a space-saving feature which enables the server to save one copy of a message sent to multiple recipients, rather than delivering individual messages to each user's personal mail database. Users' mail files receive the header information and a pointer to the message in the shared mail database. This is not a new feature in Domino 6, but it has been improved significantly. The enhancements include:

- ▶ You can use multiple shared mail databases. This reduces the contention that existed when all shared mail messages existed in one database.
- ▶ Configuration of the shared mail system is done in the server document.
- ▶ You can spread your shared mail databases over different disk subsystems, which improves performance on heavily loaded servers.
- ▶ You can have up to 10 active shared mail directories and each one of those can have up to 100 shared mail databases within it. Each directory can store up to 8 GB of data. The system can also recognize up to 40 inactive shared mail directories (users can still access their messages in the inactive shared mail databases).

- ▶ Automatic maintenance is done on the shared mail databases: messages which are no longer referenced by a user's mail file are automatically purged from the system.
- ▶ User accounts are not tied to any one shared mail database.

9.5.1 Set up shared mail with the server document

1. In the Administrator client, click the Configuration tab and expand the Server section in the navigation panel.
2. Open the Server document of the server on which you want to configure shared mail.

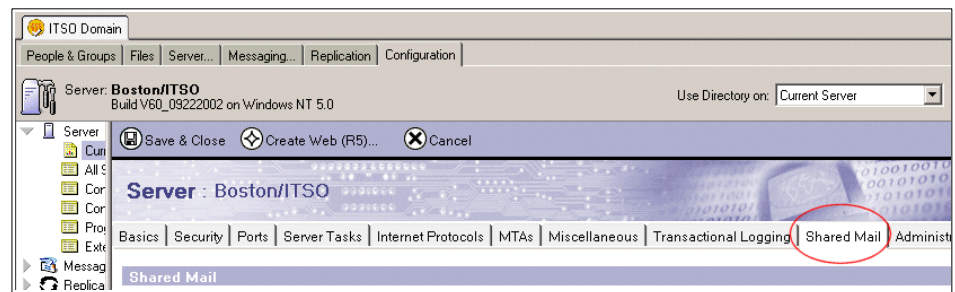


Figure 9-73 Shared Mail location in server document

3. Put the Server document in edit mode by double-clicking it or clicking the Edit server document button.

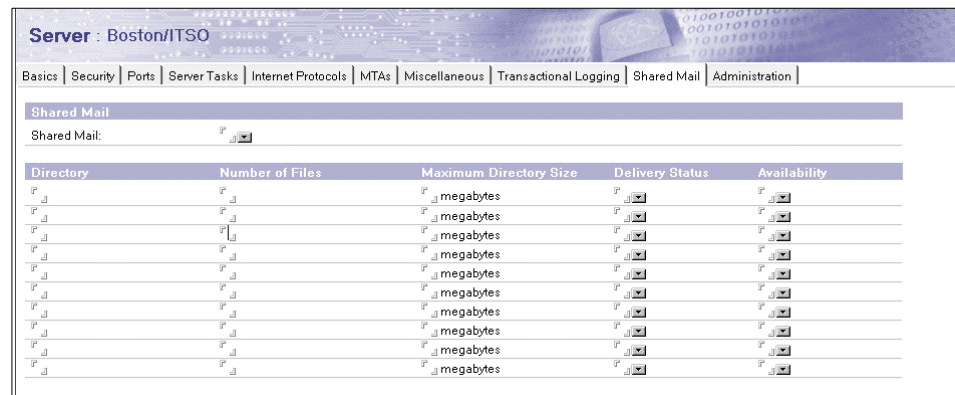
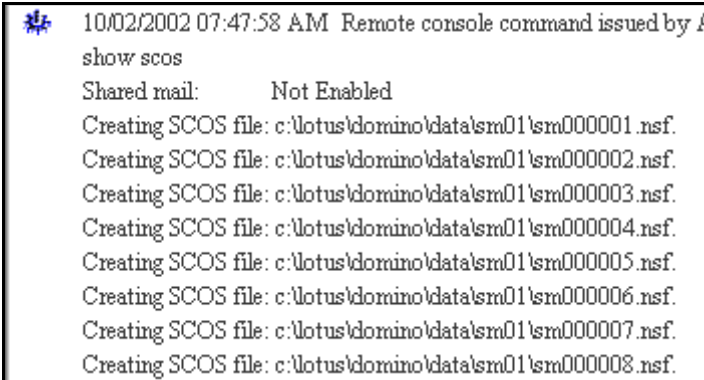


Figure 9-74 Shared Mail configuration document

4. In the Shared Mail field select Delivery or Transfer and Delivery.

- Delivery: the server uses shared mail for messages delivered to multiple local recipients.
 - Transfer and Delivery: the server always uses shared mail (all messages are stored in the shared mail databases).
5. In the Directory section of the document you see 10 lines, which correspond to the 10 active shared mail directories. Each directory is configurable for:
- The directory in which you want the shared mail files to be stored. Use the full path to the directory:
`c:\lotus\domino\data\sm01`
 - The number of shared mail files to be stored there (up to 100)
 - The total size to which the directory can grow (all shared mail files added together). Maximum configuration is 8192 (MB).
 - Delivery status (whether the router should attempt to use those shared mail databases for storage). Default is open. The system will change the status to closed if the directory reaches its limit. Users can access the shared mail databases no matter what the delivery status is.
 - Whether its availability status is online or offline. Default is online. You only take a shared mail directory off line to move the directory or one of the shared mail databases. Users cannot access their mail in these databases if the availability is set to offline.
6. Click Save & Close.
7. In the Domino Administrator client open a console session with the server you just configured for SCOS.
8. Type in the command line:

```
show scos
```



```
10/02/2002 07:47:58 AM Remote console command issued by A
show scos
Shared mail:      Not Enabled
Creating SCOS file: c:\lotus\domino\data\sm01\sm000001.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000002.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000003.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000004.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000005.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000006.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000007.nsf.
Creating SCOS file: c:\lotus\domino\data\sm01\sm000008.nsf.
```

Figure 9-75 `show scos`

9. You will see that the server is creating the shared mail databases.

9.5.2 Guidelines for configuring shared mail

- ▶ Consider using a separate disk subsystem for shared mail databases. This will increase performance since different disk controllers will be accessing hard drives to retrieve information from the users' mail files and the shared mail databases.
- ▶ Use more shared mail databases, rather than less. This will reduce the amount of contention for the shared mail databases.

9.6 IMAP improvements

The Domino code for IMAP has basically been rewritten to provide significant improvements to the IMAP implementation, in particular:

- ▶ Native support at the NSF level for IMAP

In earlier releases of Domino, the IMAP server was based on a layered approach that relied on using additional Notes items and views to maintain the IMAP-specific data for messages. In Domino 6, the core database layer (NSF) has been enhanced to include native support for IMAP semantics, and the IMAP server has been redesigned to use these new capabilities. In addition, the IMAP server now has a new multi-threaded and data-streaming architecture for additional parallelism, providing much higher performance and scalability.
- ▶ Support for NAMESPACE extension

The IMAP server now supports the NAMESPACE extension, so an IMAP client can now view folders in another user's mail file or the public folders in a shared database. This means that users can have delegated access to another user's mail via IMAP, in addition to access via the Notes client.
- ▶ Unread marks

In previous versions of Notes and Domino, mail files maintained separate sets of unread marks for IMAP clients and Notes clients, with IMAP-enabled mail files relying on special template views to indicate that a message was read. With the introduction of native IMAP in Domino 6, a mail file enabled for IMAP displays a consistent set of unread marks to the IMAP and Notes clients opening the file.

The next section describes how to configure mail files for IMAP access, IMAP server configuration options, IMAP activity logging, and how to set up databases to be accessible to IMAP clients through the NAMESPACE extension.

9.7 Configuring mail files for IMAP access

IMAP clients use a standard Domino mail file that must be specially enabled for IMAP. If you enable IMAP access for the mail file of a registered Notes user, the user can access the file from either the Notes client or from an IMAP client. Users who are only using an IMAP client do not need to be registered Notes users. They simply need a person document that points to the appropriate mail file.

To support IMAP clients and store IMAP-specific information, the Domino mail file requires the addition of special IMAP database items. IMAP stores message information within its own set of attributes. For a Domino mail file to be used with IMAP, Notes/Domino items in the mail file have to be translated into IMAP attributes.

IMAP clients request information about messages in order to display the message headers in the IMAP client more quickly. This information is stored in MIME summary attributes in a Domino mail file, but only if the file has been IMAP-enabled and the person document specifies that mail should be delivered in MIME format.

The Domino router uses the “Format preference for incoming mail” field in each person document to determine whether to add the appropriate MIME summary attributes to messages it is delivering. This significantly improves performance for IMAP clients because each message doesn’t have to be opened to get the attributes. The IMAP attributes added to messages are:

- ▶ \$Content_Type
- ▶ IMAP_BodyStruct
- ▶ IMAP_RFC822Size

You can add these summary attributes to pre-existing messages in a user’s mail file so that the IMAP client can use the summary attributes to display the header in the client, rather than downloading an entire message before it can display the header. If you anticipate that users with large accounts are going to use IMAP, you should use the convert utility (once with the -e switch and once with the -h switch; discussed in the next section) to prevent delays the first time they log in to the server to ease the burden on the server.

Attention: To be enabled for IMAP, a mail file must use the Domino Release 5 or later file format, Notes ODS (on-disk structure) version 41 or greater. If a mail file is at a previous ODS version, you must run Compact on it to update the ODS version. It is not necessary to run Compact to enable new mail files that are based on either the MAIL6.NTF or MAIL50.NTF mail templates.

There are two methods for converting mail files for IMAP use:

- ▶ Configure the IMAP service to do the conversion the first time a user connects to the server and attempts to access their mail file with an IMAP client.
- ▶ Use the convert utility to prepare the mail files for IMAP access.

9.7.1 Automatic conversion of mail files

IMAP, by default, is configured to convert mail files when a user logs into the server with an IMAP client. After the client logs in, the server detects that their mail file is not IMAP-enabled and automatically dedicates a thread to the conversion process. This can take several minutes for each mail file. On a busy server this can cause some delays in IMAP service. Also, some organizations may want to provide IMAP access to some users but not all. You can turn this configuration off.

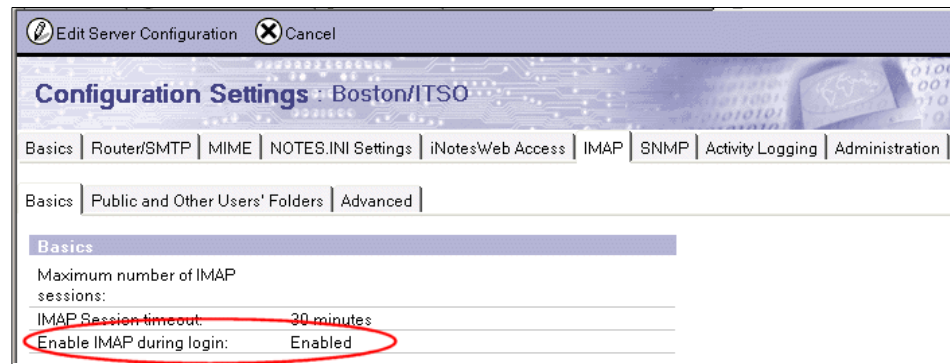


Figure 9-76 IMAP configuration document

1. In the Administrator client open the Configuration Settings document for your IMAP server.
2. Click the IMAP tab of the Server document.
3. Click Edit Server Configuration to put the document in edit mode.
4. Change the "Enable IMAP during login" field from Enabled to Disabled.

5. Click Save & Close.

Important: If you have mail files which are still at ODS 20 (R4.x) and will be accessed by IMAP clients, disable the automatic conversion feature. It will fail on these mail files. See 9.7.3, “Conversion of R4 mail files” on page 281 for a discussion of how to convert R4.x mail files for IMAP use on a Domino 6 server.

Restrictions: This method will not add the MIME summary attributes to previous messages. It simply prepares the mail file for new messages. Use the convert utility to “retro-fit” mail files.

This method will only enable the personal mail file of the user who has authenticated to the server. You must run conversions manually to enable mail files in the other users’ and public folders namespaces.

9.7.2 Manual conversion of mail files (R5 and Domino 6)

You can use the convert utility to IMAP-enable mail files. This is the same utility that you use to convert mail files from one template design to another. If you know all of your users will be using IMAP, or if all of your IMAP users’ mail files are in one directory, this can be an easy way to prepare them for IMAP connections.

Important: For users with multiple mail file replicas (for example, on clusters) you must independently enable each replica for IMAP access. Domino does not replicate IMAP database items between databases.

Enter these commands at the server console:

```
tell router quit
load convert mailfiledirectory\mailfilename -e
load convert mailfiledirectory\mailfilename -h
load router
```

You can use wild cards:

```
load convert mailfiledirectory\* -e
load convert mailfiledirectory\* -h
```

An explanation of command line parameters is in Table 9-4 on page 281.

Tip: If you have taken your server down and want to complete the steps for enabling IMAP while it is down, you can enter these commands in the Domino program directory (default for a Windows implementation is c:\lotus\domino):

```
nconvert path\mailfilename -e  
nconvert path\mailfilename -h
```

Path is the path relative to Domino data directory.

Mailfilename is the exact filename of the mail database, such as user.nsf

Attention: Folder references during upgrade of IMAP mail files

In earlier releases of Domino, the IMAP service used hidden folder reference views in the mail template to retrieve IMAP folder and message data. By contrast, the Domino Release 6 IMAP service doesn't use folder references. Instead, it enables native storage of IMAP folder and message attributes in the mail file, thus eliminating the need for hidden views in the mail template.

By default, when you convert mail files to Lotus Domino 6 IMAP format, the conversion utility disables folder references in the mail file. In most environments, use the default and disable folder references to ensure the best performance.

If your environment uses Domino applications that rely on folder references in user mail files to gather information, you may need to preserve folder references. To preserve folder references during conversion, you can set the variable `IMAP_CONVERT_NODISABLE_FOLDER_REFS` in a server's `NOTES.INI` file. When this variable is set, folder references are preserved during all mail file conversions, whether performed manually from the server console, or automatically as the result of an IMAP user logging in to the IMAP service for the first time.

Immediately following conversion, the folder and message information stored in the folder references matches the information stored in the mail file's IMAP attributes. However, because Domino does not continue to update folder references after the initial conversion, over time, as a user receives, moves, and sends messages, folder reference information will no longer be synchronized with the information stored in the mail file attributes.

Table 9-4 Convert utility command line parameters

Parameter	Effect
-r	Converts mail files in subdirectories of the specified directory
-l	Creates a text list of mail files
-f	Uses a text list of mail databases to determine which files to upgrade
-o (new in R6)	Removes IMAP information from messages
-h (new in R6)	Adds IMAP information to existing messages
-m	Converts mail files for IMAP use with R5 servers
-m-	Removes IMAP design from R5 mail files
-s (new in R6)	Upgrades design of folders without Preserve bit set
-e (new in R6)	Converts the mail database for IMAP use
-e- (new in R6)	Disables IMAP support in the mail file
-u (new in R6)	Converts all custom folders to the R6 Inbox design
Mailfilepath	Specifies which mail file or files to upgrade
Existingtemplatename	Specifies a certain mail file design to upgrade (for example, StdR50Mail)
Newtemplatefilename	Specifies the template used to upgrade mail files (for example, mail6.ntf)

9.7.3 Conversion of R4 mail files

Beginning with R4.6, Domino supported IMAP connections to mail accounts. If you still have some accounts which are at the R4 mail file design and the R4 ODS (ODS 20) you will need to run compact, fixup, and the convert utility in order for them to be IMAP-enabled with the Domino 6 server. This is not necessary for mail files based on either the mail6.ntf or the mail5.ntf, or if the mail file is at ODS 41 or ODS 43. If your users are *only* using IMAP you should upgrade their mail file design to the mail6.ntf so that the IMAP server can take full advantage of the new IMAP implementation.

Run compact at the console

1. From the Domino Administrator, on the Server pane on the left, select the server on which to run Compact.
2. Click the Server -> Status tab.

3. Click Console.
4. Type the following on the command line at the bottom of the console, and then press Enter:

```
load compact mailfiledirectory\mailfilename.nsf
```

You can also compact all of the mail files in a directory with the command:

```
load compact directoryname
```

Run fixup on the mail file

Because the Fixup task requires exclusive access to the mail file database, you must shut down the server before running Fixup.

1. Shut down the server.
2. Open a command prompt. Change to the Domino program directory (default location on a Windows server is c:\lotus\domino).
3. Enter the following command:

```
nFixup path\mailfile
```

Path is the path relative to the Domino data directory.

Mailfile is the filename of the mail file database.

```
nFixup mail\user.nsf
```

Important: If transaction logging is enabled on the server, run Fixup with the -j switch:

```
nFixup -j mail\user.nsf
```

Run the convert utility on the mail file

See the previous section about running the conversion utility. Even though these accounts were previously enabled for IMAP they will need to be enabled again after the server has been upgraded to Domino 6.

9.7.4 Checklist for IMAP accounts

- ▶ Convert the mail file by:
 - Enabling conversion upon login (OK for small mail accounts or unstressed servers).
 - Using the convert utility (better for large accounts and stressed servers). Run it twice with different switches to add MIME attributes to pre-existing messages. This will prevent the server from having to convert each message as it is downloaded to the IMAP client.


```
load convert mailfiledirectory\mailfilename -e
load convert mailfiledirectory\mailfilename -h
```

- ▶ Change the preference in the user's person document to receive mail in MIME format.
- ▶ You may want to issue an Internet certificate to your IMAP users so that they can send and receive encrypted mail using S/MIME.
- ▶ If a user will *only* be using an IMAP client consider removing the Notes public key from the Notes certified public key field in the person document. This will prevent Notes users from sending the IMAP user an encrypted message, which they will not be able to read with their IMAP client. The Notes user will see this error when attempting to send an encrypted message to a user without a public key:

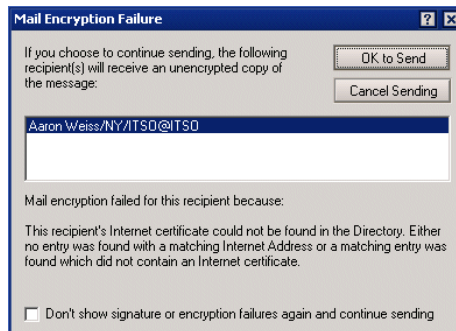


Figure 9-77 Encryption error message received by a Notes user

9.8 Server configuration for IMAP

The configuration settings for IMAP are located in two places: the server document and the configuration settings document for each server. Domino 6 has greatly improved the control that the administrator has over the IMAP functioning of the server.

9.8.1 Starting the IMAP service

The IMAP service can be started manually at the server console by typing:

```
load imap
```

You may want to stop and restart the IMAP service to force it to update its configuration. You can restart the IMAP service in one of two ways:

- Stop it and load it again:

```
tell imap quit  
load imap
```

- Use the restart command:

```
restart task imap
```

To configure the server to start up the IMAP service automatically, edit the `notes.ini` file (found in the program directory of the server). Find the line that begins with `ServerTasks` and add IMAP to that line. It should look something like this:

```
ServerTasks=Update,Replica,Router,AMgr,CalConn,AdminP,Sched,HTTP,IMAP,LDAP,POP3
```

9.8.2 IMAP port configuration

Attention: On servers that use Internet Site documents, the IMAP service obtains port authentication settings from the Security tab of the IMAP Site document, rather than the server document. If the server uses Internet Site documents, and an IMAP Site document is not present in the Domino Directory, or the authentication options in a configured IMAP Site document are set to No, users cannot connect to the IMAP service. For more information on Internet Site Documents see Chapter 12, “Internet Site architecture” on page 385.

The Domino 6 IMAP service uses the industry standard TCP/IP ports for IMAP (143 and 993), unless you specifically choose to use different ports. These are configured in the same way as they were for R5. They are located in the server document on the Ports -> Internet Ports -> Mail tab.

Web	Directory	Mail	DIIOIP	Remote Debug Manager
Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	
TCP/IP port number:	143	110	25	
TCP/IP port status:	Enabled	Enabled	Enabled	
Enforce server access settings:	No	No	No	
Authentication options:				
Name & password:	Yes	Yes	No	
Anonymous:	N/A	N/A	Yes	
SSL port number:	993	995	465	
SSL port status:	Disabled	Disabled	Disabled	
Authentication options:				
Client certificate:	No	No	N/A	
Name & password:	Yes	Yes	No	
Anonymous:	N/A	N/A	Yes	

Figure 9-78 Internet Mail port configuration

9.8.3 IMAP service configuration

In R5 the administrator had to edit the notes.ini file to specify IMAP session limits. These configurations are now manipulated through the configuration settings document for each server. There are also many new settings because of the NAMESPACE extension which Domino 6 supports, and the improved thread pool architecture.

The IMAP configuration settings are found in the Configuration Settings document for each server, or for a group of servers:

1. Make sure you already have a Configuration Settings document for the servers to be configured.
2. From the Domino Administrator, click the Configuration tab and expand the Messaging section.
3. Click Configurations.
4. Select the Configuration Settings document for the mail server you want to restrict mail on, and click Edit Configuration.

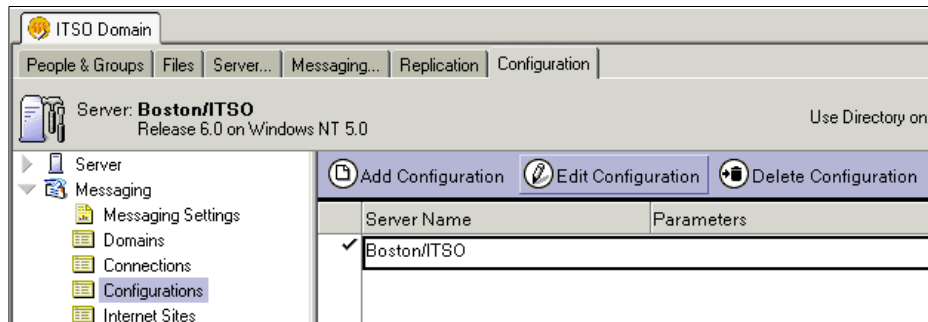


Figure 9-79 Navigate to messaging configuration document

Basics: Configure IMAP sessions

You may want to limit the number of sessions that IMAP supports and the default timeout for sessions. Configuring these values allows you to limit the amount of server resources devoted to the IMAP service. By default the IMAP service does not limit the number of connections by IMAP clients. Since each connection uses a connection thread and some server memory, you may want to limit how many IMAP sessions are allowed and how long they will stay connected if idle.

1. Click the IMAP - Basics tab. There are only two fields:
 - Maximum number of IMAP sessions. By default no limit is imposed.
 - IMAP session timeout. Enter the time, in minutes, that an IMAP client can be idle before the server ends the session. Default timeout is 30 minutes. If you set a limit on the number of IMAP sessions you may need to reduce the idle time in order to free up threads for new connections.

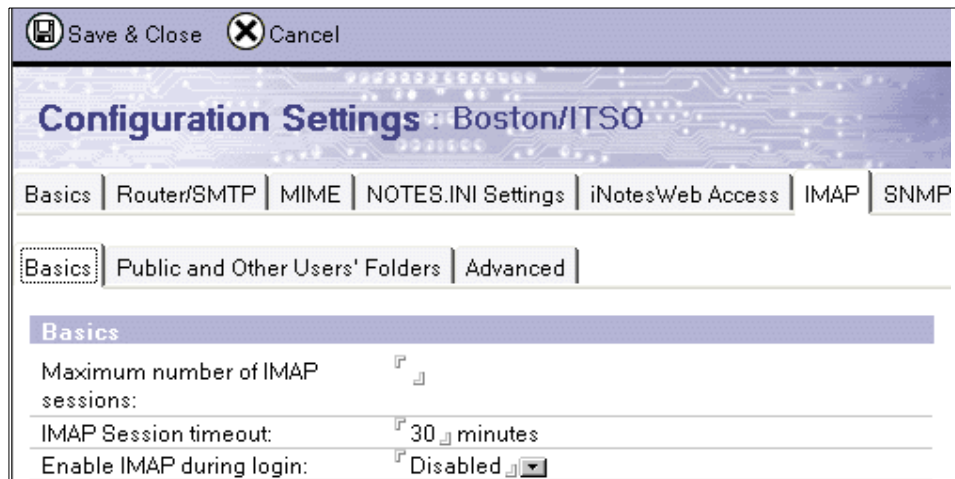


Figure 9-80 IMAP configuration settings

2. Click Save & Close.

Public and other users' folders: NAMESPACE

The IMAP protocol makes use of the idea of NAMESPACE hierarchies. Typically, most users have a personal mail file to which they alone have access. The IMAP service considers messages in a personal mail file to exist in a hierarchy known as the personal NAMESPACE. Some messages may exist in another hierarchy. For example they can exist in the public NAMESPACE hierarchy or in other users' NAMESPACEs. The IMAP client uses NAMESPACE commands to collect these other messages.

The Domino 6 IMAP service supports the NAMESPACE extension, which permits controlled access to other mail files by IMAP clients. The ACL of these other mail files still limits access to them. You can set up public mail files as IMAP public folders (for example, mail-in databases). As with personal mail files, an IMAP client can access public and other users' mail files only if they reside on the same server as the IMAP service.

For a list of clients that support the NAMESPACE extension, consult the IMAP Connection at:

<http://www.imap.org>

To configure the response of a server to NAMESPACE commands by IMAP clients, edit the Configuration Settings document.

1. Click IMAP -> Public and Other Users' Folders tab.

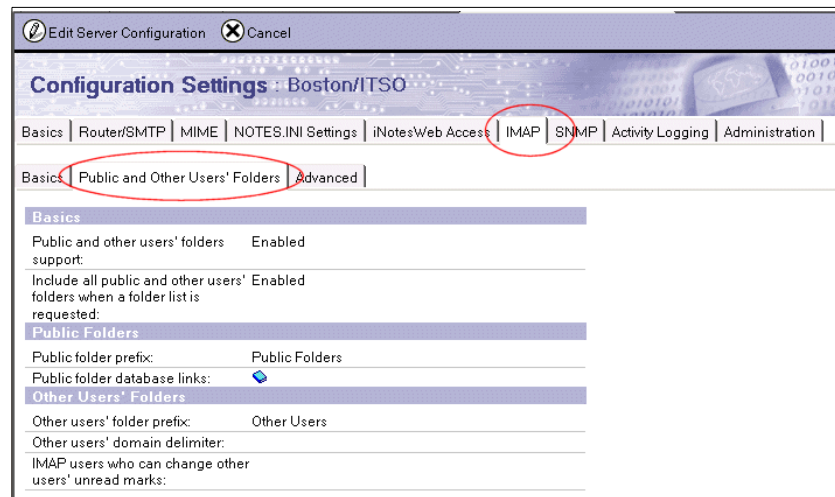


Figure 9-81 NAMESPACE extension settings

Make entries and modify selections to the fields as appropriate.

Basics

- ▶ “Public and other users’ folders support” is enabled by default. If you disable this setting users will only be able to access their own mail files.
- ▶ “Include all public and other users’ folders when a folder list is requested” is disabled by default. With the default setting, only clients which are capable of issuing the NAMESPACE command will be able to display other users’ folders and public folders. Enable this setting to support IMAP clients which do not use the IMAP NAMESPACE extension. This will present all the available folders to them when they login.

Public folders (public NAMESPACE hierarchy)

- ▶ “Public folder prefix” is an arbitrary name for a virtual directory that Domino creates when NAMESPACE extension is enabled on the server. Since IMAP clients may cache the name of the public folder on a server it is best not to change this name once it has been configured.
- ▶ “Public folder database links” requires you to paste in Notes database links. These databases will appear as IMAP public folders to IMAP clients. You limit access to them using the ACL of each database.

Other Users’ Folders (other users’ NAMESPACE hierarchies)

- ▶ “Other users’ folder prefix” is an arbitrary name for a virtual directory that Domino creates to organize mail files shared by IMAP users through delegated access.
- ▶ “Other users’ domain delimiter” allows you to configure another symbol for the hierarchy delimiter—in Notes the delimiter is a slash (/). This allows you to accomodate some IMAP clients which cannot interpret a /. For example, enter a pipe character (|) to send the name John Smith/Cambridge/ITSO as John Smith|Cambridge|ITSO
- ▶ “IMAP users who can change other users’ unread marks” allows you to configure which users can change the unread marks of other user’s messages (for example, an assistant who needs to mark the messages of a manager as read). The users defined in this field must have designer access to the mail files.

Tip: In order to allow an IMAP user the ability to change the read marks in another user’s mail file, they must have designer access to the database. You will need to change the Internet access limit in the ACL of the database from Editor to Designer.

After making configuration changes, restart the IMAP service to put the changes into effect, or wait until the IMAP service checks for configuration changes (the default time is 2 minutes). IMAP clients which had sessions already established will continue to operate under the configuration which was in effect when they logged in. New IMAP sessions will work under the new configuration.

Tip: You can change how often the server checks for new configurations by adding the following notes.ini parameter:

```
IMAP_CONFIG_UPDATE_INTERVAL=number of minutes
```

If the parameter does not exist in the notes.ini the default value is 2 minutes.

Advanced configuration settings

The IMAP service acts as an intermediary between IMAP clients attempting to retrieve messages and the Domino mail server. IMAP clients do not have direct access to mail files on the Domino server; instead, the IMAP service acts as a proxy, relaying each client's request to retrieve messages to the mail server. To return message data to the client, Domino opens the mail database and passes on the requested information to the IMAP service. The IMAP service then sends the requested message information to the client.

You can configure how the IMAP service responds to clients on the Advanced tab of the IMAP configurations tab.

Configuration Settings : Boston/ITSO

Basics | Router/SMTP | MIME | NOTES.INI Settings | iNotes\Web Access | **IMAP** | SNMP | Activit

Basics | Public and Other Users' Folders | **Advanced**

Greeting

IMAP server greeting:

IMAP SSL greeting:

IMAP SSL redirect greeting:

Worker thread pool

Maximum number of IMAP worker threads:

Maximum number of response threads per FETCH:

Maximum number of FETCH threads allowed:

Maximum number of FETCH response threads allowed:

Figure 9-82 Advanced IMAP configuration

Greetings

Enter the greetings fields as you would like them to appear to IMAP clients connecting through the unencrypted IMAP protocol, with SSL, or if you are redirecting IMAP to an SSL port (see Admin help for information on redirecting a TCP/IP port to an SSL-enabled port)

Worker thread pool (configures the internal IMAP thread pool)

The Domino IMAP service provides an internal IMAP thread pool that is independent of the thread pool that Domino uses to create client sessions. The default number of available threads is based on the amount of physical memory the server has. The service has a minimum of 50 threads available and a maximum of 400 threads.

You should leave these at the defaults unless you have been directed to change them by an IBM support person. These settings control the amount of resources the IMAP service will have and how it will distribute those threads for the various tasks.

The IMAP thread pool consists of three types of worker threads, identified in Table 9-5.

Table 9-5 IMAP thread types

Thread type	Description	Default maximum value
FETCH thread	Accepts validated FETCH commands from the client and transmits them to the Domino mail service.	80% of pool total
FETCH response thread	Transmits message data from the Domino mail service to fulfill client FETCH requests.	80% of pool total
LOGIN conversion thread	Converts mail files to IMAP format.	None

- ▶ “Maximum number of IMAP worker threads” is the total number of threads available in the IMAP service’s thread pool. It includes login conversion threads, FETCH threads, and FETCH response threads.
- ▶ “Maximum number of response threads per FETCH” is the number of threads available to transmit message data to fulfill a given FETCH request (the default is 4).
- ▶ “Maximum number of FETCH threads allowed” is the number of concurrent threads the IMAP service can use to transmit client requests to FETCH message data to the Domino mail server.
- ▶ “Maximum number of FETCH response threads allowed” is the number of threads the IMAP service can use to return message data from the Domino mail server in response to FETCH requests received from all active IMAP sessions.

Tip: To provide IMAP users with access to other users’ mail files, you must use a Notes client or iNotes client to delegate mail file access and you must be logged in as the mail file owner for the AdminP request to be properly processed. It is not sufficient to add the names of users to the ACL of the mail file.

9.9 Making use of the NAMESPACE extension

This section provides step-by-step instructions for setting up mail databases for access by IMAP clients using the NAMESPACE extension. We cover access to other users’ mail files as well as mail-in databases.

9.9.1 Sharing mail files

Use the following steps to configure access to other users' mail files through IMAP.

1. Configure the server to start the IMAP service.
2. Configure the server to allow the use of the NAMESPACE extension. It is on by default, so this should just be a matter of double-checking it.
3. The user who wants to share their mail file delegates access to someone else by creating a delegation profile through the preferences tool in his or her client.

Important: If you are doing this for a user you must be logged in with that user's ID. AdminP will not process the request correctly if you are logged onto the system with your ID and create a delegation profile in another user's mail file.

- a. With the Notes client in the Inbox view open the Tools -> Preferences on the Action Bar.

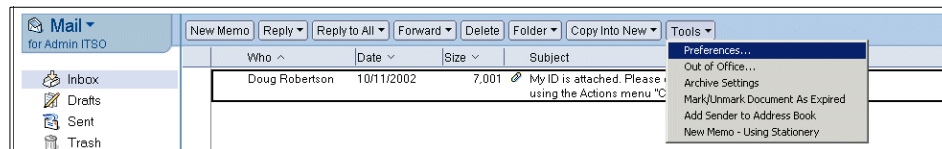


Figure 9-83 Navigate to the access to mail and calendar tool through the Preferences

- b. Click the Access & Delegation tab.
- c. Click the Access to Your Mail & Calendar tab.

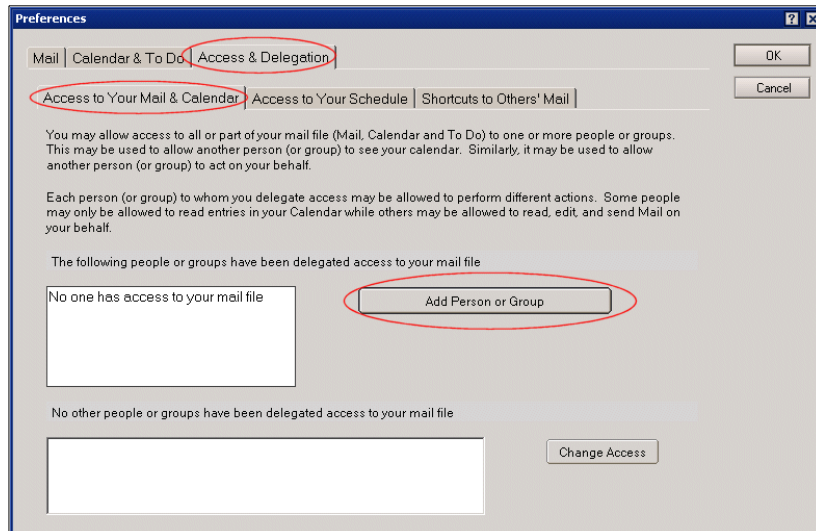


Figure 9-84 Access to Mail and Calendar tool in the Notes client

- d. Click the Add Person or Group button in the middle of the screen.

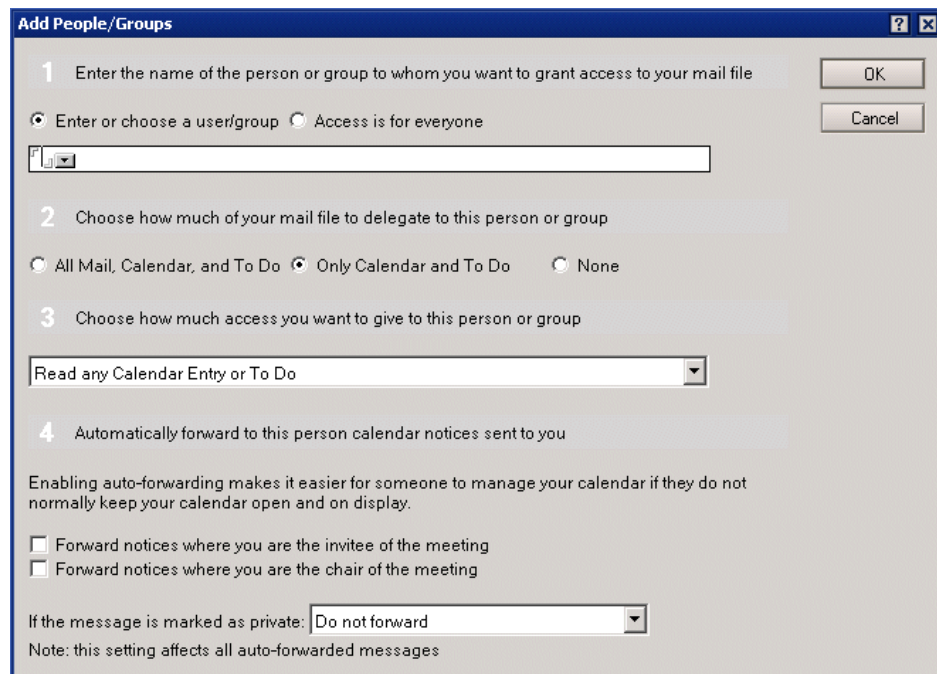


Figure 9-85 Add People/Groups

- e. In section 1 of the Add People/Groups dialog box make sure that “Enter or choose a user/group” is selected.
- f. Click the down arrow in section 1 to access the list of users; select the appropriate user from the server’s directory. You can only choose one person at a time.

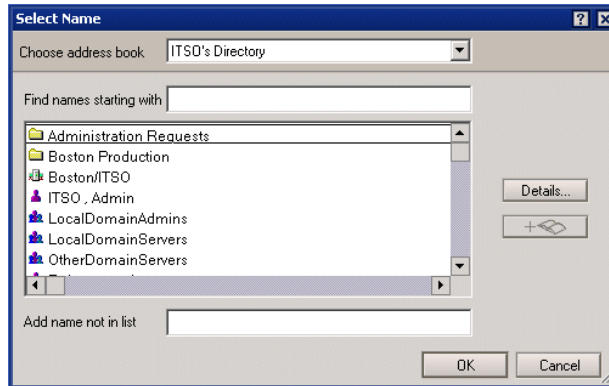


Figure 9-86 Choose people from the server's directory

- g. In Section 2 select whether you want the person to have access to:
 - All Mail, Calendar, and To Do
 - Only Calendar and To Do
 - None
- h. In Section 3 choose the level of access you want to give to this person. Note that IMAP can only handle the mail items in your mail file.

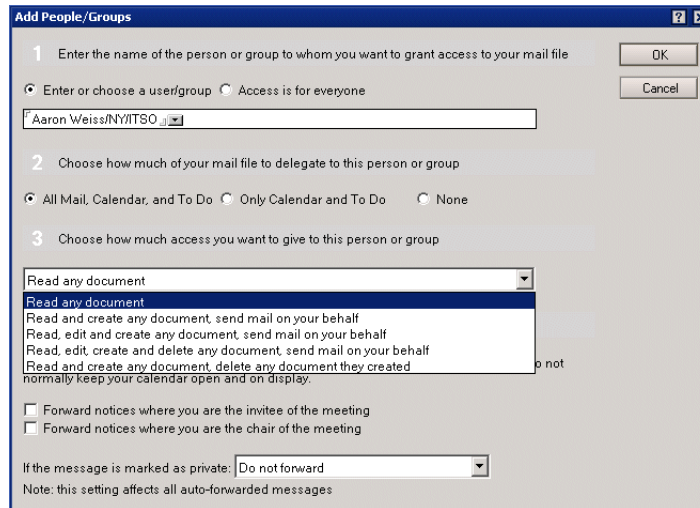


Figure 9-87 Level of access

- i. You can automatically forward your calendar notices to this person. This is not recommended for users accessing the system through IMAP.
 - j. Click OK to save the setting for this person. If you want to add another person, repeat steps d through i. The users are added to the ACL of the mail file and a request is sent to AdminP to update the delegated user's mailfile list.
4. AdminP updates the Delegated User's Mailfile List. You can expedite the running of AdminP by entering the command **tell adminp process all** at the server console.
 5. IMAP reads the new configuration and displays the new shared mail databases in the Other Users NAMESPACE. Note: IMAP users will only be able to see the accounts to which they have been delegated access. You can force IMAP to read the new configuration by restarting the service. At the server console type:


```
restart task imap
```

9.9.2 Public databases (mail-in databases)

You configure mail-in databases for IMAP access through the following steps:

1. Configure the server to start the IMAP service.
2. Configure the server to allow the use of NAMESPACE extension. It is on by default, so this should just be a matter of double-checking it.
3. Create a mail file based on the mail6.ntf template.

Important: The IMAP service only gives access to databases based on the mail6.ntf. It does not support access to NNTP or discussion databases.

4. Give a title to the database in its properties box. This is the name that will appear in the IMAP client's list of Public Folders.

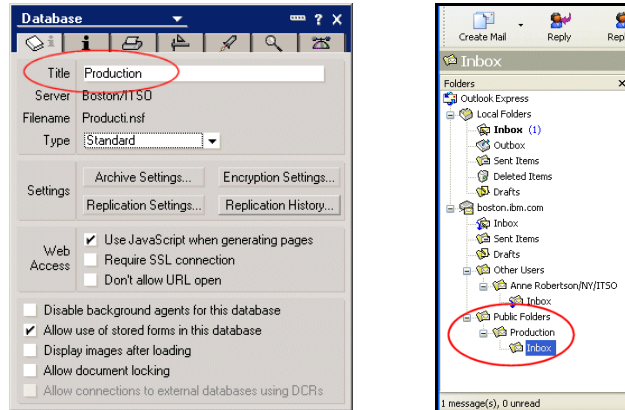


Figure 9-88 Database title corresponds to IMAP's view of the database

5. Use the mail conversion utility to enable the new database for IMAP access.
6. Create a Mail-in database document. (See Admin help, "Creating a Mail-In Database document for a new database" for more information about this.)
 - a. Give the document a Mail-in name. This is the name that will be used to send mail to the database. It may or may not correspond with the title given in the database properties, although consistency may make for easier management.
 - b. In the document, set the "Internet message storage" field to Prefers MIME.

Mail-In Database: Boston Production	
Basics Other Comments Administration	
Basics	Location
Mail-in name: Boston Production	Domain: ITSO
Description:	Server: Boston/ITSO
Internet Address: boston.production@ibm.com	File name: producti.nsf
Internet message storage: Prefers MIME	
Encrypt incoming mail: No	

Figure 9-89 Set internet message storage in mail-in db document to MIME

- c. Fill in the Location information for the mail-in db (Domain, Server, mailfilepath).
 - d. Leave “Encrypt incoming mail” set to no, unless you have issued an internet certificate for this document.
7. Add a db link to the public mail file in the server’s IMAP configuration settings document.

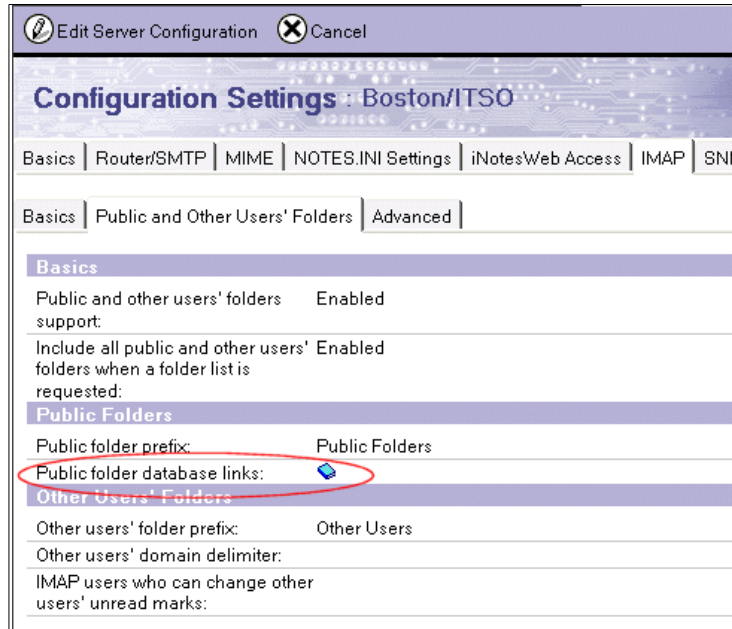


Figure 9-90 Database link to mail-in database

8. Wait for IMAP to read the new configuration and display the new public mail database in the Public Folders NAMESPACE. You can also force IMAP to read the new configuration by restarting the service. Type the following command at the console:

```
restart task imap
```

Note: Users who had already been connected to the server when the configuration change took place must shut down their IMAP client and reload it in order to see the new database in the Public Folders.

9.10 IMAP activity logging

IMAP activity logging tracks IMAP session activity, such as the user name, the server name, the IP address of the client, the number of bytes the client sent to and read from the server, and the duration of the session.

Domino writes activity logging information to the Log file (log.nsf). To create activity logging reports, you write a Notes API program to access the information in the Log file. You can also view the activity logging information by using Activity Analysis.

There are three types of activity logging records for IMAP sessions:

- ▶ Authorization records:
 - Successful login command
 - Successful auth command
 - Successful greeting command
- ▶ Checkpoint records log activity that occurs when an IMAP session has been opened for a specified length of time.
- ▶ Close records consolidate IMAP information into a single record when an IMAP session ends.

Attention: Activity logging is resource-intensive and should be used sparingly.

9.10.1 How to configure IMAP activity logging

You configure IMAP activity logging in the server configuration document using the following steps:

1. From the Domino Administrator click the Configuration tab. Expand the Server section in the navigation panel and select Configurations.
2. Select the server on which you want to enable IMAP activity logging. Click the Edit Configuration button to open the document in edit mode.
3. Click the Activity Logging tab.

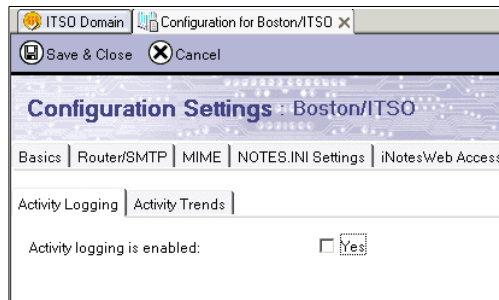


Figure 9-91 Unconfigured activity logging document

4. Click the Yes checkbox to reveal the activity logging options.

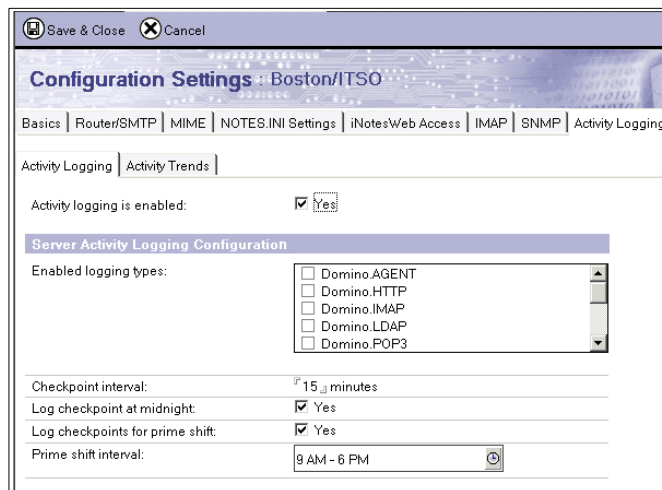


Figure 9-92 Activity logging options

5. In "Enabled logging types" select Domino.IMAP.
6. Configure logging by filling in the following 4 fields:
 - Checkpoint interval
Increases or decreases the frequency of creating Checkpoint records.
 - Log checkpoint at midnight
Automatically creates Notes session and Notes database Checkpoint records every day at midnight.
 - Log checkpoints for prime shift
Automatically creates Notes session and Notes database Checkpoint records every day at the beginning and end of a specific time period.

- Prime shift interval
Defines the times for the “Log checkpoints for prime shift” field. This should define the time period when the server is most heavily used.
7. Click Save & Close.

9.10.2 View the logging data

You can view the activity logging information by running Activity Analysis, which copies the information you request to the log analysis database (created at the time of the request on your local computer). The log analysis database includes an IMAP view for IMAP activity information. This view shows:

- Organization name
 - Server name
 - User name
 - Timestamp
 - Bytes sent and received
 - Session duration
1. In the Domino Administrator, select the Server -> Analysis tab.
 2. Expand the Tools pane, expand Analyze, and click Activity.

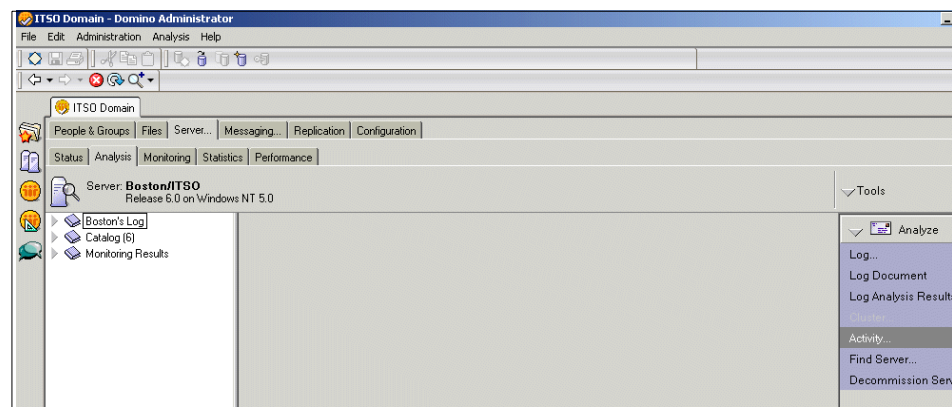


Figure 9-93 Beginning the activity logging analysis

3. By default all activities configured for logging will be in the Selected activity types field (on the right). Remove all but the Domino IMAP activity.

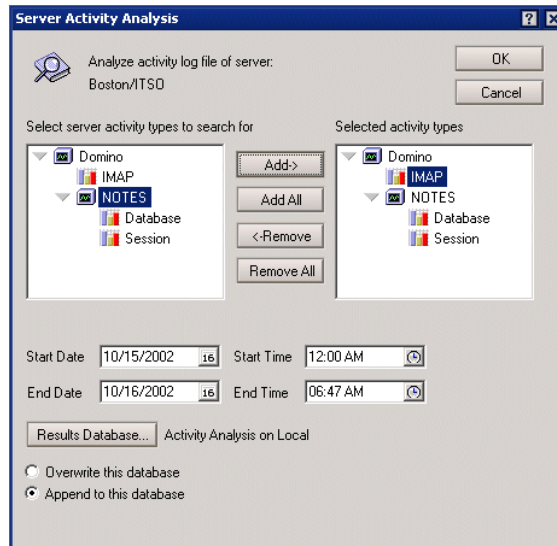


Figure 9-94 Specify scope of analysis

4. Choose the starting and ending dates and times of the activity you want to view.
5. Click the Results Database button to define the results database. Skip this step if you just want the defaults.

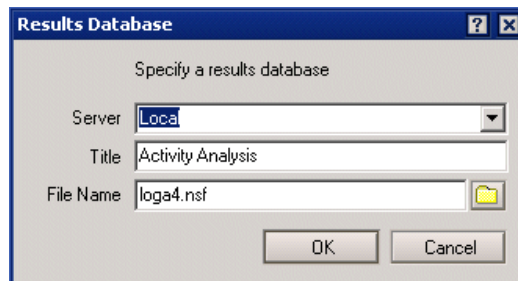
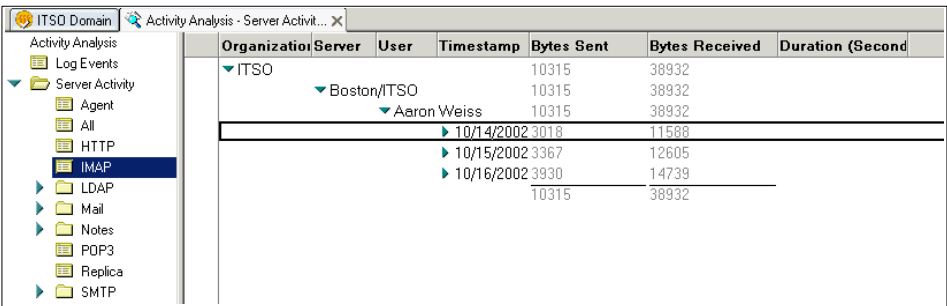


Figure 9-95 Configure the results database

6. Select whether to overwrite or append to the Results database.
7. Click OK to run the analysis and open the log analysis database.
8. When the log analysis database opens, expand the Server Activity section and click IMAP. By default all of the collapsible sections are expanded. Click the Collapse All smart icon so that you can expand the sections as needed. Click the Organization and then the server.

9. Each user will have an entry that summarizes the bytes sent and received. In order to view the days of each person’s activity expand their name.

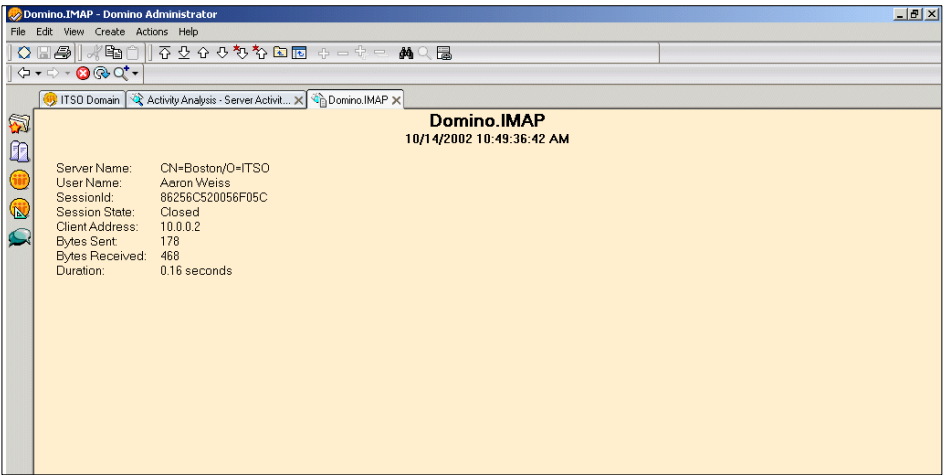


The screenshot shows the 'Activity Analysis - Server Activity' window in Domino Administrator. The left pane shows a tree view with 'IMAP' selected. The main pane displays a table of activity data for the user 'Aaron Weiss' on the 'Boston/ITSO' server.

Organization	Server	User	Timestamp	Bytes Sent	Bytes Received	Duration (Second)
ITSO	Boston/ITSO	Aaron Weiss	10/14/2002 10:18	10315	38932	
			10/15/2002 3:36	3367	12605	
			10/16/2002 3:30	3930	14739	
				10315	38932	

Figure 9-96 User activity by day

10. You can also expand each day they have connected and view each session.



The screenshot shows the 'Domino.IMAP' window in Domino Administrator, displaying details for a specific IMAP session. The session is titled 'Domino.IMAP' and occurred on '10/14/2002 10:49:36:42 AM'.

Domino.IMAP	
10/14/2002 10:49:36:42 AM	
Server Name:	CN=Boston/O=ITSO
User Name:	Aaron Weiss
SessionId:	86256C520056F05C
Session State:	Closed
Client Address:	10.0.0.2
Bytes Sent:	178
Bytes Received:	468
Duration:	0.16 seconds

Figure 9-97 A record of a single IMAP session

Tip: Use activity logging if you suspect that your users have configured their IMAP clients to hit the server every minute. This puts too much of a strain on the server. You can tell which users are the offenders by the fact that their client will have hundreds or even thousands of sessions each day.



Security

This chapter highlights the new security features available in Lotus Notes/Domino 6. This includes multi-level server administration options, agent signing capabilities, and HTTP security improvements.

10.1 Domino server security configuration

One small improvement in Domino 6 is that the server security configuration has been consolidated to one tab in the server document (the Security tab). This makes it more intuitive to configure. The tab has many areas on it, each of which is discussed in this chapter:

- ▶ Administrators
- ▶ Security Settings - no changes since R5
- ▶ Server Access
- ▶ Programmability Restrictions
- ▶ Internet Access - no changes since R5
- ▶ Passthru Use - no changes since R5

Tip: Remember that, as in R5, anyone with the netCreator or netModifier role can create or change Configuration documents. Most notes.ini parameters, not just the parameters in the pick lists, can be set via a Configuration document. For example, the ServerTasks line in your server's notes.ini file can be overwritten by an entry in a Configuration document. Configuration documents also control whether the server will accept an inbound SMTP connection.

10.1.1 Administrators

Notes 4 introduced the concept of hierarchy with hierarchical IDs. Domino R5 introduced the concept of different levels of administrator access with the Roles option in the Access Control List (ACL). Domino 6 has brought this work to completion with hierarchical levels of administrator access to servers and a hierarchical Domino Directory structure with extended access control (Extended ACL) for access to user administration.

Seven levels of administrator access to servers

In Domino R5, anyone listed in the Administrators group in the Basics tab of the Server document had full control of the server.

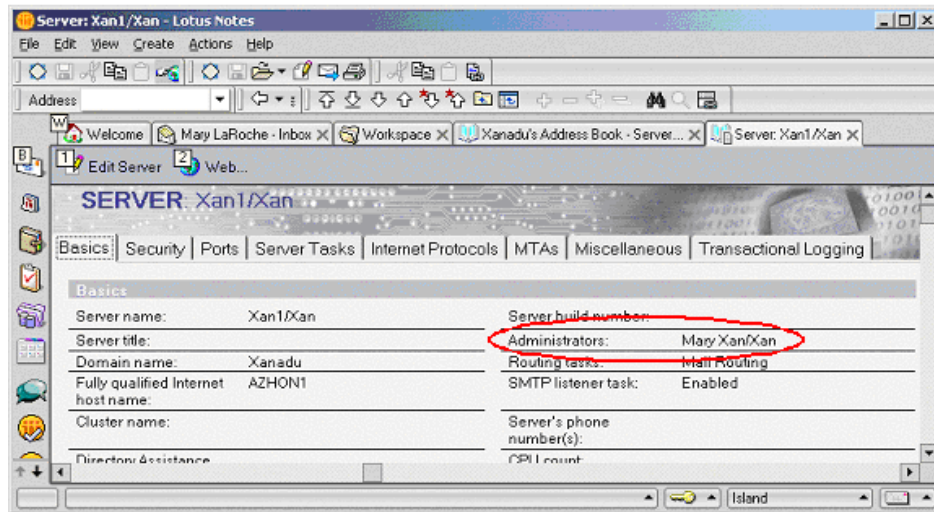


Figure 10-1 R5 server document

With Domino 6, you can specify various access levels to Domino servers for different types of administrators in your organization. For example:

- ▶ You might have a group of administrators responsible for day-to-day monitoring of the servers. These administrators are not authorized to make any changes on the servers. In R5, you were faced with the choice of either not letting them use the remote console or of adding them to the Administrators field of the Server document, knowing that they could enter commands at the console. With Domino 6, administrators can be restricted to View only, or to a limited set of commands.
- ▶ You might have a group responsible for operations who only need to enter a few operating system-level commands, but have no need to manage databases. With Domino 6, this group can be given restricted system administrator privileges.

The levels include a new, more powerful (and more dangerous) level, Full Access Administrators, that allows listed users or groups to manage databases even if they do not have Manager access in the database ACL. There are seven levels of administrator access in Domino 6. These access levels are configured on the Security tab of each Server document, so administrator access can be set per server. When you upgrade, the Administrators field on the Security tab is filled in with the same names the server had in the Administrators field on the Basics tab of the R5 server document.

Full Access Administrators is the highest level of administrative access to the server. This feature replaces the need to run a Notes client locally on a server. It

resolves such access control problems as when a manager of a database ACL has left an organization.

The administrator types have the following rights:

- ▶ Full access administrators
 - All the rights as listed below for Administrators.
 - Manager access to all databases on this server, regardless of the database ACL settings. (Note: administrators who have been granted this level of access are listed in the database ACL as having Full Administrator access.)
 - Manager access, with all roles enabled, to the Web Administrator database (WEBADMIN.NSF).

Note: Full access administrator does not allow access to encrypted data. The use of the specified user's private key is required to decrypt documents that are encrypted with public keys. Similarly, a secret key is required to decrypt documents encrypted with secret keys.

- ▶ Administrators
 - Create, update, and delete directories and links
 - Designate an administration server for databases
 - Compact and delete databases
 - Create, update, and delete full-text indexes
 - Create databases, replicas, and Master Templates
 - Get and set certain database options (for example, in/out of service, database quotas, etc.)
 - Manager access, with all roles enabled, to the Web Administrator database (WEBADMIN.NSF)
 - Use message tracking and track subjects
 - Use the console to remotely administer UNIX servers
 - Issue any remote console command

The default value for this field is the name of the administrator who initially set up the server.

- ▶ Database administrators
 - Designate an administration server for databases
 - Compact and delete databases, *even when they have no access in the database ACL*

- Create, update, and delete full-text indexes
- Create databases, replicas, and Master Templates
- Get and set certain database options (for example, in/out of service, database quotas, etc.)

Note: Database administrators are not automatically granted Manager access to databases on the server, nor do they have any access to the Web Administrator database.

- ▶ Full remote console administrators
 - Can issue any remote console commands to this server.
- ▶ View-only administrators
 - Are allowed to issue a subset of remote console commands to this server. These include only those commands that provide system status information, such as SHOW TASKS, SHOW SERVER, etc. View-only administrators cannot issue commands that affect the server's operation.
- ▶ System administrators
 - Are allowed to issue a full range of operating system commands to the server. The type and range of commands depends on the server operating system. For example, if the Domino server is a Win32 server, then these administrators can issue NT commands at the system command level prompt. Similarly, administrators for a UNIX server would be able to issue UNIX commands.

Note: This feature requires that you run the Domino server controller on the server machine.

- ▶ Restricted system administrators

Are allowed to issue only the operating system commands that are listed in the Restricted System Commands field

The type and range of commands depends on the server operating system and the tasks that restricted system administrators need to do. For example, you may want to have a restricted system administrator for managing UNIX print queues. Enter the UNIX commands for managing print queues in this field. Any names you enter in the “Restricted system administrators” field will then have access to these commands only.

Note: This feature requires that you run the Domino server controller on the server machine.

There is one more administrator access level listed in the Server document for backwards compatibility: Administer the server from a browser. This setting applies only to pre-Domino 6 servers. The Domino 6 Web Administrator client will only work on Domino 6 servers. In the case where an existing domain's Domino Directory is upgraded from R5 to Domino 6, those servers that have not been upgraded need to have this setting in their server documents so that administrators can still use their earlier versions of the Web Administrator.

To set these fields, you need to have Editor or Author with serverModifier access to the Directory.

1. With the Domino Administrator, click the Configuration tab (Figure 10-2). Expand the server section in the navigation panel and click the All Server Documents view.

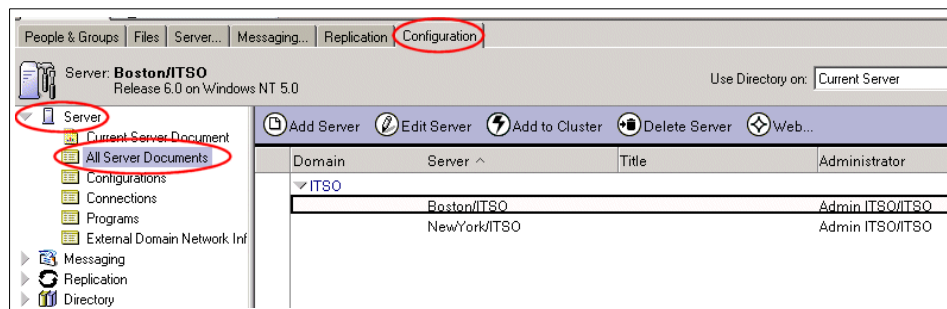


Figure 10-2 Navigate to server document in Domino Administrator

2. Double-click the server name, which opens the Server document.
3. Click Edit and then click the Security tab.

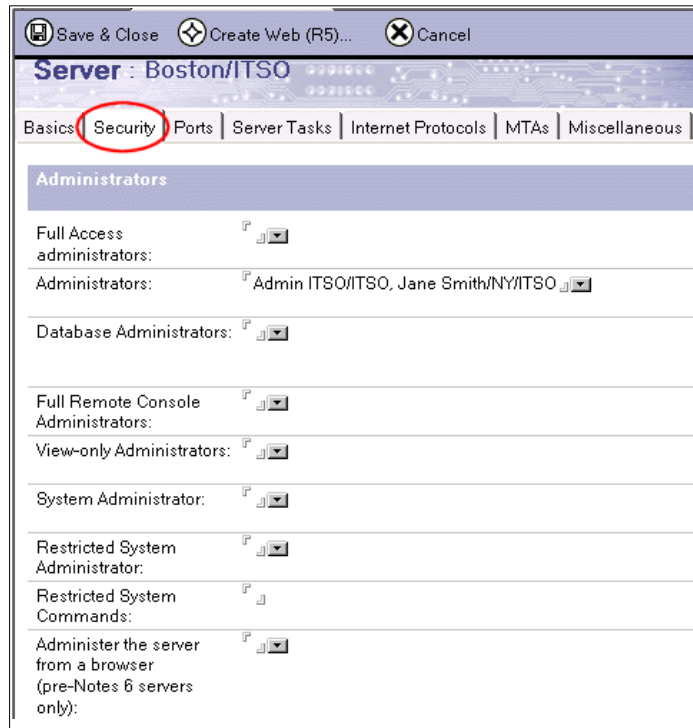


Figure 10-3 Administrators section of the security tab

4. In the Administrators section, complete one or more of the Administrator fields, and then save the document.

Tip: Implement the minimum levels of access that you will need, keep settings across servers as consistent as possible, and use groups rather than individuals, or access will quickly become very difficult to understand and manage.

Important: Be very careful about granting anyone the Full Access Administrator right. Full Access Administrators have Manager access to any database on the server, including the Domino Directory. The selection above offers several options for controlling this level of access. Pick the most restrictive option that works with your organization, and be sure to *audit* all use of this access level. Remember that anyone with Editor level or higher access to the Domino Directory can edit these fields.

When you upgrade, all the fields will be blank except the Administrators field, which operates in exactly the same way as in R5. Figure 10-3 on page 309 shows the initial default settings for the Security tab.

More about full access administrator rights

In R5, administrators could only access databases on the server if they were included in the database ACL. As a result, administrators with Windows servers sometimes resorted to using the Notes client on the server itself to correct problems with databases, such as users locking themselves out of their mail databases. Administrators on other platforms had to use other indirect approaches or live with less than optimum service to users. Agents, and the authority needed to run agents, also sometimes created problems. These problems are solved in Domino 6 with the Full Access Administrator privilege.

Full Access Administrator is the highest level of administrative access to the server. The Full Access Administrator feature replaces the need to run a Notes client locally on a server. It resolves access control problems—for example, such as those caused when the only managers of a database ACL have left an organization. With Full Access Administrator rights, an administrator automatically has manager access to all databases on a server and can correct ACL problems with his or her own client.

While Full Access Administrator rights solve some pressing Domino administration needs, a person with these rights can bypass many of Lotus Domino's key security features. These rights are not needed for everyday operation. In fact, in a high security environment and/or on a server hosting highly sensitive databases, this right should probably not be used at all.

Disabling the Full Access Administrator feature

You can specifically disable Full Access Administrator access by setting the following in the NOTES.INI file:

```
SECURE_DISABLE_FULLADMIN = 1
```

This setting disables full access administrator privilege and overrides any names listed in that field in the Server document. This NOTES.INI parameter can only be set by a user with physical access to the server who can edit the NOTES.INI file for the server. This parameter cannot be set using the server console or the remote console. You can enter this parameter with a value of 0 in the Notes.ini settings section of the Configuration document by entering SECURE_DISABLE_FULLADMIN in the Parameter field and 0 in the Value field, but it will have no effect.

Options for managing the Full Access Administrator feature

There are several ways to grant full access administrator rights and still maintain security. Pick the approach that best meets your needs. Although the server always logs use of the Full Access Administrator role, security is improved if you configure servers to send e-mail alerts to a group of people whenever the Full Access right is exercised.

The following options come from Administrator Help:

- ▶ Create a special Full Admin ID file—for example, Full Admin/Sales/Acme—and only put that name in the Full Admin field. You must then either log in with or switch to this user ID in order to gain this level of access. Optionally, you could set up this ID file to require multiple passwords.
- ▶ Create an OU-level certifier for granting full administrator access, and issue additional IDs to trusted administrators—for example, Jane Admin/Full Admin/Acme.
- ▶ Leave the Full Access Administrator field empty. Add the name of a trusted individual for emergency situations, and remove it when the situation has been resolved.
- ▶ Populate the Full Access Administrator field with a limited set of trusted administrators.

Enabling Full Access Administrator mode

In order to work in Full Access Administrator mode, an administrator must:

- ▶ Be listed in the Full Access Administrator field in the Administrators section of the Security tab in the Server document. By default, this field is empty.
- ▶ Enable Full Access Administration mode in the Administrator client. If this mode is not enabled, users will not have full administrator access to the server, even if they are listed as a Full Access Administrator in the Server document. They will instead be granted Administrator rights.

To enable Full Access Administration in the Administrator client, on the menu select Administration -> Full Access Administration; see Figure 10-4 on page 312.

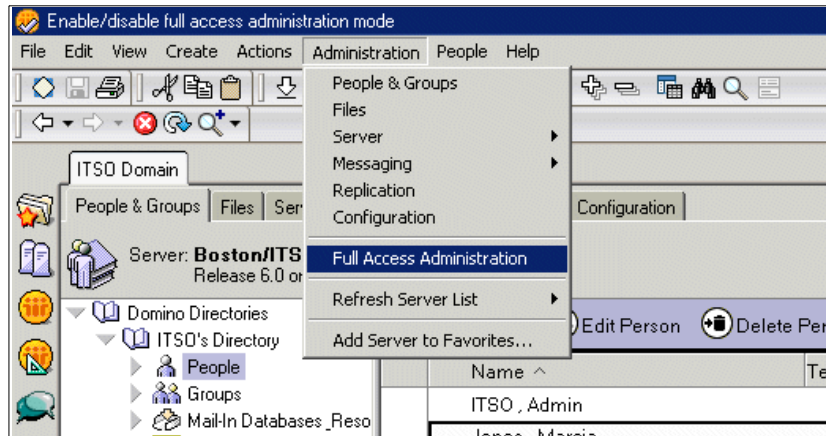


Figure 10-4 Enable full access administration

When Full Access Administrator mode is enabled, you will see a check mark next to the Full Access Administration pull-down menu item, and you will see a new bar at the top of the screen and another new bar over the Administrator menu tabs, so that you will always know if this mode has been enabled; see Figure 10-5.

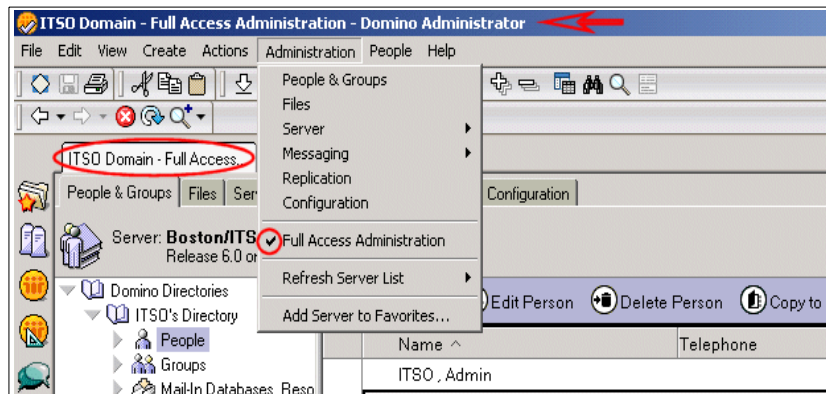


Figure 10-5 Administrator client with full access administration enabled

If you enable Full Access Administrator mode in the Administration client, this mode is also enabled for the Domino Designer and for the Lotus Notes clients. Full administrator access is also reflected in their window titles, tab titles, and status bars. The screen shot below shows the Full Access title on the Designer client.

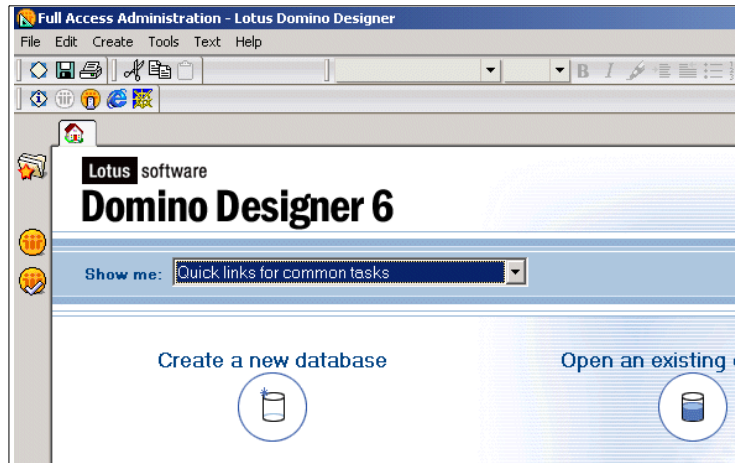


Figure 10-6 Designer client indicates full access administration is active

If you turn on Full Access Administrator mode, and connect to a server on which you are not listed as a full access administrator, you will get an error dialog box and will not have Full Access Administrator rights.

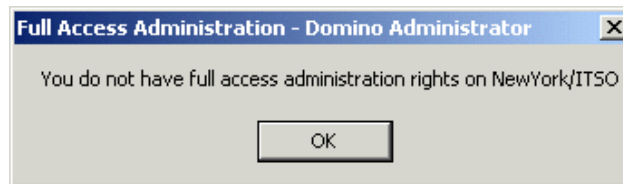


Figure 10-7 No full access administrator rights

You can switch to another server where you have Full Access rights with no problem.

10.1.2 Security settings

These work as they did in R5; see Figure 10-8 on page 314.

Security Settings	
Compare Notes public keys against those stored in Directory:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow anonymous Notes connections:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Check passwords on Notes IDs:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Figure 10-8 Security settings

Tip: It is a good idea to set Compare Notes Public Keys to Yes. Otherwise, anyone with a valid certifier can create IDs that are identical to current server and user IDs, and the server will trust the identity of those IDs. But before setting this field to Yes, be sure that your Directory contains the public keys of any servers and users not in your domain that are allowed access to the server.

10.1.3 Server access

These fields (Figure 10-9) have changed with Domino 6. A description of how they should be used follows.

Server Access	Who can -
Access server:	<input type="checkbox"/> users listed in all trusted directories
	and
Not access server:	<input type="checkbox"/> [icon]
Create databases & templates:	<input type="checkbox"/> [icon]
Create new replicas:	<input type="checkbox"/> [icon]
Create master templates:	<input type="checkbox"/> [icon]
Allowed to use monitors:	<input checked="" type="checkbox"/> [icon]
Not allowed to use monitors:	<input type="checkbox"/> [icon]
Trusted servers:	<input type="checkbox"/> [icon]

Figure 10-9 Server access fields

► Access Server

- The default value for this field is blank, which means that all users can access the server.
- If the checkbox is not selected, all users with a trusted certificate will be able to access the server (whether their name is listed in a directory or not). When the document is not in edit mode, the text “All users can access this server” appears in the field (Figure 10-10).

Server Access	Who can -
Access server:	All users can access this server
Not access server:	
Create databases & templates:	
Create new replicas:	
Create master templates:	
Allowed to use monitors:	*
Not allowed to use monitors:	
Trusted servers:	

Figure 10-10 All users can access the server

- If the checkbox is selected, the server checks all trusted directories (the primary directory and any Directory Assistance directories that are trusted for authentication) to verify that a user should be allowed to access the server.
- Valid values (separate multiple entries with commas or semicolons):
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Notes hierarchical server names
 - Groups
 - Wildcards are allowed. For example, an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.

Important: If this checkbox is not selected and you have names in the field below it, only those people will be able to access the server.

► Not access server

- Enter the names of Notes and Internet users and groups who are not allowed to access this server
- An entry in this field takes precedence over an entry in the Access server field, i.e., if the same name is entered in both fields, the individual will not be allowed to access the server.

- Valid values (separate multiple entries with commas or semicolons):
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Notes hierarchical server names
 - Groups
 - Wildcards are allowed. For example an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.
- ▶ Create databases and templates
 - The default value is blank, which means that all users can create new databases. Once a name is entered, only those listed in this field are allowed to create new databases on the server.
 - Entries are allowed to create new databases on the server.
 - Entries are allowed to create and update database templates on the server.
 - Valid values (separate multiple entries with commas or semicolons):
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Notes servers
 - Groups (including server groups)
 - Wildcards are allowed. For example an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.
- ▶ Create new replicas
 - The default value is blank, which means that no one can create new replicas.
 - Entries are allowed to create new database replicas on the server
 - An entry must appear in both the Create databases and templates field (see above) *and* the Create new replicas field in order have the correct access for creating replicas.
 - A database ACL that prohibits creation of replicas overrides the rights granted by this field.
 - Valid values (separate multiple entries with commas or semicolons):
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Notes servers
 - Groups (including server groups)
 - Wildcards are allowed. For example an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.
- ▶ Create master templates
 - The default value is blank, which means that no one can create master database templates on the server.
 - Entries are allowed to create master database templates on the server.

- An entry must appear in both the Create databases and templates field (see above) *and* the Create master templates field in order to have the correct access for creating master database templates on the server.
- Valid values (separate multiple entries with commas or semicolons):
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Notes servers
 - Groups (including server groups)
 - Wildcards are allowed. For example an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.
- ▶ Allowed to use monitors
 - The default value is * (all users), meaning that all users can set up *headline monitoring* to search databases on this server. Delete the asterisk to allow no one to use headline monitoring.
 - Entries are allowed to set up their headlines to search server databases automatically for items of interest.
 - Valid values (separate multiple entries with commas or semicolons):
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Groups
 - Wildcards are allowed. For example an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.

Attention: Headline monitoring refers to the ability of a client to search server databases. This has nothing to do with server monitoring for administrative purposes.

- ▶ Not allowed to use monitors
 - The default value is blank, meaning that no one is restricted from using monitors.
 - Entries are not allowed to set up their headlines to search server databases automatically for items of interest.
 - Valid values (separate multiple entries with commas or semicolons):
 - Use an asterisk (*) to prevent all users from using monitors,
 - Notes hierarchical user names (e.g., Jane Smith/Boston/ITSO)
 - Groups
 - Wildcards are allowed. For example an asterisk (*) followed by a certificate name: */Sales/Boston/ITSO.
- ▶ Trusted servers
 - Entries are allowed to assert the identities of users to this server. They are trusted by the current server to have authenticated those users.

- Used for remote agent access and xSP.
- Valid values (separate multiple entries with commas or semicolons):
 - Domino servers

The Trusted servers field is not used for normal user access, since users normally access a server directly. It is also not used for passthru access. The Passthru settings control this access. “Trusted servers” is used for remote agent access and in hosted environments.

10.1.4 Programmability restrictions

In R5 agents ran with the rights of their signer and could only access databases local to the server where the agent was running. In Domino 6 new agent security features increase the power (and the danger) of agents. New features include:

- ▶ Accessing remote servers
- ▶ Modifying and saving agents on the server
- ▶ Enabling scheduled agents using a Web client
- ▶ Allowing editor-level users to run LotusScript and Java agents
- ▶ Providing the ability to specify the person on whose behalf the agent is running

Tip: For a more thorough discussion of the new agent model, see “Decoding the new Notes/Domino 6 agent features,” by Julie Kadashevich. It is available on the Lotus Developer Domain (<http://www.lotus.com/LDD>).

Security for the new agent model is addressed in the programmability restrictions section on the Security tab of the server document. Whether or not programmability restrictions apply depends on how the agent is invoked. If the agent is invoked on the client, these restrictions do not apply. If the agent is invoked on the server (e.g., a scheduled agent set to run on a server), the restrictions do apply.

Two fields are provided for backwards compatibility and should only be used when the server is a pre-Domino 6 server: Run restricted Java/JavaScript/COM and Run unrestricted Java/JavaScript/COM; see Figure 10-11 on page 319.









Programmability Restrictions	Who can -
Run unrestricted methods and operations:	
Sign agents to run on behalf of someone else:	
Sign agents to run on behalf of the invoker of the agent:	
Run restricted LotusScript/Java agents:	
Run Simple and Formula agents:	
Sign script libraries to run on behalf of someone else:	
Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.	
Run restricted Java/Javascript/COM:	
Run unrestricted Java/Javascript/COM:	

Figure 10-11 Obsolete programmability fields for backwards compatibility

Tip: For easier management, create six groups, one for each of the six levels of programmability privileges, and use the group names instead of individual names.

When making entries in these fields, be very careful, because the default setting (blank) either grants or denies the privilege to everyone, depending on the field. For example, blank in “Run Simple and Formula agents” allows the privilege to everyone, while blank in “Run restricted LotusScript/Java agents” grants the privilege only to the current server, Lotus Notes Template Development, and any users or groups in “Run Unrestricted LotusScript/Java agents.” The field level help is very detailed for these fields and should be used to find the meaning of each field. For example, click on the label for the first field, “Run unrestricted methods and operations”, and you will see what is shown in Figure 10-12 on page 320.

Server : NewYork/ITSO

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | Administration

Administrators	Programmability Restrictions	Who can -
Full Access administrators:	Run unrestricted methods	
Administrators:	Select the names of users who can run agents without restrictions. This includes all programmable languages and interfaces: LotusScript, Java, JavaScript, COM, and DIIOP. The default (blank) means no users can do this. Users with this access can run any agent, even ones that can access the system by manipulating system time, file I/O, and operating system commands. The current server and the Lotus Notes Template Development id are granted unrestricted access.	
Database Administrators	Run unrestricted methods	
Full Remote Console Administrators:	Run restricted LotusScript/Java agents:	
View-only Administrators:	Run Simple and Formula agents:	
System Administrator:	Sign script libraries to run on behalf of someone else:	
Restricted System Administrator:	Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.	
Restricted System Commands:	Run restricted Java/JavaScript/COM:	
Administer the server from a browser	Run unrestricted Java/JavaScript/COM:	

Figure 10-12 Sample of field level help

The six fields in the programmability restrictions section are organized hierarchically with regard to privileges (the higher it is on the form, the more privileges it has). A user or group name in one field automatically receives the privileges associated with the fields below that field (Figure 10-13).

Programmability Restrictions	Who can -
Run unrestricted methods and operations:	
Sign agents to run on behalf of someone else:	
Sign agents to run on behalf of the invoker of the agent:	
Run restricted LotusScript/Java agents:	
Run Simple and Formula agents:	
Sign script libraries to run on behalf of someone else:	

Figure 10-13 Default programmability restrictions

- ▶ Run unrestricted methods and operations
 - The default value is blank, meaning that no one (other than the current server and Lotus Notes Template developers) has these privileges.
 - This access is enabled by default for the current server and Lotus Notes Template developers.
 - Entries are allowed to select, on a per agent basis, one of three levels of access for agents signed with their ID. Users with this privilege select one of the following access levels when they are using Domino Designer 6 to build an agent:
 - Restricted mode
 - Unrestricted mode
 - Unrestricted mode with full administration rights
 - Only users who have this access can choose an option other than “Do not allow restricted operations” when creating agents.
 - Caution: Users listed in this field can perform all agent operations, including those that can compromise security. Only a small number of the most trusted users should have these rights on a production server.

To have the ability to run agents in unrestricted mode with full administration rights, the agent signer should:

- i. Be listed in this field, or in the Full Access Administrator field.
- ii. Have this mode selected in the Agent Builder.

Being listed in Full Access Administrator list alone is not sufficient to run agents in this mode.

Note: If users in this list are also listed as a database administrator in the Server document, they are allowed to perform database operations without having to be listed explicitly in the database ACL (for example, they can delete databases without being listed in the ACL of those databases).

- ▶ Sign agents to run on behalf of someone else
 - The default value is blank, which means that no one can sign agents in this manner.
 - Entries are allowed to sign agents that will be executed on *anyone* else's behalf.
 - Caution: Users with this right can gain access to the data of another person, as well as impersonate someone (as the sender of mail or creator of documents).

- ▶ Sign agents to run on behalf of the invoker of the agent
 - The default value is blank, which means that everyone can sign agents invoked in this manner (this is for backwards compatibility).
 - Entries are allowed to sign agents that will be executed on behalf of the invoker, when the invoker is different from the agent signer.
 - This setting is ignored if the agent signer and the invoker are the same.
 - This is used currently only for Web agents.
- ▶ Run restricted LotusScript/Java agents
 - The default value is blank, which means no one can run restricted LotusScript/Java agents.
 - Entries are allowed to run agents created with LotusScript and Java features, but excluding privileged methods and operations, such as reading and writing to the file system.
 - The majority of users should be included in this field.
- ▶ Run Simple and Formula agents
 - The default value is blank, which means that all users are allowed to run simple and formula agents.
 - Entries are allowed to run to run simple and formula agents, both private and shared. If there are entries in this field only these entries will be allowed to run simple and formula agents. All others will be prevented from doing this on the server.
- ▶ Sign script libraries to run on behalf of someone else
 - The default value is blank, which means that all users are allowed this privilege. For the purpose of backwards compatibility leave the field empty, to allow all.

10.1.5 Internet access

This works as it did in R5.

10.1.6 Passthru use

This works as it did in R5.

10.2 Workstation security

Just as in R5, you use an execution control list (ECL) to set up workstation data security. An ECL protects user workstations against active content from unknown or suspect sources, and can be configured to limit the action of any active content that does run on workstations. The ECL determines whether the signer of the code is allowed to run the code on a given workstation, and defines the access that the code has to various workstation functions. For example, an ECL can prevent another person's code from running on a computer and damaging or erasing data.

Administering ECLs in Notes 6 is much more flexible than it was in R5. Because they have been incorporated into the policies structure, you can easily apply different settings to different groups of users. Changes to the ECL are pushed out automatically when you make a change to the security settings document. Each time a client authenticates with the server it checks for updates to the policies and implements them if there are any. You can also set up the ECL so that end users cannot change it in order to bypass the security standards of the organization.

Your goal as an administrator is to limit the number of trusted signers for active content, and the access that active content has to user workstations. To accomplish this goal, limit the number of trustworthy signers in your organization and ensure that workstation ECLs trust only those signers.

For each signature, the ECL contains settings that control the actions that active content signed with that signature can perform and the workstation system resources it can access. For a complete listing of the default ECL settings look in the Admin help file, "Default ECL settings." Do not change the default ECL settings for the preconfigured ECL entries. The certificates for those IDs have been hard-wired into the Notes client code.

Table 10-1 Preconfigured entries in Workstation ECL

Preconfigured ECL entry	Recommendation
BT Mail and Calendar Migration Tools/Lotus Notes Companion Products	Can be removed if your organization will not be using any of the Binary Tree migration tools or the Binary Tree companion products.
Domino Unified Communications Services/Lotus Notes Companion Products	Do not remove or modify.
Lotus Fax Development/Lotus Notes Companion Products	Leave in for future possibilities.

Preconfigured ECL entry	Recommendation
Lotus Notes Template Development / Lotus Notes	Do not remove or modify.
Sametime Development/Lotus Note Companion Products	Leave in for future possibilities.

You will need to work closely with Notes developers in your organization to determine what kind of access their applications require to the workstation. Test their applications with different ECL levels to determine the minimum amount of access they require.

10.2.1 General guidelines to create secure ECLs

- ▶ Do not grant access to unsigned content. This creates a security hole that allows potentially harmful code, malicious or otherwise, to access user workstations. Keep the default access options for unsigned content.
- ▶ Do not let your users trust unsigned content. To prevent users from changing their ECLs—for example, by giving access to unsigned content, or to content signed by signers who are not listed in the ECL—deselect “Allow user to modify” in the Administration ECL.

Important: In large organizations it may cause difficulties to lock the users out of their ECLs. Some departments may have developers who want to quickly set up a workflow database (something Domino is so good for). There may be hundreds of these kinds of developers. If you lock users out of their ECLs you may end up with a flood of calls about the new application not working, frustrate departmental developers, and thereby discourage one of the best features of Domino. The security needs of the organization must be carefully analyzed when making a decision about this setting.

- ▶ Know your signers. Trusting signed active content, especially from other organizations, is risky. Before adding an active content author to an ECL, decide if you trust that the author has created safe code.
- ▶ Create a separate certifier for an organizational unit to issue IDs specifically for users who must sign templates and applications—for example, Enterprise ECLApp Signer/West/Acme. Then users who create templates and applications use those IDs to sign templates and applications. You can then set up the administration ECL to trust any user in that special organizational unit, or fine-tune it on a per-user basis.

10.2.2 Security settings documents for ECLs

An ECL is defined in a security settings document, which is then applied through a policy. The other part of the security settings document controls password settings for both the notes IDs and HTTP access. For more information about policies and setting documents, see Chapter 15, “Policy-based administration” on page 449 and 16.2, “Making use of policies” on page 493.

1. With the Domino Administrator go to the People and Groups tab, click Settings in the navigation pane, and then click Add Settings -> Security. This will open a new Security Settings document, shown in Figure 10-14.

Figure 10-14 Security Settings document

2. Fill in the Name field on the Basics tab and then click Execution Control List.
3. Click Edit and examine the default ECL. Click on the names in the When signed by: box and notice the differences in the rights each one is granted in the Allow: column. Each signer has rights to Workstation security, Java applet security, and JavaScript security. There are hundreds of possible combinations of these settings. Note that the administrator account has rights to everything so that he or she can manage the workstation (Figure 10-15 on page 326).

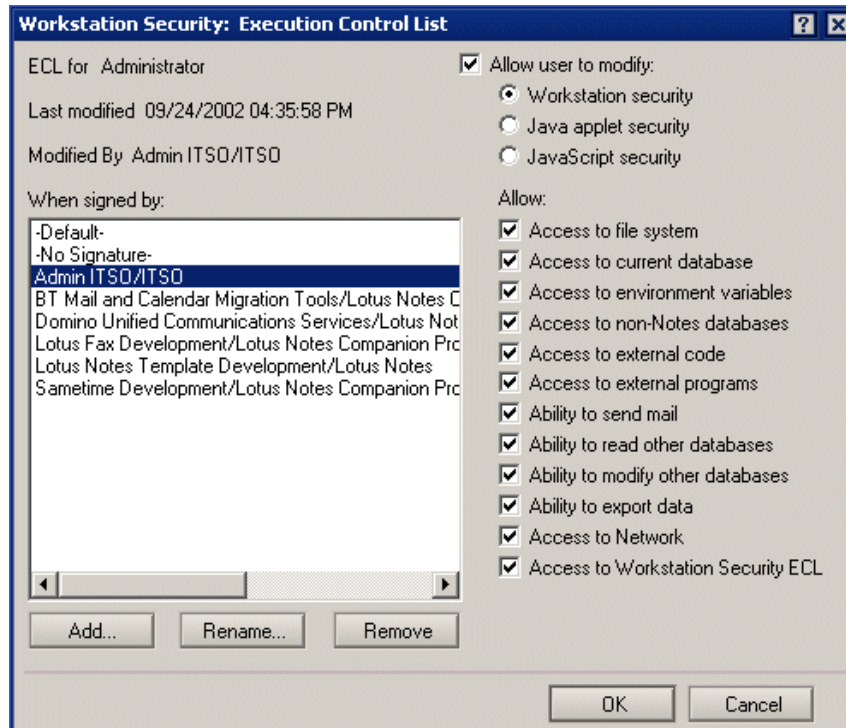


Figure 10-15 Default Admin ECL

4. Cancel out of the Default Execution Control List.
5. Click New to create a new Admin ECL (Figure 10-14 on page 325), which will be based on the Default ECL. Enter a name for the new Admin ECL (Figure 10-16) and click OK.

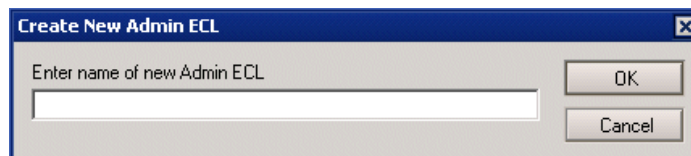


Figure 10-16 New Admin ECL name

6. The new ECL will not have a signature that is automatically configured for full access to workstations. Enter the name of the administrator for this ECL by clicking Add and choosing the appropriate name from the organization's directory. Change every setting for the administrator to "Allow." Be sure to do this for all three sections (workstation, Java applet, and JavaScript), but especially be sure to enable this account to modify the ECL.

7. It is best to leave the Default and No Signature settings as they are. Also, you will notice some Lotus signers and one setting called BT (Binary Tree) mail and Calendar Migration Tools. It is easiest to leave these as they are.
8. Add any other signers and change their access as appropriate. We recommend that you create a unique organizational unit with special IDs for signing Notes applications. Enter those IDs or OUs in as well. Make sure that people who have access to those IDs can be trusted to write good code.
9. Decide whether you want to lock users out of their ECL. Deselect the checkbox “Allow user to modify” if you want to lock them out. This will prevent your users from overriding the organizational policy and inadvertently causing damage to their workstation and perhaps many others as well. This checkbox applies to all of the ECL settings—so they will either be able to override all of them or none of them. Figure 10-17 shows what the users will see if they have been locked out of their ECL and then receive an Execution Security Alert. They have no option but to disallow the action.

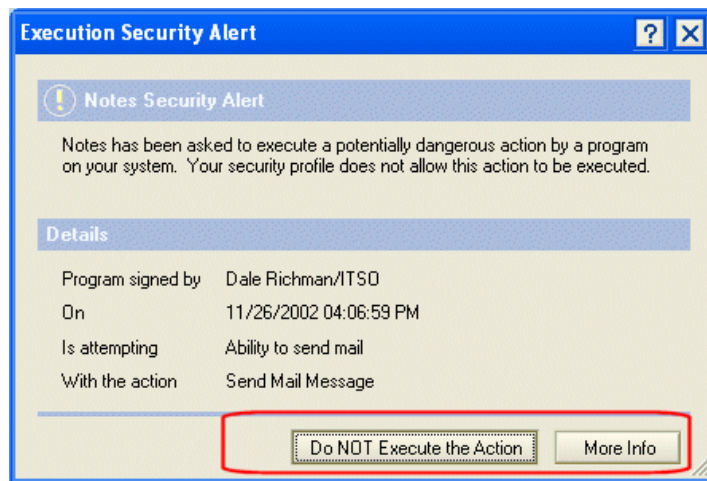


Figure 10-17 ESA for a user who is locked out of his/her ECL

10. Choose whether you want the ECL to be refreshed or replaced when users' ECLs are next checked.

Choose refresh if you simply modified one setting or added someone. Refresh does not delete entries in the workstation ECL that do not appear in the Administration ECL.

Choose replace if you want to make sure that a signer is going to be removed from the ECL. For example, if your users had the right to modify their ECL, they may have added inappropriate people as trusted signers.

11. Choose how often the users' ECLs should be updated (once daily, when the Admin ECL changes, or never).

Tip: You can prevent your users from modifying their ECL and still give them enough access to create their own Domino databases and agents. To do this, add the entry

<ECLOwner>

as an entry in the Admin ECL.

Give that entry rights to everything, except "Access to workstation security ECL" on the workstation security page.

Be sure to deselect Allow Owner to Modify.

The next time the ECL is updated, the user's own name will replace <ECLOwner> and will be given the appropriate rights.

10.2.3 Check the security settings on the workstation

Once you have created an Admin ECL, you should check to make sure that the settings are exactly what you thought they were going to be. Apply the security settings document in a test environment and check the security settings on one of the affected workstations:

1. Once the Notes client has authenticated with the server, open the security settings on the client by clicking File -> Security -> User Security. Enter the Notes password when prompted; see Figure 10-18 on page 329.

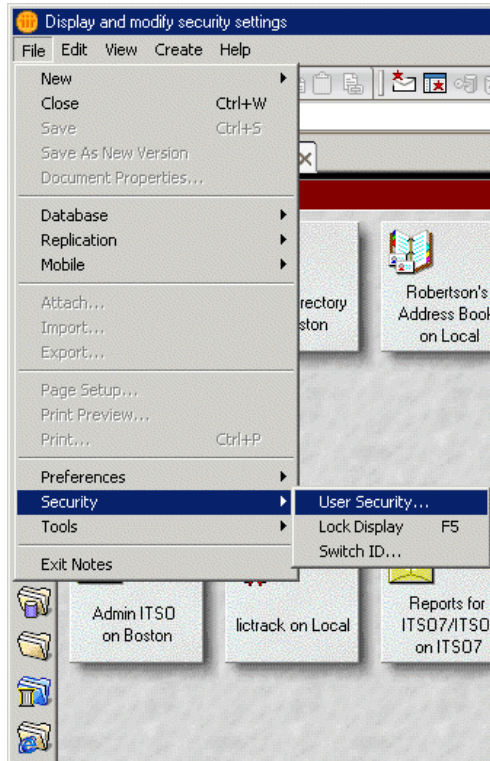


Figure 10-18 Navigate to the workstation security settings

2. All of the security options for end users are available from this screen:
 - Security Basics (password options, automatic logout, id renewal requests)
 - Your identity (aliases, internet address, Notes certificate information, Smartcard information)
 - Identity of others (certificates of others, including Certificate Authorities)
 - What Others Do (Execution Control List - using Workstation, using Applets, using JavaScript)
 - Notes data (local encryption of databases and special document encryption keys)
 - Mail (security options for both Notes and internet mail)

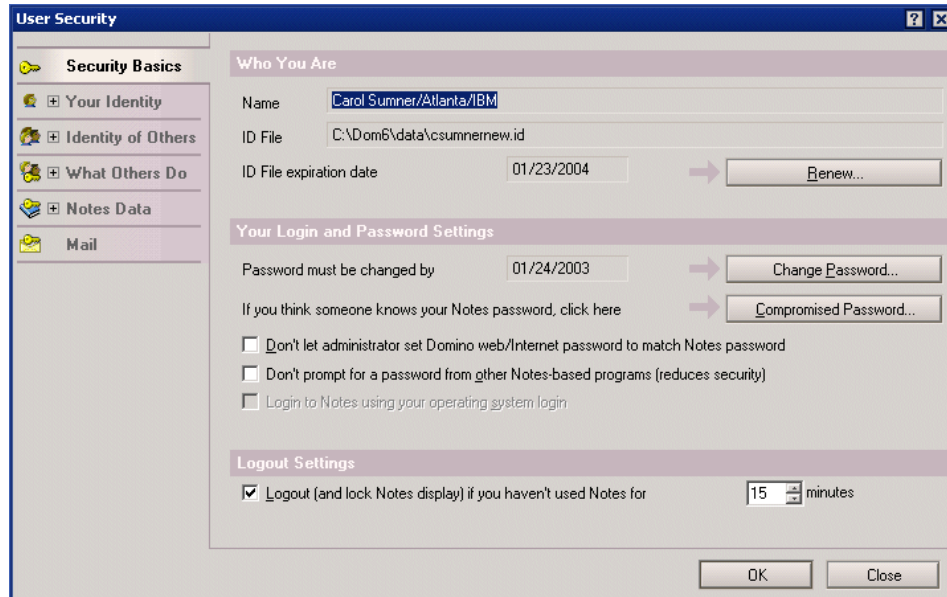


Figure 10-19 User Security menu

3. The Execution Control List is found under the menu item What Others Do (Figure 10-19). There are three pages of security choices in this section (Figure 10-20 on page 331, Figure 10-21 on page 331, and Figure 10-22 on page 332), which correspond to the three pages of security choices in the security settings document in the Domino Directory.

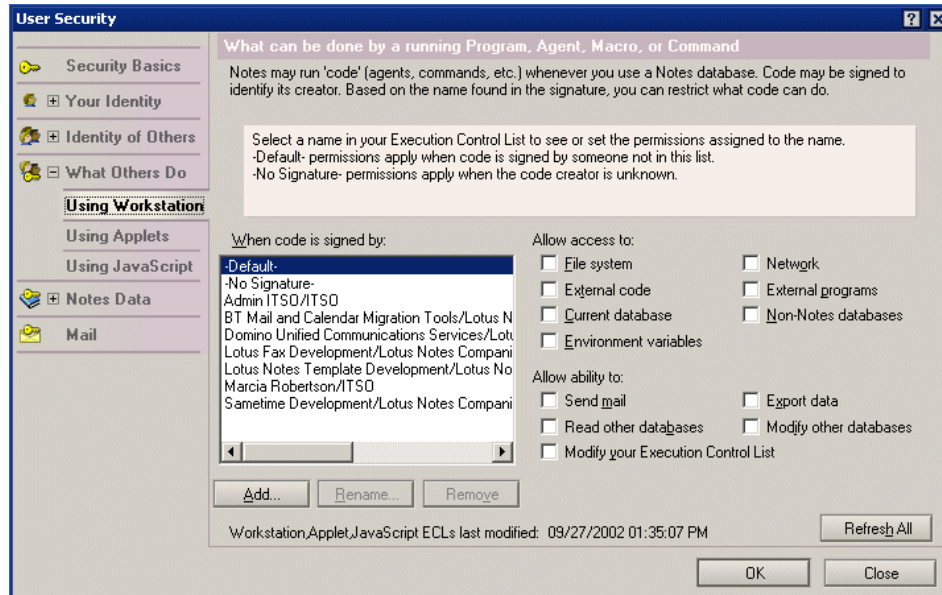


Figure 10-20 What can be done by a running Program, Agent, Macro, or Command

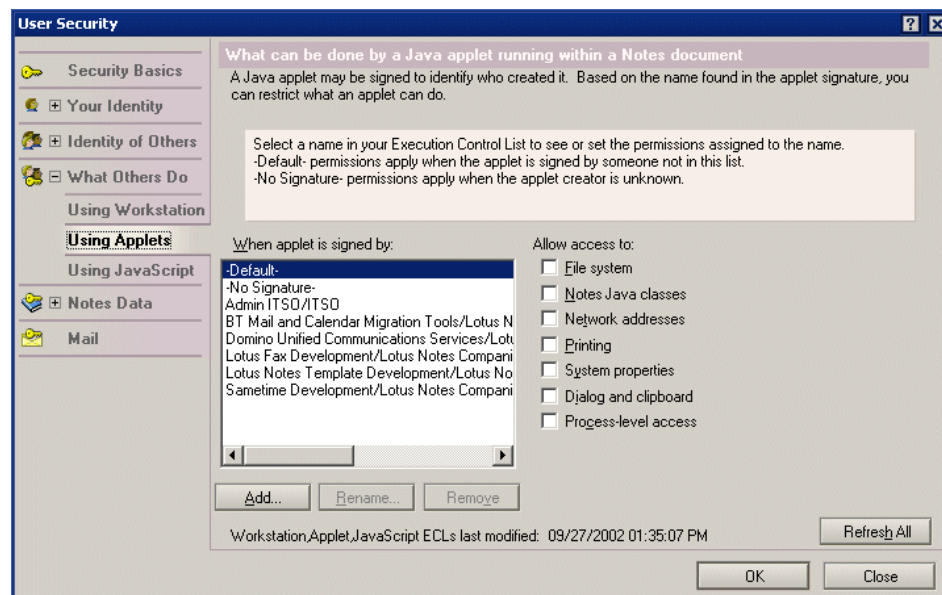


Figure 10-21 What can be done by a Java applet running within a Notes document

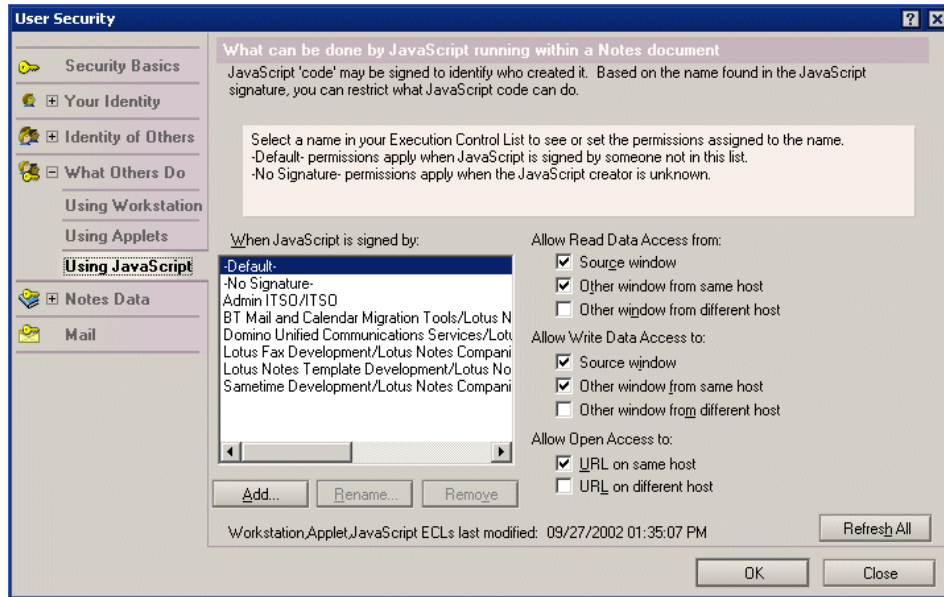


Figure 10-22 What can be done by JavaScript running in a Notes document

4. Make sure that the user's name appears in the signature boxes and that the other settings are what you expected them to be. If you deselected "Allow user to modify ECL" in the security settings document, the checkboxes on the right side of the pages and the buttons to Add, Rename, and Remove will be grayed out (Figure 10-23 on page 333).

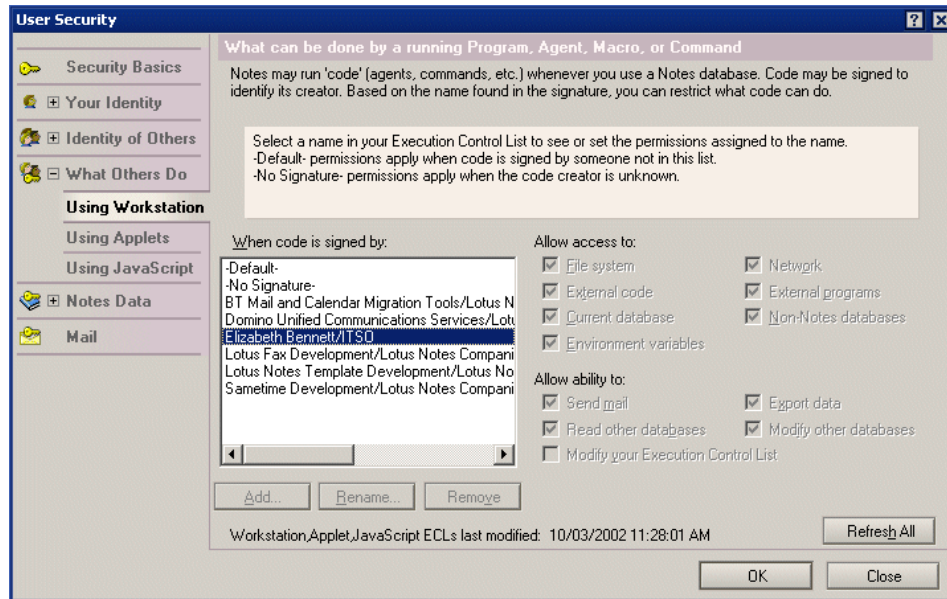


Figure 10-23 Sample ECL where the user has access to everything but the ECL itself

10.2.4 Notes Client security - automatic logout

One way to help users keep their Notes clients and data secure is to set up automatic logout. As an administrator you can create a policy that all Notes ID files will lock after x number of minutes of inactivity. When your users walk away from their workstations for lunch or at the end of the day, other people with access to their workstations will not be able to use their Notes ID. A logout screen will appear and users will have to re-enter their password before using Notes again.

Users can also set this up through the security tool in their client (File -> Security -> User Security -> Basics).

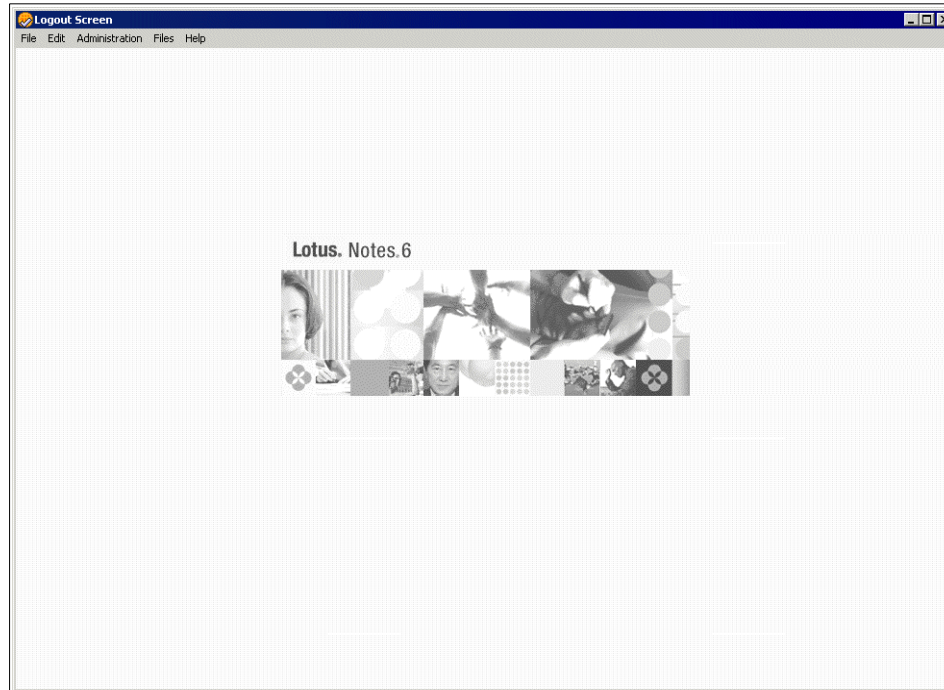


Figure 10-24 Logout screen

You will need to balance usability with organizational security needs when configuring this setting. If you configure the client to log out the ID after 5 minutes of inactivity, your users may not be very happy, although your security team may be ecstatic.

Configure automatic logout

1. With the Administrator client or the Notes client, open a Desktop Settings document or create a new one.
2. Click Preferences -> Basics (Figure 10-25 on page 335).

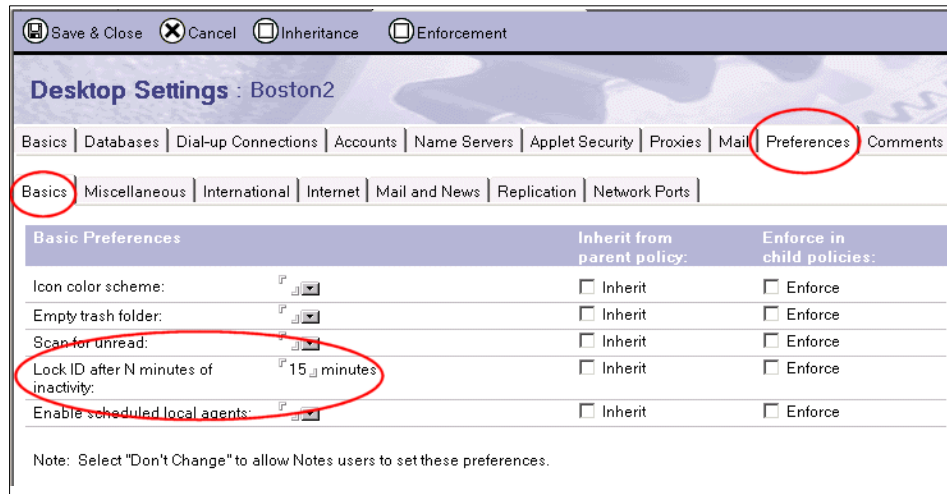


Figure 10-25 Automatic logout configuration

Note: The default setting for automatic logout is 15 minutes. Users can change this setting so that it does not log them out automatically.

10.2.5 Forcing encryption of local replicas

Many organizations hesitate to allow their users to have local replicas of their mail files and other databases because they consider it a security risk for those databases to be on a machine that is physically not secured by the organization. If your users have laptops that they travel with or take home, or if they use personal computers at home to check their e-mail or do other work, you can reduce the security risk by configuring their workstations to always encrypt local replicas.

Forcing encryption of local replicas is done through a Desktop Settings document, which then must be applied to users through a policy. If the organization has a security standard for data that is taken off site, this is an easy way to help your users meet that standard.

Changing the setting

1. With the Administrator or Notes client, open a Desktop Settings document or create a new one.
2. Click Preferences -> Replication.

3. Click the down arrow next to the Encrypt replicas: field and select Locally encrypt (Figure 10-26). This will make the client automatically encrypt local replicas with the option “Do not encrypt”.

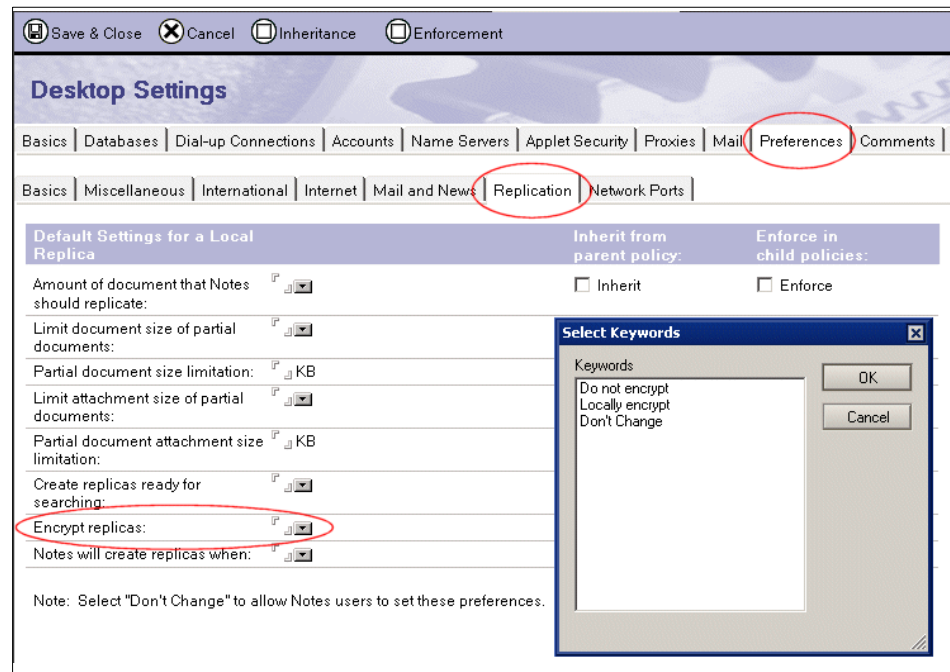


Figure 10-26 Forcing local encryption of replicas

4. Once you have selected to encrypt replicas locally, another field appears in which you can choose the level of encryption for local replicas. Medium encryption is a good choice (Figure 10-27 on page 337) because it provides more security, but with very little performance degradation.

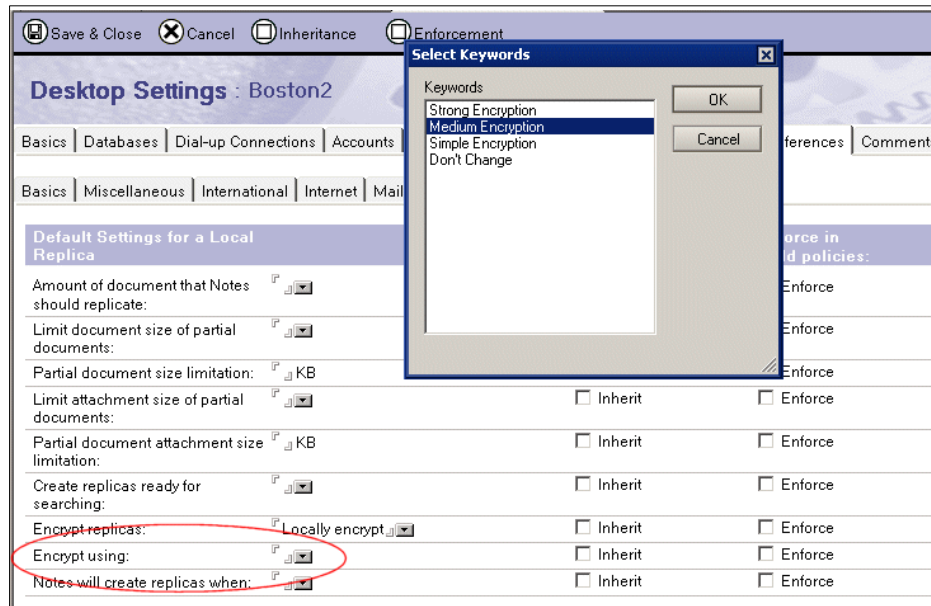


Figure 10-27 Encryption level for local replicas

5. Click Save -> Close. If this Desktop Settings document has already been applied through a policy, you do not need to do anything else. The setting will automatically be updated for those users. If not, see Chapter 15, “Policy-based administration” on page 449 for a discussion of how to apply a settings document through a policy.

10.2.6 Notes browser security

Notes can be used as a Web browser and should be configured with appropriate security settings if it is. These settings are configured in a Desktop Settings document and then applied through a policy. Whereas an ECL controls what active content in a Notes document can do, the Desktop Settings control what active content in a Notes browser window can do.

1. With the Administrator or Notes client, open a Desktop Settings document or create a new one.
2. Click Applet Security (Figure 10-28 on page 338).
3. In the Trusted hosts field enter which hosts will be allowed to execute Java applets through the browser. You can use a wildcard in order to allow all hosts within a particular domain to run applets.

4. Configure the Network access for trusted and untrusted hosts. Remember that by allowing access you are opening a window to your entire network environment.
5. Configure the Trust HTTP proxy. If you have not configured Notes to use an HTTP proxy, you should select no or leave it blank.

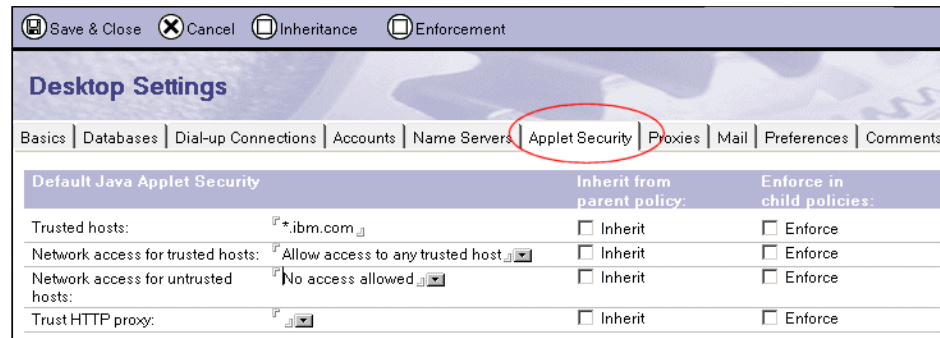


Figure 10-28 Sample Applet Security settings in Desktop Settings

After you have saved the settings document and the client re-authenticates with the server, you can verify that the settings were accepted by viewing the location document of the workstation.

1. In the lower right corner of the Notes application, click the Location field and then click Edit Current (Figure 10-29).

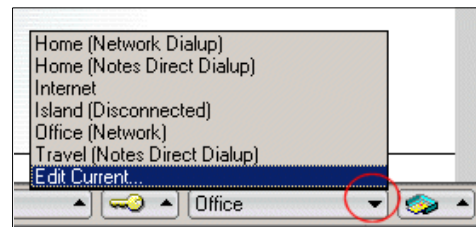


Figure 10-29 Edit current location document

2. Once the location document opens, click Advanced -> Java Applet Security (Figure 10-30 on page 339). Review the settings and verify that they match the Desktop Settings document.

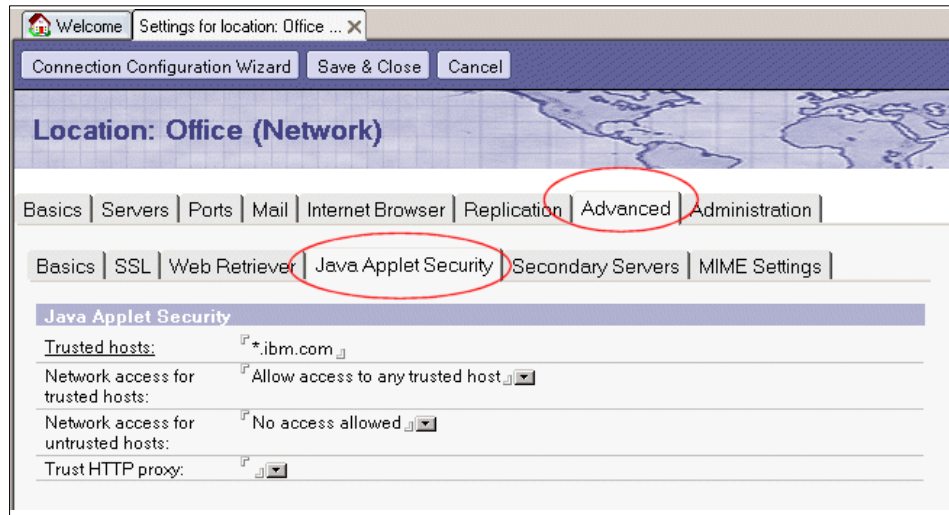


Figure 10-30 Corresponding Java Applet security in a location document

You can also look in the local log file for the user to verify that it is pulling changes down (Figure 10-31).

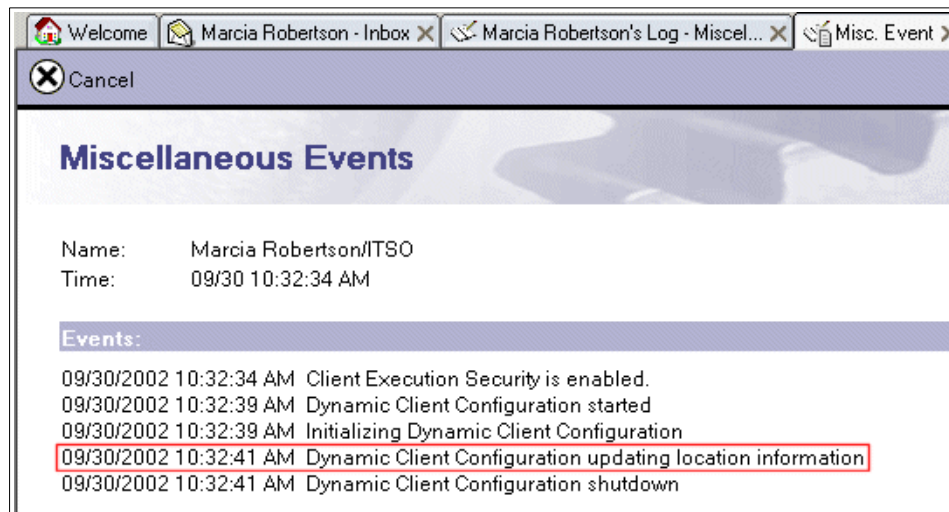


Figure 10-31 Local log file records Dynamic Client Configuration

10.3 Web security

Keeping your Domino Web server safe from attack is your biggest security challenge. Domino R5 kept Web users from accessing the operating system and enforced Domino access control on the server and each database. Domino 6 goes further and protects your server from HTTP protocol attacks. However, as in Domino R5, proper configuration is essential for Web server security.

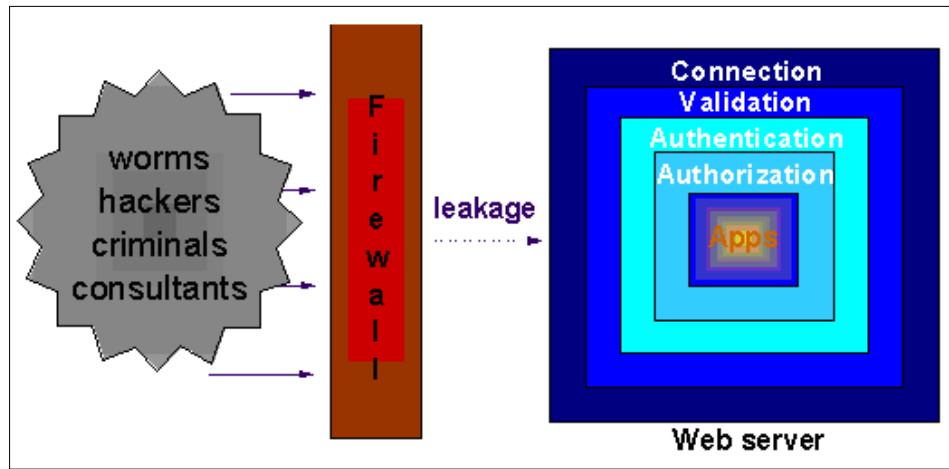


Figure 10-32 HTTP security model

Think of Web server security as having four layers:

- ▶ Connection - make sure that connections are available for clients.
- ▶ Validation - make sure the connection requests are using a valid protocol.
- ▶ Authentication - make sure the client is who it says it is.
- ▶ Authorization - make sure the client is allowed to use the application.

The improvements of Domino 6 are found in the connection and validation layers of Web server security.

All Web security settings are found in the server document on the HTTP tab, which is a subset of the Internet protocols tab. It is quite a large document, with 12 different areas of configuration.

1. With Domino Administrator, click Configuration, expand the Server section in the navigation panel, and click All Server Documents. Select the server you want to configure and then click Edit Server (Figure 10-33 on page 341).

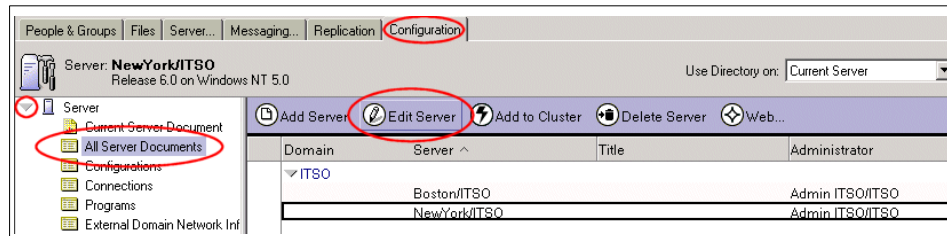


Figure 10-33 Navigate to a server document

2. Select Internet Protocols -> HTTP (Figure 10-34).

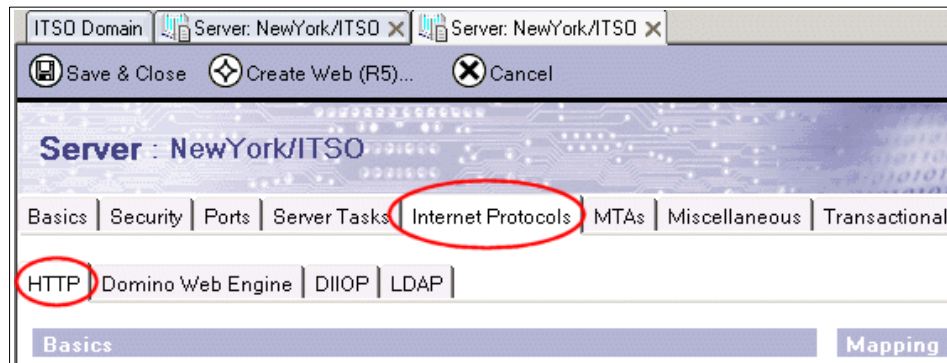


Figure 10-34 Finding the HTTP settings in the server document

3. To find the HTTP settings that have to do with the connection and validation layers of security, use the scroll bar on the right of the screen and scroll down to the bottom of the page (Figure 10-35 on page 342).

Save & Close Create Web (R5)... Cancel	
Referer log: <input type="text" value="referer"/>	User agents: <input type="text" value=""/>
Error log: <input type="text" value="error"/> (R4 and R5 only)	Return codes: <input type="text" value=""/>
CGI error log: <input type="text" value="cgi-error"/>	Hosts and domains: <input type="text" value=""/>
<div> <div> Timeouts </div> <div> R5 Timeouts </div> </div>	
HTTP persistent connections: <input checked="" type="checkbox"/> Enabled	Input timeout: <input type="text" value="2"/> minutes
Maximum requests per persistent connection: <input type="text" value="5"/>	Output timeout: <input type="text" value="20"/> minutes
Persistent connection timeout: <input type="text" value="180"/> seconds	CGI timeout: <input type="text" value="5"/> minutes
Request timeout: <input type="text" value="60"/> seconds	Idle thread timeout: <input type="text" value="0"/> minutes
Input timeout: <input type="text" value="15"/> seconds	
Output timeout: <input type="text" value="180"/> seconds	
CGI timeout: <input type="text" value="180"/> seconds	
<div> <div> Network Settings </div> <div> HTTP Protocol Limits </div> </div>	
Listen queue size: <input type="text" value="512"/>	Maximum URL length: <input type="text" value="4"/> kilobytes
Maximum number of concurrent network sessions: <input type="text" value="2000"/>	Maximum number of URL path segments: <input type="text" value="64"/>
IP address allow/deny priority: <input checked="" type="checkbox"/> Allow	Maximum number of request headers: <input type="text" value="48"/>
IP address allow list: <input type="text" value=""/>	Maximum size of request headers: <input type="text" value="16"/> kilobytes
IP address deny list: <input type="text" value=""/>	Maximum size of request content: <input type="text" value="10000"/> kilobytes (specify 0 to allow unlimited content)

Figure 10-35 Default HTTP security settings

10.3.1 Protecting your Web server at the connection level

At the HTTP connection level, attackers are probing for weaknesses or are trying to overwhelm your server so that it can no longer respond to connection requests. Some of these weaknesses may be at the operating system level. Operating system level attacks, while extremely serious, are outside the scope of Domino, so we do not discuss them here.

Trying to overwhelm your server, commonly called a Denial of Service (DoS) attack, may come in the form of a huge number of connection attempts, worm “storms,” or a connection monopoly. Domino 6 protects you from such attacks by the following methods:

1. Enforcing more types of network timeouts and setting stricter default limits on those timeouts
2. Enabling HTTP persistent connections
3. Network settings with client IP address filtering

Network timeout settings

Network timeout settings protect your server from attackers who use up server resources by opening or partially opening multiple sessions. Timeouts are more detailed and the defaults are stricter than in R5. The Domino 6 Server document includes the R5 settings for backwards compatibility with R5 servers (Figure 10-36 on page 343).












Timeouts		R5 Timeouts	
HTTP persistent connections:	<input type="checkbox"/> Enabled 	Input timeout:	<input type="checkbox"/> 2  minutes
Maximum requests per persistent connection:	<input type="checkbox"/> 5 	Output timeout:	<input type="checkbox"/> 20  minutes
Persistent connection timeout:	<input type="checkbox"/> 180  seconds	CGI timeout:	<input type="checkbox"/> 5  minutes
Request timeout:	<input type="checkbox"/> 60  seconds	Idle thread timeout:	<input type="checkbox"/> 0  minutes
Input timeout:	<input type="checkbox"/> 15  seconds		
Output timeout:	<input type="checkbox"/> 180  seconds		
CGI timeout:	<input type="checkbox"/> 180  seconds		

Figure 10-36 HTTP timeouts

Timeouts

As you can see, the default input and output timeouts are much shorter in Domino 6, and more specific timeout checks have been added. For example, the Request connection timeout setting protects your server from DoS attacks that open HTTP connect requests and do not complete them.

We recommend that you begin with the default Domino 6 timeout settings and only change them if you have a problem with valid users timing out.

Persistent connections

HTTP persistent connections are a new feature of the HTTP 1.1 protocol that allow a server that is running short of resources to use a single connection to service multiple browser clients. However, keeping connections open has a trade-off of tying up other server resources to maintain the connection information.

Domino 6 implements persistent connections with default timeout values for the persistent connection set at 180 seconds, which means that network requests and input timeouts are going to take effect first, and persistent connections will only be maintained for active sessions. Persistent connections consume more server resources than network level timeouts. You should leave the settings at the defaults unless you have a strong reason for changing them.

Network settings

Network settings determine how many sessions and what other IP addresses will be allowed to request connections (Figure 10-37 on page 344).

Network Settings	HTTP Protocol Limits
Listen queue size: <input type="text" value="512"/>	Maximum URL length: <input type="text" value="4"/> kilobytes
Maximum number of concurrent network sessions: <input type="text" value="2000"/>	Maximum number of URL path segments: <input type="text" value="64"/>
IP address allow/deny priority: <input type="text" value="Allow"/>	Maximum number of request headers: <input type="text" value="48"/>
IP address allow list: <input type="text" value=""/>	Maximum size of request headers: <input type="text" value="16"/> kilobytes
IP address deny list: <input type="text" value=""/>	Maximum size of request content: <input type="text" value="10000"/> kilobytes (specify 0 to allow unlimited content)

Figure 10-37 HTTP network settings

Concurrent sessions

The Maximum number of concurrent network sessions setting protects you from DoS attacks based on a very large number of HTTP connections. However, although your Domino server will remain online, it will refuse HTTP connections.

IP filtering

The IP Address Allow/deny settings can be very useful if your server accepts requests only from a proxy server or from a limited range of client IP addresses, or if you want to exclude certain ranges of IP addresses.

The IP Address Allow/deny priority field determines what to do with a connection request when a requestor's IP address appears in both the allow and deny fields. If the IP address does not appear in either, then the connection is allowed. The use of wildcards (*) makes it possible to list large ranges of IP addresses easily (you can exclude all IP addresses; see the table below for the proper settings).

For example, to set your proxy server as the only valid connection requestor, do the following (see Figure 10-38 on page 345):

1. Put the IP address of your proxy server in the IP address allow list.
2. Put an (*) in the IP address deny list (all IP addresses will match this).
3. Set the IP Address Allow/deny priority to Allow. When an IP address matches both the allow and deny lists, this field determines whether they will be allowed to connect. In this case, since there is only one server that can match both lists, it is the only one that will be allowed to connect. All other addresses will only match the deny list and will be denied a connection.

Network Settings	
Listen queue size:	512
Maximum number of concurrent network sessions:	2000
IP address allow/deny priority:	Allow
IP address allow list:	123.45.6.79
IP address deny list:	*

Figure 10-38 HTTP set up for a proxy server

4. Save and close the document.
5. Restart the HTTP service by typing this command at the console:

```
tell http restart
```

Table 10-2 summarizes typical IP settings and how you should use each field in each scenario.

Table 10-2 Typical HTTP network settings

Field Scenario	IP address allow priority	IP address allow list	IP address deny list
Allow access to all	Allow	blank (default)	blank (default)
Deny access to all	Deny	* (asterisk)	* (asterisk)
Deny access to a particular Web crawler	Deny	* (asterisk)	123.45.6.78
Deny access from subnets that are infected with a Web worm	Deny	* (asterisk)	123.45.*
Allow access only from two trusted proxy servers	Allow	123.48.6.78;123.45.6.79	* (asterisk)
Allow access from your intranet only	Allow	123.48.*	* (asterisk)

Important: IP address restriction should not be used as the only means of protecting your site or as a substitute for user authentication. Client IP addresses are specified in the network packets sent by the client, and this information is easily spoofed. Additionally, hackers routinely use attack techniques that hide their true IP addresses. IP address restriction cannot protect the server against such attacks.

10.3.2 Protecting your Web server at the validation level

Another common kind of attack uses invalid requests or huge headers or content to try to gain control of your server. Domino 6 protects your server from these attacks by a new set of protocol validity checks. Figure 10-39 shows the default settings.

Network Settings	HTTP Protocol Limits
Listen queue size: 512	Maximum URL length: 4 kilobytes
Maximum number of concurrent network sessions: 2000	Maximum number of URL path segments: 64
IP address allow/deny priority: Allow	Maximum number of request headers: 48
IP address allow list:	Maximum size of request headers: 16 kilobytes
IP address deny list:	Maximum size of request content: 10000 kilobytes (specify 0 to allow unlimited content)

Figure 10-39 Default HTTP protocol limits

- ▶ Maximum URL length
 - Increase the default only if you host an application that requires an extremely long URL.
- ▶ Maximum number of URL path segments
 - A segment is delimited by slashes; for example, the URL “/products.nsf/widgets” contains two segments.
 - The default is 64.
- ▶ Maximum number of request headers
 - The total number of HTTP request headers allowed.
 - The default is 48.
 - Typical requests sent from browsers usually include less than a dozen headers.
- ▶ Maximum size of request headers
 - Total length allowed for all request headers (in KB).

- The default is 16.
- Maximum size of request content
 - Total amount of data, in MB, that can be contained in a request.
 - The default is 10 MB.
 - The two most common ways for users to send data to the server is by submitting forms or by uploading files. If none of the applications on the server allow users to upload large files, you can probably set this to a much lower value.

You should leave these settings at the defaults unless you have an application that requires larger numbers.

10.3.3 Protecting your Web server at the authentication level

Lotus Domino 6 provides greater control over how Domino authenticates users accessing the server from Internet clients. In Domino 5, this setting applied only to Web browsers; in Domino 6, it now applies to all Internet protocols, including LDAP, POP3, IMAP, SMTP, and so on.

Options for user logins

On the Security tab of the Server document, the setting “Internet authentication” provides two choices: “More name variations with lower security” or “Fewer name variations with higher security.”

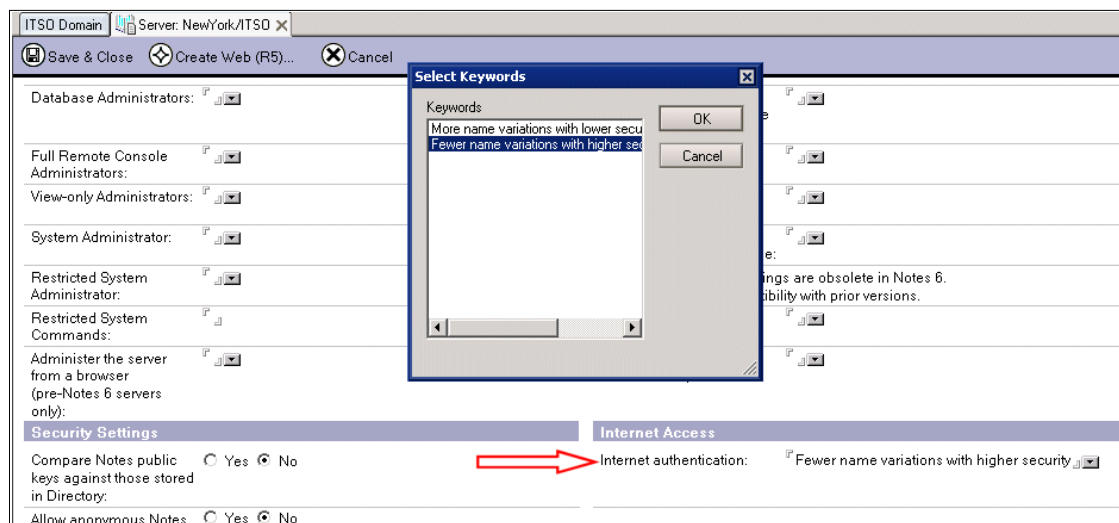


Figure 10-40 Internet authentication options

Selecting “More name variations” authenticates users the way Domino 4.6 did: users can enter any of the following as a user name when prompted by the browser or other Internet client:

- ▶ Last name only
- ▶ First name only
- ▶ Short name
- ▶ Common name
- ▶ Full hierarchical name
- ▶ Any alias in the User name field
- ▶ Internet address
- ▶ UID, if using an LDAP directory for authentication

Selecting “Fewer name variations with higher security” limits the names a user can enter when authenticating with a browser or Internet client:

- ▶ Full hierarchical name
- ▶ Common name
- ▶ Any alias in the User name field
- ▶ Internet address
- ▶ UID, if using an LDAP directory for authentication

The option “Fewer name variations with higher security” is the default setting and is recommended for tighter security. This authentication method is less vulnerable to attacks because a single authentication attempt does not produce as many matches, lessening the likelihood that a guessed password matches.

Managing Internet passwords

With Domino 6 you can use a policy to manage the standards for your users’ Internet passwords (if they have a person document in the Domino directory). You can manage the quality and length of passwords, allow users to change their passwords using a Web browser, and control expiration periods and change intervals. You can also set up Domino to synchronize the Internet password with the Notes ID password when it changes.

These features are managed through a Security settings document and applied to person documents in the Domino directory through policies. For more information on how to manage and apply policies, see Chapter 15, “Policy-based administration” on page 449.

1. Create a new Security settings document or open an existing one:
 - a. With Domino Administrator, click **People** and **Groups**, select **Settings** in the navigation panel, and click **Add Settings -> Security** (Figure 10-41 on page 349).

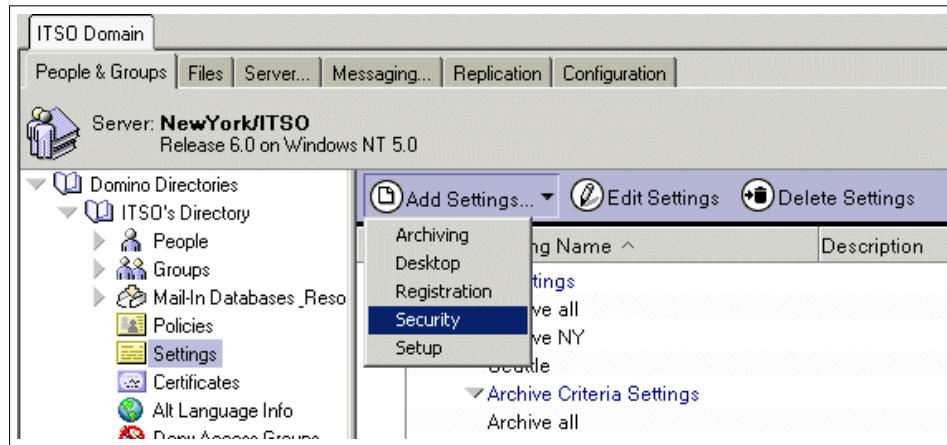


Figure 10-41 Create a new Security settings document

- b. When the new Security settings document opens, add a name to the Name field on the Basics tab.
- c. Click Password Management (Figure 10-42 on page 350).

Save & Close Cancel Inheritance Enforcement

Security Settings

Basic Password Management Execution Control List Comments Administration

Password Management Options

Allow Users to Change Internet Password over HTTP	<input checked="" type="checkbox"/> Yes
Update Internet Password When Notes Client Password Changes	<input checked="" type="checkbox"/> No
Check Notes Password	<input checked="" type="checkbox"/> No

Password Expiration Settings

Enforce Password Expiration	<input checked="" type="checkbox"/> Disabled
Required Change Interval	<input checked="" type="checkbox"/> 0 days
Allowed Grace Period	<input checked="" type="checkbox"/> 0 days
Password History (Notes only)	<input checked="" type="checkbox"/> 0 passwords

Password Quality Settings

Required Password Quality	<input checked="" type="checkbox"/> Strong Password Possibly Crackable by Automated Dictionary Attack (8)
Use Length Instead	<input type="checkbox"/> Yes

Figure 10-42 Password Management

- d. In the Password Management Options section you configure whether to allow users to change their Internet passwords through a Web application (e.g., iNotes Web Access). You can also select whether the Internet password should be updated to match the Notes ID password whenever it (the Notes ID password) changes.
 - i. In iNotes Web Access 6 for example, you can change your Internet password through the Preferences menu item, as shown in Figure 10-43 on page 351).

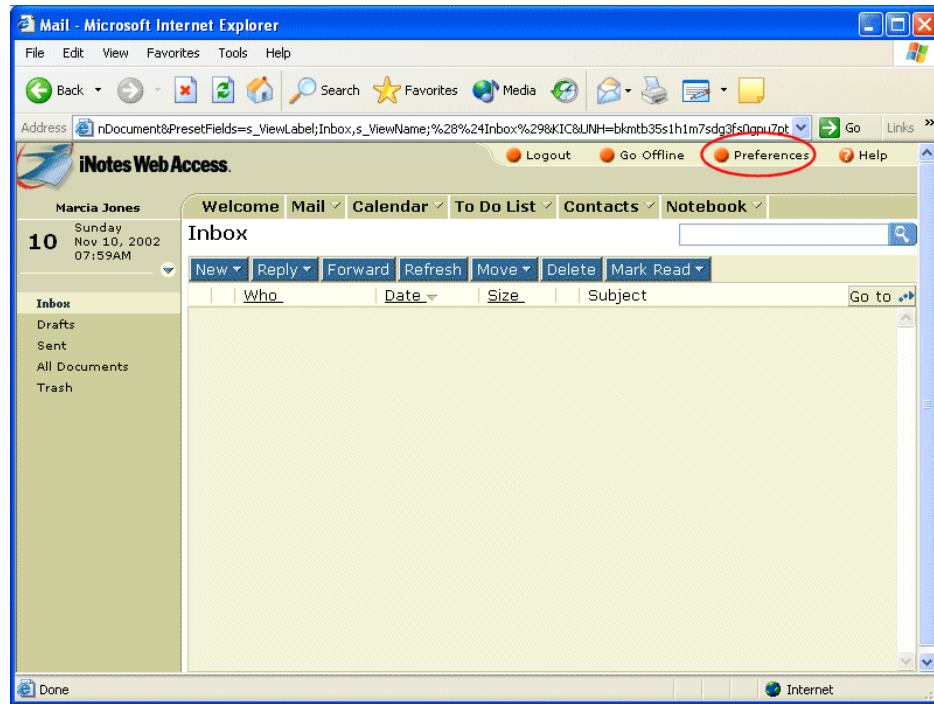


Figure 10-43 Access to the change password tool in iNotes Web Access

- ii. Once in Preferences, click Other (Figure 10-44 on page 352).

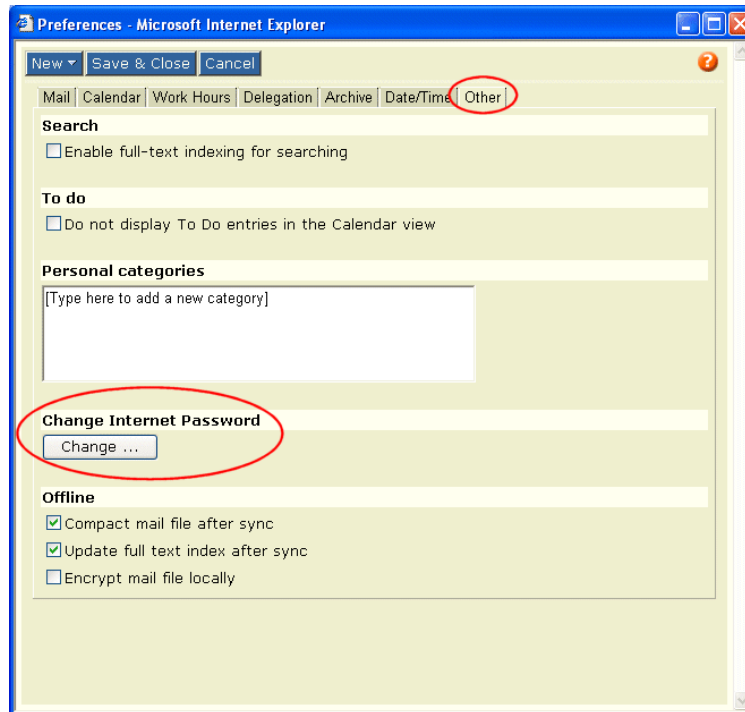


Figure 10-44 Finding the Change Internet Password button in iNotes Web Access

- iii. Click Change. Enter your old password and your new password (twice) in the appropriate fields (Figure 10-45).

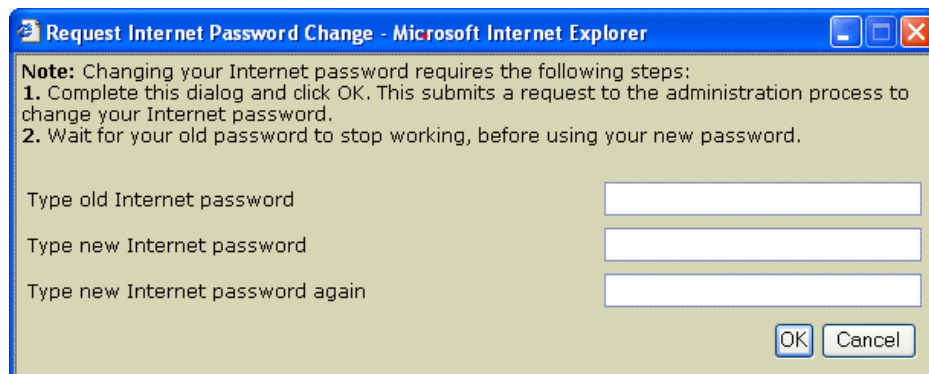


Figure 10-45 Changing the Internet password

- iv. Click OK.

- v. If the setting “Allow Users to Change Internet Password over HTTP” has been set to “Yes”, you will receive the message Your password change request has been submitted.
- vi. If the setting “Allow Users to Change Internet Password over HTTP” has been set to “No” you will receive the message shown in Figure 10-46.



Figure 10-46 Changing Internet password from a Web client is not authorized

- vii. The change password request gets submitted to adminp (Figure 10-47) and is processed by the Administration server for the Domino directory. If your Domino mail server is not the administration server for the Domino directory (which it probably is not), the change will take some time to be processed.

ADMINISTRATION PROCESS - Request

*Action:	Change HTTP Password in Domino Directory
*Server(s) to perform the action:	Administration Server for the Domino Directory
*Action requested by:	Boston/ITSO
*Name of process to perform action:	Adminp

Responses:



Date	Sched. Type	Action
11/10 08:13 AM		▼ Change HTTP Password in Domino Directory
11/10 08:13 AM		Boston/ITSO performed action on: 11/10 08:13 AM

Figure 10-47 Adminp process for changing the Internet password

- e. In the Password Expiration Settings section (Figure 10-48), configure whether you want your users' passwords to expire and how often. Note that you can apply the same settings to both Notes and Internet users, or to only one type.

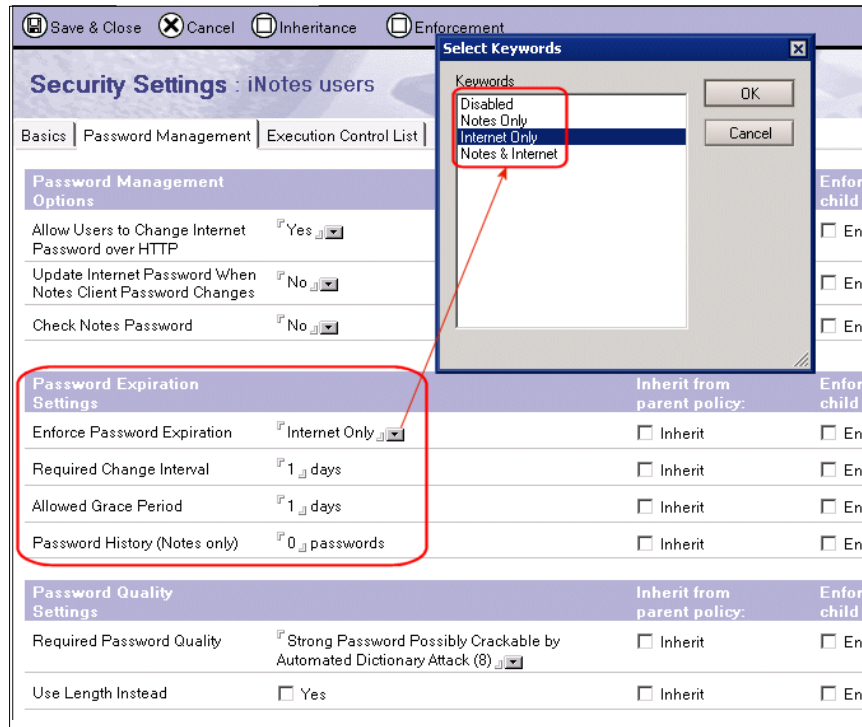


Figure 10-48 Password expiration settings

- f. The Password Quality Settings section controls the quality of both Internet and Notes passwords. Your users will have to meet the same standard for both kinds of passwords.

10.3.4 Protecting your Web server at the authorization level

Once a user has been authenticated to access the server, the database access control list determines what the user will be allowed to do. As in previous versions, Domino 6 access control lists include an entry on the Advanced tab for the maximum level of access for the name and password authentication method for Internet access (Figure 10-49 on page 355).

You can use this setting to prevent Internet users from accessing the database using name-and-password authentication. By setting it to No Access, the

database would then be accessible only to Notes users or Internet users who authenticate using SSL client certificates.

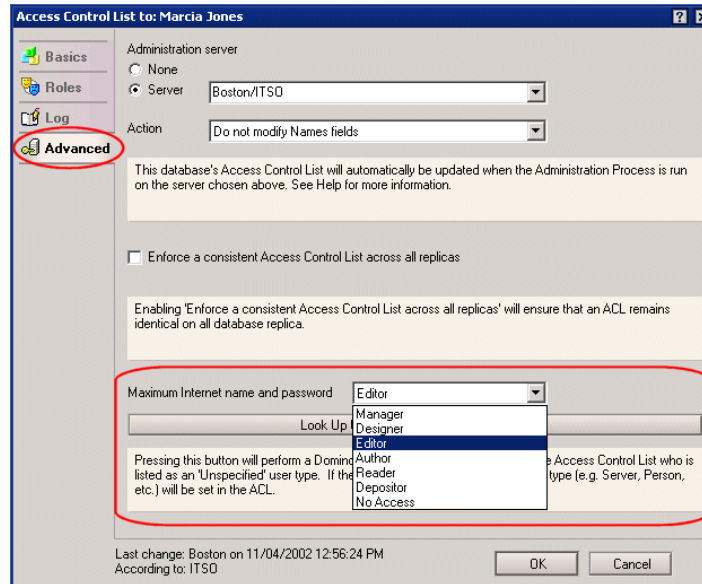


Figure 10-49 Set the database ACL to maximum Internet access

See the Admin Help section, “Maximum Internet Name and Password” for a thorough discussion of the relationship between the database ACL and this setting.

The database properties control whether SSL (Secure Socket Layer) is required for use of the database from the Web (Figure 10-50 on page 356).

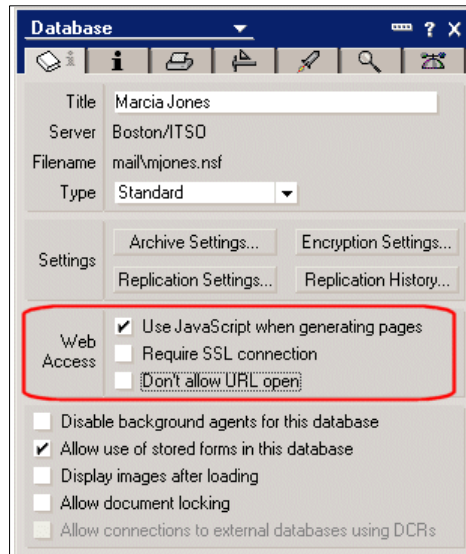


Figure 10-50 *Require SSL for use from the Web*



Certificate Authority (CA) process

Domino 6 adheres to PKIX Internet standards by incorporating the Certificate Authority (CA) process into the center of the system. This process can be used for Internet certificates, as well as Notes IDs. This chapter will discuss how the Certificate Authority process works in the Domino environment, including instructions for setting it up.

Note: For an introduction to Public Key Infrastructure, refer to the IBM Redbook *Deploying a Public Key Infrastructure*, SG24-5512.

11.1 Certificate Authority concepts

Domino 6 has significantly improved the Certificate Authority feature already present in R4.6. The certificates that Domino now issues are compliant with industry standards such as x.509 v3 and PKIX. The biggest improvement, however, is the way in which it has been implemented in Domino. It is now a server-based process, using the adminp database (admin4.nsf) as the source of requests (for Notes id requests). The Certificate Authority process can manage multiple notes and Internet certificates.

The Domino 6 server-based CA process can be used as an alternative to the R5 Notes certifier. You can migrate your R5 style certifiers to the CA process; however, you should not use a certifier in both ways, because this defeats the purpose of the Issued Certificate List (as discussed in the following section).

The Domino CA Internet certifier also offers the possibility of setting up an intranet environment where clients and servers can communicate via SSL using a corporate set of trusted root certificates. It can also issue certificates for use with secure e-mail (S/MIME e-mail).

Issued certificate list (ICL)

An issued certificate list is created for each certifier. The list stores the certifier configuration information, including the list of authorized Registration Authorities, details of all certificates the certifier has issued (for example, certificate expiration dates). In general, an administrator does not work directly in the ICL, but uses Domino Administrator's tools to interact with it. The one exception to this is Internet certificate revocation.

Adherence to PKIX standards

PKIX stands for Public Key Infrastructure based on the X.509 certificates. The PKIX Working Group of the Internet Engineering Task Force (IETF) was established in the fall of 1995 to develop Internet standards needed to support an X.509-based PKI.

Important: More information on PKI Internet standards is available at the IETF home page:

<http://www.ietf.org>

Domino 6 has moved closer to PKIX standards by incorporating two new concepts: registration authority and certificate revocation.

Registration authority (RA)

A Registration Authority is the person who authorizes the creation of new certificates. This can be (and in large organizations, should be) someone other than the administrator who makes the request for a new certificate (that is, requests the creation of a new user).

Registration authorities do not need to have access to the certifier IDs. They simply have the right to approve or reject new certificates. The process for creating a new user in the Domino environment includes these steps:

- ▶ Using the registration tool in Domino Administrator, an administrator requests that a new user receive a certificate (Notes ID).
- 2. The registration tool creates an empty ID (it has no certificates in it) to be used in setting up the Notes client.
- 3. This request is entered into the admin4.nsf and replicated to the CA host server.
- 4. A Registration Authority approves the request.
- 5. The administration process generates the ID and puts the resulting certificate in the person document in the Domino directory.
- 6. The user's workstation is set up and configured. When it logs into the Domino server for the first time, the certificate is downloaded from the Domino directory and inserted into the ID file to create a complete Notes ID file.

Certificate revocation list (CRL)

A CRL is a time-stamped list identifying revoked Internet certificates (for example, certificates belonging to terminated employees). CRLs offer a way for Internet certificates to be rescinded or revoked if the certificate is no longer trusted. The process for revoking a certificate includes these steps:

- 1. A certificate is deemed to be untrustworthy (an employee has left the organization or moved to another OU).
- 2. The employee's administrator requests that the employee's certificate be revoked.
- 3. The RA revokes the certificate.
- 4. The next time the CRL is published, it contains the user's certificate in its list.
- 5. Other users' clients receive the CRL and now recognize that the certificate is no longer valid.

Advantages to using the CA process

You will enjoy the following advantages if using the Certificate Authority process:

- ▶ It provides a unified mechanism for issuing Notes and Internet certificates.
- ▶ It supports the registration authority (RA) role, which you use to delegate the certificate approval/denial process to lower-echelon administrators in the organization.
- ▶ It does not require access to the certifier ID and ID password. After you enable certifiers for the CA process, you can assign the registration authority role to administrators, who can then register users and manage certificate requests without having to provide the certifier ID and password.
- ▶ It simplifies the Internet certificate request process through a Web-based certificate request database.
- ▶ It issues certificate revocation lists, which contain information about revoked or expired Internet certificates.
- ▶ It creates and maintains the Issued Certificate List (ICL), a database that contains information about all certificates issued by the certifier.
- ▶ It complies with security industry standards for Internet certificates (for example, X.509 and PKIX).

11.2 Domino 6 server-based CA for Notes IDs

The Certificate Authority process is a server task that can be configured to handle all of the Notes certifier IDs, as well as Internet certificates. When administrators create a new user, instead of identifying a certifier ID and password, they can now request that the CA process handle the request. This makes distributed administration much easier and more secure to set up, because the Notes certifier IDs do not have to be physically distributed; instead, they can be kept in a central database.

11.2.1 Steps to set up the CA process

The CA process is an additional task that runs on the Domino server. It makes use of the well-developed Administration process and the Domino directory with which administrators are already familiar with.

New to administrators are the console commands for manipulating the process, and the ICL database that is created for each certifier.

Migrate existing Notes certifiers to the CA process

1. With the Domino Administrator, click the Configuration tab and expand the Tools pane, if necessary. Then click Certification and click Migrate Certifier.

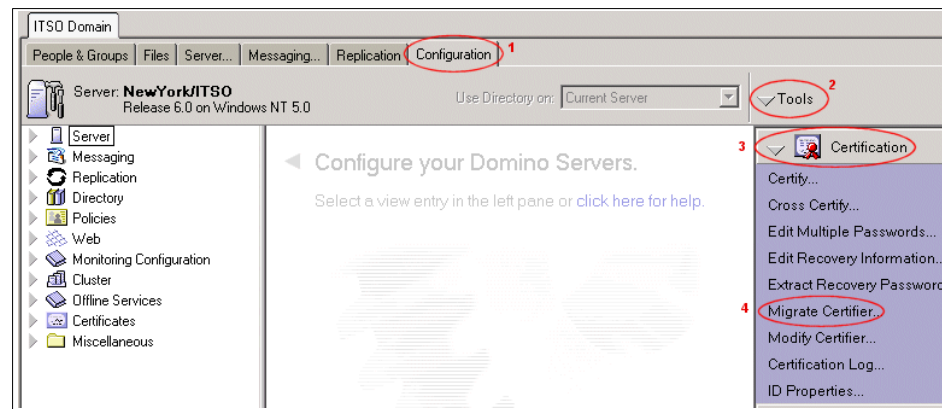


Figure 11-1 Navigate to certifier migration tool

2. Click Select to open a file browse dialog box (the ID must be on a local drive or network drive, not a Domino server). Once you have selected the ID, click OK to begin migrating the ID.

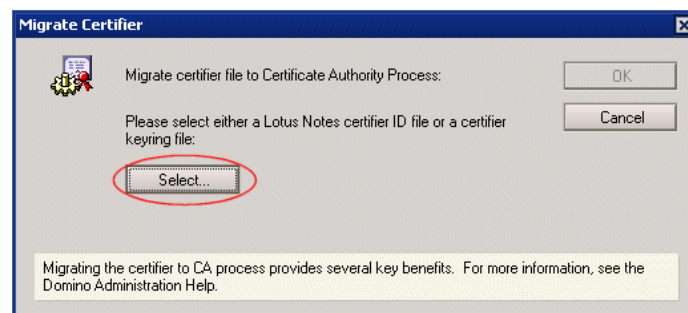


Figure 11-2 Select certifier for migration

3. Enter a password for the ID when prompted. The migration dialog box will open to the Basics tab.

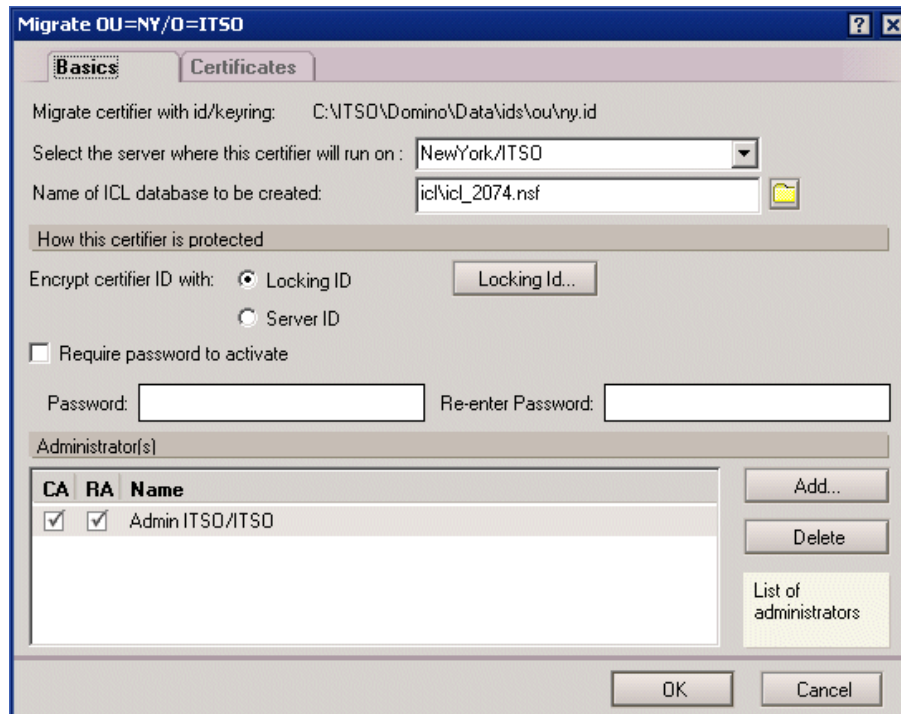


Figure 11-3 Basics tab for migrating a certifier to the CA process

- ▶ Server and ICL locations
 - a. On the Basics tab, select the server where the certification authority process for this ID will run. The ICL will be created on this server.
 - b. ICLs are created automatically as you go through this process. You can change the name of ICL database if you'd like something more intuitive than what is presented by default.
- ▶ How this certifier is protected - choose how you want to lock (encrypt) the certifier ID that you are migrating.
 - Lowest security - choose the server's ID with no password requirement
 - Medium security - choose the server's ID with a password requirement for this certifier.
 - You must activate the certifier before the CA process can use it.
 - The certifier will stay activated even when the CA refresh process runs, unless the activation password has been changed by the administrator.
 - This option provides some security for the certifiers, with minimal management issues.

Important: In order to make modifications to this certifier at a later time, you must know this activation password. Do not lose it!

- Highest security - choose a registered user ID by clicking the Locking Id... button.
 - This option automatically locks the ID.
 - You can choose any person from the Domino directory and their public key will be used to lock the ID file. In order to unlock the certifier, you must put a copy of that person's ID in a location where the server can access it (that is, not on your personal workstation).
 - Each time the CA process runs (this occurs automatically every 12 hours), the ID will automatically be locked again.
 - This option provides a high level of security, but can be a burden to manage (it's easy to forget that the certifier has been locked again, and you may think the CA process isn't working).

Tip: You'll want to consider how you encrypt the certifier IDs, and set a standard for the organization. If you want to lock the certifiers with a user ID, then you may want to create a special ID for doing that so that you don't have to leave a real person's ID on the server.

You can create a different locking ID for different certifiers, so that when one administrator unlocks the certifiers associated with their "locking ID", they won't be unlocking all the certifiers registered with the CA process on that server.

► Administrators

- The person migrating the certifier ID is automatically entered as a Certificate Authority (CA) administrator and a Registration Authority (RA) administrator.
- Add other people to this list by clicking the Add button and selecting them from the organization's directory. Deselect the role that they should not have (both CA and RA are selected by default).
 - A Registration Authority (RA) administrator registers Notes users and Domino servers, approves or denies Internet certificate requests, and, if necessary, revokes Internet certificates. While a CA administrator can also be a registration authority, the main advantage of having a separate RA role is to offload these tasks from the Domino and/or CA administrator. Moreover, the Domino administrator can establish one or more RAs for each certifier enabled for the CA process.

- CAs must have at least Editor access to the master Domino Directory for the domain.
- RAs must have author access to the master Domino Directory for the domain, with the UserCreator role enabled, and the Create document privilege enabled.

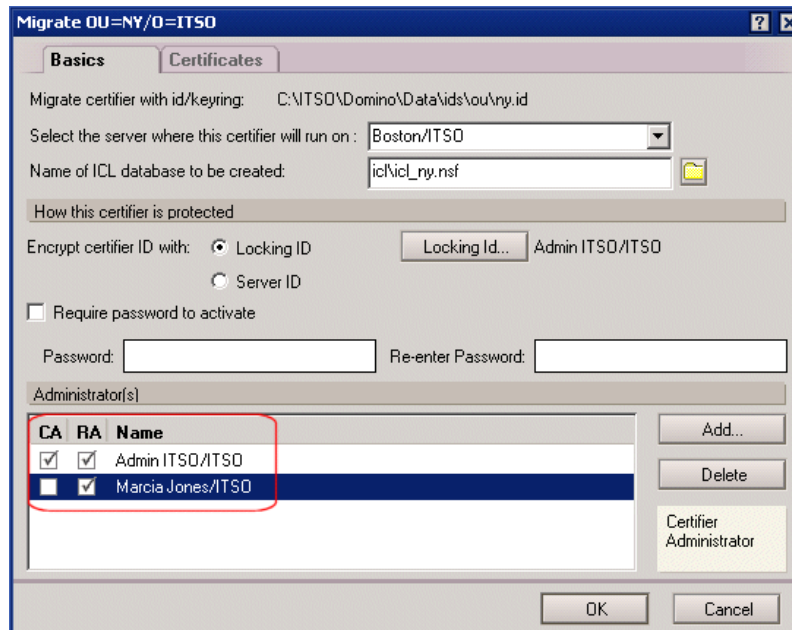


Figure 11-4 Add CA and RA administrators

4. Click on the Certificates tab.

Certifier OU=Dallas/O=ITSO

Basics | **Certificates**

Certificate Duration for EE Certificate			Certificate Duration for CA Certificate		
Default:	24	months	Default:	240	months
Minimum:	0	months	Minimum:	0	months
Maximum:	2400	months	Maximum:	2400	months

The above settings apply to the certificate this certifier will issue.

OK Cancel

Figure 11-5 Certificate settings

- **Certificate Duration for EE (End Entity) Certificate**
 - a. This setting determines how long the end user certificates that are crated with this certifier ID will be valid. You want to estimate how long someone will need a certificate so that the Certificate Revocation List doesn't grow too large.

For example, if this certificate is for temporary employees who usually work fewer than 2 months, then set the duration to 2 months. The certificates will automatically expire and you won't have to revoke their certificates to prevent unauthorized access.
 - b. The default is 24 months (2 years)
- **Certificate Duration for CA Certificate**
 - c. This field sets the maximum length of time that a certifier will be valid. This field applies certifiers created with this certifier.
 - d. The default is 240 months (20 years)
- 5. Click OK. A message appears saying that you have successfully migrated the certifier. This will take a few minutes while the tool creates the Issued Certificate List database.

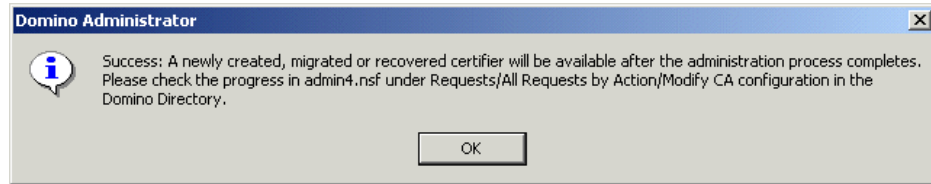


Figure 11-6 Successful migration message

6. Load the CA process on the server you designated in step 3-a by entering the following command at the console:

```
load ca
```

The server will respond by telling you which certifiers have been initialized (if any):

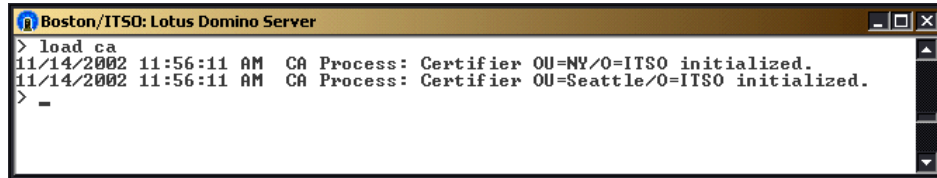


Figure 11-7 Load CA - initialize the certificates

7. If you are not the curious sort, then skip to step 9. If you are curious about what is happening in the background, look in the Administration Requests database (admin4.nsf) in the Requests/All Requests by Action view. There will be an entry titled "Modify CA Configuration in the Domino Directory" under which you will find an entry specifying that the Administration server will perform this action on the certifier:

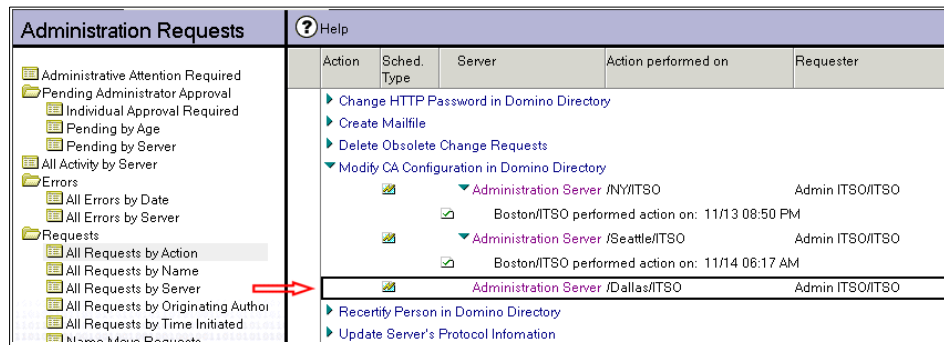


Figure 11-8 Modify CA Configuration request in admin4.nsf

8. Open the document to view the details of the request.

Edit DocumentCancelHelp

ADMINISTRATION PROCESS - Request

*Action:Modify CA Configuration in Domino Directory

*Server(s) to perform the action:Administration Server for the Domino Directory

*Name(s) to perform the action on:/Dallas/ITSO


*Action requested by:Admin ITSO/ITSO


*Name of process to perform action:Adminp

CA Administrators:CN=Admin ITSO/O=ITSO

Registration Authorities:CN=Admin ITSO/O=ITSO

Responses:

Date	Sched. Type	Action
11/14 12:03 PM		Modify CA Configuration in Domino Directory



CFG_m77879np1359615513k693k9m6nk7p5l.nsf

Figure 11-9 Modify CA Configuration - detailed view

9. Adminp will process the request the next time it looks for new requests, or you can expedite the process by entering this command at the server console:

```
tell adminp process all
```

Once adminp processes the request, you will see the request processed document in admin4.nsf:





Requests		Administration Server /Seattle/ITSO	Admin ITSO/ITSO
All Requests by Action		Boston/ITSO performed action on: 11/14 06:17 AM	
All Requests by Name		Administration Server /Dallas/ITSO	Admin ITSO/ITSO
All Requests by Server		Boston/ITSO performed action on: 11/14 12:04 PM	
All Requests by Originating Authority			
All Requests by Time Initiated			

Figure 11-10 Completed Modify CA Configuration request

ADMINISTRATION PROCESS - Log	
Action:	Modify CA Configuration in Domino Directory
Link to request:	
Name(s) acted upon:	/Dallas/ITSO
Action requested by:	Admin ITSO/ITSO
Server responding to request:	Boston/ITSO
Start time:	12:04:24 PM Today
End time:	12:04:26 PM Today
Databases processed:	Title: ITSO's Directory File name: Boston/ITSO\\names.nsf
Perform request again?:	<input type="checkbox"/> Yes

Figure 11-11 Completed Modify CA Configuration request - detailed view

You can also see the changes that were made to the certifier's document in the directory. With the Domino Administrator, click the Configuration tab, expand the Certificates section, and click the Certificates view. Expand the Notes Certifiers.

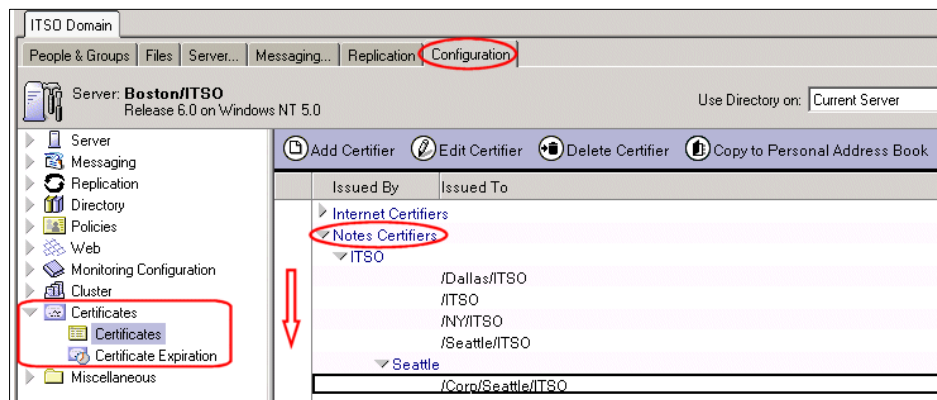


Figure 11-12 Navigate to a Notes Certifier document

Double-click the Notes certifier which you just added to the CA process so that you can view it. Notice that there is a new tab on the document called CA Configuration. This tab only appears after the Notes certifier has been enabled and remains enabled.

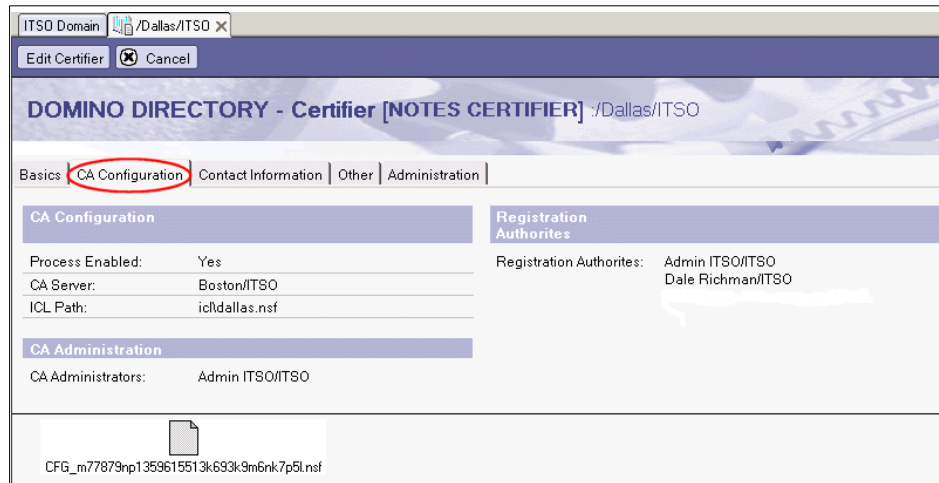


Figure 11-13 Notes certifier which has been enabled

10. The CA process adds new certifiers when it refreshes (approximately every 12 hours), or you can enter the following command at the server console to force it to refresh:

```
tell ca refresh
```

The server may warn you about certifiers that are available to the CA process, but are currently locked:

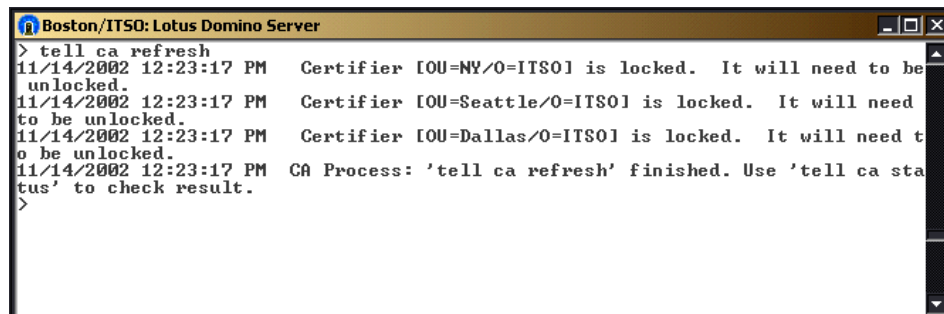


Figure 11-14 Results of refreshing the CA process

Note: If you chose to lock (encrypt) your certifier ID in step 3-c, you will need to unlock it in order to allow the CA process to use it. You do this by entering a command at the server console:

```
tell ca unlock c:\lotus\domino\data\user.id password
```

The ID file must be located on the server in order for the CA process to decrypt the certifier. Once you have unlocked the certifier by entering the preceding command, you can enter the command for the CA process to show its status:

```
tell ca status
```

You can tell that the certifier is unlocked by the Active: line in the output. If it is locked, the line will read Active: No. If it is unlocked, the line will read Active: Yes.

```
> tell ca stat
11/14/2002 03:41:49 PM CA Process Status:
11/14/2002 03:41:49 PM 1. OU=NY/O=ITSO
11/14/2002 03:41:49 PM   Certifier Type: Notes
11/14/2002 03:41:49 PM   Lock ID Name: CN=Admin ITS0/O=ITSO
11/14/2002 03:41:49 PM   Active: No
11/14/2002 03:41:49 PM   ICL DB Path: icl\icl_ny2.nsf
11/14/2002 03:41:49 PM 2. OU=Seattle/O=ITSO
11/14/2002 03:41:49 PM   Certifier Type: Notes
11/14/2002 03:41:49 PM   Lock ID Name: CN=Admin ITS0/O=ITSO
11/14/2002 03:41:49 PM   Active: No
11/14/2002 03:41:49 PM   ICL DB Path: icl\seattle.nsf
11/14/2002 03:41:49 PM 3. OU=Dallas/O=ITSO
11/14/2002 03:41:49 PM   Certifier Type: Notes
11/14/2002 03:41:49 PM   Lock ID Name: CN=Dale Richman/O=ITSO
11/14/2002 03:41:49 PM   Active: No
11/14/2002 03:41:49 PM   ICL DB Path: icl\dallas.nsf
11/14/2002 03:42:25 PM Admin Process: Searching Administration Requests databases
> tell ca unlock c:\itso\domino\data\icl\drichman.id password
11/14/2002 03:42:41 PM CA Process: 'tell ca unlock' finished. Use 'tell ca stat
us' to check result.
> tell ca status
11/14/2002 03:42:51 PM CA Process Status:
11/14/2002 03:42:51 PM 1. OU=NY/O=ITSO
11/14/2002 03:42:51 PM   Certifier Type: Notes
11/14/2002 03:42:51 PM   Lock ID Name: CN=Admin ITS0/O=ITSO
11/14/2002 03:42:51 PM   Active: No
11/14/2002 03:42:51 PM   ICL DB Path: icl\icl_ny2.nsf
11/14/2002 03:42:51 PM 2. OU=Seattle/O=ITSO
11/14/2002 03:42:51 PM   Certifier Type: Notes
11/14/2002 03:42:51 PM   Lock ID Name: CN=Admin ITS0/O=ITSO
11/14/2002 03:42:51 PM   Active: No
11/14/2002 03:42:51 PM   ICL DB Path: icl\seattle.nsf
11/14/2002 03:42:51 PM 3. OU=Dallas/O=ITSO
11/14/2002 03:42:51 PM   Certifier Type: Notes
11/14/2002 03:42:51 PM   Lock ID Name: CN=Dale Richman/O=ITSO
11/14/2002 03:42:51 PM   Active: Yes
11/14/2002 03:42:51 PM   ICL DB Path: icl\dallas.nsf
```

Figure 11-15 Unlocking a certifier with the CA process

The certifier will automatically be locked again when the CA refresh process runs (approximately every 12 hours), or you can run it manually (tell ca refresh) to relock it.

11. Set up the server to run the ca process on startup by adding CA to the ServerTasks line in the server's notes.ini. The line will look something like this:

```
ServerTasks=Update,Replica,Router,AMgr,AdminP,HTTP,IMAP,LDAP,POP3,CA
```

11.2.2 Table of ca console commands

For your convenience we've included a table of ca console commands which pertain to the Notes certifiers.

Table 11-1 The ca console commands pertaining to Notes certifiers

Command	Result
load ca	Starts the CA process.
tell ca quit	Ends the CA process.
tell ca stat	Displays summary information for the certifiers using the CA process; this includes the certifier's number, its hierarchical name, certifier type (Notes or Internet), whether it is active, and name of the ICL database.
tell ca show queue <certifier number>	Displays a list of pending certificate requests, revocation requests, and configuration modification requests for a specific certifier, using its number from the results of the "tell ca status" command. You can also use an asterisk (*) to show this information for all certifiers that are using the CA process.
tell ca activate <certifier number> password	Activates a certifier if the certifier is created with "Require password to activate certifier", or use this for any certifier that has been deactivated. Activation is enabled during CA setup and creation. Activate a specific certifier by entering its number from the results of the "tell ca status" command. Or, you can actually unlock all server ID/password-protected certifiers at one time with this command, if you specify an asterisk (*) for the certifier number. The CA process then prompts you for the password for each certifier.
tell ca deactivate <certifier number>	Deactivate a certifier. You will need to activate it again in order for it to process any request. Use * to deactivate everything, or deactivate a specific certifier by entering its number from the results of the "tell ca status" command.
tell ca lock idfile	Lock all certifiers that were set up with a lock ID, as specified during CA setup.
tell ca unlock idfile password	Unlock all certifiers using the ID and password that comprise the lock ID. The lock ID is specified during CA setup.

Command	Result
tell ca refresh	Force the CA process to refresh its list of certifiers. As a result: - Newly configured certifiers will be added to the CA process. - Previously unlocked certifiers will need to be unlocked again. - Previously activated certifiers may need to be activated again, if the activation password has changed. - The Notes certifier ID file in idstorage will be updated with the latest certificate information.
tell ca help	List tell ca options.

11.2.3 Registration Authority administrative tasks

Create a new user or server with the CA process

1. Ensure the following:
 - You have author access to the Domino directory, with the UserCreator role and the create documents property enabled.
 - You have RA administrator rights to the certifier you intend to use. You can check this in the following way:
 - i. With Domino Administrator, click the Configuration tab. Expand the Certificates section in the navigation panel.
 - ii. Expand the Notes Certifiers selection and drill down to the certifier you intend to use. Double-click the certificate document to open it.

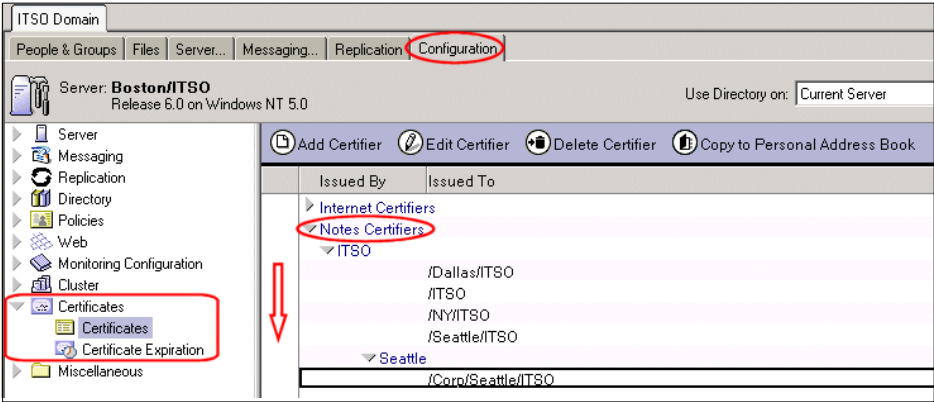


Figure 11-16 Navigate to a certificate document

- iii. Click the CA Configuration tab. The Registration Authorities are listed on the right-hand side.

DOMINO DIRECTORY - Certifier [NOTES CERTIFIER] /Corp/Seattle/ITSO

Basics | CA Configuration | Contact Information | Other | Administration

CA Configuration

Process Enabled: Yes

CA Server: Boston/ITSO

ICL Path: iclcl_0843.nsf

Registration Authorities

Registration Authorities: Admin ITSO/ITSO
Dale Richman/ITSO

CA Administration

CA Administrators: Admin ITSO/ITSO

CFG_n0486n98mo949p1m2k774018mmk7p152.nsf

Figure 11-17 Detailed view of CA Configuration of a certificate

- iv. If you are not listed there, contact the CA Administrator (listed on the lower left side of the document) and request that you be added as a Registration Authority for this certifier.
1. With Domino Administrator, click the People & Groups tab.
 2. Expand the tools pane if necessary and then expand the People section.
 3. Click Register to bring up the Choose a Certifier dialog box.

Choose a Certifier

Server... Boston/ITSO

☒ Supply certifier ID and password

Certifier ID...

☐ Use the CA Process

CA configured certifiers:

(None Available)

The 'Use the CA Process' option allows you to specify a certifier without access to the certifier ID file or certifier password.

OK Cancel

Figure 11-18 Choose a Certifier

4. Choose the registration server as you normally would.
Note: If the registration server is not the server set up to run the CA process for this certifier, then it will take a little longer for the procedure to complete because the admin4.nsf file must replicate the request back to the server that is running the CA process for this certifier.
5. Click the Use the CA Process button.
6. From the following pick list, select the certifier that you want to use for this individual.

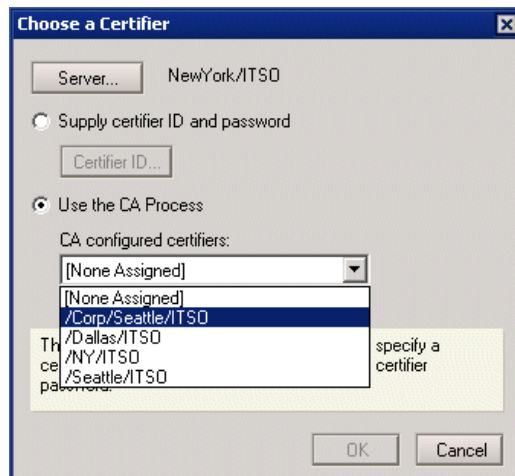


Figure 11-19

7. Click OK to bring up the Register Person utility.
8. Note that all of the options for creating the user are still available to you. Be sure to make all the changes as you normally would. Add the person to the queue, then click the Register button.
9. You will receive notification that the person was registered successfully. Click Done to exit the utility. If you try to set up the client for the new user immediately, it may fail with the following error:



Figure 11-20 Certificate not available yet for client setup

All this means is that the whole CA process has not completed (see below).

10. These steps are automatic to the CA process, but they must occur before you can successfully set up the client for the newly registered user:

- (Possibly) The Administration Requests database (admin4.nsf) and the Domino directory must replicate from the Registration server to the server that is running the CA process for this certifier file.
- The CA process certifies the new user and puts their private key in a hidden field in the Domino directory
- The Domino Directory replicates to the user's mail server.
- When the client gets set up the private key is inserted into the user's id file and it is activated for use.

11.2.4 Certificate Authority administrative tasks

Certifiers are maintained by the Certificate Authority. Each certificate has a CA. Each CA may have one or more certificates which they maintain. Maintenance consists of the creation, configuration, modification, and disabling of certifiers.

The Certificate Authority must have editor access to the Domino directory and db creation rights on the servers that run the CA process. Individuals listed in the full access administrators and administrators fields of the server document have these rights by default. If you assign Certificate Authority duties to others, you will need to give them these rights.

Modify the certifier ID

Modification of the certifier ID occurs in the same way for all types of modifications, except enabling and disabling: you must be listed as a CA for the modifier, and have editor access to the Domino directory to make modifications.

- ▶ Change the locking ID.
 - ▶ Change the activation password.
 - ▶ Add/remove the Certificate and Registration Authority administrators for the certifier.
 - ▶ Change the duration parameters for certificates created with this certificate.
1. With the Domino Administrator, click the configuration tab, expand the tools pane if necessary, expand the certification section, and click Modify Certifier....

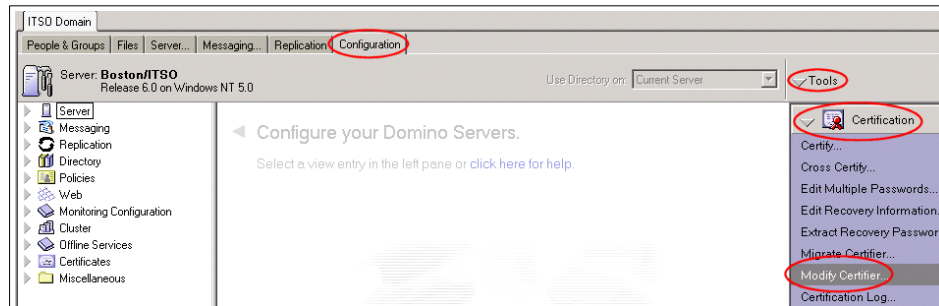


Figure 11-21 Navigate to the Modify Certifier tool

2. Select a CA process-enabled certifier from the Domino Directory drop-down list and click OK.
3. Enter the password required to open the certifier, if required (this will be the activation password, if one was set).

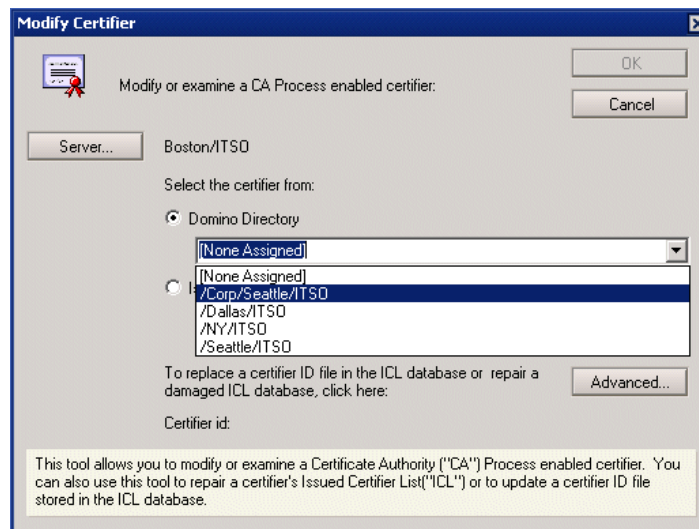


Figure 11-22 Select a ca enabled certifier

4. Make modifications to the certifier's characteristics in the same way you did when you migrated or created it. You are able to modify everything except which server it is assigned to, and which ICL database is associated with it.

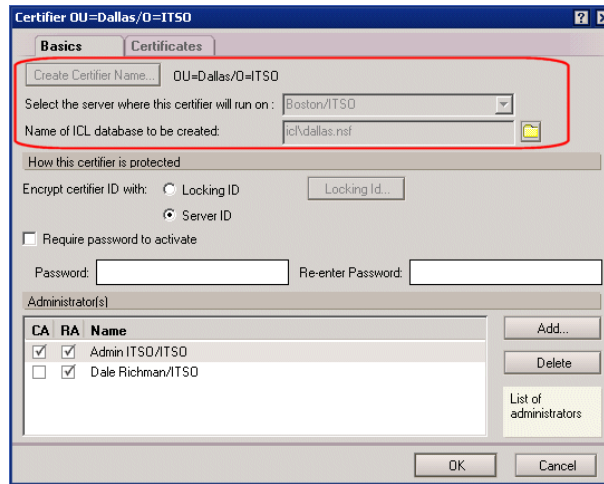


Figure 11-23 Parts of a certificate are not modifiable

5. Click OK. You will receive a warning message; click Yes. You will receive a Success notification; click OK.

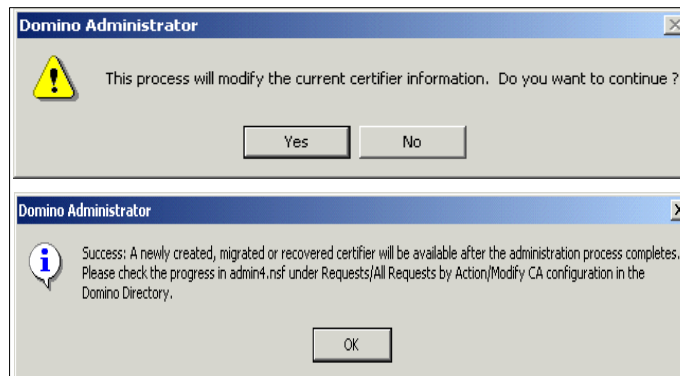


Figure 11-24 Certificate modification confirmation and success

6. Once adminp has run, the modifications will be implemented.

A disabled certifier

If you have previously disabled a certifier, it will not appear in the drop-down list. In that case, click the Issued Certificate List (ICL) database button and select the ICL database through the browse feature (be sure to change the server, if necessary). By default, ICL databases are placed in the icl directory.

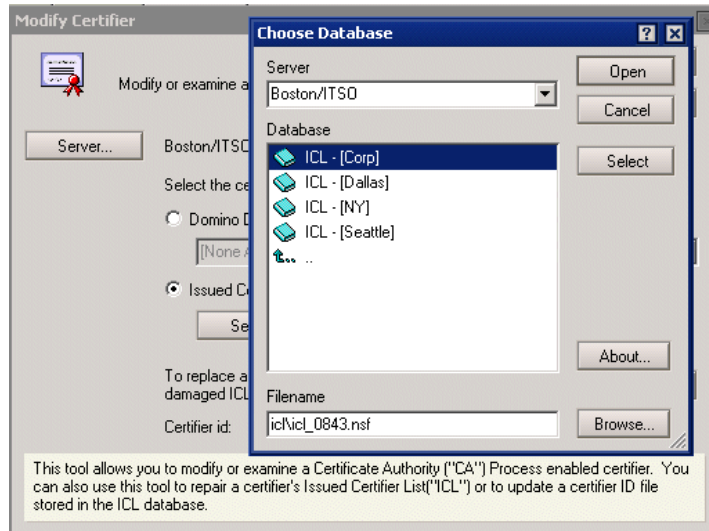


Figure 11-25 Choose a certifier by its ICL database

You can only view the characteristics of a certifier when it is not enabled. If you try to save changes to a certifier that is not enabled, you will receive an error message. You must enable the certifier through the certificate document in the Domino directory in order to modify or use it.

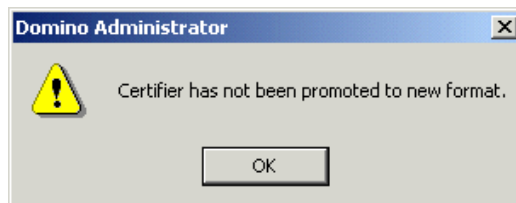


Figure 11-26 Certifier has not been promoted

Disable/re-enable certifiers

Notes certifiers are disabled and re-enabled through the Domino Directory.

Disable a Notes certifier for the Certificate Authority process

1. With Domino Administrator, click the Configuration tab. Expand the Certificates section in the navigation panel.
2. Expand the Notes Certifiers selection and drill down to the certifier you intend to disable. Select the document and click the Edit Certifier button in the Action bar.

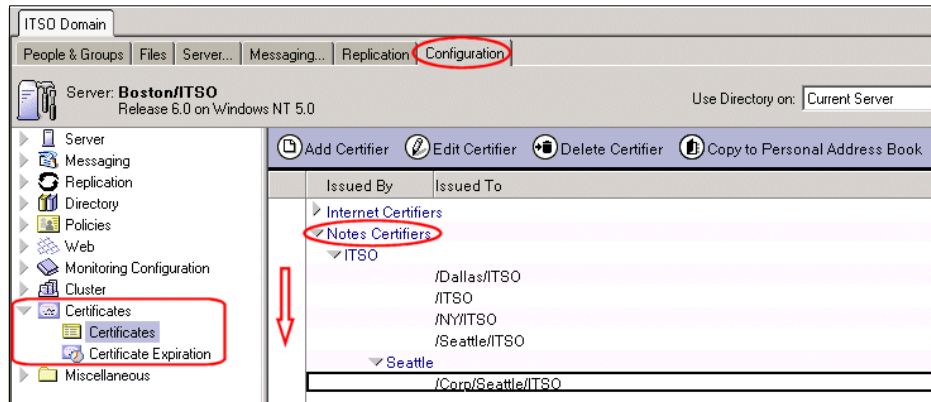


Figure 11-27 Navigate to a certificate document

3. Click the CA Configuration tab. Change the field “Process Enabled” from Yes to No.

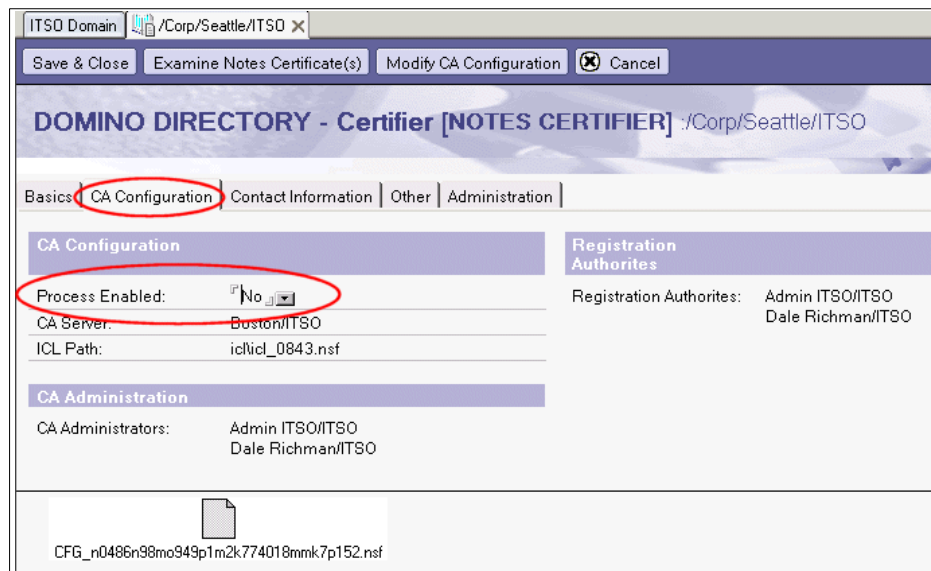


Figure 11-28 Disable certificate authority process for a Notes certifier

4. Click Save & Close. If you reopen the document, you will notice that the CA Configuration tab no longer appears. You also see that the Notes database that contains the Certificate Authority profile for this certifier remains in the document. This information is needed if you want to reenoble the certificate.

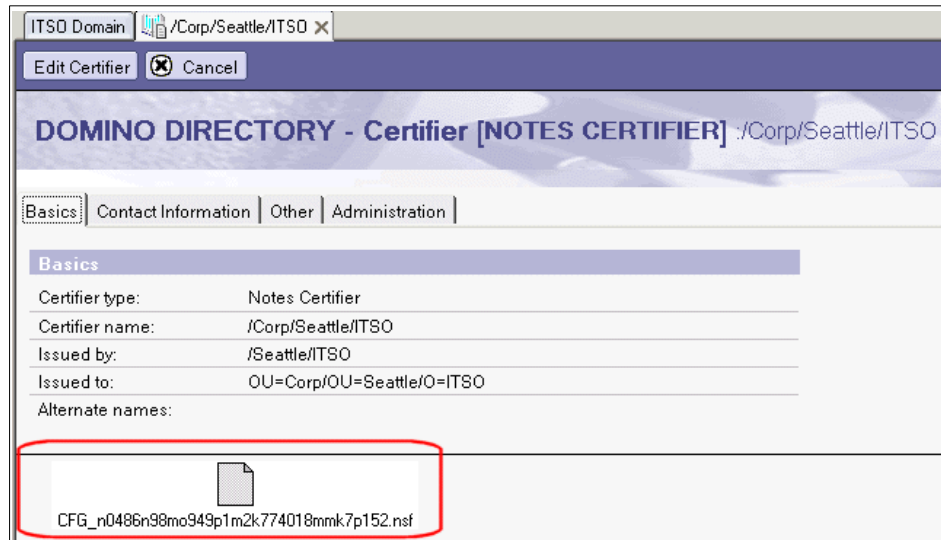


Figure 11-29 A Notes certificate which has been disabled for the ca process

Re-enable a Notes certifier for the Certificate Authority process

Since the CA Configuration tab disappears from the document when the certifier is disabled, you will need to create an agent to re-enable the Notes certifier.

1. With Domino Administrator, click the Configuration tab. Expand the Certificates section in the navigation panel.
2. Expand the Notes Certifiers selection and drill down to the certifier you intend to re-enable. Select the document.

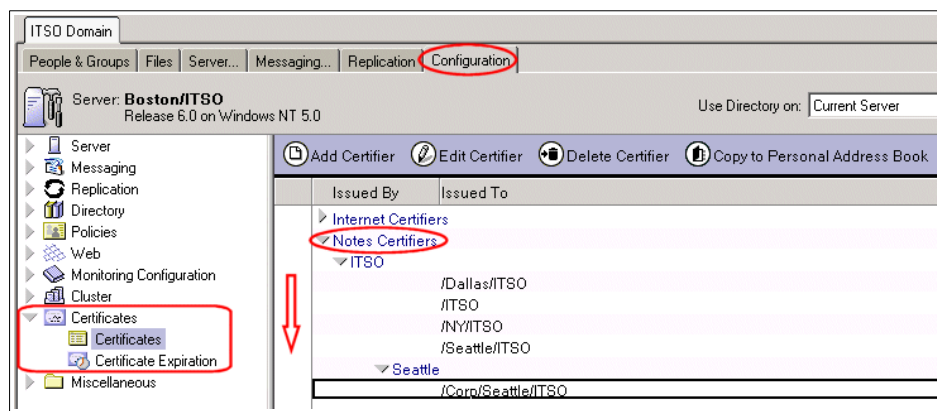


Figure 11-30 Navigate to a certificate document

3. Click Create -> Agent on the menu. This will bring up Lotus Domino Designer, prompting you for a name for the new agent.

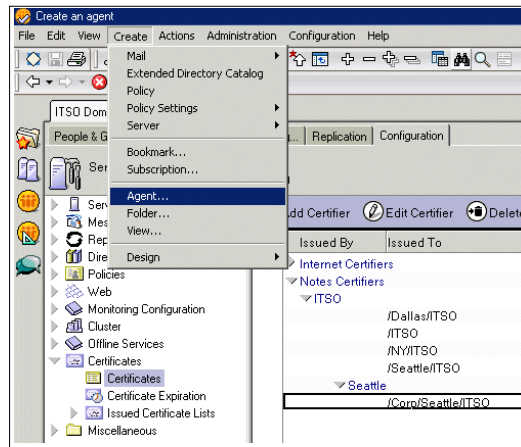


Figure 11-31 Create an agent

4. Enter a name for the agent and close the dialog box by clicking the “x” in the upper right-hand corner:

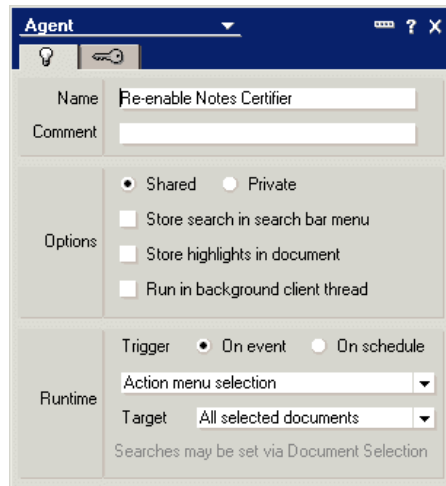


Figure 11-32 Name the agent

5. Click the Add Action... button in the lower panel.

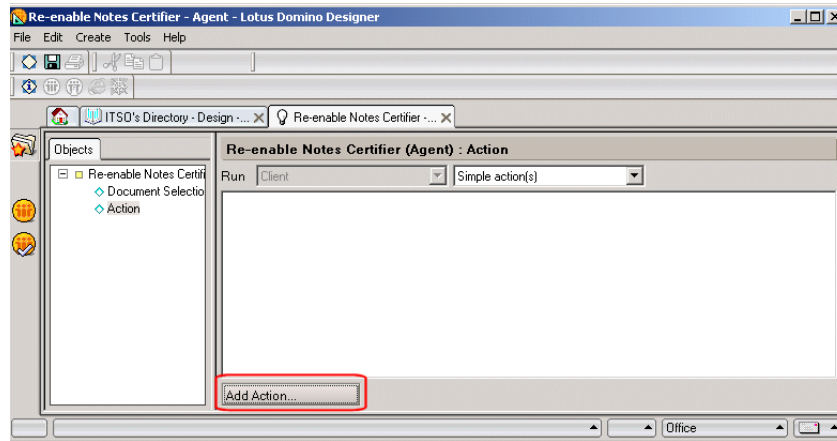


Figure 11-33 Add Action... button in the Agent builder

6. Set the fields to the following values:
 - a. Action: Modify Field
 - b. Modify by: Replacing
 - c. The value in field: CAEnabled
 - d. With the new value: 1

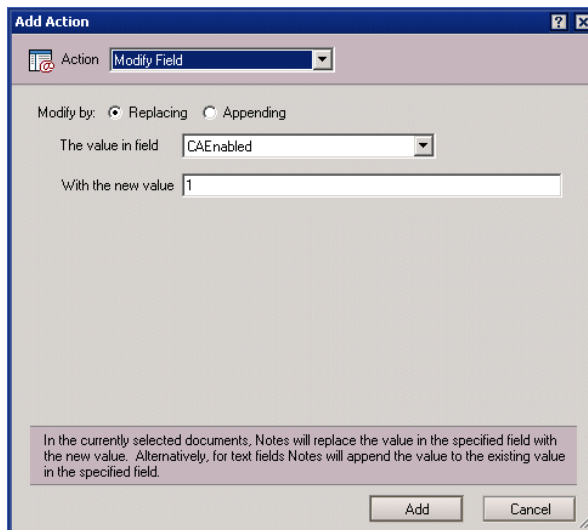


Figure 11-34 Agent settings for re-enabling a certificate

- e. Click Add to add the action to the agent. The action will appear in the central pane of the agent builder.

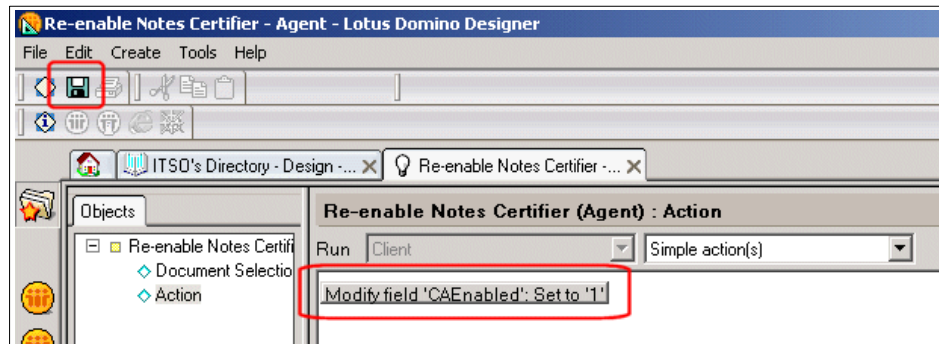


Figure 11-35 Action has been added to the agent

- f. Save the agent by clicking the colored disk in the upper left-hand corner.
- g. Switch back to Domino Administrator. With the appropriate certificate document selected, click Actions -> Name of agent (the one you just created)

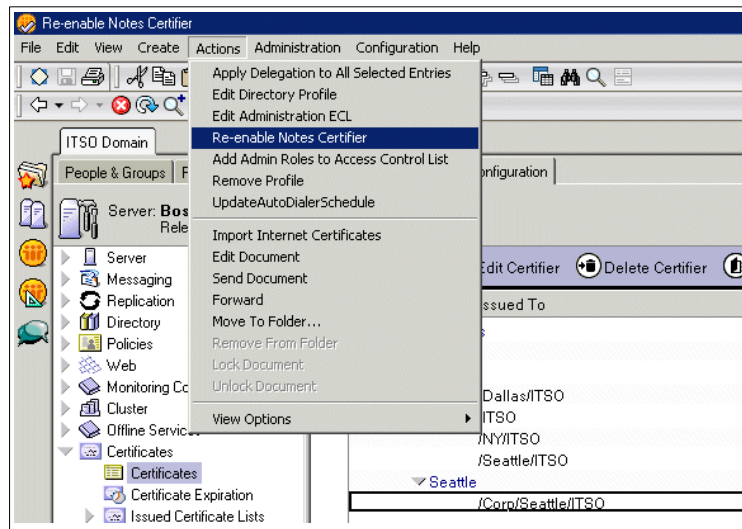


Figure 11-36 Run the agent you just created

- h. Verify that the certifier has been re-enabled by opening the certificate's document. If it has been re-enabled, you'll see the CA Configuration tab.

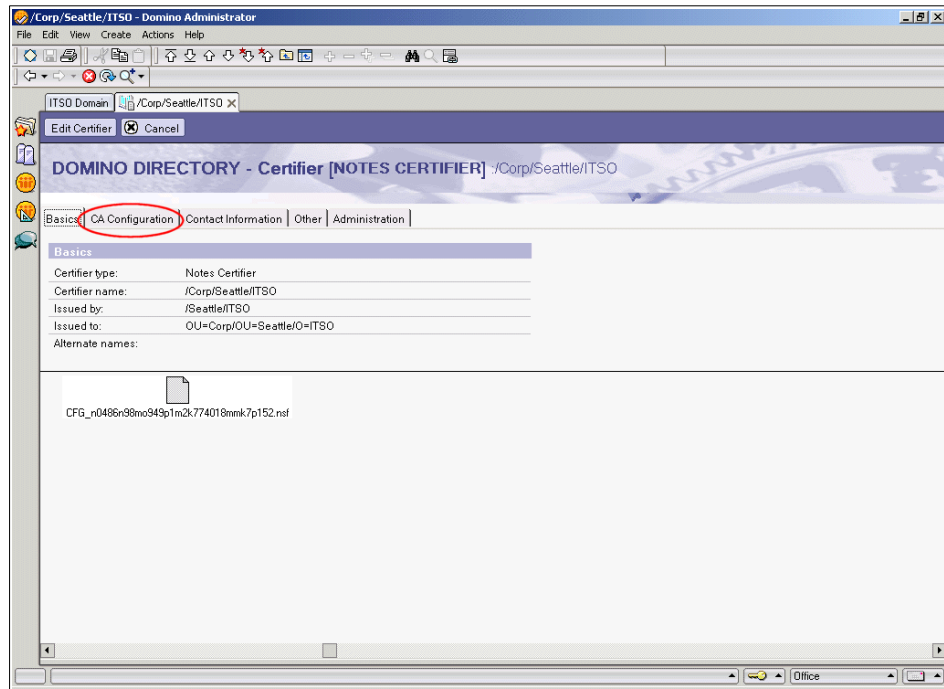


Figure 11-37 Notes certifier that has been re-enabled for the CA process



Internet Site architecture

The Domino 6 Web server provides you with enhanced performance and scalability for expanding the capabilities of Web application development and deployment.

The Domino 6 Web server task supports a summarized Internet Sites view with Internet Site documents in the Domino Directory. All servers that share the same Domino Directory share the same Internet Site documents in the Internet Sites view.

The Internet Site documents contain most of the information from the Domino 5 Server document, as well as new configuration settings. The Internet Site Rule document complements this structure by enabling administrators to seamlessly relocate or reorganize all the organizations Domino Internet sites.

Besides this structure, a number of additions have been made to the Domino core HTTP task, which allow you to configure the Domino server as a multi-functional and multi-platform enterprise application and Web server.

In this chapter, we discuss and describe the Internet Site architecture.

12.1 Domino R5 and Domino 6 documents - differences

Lotus Domino R5 uses the model of multiple virtual servers which are associated to a single Domino Web server. Domino 6 Web sites (Virtual Hosts) are not explicitly associated with physical servers, but to an organization. This allows you to set up a single Domino domain that can support many Web sites throughout your infrastructure and organization.

The most significant difference between a Virtual Server and a Virtual Host is that a Virtual Server is mapped to a destination IP address and can therefore be assigned its own SSL keyring, whereas a Virtual Host is mapped to a DNS host name and uses the default keyring (that is, the keyring specified in the Server document).

Table 12-1 shows the most important differences between Domino R5 server documents and the Domino 6 Web site documents in the Domino Directory.

Table 12-1 Differences - R5 and Domino 6 Web site configurations

Domino R5 document	Domino 6 document
Server document	Internet Site document
Virtual server	Web Site document (Virtual Host)
URL Mapping/Redirection	Rule document
File protection document	File protection
Realm	Authentication Realm

Domino 6 still uses the Server document for some low-level HTTP task configuration settings:

- ▶ Enabling and configuring the TCP/IP port
- ▶ Enabling and configuring the SSL port (including redirecting TCP to SSL)
- ▶ Server access control (such as who can access the server and how)
- ▶ Log file settings, Log file names and Exclude from Logging settings
- ▶ Timeouts
- ▶ Restricting IP addresses

12.2 Internet Site configurations

Internet Site documents contain Internet site configuration information and are managed through the Domino Administrator client, where you will find the Servers/Internet Sites view (under the Configuration tab).

Many of the HTTP task Server document settings used in Domino 5 are now available in the Internet Site documents and rules. However, the Domino 6 HTTP task remains fully compatible with the Domino R5 Servers\Web Configurations view.

The Internet Site documents correspond not only to HTTP protocol settings, but also to the SMTP, POP3, IMAP, LDAP, and IIOP protocols. This means, when you enable the Domino server to use the Internet Site documents, you must configure the above-mentioned protocols where appropriate if you use one or more of them on a specific server.

Attention: As soon as you enable the new Internet Sites architecture in the Server document, Server tasks start using the Internet Sites documents instead of those in the Server record.

Make sure all configurations have been converted before you switch to the Domino 6 Internet Site architecture.

12.2.1 Internet Site documents

Internet Site documents are used to configure the Internet protocols supported by Domino servers. A separate Internet Site document is created for each protocol, which is then used to provide protocol configuration information for a single server, or for multiple servers in a Domino organization.

The following protocols can be configured through the Internet Site document.

Table 12-2 *Configuring protocols with Internet Site documents*

Protocol	Description
HTTP (Web)	Create a Web site document for each Web site hosted on the Domino server
SMTP (inbound) POP3 IMAP	Create an individual Internet Site document for each mail protocol. Each document should have an IP address or host name mapped.
LDAP	Create an LDAP site document for LDAP protocol access to an organization in a directory.

Protocol	Description
IIOp task	Create an IIOp Site document to enable the Domino IIOp (DIIOP)server task. This task allows Domino and the Web browser client to use the Domino Object Request Broker (ORB) server program that serves your Java code.

Note: Each document must have a unique IP address or host name mapped to this site.

Creating an Internet Site document

1. From the Domino Administrator, click Configuration -> Web -> Internet Sites.
2. Click Add Internet Site, and select the type of Internet Site document to create.

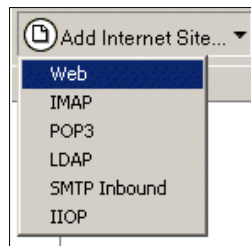


Figure 12-1 Add Site documents

3. In the newly created Internet site document, click the Basics tab, and complete all necessary fields.

Web Site

Basics

Configuration

Domino Web Engine

Security

Comments

Administration

Site Information

Descriptive name for this site:

Organization:

Use this web site to handle requests which cannot be mapped to any other web sites:

☐ Yes
☒ No

Note: only one web site should have this option set to Yes

Host names or addresses mapped to this site:

Domino servers that host this site:

Table 12-3 shows the functions of the several fields on the Basics tab, which are basically the same for all types of Internet Site documents.

Table 12-3 Internet Site - Web site document fields

Field	Action
Descriptive name for this site (Optional but recommended)	Entering a descriptive name is optional, but we recommend that you use a name corresponding to the name of the organization and Web site or URL that you use for this document. Example: www.lotus.com
Organization (Required for all Internet Site documents)	Enter the name of the registered organization that hosts the Internet Site document. The name must correspond to the organization's certifier.
Use this Web site to handle requests which cannot be mapped to any other Web sites (Web Site documents only)	Choose one: - Yes: This Web site processes incoming HTTP requests if Domino cannot locate the Web sites that were entered in the "Host names or addresses mapped to this site" field. This is a special type of Web site, so design the site to give end users the appropriate information (and also perhaps links to other Web pages, because the user probably arrived at this site by accident). - No (default): This Web site does not process incoming HTTP requests for which Domino cannot locate a Web site. This is a regular Web site.

Field	Action
Hosts names or addressed mapped to this site (Required for all Internet Site documents)	Enter the target host names or IP addresses that trigger a connection's use of this Internet Site document. If the site is set up for SSL, you must specify IP addresses.
Domino servers that host this site (Required for all Internet Site documents)	Enter the name of one or more Domino servers that host this site. You can use any variation of distinguished name (for example, Server1/Sales/Acme) as well as wildcards (for example, */Acme). The default is (*), which means that all servers in the domain can host this site. If you leave the field blank, the Internet Site will not be loaded on any Domino server.

4. For all Internet Site documents, complete the settings on the Security tab.
5. The following Internet Sites require additional configuration:
 - a. WebSites
 - a. IMAP
 - a. DIIOP
6. Save and close the document.

Enabling Internet Site documents

After you have configured all the Internet Site documents, then enable the server to use the Internet Sites document instead of the Server document by following these steps:

1. Open the Server document.
2. Click Basics and check Enabled for "Loads Internet configurations from Server\Internet Sites documents".

Figure 12-2 Enable internet Site configurations

Server : ITS08/Server/ITS0	
Basic Security Ports Server Tasks Internet Protocols MTAs Miscellaneous Transactional Logging Shared Mail Administration	
Basics	
Server name:	ITS08/Server/ITS0
Server title:	Win2K server - Located ITS0 Cambridge
Domain name:	ITS0
Fully qualified Internet host name:	its08
Cluster name:	
Load Internet configurations from Server/Internet Sites documents:	Enabled
Maximum formula execution time:	120 seconds
Server build number:	Build V60_09202002
Routing tasks:	Mail Routing
SMTP listener task:	Enabled
Server's phone number(s):	
CPU count:	2
Operating system:	Windows/NT 5.0 Intel Pentium
Is this a Sametime server?:	No
Directory Information	
Directory assistance database name:	
Name of condensed directory catalog on this server:	
Fault Recovery	
Fault Recovery:	<input type="checkbox"/> Enabled
Cleanup Script Name:	

3. Save the document, and then restart the HTTP server task to use the new view.

Attention: When you enable the server document setting, only the configurations in the Internet Site document will be active.

Make sure you converted all your settings to correspond to the appropriate Internet Site documents.

Modifying and deleting Internet Site documents

Modifications to Internet Site documents (including the creation of new Site documents) are dynamic. The server or protocol does not need to be restarted after you create a new Site document, or after you modify or delete an existing one.

Changes generally take effect only minutes after the change is made, but if you do want to enforce it, you can use the **tell http refresh** command.

During a Web Server refresh cycle, all of the configuration information contained in the Web Site documents, and documents attached to Web Site documents (file protection, authentication realms, and rules) is updated on the server.

12.2.2 Global Web Settings document

The Global Web Settings document applies to all Web Site documents that you set up on one or more specific Domino servers.

After you have created the Global Web Settings document, you can create rules for this document. These rules will apply to all of the servers that are specified in the Global Web Settings document.

12.2.3 Internet Site Rule document

Web Site Rules are defined in the Domino Directory by creating response documents to Web Site documents. As with all other information defined for Web sites, a rule applies only to its parent site. In this section, we briefly explain the rule documents that can be created when using the Internet Sites architecture.

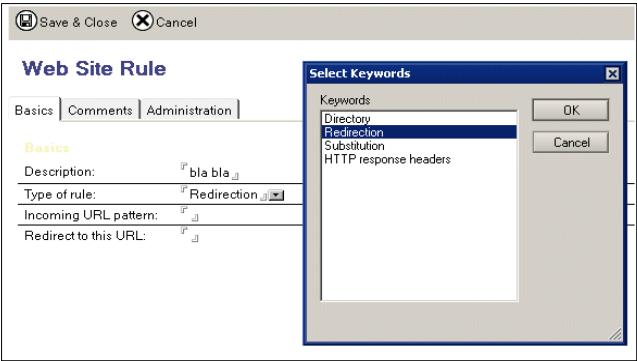


Figure 12-3 Web site rule options

In case you have an existing R5 Web server, you may already have rules defined in the Domino Directory Server\Web Configurations view. Domino 6 supports the same set of rules, but uses different terminology.

Table 12-4 shows a comparison between the terminology in R5 and Domino 6.

Table 12-4 Rule comparison

Domino R5	Domino 6
URL -. Directory	Directory
URL -> Redirection	Redirection
URL -> URL	Substitution

Directory rules

A directory rule maps a file system directory to a URL pattern. When the Web server receives a URL that matches the pattern, the server assumes that the URL is requesting a resource from that directory.

When you install a Domino 6 Web server, several file resource directories are created automatically. These default directories are mapped by directory rules that are defined on the Configuration tab of the Web Site document.

When the Web server starts up, it automatically creates internal rules to map these directories to URL patterns. The three default directories are:

- ▶ HTML directory for non-graphic files
- ▶ Icon directory for graphic images such as .GIFs
- ▶ CGI directory for CGI programs

Directory rules can only be used to map the location of files that are to be read directly (such as HTML files and graphic files), and executable programs to be loaded and run by the operating system (such as CGI programs). Directory rules cannot be used to map the location of other types of resources, such as Domino databases or Java servlets.

When you create a Directory Web Site Rule, you specify read or execute access to a file system directory. It is *critically* important to choose the right access. Only directories that contain CGI programs should be enabled for Execute access. All other directories should have Read access.

If you specify the wrong access level, unexpected results will occur. For example, if you mark a CGI directory for Read access, then when a browser user sends a URL for a CGI program, the server will return the source code of the program instead of executing it, which could be a serious security problem.

Directory rules cannot override file access permissions enforced by the operating system.

Attention: Access level is inherited by all subdirectories under the specified directory.

Redirection rules

There are two types of redirection rules that you can use: internal redirection, and external redirections:

- ▶ External redirection rules are used when the location of a Web site resource has changed and you want the browser to be aware of the new location

- Internal redirection rules are used when you do *not* want the browser to be aware of the new location

Table 12-5 lists the specifications for these rules.

Table 12-5 Redirection rule types and specifications

Rule type	Specification
Internal redirection	<p>Internal redirection can be used as to convert a URL to another path. This is mostly done to redirect users to the home page of the Web site.</p> <p>The pattern in this field starts with a slash.</p> <p>Example: /welcome.nsf Incoming URL pattern: / Redirect to this URL: /welcome.nsf</p>
External redirection	<p>External redirection is often used when all or part of a Web site has moved to another, related site. Using external redirections allows existing links and bookmarks to keep working, but insures that new bookmarks will point to the new location.</p> <p>The pattern for an external redirection needs to start with an Internet protocol string that the browser will understand.</p> <p>Example: http: or https or ftp: Incoming URL pattern: /redbooks/* Redirect to this URL: http://www.ibm.com/redbooks/*</p>

Another way to use the external redirection rule is to change ports or protocols; refer to Table 12-6.

Table 12-6 Changing protocols and ports

Redirection type	Specification
Change protocols	<p>Incoming URL pattern: /*/register.htm</p> <p>Redirect to this URL: https://www.ibm.com/*/register.htm</p>
Change ports	<p>Incoming URL pattern: /account.nsf/*</p> <p>Redirect to this URL: http://spendbucks.com:8008/account.nsf/*</p>

Wildcards are allowed in redirection rules, but are not required.

Substitution rules

Substitution rules are used to replace one or more parts of an incoming URL path with new strings.

The two main uses for substitution rules are:

- ▶ You want to reorganize your site and do not want to have to rewrite all the links within the site.
- ▶ You want to provide user-friendly aliases for complex URLs.

The following examples show how to use substitution rules.

- ▶ Creating an alias to replace a long Domino string:

Table 12-7 Substitution example alias

Incoming URL pattern	Replacement pattern
/find/*	/allsearch.nsf/products?searchview&query=*

This allows you to create short and easy-to-remember URL links.

- ▶ Creating a replacement string:

Table 12-8 Substitution example replacement string

Incoming URL pattern	Replacement pattern
/Databases/*	Replacement pattern: /Applications/*

This allows you to move databases or categories and still have your site navigation work properly.

After you configure the Web server, you can issue the following console command to dump the HTTP configuration to a text file so you can check the server configuration from another perspective:

```
Tell HTTP Dump
```

The file is now created in the Domino Data directory with the name “httpcfg.txt”. It displays complete information about security, Web settings and Web Site documents and rules.

The HTTP response header rule

Every HTTP browser request and server response begins with a set of headers that describe the data that is being transmitted. An HTTP response header rule allows an application designer to customize the headers that Domino sends

(such as an Expires header or custom headers to HTTP responses) with responses to requests that match the specified URL pattern.

The most important use of response rules is to improve the performance of browser caching. An application designer can add headers that provide the browser with important information about the volatility of the material being cached.

Unlike other Web Site rules, response rules are applied to the outgoing response, just before the HTTP task transmits the response to the browser. For response header rules, the pattern is matched against the final form of a URL, after substitution and redirection rules have been applied to it.

The pattern can include one or more asterisks as wildcard characters.

12.3 Additional new features related to Domino 6

This section describes other new features in Domino 6 that relate to Internet Site documents.

12.3.1 Language differentiation

The Web server uses language string resource modules to render Web pages in different languages. The Domino 6 Web server can support multiple languages, and be configured to handle them on the fly.

The language in which a Web server generates a Web page is based on the “Accept-Language” setting in the headers of client HTTP requests.

Example

A Web server with English and French resource modules will generate a Web page in French if a Web client sends an HTTP request with “Accept-Language:fr (French)” in its headers. Resource models are downloadable add-in language packs.

You can configure the language settings in the Web Site document on the Domino Web Engine tab by using the field shown in Figure 12-4.

Default regional locale:	<input type="checkbox"/> Browser's accept-language	
Language		
Default string resource language:	<input type="checkbox"/> English	
Additional string resource languages:	<input type="checkbox"/>	
		Character set in header: <input type="checkbox"/> Enabled
		Meta character set: <input type="checkbox"/> Disabled

Figure 12-4 Language specification for Web Sites

12.3.2 Third-party HTTP server integration

Domino 6 fully supports WebSphere plug-ins that allow you to use a third party Web server as a front-end to a Domino server. The initial release of Domino 6 supports the plug-ins for Microsoft IIS and the IBM HTTP Server, and will be extended for Apache and iPlanet in the coming Domino 6 releases.

For security reasons, many customers install their Domino server inside their firewall and provide HTTP access through a secondary server directly connected to the Internet. This method shields the Domino server from denial-of-service (DOS) attacks, and reduces the possibility of security breaches directly from the Internet. This allows a third-party Web server to be the one “facing” the browsers and serving up static content (which is their speciality), while all NSF requests are forwarded to the Domino Web server.

The plug-ins use HTTP to communicate with the server, so the third-party HTTP server can reside in the De-Militarized Zone (DMZ), with the plug-in communicating to the Domino server residing behind the firewall.

The IBM HTTP Server (IHS) is packaged as part of the IBM WebSphere Application Server. For information on installing IHS and the WebSphere server, see WebSphere installation documentation or the related IBM Redbooks listed in the “Related Publications” section of this publication.

Installing the plug-in is an option during WebSphere installation. For information on installing the plug-in during WebSphere setup, refer to WebSphere installation documentation.

Figure 12-5 shows how a Domino Web server making use of a third-party Web server can be situated.

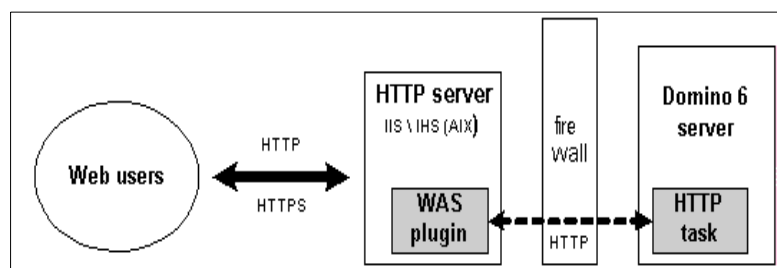


Figure 12-5 Typical HTTP integration configuration

When a Web client makes a request to the third-party HTTP server, the WebSphere plugin evaluates the request and determines the ultimate destination. If the user requested a Domino URL, the plugin forwards the request

to Domino's built-in HTTP server to be fulfilled. The requested information is sent back from the Domino 6 server Domino via the originating third-party HTTP server.

With R5, Domino required the use of a reverse proxy server, in Domino 6, the plugin architecture provides native reverse proxy capability.

Using the WebSphere Application Server HTTP transport plugin in conjunction together with Domino 6 gives you the following advantages and support:

- ▶ The front-end HTTP server does not require database access through the firewall.
- ▶ Support of Domino and WebSphere security.
- ▶ Support of Secure Sockets Layer (SSL) encryption for communications between the Web server and the application server.
- ▶ Load balancing and failover support
- ▶ Native Reverse proxy support
- ▶ Supports for Network address translation (NAT) firewalls.
- ▶ Connector performance is relatively fast.

WebSphere Application Server is integrated with Domino in multiple ways. The WebSphere Application Server servlet engine can plug into the Domino HTTP server via DSAPI, and WebSphere can use the Domino Directory for authentication via LDAP and use single sign-on (SSO) between Domino Web applications and WebSphere servers.

Set up Domino to work with Internet Information Server (IIS)

To use a Microsoft IIS server as a front-end machine, you must install the WebSphere Application Server 4.0.3 plug-in for IIS on the IIS server.

To install the WebSphere plugin on the IIS server and enable it for your Web site or multiple Web sites, you must perform the following steps:

- ▶ Install the WebSphere plugin on an IIS server
- ▶ Configure the WebSphere plugin
- ▶ Configure the Domino server to work with Microsoft IIS
- ▶ Set up security for Microsoft IIS

In the sections that follow, we walk through these steps in detail.

Note: You do not need to install any other WebSphere components to use the Microsoft IIS with the plugin.

install the WebSphere plug-in on an IIS server

Before beginning this procedure, you should be familiar with the Internet Services Manager configuration tool. On Windows NT and Windows 2000, this tool is accessed through the Microsoft Management Console.

1. Create the following directory structure on the IIS machine (you may use any drive):
 - C:\WebSphere\AppServer\bin
 - C:\WebSphere\AppServer\config
 - C:\WebSphere\AppServer\etc
 - C:\WebSphere\AppServer\logs
2. Copy the following files from the Domino server to the IIS server:
 - Copy data/domino/plug-ins/plugin-cfg.xml to C:\WebSphere\AppServer\config.
 - Copy data/domino/plug-ins/w32/iisWASPlugin_http.dll to C:\WebSphere\AppServer\bin.
 - Copy data/domino/plug-ins/w32/plugin-common.dll to C:\WebSphere\AppServer\bin.
3. Start the Internet Service Manager application.
4. Create a new Virtual Directory for the Web site instance you want to work with WebSphere. To do this with a default installation, expand the tree on the left until you see Default Web Site. Right-click Default Web Site and select New - Virtual Directory. This opens the wizard for adding a Virtual Directory.
5. In the Alias field, enter: sePlugins.
6. In the Directory field, browse to the WebSphere bin directory (C:\WebSphere\AppServer\bin).
7. For access permissions, check and uncheck all other permissions.
8. Click Finish. A virtual directory titled sePlugins is added to your default Web site.
9. Right-click the machine name in the tree on the left and select Properties.
10. On the Internet Information Services tab, select WWW Service in the Master Properties drop-down box and click Edit.
11. In the WWW Service Master Properties window, click the ISAPI Filters tab.
12. Click Add. This opens the Filter Properties dialog.
13. In the Filter Name: field, type: iisWASPlugin.
14. In the Executable: field, click Browse. Open the WebSphere bin directory and select iisWASPlugin_http.dll.
15. Close all open windows by clicking OK.

16. Open the Windows registry file and create the following key path:
HKEY_LOCAL_MACHINE - SOFTWARE - IBM - WebSphere Application
Server - 4.0. Select 4.0, then create a new string value: Plug-in Config.

Set the value for this variable to the location of the plugin-cfg.xml file
(C:\WebSphere\AppServer\config\plugin-cfg.xml)
17. To enable the plugin for additional Web sites, repeat Steps 4 through 8.

Configure the WebSphere plugin

The WebSphere configuration file WebSphere\AppServer\config\plugin-cfg.xml controls the operation of the plug-in.

In order for the plug-in to relay requests to the target Domino server, you must add directives to plugin-cfg.xml to define a transport route to the server, and pattern rules for the URL namespaces that identify requests that are to be relayed to Domino. The plugin will only relay requests that match a namespace rule; all other requests will be handled by the front-end Web server.

To configure plugin-cfg.xml:

1. Open plugin-cfg.xml in Notepad.
2. Modify the <Transport> element to target the appropriate Domino server. To do this, change the Hostname and Port parameters to the proper values required for the plugin to reach your back-end server's HTTP task.

For example:

```
<!-- Server groups provide a mechanism of grouping servers together. -->
<ServerGroup Name="default_group">
  <Server Name="default_server">
    <!-- The transport defines the hostname and port value that the web server
    plug-in will use to communicate with the application server. -->
    <Transport Hostname="mydomino.server.com" Port="81" Protocol="http"/>
  </Server>
</ServerGroup>
```

3. Add these directives to the top of the <UriGroup> section.

These directives specify common URL patterns needed for accessing Domino Web applications.

```
<UriGroup Name="default_host_URIs">
  <Uri Name="*/.nsf">
  <Uri Name="*/icons/*">
  <Uri Name="*/domjava/*">
```

If your Domino application requires additional namespaces, you can create <Uri> directives for those patterns, also.

Note: All WebSphere Application Server plugins automatically re-read the configuration file once a minute to pick up changes. If you do not want to wait that long, you must stop and restart the front-end Web server.

Configure the Domino server to work with Microsoft IIS

On the back-end Domino server, add the following line to NOTES.INI:

```
HTTPEnableConnectorHeaders=1
```

This setting enables the Domino HTTP task to process the special headers added by the plugin to requests. These headers include information about the front-end server's configuration and user authentication status.

As a security measure, the HTTP task ignores these headers if the setting is not enabled. This prevents an attacker from mimicking a plugin.

Set up security for Microsoft IIS

When you have set up an IIS plugin and a Domino back-end server, Web applications are subject to both IIS security and Domino security. After IIS authenticates a user based on the NT Windows account registry, those credentials, if any, are passed to Domino for user authorization.

Microsoft IIS supports the following methods of user authentication. The Domino plug-in configuration supports all except Digest authentication.

- ▶ Anonymous access (the user does not enter a name or password).
- ▶ Basic Authentication (the user enters a name and password).
- ▶ Digest authentication (an enhanced version of Basic authentication available only on Windows 2000). The Domino plug-in configuration does not support this authentication method.
- ▶ Integrated Windows authentication (a special protocol supported by Microsoft Internet Explorer. On NT, this protocol is called Windows NT Challenge/Response).
- ▶ SSL.

You can find additional details about IIS security options in the Lotus Domino 6 Administration help document "Details of Microsoft IIS security options".

IIS requires user authentication in order to control access to resources owned by IIS such as the file system and Active Server Pages. If a user requests access to a Domino resource, the IIS plugin passes the authentication information to Domino.

Therefore, if you want Domino to completely handle user authentication, you should enable Anonymous Access as the only security option for the IIS Web site.

To set up anonymous access on the IIS server:

1. Start the Internet Services Manager (or Microsoft Management Console) You can use Start -> Run -> and then type: mmc.
2. Right-click the IIS Web site and select Properties.
3. Click the Directory Security tab.
4. Click Edit in the Anonymous Access and Authentication Control section.
5. Choose one or more of the authentication options and click OK.

Your IIS and Domino server are now configured to serve your Web site. You can find additional information about setting up Domino authentication in 12.3.4, “Session-based name-and-password authentication” on page 404.

Setting up Domino to work with IBM HTTP Servers

The IBM HTTP Server (IHS) is packaged as part of the WebSphere Application Server.

For information on installing IHS and the WebSphere server, see WebSphere installation documentation. Installing the plugin is an option during WebSphere installation.

For information on installing the plugin during WebSphere setup, see WebSphere installation documentation. The plugin files are also packaged with the Domino 6 server.

If the plugin was not installed during WebSphere installation, you can copy the plugin files from the Domino 6 server.

To install the WebSphere plug-in from Domino, follow these steps:

1. Install a Domino 6 server. The plugin files are packaged with the server.
2. On the IHS server, create the appropriate directory structure.
 - For AIX:
 - /usr/WebSphere/AppServer/bin
 - /usr/WebSphere/AppServer/config
 - /usr/WebSphere/AppServer/logs
 - For Win32 (you can use any drive):
 - c:\WebSphere\AppServer\bin
 - c:\WebSphere\AppServer\config

- c:\WebSphere\AppServer\logs

The following instructions assume you are using an AIX server.

3. Copy the following files from the Domino server to the IHS server:
 - Copy: <Domino data directory>/domino/plugin-ins/aix/mod_ibm_app_server_http.so
to: /usr/WebSphere/AppServer/bin
 - Copy: <Domino data directory>/domino/plugin-ins/plugin-cfg.xml
to: /usr/WebSphere/AppServer/config
4. On the IHS server, edit the IHS configuration file httpd.conf (on a default installation, this file is located at /usr/HTTPServer/conf/httpd.conf).
Add the following lines to the bottom of the file:


```
LoadModule ibm_app_server_http_module
/usr/WebSphere/AppServer/bin/mod_ibm_app_server_http.so

WebSpherePluginConfig /usr/WebSphere/AppServer/config/plugin-cfg.xml
```
5. Modify the plugin-cfg.xml file according to the instructions detailed in “Configure the WebSphere plugin” on page 400 for configuring the WebSphere plugin.
6. Set up the Domino server according to the instructions for IIS.
7. Restart the IHS server and test your installation.

12.3.3 WebDAV

WebDAV, or Web-based Distributed Authoring and Versioning, is a set of extensions to the HTTP/1.1 protocol that allows developers and users to collaboratively edit and manage files on remote Web servers. WebDAV allows people to check-in, check-out, and lock Web documents and elements.

Domino 6 fully supports this feature and as an administrator, you may be asked to enable this for some of the enabled Internet Sites.

Fully covering this option is not really within the scope of this redbook, but since it is a significant change, following is a list of resources that you can consult in order to configure the WebDAV into your Internet Sites architecture:

- ▶ *Domino Designer 6: A Developer's Handbook*, SG24-6854
- ▶ Lotus Domino 6 Administrator help document “Setting up WebDAV”
- ▶ Lotus Domino Designer 6 help document “Developing applications using third-party tools and WebDAV”

Note: You must be using Web Site documents to configure and manage the Web sites on your server in order to use WebDAV.

12.3.4 Session-based name-and-password authentication

When enabling name-and-password authentication, the Domino server requests the user's name and unencrypted password with each request to the server. Session-based authentication differs in that the user name and encrypted password is stored in a cookie on the workstation. That information is sent over the network only the first time a user logs in to a server, and not each time a request is posted.

While in Domino R5 this option could be enabled per server, in Domino 6 this can be enabled per registered Internet Site. You can enable session-based name-and-password authentication for a Web site document on the Web Engine Tab by using a similar procedure as in Domino R5.

Enable single-server session-based authentication for Web Site documents

1. From the Domino Administrator, click Configuration -> Web -> Internet Sites.
2. In the Internet Sites view, select the Web Site document for which you want to enable session authentication.
3. In the Web Site document, click Domino Web Engine.
4. In the HTTP Sessions section, complete the fields listed in Table 12-9:

Table 12-9 session-based authentication fields

Field	Action
Session authentication	Select single server. This is disabled, by default.
Idle session timeout	Enter a default time period to log an inactive Web client off the server. The default is 30 minutes.
Maximum active sessions	Enter the maximum number of user sessions allowed on the server at the same time. The default is 1000.

5. Click Security, and enable name-and-password authentication for the TCP and for SSL (if using SSL).
6. Save the document

Refer to the Domino Administrator 6 Help document "Setting up session-based name-and-password authentication" for all the information you need to set up session-based authentication.

Single sign-on (SSO)

Multi-server session-based name-and-password authentication for Web users, called “single sign-on” for Web browsers, allows you to sign on to a Domino or WebSphere server once, and then have access to any SSO-enabled Domino or WebSphere server in your domain without signing on again. In addition, you can have multiple Web SSO Configuration documents in a Domino Directory or domain.

Refer to Domino 6 Administration help documentation for complete information on configuring all the options described in this section. The following documents are related to configuring SSO for Domino:

- ▶ “Setting up the Web SSO Configuration document for more than one Domino domain”
- ▶ “Multi-server session-based name-and-password authentication for Web users (single sign-on)”

You can also refer to the IBM Redbook *Domino and WebSphere Together*, SG24-5955, which explains how to set up Domino and WebSphere Application Server for single sign-on.

12.3.5 Other changes to the Domino HTTP task

The following enhancements have been made to the Domino HTTP task (but are not covered in this redbook):

- ▶ Rewritten HTTP server provides HTTP 1.1
- ▶ Persistent connections
- ▶ Improved session handling
- ▶ Better denial-of-service attack handling
- ▶ More administrative control over URL length, number of path segments, and so on
- ▶ Custom JSP tag library

12.4 Upgrading to Domino 6 Internet Site architecture

When migrating your site from Domino 5 to Domino 6, you do not need to immediately convert server documents into Internet Site documents because the Domino 6 HTTP task is fully compatible with the R5 Server configurations.

Tip: When you migrate from the R5 Server document settings to the Domino 6 Internet sites architecture, first use the current settings as configured in the Server document before changing to new settings.

However, you will need to convert to the new view to take advantage of many of the new Web features in Domino 6. When you have a mixed environment using R4 or R5 servers together with Domino 6, you can only configure the Domino 6 servers to work with the Internet Sites architecture.

Attention: If you use an Internet Site Document to configure one Internet protocol on a server, you must use Internet Site Documents for all Internet protocols on that server.

12.4.1 Upgrading steps

The following general steps must be taken when upgrading from Domino R5 Web configuration to the Domino 6 Internet Sites architecture:

1. Prepare your DNS entries to be able direct to the new architecture (this should be done at least 48 hours or more before you switch over in order to allow the change to take effect on all servers).
2. Prepare Domino replication connections to and from the Internet Site servers.
3. Register all sites according to the current server document configurations.
4. Register one Web site to serve as your organization's default Internet Site (this is optional, but recommended).
5. Convert all Virtual servers into Internet Site documents by creating the new Internet Site documents.

Virtual servers or hosts can be converted into Internet Site documents by creating one Internet Site document for each virtual site, and configuring each Site document according to the settings in the R5 server documents.

6. Convert the SSO document from your current Server document into one or more Internet Site documents.
7. Convert all URL Mapping\Redirection, File protection, and REALM documents from the Web configurations view in your Domino Directory into Internet Sites Rule documents.
8. Enable Internet Sites architecture server by server, according to the procedure described in this chapter.
9. Restart the Domino HTTP server.

Your Domino infrastructure should now be using the Internet Sites architecture.



Domino hosting features

The Domino 6 server includes new hosting features (xSP model) that allow multiple groups of users to be independently hosted by a single logical Domino server or cluster of servers in order to allow Notes- and Web-based clients to access their data from the same physical server securely using Notes/Domino or standard Internet protocols.

This new model allows you to build a hosting environment that helps you run an ASP (Application Hosting Provider) or xSP service to provide a secure and shared environment—after all, a shared environment reduces the total cost.

The major Domino components have been modified to support multiple user groups on the same server that are unaware of each other's existence.

This chapter discusses the differences and benefits that the hosted organizations can give you, including some valuable technical details.

13.1 Hosted organizations

The hosted organizations model can be created in several ways, but we can distinguish the following models:

- ▶ Dedicated IP addresses: Each hosted organization uses its own IP address.
- ▶ Shared IP addresses: All hosted organizations make use of one shared IP address.

13.1.1 Addressing models

The differences between these two options are as follows:

- ▶ Dedicated IP addresses

Each hosted organization is assigned its own IP address and its own Domain Name Service (DNS) names for SMTP addresses, IMAP, POP3, and LDAP servers, and for Web server application sites. In this configuration, when a connection is received by a single server that is hosting multiple organizations, the server examines the IP address that it received as the target of the connection. The server uses that IP address to determine what organization the connector is a part of, and uses that knowledge of a person's identity to constrain that person to their hosted organization's portion of the Domino Directory, and of the data directory.

Each end user will only see people in his/her organization's portion of the Domino Directory, and they will only see their organization's applications.

- ▶ Shared IP addresses

In this configuration, a single IP address is assigned to all organizations that use the same server, the xSP, but different DNS names are assigned for SMTP domains, IMAP, POP3, and LDAP servers, and for Web sites. For each hosted organization, a similar model is used.

When a connection occurs, the server doesn't know which hosted organization the end user is a part of. But, when the end user performs the first request, the server can determine the hosted organization. If the request is to a Web server, the URL is the identifier. If the request is to a POP3 or an IMAP server, for example, the server uses the identification of the user. When that identification comes over the wire, the server again uses that information to determine which hosted organization the user is in and then performs the same virtualization of both the Domino Directory and the applications in the data directory.

- ▶ A combination of the two IP configurations

Attention: SSL is supported only for hosted environments that use a unique IP address configuration.

13.1.2 Multiple organization Domino Directory

The multiple organization Domino Directory feature dramatically reduces the complexity of server administration. But because the Domino Directory is a database that is shared between multiple organizations in the xSP model, security is a critical element.

Hosting multiple organizations in one R5 Domino directory might have caused you several security issues because your customers were able to see all the registered persons in the Domino Directory.

In Domino 6, the Domino Directory template has been modified to allow granular configuration control for each hosted organization. A new feature in Domino Administrator allows an xSP to register a new organization, creating the hosted configuration, producing a new certificate, creating a subdirectory, and configuring additional security mechanisms like Extended ACL. The ACL files are automatically created to logically separate the organizations.

Attention: If you enable the xSP configuration, the entire domain runs in xSP mode in order to ensure the proper security environment.

The multiple organization Domino Directory feature dramatically reduces the complexity of server administration in a hosted organizations (xSP) infrastructure. The administrator works with only one server environment, one Administrator client and one monitoring mechanism instead of managing multiple systems. You now manage just one single system, yet each organization on that server can function as if it is hosted by its own unique server.

13.2 Differences between Domino and xSP Domino

Most of the features and power of Domino are available in the xSP configuration. However, in order to provide the security model which hides all users and applications in one organization from another, some constraints have been applied to the xSP configuration. The differences between an xSP and a non-xSP configuration are as follows:

1. The design focus for the xSP feature was the use of Internet clients by end users. However, in order to support DOLS, testing was also performed with

applications using Notes IDs and the Notes APIs. As a result, with some constraints, the Notes client may work for some applications.

2. The Domino Directory is virtualized.
3. Once the first server is installed, the xSP configuration cannot be changed to a non-xSP configuration, and vice versa.
4. The Domino hierarchical naming scheme is fixed so that every name contains a common name and an organizational name. Organizational units are not supported.
5. The use of Internet Site documents is mandatory.
6. The Domino Directory is xACL-enabled and the User Activity Logging Confidential option is enabled.
7. The use of ACL files is mandatory.
8. The central authority uses the Admin client for administration. Some administration can be granted to organizational admins, but they must use the Web admin tool. If organizational admins will manage users, the CA must be configured and used.
9. Global Web settings are global Web rules that are added so that common Web server files are shared by all organizations.
10. Most databases and templates in the data directory have their ACLs modified to prevent access by any end user.
11. A number of default security settings are different in an xSP environment:
 - Typeahead is disabled.
 - MailLookupExhaustive is disabled.
 - MailAddressLookup is enabled.
 - ConvertNotesAddress is enabled.
 - HTTP_DatabaseBrowsing is disabled.
 - HTTP_AsynchronizeAgents is enabled.
 - WhiteList is enabled.
 - ServerCheckPasswords is enabled.
 - LdISite is enabled.
 - The ASP admins name is added to a number of security fields by default.

13.3 Planning for the hosted organization model

This section is intended to help you determine the supportive services that the hosted organizations model gives you.

13.3.1 Scalability and reliability

Speaking in terms of scalability and reliability, there are no architectural limits or coded limits specifically for a hosted organization server environment. It is really going to depend on the users' user profiles, what actions the users are performing, and what applications they are running. You can make use of all the clustering and partitioning benefits that Domino 6 gives you. But, since the xSP model is slightly different from the traditional Domino environment, the following specific features help you scale your xSP infrastructures in a more proper way than you could with Domino R5:

- ▶ Support for a configuration-only directory to improve server performance
- ▶ Qualified name lookups per organization in the Domino Directory to provide improved name lookup performance for any size directory
- ▶ Support for the use of a network sprayer to provide load balancing or failover capabilities

Note: You can make use of all options as in every other Domino 6 environment.

13.3.2 Protocol support

The Domino server tasks and native protocols have specifically been enabled to support the hosted organizations model. The Domino router, for example, has been modified to support multiple organizations simultaneously on the same physical/logical server. Table 13-1 shows which protocols are supported by the Domino 6 server specifically for hosted organizations.

Table 13-1 Protocols supported for hosted organizations

Usage Area	Protocol	Description
Messaging	IMAP SMTP POP3	POP3 and IMAP are access protocols only, that is, they retrieve mail. SMTP is required to enable POP3 and IMAP users to send mail.
Authentication	LDAP	Lightweight Directory Access Protocol (LDAP) is a standard Internet protocol for accessing and managing directory information. You can use LDAP to provide the mail clients with addressing services.

Usage Area	Protocol	Description
Security	SSL	SSL supports data encryption to and from clients and can be used in addition to Domino's security services.
Web services	HTTP IIOp	The HTTP task serves your Domino applications to a Web browser client and has been modified to also support sending mail via iNotes Web Access. The IIOp protocol makes sure you can serve Java code and programs to a browser client.
Offline services	DOLS	With Domino offline services you can offer your customers an offline solution for Web-based mail and applications.

13.3.3 Billing

Within a hosted organization setup, the billing for your customers is very important. Since you now have several customers in one environment, you need to find a way to structure your billing information. There are two choices:

1. A fee per user per time

Advantage: the administrative cost is almost zero.

Disadvantage: some users can use a lot of resources for the fee they pay.

2. Usage billing

Advantage: users pays for what they use.

Disadvantage: it's more costly to collect the usage info and prepare bills and justify them.

This is done on a weekly or monthly per-person basis, but you might also want to bill the actual usage of the system. The data is collected on a per-server basis and can be configured per protocol. Each record contains the organization name.

You will want to consider various billing methods based on your business requirements. Consider one of these billing methods:

- ▶ The number of users at the hosted organization site
- ▶ The number of users at the hosted organization site, plus disk space usage
- ▶ Actual use

To collect activity data by database, use activity logging.

Note: To collect the data by individual hosted organization, use the activity logging API to write a custom application that sorts the data by hosted organization. Then, you can bill each hosted organization accordingly.

13.3.4 Database management in a hosted organization setup

Domino 6 enables you to have more granular control over your databases and applications. The database server utility programs (such as compact, fixup, upcall, and design) now allow a directory to be specified. This means, for example, that an xSP administrator can configure program documents in the Domino Directory to have compact run on Company One's databases at 2 A.M. and Company Two's databases at 3 P.M. Therefore, every hosted organization will benefit from specific utilities without affecting or being affected by programs that run specifically for other hosted organizations on the same server.

This makes your performance, backup, and time zone issues easier to configure and control from an administrative perspective.

13.4 Setting up the xSP Domino environment

This section describes how to install and set up the xSP Domino environment.

13.4.1 Registering hosted organizations

During the registration process of a hosted organization, which is different from a regular Domino Server setup, some documents and files are automatically created for you, as follows:

- ▶ The certificate for the hosted organization is created.
- ▶ The hosted organization certificate is cross-certified with the service provider's certificate. A Cross Certification document is created.
- ▶ The service provider's certificate is cross-certified with the hosted organization certificate. A Cross Certification document is created.
- ▶ A Global Domain document is created. This document stores the primary Internet domain name by which the hosted organization is known and stores secondary Internet domain names by which the hosted organization can receive Internet mail.
- ▶ A data directory is created for the hosted organization. This directory is assigned the name that is specified in the Directory field on the Storage panel of the Register Hosted Organization interface. You can specify another

location in the Physical Storage Location field on the Storage panel of the Register Hosted Organization interface.

- In Win32 systems, the hosted organization's data directory is placed directly beneath Domino/data.
- In UNIX systems, the default is /local/notesdata.
- ▶ A mail subdirectory for the hosted organization is created beneath the hosted organization's data directory.
- ▶ A mail file is created for the hosted organization's administrator. This is an NSF and resides in the mail subdirectory for the hosted organization.
- ▶ An ACL file is created for each hosted organization to provide security for the hosted organization's directory.
- ▶ An extended ACL is applied to the Administration Requests database (ADMIN4.NSF) and the Domino Directory (NAMES.NSF) to restrict access to the data in those databases. (The extended ACL is enabled on the Domino Directory when the first hosted organization is registered.)
- ▶ The database ACL entry for "Anonymous" is changed from NoAccess to Reader access in NAMES.NSF when the first hosted organization is registered.
- ▶ Entries are made for the hosted organization administrator in the database ACLs and the extended ACLs to allow the hosted organization administrators to Browse, Read, Create, Delete, and Write documents for their hosted organization.
- ▶ Extended ACL entries are created for all users and groups in a hosted organization (* /HostedOrganizationName) providing Browse and Read access to that hosted organization only.
- ▶ An extended ACL entry is created for "Anonymous" for each hosted organization with all access disabled. Entries are also made in the Form and Field Access in extended ACLs.
- ▶ An Internet Site document is created for each Internet service for which you provide an IP address or hostname on the Internet panel of the Register Hosted Organization interface. If you provide an address or hostname for multiple protocols, you are prompted to create the Internet Site document for each Internet protocol. You must create the Internet Site document in order to use the corresponding Internet protocol. You are also prompted to create one Web Site document for each hosted organization. If a hosted organization has multiple Web sites, create one additional Web Site document for each additional Web site.
- ▶ The Basics tab on the Server document contains the field "Loads Internet configurations from Server/Internet Sites documents," which is enabled by default and cannot be changed in a hosted environment.

- ▶ The HostedOrganizationAdmin group is created by default (when you set up the hosted environment) and administrators are automatically added to that group. Administrator groups enable you to administer groups of people with administrator rights at one time instead of individually establishing rights and settings for each hosted organization administrator.

13.4.2 Steps for setting up the environment

Setting up the xSP environment consists of understanding the information presented in this chapter, as well as completing the tasks listed below:

- ▶ Installing the first server or additional servers for hosted environments
- ▶ Setting up the Domino Certificate Authority for hosted organizations
- ▶ Setting up Policy Documents in a hosted environment
- ▶ Binding the IP addresses of the hosted organization to the xSP server
- ▶ Creating loopback addresses in a hosted environment
- ▶ Configuring Internet sites with Web Site and Internet Site documents
- ▶ Using Global Web Settings documents
- ▶ Configuring activity logging for billing hosted organizations
- ▶ Setting up additional security

Restriction: Converting an existing domain into an xSP domain is not supported, nor is conversion of an xSP domain into a non-xSP domain.

13.4.3 Installing the server

To start the installation of the first xSP server, use the following commands:

1. Run the Setup command

For Win32 systems, run this command from the directory in which the SETUP.EXE file is located.

You can use Start\Run and type (Figure 13-1 on page 415):

<filepath>\setup.exe -asp

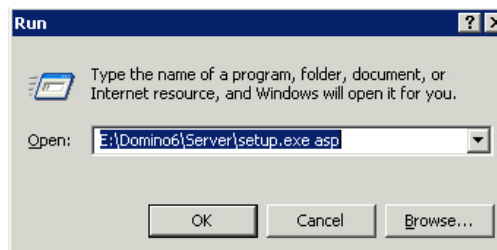


Figure 13-1 xSP installation start

For UNIX, use this command:

```
<filepath>/install -asp
```

Note: During the software installation process you will not see any indication that you specifically install the software for a xSP environment. The screen you see are just the same as installing a regular Domino server.

2. Choose the Domino Enterprise server setup.
3. After installation, start the Domino server.

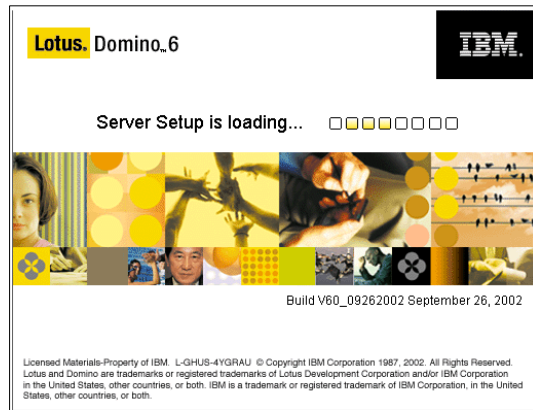


Figure 13-2 xSP server setup loading

4. As the Setup wizard runs, enter the information appropriate to your configuration.

This example procedure shows the setup of a first server in the xSP environment:

1. You need to choose one of the following:
 - a. Set up the first server or a standalone server.
 - b. Set up an additional server.
2. Enter the new server name and the server title.
3. Enter the organization name (Figure 13-3) and optionally, an OU name.

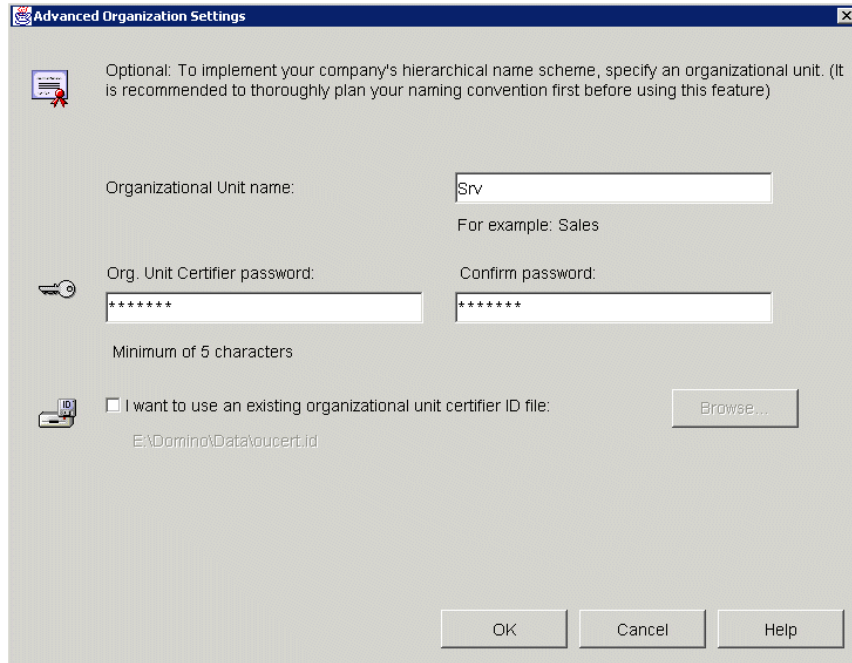


Figure 13-4 xSP - create an organizational unit

4. Set the Domain Name.
5. Register an Administrator.
6. Set the network settings (Figure 13-5 on page 419) and additional encryption and compression.

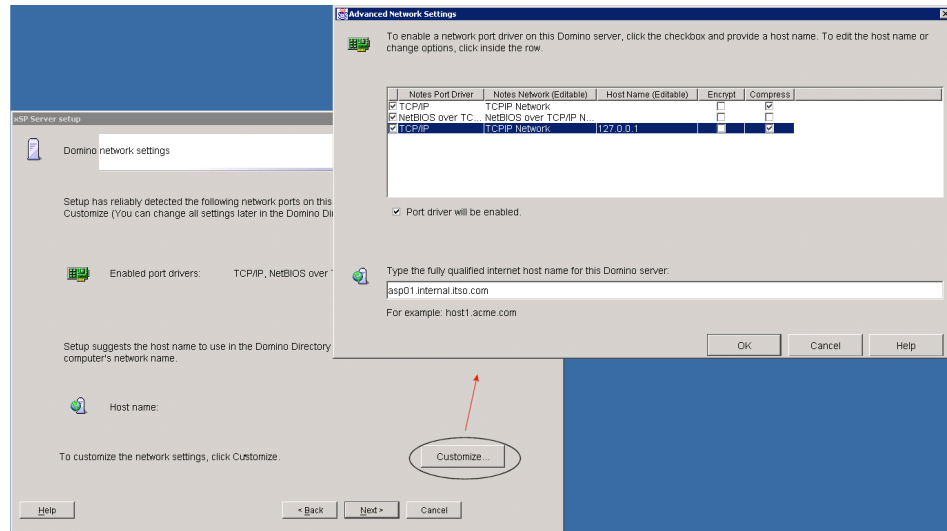


Figure 13-5 xSP - network settings

Attention: Make sure that you understand the network encryption and compression settings before using them.

7. Set the required server tasks (Figure 13-6).

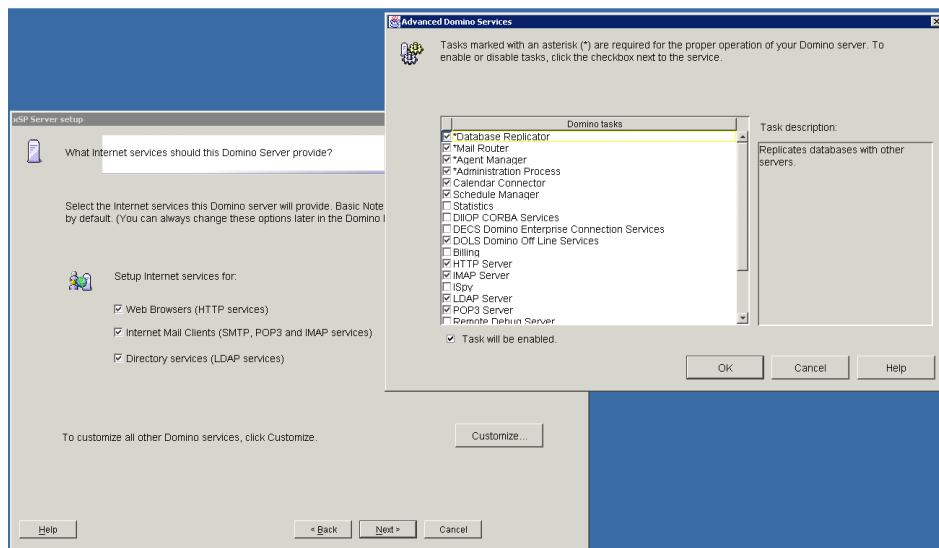


Figure 13-6 xSp - required server tasks

8. Confirm the settings displayed in the last summary box by clicking **SetUp**.

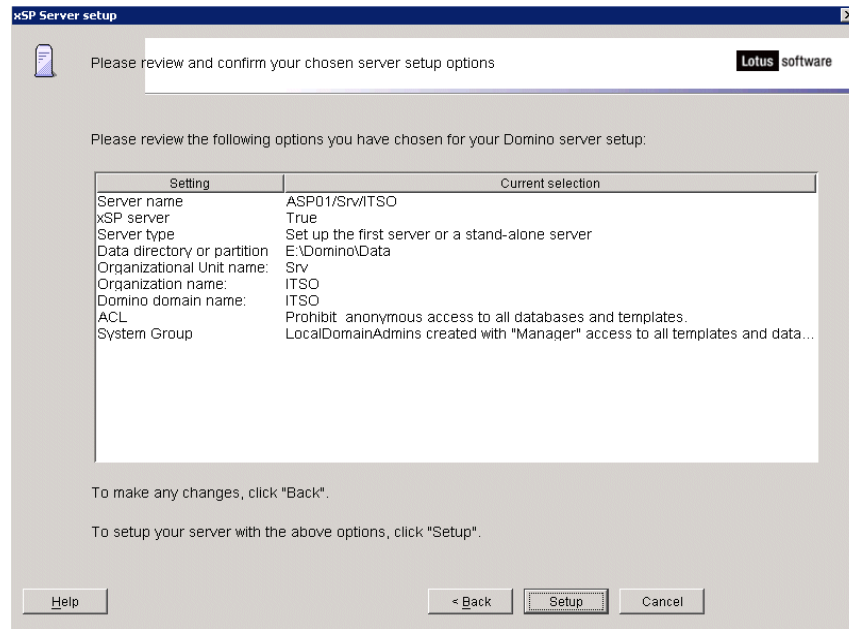


Figure 13-7 xSP - confirm settings

The installation program is now setting up the server configuration. Wait until all the screens are closed.

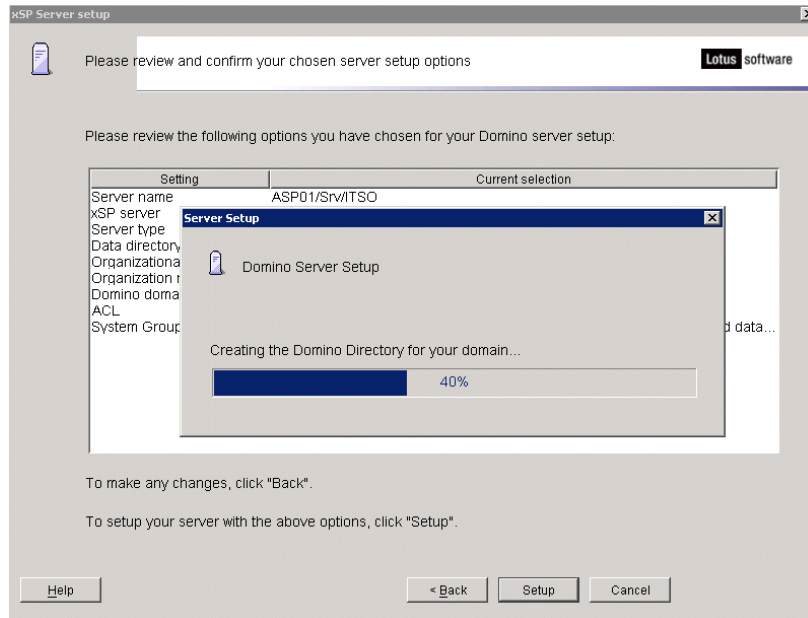


Figure 13-8 xSP - server setup

9. Start the Domino Server.

The basic server setup is now finished. Follow the steps and procedures in the remaining parts of this chapter to configure the server correctly.

Creating additional servers

To create an additional xSP server in this Domain, you can use the Domino Administrator client and use the same procedures you use when installing a regular Domino 6 server.

This is also the case when adding servers to a cluster.

13.4.4 Setting up the Domino Certificate Authority

When registering hosted organizations, you can use the Domino server-based certification authority (CA). If you don't use the server-based CA, you can use Domino's certifier ID and password for security purposes.

A CA vouches for the identity of both server and client by issuing Internet certificates that are stamped with the CA's digital signature. The digital signature assures the client and server that both the client certificate and the server certificate can be trusted.

The CA also issues trusted root certificates, which allow clients and servers with certificates created by different CAs to communicate with each other.

The following statements must be considered when using the CA process:

- ▶ When using Internet certificates, each hosted organization must have its own Domino CA.
- ▶ If the hosted organization uses DOLS, or if they require Notes IDs, the hosted organization must use the Domino server-based CA.
- ▶ If the hosted organization administrator plans to use the Web Administrator, that hosted organization must use the Domino server-based CA to register users.

Tip: As part of setting up a CA, create a Certificate Requests database. Then, using the Certificate Requests database, you can submit Internet certificate requests through a browser, pick up new or renewed certificates, and receive notification regarding request status.

More information about creating certificates with the Certificate Authority process, and the exact steps to follow, can be found in Chapter 11, “Certificate Authority (CA) process” on page 357.

13.4.5 Setting up policy documents

When you are registering a hosted organization, create an organizational policy and a registration settings document when you are prompted to do so. Also create an explicit policy that includes a registration settings document before you register users of the hosted organization.

If you want to create a policy for all hosted organizations in the Domino Directory, do not enter a policy name—by default, Domino will enter the asterisk for you and the policy will apply for all organizations.

- ▶ For hosted organizations, use: */<hosted organization>
- ▶ For hosted organizations, to indicate all hosted organizations in the Domino Directory, use an asterisk (*).

Policy-based administration is described in detail in Chapter 15, “Policy-based administration” on page 449.

13.4.6 Binding the IP addresses to the xSP server

If you assign an individual IP address to each hosted organization, use one of the following procedures to bind the IP address of each hosted organization to the network interface card in the xSP server.

This procedure applies only to configurations that include unique IP addresses.

► SUN Solaris

Enter these commands as the root user, where <hme0> is the network interface card:

- ifconfig <hme0>:1 plumb
- ifconfig <hme0>:1 <hosted_company1_ip> <server_ip> up

Adding additional IP addresses:

- ifconfig <hme0>:2 plumb
- ifconfig <hme0>:2 <hosted_company2_ip> <server_ip> up

► IBM AIX

Enter the following command as the root user, where <en0> is the network interface card:

```
ifconfig <en0> alias <IP address of hosted organization> netmask 255.0.0.0
```

► Microsoft NT 4.0

- a. From the Microsoft NT desktop, right-click the **Network Neighborhood** desktop icon and choose **Properties**.
- b. Choose **Protocols**, and then double-click **TCP/IP Protocol**.
- c. From the TCP/IP Properties box, click **Advanced**.
- d. Click **Add** to add additional hosted organization IP addresses. Accept the default subnet mask of 255.0.0.0.

► Microsoft Windows 2000

- a. From the Windows 2000 desktop, right-click the **Network Neighborhood** desktop icon and choose **Properties**.
- b. Right-click the **Ethernet** adapter, and then select **Properties**.
- c. From the Adapter Properties box, double-click **Internet Protocol (TCP/IP)**.
- d. Click **Advanced**.
- e. Click **Add** to add additional hosted organization IP addresses. Accept the default subnet mask of 255.0.0.0.

13.4.7 Creating loopback addresses

If you use a network router in the xSP configuration and you assigned a unique IP address to each hosted organization, you must create a loopback address for each hosted organization. The instructions vary by platform.

► SUN Solaris

Enter these commands as the root user:

- a. `ifconfig <lo0>:1 plumb`
- b. `ifconfig <lo0>:1 <hosted_company1_ip> <server_ip> up`
- c. `ifconfig <lo0>:2 plumb`
- d. `ifconfig <lo0>:2 <hosted_company2_ip> <server_ip> up`

Add additional loopback configurations:

- a. `ifconfig <lo0>:x plumb`
- b. `ifconfig <lo0>:x <hosted_companyx_ip> <server_ip> up`

► IBM AIX

Enter this command as the root user:

```
ifconfig <lo0> alias <IP address of hosted organization> netmask 255.0.0.0
```

► Microsoft NT 4.0

- a. From the Windows NT desktop, right-click the Network Neighborhood icon, and choose Properties.
- b. Click Adapters, choose Add, and select MS Loopback Adapter.
- c. When the adapter has been added, click Protocols and select TCP/IP Protocol.
- d. Select MS Loopback Adapter.
- e. Click the Specify an IP Protocols tab, and enter the IP address for the HTTP cluster 9.95.87.142.
- f. Enter the subnet mask 255.255.255.128 and click OK.
- g. Restart the system.

► Microsoft Windows 2000

- a. From the Windows 2000 desktop, right-click the Network Neighborhood icon, and choose Properties.
- b. Right-click the Ethernet adapter and choose Properties.
- c. From the Adapter Properties box, double-click Internet Protocol (TCP/IP).
- d. Click Advanced.
- e. Click Add to add an additional IP address. Accept the default subnet mask of 255.0.0.0.

13.4.8 Configuring Global Web Settings and Internet Site documents

The Site documents contain the information needed to run the Internet servers in a service provider configuration. They support all possible configurations of IP addresses and DNS host names.

An Internet Site document is automatically created for each Internet service for which you provide an IP address or host name on the Internet panel of the Register Hosted Organization interface. If you provide an address or host name for multiple protocols, you are prompted to create the Internet Site document for each Internet protocol.

You must create the Internet Site document in order to use the corresponding Internet protocol. You are also prompted to create one Web Site document for each hosted organization. If a hosted organization has multiple Web sites, create one additional Web Site document for each additional Web site.

Note: The Site document is created containing default information; you must enter additional information in each Site document either during hosted organization registration or later. The Internet protocol is not active until the corresponding Internet Site or Web Site document is completed and saved.

Information about Internet Site and Global Web Settings documents is available in Chapter 12, “Internet Site architecture” on page 385.

13.4.9 Using Global Web Settings documents

Domino automatically creates a Global Web Settings document when you install the Lotus Domino service provider software. The Global Web Settings document is associated with three Web Site Rule documents that automatically create several directories that may be required by numerous users at any hosted organization.

The Web Site Rule documents make files accessible from one central location on the server, so that these files do not need to be individually downloaded for each hosted organization. The benefit derives from easier administration and a substantial savings in disk space because the service provider can provide the files to all users that need them without having to duplicate them for each individual hosted organization.

By default, the Global Web Settings document applies to all servers in a Domino domain. Three associated Web Site Rule documents that contain the settings shown in Table 13-2 on page 426 are created when the Global Web Settings document is created in a hosted environment.

Table 13-2 xSP Web Site Rule documents

Web Site Rule document	Type of Rule	Incoming rule pattern	Target server directory
DOLS	Directory	/download/*	domino\html\download
iNotes help files	Directory	/inotes5/help/*	domino\html\inotes5\help
iNotes.cab	Redirection	/iNotes.cab	domino\html\inotes.cab

Note: The Web Site Rule document for DOLS-enabled hosted organizations downloads to central location files that are required when the hosted organization tries to access a DOLS-enabled database.

The iNotes.cab file is an archive file that contains controls that are installed into a browser and make iNotes features available to your browsers.

The iNotes help files are downloaded to a central location on the server so that they do not have to be individually downloaded for each hosted organization.

These Web Site Rule documents can be reconfigured at any time using the Domino Administrator client.

Information about Internet Site and Global Web Settings documents is available in Chapter 12, "Internet Site architecture" on page 385.

13.4.10 Configuring activity logging for billing

Now that your server is configured, you need to set up activity logging in order to collect information that can be used for billing purposes.

The easiest way is to set up collecting data with the new Server Activity Logging feature. In this way the data is collected on a per-server basis and can be configured per protocol. Each record contains the organization name so that the xSP can determine the appropriate billing model for its customers.

This service is an extremely low-cost, high-density mechanism. Activity data is queued in memory, well-compressed, and large records are written periodically to the log file. When the data needs to be processed, this can be done during off-peak hours, or it can be done on another machine. The collection speed is fast enough to ensure that no data is ever lost.

You can enable activity logging on one server, or on more than one server, or on all servers in your domain. You need to start in the Configuration Settings document to enable activity logging on specific servers that you designate:

1. From the Domino Administrator, click Configuration -> Server -> Configurations.
2. Do one of these:
 - a. To enable activity logging on all servers in the domain, open the existing All Servers Configuration Settings document.
 - b. To enable activity logging on all servers except one (or a small number of servers), open the existing All Servers Configuration Settings document and complete the fields on the Activity Logging tab as shown in Table 13-3. Click Add Configuration to create a new Configuration Settings document for each server that is an exception to the settings in the All Servers Configuration Settings document. Disable activity logging for the servers on which you are not running activity logging.
 - c. To enable activity logging for one server, create a Configuration Settings document.
3. On the Activity Logging tab, complete the fields in Table 13-3.

Table 13-3 Configuring activity logging

Field	Action
Activity logging is enabled	Select this check box to enable activity logging on each server that you designate.
Enabled Logging Types	Select all logging types for which you want to collect billing information.
Checkpoint interval	Enter the number of minutes that transpire between activity logging updates to LOG.NSF. The checkpoint interval applies to the logging types that you selected and that have open, active sessions.
Log checkpoint at midnight	(Optional) Select this check box to create Notes session and Notes database checkpoint records every day at midnight.
Log checkpoints for prime shift	(Optional) Select this check box to create Notes session and Notes database checkpoint records at the beginning and end of a specific time period. Specify the start and end times for the time period.

4. Click Save -> Close.

13.4.11 Setting up additional security

This section describes additional available security options.

Extended ACL

The Extended ACL (xACL) mechanism ensures that a person in a certain hierarchy can only see the Person documents whose organization name is in the same hierarchy. This makes the xACL a strong, low-level Directory security mechanism. In the Domino Directory, all of the Person and Group documents have hierarchical names. The hosted organization name is part of that hierarchy.

By default, the setup adds appropriate settings to the xACL to ensure that organizations cannot see the Person documents from other organizations.

Chapter 14, “Extended ACL” on page 431 describes how to set up and plan your Extended ACL.

Attention: Configuring the extended ACL should be done very carefully; minor manual changes may lead to security holes in your security model.

ACL files

The new ACL file security mechanism is similar to the dirlink mechanism that exists in Domino R4, R5, and still exists in Domino 6. The ACL file prevents users in one hosted organization from traversing a directory that belongs to another hosted organization.

During hosted organization registration, the new mechanism automatically creates an ACL file in a subdirectory of the data directory. In the ACL file, an administrator can specify who can see the subdirectory and who can access its databases. In this way, the ASP administrator can use the ACL files in every organization’s subdirectory of the data directory to specify that only the ASP administrators and that particular organization can see the subdirectories.

Note: If a hosted organization's ACL file is deleted, users in other hosted organizations may be able to review the content of the directories belonging to the hosted organization that is no longer protected by an ACL file.

The content of a sample ACL file for a hosted organization named “ITSO” with Anonymous access is shown below. The ACL file resides in the Domino data directory and is named ITSO.ACL (in this example) and can have the following content:

```
.ASP Admin/ASP  
*/ITSO
```

Anonymous
LocalDomainServers
LocalDomainAdmins
[owner=ITS0]

Do not confuse hosted organization ACL files with database ACLs, which control server, user, and group access to databases that reside on a Domino server.

Note: The ACL files do not ensure the protection of databases, which depends on how individual database ACLs are set.

13.5 Additional information

This section lists some additional information and references related to hosting features.

Where to store data for hosted organizations

To decide where to store a hosted organization's data, evaluate whether you are saving private data or shared data. Store a hosted organization's private data in a directory belonging to the hosted organization. Store shared data in a common data directory accessible to all.

Opening databases on an xSP server

When the service provider administrator uses the File -> Database -> Open menu commands to open a database, the Open Database dialog box does not list all of the databases on the server, but all of the databases are available by typing the database name in the Filename field, and then clicking Open.

You may want to create bookmarks for the most frequently opened databases.

Additional information

You can find any additional information about administering, creating, moving, and deleting hosted organizations in the Domino Administration 6 Help database in the section "Service Provider".



Extended ACL

This chapter describes the possibilities and benefits of the Extended Access Control List (xACL) feature that is included in the Domino 6 Directory template.

The new extended ACL controls give enterprises the ability to delegate administration to regional administrators without giving them manager access to the Domino directory. You can configure these regional administrators to allow them to administer only directory documents related to their own organizational units.

You can also create a multiple organization Domino Directory, using extended ACLs to ensure that users have access to only their organization's information, especially in a hosted organizations environment.

This chapter discusses the benefits of the xACL feature and also shows how to create and configure the extended ACL for your Domino directory.

14.1 Usage and benefits

The new extended Access Control List (xACL) enables you to delegate administration to regional administrators. In addition to the ACL and roles structure, you can explicitly give regional or local administrators access to certain documents or fields in the Domino Directory. You can configure these regional administrators to allow them to administer only directory objects within their own organizational unit.

Once you define the regional or local administrator groups, you can have them edit specific groups, users and even Policy documents for their locations.

When you have hosted organizations, as described in Chapter 13, “Domino hosting features” on page 407, you can use the xACL to create a multiple organization Domino Directory, using extended ACLs to ensure that users have access to only their organization's information. In the Domino Directory, all of the Person and Group documents have hierarchical names. The hosted organization name is part of that hierarchy. The xACL mechanism ensures that a person in a certain hierarchy can only see the Person documents whose organization name is in the same hierarchy, which makes the xACL a strong, low-level Directory security mechanism.

You can also plan on using another xACL on your Extended Directory Catalog.

14.1.1 Planning and considerations

Planning an extended ACL for your Domino Directory is just as important as setting up the regular ACL structure. Settings that have not been created correctly can cause some serious accessibility problems and a lot of work to correct them.

Attention: Server processes such as the Router task do not enforce extended ACL restrictions.

Before you enable the xACL, make sure you plan it carefully and that you understand the following implications:

- ▶ To ensure that the database replicates properly, extended access requires the use of the advanced database ACL option "Enforce a consistent Access Control List across all replicas."
- ▶ You can use the xACL options on Domino 6 servers only after you enable extended access. You can't make changes to the database on a server running an earlier release because the changes can't replicate to a Domino 6

server. If you enable extended access, you must make directory changes only to a replica on a Domino 6 server.

- ▶ Enabling extended access enforces the database ACL, extended ACL, and Readers and Authors fields for Notes clients looking up names in the directory.
- ▶ If you enable extended access, your Notes users must have at least Reader access in the database ACL.
- ▶ Enabling extended access enforces the database ACL and extended ACL for anonymous LDAP searches of the directory. Enabling extended access removes the Anonymous LDAP access settings from the domain Configuration Settings document, and they remain removed unless you disable extended access at a later point. By default the directory database ACL gives Anonymous users No Access, so if you want LDAP users to search the directory anonymously, you must change the access for the Anonymous entry if you enable extended access.
- ▶ Enabling extended access may take a few minutes on a very large directory database. The Notes or Domino Administrator client is unavailable for other purposes during this process.
- ▶ Although the access set for a user in the extended ACL can never exceed the access the database ACL, including the database ACL privileges and roles, allows the user.
- ▶ An extended ACL cannot restrict the access of the following:
 - User with Manager database access
 - Administrator with “Full Access administrators” access to a server (controlled through the Server document in the Domino Directory)
 - User with Designer or Manager database access from modifying the directory design
 - The Domino servers Server Tasks

Note: Do not enable the Directory extended Access Control List if you are not confident with all the settings mentioned in this section.

14.2 Implementing and administering the xACL

Each document in the Domino Directory is controlled by xACLs to allow or disallow access. Since the xACL is a new option available in Domino 6 and by default disabled, you need to enable it first and then Administer the ACL settings as you have planned.

14.2.1 Enabling the xACL

To enable extended access for a Domino Directory or Extended Directory Catalog, do the following:

1. Open the database and choose File -> Database -> Access Control.
2. Make sure you have Manager access in the database ACL.
3. Click Advanced, and then select Enable Extended Access.

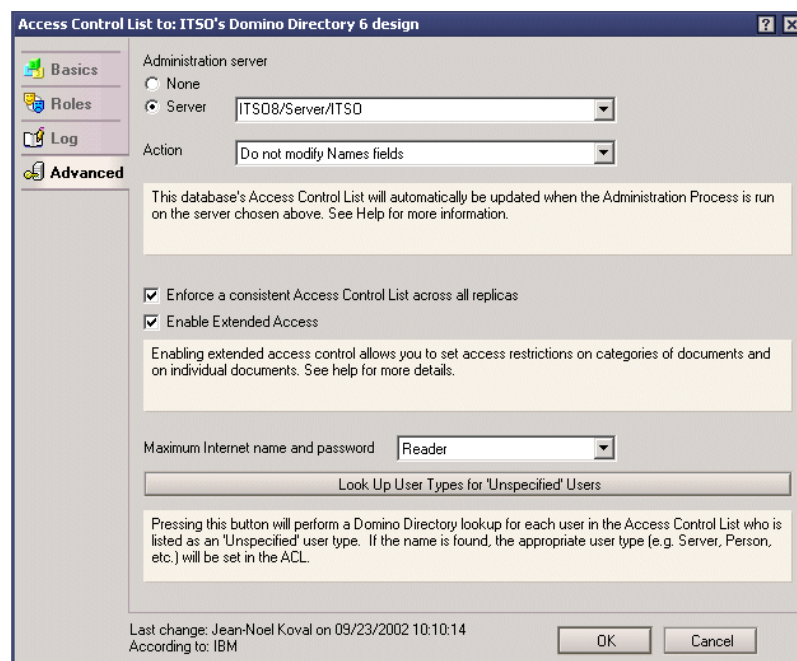


Figure 14-1 Enabling the xACL advanced setting

4. At this prompt, click Yes to continue. You will see the message: "Enabling extended access control enforces additional security checking. Do you want to continue?"

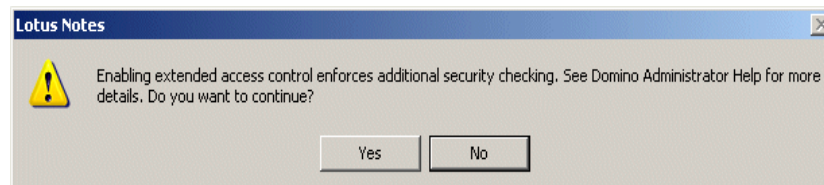


Figure 14-2 Enabling the xACL - consistent ACL warning message

5. At the prompt “Consistent access control must be enabled first. Do you want to enable it now?”, which appears only if the advanced database ACL option “Enforce a consistent Access Control List across all replicas” is not yet enabled, click Yes.

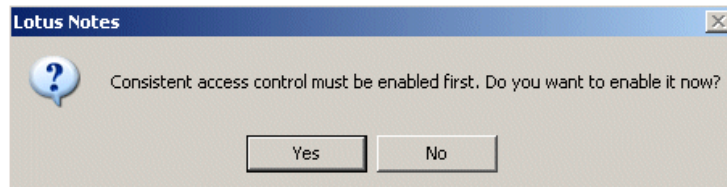


Figure 14-3 Enable xACL

6. At the prompt “If more than one administrator manages extended access control for this database, enable document locking on the database to avoid conflicts”, click OK.

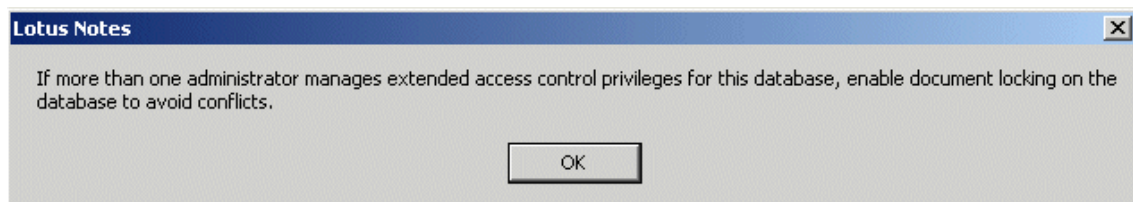


Figure 14-4 Enable xACL - document locking warning

7. Click OK in the Access Control List dialog box.
8. At the prompt “Enabling extended access control restrictions. This may take a while.”, click OK.

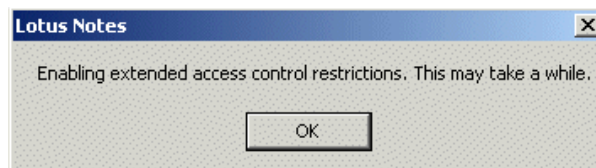


Figure 14-5 Enable xACL - final message

9. Look at the status bar on the client to see the status of this process (Figure 14-6 on page 436).

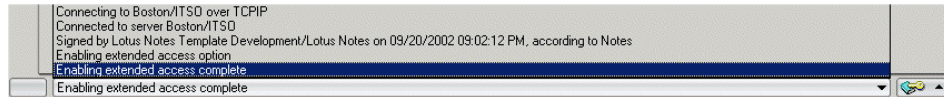


Figure 14-6 enable xACL - status bar

Your Domino Directory is now enabled to use the Extended Access Control List; you can set the xACL settings now.

Setting up the xACL

To set up an extended ACL, you must use the “Extended Access at target” dialog box, which you open from the database Access Control List dialog box by clicking Extended Access; see Figure 14-7.

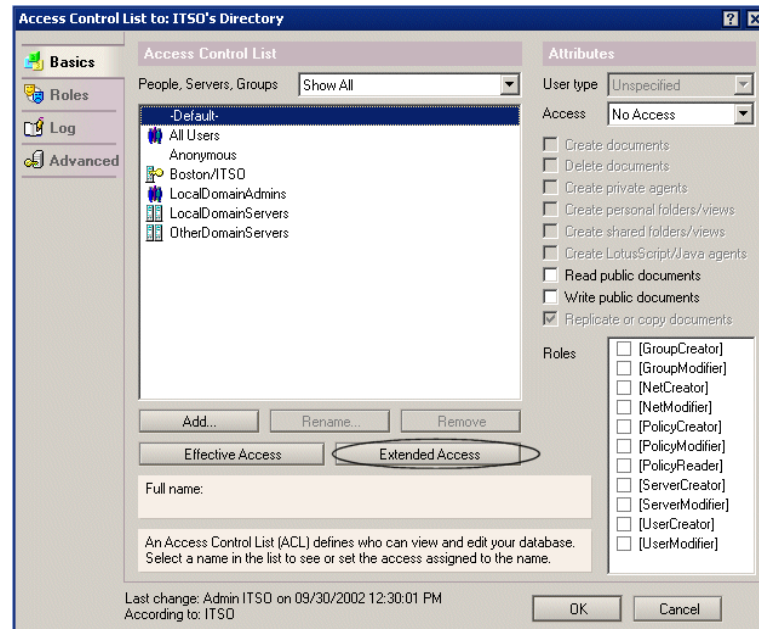


Figure 14-7 Access xACL

Once you have opened the xACL dialog box, you will see a screen as shown in Figure 14-8 on page 437 where the numbers indicate the following:

1. Target pane
2. Access list pane
3. Attributes pane
4. Form and Field access button

5. Effective Access button
6. Log button

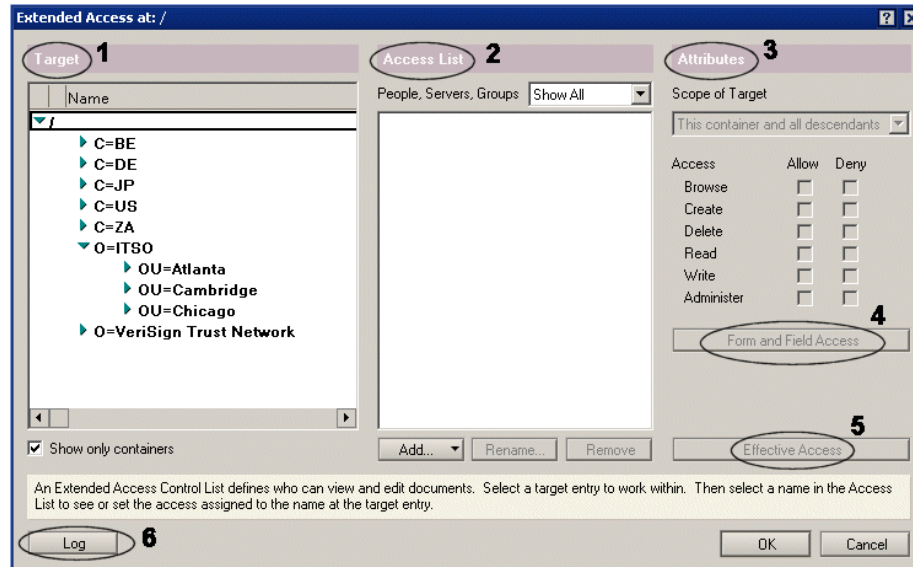


Figure 14-8 xACL - main dialog screen

This section explains the panes and buttons that are displayed in Figure 14-8 and guides you through the process of setting your Domino directories for xACL. The end of this chapter also offers two practical examples that you can use as a reference for testing purposes.

1 - Target pane

The target pane view shows the hierarchy of your registered organization, containing the following hierarchy below the /(root) entry:

- Person documents
- Server documents
- Certifier documents
- Policy documents

Select a target to specify either a category of documents or a specific document to which you are controlling the subject's access (users, servers, and groups).

Selecting a category of documents as a target is recommended because:

- You can set access to multiple documents at once
- The access applies to documents added to the category in the future

- Domino can verify a subject's directory access more quickly when there are fewer occurrences of the subject in an extended ACL than when there are many.

In addition, when you use categories as targets, it's easier to manage the extended ACL because there are fewer subjects to track.

2 - Access list pane

The access list pane lets you select a name or entry for which you are setting access to a selected extended ACL target.

The panes view shows all selected entries, including entries whose access is set at and inherited from a higher target through the scope “This container and all descendants.”

Tip: You can select "Show Modified" to see only the subjects with access set directly at the target.

To add a subject to an extended ACL, you select the target and then click Add below the People, Servers, Groups box in the “Extended Access at target” dialog box. You can specify any of the following as subjects in an extended ACL:

- Individual user or server
- Group
- Self
- Wildcard that represents documents at a specific location in the directory name hierarchy, for example, */West/Acme
- Anonymous
- -Default-

All the entries, except for self, are known entries as they are used in the ACL list. However, Table 14-1 shows the meaning of some specific subjects as we assume that you are familiar with the people and group entries.

Table 14-1 xACL entries

Entry	Purpose
Anonymous	As in the database ACL, the subject Anonymous controls the access of all users and servers that access a server without first authenticating. Anonymous access applies to access via all the supported protocols.

Entry	Purpose
-Default-	<p>Adding and setting access for the -Default- subject at a target is optional. If you set access for -Default- at a target, all users and servers whose access is not determined by another subject at the selected target get the access set for -Default-.</p> <p>If you add the -Default- subject to a target and you want some users to have different access to the target than the -Default- access, add a subject or subjects that represent those users to the target with the desired access.</p>
Self	<p>The subject Self is available only for an extended ACL and not the database ACL. At a target category only, you can use Self to define the access that all users have to their own documents that fall under the target category. A user's own document is one with a distinguished name that matches a distinguished name presented by the user.</p> <p>Use Self so that you can use one subject to control all users' access to their own documents at a target category.</p>
Servers	<p>In general an extended ACL can't restrict the access of a Domino 6 server.</p> <p>The exception is granting a Domino 6 server Administer access to a target category that represents a particular location in the directory name hierarchy. Doing so allows the server to be an extended administration server that can carry out Administration Process requests for documents under the selected target category.</p>

When possible, use subjects that represent groups of users like -Default-, Self, groups or wildcard subjects rather than individual users as subjects because when you use subjects that represent groups of users, you minimize the number of subjects in the extended ACL to add and manage and you optimize access-checking performance.

Tip: If the database ACL and an extended ACL both list a particular subject, the Administration Process requests can rename or delete the subject in the extended ACL, as well as in the database ACL.

When you remove persons from the xACL, make sure you save and close the Dialog Box before you continue. Some "old" settings might still appear in one of the panes where you just removed it.

3 - Attributes pane

There are several access settings you use to control a subject's access to an extended ACL target. For each access setting you choose Allow or Deny.

Tip: You can leave an access setting unchecked, but if you do, other subjects in the extended ACL or database ACL determine whether the subject is allowed or denied the access. It's better to select Allow or Deny to help ensure you get the access control results you expect.

Access settings apply to existing documents at a selected target and if the selected target is a category, it will also apply to documents added to this category in the future.

Table 14-2 shows the settings and the settings' purpose.

Table 14-2 xACL document attributes

Setting	Allowed/disallowed task
Browse	Allows/disallows a user to access a document
Create	Allows/disallows a user to create a new document
Delete	Allows/disallows a user to delete a document

Table 14-3 lists the access settings that control access to a field within a document.

Table 14-3 xACL field attributes

Setting	Allowed/disallowed
Read	Allows a user to read a field. The user must also have Browse access to the document.
Write	Allows a user to modify a field.

The last setting controls Administrative control to the Extended ACL; see Table 14-4 on page 441.

Table 14-4 xACL Administer attribute

Setting	Allowed/Disallowed
Administer	<p>Grant Administer access to allow someone with Designer or Editor access in the database ACL to modify access settings at an extended ACL target.</p> <p>You can allow someone to manage access to documents under a target category without granting the person Manager access in the database ACL.</p> <p>*A user with Editor or Designer access in the database ACL does not have the Administer access by default; you must grant the user that access explicitly.</p> <p>**You grant someone Administer access to a target category and not to a specific document.</p>

Using the Administer option gives you the ability, even in very large companies, to delegate tasks throughout the organization towards several levels of administrative tasks.

4 - Form and Field access

Once you select Form and Field Access, the dialog box shown in Figure 14-9 appears.

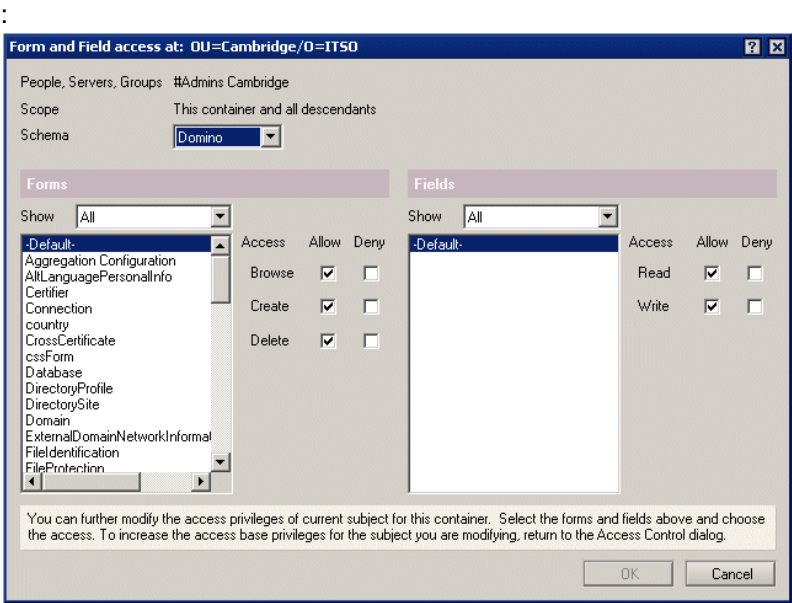


Figure 14-9 Form and Field access dialog box

You can now set form-specific access settings that are exceptions to the selected subject's default access at the selected target. As you see, the -Default- entry will be Allowed access for all options, which means that you allow access to all forms for that specific entry. When you want to Deny access in specific forms, you can scroll down, select the form, and set the correct setting. As soon as you have selected the form, you will see the field names of that form appear in the right pane.

You can, as in the form pane, select fields and Allow or Deny access to them for this specific entry. You can either start to deny the default entry and allow some specific forms and fields, or just allow all access to all forms and deny some others.

Setting Allow or Deny on specific forms and fields gives you control over the actions that your delegated employees can execute.

5 - Effective access

The Effective Access dialog box shows you all the access possibilities that belong to a specific entry. It summarizes the settings you have set in the xACL, including Form and Field access.

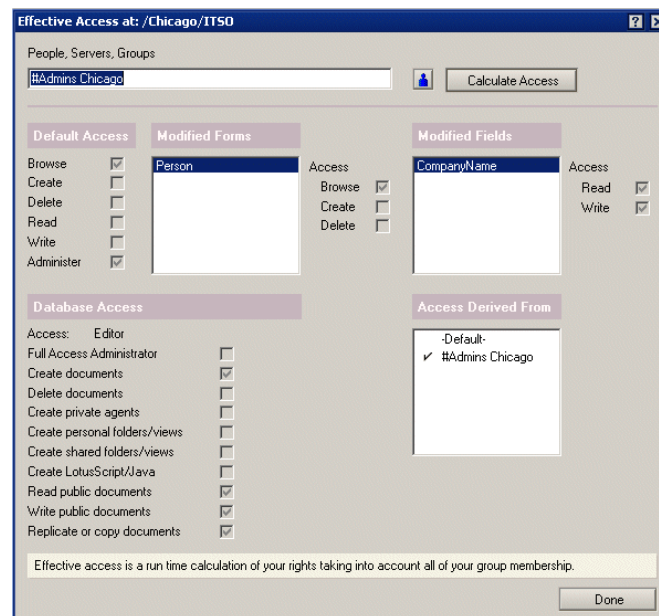


Figure 14-10 xACL - effective access summary

Make sure you always check this summary listing after you add or change settings for any entry.

6 - Log

The xACL log functionality displays all changes that have been made to an extended ACL and to the database ACL. Each entry in the list shows when the change occurred, who made the change, and which entry has been changed.

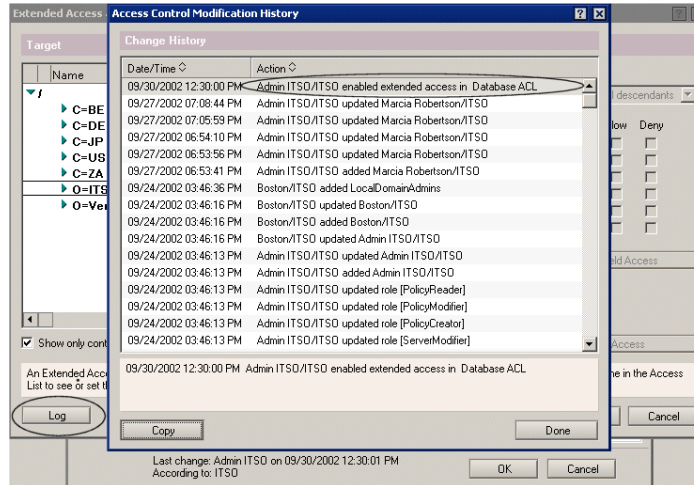


Figure 14-11 xACL - log

Disabling the xACL

Disabling extended access takes effect immediately and irreversibly removes any extended ACL restrictions that have been set, and therefore alters security checking for the database. You will remove all restrictions set on forms and fields, and the database ACL will no longer be restricted by extended ACL access settings. In addition, the database ACL will no longer be enforced for Notes client lookups to the directory, and the domain Configuration Settings will resume as the access control mechanism for anonymous LDAP searches of the directory.

Disabling extended access removes all evidence of extended ACL settings, information that cannot be recovered unless you restore it from a recent backup or archive of the directory, or unless you write down the settings prior to disabling them and then reapply them manually later.

Note: Do not disable extended access if you have any uncertainty about doing so.

To disable extended access:

1. Open the database and choose File -> Database -> Access Control.
2. Make sure you have Manager access in the database ACL.

3. Click Advanced and then deselect the “Enable Extended Access” check box to remove the selection.
4. At the prompt “Warning: Disabling extended access removes all extended access control restrictions that have been set. Do you want to continue?”, click Yes if you are sure you want to disable extended access; otherwise, click No.
5. Click OK in the Access Control List dialog box.
6. At the prompt “Disabling extended access control restrictions. This may take a while.”, click OK.

The status bar in your Notes Client or Administrator indicates when the process is complete.

14.3 Extended administration server

An extended administration server is an administration server that is allowed to process Domino Directory administration requests. It distributes the administration responsibilities across multiple servers, which is especially useful for remote administration of servers that are geographically dispersed. This concept of the extended administration server was developed in order to make remote administration available to administrators.

What practically happens is that you give one or more servers access in the extended ACL and assign them the Administration option, as shown in Figure 14-12.

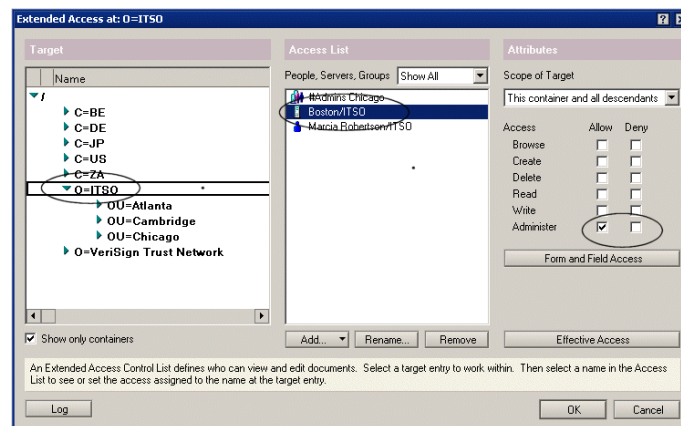


Figure 14-12 xACL extended administration server

When you delegate extended administration servers, the target documents in the Domino Directory are added to, modified, or deleted only if they belong to the particular assigned entry in the target pane.

You can designate extended administration servers for one Domino Directory by selecting an entry in the Domino Directory's extended access interface (Target pane) and designating a particular server as an administrator for that namespace. The new interface allows you to specify the exact namespace that an individual administration server is responsible for.

Attention: All your Domino servers in the domain must be Domino 6 servers to use the extended administration server feature.

Setting up an extended administration server

Complete these instructions to set up an extended administration server.

1. From the Domino Administrator, click Files and then open the Domino Directory (NAMES.NSF).
2. Choose Files -> Database -> Access Control.
3. Select Advanced -> Enable Extended Access.
4. Select Basics -> Extended Access.
5. In the Names list, select the namespace (an organization, or one or more organizational units) for which you are assigning an administration server.
6. Select the server that you are designating as an administration server.
7. Choose one of these "Access applies to" settings:
 - *This entry only:* to assign the selected administration server to the selected namespace only. Namespaces that are subordinate to the selected namespace are not affected by this selection
 - *This entry and all descendants:* to assign the selected administration server to the selected namespace and to all subordinate namespaces.
8. In the Access field, in the Allow column, click Administer.
9. Click OK -> Yes.

Removing an extended administration server

Complete the following instructions to remove an extended administration server (these are simply the reverse actions):

From the Domino Administrator, click Files and then open the Domino Directory (NAMES.NSF).

1. Choose Files -> Database -> Access Control.

2. Click Extended Access.
3. In the Names list, select the namespace (an organization, or one or more organizational units) from which you are removing an administration server.
4. Select the server that will no longer be an administration server for the selected namespace.
5. Click Remove.
6. Click OK -> Yes.

14.4 Considerations for xACL implementation

This section discusses some of the dos and don'ts (caveats) that you should keep in mind when implementing the extended ACL.

xACL control

- ▶ Plan the extended ACL carefully, maybe even on paper, before you implement it and do not start implementing before it is absolutely clear what will happen.
- ▶ Create a test environment where you can create an xACL model.
- ▶ When planning an extended ACL, use a sparse access control model that minimizes the number of extended ACL subjects you specify:
 - Use categories as targets /(root) or subcategories below /(root) rather than individual documents. To subcategorize documents below /(root), you may have to give some documents, for example Group documents, hierarchical names manually.
 - As a general rule, use “This container and all descendants” as the target scope to extend subjects' access to target subcategories.
 - Use names that represent groups of users (Self, groups, wildcard subjects, -Default-) as subjects rather than the names of individuals.
- ▶ Always use the “Check effective access” dialog to review the settings.

xACL precedence rules

The following precedence rules are applied to determine the access a user has to a target when there are multiple subjects that apply to the user at the target.

1. Access for a subject with the scope “This container only” takes precedence over access for a subject with the scope “This container and all descendants”, regardless of subject type.
2. Among subjects with the same scope, access for a more-specific type of subject takes precedence over access for a less-specific type of subject. The order of subject specificity, from most specific to least specific, is:

- Individual user or server
 - Self
 - Group
 - A wildcard
 - -Default-
3. When evaluating more than one group subject or more than one wildcard subject, the access settings of the subjects are combined, with Deny access taking precedence over Allow access.



Policy-based administration

A new technology, introduced in Domino 6, helps you to apply and manage standard corporate client and desktop-based policies. The technology is called *policy-based administration*.

With the new policy-based administration model you can control your users' desktops, security settings, archiving, client setup, and user registration in a structured way. This will put you, as an administrator, more firmly in control of your environment and also gives you a flexible way to manage and assist users, down to the client and even the document or field level, without running to each user's computer frequently.

Moving to Notes and Domino 6 will help you gain more control of your Notes client environment. Policy-based administration will even help you during the upgrade process to Notes and Domino 6, with features like seamless mail upgrade and desktop policy management.

This chapter describes what policies and the policy model are, how to perform policy-based administration tasks, and how you can implement this in your organization.

For additional information, see "Policy-based system administration with Domino 6" by Bob Balfe; this article is available on the Lotus Developer Domain.

15.1 Policies

This section describes the Policy model document structure and the execution triggers of Domino Policies.

15.1.1 Policies in Domino

A “policy” is a document that identifies a collection of individual policy settings documents. Each of these policy settings documents defines a set of default properties that apply to the users and groups to which the policy is assigned. Once a policy is in place, you can easily change a setting, and it will automatically apply to those users to whom the policy is assigned.

Policy documents are defined in your organization’s primary Domino directory, where the policy document structure is defined as shown in Figure 15-1.

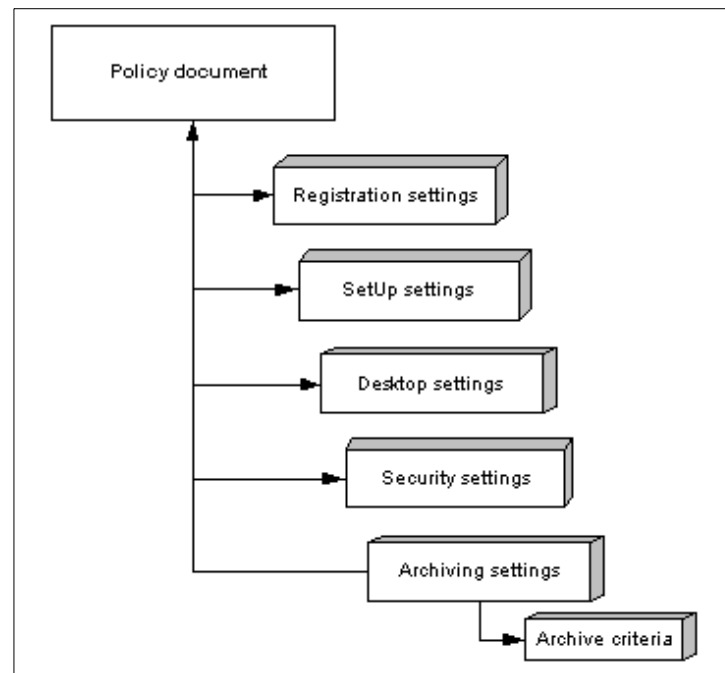


Figure 15-1 Policy-based administration: Document structure

15.1.2 Administrative areas

Policy-based administration gives you more control over the user's Notes client and desktop. From this perspective we can define five administrative areas which policy-based administration controls. They are identified in Table 15-1.

Table 15-1 Policy-based system administration: Policy areas

Policy area	Major features	Description
Archiving	Server-to-server archiving Server-to-local archiving Folder-based archiving	These settings determine whether or not to allow archiving of e-mail.
Desktop	Client upgrades Welcome page deployment Bookmarks management Seamless mail upgrade	These settings control the user's desktop environment. They are applied during the user authentication process and pushed to the user's desktop.
Setup	Client preferences like - Browser and proxy settings - Applet security	Setup settings are used only once, during the initial Notes client setup, to populate the user's location documents and bookmarks. You can change or reapply them later using Desktop policies.
Registration	Mail template setting Password length \ quality Internet address format Certificate expiration	Registration settings predefine the user registration options when applied before registering new users.
Security	Password expiration ECL management Password Length control	Security settings establish the control of user security settings defined in the client.

The Domino 6 Administration help document "Creating Policies" gives you more detailed information about each settings document's options and possibilities. At the end of this chapter we have added some examples and references to setup procedures for several policies based on the information in Table 15-1.

Execution of policies

The execution process of policies varies for each administrative area. The policy areas and corresponding execution triggers and details are summarized as follows:

- Archiving - triggered at scheduled times

Server-based archiving: Scheduled using the compact server task (you must create a program document that schedules the compact task).

Client-based archiving: The individual workstation processes mail file archiving on a scheduled basis (as defined in the policy document). If you choose not to include archiving policy settings in your policies, Notes users can still archive mail files using database archive settings in the Notes client.

- ▶ Desktop - triggered at policy change

Desktop policies are applied to a user's Client configuration whenever a change to the policy occurs. Administrators should include settings which must be kept up-to-date in desktop policies.

- ▶ Setup - triggered during client setup

Setup policies are executed once, as part of the initial Client configuration. Changes made to a setup policy will not affect existing clients to which this policy applies.

Setup policies are applied in the same manner that setup profiles were applied via dynamic Client configuration in R5.

- ▶ Registration - triggered at new user creation

Registration policies only apply when you create a new user using the Administrator client.

- ▶ Security - triggered at policy change

Security policies are applied to a user's Client configuration whenever a change to the policy occurs. Administrators should include settings which must be kept up-to-date in client Security policies.

15.1.3 Available policy types

When deciding which type of policies to use, consider the following suggestions:

- ▶ Use organizational policies to apply settings to groups in accordance with your existing naming hierarchy.
- ▶ Use explicit policies when groups or individuals to whom you want to apply settings are registered across your organizational structure or do not match your organization.

Note: You can use both types of policies within your company, though it is recommended that you plan the policy and rules architecture carefully. This is discussed in more detail in 15.3, "Planning your policy model" on page 462.

Both explicit and organizational policies can be configured as exception policies. Using an exception policy, you can explicitly exempt a specific individual or group from one or more of your standard policy settings.

Exception policies are powerful because they override all other settings, including enforced settings (specified for specific users), that apply to the exempted persons.

15.1.4 Policies versus setup profiles

If your organization uses setup profiles, which were used with Domino R5 to define common sets of desktop settings for users, you should consider migrating to the new policies-based administration model. Although setup profiles are supported in Domino 6, no new features will be incorporated in the future. Policies reach much beyond the scope of setup profiles, in terms of both where they are applied and when they are applied.

Important: If a setup profile is specified in a person record, it has precedence over any setup or desktop policy which would apply to this user.

15.2 Administering policies

This section shows you how to create and manage Domino policy and settings documents in a structured manner.

15.2.1 Parent and child

Domino allows you to construct a policy hierarchy by establishing parent-child relationships between policies. When you create a Policy document, you can also create one or more child documents for it. The original policy is then considered the child policy's parent.

Through the parent-child relationship, you create a hierarchy of policies to apply across your entire corporation. Policy inheritance, which uses the hierarchical relationship between policies, simplifies your policy-based administration model.

15.2.2 Inheritance

Inheritance plays an important role in determining a user's policy settings for both organizational and explicit policies. Because organizational and explicit policies are hierarchical, inheritance and enforcement automatically fit into a parent-child relationship. This model gives you the ability to define corporate-wide standards inherited by organizational units while allowing for the occasional exception.

Through the parent-child relationship, you create a hierarchy of policies to set your administrative practices across the enterprise. In a policy hierarchy, policy documents build the relationship, and policy settings documents determine the

value of the fields based on their position in the hierarchy. This means that when using field inheritance (inherit settings from parent document) and enforcement (enforce settings into child documents), you control the document settings of the related policies. Therefore, field values in a policy document may originate from many different policy settings documents, where each hierarchical level can have an associated policy.

► Example 1

If you want to set all the users to use the same ECL settings document, set the value in the Security policy settings document for the top-level policy. Once you have set this value, you do not have to change it or re-enter it in subsequent child policies. You simply force child policies to “inherit” this value from the parent by selecting the Inherit option in the document stated next to the configuration option.

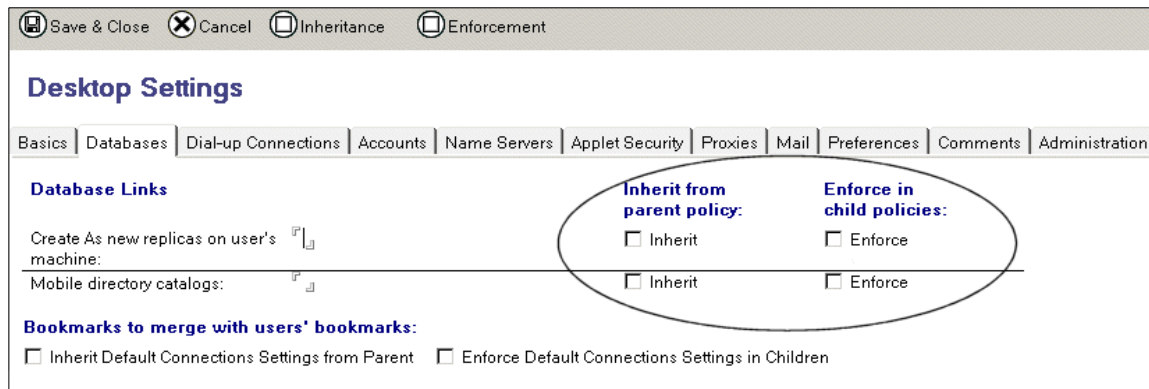


Figure 15-2 Inherit and enforce settings

► Example 2

You can have full control over some actions, for example archiving. You can have an archiving policy in which your end users have no control, some control, or complete control of where and how their mail files are archived.

Note: When creating an effective policies model, remember that “effective” policies are derived policy settings that are dynamically calculated at the time of execution.

15.2.3 Policies in the Administration client

The central place for policy administration is the Domino 6 Administrator Client; the Configuration tab and the People & Groups tab here show the policy documents that reside in your Domino directory.

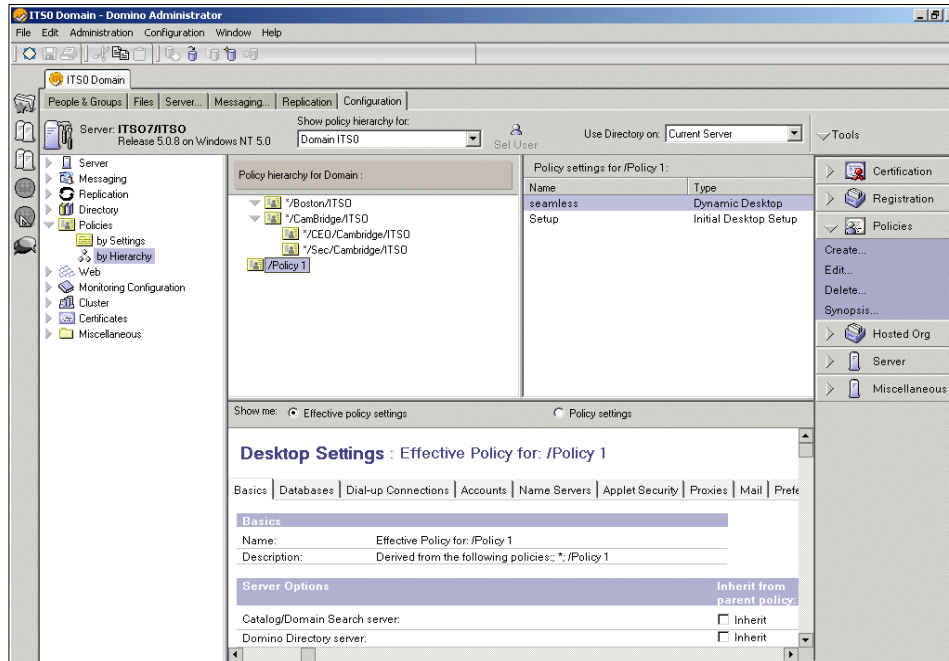


Figure 15-3 Policy management in Domino Administrator

The Administrator Client not only allows you to properly create and delete policy documents, but it also gives you a good overview of the policy structure.

Figure 15-3 and Figure show some of the Policy hierarchy panes in the Administrator client Policies section that allow you to get a detailed look at the policies created and the corresponding policy setting documents.

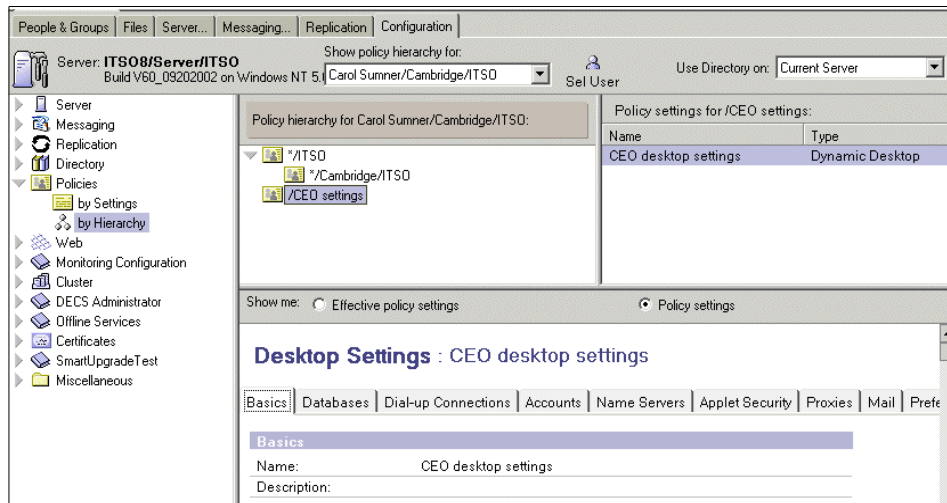


Figure 15-4 Policy overview in the Administrator client

15.2.4 Creating and explaining policy and settings documents

The policy document structure as defined in your Primary Domino directory can be divided into two main types of policy documents:

- ▶ Policy document
- ▶ Policy settings document
 - Archive criteria documents (specific archiving settings)

This section describes the purpose of the two main types of documents and how to use them functionally.

Policy documents

The policy document identifies a collection of individual policy settings documents and a high-level policy definition. When you create a policy, you use a policy document to specify which policy settings documents to include.

You can create policy settings documents before you create the policy document, or you can create them while you create the policy document.

Policy : */CamBridge/ITSO

Basics

Comments

Administration

Basics

Policy type help

Parent policy: */ITSO
Policy name: */CamBridge/ITSO
Policy type: Organizational
Description: Desktop policy for Cambridge users

Create Child

Organizational policies are implicitly applied to all users matching this policy and all of its parent policies. They cannot be explicitly assigned.

Setting Type	Setting Name
Registration:	New...
Setup:	New...
Archiving:	New...
Desktop:	New...
Security:	New...

Figure 15-5 Policy document

Once a policy is in place, you can easily change a setting in the document, and it will automatically apply to those users to whom the policy is assigned.

Creating a policy document

- Make sure that you have Editor access to the Domino Directory and one of these roles:
 - PolicyCreator role to create a policy document
 - PolicyModifier role to modify a policy document
- From the Domino Administrator, click the People & Groups tab, and then open the Policies view. Click Add Policy.
- Under Basics, complete these fields:
 - Policy name (enter one):
 - A unique Name, for an explicit policy.
 - The name of the organization or organizational unit, such as ITSO or Editors/ITSO.
 - The name of the hosted organization.
 - Policy type (choose one):
 - Explicit: to create a policy to assign to specific users and groups.
 - Organizational: to create a policy that is automatically assigned to all users in the part of the organization specified in the Policy name field.
 - Description: Enter a description of the policy.

Note: Make sure that you use a hierarchical name for the Policy name field when you create an organizational policy, for example:

*/Boston/ITS0
*/ITS0

4. (Optional) Click Create Child to create a child policy document that includes the name of the parent policy. You can save the child policy document and return to it at a later time. When you close this document you return to the parent policy document.
5. To specify the policy settings documents to include in this policy, for each type of settings do one:
 - a. Select a policy settings document from the list.
 - b. Click New to create a new policy settings document. Then, after you create the policy settings document, select it from the list.
6. (Optional) To create an exception policy, click the Administration tab and enable "Exception Policy."
7. Save the document.

Attention: Be cautious when creating an exception policy. An exception policy allows a user to override enforced policy settings.

Policy settings documents

Each policy settings document defines settings that apply to the users and groups to which the policy is assigned. The Policy settings documents cover the areas listed in Table 15-1 on page 451 and contain all the available settings.

The Notes and Domino 6 Administrator Help covers the Policy setting documents into detail in the User and Server Administration section.

Applying a Policy

When you create a Policy document or a Policy settings document, during the preparation phase for example, you do not have to worry about direct execution of the Policy as long as you do not apply and save the settings document in the Policy document. This allows you to properly create a settings document before applying it to your organization.

Attention: Before applying a Policy, make sure you have removed the setup profiles from your Domino Directory. Setup profiles have precedence over your policy documents.

Assigning Explicit Policies to users

You can create a new explicit policy and make it an exception policy. The Assign Policy tool is then used to assign the policy to individual users or groups by following this procedure:

1. From the Domino Administrator, click the People & Groups tab.
2. Open the People view and select the users to whom you want to assign policies, or open the Groups view and select the groups to which you want to assign policies.
3. From the Tools pane, click People or Groups (depending on your selection in the previous step), and then select Assign Policy.
4. Complete the Assign Policy Options dialog box appropriately. Select the Policy you want to apply from the list of Policies.

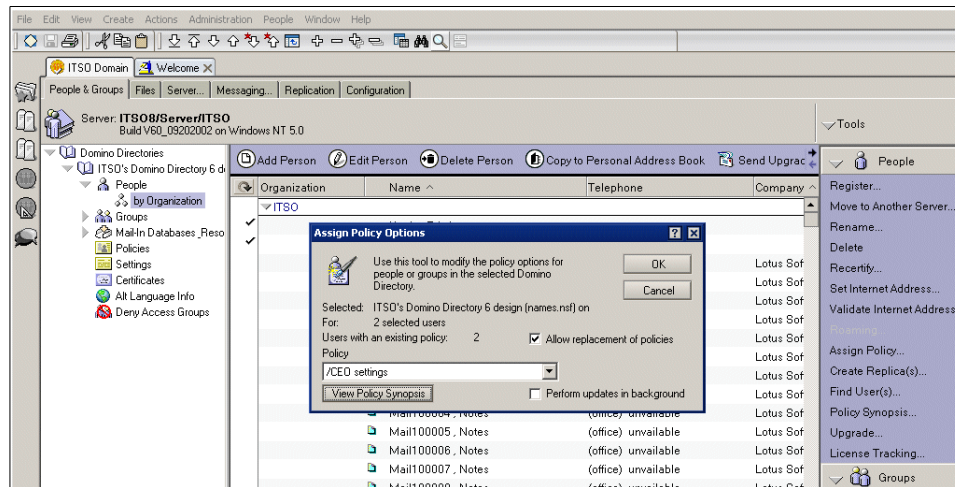


Figure 15-6 Assigning explicit policies to users

5. Optionally, click the View Policy Synopsis button to see the new effective policy for the group or users to which you are assigning this policy.
6. In the Policy dialog box, select the explicit policy you want to combine with the organizational policy to create the new effective policy.
7. Click OK and the Assign Policy tool populates the explicit policy field in each Person document in the Domino Directory.

Deleting policies

The policy model works in conjunction with the Administration process. You can use this procedure to delete policy and policy settings documents properly.

To delete a policy:

1. From the Domino Administrator, click the Configuration tab, then open the Policies - Hierarchy view.
2. Select the policy or settings document you want to delete.
3. Click Tools -> Policies -> Delete.

Table 15-2 describes the results of each type of deletion after deleting the policy document from with the Administrator client.

Table 15-2 Policy deletions

Deletion	Result
Explicit policy	An Administration Process request searches the Person documents of all users in the domain and deletes all references to the deleted policy.
Organizational policy	Deletes the policy document from the Domino Directory. All settings documents named in the deleted policy remain intact.
Settings document	Deletes the settings document from the Domino Directory. Deletes references to the policy settings document from all policy documents.

When you delete a policy settings document, you will see that this directly affects the Policy document and that the corresponding field is cleared.

15.2.5 Policy synopsis

Determining what policies and rules are in effect for specific users, groups, or organizations manually could be complicated. The Policy Synopsis tool helps you to determine the effective policies for a selected user. The output of the report will be placed, by default, as a document in the Policy Synopsis Results database (POLCYSYN.NSF). You can also customize where you want the report to be created.

You can use the Policy Synopsis tool from within the Notes 6 Administrator client, from the Configuration tab, and create a report according to the following steps:

1. Select the People view, and then select one or more users.
2. From the Tools pane on the right-hand side of the window, open Policies and select Synopsis.

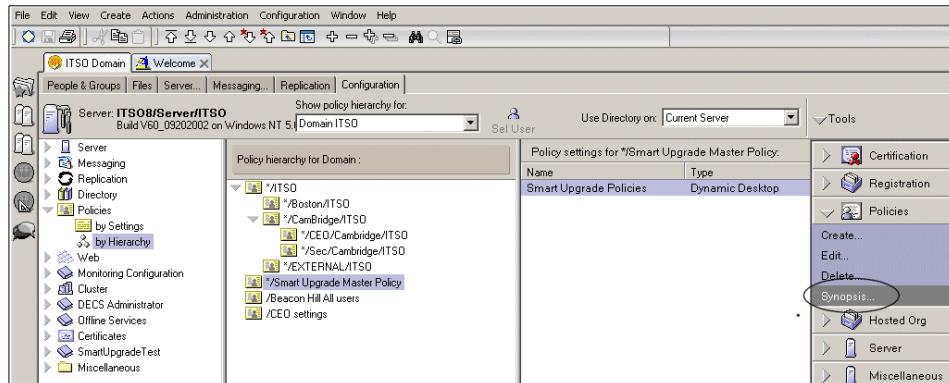


Figure 15-7 Policy synopsis in Domino Administrator client

3. Under “Select Report Type” choose one:
 - Summary Only (default) to produce a report that lists the hierarchy of policy documents used to derive the effective policy for the specified user.
 - Detailed to produce a report that lists the hierarchy of policy documents of the effective policy for the specified user, and includes the actual values, and the policy and policy settings documents from which the value was derived. Select the policy settings documents for which you want details.

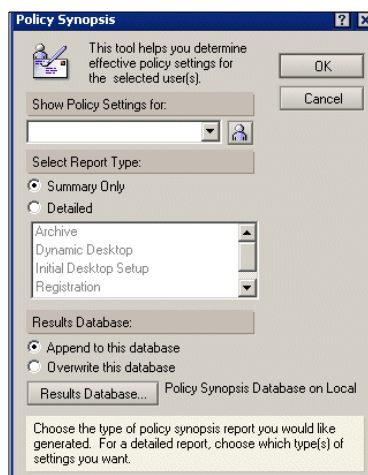


Figure 15-8 Policy synopsis dialog box

4. Under “Results Database” choose one:
 - Append to this database (default) to add to the list of previous reports.

- Overwrite this database to remove reports in the database and write the new reports.
5. (Optional) Click Results Database to change the name or location of the results database. The default is Policy Synopsis Database on local.
 6. Click OK. When the Policy Synopsis Results database (POLCYSYN.NSF) opens, double-click the report to open it.

Figure 15-9 shows the result of a Policy report request with the Summary only option set.

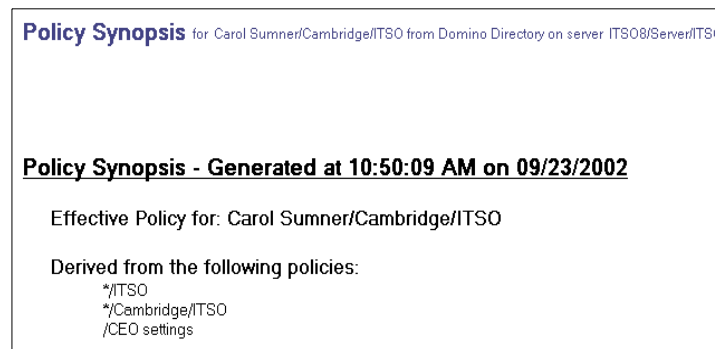


Figure 15-9 Policy synopsis summary only report

15.3 Planning your policy model

This section discusses how to plan and implement policy-based administration within your organization.

Planning the implementation of policies

Consider the following issues when planning your policies structure:

1. Determine which registration settings to assign to new users:
 - Organizational policy - When you register users with the corresponding certifier ID, that policy is automatically applied.
 - Explicit policy - You select the policy during registration and add this to the person document of users.
 - Exception policies - Can overrule all or any of the previous settings and give exception to certain organizations or users.
2. Determine which settings to assign for already registered users.
3. Determine if you use Setup profiles. Plan to migrate to Policy documents as soon as possible.

4. Determine the inheritance model you can use for the specific policy settings.

Assigning policies for your organization

A high-level view of the recommended steps for applying policies in your organization is as follows:

1. Create Policy documents that reflect your organization.
2. Create the policy setting document you need and assign the appropriate inheritance and enforcement settings.
3. Optional, but recommended: convert your setup profiles into policy documents and remove any existing setup profiles from the Domino directory.
4. Assign policy settings documents to Organization policy documents.
5. Assign policy settings documents to Explicit policy documents.
6. Assign explicit policies to users using the Assign Policy tool.

Assigning policies for a hosted organization

When you use policies for hosted organizations, your policy must include registration policy settings since the users are commonly Web users instead of Notes client users. The only way to execute policies is during the user registration process.

You can use either an organizational or an explicit policy. Depending on the type of policy you use, you create the policy either before you register the hosted organization or during registration.

Implement one of the following when you're planning to implement policies in a hosted organization:

- Create an Explicit policy.
- Create an Organization policy.

When you are registering a hosted organization, create an organizational policy and a registration settings document when you are prompted to do so and create an explicit policy that includes a registration settings document before you register the hosted organization.

If you want to create a policy for all hosted organizations in the Domino Directory, do not enter a policy name. By default Domino will enter the asterisk for you and the policy will apply to all organizations.

Example:

For hosted organizations use:

`*/<hosted organization>`

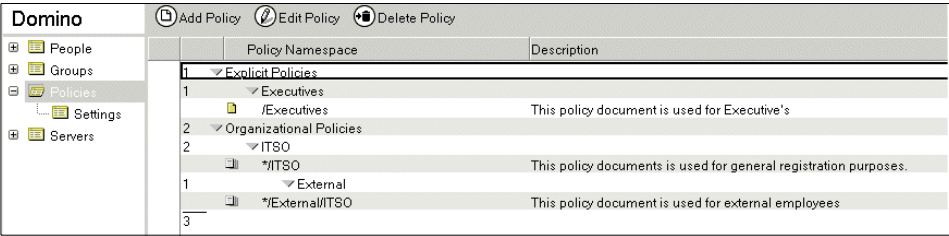
For hosted organizations, to indicate all hosted organizations in the Domino Directory, use:

`*`

15.3.1 Example of using policies

This section provides some examples of using policies in an organization (ITSO) assuming the organization wants to apply the following criteria:

1. Set the same Internet address format for all users.
2. Set a custom mail template for all CEOs.
3. Set the Creation of a local mailfile replica for all CEOs.
4. Set a 24-month certification expiration for permanent employees.
5. Set a 6-month certification expiration for temporary employees.



The screenshot shows the Domino interface with a left sidebar containing 'People', 'Groups', 'Policies', 'Settings', and 'Servers'. The 'Policies' section is selected. The main area displays a table with columns 'Policy Namespace' and 'Description'. The table content is as follows:

	Policy Namespace	Description
1	Explicit Policies	
1	Executives	
1	/Executives	This policy document is used for Executive's
2	Organizational Policies	
2	ITSO	
1	*/ITSO	This policy documents is used for general registration purposes.
1	External	
3	*/External/ITSO	This policy document is used for external employees

Figure 15-10 Policies view

To accomplish these goals, the administrator creates these policies:

- An organizational policy for all employees, `*/ITSO` in our example, that includes a Registration settings document (Figure 15-11 on page 465), that specifies the Internet mail format. These default policy settings include a 24-month certification expiration period (applies to criteria 1 and 3).

Save & Close Cancel Inheritance Enforcement

Registration Settings : Internet Mail format

Basics Mail ID/Certifier Miscellaneous Comments Administration

Mail User Registration Options

Choose the mail system:

Lotus Notes
POP
IMAP

Choose the mail server:

Server01/ITSO

Mail Template: mail6.ntf

☐ Create mail file now

☒ Create mail file in background

Internet Address Options

Internet Domain:

Choose an internet address format:

FirstName LastName
FirstName MI LastName
FI LastName
FIMI LastName

Choose an internet address separator:

None
Underscore
Dot
Equal

Advanced Mail Options

Inherit from parent policy:

☐ Inherit

Enforce in child policies:

☐ Enforce

☐ Inherit

☐ Enforce

☐ Inherit

☐ Enforce

☐ Inherit

☐ Enforce

☐ Inherit

☒ Enforce

☐ Inherit

☒ Enforce

Figure 15-11 Setting internet mail address format

- An Explicit policy, */Executives in our example (see Figure 15-10 on page 464), that includes a Desktop settings document (Figure 15-13) containing the custom mail template information and the creation of a local replica and sets these in the CEO's Person document on the Administration tab (applies to criteria 2 and 3).

Type	Setting Name	Description
Desktop Settings	Executive Mailfiles	This policy makes sure that executives use the right mailtemplate and have a local replica on their mach
Registration Settings	Expiration date for external employees	This policy sets the ID expiration date of temporary employees on 24 months
	General registration document	This policy document enforces internet mail format and certificate expiration dat for internal employees

Figure 15-12 Settings documents view

All the settings documents on our examples are listed in the Figure 15-12. Figure 15-13 on page 466 shows an example of how you can use the desktop setting to enforce a custom mail template to a set of users. In this

example, any user who is affected by the policy that contains desktop setting Executive Mailfiles is going to have a mail file based on a template StdExecutiveMail.

Desktop Settings : Executive Mailfiles

Basics | Databases | Dial-up Connections | Accounts | Name Servers | Applet Security | Proxies | Mail | Preferences | Comments | Administration

Basics

Name: Executive Mailfiles

Description: This policy makes sure that executives use the right mailtemplate and have a local replica on their machine's.

Server Options

	Inherit from parent policy:	Enforce in child policies:
Catalog/Domain Search server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Domino Directory server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Sametime server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Local mail file:	<input checked="" type="checkbox"/> Create local mail file replica	<input checked="" type="checkbox"/> Enforce
Deploy version:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Upgrade deadline:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Mail Template Information

	Inherit from parent policy:	Enforce in child policies:
Prompt user before upgrading mail file: (If user's have multiple machines or custom folders that they don't want the design replaced on) <input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes
Old design template name for your mail files: StdExecutiveMail	<input type="checkbox"/> Inherit	<input checked="" type="checkbox"/> Enforce
If Running This Version Of Notes: Use This Mail Template:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Figure 15-13 Using Desktop setting document to enforce a custom mail file

- An Organization policy for temporary employees (* /External /ITS0 in our example) that specifies a 6-month certification expiration, which you can set with a registration settings document (Figure 15-14 on page 467). When temporary employees are registered, this explicit policy is applied along with the organizational policy that correlates to the organizational unit in which the employees are registered. If you do not use a specific OU for temporary employees, you can create an explicit policy which you can assign to these users (applies to criteria 5.)

Registration Settings : Expiration date for external employees					
Basics	Mail	ID/Certifier	Miscellaneous	Comments	Administration
ID/Certifier User Registration Options <input checked="" type="checkbox"/> Create a Notes ID			Inherit from parent policy: <input type="checkbox"/> Inherit		Enforce in child policies: <input type="checkbox"/> Enforce
Certifier Information Security Type: <div> <input type="text" value="North American"/> <input checked="" type="text" value="International"/> </div>			<input type="checkbox"/> Inherit		<input type="checkbox"/> Enforce
Certificate Expiration Date: <input type="radio"/> Static Date <input checked="" type="radio"/> Months from user creation <div> <input type="text" value="6"/> </div>			<input type="checkbox"/> Inherit		<input type="checkbox"/> Enforce <input checked="" type="checkbox"/> Enforce
Location for Storing User ID <input type="checkbox"/> In Domino Directory			<input type="checkbox"/> Inherit		<input type="checkbox"/> Enforce
<input checked="" type="checkbox"/> In File			<input type="checkbox"/> Inherit		<input type="checkbox"/> Enforce
<div> <input type="button" value="Set ID File Directory..."/> <input type="text" value="\\DS\\People"/> </div>			<input type="checkbox"/> Inherit		<input type="checkbox"/> Enforce

Figure 15-14 Expiration date setting for external employees

Policies can also help you establish the upgrade process from Domino R4 or R5 to Domino 6. See “Using policies with smart upgrade” on page 489 for details about how the use of policies can help during the client upgrade process, and see 7.4.3, “Seamless mail upgrade” on page 141 detail about how to use Seamless Mail Upgrade to upgrade users’ mail files.



Administering the Notes 6 client

This chapter describes the new features available for administering the Notes 6 client environment. It includes client installations, managing the desktop, automatic upgrades, new user interfaces that the administrator should be aware of, and license tracking.

16.1 Client installations

This section describes the various ways of performing client installations for Lotus Notes. It includes shared network installations, multi-user workstations, using the InstallShield tuner to customize installations, silent installs, and smart upgrades.

16.1.1 Shared network installation

With a shared network installation the Lotus Notes executables are installed on a network application server and users access the Notes client from the network server. When they install the client on their workstations from the shared network installation only the data directory structure and files are put on the workstation. With this configuration the notes.ini file is installed in the default notes data directory (instead of the notes program directory).

During the installation of the network image, all program files for Lotus Notes, Domino Administrator, and Domino Designer are installed. In order to customize client installs, that is, to limit an installation to the Notes client only, you create a transform file for each type of installation (see 16.1.3, “Customizing client installations with transform files” on page 476).

There are limitations to this type of setup:

- ▶ Users must have access to the network in order to run the Notes client.
- ▶ Multi-user installations are not supported with a shared network installation.
- ▶ It is not available for the Macintosh client.

Shared network installation setup

1. Open a command prompt and navigate to the location of the installation files.
2. Enter the following command:

```
setup.exe /A
```
3. The Install Wizard window is displayed. Click Next to proceed to the Network Location screen.

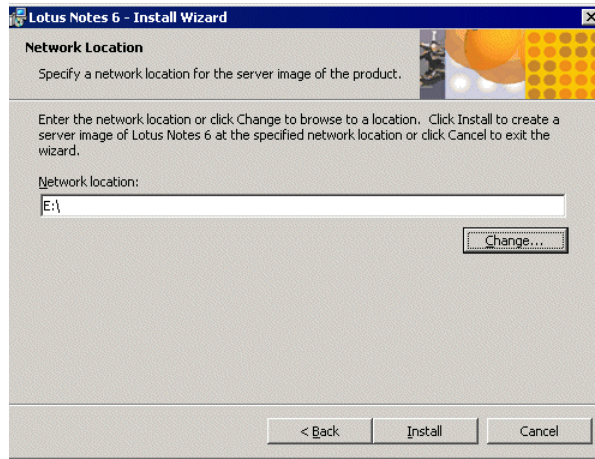


Figure 16-1 Network Location during Administration Install

4. Specify the appropriate location on your network for the shared network files. This is the location from which your users will install the client, so users must have Read access to this location. Click Install. All client types and options will be installed to the network location. Your users can install the clients and options which they need from this location by using the Lotus Notes 6.msi. You can create transform files to customize your users' installations.
5. When the Install Wizard Completed screen appears, click Finish.

The Lotus Notes installation files have now been installed onto the network drive and are ready for your users to install Notes to their workstations.

When your users install Notes from this directory everything will look the same as for a normal installation. They will see the welcome screen, the license agreement screen, and the customer information screen as they would for a full workstation installation.

The Installation Path Selection screen, shown in Figure 16-2 on page 472, will only have the option to change the location of the data files (because you configured the Notes client code to run from the network location).

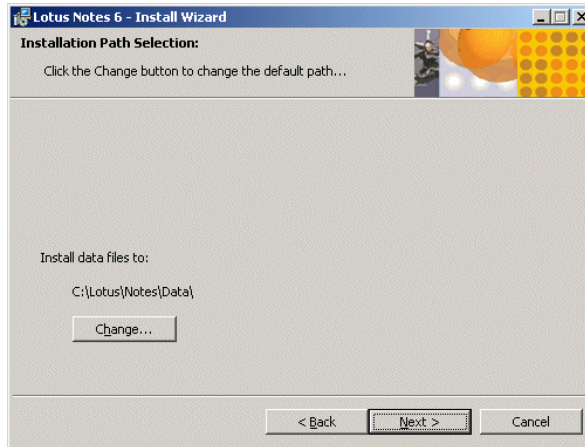


Figure 16-2 Installation Path Selection during shared network installation

Upgrading a shared network installation

To upgrade a Shared Network Installation, you should delete all the files from the previous installation and make a fresh installation with the new code. Upgrading in place is not recommended. If you have created transform files to customize installations you will need to recreate them for the new code.

16.1.2 Multi-user workstations

The multi-user install is for Win32 workstations that are shared by more than one user. It allows each user to store their own desktop, address books, local databases, preferences, and so forth. In essence, it creates a separate data directory for each user.

Note: This option is available for the Notes client only and not for the Administrator or Designer clients. It will not even be visible unless you are installing the client-only version of the software, from the x:\Notes directory on the CD.

The Notes program files are installed to a central directory, and each user's personal files, including the notes.ini file, are stored in the hidden Documents and Settings\User Name\Local Settings\Application Data\Lotus\Notes\Data folder.

Preparations

The user installing the base Notes code must have administrator access to the workstation's OS; however, those using the client need only enough to be able to access the directory in which the base executables are installed.

The workstation will need to have enough disk space for a separate notes data directory for each user. This will initially be about 12 MB, but could grow if the user were to create local replicas of databases on a server, or personal databases.

Note: The size of the data directory for each user is kept to a minimum because it is feasible to share some of the data directory's files, like Notes template files, modem files, and help files. These will be installed in c:\Documents and Settings\All Users\Application Data\Lotus\Notes\Data. A setup notes.ini file for future installations by users is also stored here.

Each person using Notes on this machine will need to have their own logon to the Windows system. This will create their own directory under the Documents and Settings directory into which Notes will install their personal data directory.

Installation of Notes 6 for a multi-user workstation

1. Start the client install normally, with **setup.exe**. On the second screen (Customer Information), select "Anyone who uses this computer (Multi-User Install)" under "Install this application for:"

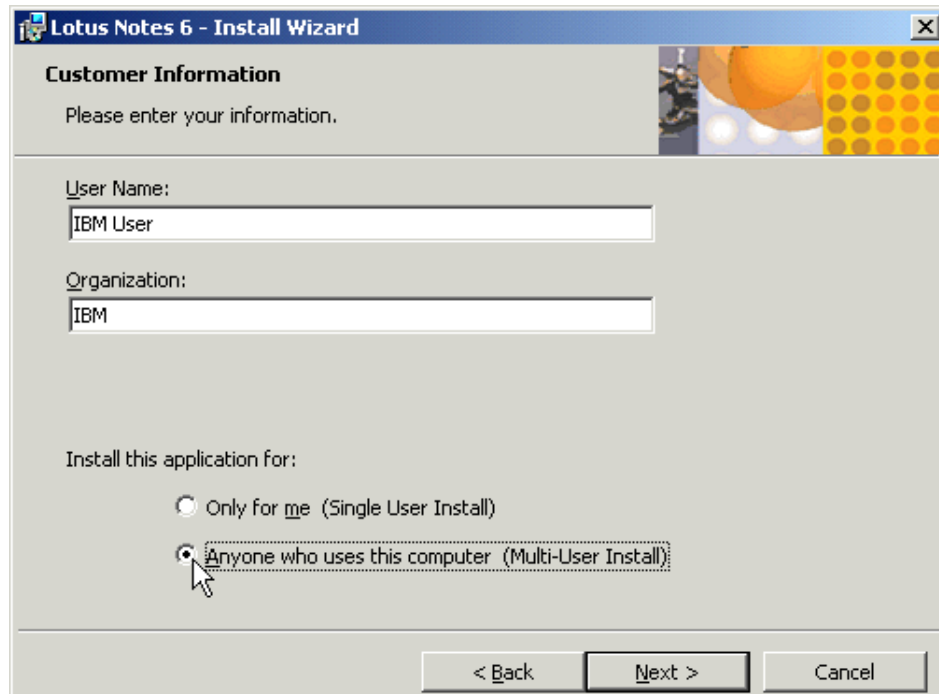


Figure 16-3 Multi-user installation: Customer Information screen

2. In the next screen, you are prompted for the installation path. This is the directory where the common, shared files will be installed (such as the .exe for starting Notes). Make sure you select a directory that all users of the machine will have sufficient access rights to.
3. On the Custom Setup screen, choose the options you would like installed, then click Install on the next screen and the installation will begin.

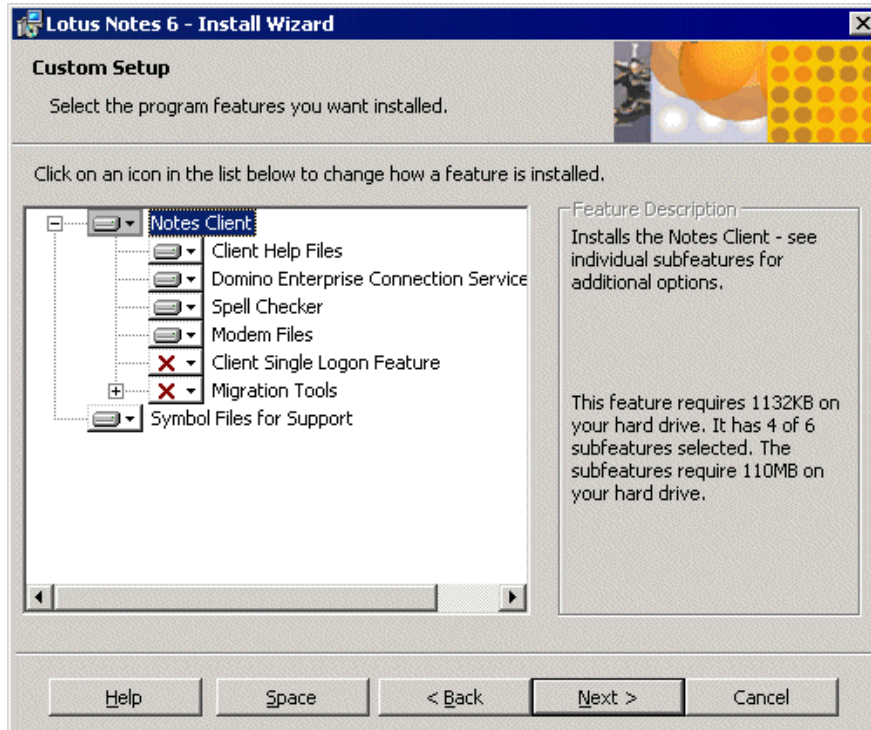


Figure 16-4 Custom setup for multi-user installation

4. When the install has finished, a user simply has to log on to the machine and start Notes. Each new user will be presented with the standard client setup options, and their choices will be saved to their respective user directories.

Upgrading a multi-user installation

To upgrade the Notes client version on a machine with a multi-user install, simply log on with the administrator account used to install the client initially, and run through the upgrade process as normal. Ensure that you are installing the client-only version, and that the option for a multi-user install is still selected on the Customer Information Screen.

The next time each user starts Notes, the Notes client will automatically upgrade their personal address book. The design of the mail file will not be upgraded automatically. The mail file on the server should be upgraded through the design task on the server (for minor upgrades), or you can set up seamless mail upgrade (see 7.4.3, “Seamless mail upgrade” on page 141 for details about this).

Uninstalling a multi-user installation

1. Log in as an administrator of the workstation.
2. Use the control panel utility “Add/Remove Programs” to uninstall Notes.
3. Delete the Lotus directory for each user. Be sure to save the names.nsf, ID file, desktop.ndk, bookmark.nsf, and any personal databases (*.nsf) for each user if you will be setting them up on Notes on a different machine. The notes.ini file may need to be different on a different machine, so it is best to not reuse it.
4. Delete the Lotus directory in c:\Documents and Settings\All Users\Application Data.

Removing one user from a multi-user installation

1. Log in as an administrator of the workstation.
2. Delete the Lotus directory for the user. Be sure to save the names.nsf, ID file, desktop.ndk, bookmark.nsf, and any personal databases (*.nsf) for the user if you will be setting them up on Notes on a different machine. The notes.ini file may need to be different on a different machine so it is best to not reuse it.

16.1.3 Customizing client installations with transform files

This section introduces you to Windows Installer technology and walks you through the process of customizing an installation of Lotus Notes using that technology.

Brief description of Windows Installer technology

Notes 6 takes advantage of the Windows Installer technology, which allows an administrator to standardize custom installations by distributing pre-configured installation packages. The administrator manipulates the configuration by means of a transform file that the Windows Installer service uses when it is installing an application.

The InstallShield Tuner for Lotus Notes provides administrators with a graphical and easy-to-use method of modifying the default install options of the new installer in Notes 6. This allows administrators much more flexibility in their options and enhances control over what an end user can and cannot do or see when installing the program.

Using the InstallShield Tuner

This section provides a brief introduction to using the InstallShield Tuner for Lotus Notes. For more information, along with training opportunities, visit the InstallShield website at:

<http://www.installshield.com>

Initial setup

1. Begin by installing the InstallShieldTuner for Lotus Notes from your Lotus Notes CD. After the install is complete, start the Tuner from your Lotus Applications program directory. You will immediately be prompted for a Tuner Configuration (.ITW) file. Select the lotusnotes.itw file from the x:\apps directory (where “x” is the location of your Notes install files) and click Open.
2. The first screen you are presented with is the InstallShield Today welcome screen. Select “Create a new transform file” in the second pane.
3. In the Base Windows Installer Package section of the third pane, click the Browse button and navigate to the x:\allclient directory on the Notes CD. Select the Lotus Notes 6.msi file, and click Open.
4. Create the transform file.

In the Windows Installer Transforms section, specify the location and name of the install modification (.MST) file. This is the file that stores all of the modifications, and must be included in the install package that will be distributed to the users when they run the install.

- a. Browse to the directory to which you wish to save the .MST file, type a name, and click Save.
- b. Click the Create Transform File button.

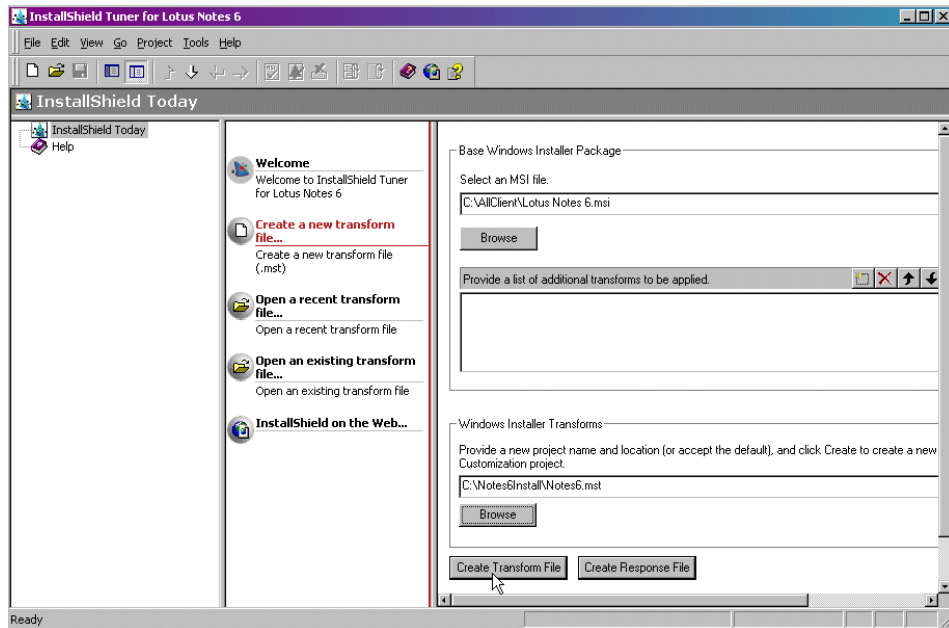


Figure 16-5 Create the Transform File

Modify the Transform File

1. MSI File Prevalidation

The next screen displayed is the MSI File Prevalidation screen. Since the Lotus Notes 6.msi file has already been verified, this step can be skipped. If you do perform the prevalidation check, you may receive many (up to 100) errors and warnings. These errors are harmless and should be ignored.

2. Setup organization

In this step you select the features to install, as follows:

- a. Using the navigator in the first pane, select step 2, Setup Organization -> Features. (You will be specifying the information under “Default Destination and Organization” later in the process). This is where you will choose the default features that will be installed on the user’s machine.
- b. Highlight each feature that you want installed by default in the second pane, and change the Initial State (in the third pane) to “The feature is installed on the local drive.”
- c. If this is going to be a User Interface install, and you do not want the users to have the option of turning a certain feature on or off (for example, you do not want to give them the ability to install the designer client), then

change the “Visible” field to either Not Visible or Visible, depending on your preference.

- d. Note that the default for the Notes Client and CoreProgramFiles is “The feature is run from source, CD, or network.” In most cases, you will want to change both to “The feature is installed on the local drive.”

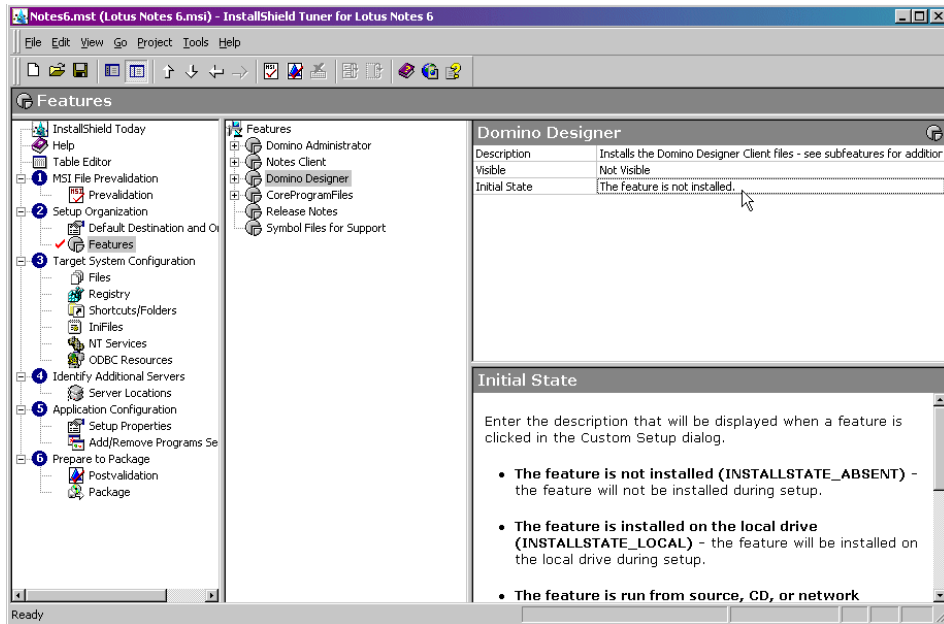


Figure 16-6 Modifying the Install Options for the users

3. Target system configuration

a. Files (optional)

- i. If there are any extra files you wish to have installed along with Notes (for example, a modified bookmark.nsf file with some bookmarks already selected), select “Files” under step 3, Target System Configuration.
- ii. In the “Source computer’s directory tree” box navigate to the location of the file you want to include.
- iii. In the “Destination computer’s folders” box, specify the destination directory path. To do this, highlight “Destination computer” and press Insert. This will create NewFolder1, which should be renamed at the top level directory (below the root) that you wish to use (that is, Notes). Highlighting that directory and pressing Insert will create NewFolder2 beneath NewFolder1. It should be renamed to the next level folder (that is, data).

- iv. Drag the selected file from “Source computer’s files” to the “Destination computer’s folders.” See Figure 16-7 for an example.

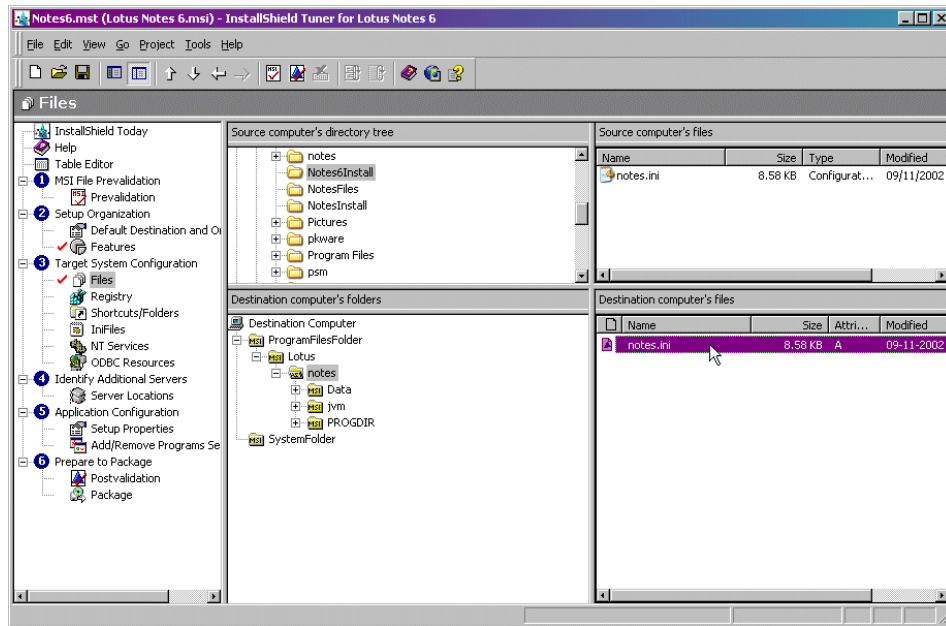


Figure 16-7 Adding files to the install package

b. Registry

Any registry changes you wish to make can be made in a similar way through the Registry tab in step 3. However, since Notes adds very little to the registry, this step can be skipped in most cases.

c. Shortcuts/Folders

The Shortcuts/Folders tab is used to control which shortcuts you wish to have installed on the user's OS desktop and Start menu. To remove a particular shortcut, highlight it and press Delete.

d. Notes.ini file changes

If there are any preferences stored in the notes.ini that you would like to specify for all users, do so by clicking the IniFiles tab.

e. The NT Services and ODBC Resources tabs should be skipped in most cases.

4. Identify Additional Servers

If you are going to put the Notes install files on a network drive, specify it here. Doing so will allow users to automatically repair Notes installations through

their add/remove programs option in the control panel if a file becomes corrupt.

5. Application Configuration

Select that Setup Properties view, and leave the defaults for most of the options. The ones worth noting are:

- DATADIR: This is the default location of the user’s data directory (usually a subdirectory called “data” under the PROGDIR).
- PROGDIR: The directory that the main Notes files will be installed to.
- AgreeToLicense: This must be set to “Yes” if you will be doing a silent install, and will require one less click from users in a User Interface install.

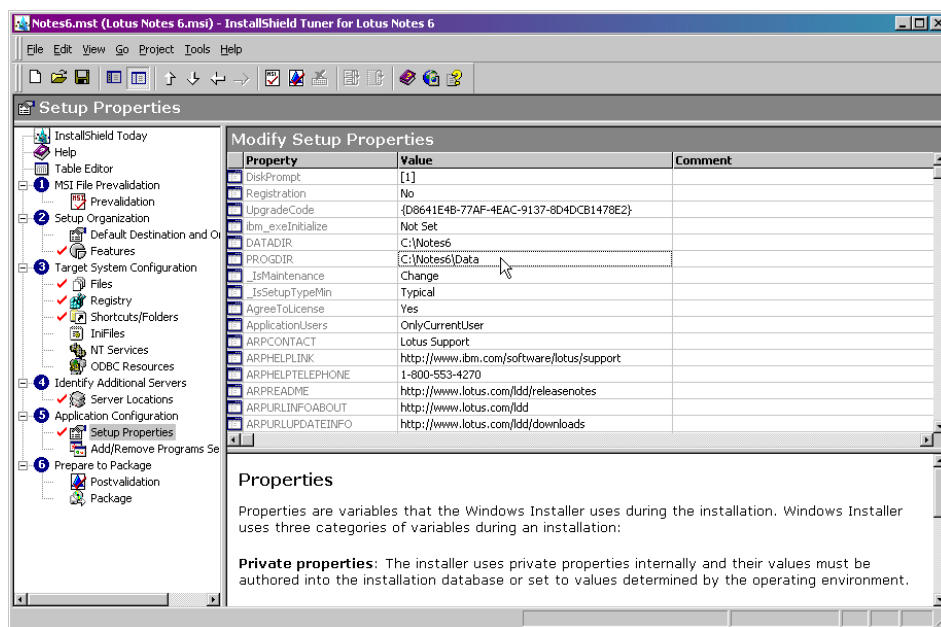


Figure 16-8 Modifying Setup properties

- Other options

If you would like to modify the options available to the users from the Add/Remove programs list in the Windows control panel, (such as disabling their ability to uninstall the software), select Add/Remove Programs Setting, and select Yes for Disable Modify Button, Disable Remove Button, and Disable Repair Button, depending on your preferences.

6. Prepare to Package

- a. Postvalidation step should be skipped since you will once again see many harmless errors and warnings if you run it.
- b. The final step is to package the installation.
 - i. Select the Package view from the first pane, and Location from the second pane. This is the location (your local drive, a network drive, or an FTP site) to which Tuner will copy all of the files required for the installation.
 - ii. Choose the Setup view. This option will create a customized setup.exe that includes the .MST file along with any other files needed for the install. This is much easier than running a command line with parameters for the transform file. If any of your users are running Windows 95, Windows 98, or Windows NT, then select the appropriate checkboxes.
 - iii. In the Windows Installer Command Line Arguments field you can specify any switches that should be incorporated into the setup. For example, you can specify that this package should always do a silent install by typing `/qn` in this field. For a list and description of the various command line options available look in the MSI help file.

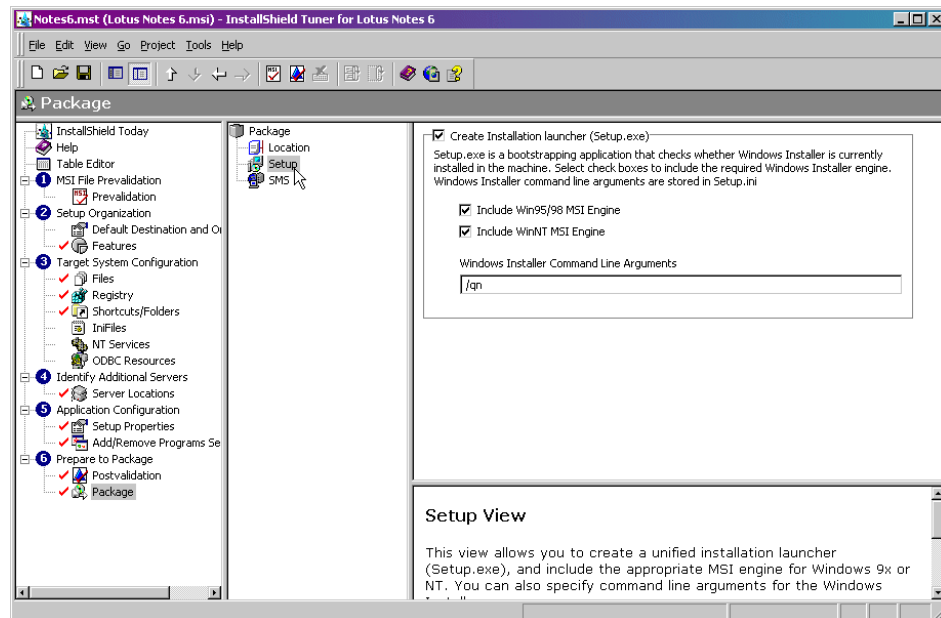


Figure 16-9 Creating the install package

- iv. The SMS tab is for companies that have deployed Microsoft Systems Management within their organization. To create the necessary files to

use SMS with Notes 6, select the appropriate options (depending on the version of SMS), and the necessary .pdf and .mif files will be created.

Save the transform file and the package

1. Click Save on the toolbar.
2. Select Package from the Project menu. Tuner will copy all of the required files to the location you selected on the Location tab. You will see a log of the files being copied in the lower pane.

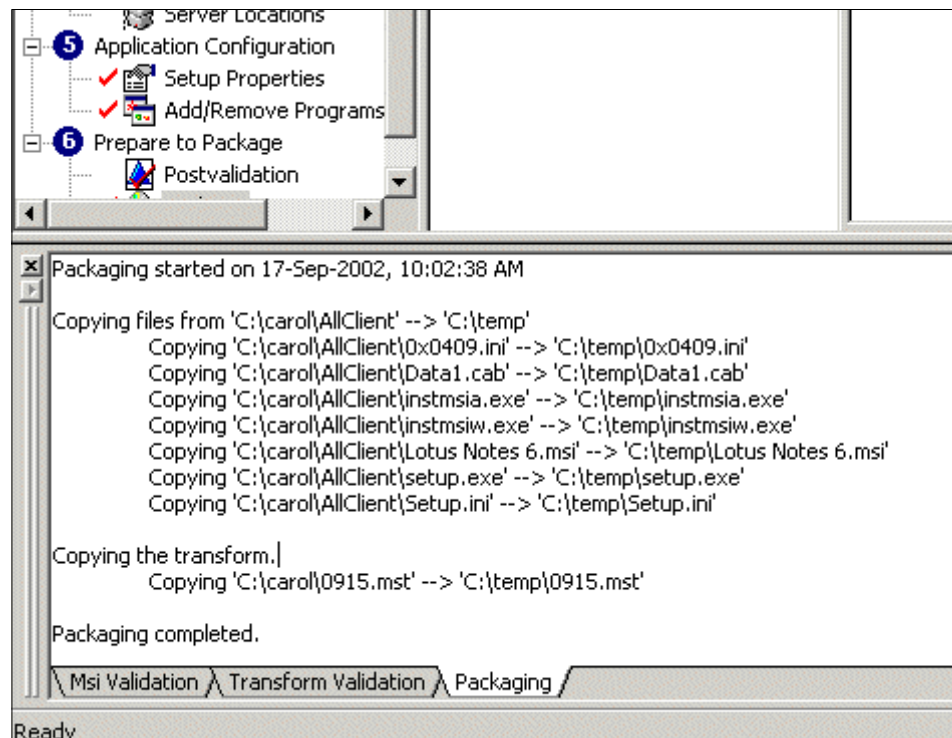


Figure 16-10 Packaging log

3. Click Save on the toolbar one more time and close Tuner.

The package is now ready to be distributed to your users. They will run the install with the setup.exe included with the package. If you ever need to make changes to the package, simply start Tuner and choose “Open an existing transform file” from the menu. Note: Once you have made changes to a transform file you must save the .mst and then re-package the install by selecting “Package” from the project menu.

16.1.4 Silent install

Automated client installation supports all three Domino clients and simplifies installation for end users because it presents very few or none of the installation windows; thus, it is called a silent installation.

Use this format to run the install in silent mode:

```
Setup.exe /s/v"/qn"
```

When the installation is complete, the shortcut icons appear on the desktop.

To display a prompt when the installation is complete or when it fails, use the + parameter as follows:

```
Setup.exe /s/v"/qn+"
```

Running a silent install provides users with the default installation options. To customize the type of installation or to specify options to install on the user's system, use a transform file with the silent install.

You can create a batch file in the installation directory with the command line for silent install in it. Even if you have network or desktop specialists helping with installations, this method of distributing the client will keep the installations consistent, which will make them easier to support in the future.

Note: Users must have similar drive mappings and directory structures in order for this to be the most successful installation strategy. In other words, the more standardized the workstations are, the easier it is to automate the distribution of any new software, including Lotus Notes.

16.1.5 Smart Upgrade

Smart Upgrade is a new feature in Notes/Domino 6.0 that allows administrators control over the client versions that their users are running. When a user hits a server that is configured for Smart Upgrade, they will receive a pop-up box informing them that an upgrade is available, along with a button that will automatically upgrade their client. The administrator has the flexibility to force upgrades on users, or restrict the upgrade to only certain users.

Upgrade kits will be posted on the Lotus Developer Domain website at:

<http://www.lotus.com/1dd/smartupgrade>

Note: Smart upgrade does not work for R5 and earlier clients.

Important: Users' location documents must specify the correct home server on the Servers tab of the document. If the wrong home server is specified (that is, the server specified is not the same one that the Domino Directory lists as the user's mail server) then Smart Upgrade will not begin the upgrade process.

Initial server configuration

1. Create a Smart Upgrade database on the server. Using the Notes client, create a new database with the smupgrade.ntf template (you must select "Show advanced templates" to see the Smart Upgrade Kits (6) template.)

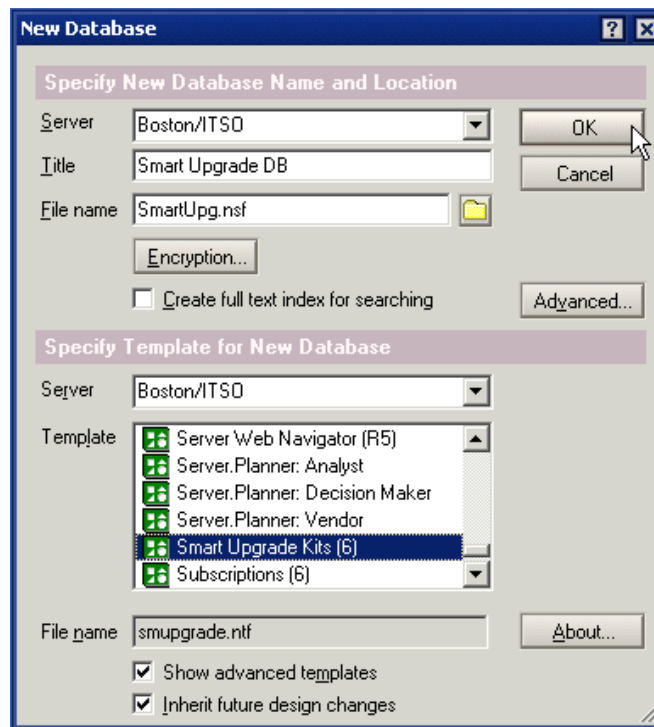


Figure 16-11 Smart Upgrade Kit template

2. Open the database. Close the About page if it appears.
3. Click the New Kit button. This will create a Smart Upgrade configuration document.

Save & Close Cancel

Smart Upgrade Kit

Basics | Data | Admin Notes | Administration

This Smart Upgrade kit can be used to upgrade this version of Lotus Notes:

Source version: Release 6.0

Operating system: Windows/32

Localization: English

After applying this kit, the client will be running this version of Lotus Notes:

Destination version: Release 6.01

☐ Restart Lotus Notes after upgrade completes

☒ Enabled

Figure 16-12 Basics tab of the Smart Upgrade Kit

4. In the Source version screen of the New Kit form, input the version of Notes which is eligible for this upgrade. You must input this *exactly* as it appears in the “About Notes” screen on the version of the client which is eligible for the upgrade. Open the splash screen by clicking Help -> About Notes from the menu.

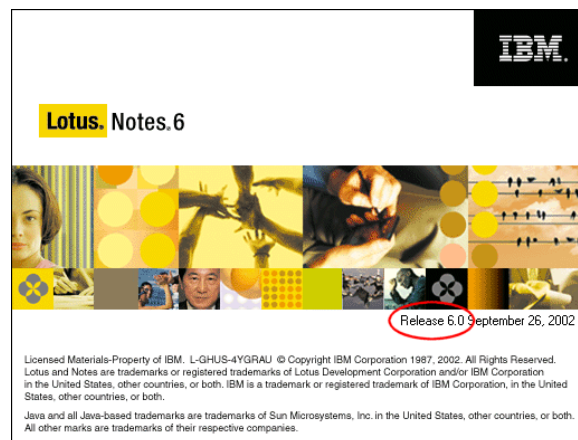
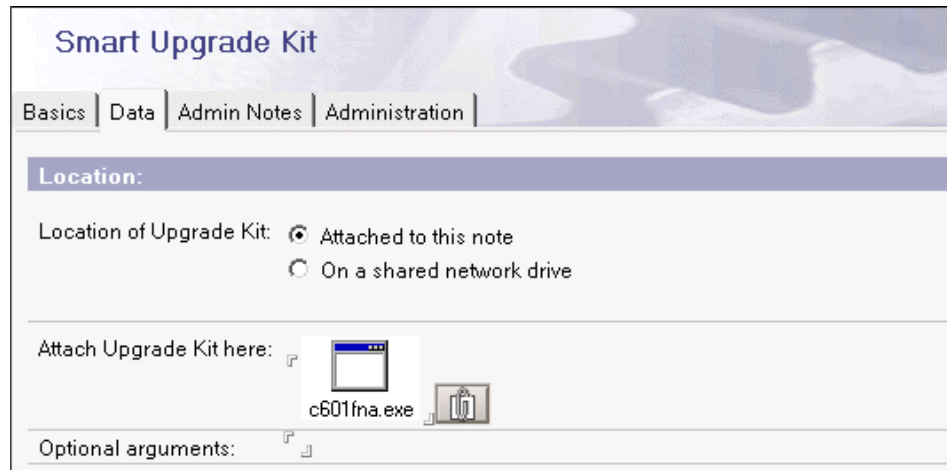


Figure 16-13 Release Version on the Splash Screen

Tip: This may or may not be the version which you are personally using. Be sure to enter the release of the Notes clients that you want to upgrade.

5. The Destination version is the version you are upgrading to, such as Release 6.01.
6. Select the “Enabled” checkbox.
7. Click the Data tab. The Data tab is used to specify the location of the upgrade files. There are two methods for distributing the upgrade software:
 - a. Attach the upgrade kit to the database by clicking the attachment icon and selecting the kit. Attach the EXE file that you downloaded from the Lotus Web site to the document without decompressing the file.

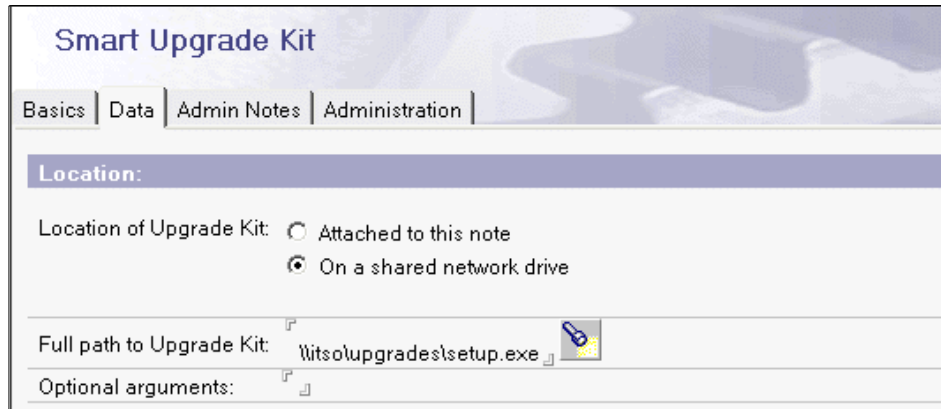


The screenshot shows the 'Smart Upgrade Kit' dialog box with the 'Data' tab selected. The 'Location:' section has two radio buttons: 'Attached to this note' (selected) and 'On a shared network drive'. Below this, the 'Attach Upgrade Kit here:' section shows a file named 'c601fna.exe' with a folder icon. The 'Optional arguments:' section is empty.

Figure 16-14 Attached location of upgrade kit

- b. Put the software on a shared network drive. Be sure that all your users have access to this location. When you use the shared network drive option, decompress the file, then copy all files in the installation kit to the network location specified. Use the universal naming convention to specify the location:

`\\networkfileservername\shareddirectoryname\setup.exe`



Smart Upgrade Kit

Basics | Data | Admin Notes | Administration

Location:

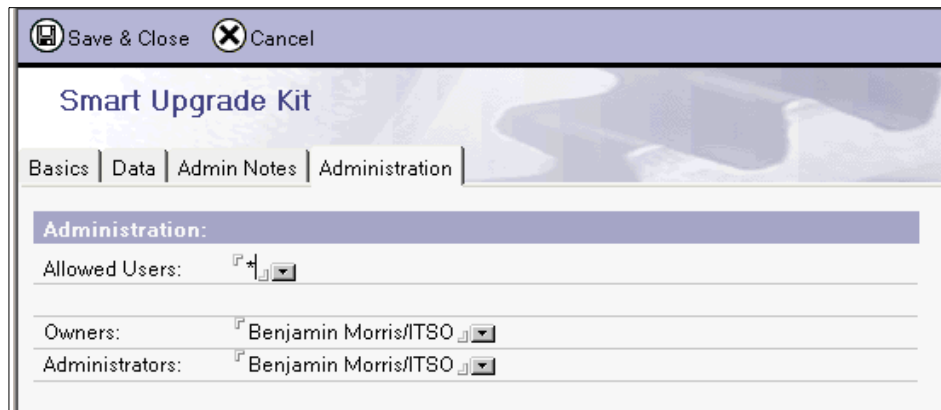
Location of Upgrade Kit: ☐ Attached to this note
☒ On a shared network drive

Full path to Upgrade Kit: Witsol\upgrades\setup.exe

Optional arguments:

Figure 16-15 Network location of upgrade kit

8. On the Admin Notes tab, you can insert a message that will be displayed to users if they click the Read Me First button on the screen that is presented to them.
9. The Administration tab is where you can restrict the upgrade to certain users. In this example, the update is going to be available to all users, so a * is used.



Save & Close Cancel

Smart Upgrade Kit

Basics | Data | Admin Notes | Administration

Administration:

Allowed Users: *

Owners: Benjamin Morris/ITSO

Administrators: Benjamin Morris/ITSO

Figure 16-16 Administration page of the smart upgrade kit

10. Save and close the kit.
11. Open the Domino Directory on the server. Open the Configuration document (under Servers -> Configurations) for All Servers or for a specific server and put it in edit mode.

Attention: Lotus Notes Smart Upgrade first checks for the Lotus Notes Smart Upgrade database link in the Configuration Settings document of the home server specified in the Notes client location document. If that Configuration Settings document does not contain a Lotus Notes Smart Upgrade database link, Lotus Notes Smart Upgrade next checks the * - [All Servers] Configuration Settings document for the database link. If you want Smart Upgrade to apply to your whole organization without exception, use the All Servers configuration settings document. If you need different upgrade paths for users on different servers use the configuration document for each server.

12. Paste in a link to the Smart Upgrade database that you just created in the Smart Upgrade Database Link field on the Basics tab.

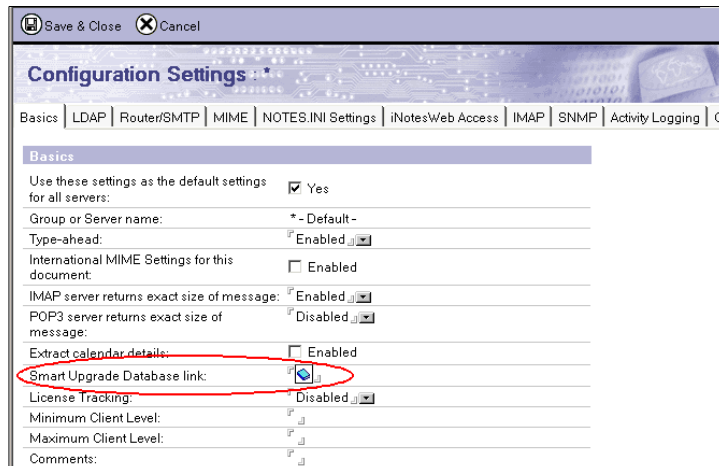


Figure 16-17 Smart Upgrade database link on basics tab

13. Save & Close the configuration settings document. Smart upgrade should now be working.

Using policies with smart upgrade

Desktop policies extend the options available to the administrator when using Smart Upgrade, by allowing him or her to set a “grace period” in which the user has the option of deferring the install. Once the grace period has run out, the user will be forced to install the client. If no policy is used, the upgrade will never be forced on the user.

Tip: If your organization has already implemented a policy that uses a desktop settings document, you can just add this information to that settings document.

1. To deploy smart upgrades through a policy, you must first create a desktop settings document. Select the People & Groups tab from the Domino Administrator, then the Settings view. Click the Add Settings button, then Desktop.
2. Fill in values for the “Name” and “Description” fields.
3. The “Deploy version” field should be populated with the exact name that you set in the “Destination version” field in the kit you created previously.
4. The “Upgrade deadline” field sets the grace period.

Desktop Settings: Smart Upgrade Settings - Domino Administrator

File Edit View Create Actions Text Help

ITSO Domain Desktop Settings: Smart Upgrad... X

Save & Close Cancel Inheritance Enforcement

Desktop Settings: Smart Upgrade Settings

Basics Databases Dial-up Connections Accounts Name Servers Applet Security Proxies Mail Preferences Comments Administration

Basics

Name: Smart Upgrade Settings

Description: SU Settings

Server Options	Inherit from parent policy:	Enforce in child policies:
Catalog/Domain Search server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Domino Directory server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Sametime server:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Local mail file:	<input type="checkbox"/> Create local mail file replica	<input type="checkbox"/> Enforce
Deploy version:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Upgrade deadline:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Mail Template Information	Inherit from parent policy:	Enforce in child policies:
Prompt user before upgrading mail file: (If user's have multiple machines or custom folders that they don't want the design replaced on)	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes
Old design template name for your mail files:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
If Running This Version Of Notes: Use This Mail Template:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Ignore 200 category limit:	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enforce
Mail file to be used by IMAP mail clients:	<input type="checkbox"/> Yes	<input type="checkbox"/> Enforce

Enforce this setting in child policies?

Office

Figure 16-18 Smart upgrade configuration in a desktop settings document

5. Click Save & Close.
6. Switch to the Policies view in the People & Groups tab.
7. Click Add Policy, and fill in values for the “Policy name” and “Description” fields.

8. Click the drop-down arrow next to Desktop, and choose the Smart Update document you just created.
9. The “Policy type” field can be set to either Explicit or Organizational.

Tip: Explicit policies must be assigned to each user (in their person document in the names.nsf), while organizational policies are applied to every user whose certificate matches the organization named in the Name field of the policy document. For example, if you name the policy document /Boston/ITSO all users who are a part of the organizational unit /Boston/ITSO will be subject to the policy.

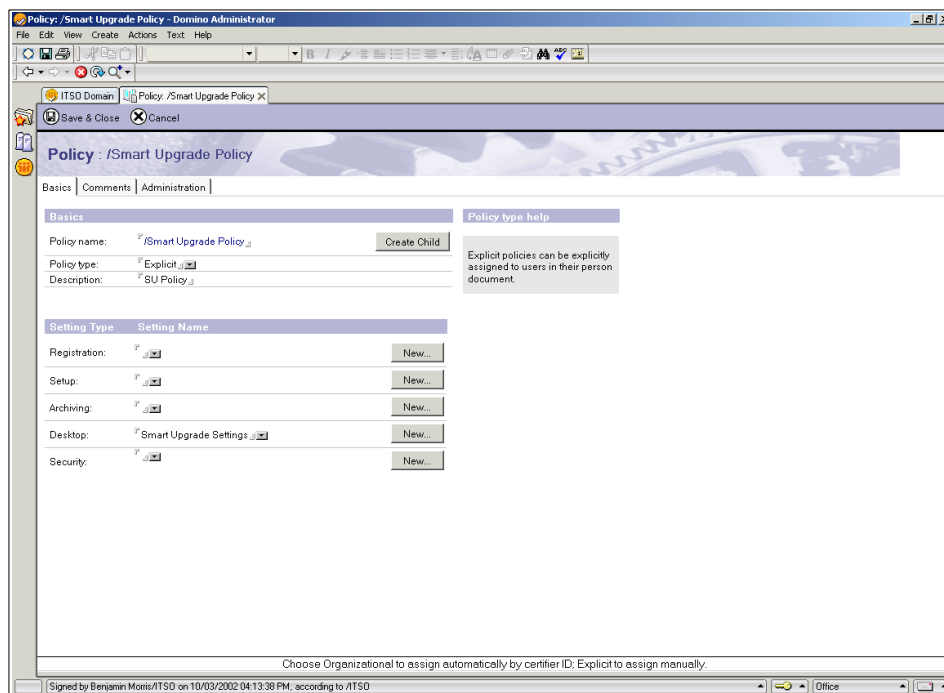


Figure 16-19 Policy document

10. Save and close this document. If you selected an Explicit policy, you must now apply the policy to the individuals or groups who should be subject to it (see Chapter 15, “Policy-based administration” on page 449 for details). The policy section of their person documents will be updated.

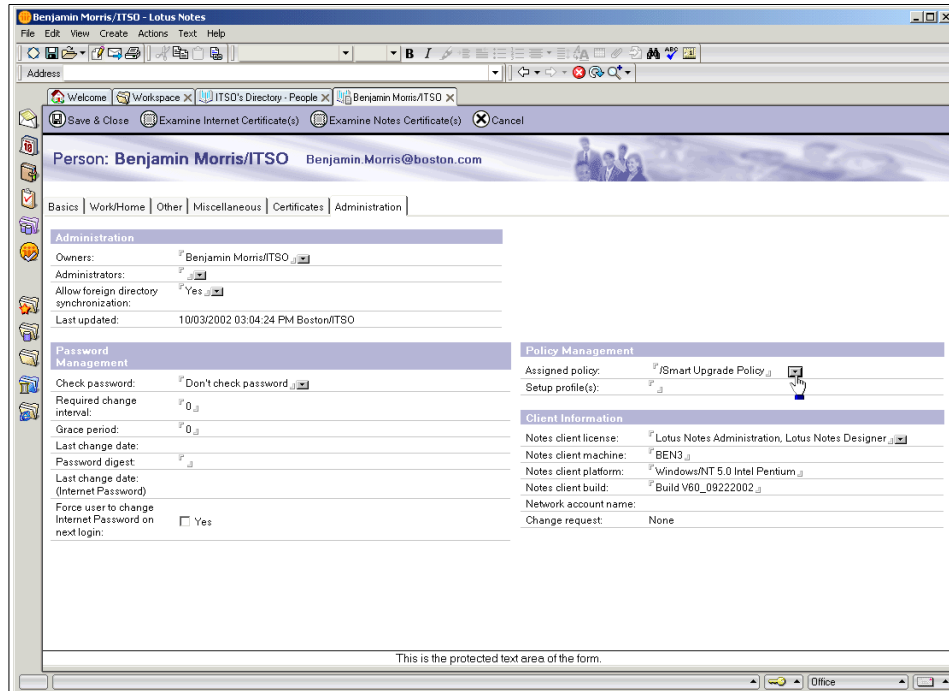


Figure 16-20 Policy set in a person document

At this point, when the user accesses the server, they should see a pop-up box similar to the one shown in Figure 16-21. You can see that the user has the option of upgrading the client or postponing the upgrade. The dialog box also contains the information about how many days until the client the client is automatically upgraded.

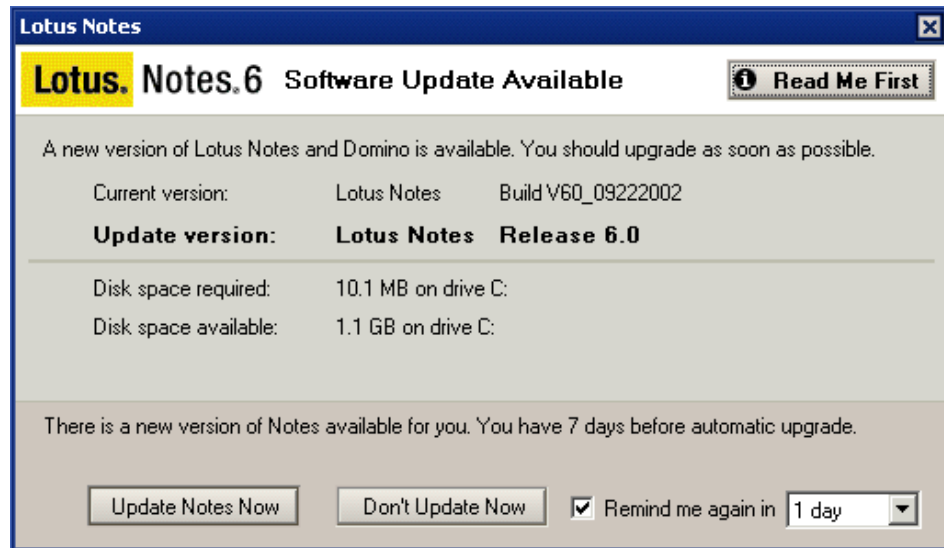


Figure 16-21 Smart upgrade popup screen

Tip: Because the servers now record client information in users' person documents, you will be able to determine which client levels are active in your environment without the need for a special utility. This will help you determine the need for automatic upgrade procedures such as smart upgrade. In order to make use of this information, create a private view in the name and address book which sorts person documents according to client builds, client platforms, or client types.

16.2 Making use of policies

You can use policies to control the Notes 6 desktop environment. Policies can be divided into two kinds: those which are implemented when the client is first installed and set up, and those which are dynamic (the client's settings get updated when it authenticates with the server). For a complete description of policies see Chapter 15, "Policy-based administration" on page 449.

Setup policies give the initial settings to the client when it is first set up on a workstation. Once these are in place, the dynamic policies take over so that the administrator retains flexibility in administering the clients. As Figure 16-22 illustrates, setup policies and dynamic policies cover much of the same territory.

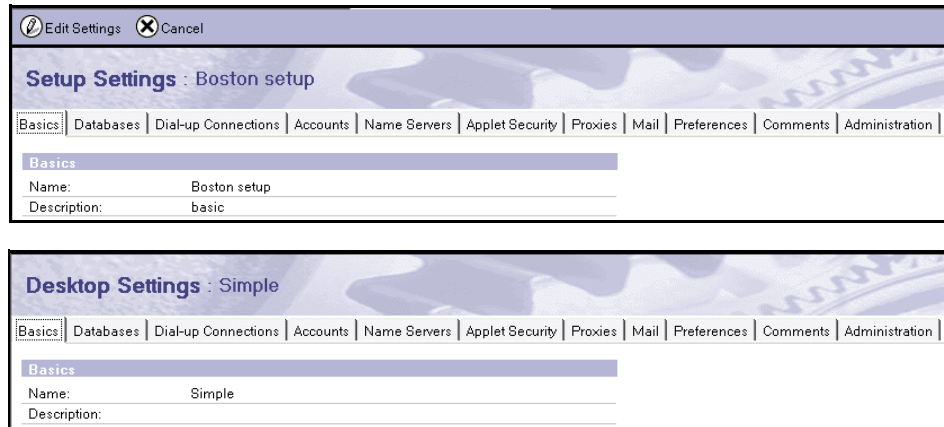


Figure 16-22 Similarities of Setup and Desktop settings

There are two desktop settings that are not also available as setup settings:

- ▶ Smart Upgrade (see 16.1.5, “Smart Upgrade” on page 484)
- ▶ Corporate welcome pages

The following sections describe the interaction between policy settings and desktop configurations. After describing each setting, we explain how it affects the client.

16.3 Corporate welcome pages

For a consistent, custom appearance across a company or organization, you can create custom welcome pages, and then deploy them to users through policies and desktop settings documents. They can be as simple as a background with a company logo, or sophisticated pages with multiple frames and many different types of content.

16.3.1 Create the new welcome page

1. With the Designer client, create a new welcome page database on your local workstation using the bookmark.ntf template as the design. You will need to check the “Show Advanced Templates” box in order to see this template.

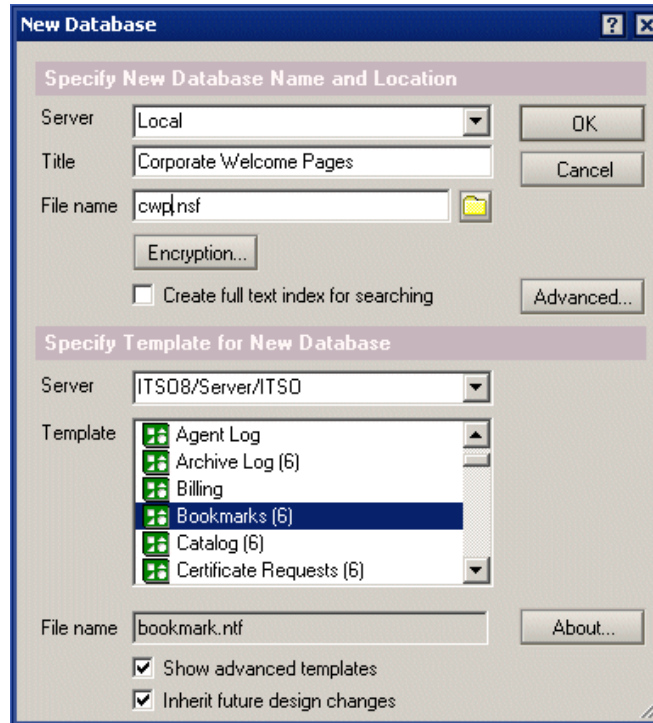


Figure 16-23 Bookmarks (6) template

2. With the Designer client, open the new database. Click the shared code section of the database in the navigation panel and click Agents.
3. Right-click the agent named (Toggle Advanced Configuration Editor) and click Run.

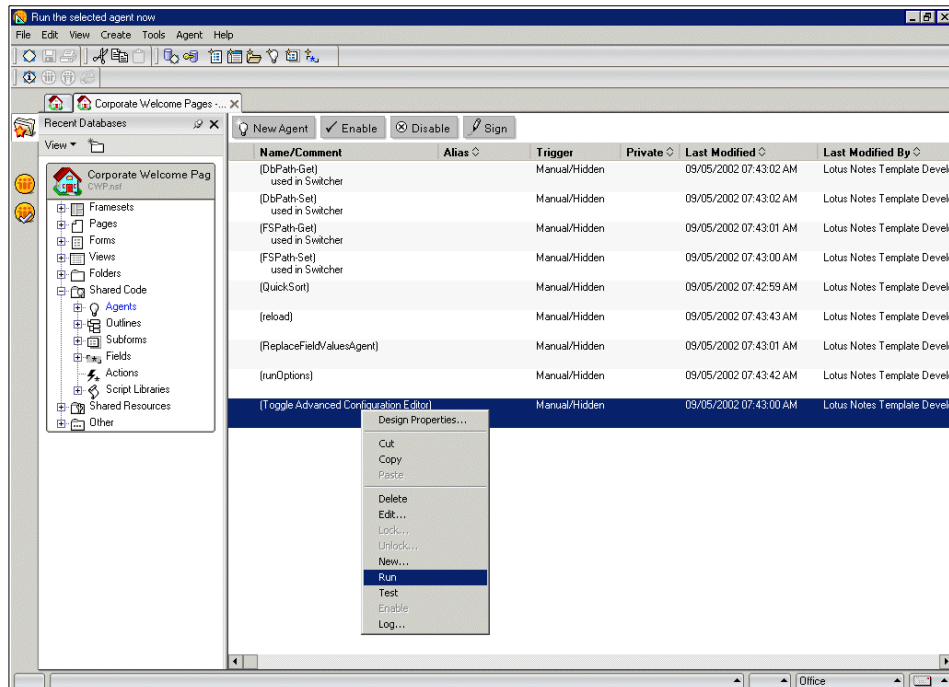


Figure 16-24 Run the Agent (Toggle Advanced Configuration Editor)

You will be informed that the Advanced Configuration Mode has been turned on after the agent runs. Because this agent is a toggle, if you run it again it will turn Advanced Configuration Mode off.

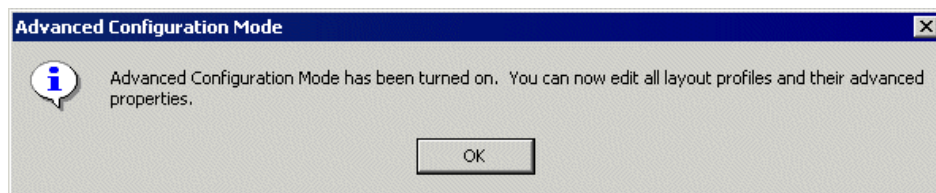


Figure 16-25 Advanced Configuration Mode confirmation

Tip: In order to configure the desktop settings document you have to have toggled the Advanced Configuration Editor on. You can double-check that this has occurred properly by looking in your notes.ini file. If the toggle worked it should have the line:

`$CurrentLayout=`

This line will have more added to it once you create the new welcome page and set it up for deployment.

Once the agent runs the log shown in Figure 16-26 will appear.

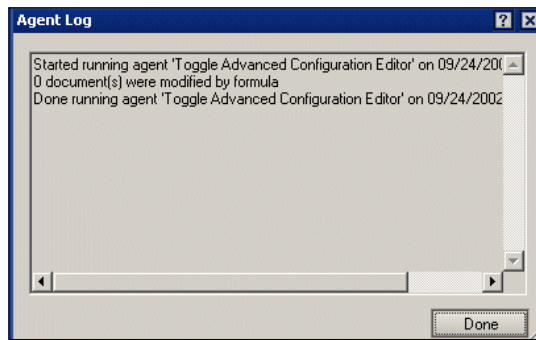


Figure 16-26 Agent log for “Toggle Advanced Configuration Editor”

4. Close the Designer client.
5. Change the ACL of this database so that everyone to whom you wish to distribute the custom welcome page will be able to access the database after you put it on the server. They will need reader access to the database.
6. With the Administrator client, open the new Welcome Pages database.
7. If the panel for customizing welcome pages is not open, open it by clicking the black triangle near the top center of the screen, as shown in Figure 16-27.

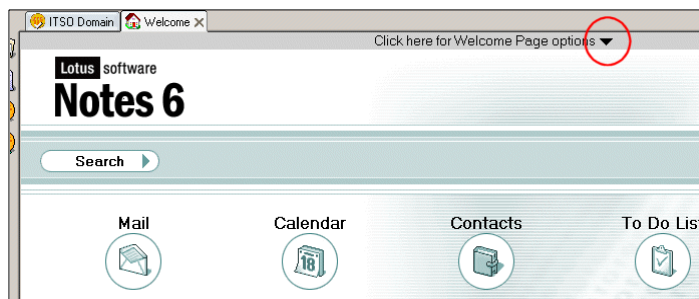


Figure 16-27 Open the Welcome Page options panel

8. Click the Create a new Welcome Page button.
9. Notice that the page name is preceded automatically with a “\$” sign. Do not delete the \$ sign. Give the new page a descriptive name by erasing New Page and putting something else after the \$ sign. Click Next.

Tip: If the \$ sign does not appear in the New Page name field, open the Designer client again and run the Advanced Configuration Editor toggle again (twice—once to turn it off and once to turn it back on).

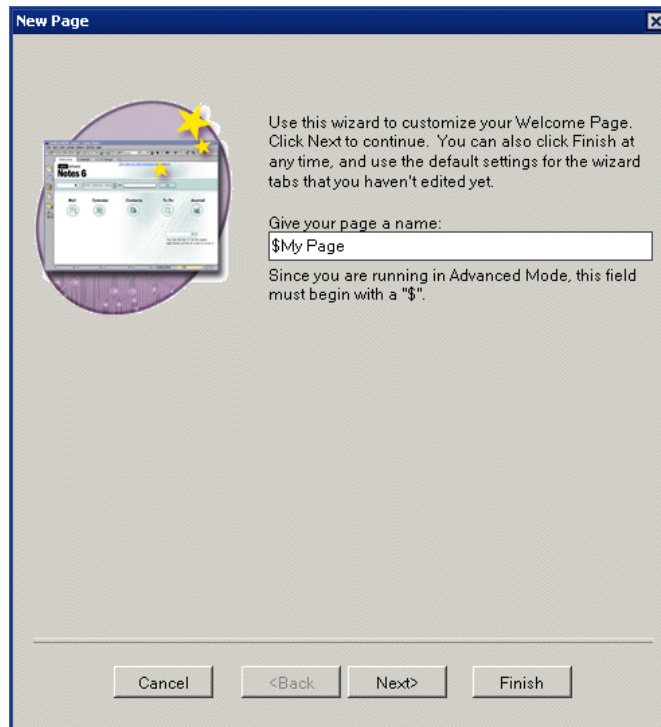


Figure 16-28 New Welcome Page

10. Choose between Frames or a Personal Page. Choosing Frames allows you to specify the content for one or more frames. For example, you could put a corporate discussion database in one of the frames and configure another one with the user's inbox. Personal Pages are predefined layouts, some of which include Java elements like a calculator and an analog clock. Both Frames and Personal Pages will work.

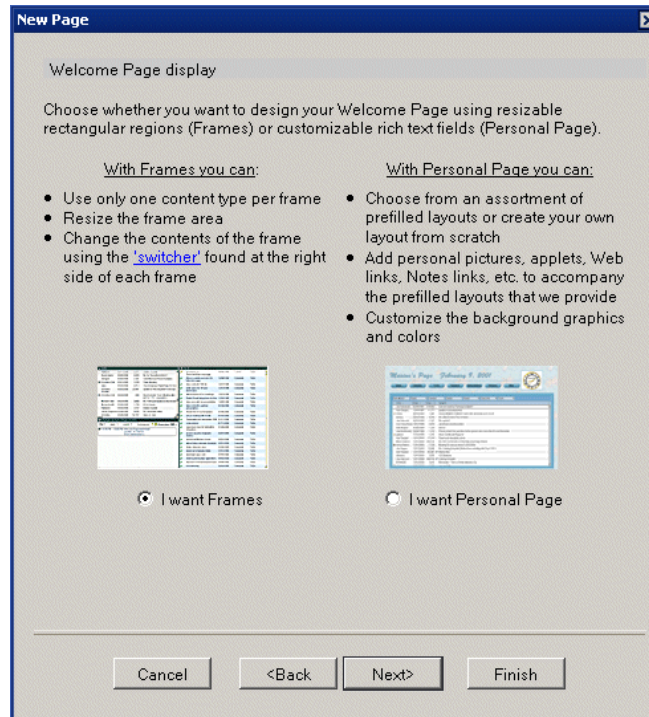


Figure 16-29 Frames or personal page

11. You will be given several more options depending on your choice in the previous step. Eventually you will get to a page that gives you the “List sort” for the welcome pages in the database (see Figure 16-30). You may want to change the list sort number for this page because the desktop settings document can only display about 10 pages for you to choose from. If the page you have just created is at the bottom of a list of 15 pages you won’t be able to choose it.

New Page

List sort

Sort key:

The sort key determines the order in which the profiles are displayed in the drop down list.

[Click here to see a popup list of all the current pages and their sort keys.](#)

Ignore layout settings

☐ Ignore all layout settings and instead load this frameset:

Checking this will cause the all layout settings to be ignored and instead the specified frameset will be displayed. When this is checked you should uncheck the box below to avoid confusing users.

User editable

☐ Allow end users to edit this page:

Checking this will allow the normal end user to edit the layout settings. They will not be able to see or edit any of the settings on this tab.

Figure 16-30 Welcome page list sort page

12. Click “Click here to see a popup list of all the current pages and their sort keys” to determine a sort number that has not been used before.

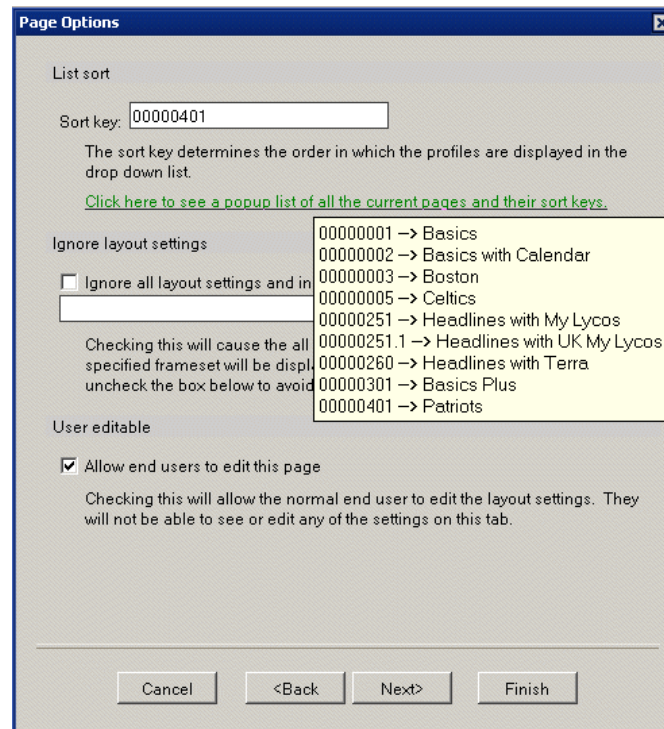


Figure 16-31 Check the sort order of the welcome pages

In this example you can see that the new page named “Patriots” appears at the bottom. You can move it up the list by changing the Sort key to something lower. Be sure to change it to a sort key that does not already exist. The sort key will not be saved until you complete the configuration of the welcome page.

13. Click Next and on the next page click Finish.
14. The new page will be saved. Click the black triangle again to close the Welcome Page options panel, and then close the database.
15. Open the database one more time to establish the correct sort order.
16. Make a copy of the database on the server. Double check the ACL to make sure your users have reader access.

16.3.2 Configure the desktop settings document

1. With the Domino Administrator client, open the new welcome pages database on the server.
2. Click the People & Groups tab in Domino Administrator.
3. Either open a desktop settings document that already exists or create a new one by clicking Settings -> Add Settings -> Desktop. If you are creating a new desktop settings document enter a name for it in the Name field.

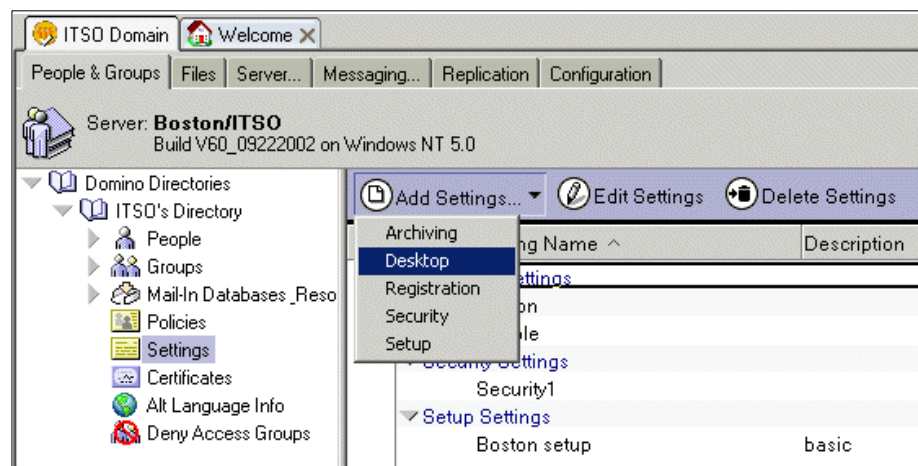


Figure 16-32 Create a new desktop settings document

4. Scroll down to the Homepage/Welcome Page Options section of the desktop settings document. From the Domino Administrator task bar, click the Welcome Page database and drag it to the "Corporate Welcome Pages database" field. This creates a database link (this must be a database *link* and not the path to the Welcome Pages database).



Figure 16-33 Create a database link to the Welcome Pages database

- In the “Default Welcome Page” drop-down list select the page that you just created. If you do not see the page you just created on the list, save and close the desktop settings document. When you reopen it the page should be included.

Homepage/Welcome Page Options		Inherit from parent policy:	Enforce in child policies:
Corporate Welcome Pages database:		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Default Welcome Page:	No default Welcome Page	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Home page selection:	No default Welcome Page Boston Celtics Patriots	their home page <input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Browser Options		Inherit from parent policy:	Enforce in child policies:

Figure 16-34 Select the Welcome Page

- (optional) Click “Do not allow users to change their home page” to prevent users from creating or selecting a home page other than the default. The corporate welcome page will appear on their desktops instead of their personal page.
- Click Save & Close. Enter a name for the desktop settings document if you have not already done so.
- Open an existing policy document or create a new one. You can use either an explicit or an organizational policy. Put the document in edit mode.
- In the Setting Type section click the drop-down box in the “Desktop” field and select the desktop settings document you created in steps 1 through 8.

Setting Type	Setting Name	
Registration:		New...
Setup:	Boston setup	New...
Archiving:		New...
Desktop:	Patriots	New...
Security:		New...

Figure 16-35 Select the desktop settings document in the policy

- Click Save & Close.

16.3.3 Apply the policy

If the policy is not an organizational policy you will need to apply it to specific individuals using the following steps.

1. In the Administrator client click the People & Groups tab.
2. Click People and select the individuals who should have this policy applied to them.
3. In the Tools pane click Assign Policy.
4. In the Assign Policy Options dialog box select the explicit policy you just created. Click OK.

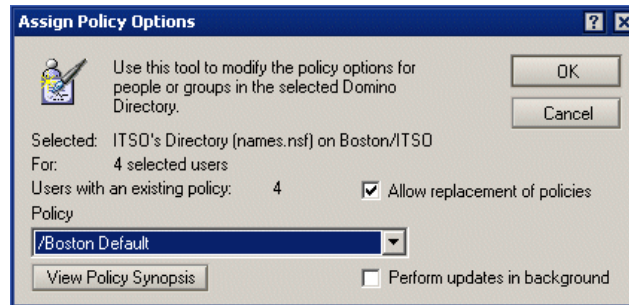


Figure 16-36 Assign Policy Options

5. You will be notified if it replaced the policy for any of the users. Click OK.

Note: If you apply an explicit policy to a user who is also subject to an organizational policy, the explicit policy will take precedence.

6. You can double-check to make sure that the policy was applied to the individuals by looking on the Administration tab of their person document.

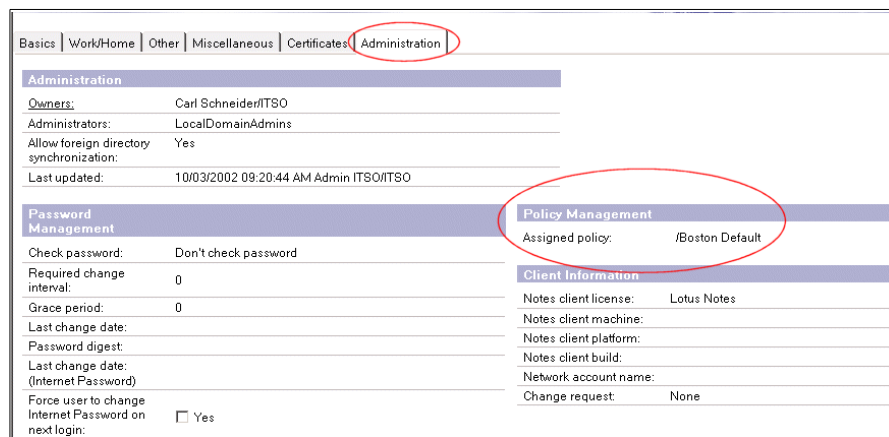


Figure 16-37 Policy Management section of a Person Document

Once you have applied the policy, check to make sure that a test user has received the new welcome page. It should appear by the second time they log in to Notes.

16.4 Other user interface features

Notes has over 1000 new features in the client alone. A few of them initiate interaction between the user and the administrator, or are likely to generate calls for help. This section covers the items we believe the administrator should be aware of: security basics, ID file information, other users' certificates (Notes and Internet), Notes data, and Mail options.

16.4.1 Notes ID files

A *certificate* is a unique digital signature that identifies a user or server. Notes user ID files contain one or more Notes certificates; they may also contain one or more Internet certificates. Internet certificates identify users when they use SSL to connect to an Internet server or send a signed S/MIME mail message. For more information on certificates and how they work, see Chapter 11, "Certificate Authority (CA) process" on page 357.

A certificate contains:

- ▶ The name of the certifier that issued the certificate.
- ▶ The name of the user or server to whom the certificate was issued.
- ▶ A public key that is stored in both the Domino Directory and the ID file. Notes uses the public key to encrypt messages that are sent to the owner of the public key and to validate the ID owner's signature.
- ▶ A digital signature.
- ▶ The expiration date of the certificate.

S/MIME is a protocol used by clients to sign mail messages and send encrypted mail messages over the Internet to users of mail applications that also support the S/MIME protocol, for example, Microsoft Outlook Express and Netscape Communicator. The Notes client uses the recipient's public key, stored in the Internet certificate in the Personal Address Book, Domino Directory, or LDAP directory, to encrypt messages.

The Notes 6 client is well equipped to help users manage their own certificates. In the user security documents the user can view and manage several different kinds of certificates.

To open the security settings on the Notes client, click File -> Security -> User Security. Enter the Notes password when prompted.

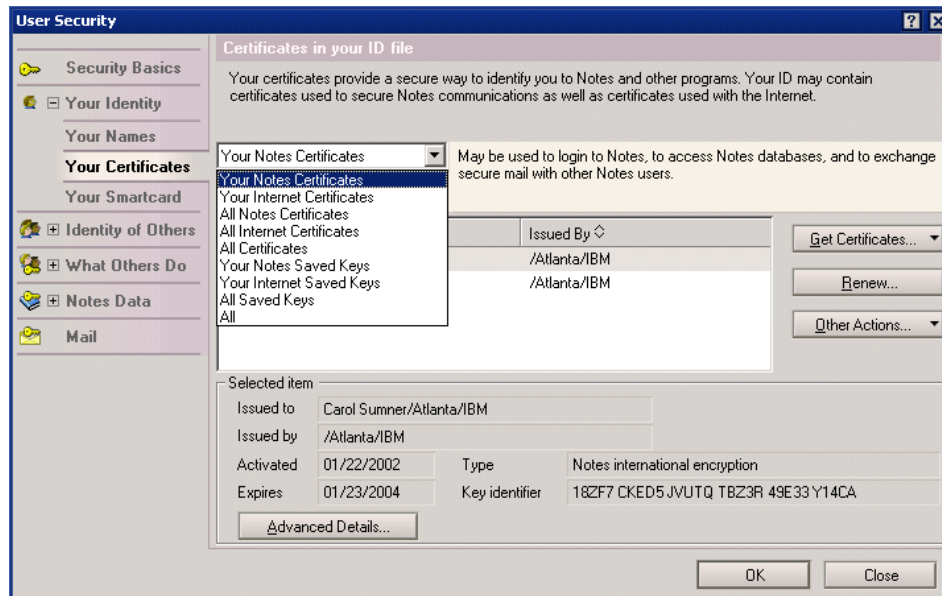


Figure 16-38 Certificate tool in the Notes 6 client

With the Certificate tool the user can request an Internet certificate from a Domino Certificate Authority or a third party certificate authority, like Verisign, and then import that certificate once it has been issued. The process for obtaining Internet certificates varies depending on the certificate authority. This can be a very complicated and confusing process for end users.

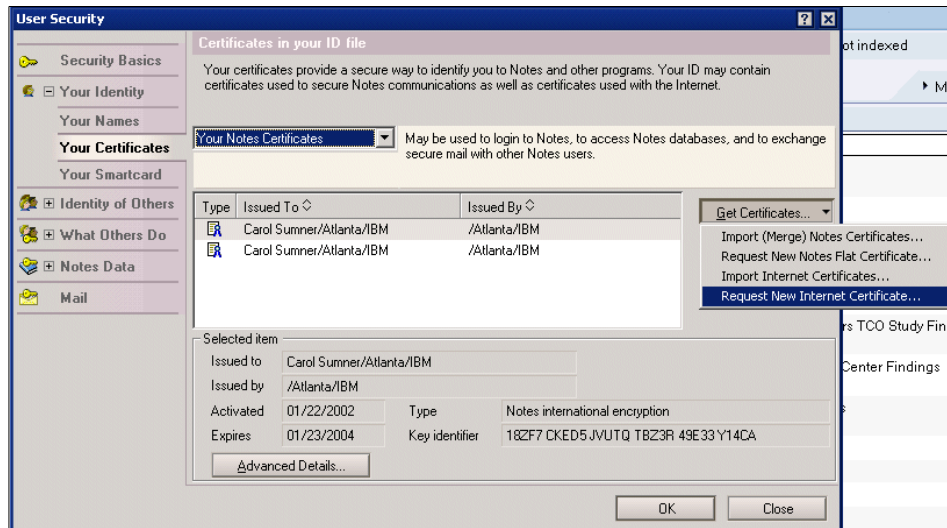


Figure 16-39 Request a new Internet certificate

If your users need an Internet certificate and you do not want to require each user to submit an Internet certificate request and then merge the certificate into the ID file, you can issue the Internet certificate using the existing public and private keys in the Notes ID file and add it to the user's Person document. Using the Domino Directory to issue Internet certificates simplifies the process of distributing Internet certificates to users. See Chapter 11, "Certificate Authority (CA) process" on page 357 for detailed information.

Request renewal of a Notes certificate

If a user notices that their Notes certificate is about to expire they can use the certificate tool in their client to request a renewal from their administrator by following these steps:

1. Open the security tool in the client by clicking File -> Security -> User Security.

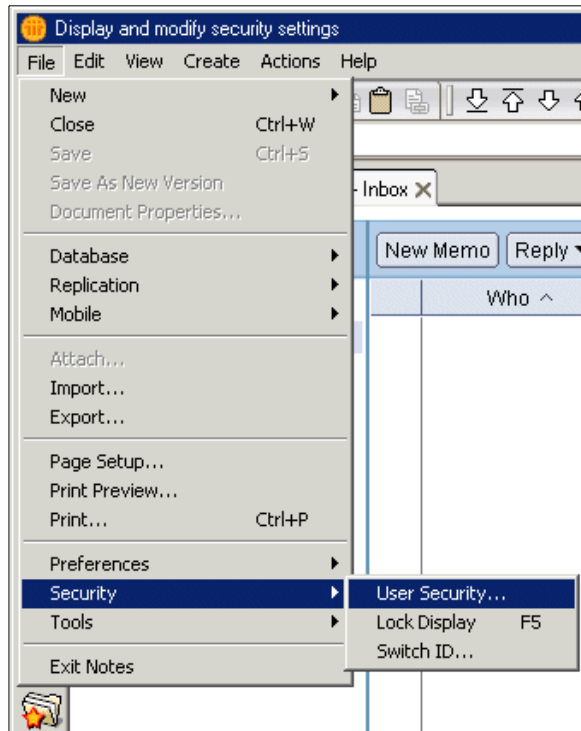


Figure 16-40 User security

2. Enter your password when prompted and click OK. The User Security tool will appear.
3. Expand the Your Identity section in the navigation pane.
4. Click Your Certificates.

5. Your name will appear twice in the box in the middle of the screen. This represents two different certificates that are already in your ID file. Click the second instance of your name and verify that it is the Notes multi-purpose certificate.

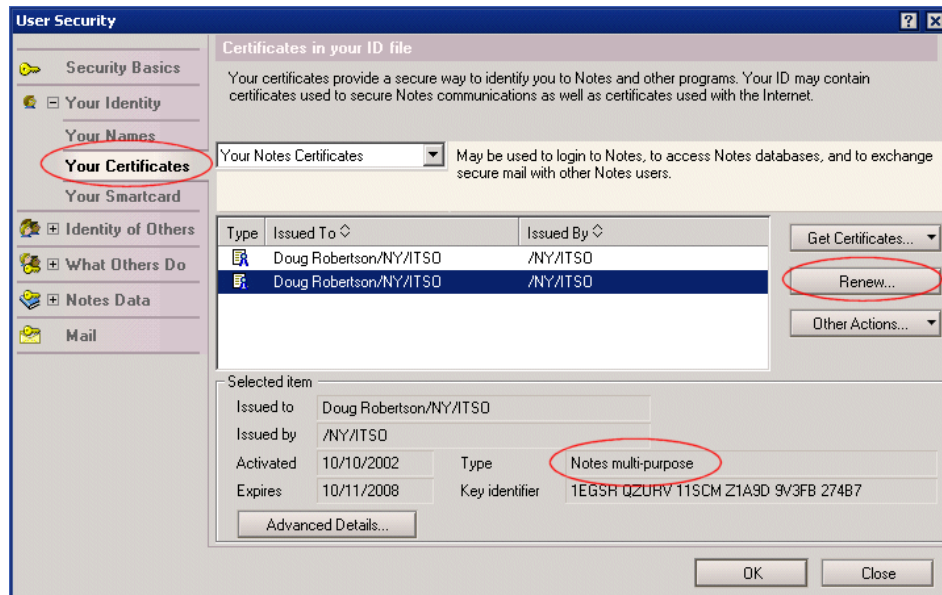


Figure 16-41 Request certificate renewal

6. Click the Renew button on the right-hand side of the screen.

7. You will be prompted with a Confirm Renewal dialog box. If you are sure that you want to renew your ID click Continue.

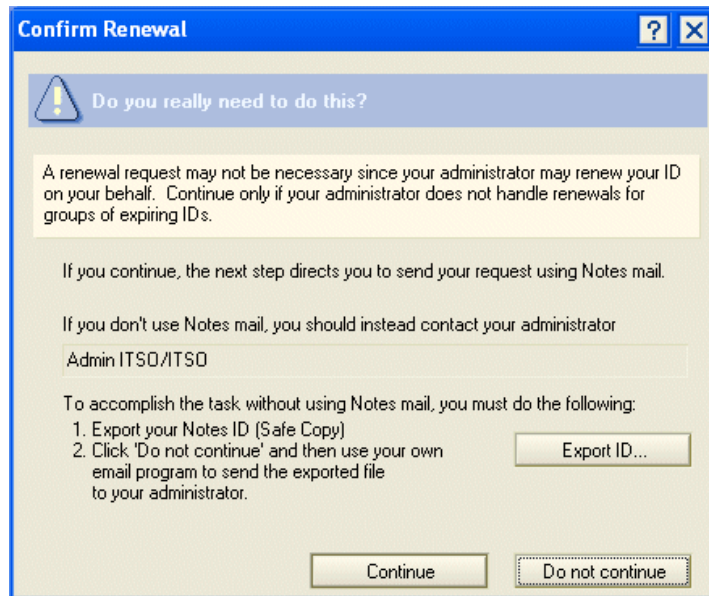


Figure 16-42 ID Renewal request confirmation

8. The Mail Certificate Request screen will appear. Change the "To:" field if you know a more appropriate recipient. Do not send this to someone who is not your administrator. Click Send.

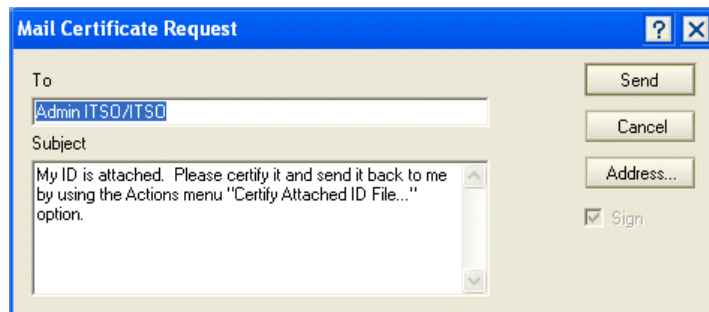


Figure 16-43 Mail Certificate Request

9. Your administrator must now act on your request before you can proceed. Once your administrator has renewed your ID it will be sent back to you.

10. Open the message from your administrator. It will have a new ID file attached to it.

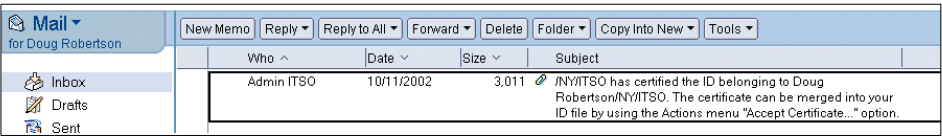


Figure 16-44 Certificate Renewal response from administrator

11. Click Actions -> Accept Certificate.

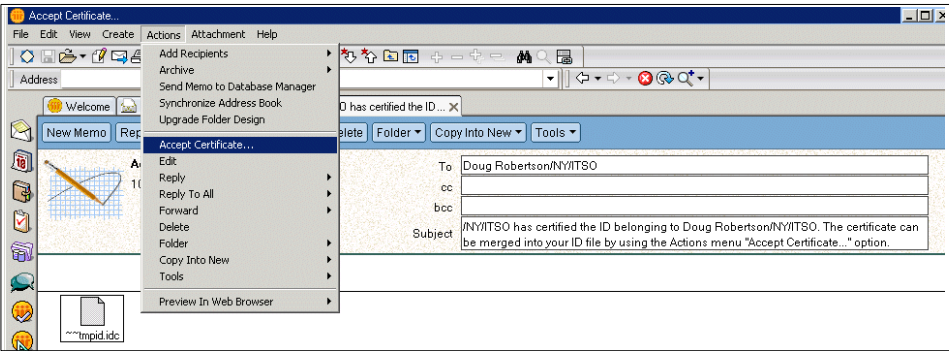


Figure 16-45 Accept certificate action in user's mail file

12. Enter your password when prompted. You will receive confirmation that the certificate has been inserted into your ID file. Click OK. You will receive another message warning you that your ID file has been modified. If you have other copies of your ID file (for example, on other workstations), replace them with a copy of the ID file on this workstation.

Administrator's response to a request for certificate renewal

When a user requests a renewal of their certificate, you handle it in exactly the same way as if they were requesting new public keys:

1. Find the request from the user and open it. It will have a subject line that begins with "My ID is attached" unless the user modified that when submitting the renewal request.

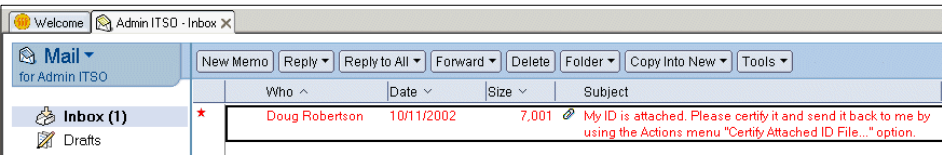


Figure 16-46 Certificate renewal request as it appears in administrator's inbox

2. Click Actions -> Certify Attached ID File. You will be prompted for the correct certifier to use. You can also choose to use the CA process if that has been configured. Use the Certifier ID button to browse to the correct certifier.

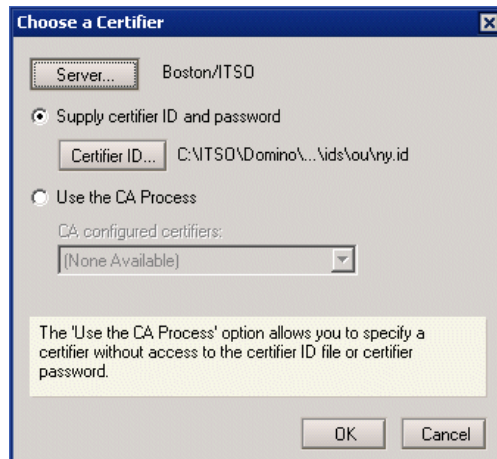


Figure 16-47 Choose a Certifier

3. Click OK. Enter the password for the certifier when prompted. The Certify ID screen will appear.

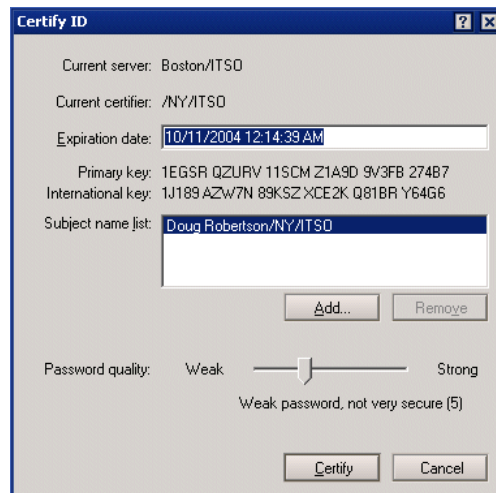


Figure 16-48 Certify ID screen

4. Change the date in the "Expiration date" field to a new date (your organization should have a policy about the length of time an ID file is valid).

5. Click Certify. The person document in the address book will be updated with a new public key. The Mail Certified ID screen appears.

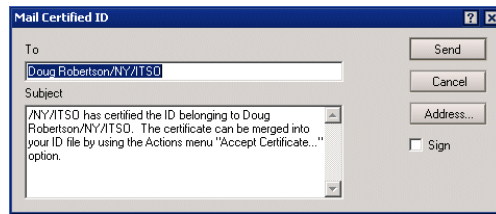


Figure 16-49 Mail Certified ID

6. Click Send to send the newly certified ID file to the user.

Smartcards

Beginning with Lotus Notes 6 you can use a *smartcard* with your Notes user ID to log in to Notes—provided you have a smartcard reader attached to your workstation or laptop and the appropriate software installed.

How smartcards work with Notes

In the default configuration Notes users must have access to their ID file and know the password to it in order to access the Notes client and server databases. Typically the ID file resides on the workstation, and in some instances in the user's directory on a network file server. This makes the ID file vulnerable to theft.

In a smartcard configuration the ID file can only be accessed with the aid of the smartcard. When the user wants to access Notes she or he must insert the smartcard into a reader attached to the workstation and enter a pin number to open the ID file. Thus, in order to log in to Notes, a user has to have their Notes ID, the smartcard, and the smartcard pin number.

Important: If you enter the wrong pin number to a smartcard too many times, you can lock yourself out of the smartcard. Since your smartcard controls access to your Notes ID, you'll be locked out of your Notes ID as well.

Notes users can enable smartcards entirely from within their own client. However, it is not recommended that you encourage your users to do so on their own. It is a better idea to have an organizational strategy for handling smartcards. As you are no doubt aware, anything which increases security also increases administrative overhead.

Attention: Turn off password expiration for those users who will be enabling their clients for smartcard login. If you do not they will eventually get locked out of their accounts.

Important: Make sure the ID file being locked with a smartcard has been enabled for ID recovery. Disable password checking for the users who will be enabling their IDs with smartcards. If password checking has been enabled the user will not be able to use the recovered ID.

Steps for enabling a client to use a Smartcard

1. Verify that the ID file on the client was configured for ID recovery when it was created. At the very least, make sure that there is a backup copy of the ID file somewhere.
2. Make sure the Smartcard reader and any supporting software have been installed on the workstation.
3. Once the Notes client has authenticated with the server, open the security settings on the client by clicking File -> Security -> User Security. Enter the Notes password when prompted.
4. Click Your Identity -> Your Smartcard in the navigation pane.

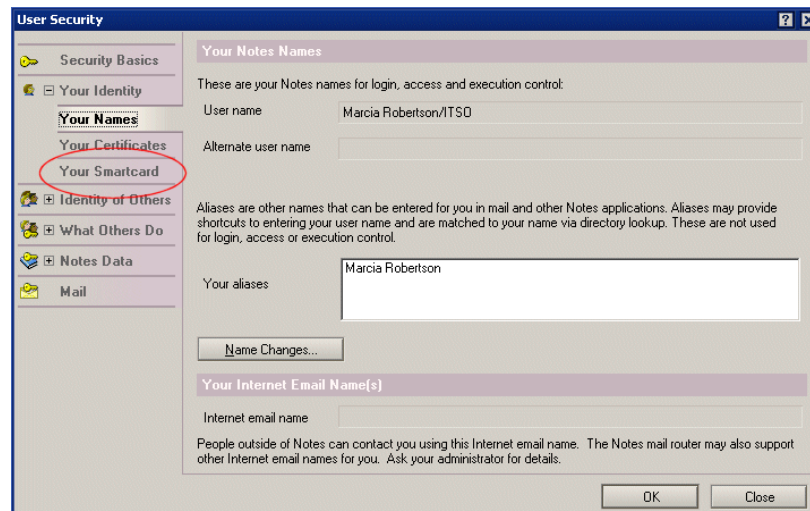


Figure 16-50 Navigate to Your Smartcard in User Security

5. The Smartcard Configuration utility will be displayed.

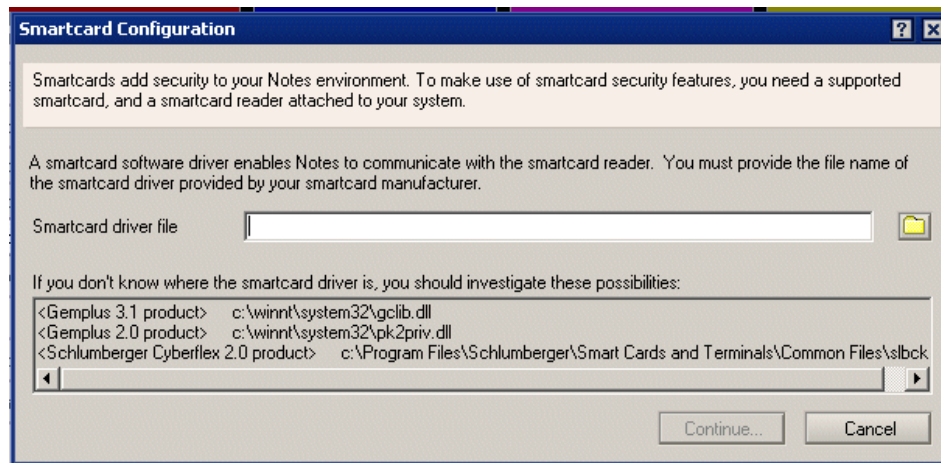


Figure 16-51 Smartcard configuration utility

6. In the configuration dialog box enter the location of the Smartcard driver file. If you don't know where it is try the suggestions Notes gives you in the bottom third of the screen. The documentation for your smartcard reader should indicate where the driver file is.
7. Click Continue.
8. Once Notes recognizes the Smartcard driver file it will bring you back to the User Security screen. Click the Enable Smartcard Login button under "Using your smartcard with Notes."

Important: Once you enable an ID file to work with a Smartcard you cannot disable it. You cannot switch between an ID that is enabled to work with a Smartcard and one which is not if password checking has been enabled on the Notes account.

9. You will be prompted for the Notes ID password and the smartcard pin number. Enter as prompted.
10. You may be prompted for a descriptive name for the smartcard. Enter one if prompted.
11. The next time this user logs in to Notes they will need to use the smartcard pin number instead of the Notes ID password.

Worst case scenario

One of your users has smartcard-enabled their ID file and now they can't seem to log in to Notes. The server is set up to expire passwords and to do password checking.

Possible Problems:

- Notes has expired the password because it has not been changed in the allotted time.
- The user has forgotten their smartcard pin number.

Take the following steps.

1. Verify that the user is entering the correct pin number for the smartcard and that Notes is able to open local databases. If they cannot use the Notes ID file because they have forgotten the smartcard pin number perform all of the following steps *and* give the user a copy of their ID file from a time before it had been smartcard-enabled. You can use the ID recovery database for this, or a copy from another source if the ID was not created with ID recovery enabled.
2. Open the user's person document in the Domino Directory.
3. Click the Administration tab. Look in the Password Management section of the document.





Password Management	
Check password:	<input checked="" type="checkbox"/> Check password 
Required change interval:	<input checked="" type="checkbox"/> 30 
Grace period:	<input checked="" type="checkbox"/> 7 
Last change date:	
Password digest:	<input checked="" type="checkbox"/> F421F516F8B17DCA7C837D06B8C58954 
Last change date: (Internet Password)	
Force user to change Internet Password on next login:	<input type="checkbox"/> Yes

Figure 16-52 Password Management in the person document

4. Change the "Check password" field to Don't check password.
5. Delete the entries in the "Required change interval," "Grace period," and "Password digest" fields.





Password Management	
Check password:	<input type="radio"/> Don't check password 
Required change interval:	<input type="radio"/> 
Grace period:	<input type="radio"/> 
Last change date:	
Password digest:	<input type="radio"/> 
Last change date: (Internet Password)	
Force user to change Internet Password on next login:	<input type="checkbox"/> Yes

Figure 16-53 Password Management settings for Smartcard enablement

6. Click Save & Close. Test the user's access from their workstation.

16.5 License tracking

License tracking allows you to monitor the number of active Notes users within a Notes domain. You can use license tracking to determine how many client licenses you have, whether you need to purchase additional licenses, and when you need to purchase them.

Client usage is tracked on each server. When a user authenticates with a server using the Notes client, HTTP, IMAP, POP3, SMTP, or the LDAP protocol, the user's full canonical name, protocol, and time and date of access are collected. Once each day, an administration request sends information regarding new users and information regarding users who have not accessed the server within the last 30 days to the administration process. The administration process running on the administration server processes the request.

Enabling license tracking

1. From the Domino administrator, click the Configuration tab.
2. Choose Server -> Configurations.
3. Select the server and click Edit Configuration.

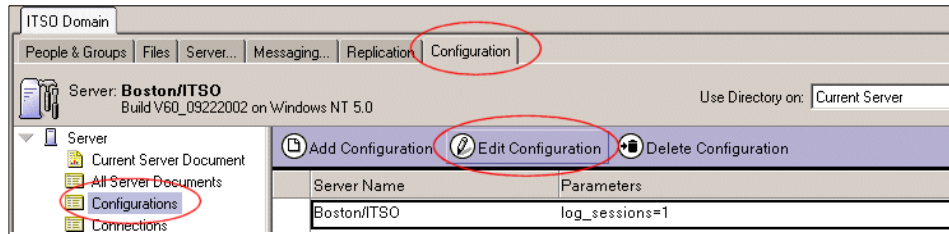


Figure 16-54 Navigate to the Configuration Document

4. On the Basics tab, in the “License Tracking” field, click Disabled or Enabled according to what you want to do.

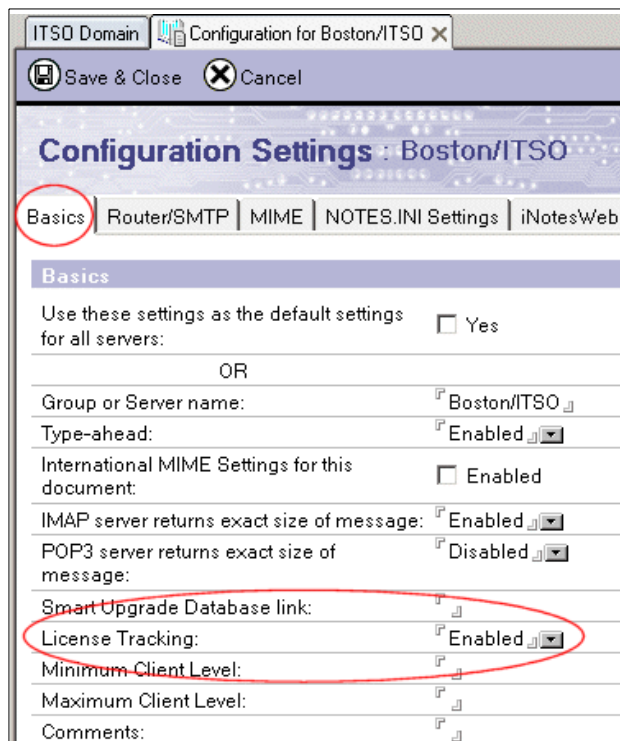


Figure 16-55 License tracking configuration

5. Click Save & Close.

Tip: After you set this up you will need to wait at least one day before viewing the license tracking information. License tracking information is collected and processed by adminp only once per day. The license tracking database (userlicenses.nsf) is not created until the first time that adminp processes license information. It will be created on the administration server of your Domino Directory.

Viewing the license tracking information

1. From the Domino administrator, click the People & Groups tab. Once you have enabled license tracking a new view appears under the People & Groups tab, called Domino User License Tracking. This view is actually pulled from the Domino User License Tracking database which was created by the adminp process when you enabled license tracking.
2. Click View Domino User License Tracking and then click the Active Users view (not the Active Users folder).

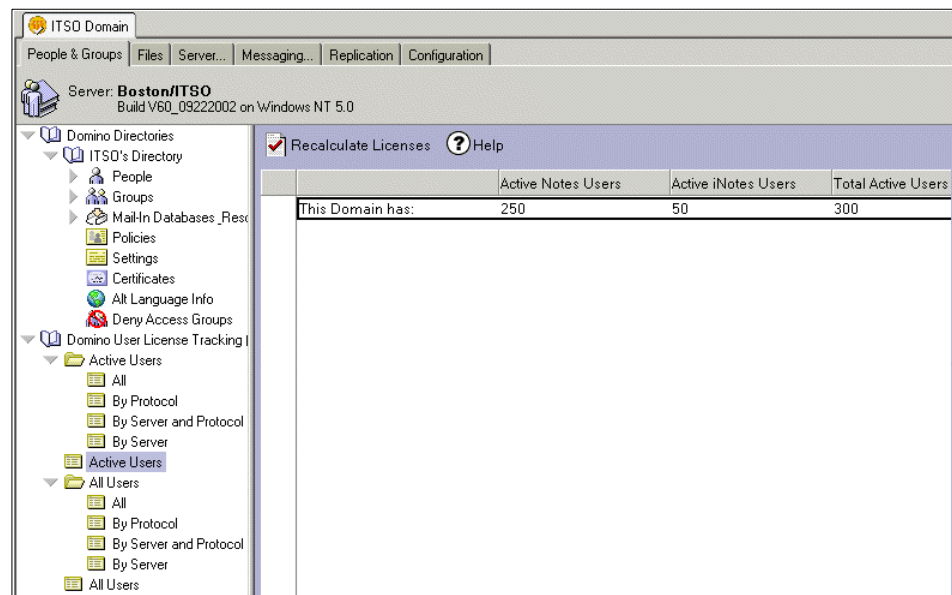


Figure 16-56 Viewing license tracking information

3. You can force an immediate recalculation of the number of licenses by clicking the Recalculate Licenses button in the action bar:

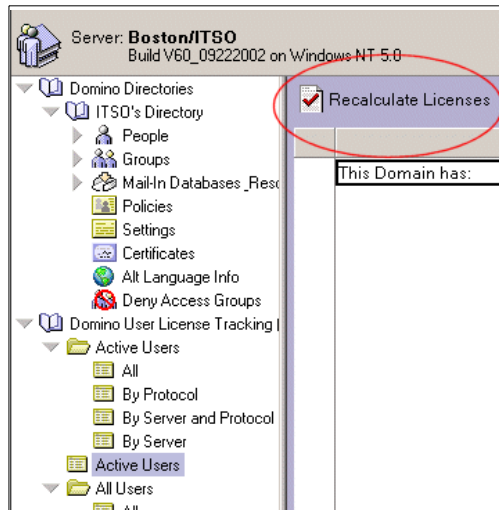


Figure 16-57 Recalculate licenses

4. Look at the section in the navigation panel named Domino User License Tracking. You can see different views of the server access records. You can view them by all users, or active users only, by protocol, by server, by server and protocol, or uncategorized.

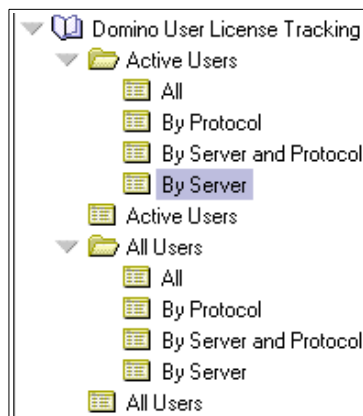


Figure 16-58 License Tracking views

5. Click All under either the Active Users or All Users section to open a list of all the server access records. Open one of the server access records and examine it. Note that you can determine all the ways in which an individual is accessing your servers and how long it has been since they accessed any of the servers.

ITSO Domain CN=Marcia Robertson/O=ITSO X

Close

Marcia Robertson/ITSO - Server Access Record

Usage

Server(s) Accessed: Boston/ITSO
 Month of last access: 09/2002
 Protocol(s) Used:

- ☐ HTTP
- ☐ IIOP
- ☐ IMAP
- ☐ LDAP
- ☒ Notes
- ☐ POP3
- ☐ SMTP

Figure 16-59 Server Access Record

Note: By default the license tracking system keeps records of individuals for one year past the last time that they accessed the system. After that it automatically deletes the record so that you can keep track of the number of licenses actually needed.

Tip: You can change the expiration period for the old documents by editing the Domain Settings document in the User License Tracking database and changing the field “Delete Days” to whatever best fits your environment:

1. In the Domino Administrator client go to the People & Groups tab.
2. Open the view under Domino User License Tracking and click the Active Users view (not the Active Users Folder).
3. Double-click the document, “This Domain has:”
4. Double-click to put the document in edit mode. At the bottom of the document you will see that there is only one field, “Delete documents in:” that you can edit. Change it from 365 to whatever value you want.
5. Click Save & Close.



A

Consolidation

This appendix describes the possibilities for consolidation that Notes and Domino 6 gives to administrators.

The improved scalability and consolidation support features of Notes and Domino 6 offer you the opportunity to really focus on the business applications, application data, reducing costs, simplifying administration, and improving the availability of your application service.

Benefits of consolidation

Consolidation is a lot more than just replacing a number of small distributed servers with a few bigger centralized ones. It is about aligning your infrastructure to meet your current business model requirements and achieving improvements in control and reliability. The goal of consolidation is to optimize and simplify your end-to-end infrastructure.

The reasons why companies choose to consolidate their Domino environment can vary quite a bit. Among the reasons are:

- Reducing the total cost of ownership (TCO)
- Easier administration and system management
 - Centralizing system administration
 - Bundling knowledge in central locations
 - Reducing the number of administrators
- High availability and performance improvements
 - Larger and more robust systems
 - Redundancy and failover capabilities
- Improving backup and restore operations
- Effective utilization of hardware and software
 - Better storage utilization
 - Better CPU utilization
 - More efficient utilization of network bandwidth
- Standardized environment
- Increased security and control

All of these factors can contribute to higher performance at lower cost, which is generally a compelling reason for undertaking a consolidation effort.

Table A-1 describes four consolidation scenarios and what the benefits of each scenario can be to an organization.

Table A-1 Consolidation benefits

Type of consolidation	Definition	Potential Benefits
Location centralization	Location centralization Relocate to fewer sites	Increased reliability and availability Reduced facilities costs Lower operations costs Improved security and management Reduced hardware and software costs Improved processor utilization Reduced facilities costs Lower operations costs Improved manageability Hardware and software standardization
Server consolidation	Replace small servers with large servers	Reduced storage management costs Improved resource utilization Lower administrative costs Improved backup/recovery capabilities Enhanced data access and integrity
Data consolidation	Combine data from multiple sources onto a single repository	Reduction in number of administrators Increased reliability and availability Reduced facilities costs Lower operations costs Scalability
Application consolidation	Consolidate to one platform	Reduction in variety of skills required by administrators Increased reliability and availability Reduced facilities costs Lower operations costs Scalability

Attention: The consolidation scenario most appropriate in your organization depends on your current infrastructure. There is no single off-the-shelf solution for server consolidations, only best practice guidelines and advice from experienced practitioners.

See more details in:

<http://www-1.ibm.com/servers/solutions/serverconsolidation/views.html>

Consolidation and Domino 6

With the development of Domino R5 there were significant changes to support larger consolidated environments, increasing the servers' availability to end users. Options like transactional logging, multi-client support and cluster load balancing gave huge benefits to R5 deployments.

Domino 6 has gone even farther, adding to the benefits of R5 with new technologies that help your organization to work more efficiently.

The following specific solutions help you to install, configure, manage, and monitor a consolidation process that accommodates all the new features of Domino 6 mentioned previously in this book.

- ▶ **Multi-language**

The Domino 6 server supports multiple languages to be configured on one single server. This reduces the need for single or dual (R5) language servers and supports centralized implementation.

This is supported by your Domino servers, the most common Web browsers, and the Notes 6 clients.

- ▶ **Multi-client support (Notes, IMAP, POP3, iNotes)**

The Domino 6 server is able to host Lotus Notes, Lotus iNotes Web Access, POP3, and IMAP clients within a single messaging infrastructure, so multiple clients can be consolidated onto a single server. This was also the case in Domino R5, but now the possible workload has been increased significantly. In the case of IMAP the entire code was rewritten to improve performance and take advantage of advanced IMAP features (for example, the NAMESPACE extension).

- ▶ **Storage compression**

Attachments are now stored with LZ1 compression, and features such as “edit in place” and “reply without attachment” also help reduce costs and disk space. This might save up to 50% of your storage growth in the near future.

- ▶ **Network compression**

Network compression is an efficient way to reduce network traffic and therefore give better replication support for mobile or remote users and heavily loaded WAN links. The amount of bytes sent during transactions might be decreased up to 50%.

- ▶ **Streaming replication**

Faster replication for servers and users enables you to replicate more often and handle more effective replication connections.

► Enhanced management and monitoring tools

The management of load balancing, and the monitoring of system resources, activity trends, and events will give you more control over and insight into your environment. Additionally, the Tivoli monitoring and load balancing capabilities help you improve your server environment even more.

► Mixed-version partitions

Domino 6 lets you run different versions on separate partitions on the same physical hardware (UNIX only). This allows you to upgrade one server at a time in partitioned environments and possibly leave a dedicated R5 server for specific purposes. This option enables you to create a mixed R5 and Domino 6 partitioned environment on a single piece of hardware.

► Server reliability

These improvements make it possible to consolidate servers to a more reliable Domino server environment when moving to Domino 6:

– Domino clustering enhancements:

- Cluster awareness when registering users.
- Cluster replication can be stopped.
- Making the Cluster Administrator a server thread, so it automatically starts the Cluster Replicator and Cluster Database Directory Manager.
- Ensuring the server availability index gives a more accurate indication of the availability of each server in a cluster. (You no longer need to use the NOTES.INI setting `Server_Transinfo_Normalize` to improve accuracy.)
- Adding new settings to control the number of active cluster replicators.
- Using the Domino 6 Server Monitor to monitor all servers in a cluster.
- Allowing cluster replication to ignore database size quotas.
- Making activities, like database replication and deletion, cluster-aware.
- Adding new Cluster Replicator commands for better control over cluster replication and information gathering.

– Enhanced transactional logging:

- View logging of critical views.
- Enhanced transactional logging.
- Added linear logging style.
- Quota enforcement based on actual usage instead of file size.

– Fault tolerance and fault isolation including the capture of more details:

- Isolation and capturing of system fault events.

- Automated recovery including cleanup scripts.
- Automatic server restart and administrator notification.
- Extended logging information including severity indications.
- Faster restart due to the start of server tasks before starting the database consistency checks.
- Full text searches have been redesigned and need fewer resources to perform faster.

Planning for consolidation

You cannot just start to consolidate by examining your inventory and moving data around. The consolidation process should be planned carefully to provide your users with a seamless Domino consolidation and possible server upgrade.

This section describes some issues you should consider when planning a consolidation project.

Service level requirements

Consolidations are often planned so that service level for users can be increased while costs are decreased. When planning to consolidate your environment, you need to gather the business requirements of your users about sever uptime, service levels, functionality, performance, user locations, and connectivity. Write these requirements down in an agreement, usually called an SLA (Service Level Agreement). Such an agreement covers the responsibilities and expectations of all the parties involved.

Logical environment considerations

The application, in this case Domino, is the most important part of the service you give to the users. Many organizations start thinking about hardware and network requirements while the most important part, the application, comes last. We recommend that you start your considerations about the application infrastructure immediately after you have gathered the service level requirements.

Some of the considerations for a logical definition may be:

- Do I want to implement new Domino 6 features.?
- Do I want to consolidate or expand Domino domains?
- Do I need to have more or fewer logical Domino servers?

- Do I want to enhance my Domino security?
- How do I host my external domains?
- Do I want to use Domino clustering and/or partitioning?
- Can I decrease the number of Notes Names Networks?

Of course there are many more factors to be considered. Review the consideration section in Chapter 4, “Upgrade considerations for Domino servers” on page 29.

Physical environment considerations

After you have created a logical Domino design you can start gathering information about the location, hardware, network, backup, and restore requirements that define the service level you have agreed to deliver.

Some of the considerations for the physical environment may be:

- Do I want to use the current operating system?
- Do I need to upgrade or replace my server hardware?
- Do I need to consolidate or just centralize hardware?
- Do I need to increase my network bandwidth?
- Do I need more or less floorspace in the server room?
- Do I have enough power to feed high availability power consuming machines?
- Do I need to add more redundant elements (network, power, cooling)?

All of these questions, and probably many more, need to be considered and planned out in detail before you can design and offer a secure, highly available Domino environment with the appropriate service levels that meet your users’ expectations.

Planning your consolidation path

The following list of items is a generic path to follow when you start preparing for consolidation. For each area you should document what the current situation is, so that at the end of the implementation you can verify that the consolidation has helped the organization meet its goals. Each area may need customization depending on the situation at hand.

- Definitions and requirements:
 - Define business goals and requirements

- Define applications requirements
- Define response time and availability expectations (service levels)
- Create policy model
- ▶ Create a logical design
 - Create logical Domino infrastructure design
 - Create standards model
 - Define platform requirements (OS choice)
 - Choose platform operating system
- ▶ Create a physical design
 - Define network requirements (bandwidth, locations, protocols, routers, carrier)
 - Define hardware requirements (Processing power, file systems, storage, backup)
 - Create network design
 - Create hardware design
- ▶ Clean up your existing environment
- ▶ Implement the plan
 - Develop repeatable procedures and document
 - Plan communications with end users if they will see a change
 - Train help desk, administrators as needed
 - Conduct limited pilot
 - Conduct expanded pilot, incorporating lessons learned from limited pilot
 - Create implementation schedule and follow through
 - Communications
 - Post-consolidation support
 - Helpdesk
 - Verify that the new design is working as planned
 - Verify that new service levels are being met



Monitoring and troubleshooting

This appendix introduces some server monitoring tools that are available for the various operating systems that Domino runs on, as well as tools for Domino server. We also describe troubleshooting techniques and introduce you to some of the tools available for this task.

Monitoring your Domino server

Once you have upgraded your server to Lotus Domino 6, you will have to ensure that everything is working as expected. This section describes just a few of the key statistics you should watch, specifically:

1. Operating system statistics
2. Domino core statistics

Operating systems statistics

Platform performance statistics were introduced in Domino R5.02. Now, OS statistics can be directly retrieved from Domino server console, mailed or displayed in the Domino Administrator 6 client, and you can use Monitoring Configuration and Monitoring Results databases for both real-time and historical statistics. Furthermore, using IBM Tivoli Analyzer for Lotus Domino, you will be able to draw some charts directly from your Domino administration 6 client, as well as perform continuous server health monitoring. For more details about IBM Tivoli Analyser for Lotus Domino, refer to Domino Administration 6 Help database.

Lotus Domino 6 includes Platform statistics for the following platforms:

- ▶ AIX 4.33 and AIX 5.1
- ▶ OS400
- ▶ Solaris 8 Sparc
- ▶ Windows 2000 on Intel
- ▶ Windows NT4 on Intel
- ▶ Z/OS
- ▶ Linux (Red Hat, SuSE)

Tip: If for any reason you don't want to have platform statistics running, you can turn it off by using this notes.ini parameter:

```
Platform_Statistics_Disabled=1
```

To display platform statistics using your Domino Administration 6 client, select the server that you want to monitor, then go to the Server - Statistics tab and expand Platform as shown in Figure B-1 on page 533.

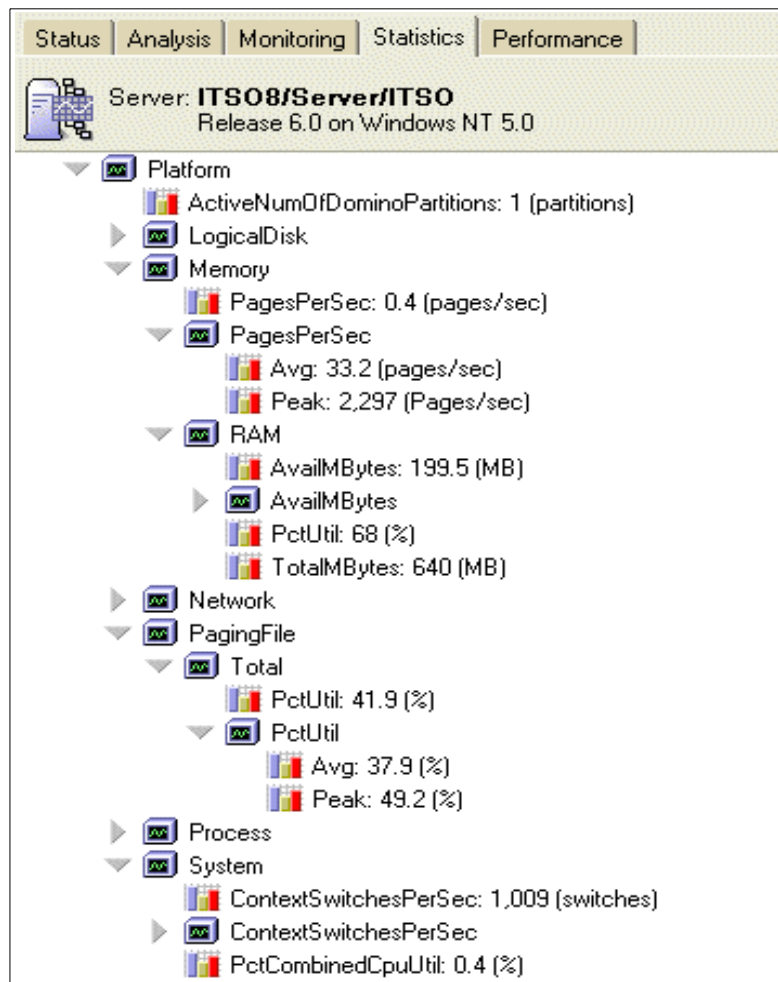


Figure B-1 Showing Platform Statistics in your Domino Administrator client

You can get a full description of each statistic displayed by right-clicking it and selecting Get Info, as shown Figure B-2. Figure B-3 shows the description of the selected platform statistic.

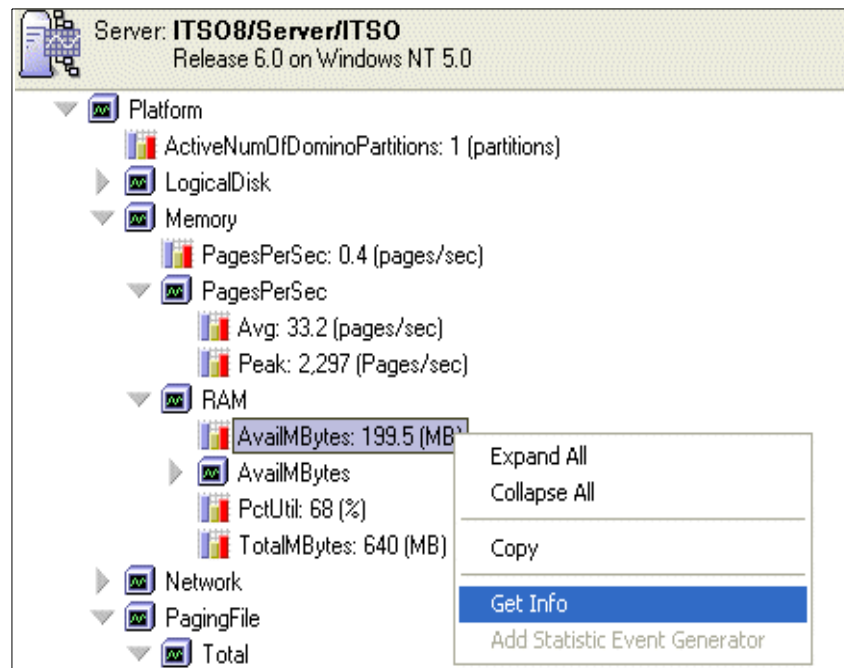


Figure B-2 Selecting Get info to show platform statistic description

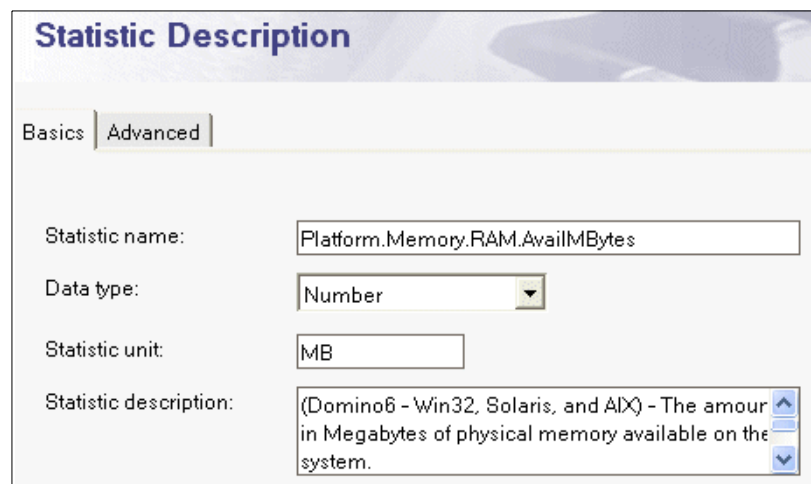


Figure B-3 Platform statistic description

If you prefer to have a complete overview of all statistics descriptions, you can go directly to the Configuration tab in your Domino Administrator client, open the Monitoring Configuration\Name_Messages (Advanced) folder, and open the Statistic Names view.

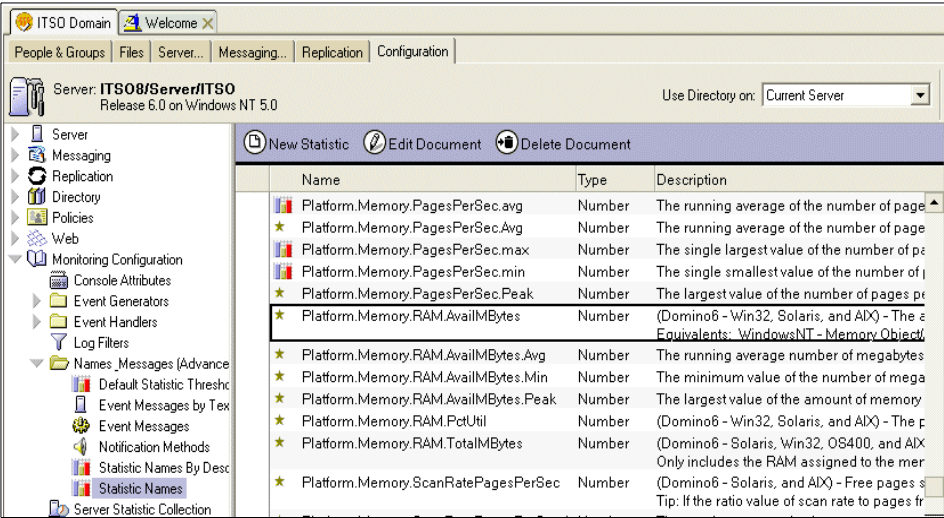


Figure B-4 All statistics description displayed in your Domino administrator client 6

There is a full range of platform statistics to monitor, but the most essential ones to monitor, especially after the server upgrade, are:

- ▶ CPU utilization
- ▶ Memory utilization
- ▶ Disk I/O activity
- ▶ Disk capacity

Compare your current values with the average utilization that you had when your server was running Domino R5, and verify that there is no bottleneck on your platform system.

Depending on your server platform and usage pattern, you can roughly apply the critical thresholds shown in Table B-1 for some OS components.

Table B-1 Maximum limit allowed for each OS components

OS components	Win2K	AIX	OS/400
CPU load	85 %	95 %	97 %
Disk utilization	60 %	60 %	40 %
Memory utilization	90 %	90 %	90 %

Attention: These values are just some common limit,s; you will have to define your own limits as a function of your infrastructure design.

You can also display platform statistics at the server console level by issuing the server console command **show stat platform.***

```
sh stat platform.*
Platform.ActiveNumOfDominoPartitions = 1
Platform.LogicalDisk.1.AssignedName = C
Platform.LogicalDisk.1.AvgQueueLen = 0
Platform.LogicalDisk.1.AvgQueueLen.Avg = 0
Platform.LogicalDisk.1.AvgQueueLen.Peak = 5.6
Platform.LogicalDisk.1.PctUtil = 0
Platform.LogicalDisk.1.PctUtil.Avg = 2.4
Platform.LogicalDisk.1.PctUtil.Peak = 100
Platform.LogicalDisk.2.AssignedName = D
Platform.LogicalDisk.2.AvgQueueLen = 0
Platform.LogicalDisk.2.AvgQueueLen.Avg = 0.1
Platform.LogicalDisk.2.AvgQueueLen.Peak = 14.2
Platform.LogicalDisk.2.PctUtil = 0.3
Platform.LogicalDisk.2.PctUtil.Avg = 5.5
Platform.LogicalDisk.2.PctUtil.Peak = 100
Platform.LogicalDisk.3.AssignedName = E
Platform.LogicalDisk.3.AvgQueueLen = 0
Platform.LogicalDisk.3.AvgQueueLen.Avg = 0
Platform.LogicalDisk.3.AvgQueueLen.Peak = 0.5
Platform.LogicalDisk.3.PctUtil = 0
Platform.LogicalDisk.3.PctUtil.Avg = 0.8
```

Figure B-5 Results from show stat platform. console command*

Domino statistics

As with platform statistics, you should only be focused at this stage on the key Domino components. In this section we highlight appropriate patterns that help you to determine if your server runs well without any impact from the upgrade.

In the following list, we identify items that we have think are the most useful and critical to monitor. The list is based on experiences IBM's internal Domino administrators have had over the years.

- Domino server availability
Monitor whether the server is up or down.

- Domino server tasks

Monitor whether the main tasks, such as replica, router, and adminP are running on the server. Be aware that a Domino task can fail without causing the Domino server to be fully down.

- Domino server connectivity

Are your users able to connect using Notes and Web browsers? Depending on the communication service that you have enabled on your server, you should test connectivity over several communication ports.

- Mail routing

Monitor the number of unsuccessful mail deliveries, and the number of dead mail items in your server-based mail.box. Mail routing is the core application for any organization, and any issues with mail routing latency have to be resolved as soon as possible.

- Replication events

It's essential, at the minimum, to ensure that Domino directory is replicated correctly throughout your Domino infrastructure (and thus remains consistent across your domain). Make sure that the Administration Requests database (Admin4.nsf) is replicated as well. Replication events can be checked in the log database (log.nsf) under the Replication Events view.

Tools for monitoring Domino

For a more detailed description of available tools, including those in Lotus Notes/Domino 6 to monitor your Domino environment, refer to Chapter 8, “Monitoring your infrastructure” on page 149.

Monitoring configuration and results databases

These two databases were known as “Statistics and Events” in previous Domino releases (events4.nsf and statrep.nsf), and though some changes have been introduced, the principles remain the same. This “out of the box” application is your main tool to monitor your Domino activities. You can configure, create and report information on all the Domino servers in your infrastructure

Attention: There are some differences between events.4.nsf (Configuration Monitoring) and statrep.nsf (Results Monitoring) in Lotus Domino 6 compared to Domino 5. The most obvious change is that the events.4.nsf, which in R5 was known as Statistics and Events, is now called Monitoring Configuration; while the statrep.nsf, which was known as Statistics Reports in R5, is now called Monitoring Results.

In R5, the default events are just called Events, while in Domino 6 they are referred to as Event Handlers. In R5, the result of an event was called an event notification, while in Domino 6, it is referred to as an Event Generator.

For additional information, please refer to Chapter 5 on this book.

By using this application, you will have the ability to use the monitoring options identified in Table B-2.

Table B-2 Available Event Generators in Domino 6

Event generator	Description
Database	Monitor ACL changes Monitor Replication Monitor unused space Monitor for user inactivity
Domino server	Check connectivity and port status in the network
TCP server	Verifies the availability of Internet ports (TCP services) on servers and generates statistics to measure time needed to get a response on the specified port
Mail routing	Sends a mail-trace message to a user's mail server and collect statistics indicating the amount of time it takes to deliver the trace
Statistic	Monitors a specific Domino or Platform statistic
Task status	Monitors the status of Domino server and add-in tasks

Domino log

The log databases on your Domino servers contain a huge amount of information providing you know where to look.

Depending on which view you select, it is possible to do the following:

- ▶ Check use and size of databases on your servers
- ▶ Ensure that replication occurs as expected

- Find out how many users are accessing the server and who they are
- Take a look at how much mail traffic is being generated
- Check for database corruption

Domino Server Log		Help					
	With Server	Date	Starting Time	Ending Time	Minutes	Average	Initiated By
<div>Miscellaneous Events</div> <div>Mail Routing Events</div> <div>Replication Events</div> <div>Newsgroups Events</div> <div>Passthru Connections</div> <div>Usage <div>by Date</div> <div>by User</div> <div>by Database</div> <div>by Size</div> <div>Object Store</div> </div> <div>Phone Calls <div>By Date</div> <div>By User</div> </div> <div>Log Analysis Results</div>	ITS010/Server/ITSO				0.0	0.0	
	11/11/2002				0.0	0.0	
	11/12/2002				0.0	0.0	
		12:31 AM EST	12:31 AM EST		0.0		ITS08/Server/ITSO
	11/13/2002				0.0	0.0	
		12:30 AM EST	12:30 AM EST		0.0		ITS08/Server/ITSO
	ITS011/Server/ITSO				18.4	6.1	
	11/11/2002				17.9	17.9	
	11/12/2002				0.3	0.3	
		12:31 AM EST	12:31 AM EST		0.3		ITS08/Server/ITSO
	11/13/2002				0.2	0.2	
		12:30 AM EST	12:31 AM EST		0.2		ITS08/Server/ITSO
					18.4	9.2	

Figure B-6 Domino server log

This database can be fully searching when you use the new extended log analazis tool from Domino Administrator 6 client, and results of your log searches are stored in the Domino log database for further references.

Domino Administrator 6 (server monitoring)

Lotus Domino Administrator 6 client provides a visual representation of the status and availability of selected Domino Servers, tasks, real-time system statistics, and status indicators.

This tool is very useful to provide a quick overview of infrastructure status and identifying tasks that may have failed.

The screenshot shows the 'Monitoring' tab of the Domino administration console. It displays a table of server status for three servers: ITS010, ITS011, and ITS08. The table includes columns for server name, status icons, and various performance metrics.

Hea	09:47:53 AM - 09:40:22 PM	Adm	Age	Dat	Eve	Ind	Rep	Rou	Sta	Use	Avai	ElapsedTime	PerMin	TotalRc	PotCombine	Context
ITS010/Server/ITS0									-	2	0	100	42 days 18:58:13	2	0	0
ITS011/Server/ITS0									-	2	0	100	50 days 21:09:27	2	0	1.9
ITS08/Server/ITS0										5	0	100	46 days 19:39:35	2	0	0.4

Figure B-7 Domino server monitoring

Troubleshooting

In this section we show you some simple things that you can do to make your troubleshooting easier. The section does not aim to list every possible problem scenario and appropriate solution.

Defining the problem

In all cases, you need to find out more information than simply “it is not working,” which is commonly the amount of information reported to you by end users. You need more details. The most simple task is to ask the user to explain to you what they were doing before the problem occurred, and if there is an error message. You need to get the error message since it will usually carry you far. Information about a problem often arrives from several sources; try combining all this information together.

User-reported problems

The important first step most people should take is to clearly define the problem. You need to ask the user to tell you everything about their problem and describe all the steps he followed to raise the problem. If appropriate, try to reproduce the problem to rule out the possibility it was a user error.

If it turns out that the user is doing something wrong, you can simply explain to him the recommended procedure. If you find out that the error is specific to the user’s machine, then you have to find out what is different between the workstations. If you find out that the problem is occurring on your machine and several others, then the problem is probably affecting most or all of the users and you need to look at the root cause.

Help desk support

Your help desk provides a single point of contact for inquiries, requests, and problem calls. Typically, the steps described earlier are done by the help desk team. In a hierarchical organization, you will usually not be dealing with the end users or customers directly to troubleshoot a problem.

You will be involved if the problem needs to be escalated to a second or third line of support; be certain to get a clear definition of the problem from the help desk

Administrator-reported problems

You might also need to use the same procedure (end-users/help desk) when receiving a call from another administrator.

Looking for the cause

Once you get a clear picture of what is happening, you can start tracking down the cause of the problem.

Looking for more information

Try to collect all the information that you can. Look at existing knowledge databases, support Web sites and the like, to find out if someone else has encountered the same problem and to ensure the problem has not been already fixed. Try to reproduce and document all steps for further reference and to narrow down the issue.

Process of elimination

When you have gotten all information, you can now start to use a phased determination approach. The best way to do this is to have a list that you can simply follow and strike out steps. This list should include both Domino and non-Domino items, such as:

- ▶ Network connection failure (network drivers error or corruption)
- ▶ System hardware error
- ▶ Domino configuration problems (a change has been made recently)
- ▶ Physical connection between client and server

Table B-3 on page 542 identifies some exemplary scenarios where your server is not responding. This is reported by your end users, as they cannot connect to the server. You will have to determine in which state your server really is.

Table B-3 Domino Server error states

Server state	Description/symptom
Server crash	Domino server is no longer running; message at the server console, for example: "Freezing all server threads" or "Panic: Lookup handle" Operating System is still responsive and active Server is not responding to client request
Server hang	No keyboard input is allowed at the server console level Server is not responding to client request No freezing or panic message Domino processes seem to be running
Server performance issue	Slow answer from client request No freezing or panic message Some Domino threads are serving client request Domino processes are still active
Individual task crashes	Individual task is no longer responding and/or cannot be stopped /restarted (router, http, replica) Server remains up and running Client requests are serving if they don't use crashed task
OS-related problem	Operating System is not responding (no keyboard input is accepted) Root cause is not initiated by Domino and you should let the operating system administrator determine the cause and the resolution of the problem

After determining the state of your server, you can start going through the checklist you have for that specific server state, for further problem determination and to find the solution for the problem.

Finding possible solutions

Once you have determined what the problem is, you now have to find a solution.

If your problem is not Domino-related, you should use the proper support channels:

- ▶ Network team if the problem is related to a network issue, configuration, physical path.
- ▶ System administrators for any inquiries about operating systems.
- ▶ Helpdesk team if your problem is more user-related.

If it appears that the problem is a Domino-related issue, you might know the solution right away; if not, consult:

- ▶ Internal knowledge databases (as discussed in the previous section)
- ▶ Other Domino administrators in your organization
- ▶ Outside help from Web sites, discussion groups, books
- ▶ Open an incident with the IBM Lotus Support organization

Implementing the solution

If you find a solution that has never been used before in your organization, you will have to test it before you implement it. You don't want to cause new problems by applying a solution to the problem you are having.

If a server change is required, you need to be careful when implementing the solution. All changes to production servers should be implemented carefully and be fully tested on a test environment to make sure the change does not affect any other aspect of your infrastructure. You should schedule any changes during non-business hours, and treat any change made to your environment with the same seriousness as the upgrade process itself.

If many solutions are possible, you should test each of them to evaluate the most appropriate, weighing pros and cons of each solution.

After solving the problem, do not forget to document which solution you have applied to fix your problem in your internal knowledge database. If the problem reappears somewhere, it can be quickly fixed.

Tools and utilities to monitor your infrastructure

There are a number of tools and utilities you can use to monitor and troubleshoot your infrastructure. These tools and utilities can help you to determine the source of any problems, find the root cause, and fix the problem. Among the available tools are the following:

Domino databases

- ▶ Domino log (log.nsf)
- ▶ Administration request (Admin4.nsf)
- ▶ Monitoring Configuration (events4.nsf) and Monitoring Results (Statrep.nsf)
- ▶ Mail router mail.box (mail.box)
- ▶ Certification log (certlog.nsf)
- ▶ Catalog (catalog.nsf)

- ▶ Domino directory (names.nsf)
- ▶ Domino Mail tracking Store (mtstore.nsf) works with MTC task and reports.nsf
- ▶ Domino Web Server Configuration (domcfg.nsf)
- ▶ Domino Web Administration (Webadmin.nsf)
- ▶ Notes Log Analysis (log4.nsf)
- ▶ Cluster Analysis (clusta4.nsf)
- ▶ Agent Log (alog4.nsf)

For more details on using some of these databases, refer to Chapter 8, “Monitoring your infrastructure” on page 149.

Domino utilities

- ▶ NSD (Notes System Diagnostic)
- ▶ Memcheck
- ▶ Notes.ini debug variables
- ▶ Lotus Notes Trace connection (File -> Preferences -> User Preferences -> Ports)
- ▶ NotesPeek
- ▶ Domino Administrator Client 6
- ▶ Server Console commands

Attention: NSD and memcheck are now bundled with the core Lotus Domino 6 product. NSD is now the default debugger. For a more detailed description refer to the redbook *Domino 6 for Linux*, SG-24-6835.

Operating system logs

Each operating system has a set of logs that track down the OS activity, for example Event Viewer for a Win32 platform, or Syslog on a UNIX platform.

For a detailed description of Operating System logs, see the documentation for that specific operating system.

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 on ordering these publications, see “How to get IBM Redbooks” on page 546.

- ▶ *Lotus Domino 6 for Linux*, SG24-6835
- ▶ *Lotus Domino Designer 6: A Developer's Handbook*, SG24-6854
- ▶ *Active Directory Synchronization with Lotus ADSync*, REDP0605
- ▶ *Lotus Notes and Domino Take Center Stage: Upgrading from R4 to R5*, SG24-5630
- ▶ *Domino and WebSphere Together Second Edition*, SG24-5955
- ▶ *iNotes Web Access Deployment and Administration*, SG24-6518
- ▶ *Applying the Patterns for e-business to Domino and WebSphere Scenarios*, SG24-6255
- ▶ *Lotus Domino R5 for Sun Solaris 8*, SG24-5969

Referenced Web sites

These Web sites are also relevant as further information sources:

- ▶ Lotus Developer Domain

<http://www.lotus.com/1dd>

Refer to the following articles for related information:

“Decoding the new Notes/Domino 6 agent features” by Julie Kadashevich

“Notes 6 Technical Overview” by

“Domino 6 technical Overview” by

“Policy-based system administration with Domino 6” by Bob Balfe

“Domino 6 performance features” by Razeyah Stephen

“Network compression in Domino 6” by Mike Gazda and Dick McCarrick

“Be the authority on the Domino 6 Certificate Authority” by Amy E. Smith, ShiuFun Poon and John Wray

“Start using Domino 6 Server Health Monitoring now!” by Carol Zimmet

“Early adoption of Notes/Domino 6 at IBM” James Grigsby and Cynthia Mamacos interviewed by Tara Hall

- ▶ Wolcott, Application Deployment Toolkit

<http://www.wolcottgroup.com>

- ▶ Internet Engineering Task Force (IETF)

<http://www.ietf.org>

- ▶ InstallShield

<http://www.installshield.com>

How to get IBM Redbooks

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

ibm.com/redbooks

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

IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the CD-ROMs button on the Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.

Index

Symbols

\$ServerAccess view 68
\$Users view 68
.IND file 107

Numerics

3rd party deployment tools 28
3rd party products 35

A

Access remote servers 318
Accessing locked databases 310
Accessing public databases with IMAP 295
ACL files 428
Activity logging 198
 enabling 198
Activity logging for IMAP sessions 298
Activity trends 48
Administering ECLs 323
Administration delegation possibilities 48
Administration levels 51
 Administer the server from a browser 50
 Administrators 49
 Database Administrators 49
 Full Access Administrator 49
 Full access administrators 306
 Full Remote Console Administrators 50
 Restricted System Administrator 50
 System Administrator 50
 View-Only Administrator 50
Administration Requests database 65
Administrators 304
 defined 306
AdminP 81
Allowing more fields 52
Allowing more fields in a database 34
Allowing relaying 236
Anti-spam features 210, 229, 238, 240–241
Anti-virus software 35
Application Hosting Provider 407
Applications
 listing functionality 24

 testing 24
 upgrading 24
Applying a Policy 458
Archiving settings document 255
 configuring 255
 specifying options 257
ASP 90
Assigning Explicit Policies to users 459
Authentication Realm 386
Automatic archiving 209
Automatic forwarding 227
 disabling 229
Automatic logout 333
Automatic mail archiving 245
Automatic restart 51
Automatic upgrade of clients 141

B

Backup 79
Backup software 35
Bitmap optimization 54

C

CA

 activating the certifier 371
 adherence to PKIX standards 358
 administration tasks 375
 advantages of using the process 360
 concepts 358
 console commands 370
 creating a user or a server 372
 deactivating the certifier 371
 described 358
 disabling certifiers 378
 ending the process 371
 for Notes IDs 360
 issued certificate list 358
 loading the process 366
 locking certifiers 371
 locking the certifier ID 369
 migrating existing Notes certifiers 361
 modifying the certifier ID 375
 Notes certifier 368

- process 360
- re-enabling certifiers 378
- refreshing the process 369
- registration authority 360
- setting up 360
- starting the process 371
- statistics 371
- unlocking the certifier 371
- unlocking the certifier ID 369
- Calculate database size by usage instead of file size 226
- Calendaring and scheduling 19
- Calendaring and scheduling features 6
- Cascading Domino Directories 61
- Centralization 30
- Certificate Authority
 - See CA
- Certificate revocation list 359
- Check OS 94
- Client
 - administering 469
 - administrative assistant 120
 - administrative rights 119
 - archiving 245
 - automatic logout 333
 - backup 121
 - calendaring and scheduling 6
 - changes compared to R5 134
 - components to install 125
 - determining client versions 119
 - documentation 146
 - dynamic configuration 26, 120
 - ECL 26
 - files to backup 121
 - help 146
 - improvements 4
 - installation options 122
 - installation path 124
 - installation steps 123–127
 - installing 122, 470
 - interoperability 19
 - inventory 119
 - licensing 8
 - manageability 4
 - manual upgrade 28
 - maximum level allowed 45
 - minimum level allowed 45
 - mixed versions 19
 - multi-user workstations 472
 - planning for the upgrade 119
 - policies 451, 493
 - preparing for installation 121
 - requesting certificate renewal 507
 - requirements 18
 - rolling back 135
 - security 333
 - shared network installation 470
 - silent installation 122
 - Smart upgrade 27, 484
 - smart upgrade 145
 - smartcards 513
 - specifying which versions to upgrade 132
 - standard files 145
 - standard templates 145
 - system requirements 118, 121
 - tracking versions 521
 - training 121
 - transform files 476
 - types 122
 - upgrade by mail 26, 130
 - upgrade options 26
 - upgrading automatically 141
 - upgrading post Notes 6.0 clients 145
 - upgrading strategy 120
 - usability 4
 - user interface changes 18
 - using older applications 24
 - versions 521
 - welcome page 26, 127
- Client-based archiving 452
- Clients 17
 - upgrading before servers 19
- Client-side archiving 245–246
 - enabling 252
 - scheduling 253
 - setting up 246
 - specifying criteria 249
- Clusters, mixed release 23
- Coexistence 34
- commands
 - ca concole commands 370
 - compact 78, 105, 107, 114
 - design 104
 - drop all 83
 - fixup 104
 - load ca 366
 - load convert 137
 - load imap 283

- restart task imap 284
- set conf server_restricted 83, 112
- tell adminp process all 81, 367
- tell ca refresh 369
- tell ca status 370
- tell ca unlock 369
- tell http refresh 391
- tell ldap quit 112
- tell router quit 137
- tell router update config 220
- upcall 106, 108
- Communication
 - informing users 18
- compact 52, 68, 72, 78, 105, 267
 - described 106
- Compacting
 - copy-style 106
 - in-place style 106
- Compare Notes Public Keys 314
- Condensed Directory Catalog 61
- Configuration document 44, 304
 - activity logging 47
 - activity trends 48
 - areas 44
 - basics table 45
 - creating 304
 - differences compared to R5 45
 - failure messages 46
 - IMAP settings 285
 - iNotes Web Access settings 44
 - license tracking 45
 - mail journaling 46
 - maximum client level 45
 - minimum client level 45
 - new features 45
 - router settings 44
 - Smart upgrade 45
 - SMTP settings 229
- Configuration Domino Directory 39
- Configuration Monitoring database 156
- Configuring automatic logout 334
- Configuring mail files for IMAP access 277
- Configuring the Domino server to work with Microsoft IIS 401
- Configuring the WebSphere plugin 400
- Configuring Upgrade by Mail 130
- Connection documents 79
- Considerations
 - calendar and scheduling 19

- server upgrade 29
- upgrade sequence 31
- Consolidation 30
 - benefits 524
 - considerations 528
 - Domino 6 526
 - easier administration 524
- Controlling access 54
- Controlling automatic forwarding 227
- Controlling spam 46
- Converting ODS 114
- Corporate welcome pages 494
- Creating 457
- Creating a policy document 457
- Creating a program document 268
- Creating settings documents 456
- Customized templates 103
- Customizing client installations 476
- Customizing mail templates 23

D

- Database
 - advanced properties 52
 - allowing more fields 34, 52, 59
 - bitmap optimization 54
 - creating master templates 41
 - creating templates 41
 - customizing 23
 - disabling inheritance 56
 - ODS 20
 - preventing design to replicate 21
 - quota 21
 - replacing design 64, 140
 - single copy template 33
 - unread marks 54
 - using with newer client 24
- Database administrators 306
 - defined 306
- Defining network timeouts 343
- Delegating administration 432
- Delegating administration privileges 48
- Delegating privileges to the calendar 19
- Delegation 120
- Deleting a full-text index 82
- Deleting busytime.nsf 109
- Deleting unused program documents 77
- Denial of Service (DoS) attack 342
- Denying access to server 315

- Denying automatic forwarding 227
 - Design task 104
 - Desktop settings document 141
 - configuring automatic logout 334
 - setting Notes browser security 337
 - Determining client versions 119
 - Directory
 - \$Server access view 68
 - \$Users view 68
 - access control 55
 - backup 79
 - backward compatibility 34
 - Cascading Domino Directories 61
 - changes 38
 - commands to run after the Directory upgrade 67
 - configuration document 44
 - connection documents 79
 - consistent ACL across all replicas 55
 - defining primary 39
 - deploying custom templates 59
 - disabling inheritance 56
 - disabling replication 59
 - distributing changes 54
 - ECL 26
 - fault recovery 39
 - fixup 105
 - for multiple organizations 409
 - new design 38
 - new features 38
 - preventing spam 230
 - program documents 77–78
 - re-enabling replication 113
 - replacing design 64
 - replication 54
 - retaining old design 59
 - secondary 60
 - server document 39
 - tasks 37
 - template name 58
 - type 39
 - upgrade 37
 - upgrade considerations 33
 - upgrade steps 64–66
 - upgrading 33
 - upgrading before servers 64, 66
 - upgrading the design 63
 - upgrading together with the server 65
 - user interface 38
 - using a custom design template 56
 - using customized 34
 - using with Lotus companion products 35
 - version 6 38
 - virtualized 410
 - xACL 445
 - Directory Assistance 61–62
 - Disable design replication 22
 - Disabling inheritance 56
 - Disabling program documents 77
 - Disabling server tasks 78
 - Disabling the full access administrator feature 310
 - DNS Blacklist
 - configuring 243
 - exempting hosts 245
 - specifying sites 243
 - statistics 245
 - DNS Blacklist filters 242
 - DNS Blacklists 209
 - Domino 6 Internet Site Architecture. 387
 - Domino 6 Web Administrator client 308
 - Domino Directory 33, 37
 - Domino Enterprise Server 8
 - Domino hosting features 407
 - Domino Log 538
 - Domino Messaging Server 8
 - Domino server
 - Policy based administration 18
 - Domino server statistics 536
 - Domino Utility Server 8
 - Dynamic client configuration 120
- ## E
- e 424
 - ECL 26, 323
 - admin ECL 326
 - administering 323
 - certifier 324
 - distributing with policies 323
 - execution security alert 327
 - guidelines 324
 - locking from users 323
 - locking user out of ECLs 327
 - on a workstation 330
 - preconfigured entries 323
 - preventing use of unsigned content 324
 - trusted signers 323
 - unsigned content 324

- Enabling full access administrator mode 311
- Enabling the xSP configuration 409
- entirely 19
- Error messages 196
- Event task 180
- Events 150
- events4.nsf 150
- Exception policies 453
- Execution Control List
 - See ECL
- Explicit policy 452
- Extended Access Control List
 - See xACL
- Extended ACL
 - See xACL
- Extended Administration Server 444
- Extended administration server
 - removing 445
 - setting up 445
- Extended Directory Catalog 60
- External redirection 394

F

- Failure messages 46
- Fault recovery 39, 51
 - defining cleanup script 51
 - disabling 51
 - enabling 39, 51
 - limiting script execution 51
 - restarting 51
 - setting execution time limit 39
 - setting up 51
 - settings 39
 - specifying cleanup script 39
- Fax software 35
- File protection document 386
- fixup 104
 - described 105
- Forcing encryption of local replicas 335
- Full access administrator
 - where to use 310
- Full Access Administrator mode
 - enabling 311
- Full access administrators 305
 - access to encrypted information 306
 - defined 306
 - disabling 310
- full access administrators

- privileges 306
- Full Access Administrators 48
- Full remote console administrators 307
 - defined 307
- Full-text engine 105, 108–109
- Full-text index 81
- Full-text search engine 61

G

- GTR engine 61

H

- Hardware 30
- Hosted organizations 408
- HTTP response header rule 395
- HTTP security model 340

I

- IBM HTTP Server 397
- IBM Tivoli Analyzer for Lotus Domino 48
- IBM WebSphere Application Server 397
- IIS 398
- IMAP 209, 276
 - access to public databases 295
 - activity logging 298
 - automatic conversion of mail files 278
 - configuration 282
 - configuration document 278
 - configuring 286
 - configuring activity logging 298
 - configuring mail files 277
 - conversion of R4 mail files 281
 - convert utility 281
 - improvements 276
 - manual conversion of mail files 279
 - namespace 287, 291
 - namespace extension marks 276
 - native support 276
 - port configuration 284
 - server configuration 283
 - service configuration 285
 - sharing mail files 292
 - starting the IMAP service 283
 - stopping the service 283
 - unread marks 276
- IMAP database items 277
- Inbound connection controls 238

- Inbound intended recipients controls 241
 - Inbound relay controls 231
 - destination restrictions 232
 - managing conflicts 234
 - source restrictions 233
 - Inbound relay enforcement 236
 - Inbound sender controls 240
 - Information about error messages 196
 - Informing users 18
 - iNotes Web Access 44, 351
 - changing passwords 352
 - password change tool 351
 - preferences 351
 - Installing Domino
 - coexistence of mixed versions 91
 - installation steps 91
 - multiple installations 91
 - partitioning a Domino server 92
 - running multiple instances 92
 - Installing Notes 6 for a multi-user workstation 473
 - Installing the WebSphere plug-in 399
 - InstallShield Tuner
 - creating the transform file 477
 - data directory 481
 - described 477
 - determining files to install 479
 - modifying the transform file 478
 - preparing to package 481
 - program directory 481
 - registry changes 480
 - saving the transform file 483
 - setup 477
 - silent install 481
 - using 477
 - InstallShield Tuner for Lotus Notes 476
 - Internal redirection 394
 - Internet Site architecture 385
 - Internet Site documents
 - WebDAV 403
 - Internet site documents 387
 - changing ports 394
 - changing protocols 394
 - configuration 387
 - configuring protocols 387
 - creating 388
 - deleting 391
 - difference from R5 386
 - Directory Rules 393
 - enabling 390
 - fields for a Web site document 389
 - Global Web Settings document 392
 - HTTP 387
 - IIOIP 388
 - IMAP 387
 - IMAP service 284
 - language differentiation 396
 - LDAP 387
 - modifying 391
 - organization 389
 - POP3 387
 - Redirection Rules 393
 - session-based authentication 404
 - Single sign-on 405
 - SMTP 387
 - substitution rules 395
 - upgrading steps 406
 - upgrading to 405
 - Web site rule document 392
 - Interoperability 9, 19, 21, 24
 - Administrator client 14
 - applications 34
 - client/mail template 10
 - clients 13
 - Lotus companion products 35
 - ODS versions 13
 - sorting 13
 - TeamRoom 14
 - templates 14
 - types 9
 - unread marks 13
 - interoperability 34
 - IP filtering 344
 - ISpy task 168
 - Issued certificate list 358
- ## J
- Java
 - execution rights 318
 - Java applet security 325
 - JavaScript security 325
- ## L
- LDAP 81, 112
 - LDAP Schema changes 62
 - Levels of Administrator access to servers 304
 - License Tracking 517
 - enabling 517

- viewing information 519
- License tracking 119
- License types 30
- Licensing 8
- load convert 137
- Loading the CA process 366
- Locking user out of ECLs 327
- Log 538
- Log analysis
 - creating a search 181
 - options 183
 - saving a search 186
 - specifying details 183
- Log analysis tool 180
- Log filters 193
- Log search 180
- Log.nsf 109
- Logging 47, 109
- Logout 333
- LZ1 33

M

- Macintosh 118
- Mail
 - file size 18
 - rules 46
 - shared 43
- Mail and calendaring delegation 120
- Mail file
 - convert utility 137
 - IMAP 277
 - replacing design 140
 - upgrading manually 139
- Mail files 21
 - clustered 23
 - customized 23
 - interoperability 21
 - non-clustered 21
 - Seamless mail upgrade 23
 - using shared 43
- Mail journaling 46, 209, 218
 - configuration 220
 - configuring 219
 - described 218
 - local 219
 - remote 220
 - types 218
 - why to use 218

- Mail rules 46, 210
- maintain 54
- Maintaining unread marks 54
- Making a backup 79
- Making a server unavailable 83
- Making use of policies 493
- Managing database quotas 223
- Managing system rules 216
- Manual upgrade 139
- Maximum number of request headers 346
- Maximum number of URL path segments 346
- Maximum size of request content 347
- Maximum size of request headers 346
- Maximum URL length 346
- Memcheck 544
- Microsoft SMS 28
- Migrating certifier 361
- Mixed versions 34
- Mobile Directory Catalog 61
- Monitoring 150, 532
 - built-in events 173
 - creating a Event generator for sever 163
 - creating an Event Handler 174
 - database events 159
 - Event generator 150, 156
 - event generators 538
 - Event Handler 172
 - event handling 154
 - events 150
 - ISpy task 168
 - log 538
 - Mail Routing Event Generator 168
 - Monitoring Configuration database 537
 - replication 160
 - Results database 537
 - server 163
 - setup wizard 158
 - severity levels 174
 - TCP Server Event Generator 164
- Monitoring Configuration database 150
- Monitoring configuration database 150
- Monitoring Results database 150
- Monitoring results database 150
- msiexec command 122
- Multiple organization Domino Directory 409
- Multi-user workstations 472

N

- netCreator role 304
- netModifier role 304
- Network timeout settings 342
- New Domino Directory design 38
- New features in Domino 6 3
- New features in Notes 6 4
- NNTP 85
- Non-delivery report 216
- Notes browser security 337
- Notes Named Network 79
- Notes.ini 51, 61, 63, 78–79, 84–85, 122, 304, 310
- NSD 544

O

- ODS 33, 68, 107, 114, 226
 - checking 68
 - checking for the version 21
 - checking using server console 70
 - database design 73
 - defined 68
 - levels 71
 - mix of versions 72
 - mixed versions 21
 - replication 72
 - retaining older version 72
 - scenarios 73
 - upgrade 33
 - upgrading 71
 - versions 20
- Once 351
- Open relay 229
- Organizational policy 452

P

- Personal address book 128
 - allowing LDAP queries 129
 - owner 129
 - preferences 128
 - profile 128
 - sorting 129
 - template 145
- PKIX 357
- Planning 17
- Platform statistics 534
- Platform_Statistics_Disabled 532
- Policies 25, 141
 - administration 453

- applying 458, 503
- archiving 451
- assigning to users 459
- compared to setup profiles 453
- creating 144, 451, 455–456
- deleting 455, 459
- described 449–450
- desktop 451
- documents 450, 456
- dynamic 493
- ECL 323
- example 503
- examples 454, 464
- exceptions 453
- execution 451
- explicit 452
- for hosted organization 463
- hierarchical relations 453
- in Domino Administrator 454
- Inheritance 453
- installation time 493
- managing Internet passwords 348
- organizational 452
- planning 462
- policy settings documents 458
- registration 451
- seamless mail upgrade 144, 451
- security 451
- server-side archiving 255
- settings documents 456
- setup 451, 493
- Smart Upgrade 489
- synopsis 460
- types 452
- use of exception policies 459
- using for administering ECLs 323
- welcome page deployment 451
- welcome pages 494
- Policy based administration 18, 25, 449
 - converting user profiles to policies 25
 - desktop setting documents 23
 - registration settings documents 25
- Preventing automatic forwarding 209
- Preventing design to replicate 21
- Primary Domino Directory 39
- Public Key Infrastructure 357
- Purging administration requests 81
- Pushing ECL changes to users 323
- Pushing information to users 26

Q

- QuickPlace 59
- Quickplace 35
- Quota enforcement 43
- Quota management 209, 223
 - configuring 223
 - mail databases 224
 - notifying the user 224
 - over quota enforcement 225
 - overriding 225
 - size by file size 226
 - size by usage 226
 - transactional logging 226
 - threshold 224

R

- r 150
- R4 19, 34, 135
- R5 19, 34, 84, 135, 305
- Realm 386
- Redbooks Web site 546
 - Contact us xvi
- Refreshing design 56
- Registering users 372
- Registration Authority
 - described 359
- Registration authority 359
- Registration settings documents 25
- Rejecting email from spoofed sender addresses 229
- Rejecting relaying 229
- Relaying spam, disabling 229
- Releasing unused storage 106
- Remote agents 41
- Remote debug manager 41
 - configuration menu 42
 - enabling 41
 - setting up 41
- Removing obsolete settings 84
- Renewing certificates 507, 511
- Replication 79
- Request renewal of a Notes certificate 507
- Responding to certificate renewal requests 511
- Restricted 50
- Reverse proxy server 398
- Roll-back 135
- Router 137, 210
- Routing mail 83

- Rule document 386
- Rules 210
 - forwarding messages automatically 228
- Run restricted methods 318
- Run unrestricted methods 318
- Running compact on subdirectories 107
- Running unrestricted agents 321

S

- S/MIME 358
- S/MIME mail 505
- Sametime 35, 59
- SCOS 273
 - guidelines 276
 - setting up 274
- Seamless mail upgrade 23, 141
 - client versions 142
 - defining a policy 23
 - described 141
 - Domino 6 141
 - mail template 143
 - notifying the server after the upgrade 144
 - pre upgrade steps 23
 - prompting the user 142
 - setting up 142
 - user notification 142
- Searching 109
- Secondary directories 60
- Secure email 358
- SECURE_DISABLE_FULLADMIN 310
- Securing data on the workstation 323
- Security 303
 - access control 54
 - access remote servers 318
 - ACL 54
 - ACL files 428
 - administrators 304
 - agent execution rights 319
 - agents 40
 - authentication 347
 - authorization 354
 - bypassing security 310
 - Certificate Authority 363
 - changes in Domino 6 304
 - Compare Notes Public Keys 314
 - configuration 304
 - controlling access to server 315
 - controlling code execution on the workstation

- 323
- correcting erratic ACLs 310
- create replicas 316
- creating databases 316
- creating secure ECLs 324
- denying access 315
- ECL 26
- execution rights 319
- fewer name variations with higher security 347
- forcing encryption of local replicas 335
- Full Access Administrators 48
- HTTP connection level 342
- iNotes Web Access 352
- Internet access 322
- locking ECLs 323
- locking user out of ECLs 327
- logout 334
- managing full access administrator feature 311
- managing Internet passwords 348
- network settings 343
- Network timeout settings 342
- passthru use 322
- password quality 354
- protecting at the validation level 346
- remote agents 41
- requiring use of SSL 356
- run restricted LotusScript/Java agents 322
- run restricted methods 318
- run simple and formula agents 322
- run unrestricted methods 318
- server security configuration 304
- settings 313
- sign agents to run on behalf of someone else 321
- sign agents to run on behalf of the invoker of the agent 322
- signing agents on behalf of someone else 40
- trusted servers 41, 317
- using monitors 317
- Web 340
- Web server security 340
- workstation 323
- xACL 436
- Security settings 313
- Security settings document 325
 - ECL 325
- Server
 - activity logging 47
 - administration delegation 48

- administration requests 81
- archiving 245
- backup 79
- before restarting 109
- CA process 358
- capacity planning 30
- configuring IMAP 283
- connection documents 79
- controlling access 315
- deleting indexes 81
- denying access 315
- disabling tasks 78
- Domino Application Server 8
- Domino Enterprise Advanced Server 8
- Domino Enterprise Server 8
- Domino Extranet Server 8
- Domino Mail server 8
- Domino Messaging server 8
- Domino Utility Server 8
- error messages 196
- error states 542
- fault recovery 51
- implementing new features 32
- improvements 3
- installing on UNIX 86–88, 90–94
- installing on Win32 95–102
- installing on Windows 95
- licensing 30
- lisensing 8
- log 47
- making unavailable 83
- multiple installations 91
- multiple Web sites 386
- partitioned 92
- performance 30
- post-upgrade tasks 103, 112
- quota management 21
- recommended version 32
- recovering from a crash 51
- routing mail 83
- security 304
- server tasks 42
- starting after the upgrade 112
- statistics 48
- stopping 85
- third party products 35
- tools for monitoring 537
- upgrade 75
- upgrading code 85

- upgrading the directory at the same time 65
- upgrading the Directory first 64
- using different mail file versions 21
- using external HTTP server 397
- using IIS server 398
- using with IBM HTTP Server 402
- Web security 340
- Server document 39
 - administrators 40, 48
 - basic table 39
 - Configuration Domino Directory 39
 - directory type 39
 - enabling Internet site documents 390
 - fault recovery 39
 - Full Access Administrators 40
 - IMAP 283
 - keyring 386
 - mail rules 211
 - master templates 41
 - Ports table 41
 - Primary Domino Directory 39
 - programmability restrictions 40
 - quota enforcement 43
 - security 308
 - security tab 48
 - server settings 313
 - server tasks table 42
 - template creation rights 41
 - transactional logging 43
 - Trusted servers 41
 - Web site settings 386
- Server mail rules 46
- Server tasks 42
- server_restricted command 83
- Server-based archiving 451
- Server-side archiving 245, 255
 - by using compact 267
 - by using Domino Administrator 270
 - logging 266
 - setting up 255
 - specifying criteria 259
 - specifying destination 259
 - statistics 265
- Session-based filter 189
- set conf server_restricted 83
- Setting quota 43
- Setting up Domino to work with IBM HTTP Servers 402
- Setting up the xACL 436
- Setup profiles 453
- SetupLeaveServerTasks 78
- Shared mail 43, 273
 - using multiple databases 43
- show directory command 70
- Shutting down router 137
- Signing agent on behalf of someone else 318
- Signing agents on behalf of someone else 40
- Silent Install 484
- Single copy object store 43, 209, 273
- Smart Upgrade
 - configuration 485
 - setting a grace period 489
 - user notification 493
 - using policies 489
- Smart upgrade 27, 45, 145, 484
- Smart Upgrade database 489
- Smartcards 513
 - enabling 514
 - on Notes 6 514
 - troubleshooting 515
- SMTP inbound controls 231
- SMTP relay controls 209
- Spam 46, 229, 238, 240
- Spam prevention 210
- Spoofing 229
- Standard templates and files installed on the client 145
- Statistic Reports database 150
- Statistics 48, 532
 - CPU utilization 535
 - disk capacity 535
 - disk I/O activity 535
 - Domino 536
 - in Domino Administrator client 534
 - memory utilization 535
 - operating system 532
- Statistics & Events database 150
- statrep.nsf 150
- Stopping the server 85
- System administrators 307
 - defined 307
- System mail rules 46, 209–210
 - conditions 214
 - configuring 210
 - creating 212
 - defining actions 214
 - denying message 215
 - journaling the message 215

- managing 216
- moving a message to a database 215
- non-delivery report 216
- quarantining 215
- refusing delivery 216
- setting conditions 212
- System requirements 18, 118, 121
- server 30

T

- Task Status Monitor 170
- tell adminp process all command 81
- Templates 66, 103
- Third-party HTTP server integration 397
- Tivoli Analyzer for Lotus Domino 48
- Tools for monitoring Domino server 537
- Training 18
- Transactional logging 110
 - circular 43
 - linear 43
 - setting maximum size 43
- Transform files 476
- Troubleshooting 135, 540
 - defining the problem 540
 - determining the cause 541
 - implementing the solution 543
 - tools 543
- Trusted servers 41
- trusted servers 317

U

UNIX

- ASP 90
- Check OS 94
- compact 105, 114
- data directories 92
- directory for binaries 91
- fixup 104
- group 93
- installing code 94
- installing data directories only 89
- installing templates 90
- multiple installations 91
- notes user 93
- partitioned server 92
- patches 94
- reviewing configuration 94
- server type 89

- standalone Domino server 86
- upcall 106
- upgrade steps 86
- upgrading server code 86
- user 93

Unix

- server installation 86–88, 90–94
- UNK table 34, 52

- upcall 61, 68, 106
 - described 107

Upgrade by mail

- configuring 130–131
- described 130
- e-mail notification 130
- instructions 130
- mail template 133
- pre-requisites 130
- sending upgrade notifications 131
- specifying client versions 132
- specifying installation kit location 133

Upgrade checklist 80–81

Upgrade sequence 31, 77

Upgradin

- servers before clients 77

Upgrading

- a multi-user installation 475
- Administration Requests database 65
- administration server 104
- anti-virus software 35
- applications 114, 120
- backup software 35
- benefits 2
- busytime.nsf 109
- by mail 26
- checklist 80
- client upgrade options 26
- clients automatically 141
- clients before server 19
- Condensed Directory Catalog 61
- considerations 7, 17
- customized templates 103
- diagram 76
- Directory 64
- directory 33, 37, 65
- Domino LDAP Schema 62
- Extended Directory Catalog 60
- Fax software 35
- interoperability 120
- LDAP 81

- log.nsf 109
- manually 28, 139
- new features 2
- ODS 33, 114
- ODS levels 107
- plan 76
- preceding tasks 80
- recommended sequence 31
- Seamless mail upgrade 23
- seamless mail upgrade 141
- sequence 77
- server 75
- server code 85
- servers 29
- Smart upgrade 27
- steps 76
- TCO 2
- templates applied during server upgrade 66
- to Internet site architecture 405
- transactional logging 110
- upgrading clients by mail 130
- view indexes 108
- with 3rd party tools 28
- Upgrading full-text indexes 108
- Upgrading clients 17
- URL Mapping 386
- Usability 38
- User interface changes 38
- User profiles 25
- User registration 372
- User security 330
- Using another HTTP server 397
- Using compact to archive documents 267

V

- Versions used 521
- View-only administrators 307
 - defined 307
- Virtual hosts 386
- Virtual servers 386

W

- Web Administrator 50, 306
- Web security 340
- WebDAV 403
- Welcome page
 - \$CurrentLayout= 497
 - ACL 497

- applying with a policy 503
 - configuration 496
 - configuring 499
 - creating 494, 499
 - desktop settings document 502
 - sort order 501
- Welcome page administration 26
- Welcome pages 494
- Win32
 - client 118
 - compact 105, 114
 - fixup 104
 - installation directory 99
 - installation steps 95
 - re-enabling the service 112
 - removing service 95
 - selecting components to install 100
 - server installation 95–102
 - server type 98
 - upcall 106
- Windows installer 476
- Workstation requirements 18
- Workstation security 26, 323, 325, 329

X

- X.509 certificates 358
- xACL 410, 431
 - administering 433
 - administration server 444
 - benefits 432
 - considerations 432
 - delegating administration 432
 - described 432
 - disabling 443
 - enabling 432, 434
 - implementation considerations 446
 - planning 432
 - presedence 446
 - setting up 436
- xSP Domino
 - ACL files 428
 - activity logging 426
 - additional security 428
 - billing 412
 - binding IP addresses 423
 - Creating Loopback addresses 424
 - differences to Domino 409
 - Directory 409

- extended ACL 428
- Global Web settings documents 425
- hiding applications from other organizations 409
- hiding users from another organization 409
- installing the server 415
- Internet site documents 425
- planning 411
- policy documents 422
- protocol support 411
- registering hosted organizations 413
- scalability 411
- setting up 415
- setting up Certificate Authority 421
- xACL 428
- xSP model 407
 - addressing models 408
 - dedicated IP addresses 408
 - shared IP addresses 408

Y

- you 51

Z

- ZenWorks 28



Redbooks

Upgrading to Lotus Notes and Domino 6

(1.0" spine)
0.875" <-> 1.498"
460 <-> 788 pages



Upgrading to Lotus Notes and Domino 6



Redbooks

New features of Notes and Domino 6 described

Details about upgrading servers, clients, and directory

Administering the new environment

In this IBM Redbook, we show how to upgrade existing Lotus Notes and Domino installations to IBM Lotus Notes and Domino version 6. The chapters have been structured as a series of logical steps that you can follow when upgrading your environment.

First, we introduce the new features of Lotus Notes and Domino 6, and discuss overall upgrading considerations, coexistence issues, and interoperability. Next, we examine upgrading considerations specifically related to clients and servers. Then we guide readers through the actual steps needed to upgrade the Domino Directory, the Domino Server, and Lotus Notes Clients.

New functionality of the Domino 6 environment is presented, along with topics related to administering the new environment, including server monitoring, messaging, security, administering clients, policy-based administration, and more. Information on troubleshooting is also provided.

This redbook is written for Domino R5 administrators who need to upgrade to Notes and Domino 6. Working knowledge of Domino infrastructures and Domino servers is assumed.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks