



F r o m T e c h n o l o g i e s t o S o l u t i o n s

Upgrading to Lotus Notes and Domino 7

A comprehensive guide to moving to the latest version
of this established collaboration platform

Tim Speed
Dick McCarrick

Tara Hall
Barry Heinz

Matthew Henry
Wendi Pohs

PACKT
PUBLISHING

www.allitebooks.com

Upgrading to Lotus Notes and Domino 7

A comprehensive guide to moving to the latest version of this established collaboration platform

Tim Speed

Dick McCarrick

Tara Hall

Matthew Henry

Wendi Pohs

Barry Heinz



BIRMINGHAM - MUMBAI

Upgrading to Lotus Notes and Domino 7

Copyright © 2006 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, Packt Publishing, nor its dealers or distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: January 2006

Published by Packt Publishing Ltd.
32 Lincoln Road
Olton
Birmingham, B27 6PA, UK.

ISBN 1-904811-63-9

www.packtpub.com

Cover Design by www.visionwt.com

Warning and Disclaimer

The authors have attempted to ensure the contents of this book are as complete and accurate as possible, but no warranty or fitness is implied regarding any information and/or products referenced in this book. Several of the authors, at the time of publishing, were employees of IBM. The IBM Corporation provides a set of rules regarding publishing that applies to each employee. The IBM employees followed each of these rules as stated by IBM. Based on those rules, be advised that:

- This book is not sponsored by IBM/Lotus or ISSL.
- The IBM employees received IBM's legal permission to publish this book, using an outside IBM Press publisher.
- All users of this book do so at their own risk.
- The products referenced or mentioned in this book are listed for informational purposes only. The publisher and authors may have received demo copies to review. Several different vendors are mentioned in this book, and vendor products are used for reference. The publisher and authors do not recommend any product, software, or hardware. You, the owner of your hardware, software, and data, are responsible to make a determination of what is best for you. The authors do advise that you take careful consideration in determining your software, security, and infrastructure needs, and review more than just one vendor.

Lotus Domino 7 is a great product with many new features. Due to publishing deadlines, parts of this book reference Beta code, including some screenshots. If you find an error, please let us know.

IBM

The IBM list of copyrights and trademarks can be found at <http://www.ibm.com/legal/copytrade.shtml>.

In no event will IBM be liable to any party for any direct, indirect, special, or other consequential damages for any use of this book. All information is provided by the authors on an "as is" basis only. IBM provides no representations and warranties, express or implied, including the implied warranties of fitness for a particular purpose, merchantability and non-infringement for any information in this book.

Credits

Authors

Tim Speed
Dick McCarrick
Tara Hall
Matthew Henry
Wendi Pohs
Barry Heinz

IBM/Lotus Reviewer

Paul Raymond

Technical Editor

Niranjan Jahagirdar

Editorial Manager

Dipali Chittar

Development Editor

David Barnes

Indexer

Niranjan Jahagirdar

Proofreader

Chris Smith

Production Coordinator

Manjiri Nadkarni

Cover Designer

Helen Wood

About the Authors

Timothy Speed is an IBM Certified IT Architect working for the IBM Lotus Brand (ISSL). Tim has been involved in Internet and messaging security since 1992. He has also participated with the Domino infrastructure team at the Nagano Olympics, and with the Lotus Notes systems for the Sydney Olympics. His certifications include CISSP, MCSE, A+ Plus Security from CompTIA, Lotus Domino CLP Principal Administrator, and Lotus Domino CLP Principal Developer. (Notes/Domino certifications in R3, R4, R5, ND6, and Notes and Domino 7.)

Knowledge is based on many different facets—what you know, knowing where information can be found, and who you know. The information in this book is a combination of all these facets. Data sources have been referenced in this book; these include references to people, URLs, and other books. But much of the knowledge that is in this book comes from very smart people. Not all the people listed in this 'acknowledgement' section actually participated in the writing of this book, but all have influenced and guided me in my life that has culminated in this work. First and foremost I need to thank my wife for helping me with the book and providing some of the editing throughout the various chapters. Next I want to thank Johnny Speed, a great son who not only provided his support but also edited various chapters in this book. I thank my daughter Katherine for tolerating me during the months that I worked on this book. Thanks to Ed Speed for the inspiration to keep publishing. I am very grateful to Dick McCarrick for being crazy enough to co-author this book. Special thanks to David Barnes the Development Editor, and Niranjana Jahagirdar the Technical Editor. Also, thanks to Lotus/IBM (and ISSL), Chris Cotton, and Jack Shoemaker for allowing me to co-author this book. Thanks to Paul Raymond and Andrea Waugh-Metzger for reading/reviewing this book before publishing. Many thanks to Katherine Spanbauer, for writing the foreword for this book. Finally thanks to Scott Souder (IBM) for his support in getting the approvals for writing this book.

Thanks to the following content authors:

Dick McCarrick
Wendi Poh
Tara Hall
Barry Heinz
Matthew Henry

Now to talk about the really smart people—due to legal issues, the people listed below could not directly contribute to this book, but I have learned a lot from these people via work and their friendship:

Joe Christohper (a great educator and technologist), Lillian Speed, Ted Smith, Jeff Jablonowski, Barbara Robertson, Beth Anne Collopy, Bob Thurston, Bob Stegmaier, Charles DeLone, Cheryl Rogers-McGraw, Shawn Scott, Bill Kilduff, Kevin Mills, Boris Vishnevsky, Brad Schauf, Greg Prickril, David Byrd, Glenn Druce, Kathrine Rutledge, Charles Carrington, Vivian M. Fleitstra, Ann Marie Darrough, Larry Berthelsen, Craig Levine, Daniel Suster, Mark Harper, Jeff Pinkston, George Poirier, Jordi Riera, David Via, Heidi Wulkow, Dave Erickson, David Bell, Mark Leaser, John Kistler, Jon P Dodge, Luc Groleau, Zena Washington, Burk Buechler, Robert Thietje, Francois Nasser, Marlene Botter, Roy Hudson, Mike Dudding, Stephen Cooke, Ciaran DellaFera, Tom Agoston, Mike Confoy, Carl Baumann, Shane George, Tery W. Corkran, David Bell, David Hinkle, Delbert W Blackketter, Brian Ford, Carlos Miranda, Don Nadel, Doug Parham, Ed Brill, Gary Ernst, Steve Keohane, Steven Kramer, Gregg Smith, Hartmut Samtleben, Hissan C Waheed, Ian Reid, John Norton, Katherine Emling, Kevin Lynch, Mac Jones, Marc Galeazza, Mark Steinborn, Mary Ellen Zurko, Matthew Milza, Matthew Speed, Melanie Pocock, Michael Lenhart, Naemi Engler, Peter Burkhardt, Ralph Vawter, Sherry Price, Stephen Hardison, Lisa Herrera, Terry Fouchey, Ed Rich, Kenneth Neisler, Laurie Jones, Christopher Byrne, Steve Matrullo, Elie AbenMoha, Michael Getzinger, David Caldwell, David Morrisey, Randy LeTourneau, Marco M. Noel, and the brilliant Chuck Stauber.

Finally, a special acknowledgment to Wayne Hamit and Mountain Movers.
(<http://www.mountain-movers.org>)

Dedicated to Linda Speed—"just me".

Dick McCarrick is a content developer for IBM's developerWorks Lotus website (www.ibm.com/developerworks/lotus). Dick joined the Lotus Notes team in 1990 as a documentation writer, and moved over to developerWorks Lotus in 2001.

Tara Hall is the Web Content Manager for IBM's developerWorks Workplace and developerWorks Lotus (formerly the Lotus Developer Domain/Notes.net) websites. She has been writing and editing technical documentation since graduating from New Mexico State University in 1997 with a Masters of Art degree in Creative Writing.

Matthew Henry is a Technical Architect working for KEMET Electronics Corporation. Matthew has worked with Lotus Notes since release 3.0, when he led the rollout of Lotus Notes as KEMET's email and collaborative platform of choice. He has served with various Lotus Notes and Domino activities and customer councils including presenting at Lotusphere for several years.

Wendi Pohs is CTO at InfoClear Consulting, a company that specializes in taxonomy management and toolkit integration. Prior to that, she was a consulting IT specialist on IBM's intranet user experience team. Wendi is the author of a book about knowledge management methodologies, *Practical Knowledge Management: The Lotus Knowledge Discovery System*, published by IBM Press. Wendi joined IBM/Lotus in 1996, and has worked on various projects as a spec writer, online help designer, user assistance manager, and lead for search and taxonomy for w3, IBM's corporate intranet. Prior to joining IBM, Wendi worked at the American Mathematical Society and at Digital Equipment Corporation. She received her BA and MILS degrees from the University of Michigan.

Table of Contents

Preface	1
Chapter 1: A Short History of Notes and Domino	5
Chapter 2: New Notes/Domino 7 Features	11
Lotus Notes	11
Domino Designer	13
Domino Administrator	15
Domino Server	16
LEI	17
Summary	17
Chapter 3: Domino Domain Monitoring	19
Domino Domain Monitoring (DDM)	20
Probes	22
Configuring Probes	22
Filters	23
The Event Resolution Center (ERC) Database	24
Types of Probes	24
Application Code	24
Database	25
Directory	26
Messaging	28
Operating System	29
Replication	30
Security	32
Server	34
Web	35
Event Notification Using an Agent	35
Create a Tracking Database	44
Create a Simple Agent, View, and Form in the Tracking Database	44
Create a Database Event Generator Document in events4.nsf	46

Create an Event Handler (Run an Agent)	47
Basics Tab	47
Event Tab	47
Action Tab	47
Enable the Event Handler and the Event Generator	47
Testing	47
Summary	48
Chapter 4: AdminP	49
AdminP Server Task	49
Administration Client	49
Notes Client	50
Domino Directory	50
Certification Log	51
admin4.nsf	51
Administration Server	51
Proxy Actions	52
Types of Proxy Actions	60
Operations that Execute on the Primary Administration Server	60
Operations that Execute on all Spoke Administration Servers	61
Operations that Execute on a Targeted Server	62
admin4.nsf	62
Cross-Domain Administration Requests	62
Replica ID Relationship for admin4.nsf and names.nsf	63
Name-Change Management	63
Summary	64
Chapter 5: Policy Management	65
Policy Basics	65
Basics Tab	65
Comments Tab	66
Administration Tab	66
Policy Lock Down	66
Registration Policy	67
Setup Policy	68
Preferences Tab	68
Miscellaneous Tab	69
Internet Tab	70
Mail and News Tab	70
Instant Messaging Tab	71

Desktop Policy	72
Basics Tab	72
Smart Upgrade Tab	73
Preferences Basics Tab	73
Preferences Miscellaneous Tab	73
Preferences Internet Tab	74
Preferences Instant Messaging Tab	74
Preferences Diagnostics Tab	74
Mail Archiving Policy	74
Security Policy	78
Mail Policy	79
Basics Tab	80
Mail File Preferences Mail Basics Tab	80
Mail File Preferences Mail Letterhead Tab	81
Mail File Preferences Calendar & To Do Tab	82
Basics Tab	82
Display Tab	82
Scheduling Tab	84
Alarms Tab	85
To Do Tab	86
AutoProcess Tab	87
Room and Reservations Tab	88
Access to Your Mail & Calendar Tab	89
Access to Your Schedule Tab	90
Message Disclaimers	91
Server Disclaimers	91
Client Disclaimers	91
SMTP	92
DNS Whitelist Filters	94
Private Blacklist Filters	95
Private Whitelist Filters	97
Statistics	98
DNS Whitelist Statistic	98
Private Blacklist Statistic	98
Private Whitelist Statistic	99
Summary	99
Chapter 6: Smart Upgrade	101
Smart Upgrade Process	101
Create the Smart Upgrade Kit Database	102
Create or Modify a Server Configuration Document	102

Create a Kit Document	103
Basics Tab	104
Administration Tab	110
Create or Modify a Desktop Policy Document	110
Smart Upgrade Tracking Database	112
The End-User Experience	112
Summary	113
Chapter 7: Performance Aspects and Additional Standards	115
Performance	115
Identify Monitoring Tools	116
Server.Load	121
LEI	131
Automatic Data Collection and Fault Analyzer	137
Fault Analyzer Settings	140
IPv6	141
DNS and Resource Records	144
Zones	145
Enabling IPv6 on Domino 7 Servers and Notes 7 Clients	145
Summary	146
Chapter 8: Client Features	147
Notes 7	147
New Mail Features	148
Autosave	150
Other Mail Features	151
Archiving	152
Background View Indexing	154
Mail Rule Processing	154
Calendaring and Scheduling	155
New Right Mouse Button Selections	157
Preventing Expansion of Personal Groups	157
Rooms and Resources	158
Sametime Integration	159
Domino Designer 7	166
Shared Columns	168
Administration Client	169
Hotkeys	173
Summary	174

Chapter 9: Domino Web Access	175
Security	175
Integration with DOLS and Instant Messaging	176
Instant Messaging	176
Import Corporate Holidays	176
Stationery	177
Mail Threads	179
S/MIME Support	179
Importing a Notes ID	181
Domino Web Access Configuration	190
Mail Encryption	191
Instant Messaging	191
International	194
Browser Cache Management	195
Other Domino Web Access Settings	200
Summary	201
Chapter 10: Programming	203
AutoSave	203
Recovering Documents Saved with the AutoSave Feature	204
Enhanced Java Support	205
New Formula Language Commands	206
New LotusScript Elements	207
Admin Support	207
General Document Support	207
XML Support	208
IBM Workplace Client Support	208
Summary	209
Chapter 11: Security	211
New Encryption Options	211
Interoperability	214
Key Rollover	214
Smartcards	214
Security APIs	216
ID Recovery Enhancements	217
Configurable Password Length and Recovery Message	217
Suppression of Standard Export Recovery Message	218
Timestamps	218

Recover User IDs from the Administration Client	218
Mail ID Recovery	219
Expanded Logging	219
Obsoleting Recovery Passwords	219
Password Management	220
Summary	221
Chapter 12: Upgrading to Domino 7	223
Use Cases	223
Notes/Domino 7 Upgrade	230
Review the Current Infrastructure	230
The Upgrade Process	233
Use Case: Domino Server Upgrade	234
Summary	236
Chapter 13: Domino and the Web	237
IBM WebSphere Portal for Beginners	237
Advantages of Lotus Domino and WebSphere Portal Integration	238
Lotus Domino and WebSphere Portal	239
Server Integration	240
Configuring Lotus Domino for WebSphere Portal	241
Configuring Domino LDAP	241
Enabling LDAP for SSL	243
Setting the Domino Server Document for WebSphere Portal	244
Enabling the DIIOP Task	245
Application Integration	245
Application Integration Types	245
Application Integration Techniques	246
Collaboration Center	246
Domino Application Portlet	247
Lotus Domino Extended Products Portlets	247
Common Personal Information Management (PIM) Portlets	247
Portlet Builders	248
Domino JSP Tag Libraries	248
Java Programming	249
The Notes Application Plug-In	250
IBM Workplace Collaboration Services	250
IBM Workplace Managed Client	251
Summary	252

Chapter 14: Directories	253
Directory Uses	254
Directory Architecture	256
X.500	258
LDAP	258
New Directory Features in Domino 7	261
LDAP UNID	261
Directory Assistance	261
LDAP Connections and Domino 7	262
LTPA	262
The Domino Directory	263
Summary	267
Chapter 15: Domino Access for Microsoft Outlook	269
Requirements	269
Installing Domino Access for Microsoft Outlook	270
Upgrading from DAMO 6.5.x to 7	270
Setting Up Condensed Directories for Working Offline	270
Keeping Your Mail File Secure	270
Installation Notes for Administrators	271
DAMO Performance	272
DAMO 7 Improvements and Enhancements	273
Option for Separate Program and Data Directories	273
Productivity Enhancements	273
New Mail Notification	273
Offline Address Book Support	274
User Security	275
X.509	276
Notes Encryption	276
Out-Of-Office Management	276
Replication Management	277
Password Management	278
Mail File Ownership	279
Calendar and Scheduling	280
S/MIME	281
Issues	282
Summary	282

Chapter 16: Troubleshooting	283
Domino Domain Monitoring	283
log.nsf (Server Log File)	283
Events Monitoring (events4.nsf and Event Monitor Task)	283
Domino Web Logging	284
Mail Tracking	285
The Server's mail.box Database	286
Mail Trace	286
Maps Tool	286
TCP/IP Connection Logging	286
SMTP Troubleshooting Examples	287
NOTES.INI Logging and Debug Parameters	288
Database Analysis	289
Log Analysis	290
Cluster Analysis	291
Predictive Activities Using Server Health Monitor	292
Notes System Diagnostic (NSD)	293
Server Commands	293
Summary	294
Chapter 17: Case Study	295
developerWorks Lotus	295
Notes/Domino Upgrade Process	296
Plan	296
Deploy on a Non-Production Test Server	296
Set Up a Forum to Discuss Issues Found	297
Start Small (Deploy on a Cluster Member and Expand)	297
Deploy on One Platform (Win32) and Gradually Move Out to Others (Unix Dialects)	297
Work Closely with Application Designers	297
Watch for Issues, Trends, and Assorted Weirdness	297
Document Everything!	298
Summary	298

Appendix A: Tools and References	299
Binary Tree Migration Tools for Lotus Notes 7 and Domino 7	299
Migration to Notes/Domino 7	299
Coexistence Solutions for Notes/Domino 7 and Microsoft Outlook/Exchange	300
DNA Network Analysis for IBM Lotus Domino	300
End-User Demand	301
Session Concurrency	302
Deployment Integrity	303
Server Platform Health	304
Angkor	305
Securing and Assuring Delivery of Lotus Domino Web Applications	306
Index	309

Foreword

In the history of software, there have been a number of "killer applications" that were not only successful, but also helped change the entire industry. There was Microsoft Basic, the simple yet powerful programming language that made it possible for almost anyone to be an application developer, VisiCalc, the spreadsheet that helped transform the personal computer from a home hobby to a powerful business tool, CP/M, the pioneer PC operating system that helped pave the way for standardization, Netscape, the web browser that helped bring the internet to everyone.

If you can forgive a longtime Loti for a moment of immodesty, I believe that Lotus Notes/Domino deserves to be included on this list. When Lotus Notes first appeared in 1989, there was nothing like it—indeed, a whole new vocabulary that included words like *groupware* and *replicator* had to be invented to describe it. Early adopters soon discovered that Lotus Notes provided them with tools so powerful, it could actually change the way they did business and provided a possible advantage over their competitors. Within a few years, the installed base of Notes users grew from a few thousand, to tens of thousands, to millions, and finally, well over a hundred million now. Notes became a global phenomenon; like the former British Empire, nowadays the sun never sets on Lotus Notes/Domino!

But the impact of Lotus Notes/Domino goes far beyond its success in the marketplace. Notes/Domino actually changed the way people work. Previously, company experts in a particular area were tacitly encouraged to hoard what they knew, to keep it to themselves, and thus ensure their value and importance within the corporation. "Knowledge is power" was the general philosophy, and power wasn't something to be shared. But when Lotus Notes came along, it brought with it a major paradigm shift. With Notes, employees were encouraged to share what they knew, to record this knowledge in Notes documents where it could be found and referenced by others within the organization. An employee's value was no longer measured by what was inside his or her head, but by how much he or she could contribute to the corporate store of expertise. In this way, Lotus Notes served as one of the pioneer knowledge management tools, years before that term became trendy.

An early industry analyst probably said it best. Before Lotus Notes, software products were very good at helping people work—inefficiently. Spreadsheets, word processors, and similar products were all designed to help the single, isolated user be more productive—at working alone. Lotus Notes, on the other hand, encouraged people to work together, sharing information, automating processes—in a word *collaborating*, a term seldom applied to business software before Notes appeared on the scene.

Today, Lotus Notes/Domino is more widespread and relevant than ever. At one time Lotus/IBM listed the major corporations that used Lotus Notes; today it might be easier to list the companies that *don't*. And the number of different ways that people use Notes/Domino has also grown exponentially, especially with new features such as instant messaging integration, support of industry standards, and third-party products (and increasingly, tight coordination with the new IBM Workplace family of products, which promise to open up Notes/Domino technology to a whole new community of users). Collectively, these provide Notes/Domino with an unmatched flexibility.

This flexibility leads to versatility, versatility leads to complexity, and complexity often leads to a lot of sleepless nights for Notes/Domino administrators. Right from the beginning, Lotus Notes has never been an out-of-the-box application. Instead, it comes with customization capabilities that let you tailor it to your organization's precise needs. In some ways, each Notes/Domino environment is unique, with its own set of requirements, capabilities and, frankly, challenges. Among the biggest of these challenges are deployment and upgrade.

One of the authors of this book recalls working on the very first Notes deployment documentation. As part of the research for this documentation, the author went on a fact-finding mission at Notes sites throughout the United States. Two of the questions asked at each site were:

1. How many people in your company use Notes now?
2. How many people do you plan to be using Notes 12 months from now?

A typical answer was something like, "We currently have 80 people using Notes now. Next year we plan to have 5,000." Invariably, these customers listed lack of deployment information as the primary obstacle to reaching their goal. So very early on, this information was identified as critical to the success of Notes/Domino.

That was 15 years ago, and this situation is still true, perhaps more so than ever. This especially applies to upgrades. Moving your Notes/Domino environment to a new release is a very significant undertaking. You need to plan carefully taking into consideration all the new features you plan to use, and their incorporation into your environment. You need to examine all possible compatibility issues. You need to think about all performance and capacity enhancements to take advantage of the opportunity to possibly simplify and streamline your infrastructure. In short, you need to do two things: learn what the new release brings to the table, and ensure that the processes you use to upgrade to a new release are as efficient and logical as possible.

This book is aimed squarely at these two tasks. It reviews all the major new features in Notes/Domino 7, the latest release of this product, and pays special attention to functionality that presents special upgrade considerations. The book also offers a wealth of useful upgrade information including processes and procedures, points to consider,

examples, and guidelines. This information isn't the result of some classroom exercise or hypothetical guesswork; instead, it reflects the hands-on experience of veteran Notes/Domino professionals—people who have worked directly with customers to help them with their upgrades and deployments, who have collectively worked with and written about Notes/Domino for years. And although this information is intended to help you upgrade to Notes/Domino 7, much of it is general enough to apply to nearly any Notes/Domino upgrade. Therefore this book should be useful for years to come.

So if you're in the process of (or will be soon be) planning your upgrade to Notes/Domino 7, you should consider adding this book to your Notes/Domino library. Look it over and browse through its chapters and topics. It's likely that you'll soon find a lot of valuable information that directly applies to your environment, information that may save you a lot of time and effort (and maybe avoid a headache or two) as you undertake your upgrade campaign. And if you have already purchased this book—what are we waiting for? Let's get going!

Katherine Emling

Katherine Emling is a development manager on the Domino server team, responsible for security and platform strategy. Since joining Lotus in 1992, she has held various roles in the Technical Support, Professional Services, and Product Management and Development organizations. Katherine is a graduate of the University of Wisconsin, where she earned her Bachelor of Business Administration degree.

Preface

If you're reading this book, you're probably already familiar with Lotus Notes/Domino. You know about all the powerful productivity features offered by this product (actually multiple products, although most of us in the Notes/Domino universe still think of it as one). You know how much your company relies on it to communicate, collaborate, and manage its collective store of corporate knowledge. (An industry analyst once described Notes as something you can't quite define, but within 15 minutes of using it you realize you can't live without it.) And you realize (perhaps all too well) that upgrading from one major release to the next can be a significant undertaking, especially if you maintain a 'mixed' environment that includes multiple versions of Notes and/or is integrated with other third-party products.

This book is intended to help you with that task. It is specifically intended for upgrading to Notes/Domino 7, the latest release of the product. But much of the information we provide is also applicable to any Notes/Domino version, and can be used as a general guide whenever it comes time to upgrade to the next major release.

This book has been written by Notes/Domino 'insiders'. Collectively, we possess decades of Notes/Domino experience; we've been with the product since Notes 1.0, and since then have worked directly with customers to help them with their Notes/Domino upgrade and deployment issues. This book represents a compendium of what we've learned during that time. It addresses all the major issues that we've seen customers wrestle with during their upgrades. Our goal is to help you avoid these issues when possible, and work around them when it's not. At the same time, we identify considerations that are unique to Notes/Domino 7, to help you understand and prepare for all the exciting new capabilities offered in this release.

What This Book Covers

Chapter 1 puts Notes and Domino into their historical contexts, showing how Notes turned from college students' dreams into a major business product.

Chapter 2 takes you on a tour of the new features of Notes and Domino, laying a foundation for the chapters that follow.

Chapters 3-6 take a deeper look at the new features: DDM and event monitoring, AdminP, Policy Management, and the Smart Upgrade process.

Chapter 7 looks at performance issues. *Chapter 8* moves the focus to the Notes/Domino 7 clients, while *Chapter 9* looks at how users can access Notes/Domino through Domino Web Access 7.

Chapters 10-12 deal with the technical issues of programming Notes/Domino, managing security, and then bring the topics so far together with a practical look at the upgrading process.

Chapters 13-15 look even further into the new features of domino. *Chapter 13* explores WebSphere integration, and *Chapter 14* shows how and why Domino/Notes 7 works with directories to maintain its data. *Chapter 15* concludes the feature exploration with a look at integrating Notes/Domino 7 with Microsoft Outlook.

Chapters 16-17 round off the book by looking at some troubleshooting methods, followed by a case study that shows how developerWorks Lotus team made their Notes/Domino 7 upgrade work for them.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

There are three styles for code. Code words in text are shown as follows: "We can include other contexts through the use of the `include` directive."

Any command-line input and output is written as follows:

c: \tel net [*Servername. DNS or IP address*]

New terms and **important words** are introduced in a bold-type font. Words that you see on the screen, in menus or dialog boxes for example, appear in our text like this: "clicking the Next button moves you to the next screen".

Warnings or important notes appear in a box like this.

Reader Feedback

Feedback from our readers is always welcome. Let us know what you think about this book, what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply drop an email to feedback@packtpub.com, making sure to mention the book title in the subject of your message.

If there is a book that you need and would like to see us publish, please send us a note in the SUGGEST A TITLE form on www.packtpub.com or email suggest@packtpub.com.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on www.packtpub.com/authors.

Customer Support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Downloading Extra Material for the Book

There is an exclusive PDF to accompany this book, covering the new DB2 features in Notes/Domino 7. To access it, visit <http://www.packtpub.com/support>, and select this book from the list of titles to see the files available for download with this book. (This PDF should be released by February 2006.)

Errata

Although we have taken every care to ensure the accuracy of our contents, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in text or code—we would be grateful if you would report this to us. By doing this you can save other readers from frustration, and help to improve subsequent versions of this book. If you find any errata, report them by visiting <http://www.packtpub.com/support>, selecting your book, clicking on the Submit Errata link, and entering the details of your errata. Once your errata have been verified, your submission will be accepted and the errata added to the list of existing errata. The existing errata can be viewed by selecting your title from <http://www.packtpub.com/support>.

Questions

You can contact us at questions@packtpub.com if you are having a problem with some aspect of the book, and we will do our best to address it.

1

A Short History of Notes and Domino

As with all great ideas, Lotus Notes started out as the solution to a specific need. Three programming students attending a mid-western University in the late 1970s wanted a way to share notes and information. To do this, they used a software program called PLATO Group Notes, which ran on their mainframe-based college computer system. This program really wasn't intended for this purpose—it was originally designed for bug reporting—but it did provide just enough communication and collaboration functionality to offer a hint at what could be done, given the right software and technology.

After graduation, these three students—Ray Ozzie, Tim Halvorsen, and Len Kawell; names that have since achieved near-legendary status within the Lotus Notes community—went their separate ways. But none forgot the potential they saw in PLATO Group Notes. Halvorsen and Kawell took jobs at Digital Equipment Corporation, where they eventually created an in-house communication tool that resembled PLATO. Meanwhile, Ozzie took programming positions with other corporations, but never lost sight of his vision to form his own company and develop a more advanced, PC-based collaboration program. Eventually (1984 to be exact), with funding provided by Lotus Development Corporation (makers of the famous Lotus 1-2-3), Ozzie founded Iris Associates Inc., to develop the first release of Lotus Notes. Ozzie was soon joined by former classmates Halvorsen and Kawell, followed shortly by Steve Beckhardt.

This first version of Lotus Notes was modeled after PLATO Group Notes, but was far more advanced, sporting powerful features such as online discussion, email, phone books, and document databases. This functionality presented some serious challenges to the hardware and supporting infrastructure upon which Notes ran at the time. To meet these challenges, Notes was built upon a then-radical client/server architecture that featured PCs connected to a **local area network (LAN)**. Groups set up a dedicated server PC that communicated with other servers. These servers exchanged information through **replicated data**, a concept familiar to us today, but extremely revolutionary at the time.

This allowed users to exchange information with co-workers (however remote), while maintaining high performance. Equally important, Notes, from the outset, was designed to be highly customizable, with a state-of-the-art multi-faceted programmatic interface that allowed developers to create powerful applications specifically suited to the needs of their workgroups.

The first release of Notes shipped in 1989. (A five-year development cycle may seem like a long time by today's standards, but bear in mind, the Iris folks were basically creating an entirely new genre of software.) Release 1.0 provided several 'ready to use' applications such as Group Mail, Group Discussion, and Group Phone Book. Notes also provided templates that assisted developers in the construction of custom applications, which led to a vibrant business partner. Release 1 features included:

- Email
- Advanced security features, including Access Control Lists (ACLs) determining who can access which database, as well as encryption, signing, and authentication using the RSA public-key technology
- Dial-up functionality
- Import/export capability, including Lotus Freelance Graphics metafile import, structured ASCII export, and Lotus 1-2-3/Symphony worksheet export
- Online help (a novel idea at the time!)
- Formula language for programming Notes applications
- DocLinks providing 'hotlink' access between Notes documents
- Central administration

The next major release of Notes shipped in 1991. For release 2.0, scalability became the focus. Notes was initially intended for small- to medium-sized businesses, basically because the PCs at the time didn't really lend themselves to the multi-thousand user communities we're familiar with today. Release 2.0 included:

- C Applications Programming Interface (API)
- Tables and paragraph styles
- Rich text support
- Additional formula language @functions
- Address look-up in mail
- Multiple Name and Address books
- Mail enhancements

Notes 3.0 shipped in mid-1993. At the time of this release, the Notes community had grown to more than 2,000 companies with nearly 500,000 users. Release 3.0 introduced many now-familiar features, such as:

- Full-text search
- Hierarchical names, views, forms, and filters
- Background replication
- Alternate mail
- Selective replication
- Support for the Macintosh client (a major customer demand)
- Windows server

It was around this time that the Internet began drawing attention as a serious business tool, rather than merely the domain of students and socially-inept 'geeks'. This led to the release of InterNotes News, a product that provided a gateway between the Internet news sources and Notes. Although largely forgotten today, this was the first project that reflected the growing influence of the Internet on Notes.

In January 1996, Lotus released Notes 4.0, offering a radically redesigned user interface that simplified many Notes features, making it easier to use, program, and administer. This interface quickly became popular among users and developers. The product continued to become faster and more scalable. In addition, Notes began to integrate with the Web, and many new features reflected emerging web technology. For instance, the new Server Web Navigator allowed the Notes servers to retrieve pages from the Web, allowing users to view the pages in a Notes client.

Release 4.0 also offered:

- LotusScript, a programming language built into Notes
- A three-paneled UI for mail and other applications with preview capability
- Pass-through servers
- View, folder, and design features
- Search features, such as the ability to search a database without indexing it
- Security features, such as the ability to keep local databases secure and the ability to restrict who can read selected documents
- Internet server improvements, including SOCKS support, HTTP proxy support, and Notes RPC proxy support

In July 1995, IBM purchased Lotus. This gave the Notes developer team access to world-class technology, including the HTTP server now known as Domino (which eventually led to the Notes product being known by the current name Notes/Domino). This helped

transform the Notes 4.0 server into an interactive web applications server, combining the open networking environment of Internet standards and protocols with the powerful application development facilities of Notes. Domino allowed customers to dynamically publish Notes documents to the Web—a major development in the life of the product.

Among the major enhancements offered in release 4.5 was Calendar and Scheduling (hard to believe it hasn't been in the product all along), as well as:

- Personal Web Navigator
- Scalability and manageability improvements, including Domino server clusters and directory assistance
- Security enhancements, such as Execution Control Lists and password expiration and reuse
- Programmability, including script libraries
- Seamless web access from the Notes client

Notes and Domino release 5.0 shipped in early 1999. The release continued the Notes/Domino integration with the Web, to the point where the two technologies were now inseparable. This was reflected in the release 5 interface, which bore a more browser-like feel. It also supported more Internet standards and protocols. Release 5 also introduced **Domino Designer**, the third member of the Notes/Domino triumvirate of products. And the new Domino Administrator made Domino network administration easier.

Domino 5 featured:

- Internet messaging and directories
- Expanded web application services, including CORBA
- Database improvements, such as transaction logging

The Notes 5 client included a new browser-like user interface with a customizable welcome page for tracking daily information. It also included improvements to applications such as mail, calendar and scheduling, web browsing, and discussions.

By the time Notes 6 and Domino 6 were introduced in late 2002, industry talk focused on concepts such as lower total cost of ownership (TCO for the buzzword-inclined), increased productivity, and faster development and deployment. Basically, our customers were telling us they needed to do more with less, and they needed to do it faster (sound familiar?).

In response, Domino 6 offered enhanced installation, scalability, and performance. Domino Designer 6 allowed developers to create complex applications more easily and to reuse code. And we improved the Notes 6 client, with an eye towards improving each user's personal productivity. Our overarching theme was to help our customers work more efficiently. For example, installation and setup offered more options and an

improved interface. We made central management of multiple remote servers easier, through features such as policy-based management. And we improved server scalability and performance, with new features such as network compression and Domino Server Monitor. We carried these themes through Notes/Domino 6.5, which offered enhanced collaboration with tighter integration with Sametime, QuickPlace, and Domino Web Access. For programmers, release 6.5 included the Lotus Domino Toolkit for WebSphere Studio, a set of Eclipse plug-ins you can use to create JavaServer Pages (JSPs) using the Domino Custom Tags.

As for Notes/Domino 7—well, its features are the subject for the next chapter. Let's just say for now that this latest release continues the tradition of cutting edge technology and functionality built into that first release, the culmination of the idea of three forward-thinking students who (not to wax overly dramatic) launched an entirely new software industry, and with it a whole new way of doing business, based on communication, collaboration, and sharing and managing the collective expertise of your corporation—in short, getting the most out of *all* your resources, hardware, software, and (most important of all) human!

2

New Notes/Domino 7 Features

This chapter of the book covers a high-level review of many of the new features in Notes and Domino 7. This includes new features in:

- Lotus Notes
- Domino Designer
- Domino Administrator
- Domino server
- LEI

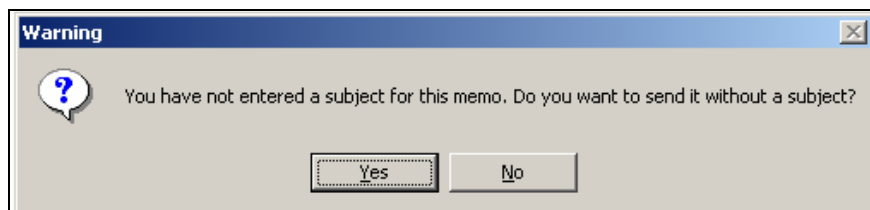
The following sections briefly examine the major new features in all these products.

Lotus Notes

The Lotus Notes client includes a large set of new features. Details on these features are included in Chapter 8. This section takes a quick review of many of these new features.

You can now, with a single click, close all open windows. Also, you can save the state of your work. Use this ability to save the window state for Lotus Notes to remember where you were working by permanently setting the window state to the currently opened windows.

Notes now offers the ability to be prompted when you send a message with no subject:



There are new client follow-up actions to help with messaging tracking and workflow. (This displays with the right mouse button.)

There are new mail rules for spam management. For those looking for a quick status on digital message signatures and encryption, there are new status bar icons that will display this status. And there are improved Workspace wizards.

One of the best new client features is the ability to automatically save your work. This can really be helpful in the event that your computer crashes and/or has a power loss. This feature will save the work so you can retrieve it when the Lotus Notes client starts.

With Notes 7, you can sort by subject in your mail files. This option is available in the views All Documents, Inbox, Sent, Drafts, and others. Mail threads allow you to track a set of mail messages through the lifetime of that set of messages.

Notes 7 Calendar and Scheduling (C&S) includes a new Calendar Cleanup action that helps the end user to quickly and easily maintain calendar entries.

Also with C&S, you can now set up the online portion of the meeting to restrict attendees to only those on the invite list. You can also provide a password for an online meeting. Other enhanced C&S support includes new options for managing rooms and resources. Now end users can specify a preferred site and a preferred list of rooms and/or resources to use when scheduling meetings.

In addition, end users can now configure the calendar to accept a meeting, even if it conflicts with an earlier meeting.

Calendar owners can also mark messages for follow up in mail files that they manage. And they are prompted to specify where forwarded mail is saved.

Consider this scenario: you found the document you want, but how can you find what folders it is listed in? You can do this now with the ability to 'discover' folders. When a document is selected in the view, and the Folder | Discover Folders action is selected, a dialog box will be displayed, showing which folders the selected document is in.

Lotus Notes 7.0 also offers enhanced presence awareness based upon Lotus Sametime. End users can now see a person's name in a document or view and determine if that person is online. Presence awareness has been added to Team Rooms, Discussions, To Do documents, Personal Name and Address Book, Rooms and Resources templates, and various C&S views.

You can also access Notes mail through the Microsoft Office XP Smart Tags. Microsoft Office Smart Tags recognize certain types of text, for example, a person's name.

Notes 7 additionally includes improved Rooms and Resources usability (including a simple form to create a reservation and the ability to transfer a reservation), and improved email archiving.

Domino Designer

Domino Designer 7 is based the solid platform of previous versions. This improved Designer also provides tighter integration with web standards. Other features include the Print Source dialog box. This lets you print source code from within the programmer's pane. You can print source code for formulas, simple actions, HTML, LotusScript, and JavaScript. Also, the Print Frameset dialog box lets you print the entire frameset or individual frames within the frameset.

Shared columns allow the creation of a common column for insertion in multiple views in the same database, eliminating the need to create the same column multiple times. This creates a single point for propagating changes to all views using the same column.

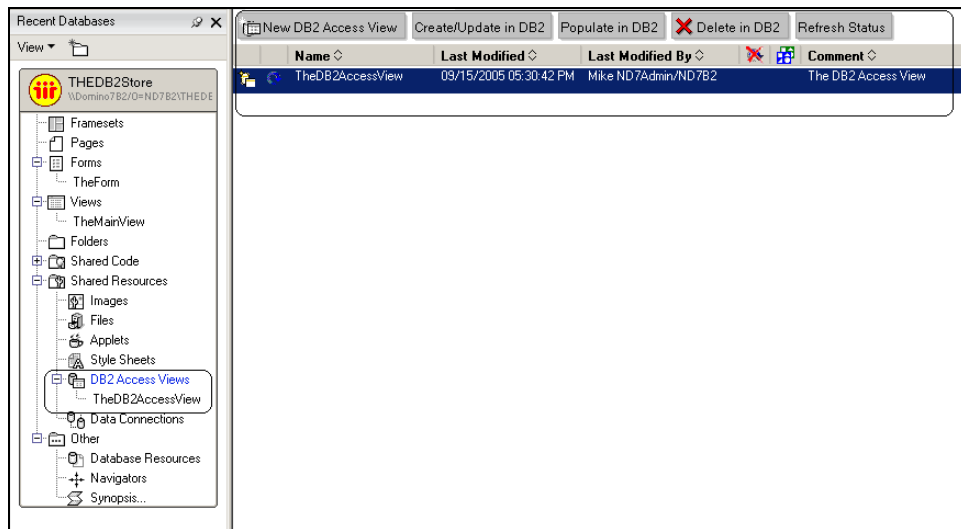
There are new LotusScript debugger enhancements. You can now start and terminate debugging with an icon. Also, messages go to the status bar rather than a message box. Another new feature is the ability to debug Java code remotely. With this feature you can debug Java agents, perform web previews, and debug script libraries running under control of a Notes client Java Virtual Machine (JVM).

Domino 7 now supports web services, as defined in the W3C document *Web Services Architecture* (see <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211>).

Domino Designer 7 offers a number of other usability features, including a sortable 'comments' column, and a new toolbar icon to toggle the LotusScript debugger state. This toolbar icon also indicates whether the debugger is on or off.

Domino Designer 7 now includes two new types of views for DB2-enabled databases:

- **DB2 Access views:** These define how your data is organized, enabling you to leverage features available in DB2. These views identify a common set of notes in an NSF file. This information can then be used by DB2. A screen shot overleaf shows how you can create and manage DB2 Access views via the Designer client.
- **DB2 Query views:** These use an SQL query to populate data, instead of a view formula that selects documents from within the NSF file. With Query views, you can access non-Domino content. A Query view can also join data from multiple DB2 tables and views, allowing you to join data from two NSF files indirectly by joining two separate DB2 Access views.



Domino Designer 7.0 also offers a set of programmability enhancements. This includes a number of new functions, methods, and properties; a few examples include:

- @IsEmbeddedInsi deWCT
- @DbBui l dVersi on
- @GetDB2Schema
- @IsDB2, @Command([DiscoverFolders])
- @Pol i cyFi el dLocked
- NotesDatabase. GetModi fi edDocuments (LotusScript)
- Database. getModi fi edDocuments (Java)
- NotesAdmi ni strati onProcess. ApproveHostedOrgStorageDel eti on (LotusScript)
- Admi ni strati onProcess. approveHostedOrgStorageDel eti on (Java)
- NotesDocumentCol l ecti on. Unti l Ti me (LotusScript)
- DocumentCol l ecti on. getUnti l Ti me (Java)
- NotesDocumentCol l ecti on. Unti l Ti me (LotusScript)
- DocumentCol l ecti on. getUnti l Ti me (Java)

Domino Administrator

There are several significant new features and improvements with release 7 of the Domino Administrator client. These new features will help administrators with configuration, maintenance, and uptime. One of the most important new features is Domino Domain Monitoring (DDM). Chapter 3 is dedicated to this new powerful feature. Other features and tools include administration event script handling (via Lotus Script).

Policy administration has been enhanced. This includes the ability to lock down end-user desktops, and a new mail policy.

Domino 7 provides integration with **Tivoli Autonomic Monitoring Engine (TAME)**. This provides event-reporting capabilities to other Tivoli interfaces (for example, Tivoli Enterprise Console). Domino resource modules, built for Domino TAME, can report CPU-, memory-, disk-, and network-utilization statistics. The resource modules are configured with and report to DDM interfaces and to Tivoli Enterprise Console.

The improved 'activity trends' feature uses these Domino server features:

- Activity logging to collect information used for resource balancing
- Activity trends to set up times for data collection and retention
- Domino Change Manager to implement a workflow process in which changes made to the system are controlled and approved

Enhancements to Smart Upgrade include the ability to detach kits in the background, to prevent time lost to a non-working client; and failover from a shared (network) upgrade kit to another server's attached kit. If clustered, Smart Upgrade uses a cluster mate if the first server is unavailable. Smart Upgrade also helps prevent excessive server load by limiting the number of downloads from a single server. And it provides notification to administrators, via a mail-in database, of the Smart Upgrade status by user/machine (Success, Failed, or Delayed). In addition, you can provision the Smart Upgrade Tracking database.

DB2 Management tools let you enable Domino to run with a DB2 data store, configure a connection document from DB2 Access for a Domino server to Domino, and allow DB2 usernames/passwords to be added to server IDs. You also have enhanced support in status and statistics panels indicating DB2 usage and statistics plus other visual cues.

Other new features include:

- The ability to write status-bar history to a log file
- The ability to suppress the Roaming User Upgrade prompt

- Domino Web Administrator support for Mozilla browsers
- Three new event-notification methods, which are programmable via LotusScript, batch language, Java, C, and so on
- An enhanced Message ID feature that allows a message ID to be prefixed to console messages, via the `notes.ini` settings `Display_MessageID=1` and `Display_MessageSeverity=1`

The Administration process will no longer revert name changes automatically, but will require that the administrator either approve or reject the name change reversion.

Domino Server

The Domino 7 server enhancements include **autonomic diagnostic collection**, a feature that can be considered both an administration feature and a server feature. This powerful feature is used to analyze various processes and events that are generated from a Notes client or Domino server after a crash. Autonomic diagnostic collection was first released with Notes and Domino 6.0.1. Be sure to take some time to understand and utilize this powerful tool.

Domino 7 includes more improvements to directories and LDAP; for example, support for Universal Notes IDs (UNIDs) through 32-character values of the new `dominoUNID` operational attribute. LDAP searches have been enhanced to work with IBM Workplace products that use the WebSphere Member Manager (WMM) service to access user/group objects. To optimize performance, Domino 7 reuses existing LDAP connections, rather than initialize and close new ones each time a user whose credentials need to be verified in the external LDAP directory tries accessing protected resources.

IPv6 protocol support has been upgraded to include additional platforms and services. CIDR format is now supported in IP address pattern strings. IOCP support in Linux Intel is included, as well as support for 1024-bit RSA and 128-bit RC2 Notes keys.

Administrators can limit how far into the future users can make reservations. Administrators can also set automatic reminder notices to be sent to the chairperson who books a particular room or resource so that if a meeting is canceled, the room or resource may be released. In addition, embedded graphics in the Description field now appear when you send an invitation through iCalendar.

Domino 7 has centralized the processing of reservations of rooms and resources into a new Rooms and Resources Manager (RNRMgr) task. This task is designed to prevent overbooking of rooms or resources, and is responsible for the processing and the workflow that is related to reserving a room or resource, as well as accurately updating the Busytyme database. (Note that this task replaces functionality that was previously

handled in multiple places such as the router, the template of the Rooms and Resources database, and the Schedule Manager.) You can rename a resource by changing its name, site, and (if the resource is of type 'other') its category.

Domino 7 also offers improvements with the Lightweight Third Party Authentication (LTPA) scheme. Domino 7 provides the ability for an administrator to configure the name that should appear in an LTPA token when a Domino server generates it. Setting up an alternative LTPA username does not require a pure Domino environment.

LEI

In Lotus Enterprise Integrator (LEI) 7, failover support in the Domino cluster environment is provided, so that if one server in a given implementation fails, activities continue processing on secondary, or subsequent, servers. The LEI administrator incorporates new functionality, such as Sametime presence awareness and form-based connection testing.

LEI 7 includes the ability to control how dependent activities are run, based on the results of the calling activity. You can also have data-management activities that use Notes connections to run under different Notes IDs.

Domino remote script-debugging will now be able to debug the scripts used in Scripted Activities. Scripted Activities now record the connections used by the scripts, providing improved serviceability.

LEI, DECS, and the LSXLC are now fully integrated into Domino's NSD services. LEI scheduling dexterity is now improved, with better handling when you need to 'Restrict to Schedule'. LEI connection documents let you directly test your connections for validity. Also, virtual documents now properly handle back-end update and deletion synchronization.

Summary

This chapter reviewed the major new features introduced in release 7, the latest version of the Notes/Domino 'franchise'. We also briefly discussed new features and functionality added to the Notes client, Domino Designer, the Domino Administrator client, and Lotus Enterprise Integrator (LEI). The following chapters in this book discuss these areas, and Domino Domain Monitoring (DDM), DB2 support, mail policies, and other enhancements, in more detail.

3

Domino Domain Monitoring

This chapter, along with the ones that follow, discusses the many new features found in the Domino 7 server. Here is a list of the features:

- Domino Domain Monitoring (DDM)
- DB2 support and administration
- Autonomic data collection
- Policy improvements, including new management features and mail policies
- AdminP enhancements
- Rename reversion
- SMTP improvements
- Client lock down
- Smart Upgrade enhancements
- Linux/Mozilla Web Administration client
- New ID and password recovery features
- CA process improvements
- Support for additional standards, including IPV6, CIDR, and IOCP
- Improvements and additions to rules, configuration, backup and restore, and server administration

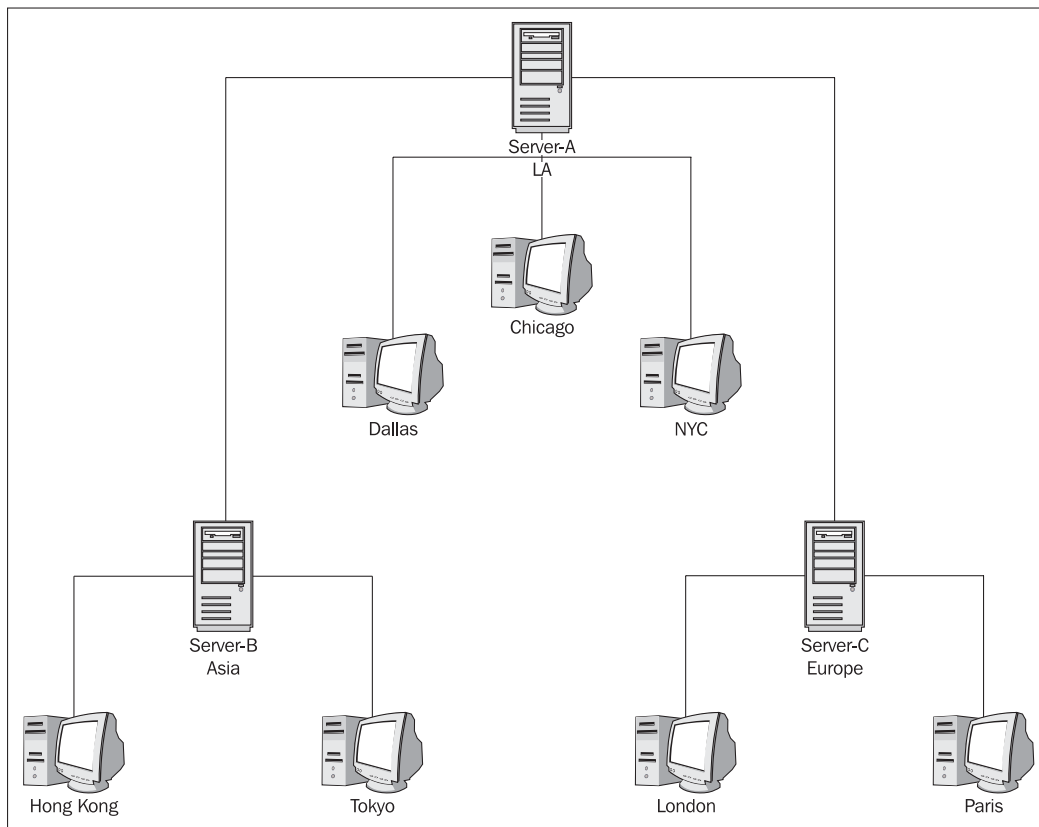
Domino Domain Monitoring (DDM)

One of the most significant new Domino 7 features—one that's gotten a lot of attention throughout the early beta programs—is Domino Domain Monitoring (DDM). This feature allows you to monitor the status of multiple servers in one or more domains, all from a single location.

DDM uses a set of preconfigured probes to gather status and process information about the servers being monitored. These probes collect data relating to applications, databases, directories, messaging, the operating system, replication, security, the server, and the Web. Special filters allow you to select the type and level of data recorded by the probes. After this data has been collected, it is consolidated, organized, and processed into easy-to-read summary reports. The data is then entered automatically into the Event Resolution Center (ERC). Each event that is processed and placed into the ERC database has a document link back to the specific monitor that generated the event. The ERC is updated with a status document each time a probe detects an error, or a particular threshold is exceeded. By viewing DDM events recorded in the ERC, you can identify (and in some cases even predict) systemic Domino events. The ERC is automatically created when you start the first server. The ERC database is based on the new template `ddm.ntf`; by default its file name is `ddm.nsf`.

By default, results generated by DDM probes are placed in the ERC on each server that runs the probes. You can create a DDM server collection hierarchy to aggregate data from several servers to a single server. By using this collection hierarchy, you can designate that a single server can collect all DDM-based event data (and thus use this single server to monitor multiple servers in your domain). Alternately, you can set up several servers to collect data across a domain.

The following figure shows how you can set up servers to collect DDM data in a worldwide domain. In this case, we use a multi-tiered collection model. The top server in our example is Server A in Los Angeles. This server collects data from itself and three other collection servers located in the USA. Collection Server B, located in a data center in Asia, collects data for itself and two other servers in Hong Kong and Tokyo. Collection Server C collects data from itself and two servers located in London and Paris.



Reported data is generated in each ERC based on its location in the collection architecture. To review data about the London server, an administrator can open the ERC on Server C, where data for the London and Paris servers is stored. It's also possible to view London data by opening the ERC on Server A, which contains all DDM data for all servers in the hierarchy.

This collection hierarchy is possible because each Domino 7 server writes its own probe results into a local ERC replica on each collection server. As a result, the ERC maintains data about its own probes as well as the probe data from every server that is monitored by this server. As you can see from the preceding figure, data is rolled up and pushed into the collection server that represents the next higher level in the tree. This process is managed by Lotus Notes **replication**. Selective replication formulas are automatically created when you create the DDM server hierarchy. Using this simple technique, you see the rolled up data where you want to see it—for instance, in the figure, data from Hong Kong exists on Server B (the Asia server) and Server A (the top-level server), but not on Server C (the Europe server).

Probes

Probes are the internal engines that make DDM work. There are nine types of probes available in Domino 7:

- **Application code** monitors an agent's schedule and resource (CPU and memory) usage.
- **Database** monitors database status and various activities.
- **Directory** monitors various directory functions.
- **Messaging** monitors the Domino-based messaging infrastructure.
- **Operating System** monitors operating system statistics and events.
- **Replication** monitors various replication activities. Replication probes can be configured to monitor all database replication, or specific databases.
- **Security** monitors the overall security of servers and databases in the domain.
- **Server** monitors the administration process for errors and reports them back to the ERC database.
- **Web** monitors web field settings and HTTP configuration fields.

Each of these probes is described in more detail later in this section.

Configuring Probes

You can select which probes you want to run, and what data these probes collect, through Probe documents. These documents reside in the Events database (events4.nsf).

Through Probe documents, you can specify when the probe runs. Many probes can be configured to run on a schedule, on an event, or real-time. The function of the probe will dictate what type of schedule can be executed. For example, if you select the Schedule option, you can choose to run the probe:

- Multiple times per day (including the time between each probe execution)
- Daily (including the days of the weeks and the time when the probe will execute)
- Weekly (including the day and time for the probe to run)
- Monthly (including the calendar day number that the probe will execute; for example, if you want the probe to run on the fifteenth day of each month, enter 15)

In some cases (for example, the Security probe), you can enable the probe to run when a particular event occurs, such as when a Person, Server, and/or a Configuration document has changed. This can provide a very quick alert back to an administrator. You can also determine how missed probes are handled—you can ignore the missed probe, run the missed probe on startup, or run it at the next time range.

One very convenient feature is the ability to assign probe events based on server type. For many probes, you can select an option called **Special Target Servers**, which offers a set of server types, including:

- The Administration server of the Domino Directory
- LDAP server
- POP3 server
- IMAP server
- SMTP server
- Mail server
- Scheduled directory catalog aggregation servers

For instance, if you select the type as mail server, the probe will run on *all* mail servers in your domain.

Filters

You can create DDM filters to control the event type and event severity of events generated inside and outside of DDM. These filters determine what data is included in the DDM log file. You can specifically include all DDM events or include/exclude specific type of events. The DDM filter is created in the events4.nsf database. After the filter document has been created, you can determine the following for each filter document:

- **Description:** Provides explanatory information about this filter.
- **Event Filter Type selection:** Offers two choices: apply filter to DDM and non-DDM events, and apply filter only to non-DDM events.
- **Event Types and Severities to Log:** Determines which event types are recorded in the ERC. You can choose to log all event types, which would record all the types of events and all severity levels shown in the following figure. Or you can choose to log selected event types. If you choose this option, you can then select the types of events and their levels of severity.
- **Servers on which the filter will be applied:** Identifies the servers on which this filter will apply. You can choose all servers in the domain, or select the option **Special Target Servers** to specify the type of server for this filter (as described in the preceding section). You can also identify individual servers by name.

The Event Resolution Center (ERC) Database

The Event Resolution Center (ERC) database (ddm.nsf) contains the data generated by active DDM probes. When a probe runs, it records all the relevant data that it finds (if any) to a report that is placed in the ERC. This report contains the results of the specific probe, the probable cause that generated the result, suggested solutions for each event, and a link to the probe that was used to generate this event.

The ERC includes seven navigator views and a link to events4.nsf. Each view can help you find and/or diagnose a particular problem. The views are as follows:

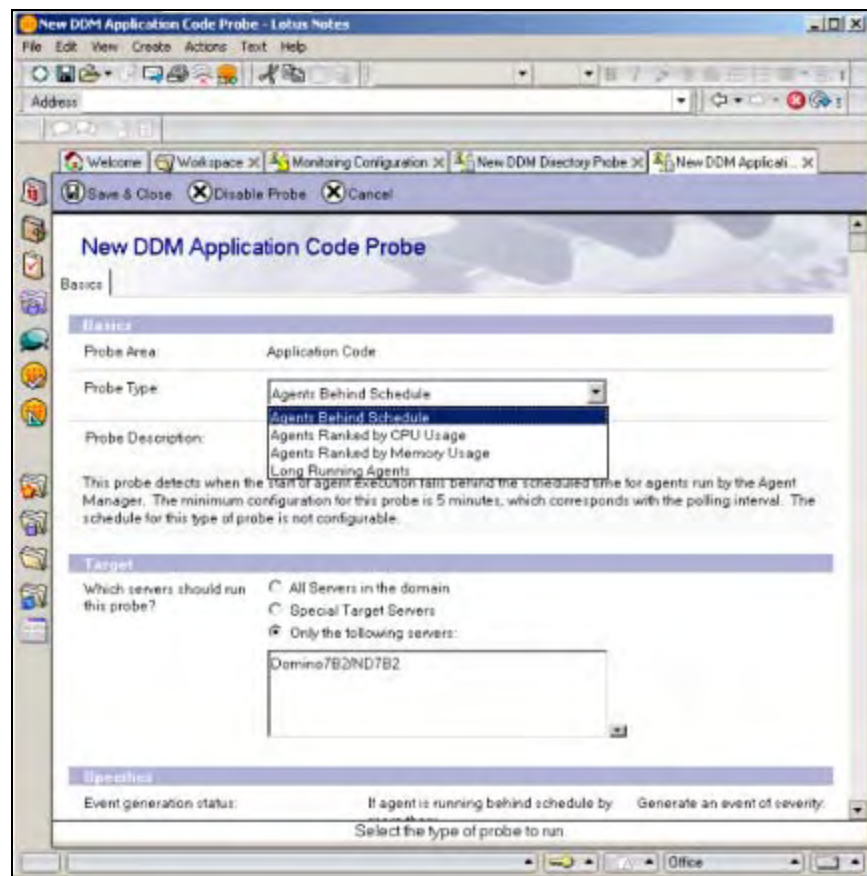
- By Severity shows a list of probe results documents organized by severity level (Fatal, Failure, Warning (high), Warning (low), and Normal).
- By Type shows the probe results by the probe type (Application Code, Messaging, and so on).
- By Server displays results based first on the domain names, and then by a list of servers that the probes reported on.
- By Date shows all probe events in chronological order.
- By Assignment provides you with the ability to assign events to people and/or groups.
- My Events shows the events that are assigned to your username. This is a formula-based view (@Name([Abbreviate]; @UserName).
- Open Monitoring Configuration provides a link to events4.nsf.

Types of Probes

As we mentioned earlier, there are nine types of probes. You select the type of probe you want to create in the Probe document:

Application Code

This probe monitors an agent's schedule and resource usage. It also checks for agent-related conditions and events such as agents that are disabled by the design server task, agent security errors, and agent full-text index errors resulting from search operations.



Database

The Database probe monitors database status and activities such as database compacting errors and design errors, as well as status on the ability to actually open this database. This probe has four different probe types that you can enable:

- Compact reports errors about the status of many server-based database compaction activities.
- Design reports any errors that occur during the design process.
- Error Monitoring is a very powerful database probe type. This monitors a number of database activities, including the internals of the **Notes Storage Facility (NSF)** and the **Notes Indexer Function (NIF)**. The following screen shows the configuration document for this probe option:

The screenshot shows the 'Domino Domain Monitoring' configuration window. It has three main sections: 'Basics', 'Target', and 'Specifics'.
 - In the 'Basics' section, 'Probe Area' is set to 'Database'. 'Probe Type' is set to 'Error Monitoring'. 'Probe Description' includes a text box with the following text: 'This probe monitors key locations in the database software layer (NSF/NIF) and generates event documents for any errors that occur. Because some errors occur naturally, an error exclusion list can be configured using this probe. The schedule for this type of probe is not configurable.'
 - In the 'Target' section, under 'Which servers should run this probe?', the radio button 'Only the following servers:' is selected. Below it, a text box contains 'Domino7B2/ND7B2'.
 - In the 'Specifics' section, 'Severity' is set to 'Warning (high)'. At the bottom, there are two buttons: 'Add Error Codes To List' and 'Remove Error Codes from List'.

Note the option to remove error codes from the list of errors that are to be recorded. By default, a number of error codes are automatically ignored, such as "Document has been deleted", "Entry not found in index", "File does not exist", and so on.

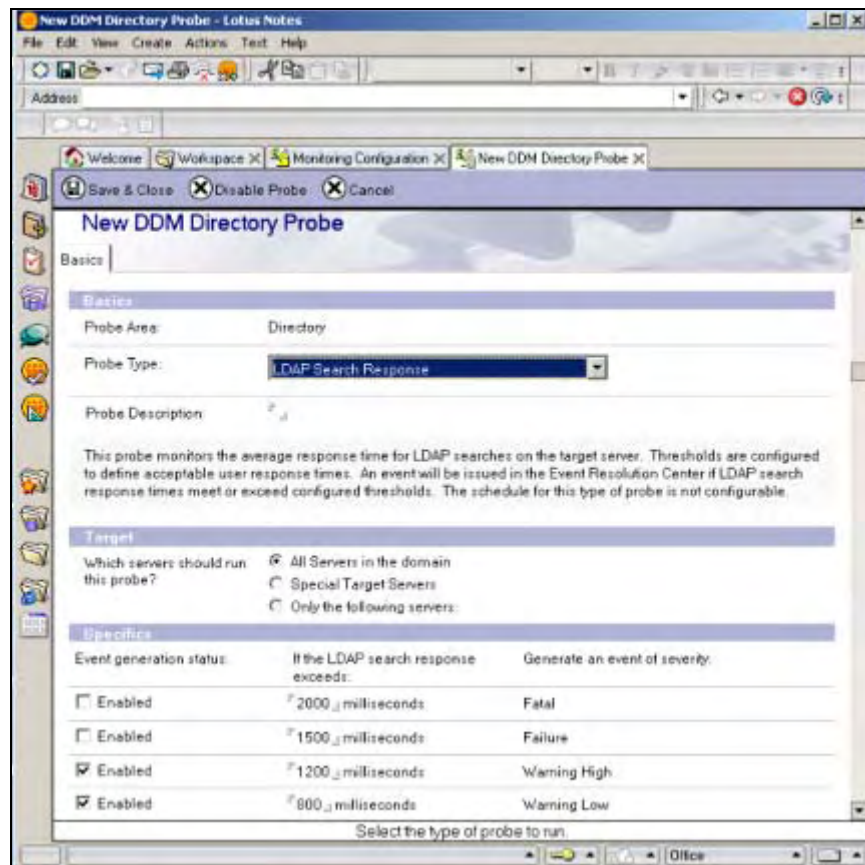
- Scheduled Database Checks 'pings' each database to check whether the selected database can be opened. Additional options for this include the ability to check for unused space in the targeted database and for any database inactivity.

Directory

The Directory probe is one of our favorites. This powerful probe monitors many different directory functions:

- Directory Availability monitors the availability of all directories being hosted and then reports any identified errors. The directories that are monitored can include the primary Domino Directory (names.nsf), Domino configuration directories, directory catalogs, directories enabled via directory assistance, and LDAP directories.

- Directory Catalog Aggregation Schedule monitors the scheduling of the Directory Catalog. The Directory Catalog is maintained by the DirCat Domino server tasks. This option monitors the schedule status of the task looking for scheduling elements, including missed directory aggregation and any aggregations that are taking too long to process.
- Directory Catalog Creation monitors the server-based DirCat Directory Catalog task process that creates the directory catalogs. This helps you take quick action to get this task back online.
- Directory Indexer Process State monitors the running status of the Directory Indexer.
- LDAP Process State monitors the status of the LDAP Domino server task.
- LDAP Search Response monitors the server's average search response time for LDAP searches. This can be configured via a set of thresholds. The following figure shows that there are four different events that can be generated based on each threshold, Warning Low, Warning High, Failure, and Fatal:



- LDAP TCP Port Health monitors the TCP port response for both the standard LDAP TCP port (389) and the LDAP-SSL port (636).
- LDAP View Update Algorithm monitors the algorithms that are used to update the LDAP server directory views. This algorithm can be tuned by using the LDAPBatchAdds NOTES.INI setting.
- NAMELookup Search Response monitors the average search response time of directory NAMELookups performed on the Domino server.
- Secondary LDAP Search Response monitors the average search response time of searches of secondary LDAP servers that are performed on the probed server.

Messaging

The Messaging probe monitors the Domino-based messaging infrastructure. Features include the ability to monitor SMTP activity, Notes (NRPC) mail routing, and various mail-routing statistics. There are currently ten options that you can choose from:

- Mail DSN tests the SMTP mail flow using a Delivery Status Notification (DSN) technique. This can help you determine whether a particular site is online. This can be effective if the target domain supports DSN extensions.
- Mail Flow Statistic Check uses a metric known as the 'slack percentage' to monitor a series of messaging-based statistics, including Mail.Total.Pending, Mail.Dead, Mail.Held, and Mail.Waiting. This lets you monitor the quantity of mail moving through the Domino server. The slack percentage is a representative indication of how the router is processing mail.
- Mail Reflector provides a mechanism to test mail flow to a variety of mail systems. You specify a mail recipient as part of this configuration, but you also will need to configure the recipient to send the message back to the originating server. One method is to enable auto-forward messages from the mail recipient to an ISpy mail-in database on the server that is executing the probe.
- Message Retrieval Process State verifies that the IMAP and POP3 server tasks are executing properly on the server being probed.
- Message Retrieval TCP Port Health monitors the Domino Internet Message Access Protocol (IMAP) and Post Office Protocol (POP3) messaging protocols, and reports service status on each process. Additional options include the ability to monitor POP3SSL and IMAPSSL.
- NRPC Routing Status tests the status of the Notes NRPC mail router by placing a message in the mailbox. This message will then route to a mail-in database. This can report status based on a set of thresholds.

- Router Process State monitors the status of the Domino router server task.
- SMTP Process State monitors the status of the Domino SMTP server task.
- SMTP TCP Port Health verifies that the SMTP mail routing services are working correctly.
- Transfer Queue Check tests SMTP- and/or NRPC-based mail to individual destinations. This can be configured via a set of thresholds and can report when messages are not being delivered.

POP3 is defined in RFC-1725, and IMAP4 is defined in RFC-1730.

Operating System

One of the many challenges that an administrator must deal with is the status of system resources. Operating System probes provide a mechanism to alert you about potential problems at the OS level. There are four types of Operating System probes that you can enable: CPU, Disk, Memory, and Network.

- CPU monitors the CPU performance status on a variety of operating systems. The following operating systems and statistics can be monitored:

OS	Statistics monitored
AIX	Processor utilization percentage Processor queue length
zOS	Processor utilization percentage
Linux, zLinux	Processor utilization percentage
Solaris	Processor utilization percentage Processor Queue Length
OS400	Processor utilization percentage
Windows	Processor utilization percentage

Each selection can be configured with a high/low threshold based on each statistic percentage.

- Disk monitors and analyzes disk activity on each Domino server. The following table shows operating systems and statistics that can be monitored:

OS	Statistics monitored
AIX	Disk utilization percentage
Linux, zLinux	Disk utilization percentage Disk Service Time (ms)
OS400	Disk utilization percentage
Solaris	Disk utilization percentage Disk service time (ms)
Windows	Disk queue length

- Memory monitors and analyzes memory performance on each Domino server:

OS	Statistics monitored
AIX	Scan rate
OS400	Fault rate formula
ZOS	Available frames Out ready queue length Paging rate
Solaris	Scan rate
Windows	Available physical memory (MB)

- Network monitors and analyzes network performance on each Domino server:

OS	Statistics monitored
AIX	Network bandwidth utilization percentage Network collision rate percentage
Linux; zLinux	Network collision rate percentage
OS400	Network bandwidth utilization percentage
Solaris	Network bandwidth utilization percentage Network collision rate percentage
Windows	Network bandwidth utilization percentage

Replication

The Replication probe lets you monitor various replication activities within your Domino domain. Replication probes can be configured to monitor all database replication, or

replication on specific databases. There are two options available with this probe: Errors and Replication Check.

- Errors monitors replication events for errors. Any errors found are captured in a report that can include a document link for any document that did not replicate. There are several associated configuration settings that you can enable, including:
 - Which servers should run this probe?
 - Which servers should be probed?
 - Select one or more databases to probe:
 - Select one or more databases not to probe:

You can also monitor push- and/or pull-type replication events.

- Replication Check monitors specified database replication activities. Previous releases of Domino offered similar functionality, but this included replications, which resulted in the replication history being updated. Therefore, only successful replications were indicated. This new probe type takes null replication into consideration. You can enable the same configuration settings that you can with the Errors probe type, described in the preceding paragraph. In addition, you can generate an event if the included databases have not replicated within the following interval, and choose to attempt to diagnose problems:

Replication Probe: DADN-6AB3VT

Basics | Schedule

Basics

Probe Area: Replication

Probe Type: Replication Check

Probe Description: asdl

This probe monitors configured database(s) to ensure that replication occurs on the target servers within the configured time interval. database has not replicated within the configured time interval, it will generate an event in the Event Resolution Center database. **Note:** This probe takes into account replication attempts which did not actually replicate notes (i.e. databases which are up to date).

Target

Which servers should run this probe? All servers in the domain

Which servers should be probed? All servers in the domain

Select one or more databases to probe: All Databases

Select one or more databases not to probe:

Specifics

Severity: Warning (high)

Generate an event if the included databases have not replicated within the following interval: 6 Hours

Check the following: ☒ Push

Security

You can create a Security probe to assess the overall security of servers and databases in your domain. A Security probe can identify a security-related server configuration problem and/or security issues with specific databases.

One significant variable with security probes is how the event severity is assigned. Severity is assigned during runtime and is calculated based on the number of various potential issues found. This severity is a percentage-level score that is generated for each Server Configuration document analyzed. (Consult the product documentation for details about how these percentages are calculated.) The basic percentages are shown in the following table:

Probe percentage	Severity level
0.00	Normal
< = 50%	Warning (low)
> 50%	Warning (high)

There are five Security probe types: Best Practices, Configuration, Database ACL, Database Review, and Review.

- **Best Practices** compares a set of baseline security configuration settings to the existing configuration in a Notes domain. You can modify the default values assigned to the security configuration. The following options are available for the Best Practices probe type:
 - Compare Notes public key against those stored in directory
 - Check password
 - Allow anonymous Notes connections
 - Required change interval
 - Check passwords on Notes IDs
 - Check for existence of ID file in the person document
 - Internet authentication
 - Check the security of SSL settings
 - Check the security of Web settings
 - Check the security of Domino Directory settings
 - Check the security of Mail settings
 - Check the security of DIIOP settings
 - Check the security of the Remote Debug Manager

- Use more secure internet passwords
- Security settings in my Configuration document
- Internet password
- Verify all Server Document Security Tab sections. (This includes the Admins, Program, Web, Security Settings, Server Access, and Passthru Use sections.)

Security Probe: TSPD-67MPKD

Basics | Specifics | Schedule

Basics

Probe Area: Security

Probe Type: Best Practices

Probe Description: The probe...

This probe can be configured to audit various security settings found on Server documents, Server Configuration documents, and Person documents. A best practices probe will review & analyze key fields in these documents and generate detailed reports, recommending settings that might improve Security for the configured areas.

Targeted

Which servers should run this probe?

☐ All Servers in the domain

☐ Special Target Servers

☒ Only the following servers:

Domino7B2ND7B2

Which servers' security configurations should be probed?

☐ All Servers in the domain

☒ Only the following servers:

Domino7KGFND7B2

Select one or more databases not to probe: TheBlastFishingDatabase.nsf

Basics TAB

- Configuration compares a known 'good' Domino server document and a target server document, and then reports any differences or discrepancies. This type of security probe also has a Specifics section that you can configure. This allows you to compare a known good server configuration to the server being probed. Options include:
 - Which server should be used as the guideline server?
 - Which server settings should be compared to the guideline server's settings? You have several options here: Directory Profile Note, Security settings in the Server Configuration document, Server document (all sections or individual sections such as Admins, Program, Web, and so on).
- Database ACL monitors the Access Control List (ACL) of individuals and groups in various databases. You can set this up to monitor specific databases and list access levels in the probe configuration document. You can also

check the access level status of any particular group. For instance, suppose you have a group known as 'External Contractors'. This group needs access to the 'Bass Fishing' Database with read-only access. You can configure a probe to monitor this critical database and report whether this group has been given an access level greater than Reader. This particular probe has the ability to monitor all basic ACL access levels, including Designer, Editor, Author, Depositor, Reader, and Default.

- Database Review is the 'inverse' of Database ACL. This monitors changes in access levels for all ACL members against a specific ACL level. You can create a probe and then select a database for it to monitor. You can then select a base level to monitor, for example review all ACL members whose privileges are equal or greater than Editor. You can also select one of the following parameters:
 - Review the following database properties: enforcing consistent ACLs across replicas, enabling of extended ACLs, encryption settings, and the Administration server of the database.
 - Review agents defined as restricted or unrestricted.
- Review creates a report on the security settings specified in the Specifics tab of the Security Probe document. You can select the same settings available for the Configuration type of security probe.

Server

The Server probe monitors the administration process for errors, and reports the errors back to the ERC database. The following administration requests can be monitored:

- Change HTTP password in Domino Directory
- Change user password in Domino Directory
- Initiate rename in Domino Directory
- Initiate web user rename in Domino Directory
- Recertify Certificate Authority in Domino Directory
- Recertify Cross Certificate in Domino Directory
- Rename in person documents
- Rename person in calendar entries and profiles in mail file
- Rename person in Domino Directory
- Rename web user in Access Control List
- Set Password Information

Web

The Web probe monitors Web-related statistics and events. You can select from two probe types, Web Best Practices and Web Configuration:

- Web Best Practices monitors HTTP configuration fields in the domain by comparing these fields to recommended base 'best practices' values. Fields that don't match these values are recorded in a report in the ERC database. This allows you to:
 - Verify that server is using the most current web server configurations
 - Verify basic web server configuration settings
 - Verify web server performance settings
 - Verify web server debug-log settings
 - Verify web server security settings
- Web Configuration monitors web field settings in relation to a base configuration document. As with Web Best Practices, settings that do not match the base configuration are reported to the ERC. The settings you can monitor are similar to Web Best Practices settings.

After you open the configuration setting for a Web probe, you will notice that you cannot assign severity levels. The severity of an event generated by Web probes is determined using a percentage formula. This score is based on the number of potential problems that are found. After this calculation is complete, a 'severity percentage score' is calculated and logged to the ERC.

Event Notification Using an Agent

Domino has the ability to monitor and execute specific actions based on a large variety of events. These events can be the results of normal processing activities or can be error-type events. Event examples include:

- AdminP
- Agent
- Comm/Net
- Compiler
- Database
- Directory (LDAP)
- Mail

- Misc
- Monitor
- Network
- News (NNTP)
- Replica
- Resource
- Security
- Server
- Statistic
- Update
- Web (HTTP/HTTPS)

With Notes/Domino 7, the Domino administrator now has several new options that can be triggered by an event. When an event takes place, an administrator now has the option to run an agent, run a program (with new parameters), send a console command to the server, or send a Java controller command.

Domino 7 includes processes called 'event generators'. These generators gather information by monitoring Domino tasks and statistics. Also, there is a built-in probing system that can be enabled and linked into the event generators. Specific conditions and/or thresholds can initialize event generators. Once an event generator has been started, it can pass data into the event monitor task. The event monitor task can be loaded manually at the Domino server console, or can be set to load each time the server is started via the `NOTES.INI` file, in the `servertasks` line. Once the event has been passed into the event monitor task, it will be processed against event handler configuration documents in the `events4.nsf` database. If there are no configuration documents defined, then no actions are executed when an event is passed into the event handler.

The Domino Administrator includes a set of default event generators; these are shown in the Event Generators view of the Monitoring Configuration database (`events4.nsf`). The following table lists the types of event generators that can be created:

Event generator	Description
Database event generator	Monitors database activity and free space. Monitors frequency and success of database replication. Reports on ACL changes, including those made by replication or an API program.
Domino server response event generator	Checks connectivity and port status of designated servers in a network.
Mail routing event generator	Sends a mail-trace message to a particular user's mail server and gathers statistics indicating the amount of time, in seconds, it takes to deliver the message.
Statistic event generator	Monitors a specific Domino or platform statistic.
Task status event generator	Monitors the status of Domino server and add-in tasks.
TCP server event generator	Verifies the availability of Internet ports (TCP-based services) on servers and generates a statistic indicating the amount of time, in milliseconds, it takes to verify that the server is responding on the specified port.

Each event document can have a severity assigned. The severity levels can be assigned to each event as needed. Examples of these are shown below:

Severity level	Meaning
Fatal	Imminent system crash
Failure	Severe failure that does not cause a system crash
Warning (high)	Loss of function, requiring intervention
Warning (low)	Performance degradation
Normal	Status messages

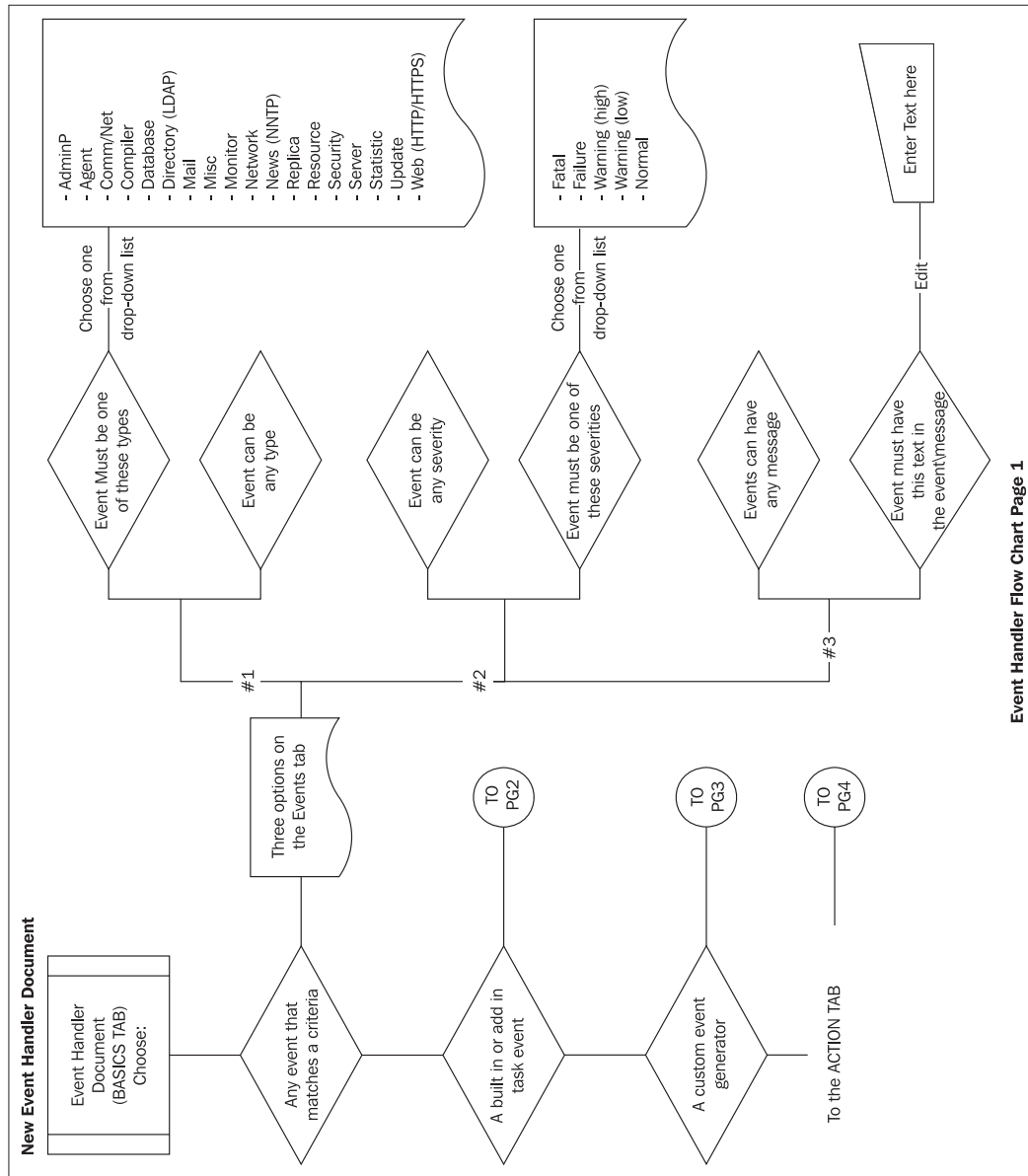
To create a new event, just open the events4.nsf and select New Event Handler. The following screenshot shows how this looks:

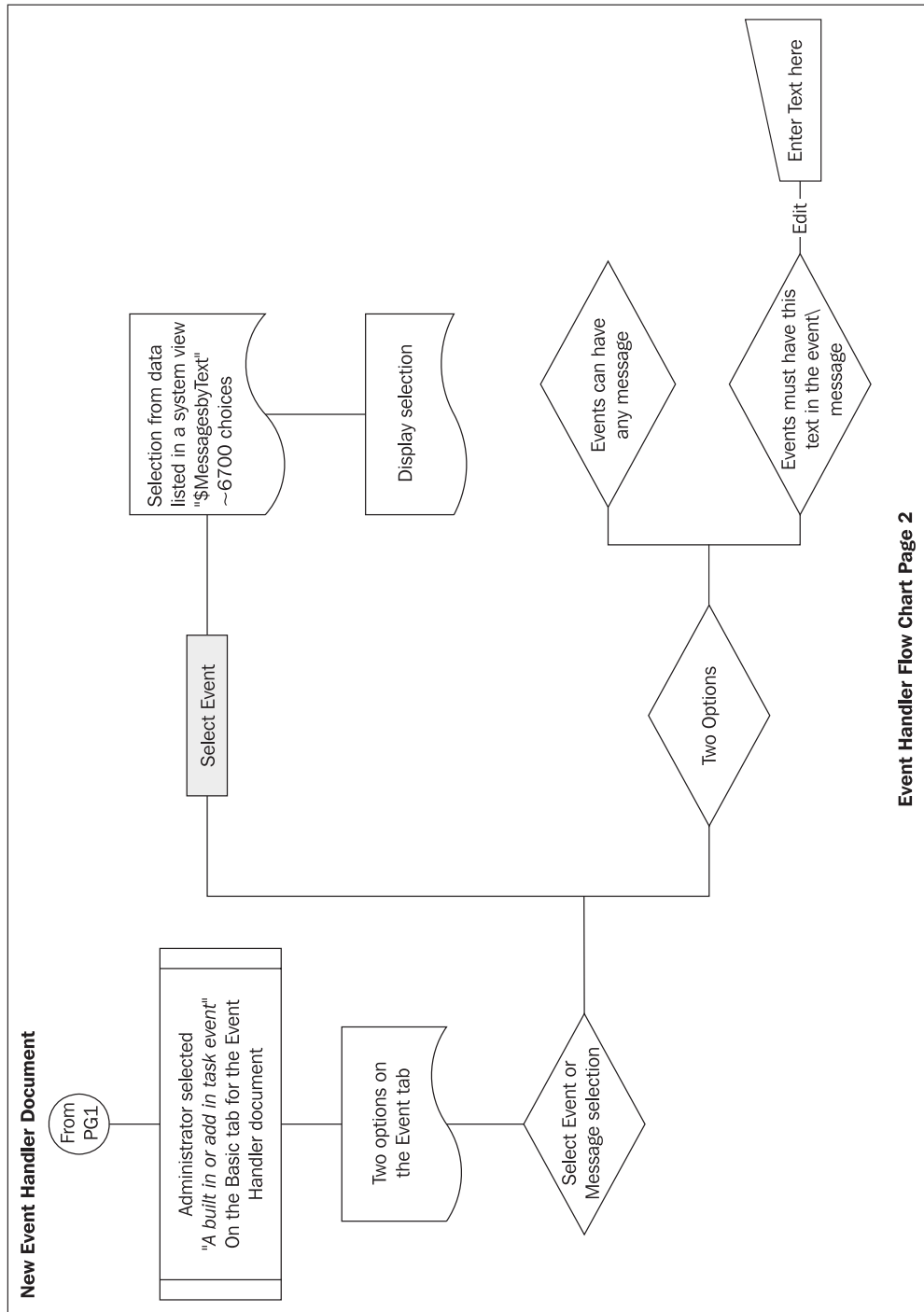
The screenshot shows a dialog box titled "Event Handler" with a subtitle "Created: 08/27/2005". At the top, there are buttons for "Save & Close" and "Cancel". Below the title bar, there are three tabs: "Basics", "Event", and "Action", with "Basics" being the active tab. The "Basics" tab contains two main sections. The first section, "Server(s) to monitor", has two radio button options: "Notify of the event on any server in the domain" (which is selected) and "Notify of the event only on the following servers:". The second section, "Notification trigger", has a label "Trigger:" followed by three radio button options: "Any event that matches a criteria", "A built-in or add-in task event" (which is selected), and "A custom event generator".

There are three tabs: Basics, Event, and Action. The Basics tab provides two basic sections: Server(s) to monitor and Notification trigger. The first section is where the servers to monitor are set. The second section has three choices:

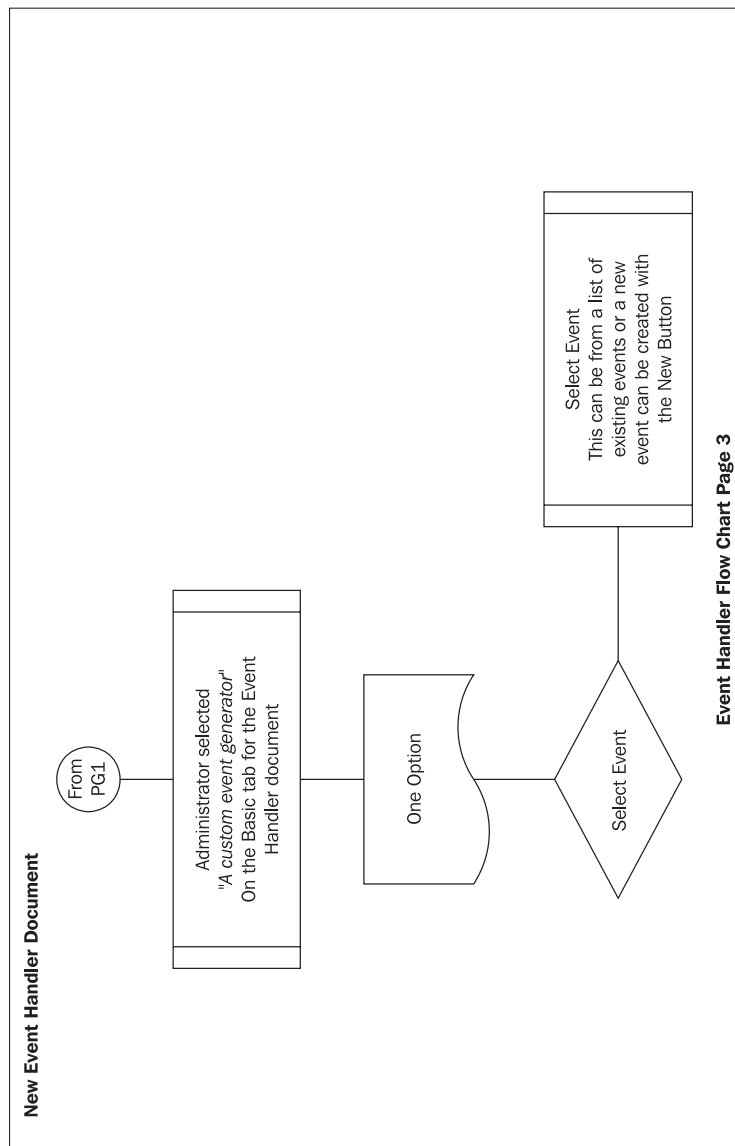
- Any event that matches a criteria
- A built in or add in task event
- A custom event generator

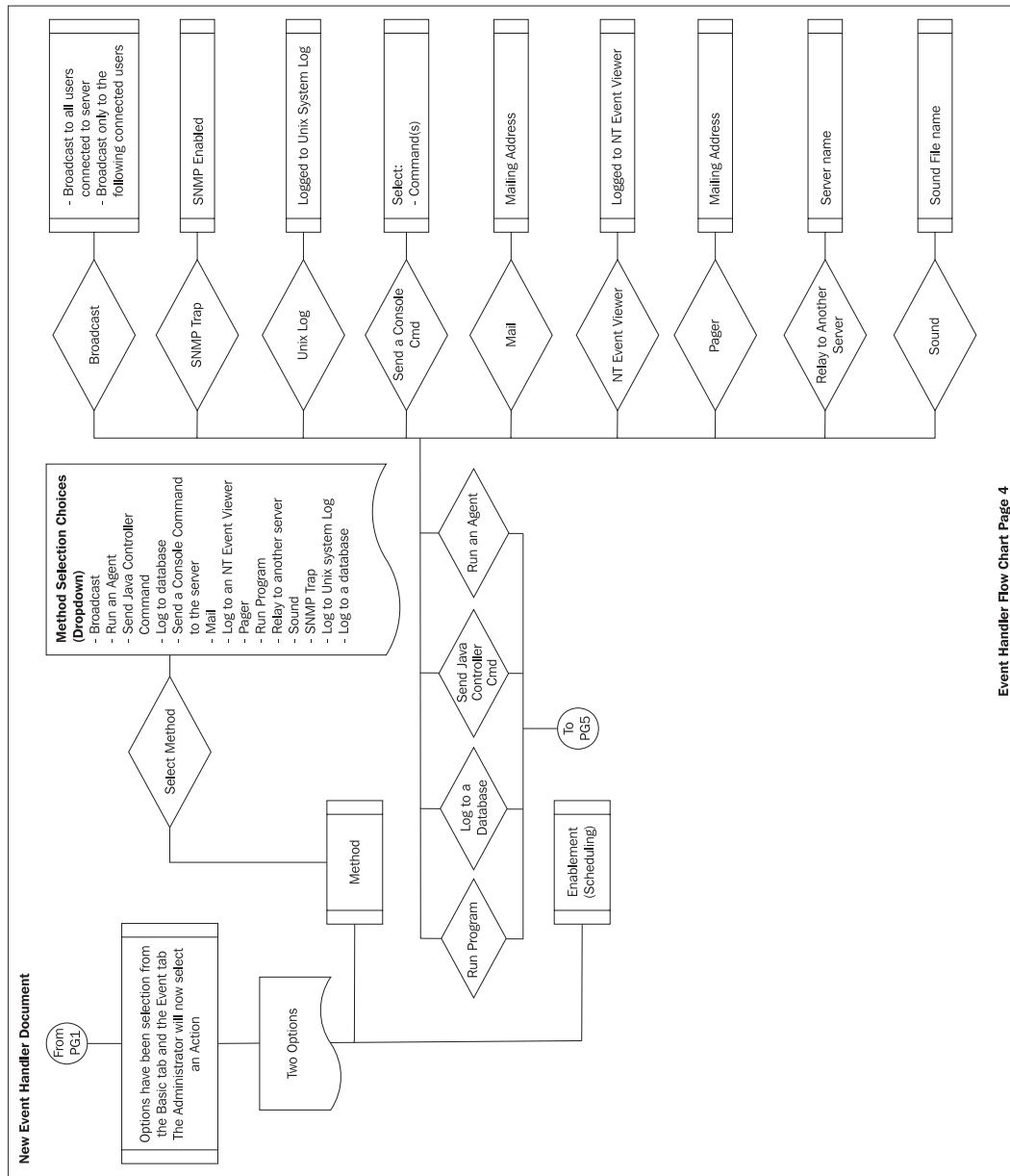
Each choice will display additional choices on the Event tab. The following illustration shows these choices:

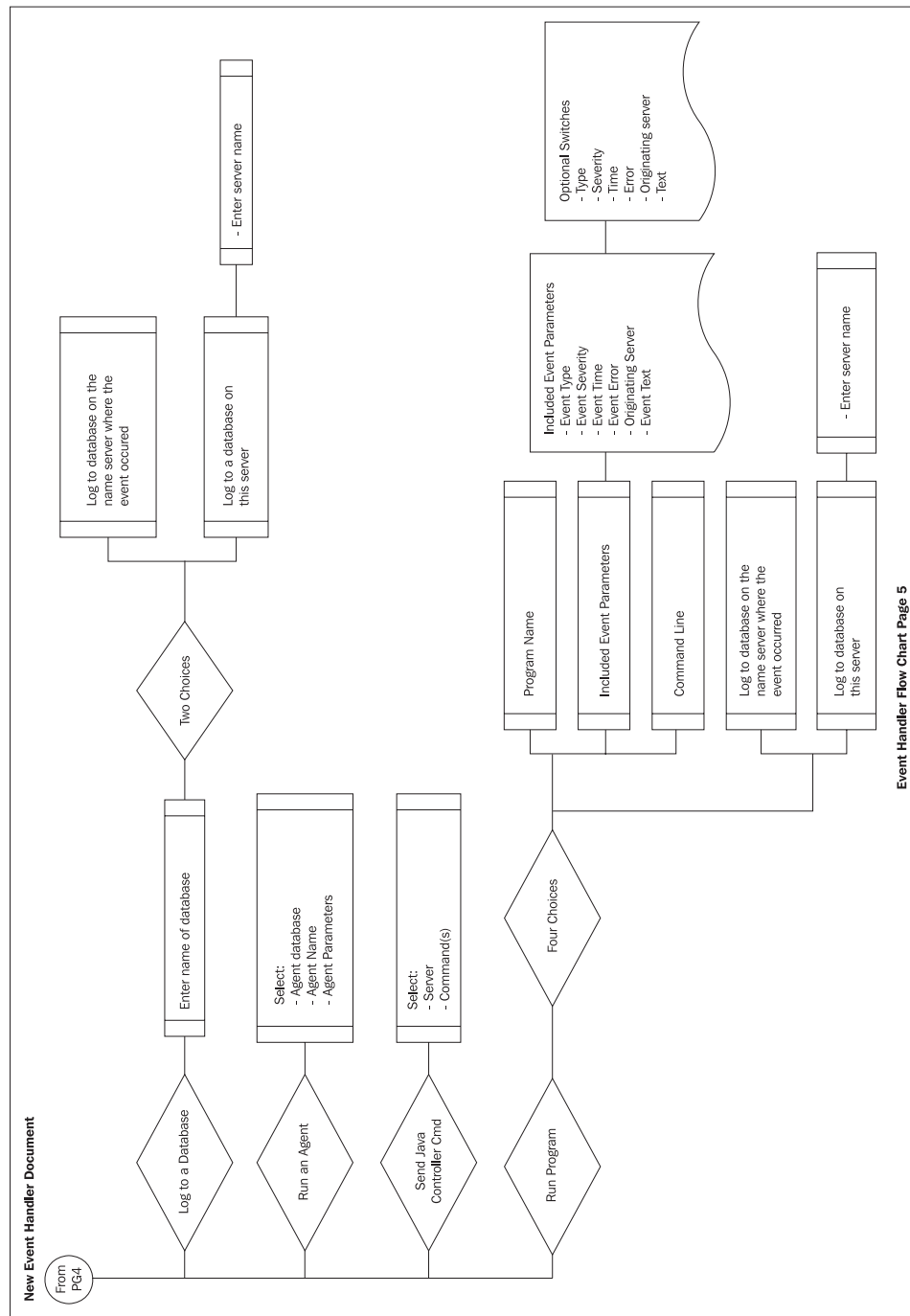




Event Handler Flow Chart Page 2







The administrator can create an event handler document to specify how to log the event to a specified destination. Also, administrators can prevent events from being logged or handled in any circumstance.

At this point, you might be asking, "What is this scripting stuff that I keep hearing about?" Let's start with an example and a goal. The goal is to send a notification and track ACL notifications in a log database. Use the following steps:

1. Create a tracking database.
2. Create a simple agent, view, and form in the tracking database.
3. Create a database event generator document in events4.nsf.
4. Create an event handler (run an agent).
5. Enable the event handler and the event generator.

Create a Tracking Database

Overall, almost any database format will work. Once the database has been created, you will need to create a form, agent, and a view.

Create a Simple Agent, View, and Form in the Tracking Database

The form can have the following fields defined:

Field name	Field Data Type	Field Description
EventText	TEXT	Text of event
TargetServer	TEXT	Target server for this event
EventTime	TIMEDATE	Time and date stamp of event
EventType	NUMBER	Type of event
EventSeverity	NUMBER	Severity of event
EventPrms	TEXT	Text parameters in event
ErrorCode	TEXT	Event type error code
OriginatingServer	TEXT	Server that originated the event
EventSeverityText	TEXT	Textual representation to Severity
EventTypeText	TEXT	Textual representation to Type

Here's a screenshot example of a form:

Event Results from Event Agent	
Event Information for server = <input type="text" value="OriginatingServer_1"/>	
Event Severity Data:	<input type="text" value="SeverityText T"/> <input type="text" value="EventSeverity T"/>
Time of Event:	<input type="text" value="EventTime T"/>
Target Server	<input type="text" value="TargetServer T"/>
Event Parameters	<input type="text" value="EventPrms T"/>
Target Database	<input type="text" value="TargetDatabase T"/>
Event Severity Text / Type:	<input type="text" value="EventSeverityText T"/> / <input type="text" value="EventTypeText T"/>
Event Type error code	<input type="text" value="ErrorCode T"/>
Event type name:	<input type="text" value="EventType T"/>
<div>Event Informational Text</div> <input type="text" value="EventText T"/>	

Create a default view as well. Any view will do; you can customize it as you like.

Next up is the agent. Below is a sample agent that you can base your agents on. Name the agent EventAgent. This agent uses the DocumentContext method. This method is a Read-only property. Basically, an in-memory document is created when an agent starts. This method is defined in the NotesSession class, and uses NotesDocument as its data type.

The basic syntax for the DocumentContext is:

To get: `Set notesDocument = notesSession.DocumentContext`

```
Sub Initialize
    Dim session As New NotesSession
    Dim doc As NotesDocument
    Set doc = session.DocumentContext
    Print "Event Text = " & doc.EventText(0)
    Print "Event Error Code = " & doc.ErrorCode(0)
    ' Document Information
    Call doc.Save(True, True)
    Set db = session.CurrentDatabase
    Set tardoc = db.CreateDocument
    tardoc.form = "EventForm"
    tardoc.Subject = "Event Information"
    tardoc.EventText = doc.EventText(0)
    tardoc.EventPrms = doc.EventPrms(0)
    tardoc.ErrorCode = doc.ErrorCode(0)
    tardoc.EventSeverity = doc.EventSeverity(0)
    tardoc.EventSeverityText = doc.EventSeverityText(0)
```

```

tardoc.EventTime = doc.EventTime(0)
tardoc.EventType= doc.EventType(0)
tardoc.EventText = doc.EventText(0)
tardoc.EventTypeText = doc.EventTypeText(0)
tardoc.OriginatingServer = doc.OriginatingServer(0)
tardoc.EventErrorcode = doc.errorcode(0)
Call tardoc.Save( True, True )
Print "Agent Complete ! ! ! "
End Sub

```

Don't forget to:

- Sign the agent
- Add the correct permission into the security document in order for the agent to run
- Make sure the events process is loaded on the server

Create a Database Event Generator Document in events4.nsf

Open the events4.nsf database on the server and select New Database Event Generator. Enable the event generated to monitor ACL changes for names.nsf. Here's an example screenshot:

Save & Close Cancel

Database Event Generator

Event Number: TSPD-6FR4CG

Basics Other

Database to monitor

File name: names.nsf

Server(s):

☐ All in the domain

☒ Only the following:

Enter a servername here

What to monitor

☒ Monitor ACL Changes:

☐ Monitor replication:

☐ Monitor unused space:

☐ Monitor for user inactivity:

Notice the TSPD-6FR4CG string in the screenshot. You will see a similar string, and it can be used as a reference point for the event handler.

Create an Event Handler (Run an Agent)

In `events4.nsf`, you can also create the event handler document. Using the flowchart as a reference, select **New Event Handler**. We'll now take a look at the changes/settings to be made.

Basics Tab

Select and complete the following fields (refer to the first screenshot under the *Event Notification Using an Agent* section):

- Notify of the event only on the following servers
- A custom event generator

Event Tab

Select the event using the reference string from the event generator. Once this is selected, you will be able to see details on that document.

Action Tab

Select **Run an Agent**. Complete the following fields:

- Agent Database (use the name of your new database)
- Agent Name: EventAgent (from the preceding example)
- Agent Parameters (any specific parameters and/or field names from your form)

Enable the Event Handler and the Event Generator

On the Action tab, enable the event handler and set a schedule if needed.

Testing

It is now time to test your event handler, agent, and event generator. Open the `names.nsf` database on the server where you have enabled each of the event handlers and the generator. Make a simple change to the ACL of the `names.nsf` database. As soon as this happens, you should see a display on the server console and a document created in your database. An example is shown in the following screenshot:

Event Results from Event Agent	
Event Information for server = Domino7NSF/ND7B2	
Event Severity Data:	3
Time of Event:	11:03:51 PM Yesterday
Target Server	
Event Parameters	
Event Severity Text / Type	Warning (high) / Security
Event Type error code	Event Monitor0x33A3
Event type name:	2
Event Informational Text	
The ACL in database names.nsf has been changed by Tim Speed/Dallas/IBM.	

Summary

In this chapter, we have taken a detailed look at Domino Domain Monitoring (DDM), one of the major new administration features introduced in Domino 7. We reviewed the set of pre-configured probes that gather status and process information (applications, databases, directories, messaging, the operating system, and so on) about the servers being monitored. We discussed the Event Resolution Center (ERC), where processed events are placed. We also talked about event monitoring, Domino 7's ability to monitor and execute specific actions based on a large variety of events. These events can be the results of normal processing activities and/or error-type events. The next chapter discusses the Administration process.

4

AdminP

The Administration process (commonly called AdminP) contains seven basic components:

- The AdminP server task
- The Lotus Notes 7 Administration client (Notes and/or Web)
- End user Notes client(s)
- Domino Directory (names.nsf)
- Certlog.nsf
- Admin4.nsf
- Administration server assignments on each database (including mail files)

Each of these is described in more detail in the following sections.

AdminP Server Task

The AdminP server task runs on all Domino servers. This task loads when the Domino server is started, and is controlled through the NOTES.INI variable ServerTasks. This variable lists the AdminP server task, along with other server tasks. After it is loaded, the AdminP server task will continuously process all AdminP-related activities.

Each AdminP action is controlled via a **proxy action**. AdminP-related commands are placed into the admin4.nsf database. Each proxy action is represented in admin4.nsf as a document (and in some cases a corresponding response document). The proxy action is displayed in each document in the Proxy Action field.

AdminP requests are not limited to a single Notes domain. Cross-domain documents can be enabled to share some of the AdminP actions between domains.

Administration Client

The Administration client includes all of the tools needed to manage the AdminP environment. These tools include processes to rename and delete users, delete replicas, move databases between servers, and much more.

Notes Client

Starting with Lotus Notes 5 and 6, the Notes client became a more active participant in server administration. This trend continues in Notes/Domino 7, as Domino administrators can now lock-down client features with the Notes 7 client.

Some examples of the symbiotic relationship between AdminP and the Lotus Notes client include:

- User renames
- X.509v3 certificates pushed into the client Lotus Notes ID file
- Calendar ACL delegation
- Moving users from one server to another
- Synchronization of the Lotus Notes ID file and the HTTP password

Domino Directory

The Domino Directory provides some of the processing that is used with AdminP. One example is when a user is renamed and certificate information is changed. Part of this particular process is to store the changed certificate in a Person document in the Domino Directory. You can view the changed information indicated in the Person document under the Change Request field. Also, you will notice that each person's name is stored in various fields in the Person document. As a result, when a user is renamed, both the old name and new name are stored in the Person document. Part of the AdminP process is also controlled by the Server document; each and every Server document has a section on AdminP parameters.

A number of AdminP commands impact on Domino Directory information such as:

- Resource names
- Clusters
- Person documents, including client information
- HTTP password synchronization
- Group updates and deletions
- Server information (protocol and version)
- Policies
- CA configuration
- License tracking

Certification Log

Another important part of the AdminP process is the **Certification log**. This log database (certlog.nsf) is created when you install the first server in a Domino Domain. This log records certification-related activities from Domino, including new user and server registration, user re-certifications and renames, as well as moving users from one organization-level certifier to another. AdminP requires a Certification log on each server used to initiate administration requests. Domino administrators can place a replica copy of this database on each server as needed.

admin4.nsf

By default, the admin4.nsf database contains all the administrative requests from a single domain. Every request, via proxy actions, is placed into admin4.nsf. This database should be replicated to each server.

Administration Server

Every database must have an Administration server assigned to it. This assignment is part of the database's ACL. The Administration Server field instructs AdminP where to update each database. The Administration server appears in the ACL with a 'key' icon next to its name. Each Domain will have a single Administration server that is assigned to the Domino directory. To set the Administration server for a database (including the main Domino Directory server), highlight the database and select File | Database | Access Control, and click Advanced.

By design, only one server is allowed to update (via replica ID) any single application. As a result, you will need to add an Administration Server entry for *every* database in a Domino environment. This looks like a big task, but don't panic; there are a number of ways you can do this:

- **Manually:** Open the Advanced section of the ACL dialog and edit the Administration Server field. This works fine for one or two databases, but in large environments, this obviously would take a very long time.
- **Via the Administration client (Notes or Web):** The Administration client allows you to set individual databases or a large group of databases with a single operation. Open the Administration client and select the databases that need to be updated. Click the right mouse button and select Access Control | Manage. This opens the standard ACL dialog box. Edit the ACLs as needed and save the entry. This updates the Administration Server setting on all selected databases.

- **Via LotusScript:** The NotesACLEntry class has a Read/Write property that you can use in a LotusScript agent. Using the ISAdminServer property, you can create a simple agent that will read and/or set the Administration server of an ACL entry.
- **Via the Lotus Notes API:** You can create your own custom tools to edit and manage the Administration server name of a database. Two functions commonly used for this are ACLGetAdminServer and ACLSetAdminServer.
- **Using external vendor tools:** There are many different vendor tools that include Administration server management features. Check with your vendor for details.

Proxy Actions

As mentioned previously, AdminP works off a set of fields known as **proxy actions**. Each proxy action is placed into an individual document that resides in admin4.nsf. Proxy actions can be viewed in two places: the field properties of a document in the admin4.nsf database, or in the Administration Request Document form. You can open the Proxy Action shared field and look at the list of choices. The following tables show the various proxy actions for each base release of Domino.

Release 4 AdminP Proxy Actions

R4 includes the following proxy actions. Note that all these proxy actions are available in all subsequent releases of Notes/Domino, including release 7.

Proxy action	PA
Delete in Address Book	0
Rename in Access Control List	1
Copy Server's Certified Public Key	2
Place Server's Notes Build Number into Server Record	3
Rename Server in Address Book	4
Rename Person in Address Book	5
Move Person's Name in Hierarchy	6
Delete Statistic Monitors in Address Book	7
Initiate Rename in Address Book	8
Recertify Server in Address Book	9
Recertify Person in Address Book	10
Add Server to Cluster	11

Proxy action	PA
Remove Server from Cluster	12
Create Replica	13
Move Replica	14
Delete Original Replica after Move	15
Delete in Person Documents	16
Delete in Access Control List	17
Delete in Reader/Author fields	18
Rename in Person Documents	19
Rename in Reader/Author Fields	20
Delete Mail File	21
Approve File Deletion	22
Delete Unlinked Mail File	23
Create Mail File	24
Monitor Replica Stub	25
Delete Obsolete Change Requests	26
Get File Information for Deletion	27
Request File Deletion	28
Add Resource	29
Delete Resource	30
Approve Resource Deletion	31
Check Access for New Replica Creation	32
Check Access for Move Replica Creation	33
Set Password Fields	34
Change User Password in Address Book	35
Set Master Address Book Field	37
Rename Person in Free Time Database	38
Rename Person in Calendar Entries and Profiles in Mail File	39
Rename Group in Address Book	40

Proxy action	PA
Rename Group in Person Documents	41
Rename Group in Access Control List	42
Rename Group in Reader/Author Fields	43
Add SSL X.509 Client Certificate to Person Record	44
Unrecognized Request	999

Release 5 AdminP Proxy Actions

Release 5 has all the proxy actions included in release 4, shown in the previous table. In addition, release 5 introduced the following 36 new proxy actions, for a total of 81 proxy actions. (Note that not all these proxy actions are consecutively numbered.) All these proxy actions are also available in subsequent releases of Notes/Domino.

Proxy action	PA
Check Mail Server's Access	45
Update Client Type in Person Record	46
Update External Domain Information	47
Promote New Mail Server's Access	48
Create New Mail File Replica	49
Add New Mail File Fields	50
Monitor New Mail File Fields	51
Replace Mail File Fields	52
Push Changes to New Mail Server	53
Delete Person in Address Book	54
Delete Server in Address Book	55
Delete Group in Address Book	56
Delegate Mail File	57
Approve Delete Person in Directory	58
Approve Delete Server in Directory	59
Approve Rename Person in Directory	60
Approve Rename Server in Directory	61
Modify Room/Resource in Directory	62

Proxy action	PA
Update Server's Protocol Information	63
Create ISPY Mail in Database	64
Check Access for Non-cluster Move Replica	65
Non Cluster Move Replica	66
Store Server's CPU Count	67
Rename Person in Unread List	68
Delete Replica After Move	69
Store Server's DNS Hostname in Server Record	70
Store Server's Platform in Server Record	71
Approve Deletion of Private Design Elements	72
Request to Delete Private Design Elements	73
Delete Private Design Elements	74
Approve Deletion of Moved Replica	75
Request to Delete Moved Replica	76
Domain Catalog Configuration	77
Delegate Web Mail File	78
Set Web Admin Fields	83
Sign Database with Server's ID File	101

Notes/Domino 6 and 6.5 AdminP Proxy Actions

As with their previous versions, Notes/Domino 6 and 6.5 retained all the proxy actions available in previous releases. In addition, Notes/Domino 6 introduced 83 new proxy actions, for a total of 164. Notes/Domino 6.5 introduced two additional proxy action, bringing to total to 166. All these proxy actions are available in Notes/Domino 7 as well.

Proxy action	PA
Get Replica Information for Deletion	79
Request Replica Deletion	80
Delete Replica	81
Approve Replica Deletion	82

Proxy action	PA
Accelerated Create Replica	84
Store Directory Type in Server Record	85
Set Directory Filename	86
Create Roaming User's Roaming Files	87
Promote New Roaming Server's Access	88
Replace Roaming Server's Field in Person Record	89
Monitor Roaming Server's Field in Person Record	90
Create Roaming User's Replica Stubs	91
Remove Roaming User's Roaming Files	92
Check Roaming Server's Access	93
Create Roaming User's Replicas	94
Store Certificate in Domino or LDAP Directory	95
Store Certificate Revocation List in Domino or LDAP Directory	96
Modify User Information Stored in Domino Directory	97
Remove Certificate from Domino or LDAP Directory	98
Modify CA Configuration in Domino Directory	99
Push Changes to New Roaming Server	100
Configure Certificate Authority Publication	102
Remove Certificate Revocation List from Domino or LDAP Directory	103
Update Delegated User's Mail File List	104
Certificate Authority Configuration To Be Signed	105
Approve Refused Name Change	106
Retract Person's Name Change	107
Set User Name and Enable Scheduled Agent	108
Update License Tracking Information in Domino Directory	109
Re-Initiate Rename in Domino Directory	110
Delete Server in Domain Catalog	111
Maintain Trends Database Record	112

Proxy action	PA
Delete Policy Record in Domino Directory	113
Approve Revert Name Change	114
Approve Certificate Request	115
Approve Person's Name Change Request	116
Approve New Public Key Request	117
Initiate Web User Rename in Domino Directory	118
Rename Web User in Access Control List	119
Rename Web User in Domino Directory	120
Rename Web User in Person Documents	121
Rename Web User in Reader/Author Fields	122
Rename Web User in Free Time Database	123
Rename Web User in Calendar Entries and Profiles in Mail File	124
Rename Web User in Unread List	125
Delete Web User in Domino Directory	126
Change HTTP Password in Domino Directory	127
Create Monitoring Report	128
Collect Monitoring Report Information	129
Add Information to Monitoring Report	130
Create IMAP Delegation Requests	131
Delete Hosted Organization	132
Update Roaming User State in Person Record	133
Update Roaming User Information in Person Record	134
Create Hosted Organization Storage	135
Recertify Cross Certificate in Domino Directory	136
Create Object Store	137
Get Hosted Organization Storage Information for Deletion	138
Approve Deletion of Hosted Organization Storage	139
Delete Hosted Organization Storage	140
Recertify Certificate Authority in Domino Directory	141

Proxy action	PA
Find Name in Domain	142
Verify Hosted Organization Storage	143
Add or Modify Group in Domino Directory	144
Modify ID Recovery Information in Domino Directory	146
Delete Person In Unread List (introduced in Notes/Domino 6.5)	147
Monitor Roaming User's Replica Stubs	148
Delegate Mail File on Administration Server	149
Check Access for New Replica Creation (time-based execution)	150
Check Access for Move Replica Creation (time-based execution)	151
Check Mail Server's Access (time-based execution)	152
Check Access for Non-cluster Move Replica (time-based execution)	153
Create SSL Certificate and Keyring File	156
Enable Server's SSL Ports in Domino Directory	157
Change the Server on which the Agent Runs	158
Store Cross Certificate in Domino or LDAP Directory	159
Set Web User Name and Enable Scheduled Agent	160
Update Replica Settings	161
Rename in Shared Agents	162
Web Set Soft Deletion Expire Time	163
Rename in Agent's Readers Field	164
Delete in Agent's Readers Field	165
Monitor Server's SSL Status in Domino Directory	166
Delegate Mail File on Home Server	167
Maintain Server's Fault Recovery Settings (introduced in Notes/Domino 6.5)	168

Notes/Domino 7 AdminP Proxy Actions

Finally, let's look at the new proxy actions introduced in Notes/Domino 7. As you've probably caught on by now, this latest release includes all the proxy actions available in previous releases of Notes/Domino since release 4. In addition, Notes/Domino 7 includes 12 new ones, for a total of 178. These actions primarily concern DB2 management and design-element management processing.

Proxy Action	Code	Process involved
Certify New Server Key Request	169	This is initiated by an administrator modifying one of the key-related fields on the Administration tab of the Server document. (See the screenshot following this table.)
Certify New Person Key Request	170	This is initiated by the administrator modifying the key-related fields on the Notes Certificate tab of the user's Person document. The user initiating the Create New Public Keys action and choosing Authentication Protocol on the User Security panel in the Notes client can also generate this request.
Certify New Certifier Key Request	171	The administrator requesting a new certifier key request starts this process.
Store DB2 Information in Server Record	172	This will update the Server document when the Domino server is enabled to communicate with the DB2 server.
Monitor Server Record for DB2 Fields	173	This will use the administration process, along with automatic server restart, to enable the Domino server for DB2.
Set DB2 Password in Server's ID File	174	This will use the Set Server's DB2 ID menu item to modify the password and username that the Domino server uses to communicate with the DB2 server.
Move DB2 Tablespace to New Container	175	This is initiated by executing the tablespace move using the Tools Database DB2 Move Container menu item.
Rename in Design Elements	176	This will rename users in design elements.
Delete in Design Elements	177	This will delete users in design elements.
Modify DB2 Access Connection	178	This will modify the DB2 access connection.
Rename Web User in Design Elements	179	This will rename Web users in design elements.
Rename Group in Design Elements	180	This will rename Groups in design elements.

Server : Domino7NSF/ND7B2

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous | Transactional Logging | Shared Mail | **Administration**

Administration

Owner:

Administrators:

Public Key Requirements

Minimum Allowable Key Strength:	Compatible with all Releases (630 bits)	▼
Maximum Allowable Key Strength:	Compatible with all Releases (630 bits)	▼
Desired Default Key Strength:	Compatible with all Releases (630 bits)	▼
Maximum Allowable Age for Key (in days):	<input type="text" value="36500"/>	
Earliest Allowable Key Creation Date:	<input type="text" value="08/01/77"/>	
Don't automatically generate a new key before:	<input type="text" value="03/04/2105"/>	
Maximum number of days the old key should remain valid after the new key has been created:	<input type="text" value="365"/>	

Types of Proxy Actions

There are three basic types of AdminP proxy actions:

- Operations that execute on the Primary Administration server
- Operations that execute on all spoke Administration servers
- Operations that execute on a targeted server

The following sections describe these proxy action types.

Operations that Execute on the Primary Administration Server

Many AdminP processes start on the Primary Administration server. The actual proxy action command can be created on virtually any server.

The following table lists several AdminP proxy actions that execute only on the Primary Administration server. (Note that this is not the complete list.)

Delete in Domino Directory	Accelerate create replica
Place server's Notes build number into Server document	Store directory type in Server record
Rename server in Domino Directory	Replace roaming server's field in Person document
Rename person in Domino Directory	Modify user information stored in Domino Directory

Move person's name in hierarchy (actually this action can be approved on any server)	Modify CA configuration in Domino Directory
Delete statistic monitors in Domino Directory	Update license tracking information in Domino Directory
Initiate rename in Domino Directory	Re-initiate rename in Domino Directory
Recertify server in Domino Directory	Delete Policy record in Domino Directory
Recertify person in Domino Directory	Initiate web user rename in Domino Directory
Delete in Person documents	Rename web user in Domino Directory
Change user password in Domino Directory	Rename web user in Person documents
Add Internet certificate to Person record	Delete web user in Domino Directory
Delete person in Domino Directory	Change HTTP password in Domino Directory
Delete server in Domino Directory	Update roaming user state in Person document
Delete group in Domino Directory	Update roaming user information in Person document
Approve delete person in Domino Directory	Recertify cross certificate in Domino Directory
Approve delete server in Domino Directory	Recertify Certificate Authority in Domino Directory
Approve rename person in Domino Directory	Add or modify group in Domino Directory
Approve rename server in Domino Directory	Modify ID recovery information in Domino Directory
Modify room/resource in Domino Directory	

To review each type of command, open the `admi n4. nsf` database and find the AdminP Request document. You will see a field titled `Server(s)` to perform the action.

Operations that Execute on all Spoke Administration Servers

Next up are the operations that will execute on all servers. Again, you need to look at the command document in the `admi n4. nsf` database. If an asterisk appears in the `Server` to

execute on field, then this command will execute on all servers in the domain. Here are a few examples of 'asterisk' commands:

- Delete user in Access Control List
- Rename in Access Control list
- Move person's name in hierarchy
- Delete in Reader/Author fields
- Rename person in unread list

Operations that Execute on a Targeted Server

This is a limited set of commands that will execute only on the spoke and/or targeted server. AdminP will analyze the Person Document of this user and will determine whether any targeted commands need to be created. One example would be if a user were renamed; in this example AdminP would create two commands:

- Rename person in calendar entries and profiles in mail file
- Rename person in Free Time database

These commands replicate to the targeted server and execute there. You can determine which commands are for a targeted server by opening the Request document and looking at the field Server(s) to perform the action on.

admin4.nsf

All AdminP proxy actions are hosted in the `admin4.nsf` database. This contains all requests from a single domain. Every request (via a proxy action) placed into `admin4.nsf` replicates to every server in the domain.

Cross-Domain Administration Requests

AdminP can be configured to execute an administration request from one Domino domain and then send that request to another Domino domain. There is a limited set of commands. These tasks can be processed across domains:

- Delete person in Domino Directory
- Delete server in Domino Directory
- Rename server in Domino Directory (that is, upgrade the server name from flat to hierarchical)
- Rename person in Domino Directory
- Create replica
- Get replica information for deletion (this request is generated when you delete a database and its replicas)

Each `admin4.nsf` database in a domain has the same replica ID and must replicate to all other servers in the domain that runs AdminP. This allows one server to issue a request and another server to process that request. When an additional server in your domain is set up, `admin4.nsf` is replicated from the server that is known as the Administration server for the Domain.

Replica ID Relationship for `admin4.nsf` and `names.nsf`

The replica ID for `admin4.nsf`, along with `catal.og.nsf`, `events4.nsf`, `log.nsf`, and `statrep.nsf`, has a mathematical relationship with that for the domain's `names.nsf`. The Domino server builds these databases automatically when it first starts. For example, if the primary Domino Directory `names.nsf` has a replica ID of `852534AB:004EBCCA`:

- `catal.og.nsf` has a replica ID of `852534AB:014EBCCA`
- `events.nsf` has a replica ID of `852534AB:024EBCCA`
- `admin.nsf` has a replica ID of `852534AB:034EBCCA`
- `statrep.nsf` has a replica ID of `852534AB:044EBCCA`

Take a look at each example replica ID. The first eight characters are the same, and the last eight are similar. The difference lies in the first two numbers of the second eight. `names.nsf`, in this example, starts with `00`, and each of the other replica IDs has `01`, `02`, `03`, and `04` respectively.

One of the advantages of this relationship occurs when a new server is added to your domain. In the case of `admin4.nsf`, a stub is created with the correct replica ID, is initialized, and then replication occurs with another server with the same replica ID of `admin4.nsf`.

The `admin4.nsf` database includes a number of default views. Each of these views provides reporting information. Also, there are views that display documents that require approval from an administrator.

Name-Change Management

Another new feature for Domino 7 is new management of name changes. The Domino 7 Administration process will no longer revert name changes automatically, and will require that the administrator either approve or reject the name-change reversion.

In order to provide contiguous access to end users' databases during a name change, there is a period of time where both the old and new usernames will be allowed access to the Domino server and associated databases. By default this period is 21 days. The administrator can define this value when the rename is performed (14 to 60 days). Once this period of time has expired, the old name will no longer be supported.

There are cases where the old name must remain active and the new name be abandoned. One example is when an end user is unable to accept the name change because he or she is out of the office for an extended period. In this situation, the name change started by the administrator would need to be reverted. This reverted name would continue to provide access to the user whose name was being changed. In previously releases, the reversion would be performed automatically after the expiration time had passed. Now, with the new Domino 7 AdminP approval process, the capability to approve or reject a name change reversion is provided to the administrator.

Summary

This concludes our tour of new Administration process (AdminP) features introduced in Domino 7. We've looked at each of the major components of AdminP (including the AdminP server task and `admin4.nsf`), and how they have been enhanced in release 7.

5

Policy Management

Next up on our tour of new Domino 7 features is policies. Policies can help administrators control how end users work within various parts of the Notes/Domino enterprise. As you probably know, policies are not new to Domino 7. However, policy functionality has been significantly enhanced in this release.

Policy Basics

Before we get into the various types of policy documents offered in Domino 7, let's review a few points about how policies work. There are two types of policy documents, explicit and organization:

- Explicit policies assign a policy directly to specific users and groups.
- Organizational policies automatically assign a policy to all users in an organization or organizational unit.

All policies start with a master policy document. Each policy document, of either type, can have up to six different policy settings: Registration, Setup, Desktop, Mail Archiving, Security, and Mail. The base policy document has three tabs: Basics, Comments, and Administration.

Basics Tab

The base policy document Basics tab includes two sections:

- **Basics:** This section includes fields that define the name of the policy document, type of policy document (organizational or explicit), and a description.
- **Settings type** (with setting name): This section includes settings assigned to this particular policy.

Comments Tab

The Comments tab contains descriptive information about the policy. This tab is unchanged in Domino 7.

Administration Tab

This tab has only one section, Administration, and includes fields for identifying owners and administrator, as well as tracking last updated information. There is also a new selection with Domino 7: Ignore settings from ancestor policies. As experienced administrators are aware, an important feature of policies is the ability to set a value in a top-level policy document and have that value inherited by all children of that policy. Through this new setting, you can 'turn off' inheritance for a policy, even if its ancestor policy has specified that the policy inherits its settings from the ancestor.

Policy Lock Down

One of the biggest enhancements with Domino 7 is the ability to enforce Notes client policy **lock down**. This lock-down feature provides a way for policy administrators (see information box) to control who can change which policies.

In this book, we use the term **policy administrator** to refer to the person and/or group that will manage policies. This is not an 'official' role within Notes/Domino. Thus, policy administrator can be considered a 'virtual' role. However, Domino 7 does provide several actual roles and ACLs that collectively compose this virtual role. These include PolicyCreator, PolicyModifier, PolicyReader, and **extended ACL control (xACL)** features. It is up to each organization to determine the best method to implement policy management.

The lock-down client policy settings are available for the Desktop and Mail policy documents. The implementation of the lock-down feature is a bit different for each policy document. The desktop policy settings use a per-tab setting to manage client lock down. The Mail policy settings use per-field settings. Each of these sets of settings is obvious in each policy setting document. Examples of each will be described later in this chapter.

The Notes dynamic client configuration process will take over after the policy administrator has configured each of these settings in the Domino Directory. End users authenticate using Notes clients. The dynamic configuration process takes the information that was pushed down into the clients from the Domino server. The dynamic configuration reviews each setting and determines the status in relation to each policy, field setting, and tab setting. After this is determined, each field is updated (unless the configuration allows end users to make changes).

Now let's look at the types of policies available to you in Domino 7.

Registration Policy

The registration policy provides a way for administrators to create domain-level defaults to be applied at the time of end-user registration. Registration policy settings include:

- Registration server
- Password quality
- Mail type (Notes, POP, IMAP, and so on)
- Mail server
- Internet domain (and internet address format settings)
- Mail template
- End-user access level to the mail file (Manager, Designer, Editor)
- Various mail file settings
- Certifier to use
- Certification expiration
- Group assignments

A new feature in the Domino 7 registration policy setting is the ability to configure the key length. In the figure that follows, notice two new dialog boxes. The first is labeled Public Key Specification. This lets you choose the length of the public key: 630 bit or 1024 bit. (The longer key offers a higher level of security, but may result in additional encryption/decryption processing time.) The second box is the Password Key Width, which offers three options relating to password length and strength:

- Base strength on RSA key size
- Compatible with all releases (64) bits
- Compatible with 6.0 and later (128) bits

Registration Settings : Reg-Sales

Basics | Mail | **ID/Certifier** | Miscellaneous | Comments | Administration

ID/Certifier User Registration Options	Inherit from parent policy:	Enforce in child policies:
<input checked="" type="checkbox"/> Create a Notes ID:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Certifier Information		
Security Type: North American International	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Public Key Specification: Compatible with all releases (630 bits) Compatible with 6.0 and later (1024 bits)	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Password Key Width: Base strength on RSA key size Compatible with all releases (64 bits) Compatible with 6.0 and later (128 bits)	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Certificate Expiration Date: <input checked="" type="radio"/> Static Date <input type="radio"/> Months from user creation 03/21/2007 09:06 PM	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Location for Storing User ID		
<input checked="" type="checkbox"/> In Domino Directory	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="checkbox"/> In File	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Setup Policy

As with Notes/Domino 6.x, administrators have the ability to create and use a setup policy. The setup policy will initialize during the Lotus Notes client-setup process. The Notes client will use these settings as part of its first-time initialization. Specific setup entries include internet browser settings, location document, and (in Domino 7) many preferences settings.

Preferences Tab

In Notes/Domino 7, end users can save the state of the window's tabs when they exit Notes. These tabs then display the next time the user starts Notes. For instance, suppose you open four different databases when suddenly you feel the immediate need to go and play racquetball. You have two choices to save the state of the 'open' databases. You can

select the option **Save Window State** from the File menu. This saves the state of open databases. Or you can set the new Notes preference **Save window state on exit** to save the state each time the Notes client is shut down. As the administrator, you can set this preference so that by default users have this option set when they first start up Notes. (We talk more about the 'save window state' feature when we discuss new features in the Lotus Notes 7 client.)

In addition, the setup policy lets you set the new Notes preference **AutoSave every N minutes**:—this setting controls how often the AutoSave process saves a document.

The following figure shows these options (and other new options for controlling default preference settings) in the setup policy document's **Basics** tab:

Basic Preferences		Inherit from parent policy:	Enforce in child policies:
Icon color scheme:		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Empty trash folder:		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Scan for unread:		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Save state on exit:		<input checked="" type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
AutoSave every N minutes:	15 minutes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Lock ID after N minutes of inactivity:	15 minutes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Enable scheduled local agents:		<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Note: Select "Don't Change" to allow Notes users to set these preferences.

Miscellaneous Tab

There are five new selections available in this tab. Each corresponds to a setting in the Notes Preferences menu:

- **Disable View updates as a background task.** By default, Notes 7 updates views in the background. This option allows the user to continue working while Notes performs other tasks.
- **Enable MS Office 97 SendTo to Notes:** This feature is not new in the Notes client, but policy administrators can now remotely set this feature in a Notes 7 client. When this feature is enabled, it effectuates all mail 'Send To' commands in Microsoft Office 97 applications to start Notes mail and sends the file as an attachment in a mail memo.

- **Enable Icon Popup Help in View:** This shows pop-up help on these and other message icons.
- **Expand Names field contents when printing:** Again, this is not a new Notes client feature but is new in Domino 7 policies. This feature expands the contents of To or CC fields when printing. This feature is disabled by default.
- **Do not prompt when marking all documents read or unread:** This is a new Notes 7 feature and preference setting. This setting controls the prompt for marking all document read or unread.

Internet Tab

In the setup policy's Internet tab, a new setting has been added: Lotus Notes should check on startup to see that it is my default email program. This allows administrators to disable this prompt for a group of users or a complete organization:

Setup Settings : ND7 only

Basics | Databases | Dial-up Connections | Accounts | Name Servers | SSL | Applet Security | Proxies | Mail | **Preferences** | Comments | Administration

Basics | Miscellaneous | International | **Internet** | Mail and News | Instant Messaging | Replication | Network Ports

Internet Settings	Inherit from parent policy:	Enforce in child policies:
Internet mail format:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Multilingual Internet mail: Use Match and prompt	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Internet News format:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Prefix each line with:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Wrap lines at:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Lotus Notes should check on startup to see that it is my default email program:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Note: Select "Don't Change" to allow Notes users to set these preferences.

Mail and News Tab

Domino 7 introduces one change to the setup policy's Mail and News tab. Since Notes/Domino 6, users can show an icon in the system tray for new mail. The setting is found under the When New Mail Arrives area of the user preferences. Now a Domino 7 policy administrator can enable this setting via a new Domino 7 policy setting:

Setup Settings : ND7 only

Basics | Databases | Dial-up Connections | Accounts | Name Servers | SSL | Applet Security | Proxies | Mail | **Preferences** | Comments | Administration

Basics | Miscellaneous | International | Internet | Mail and News | Instant Messaging | Replication | Network Ports

Mail and News Settings	Inherit from parent policy:	Enforce in child policies:
Save sent mail:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Sign sent mail:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Encrypt sent mail:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Encrypt saved mail:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Check for new mail:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Mail checking interval: minutes	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Show a Popup:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Play a Sound:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Automatically Refresh Inbox:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Show an icon in System Tray:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Note: Select "Don't Change" to allow Notes users to set these preferences.

Instant Messaging Tab

On the Instant Messaging tab you will find two new policy settings that can be enabled in Domino 7:

Setup Settings : ND7 only

Basics | Databases | Dial-up Connections | Accounts | Name Servers | SSL | Applet Security | Proxies | Mail | **Preferences** | Comments | Administration

Basics | Miscellaneous | International | Internet | Mail and News | Instant Messaging | Replication | Network Ports

Instant Messaging Settings	Inherit from parent policy:	Enforce in child policies:
Show instant messaging status for names:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Log onto IBM Lotus Instant Messaging using Single Sign-On (SSO):	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Use canonical name for instant messaging status lookup:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Note: Select "Don't Change" to allow Notes users to set these preferences.

- **Show instant messaging status for names:** This Notes feature (introduced in Notes/Domino 6.5) can be enabled or disabled to display the IBM Lotus Instant Messaging (Sametime) status of any users that are online.
- **Log onto IBM Lotus Instant Messaging using Single Sign-On (SSO):** This allows a user to save their instant-messaging password used during instant-messaging authentication.

Desktop Policy

The desktop policy controls and updates your Notes client desktop when you authenticate with your home server. Domino 7 has many new settings and features available in the desktop policy document.

Apart from using the desktop policy document, you can control many of these settings through the Notes client's NOTES.INI file. This is especially useful if you want to deploy these settings to all your users, and not just particular groups (in which case policy settings would be a better choice).

You can modify your users' NOTES.INI file through the desktop policy document. To do so, you must modify the standard desktop policy document form to include a new field named \$PrefVariableName. This contains the name of the variable you want to change in NOTES.INI. After this field has been added to the policy document form, you can enter the value you want assigned to the specified NOTES.INI variable. This setting then becomes part of each user's local NOTES.INI file.

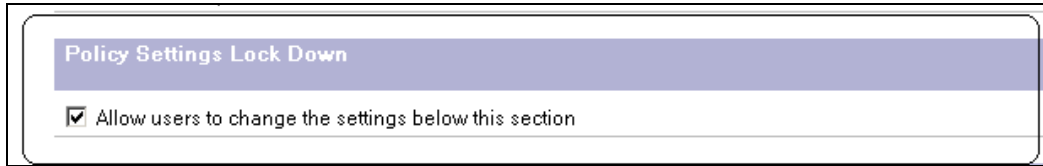
Similarly, you can edit location document settings through the desktop policy document. This requires adding a new field to the policy settings document form. The new field must be named \$LocalVariableName, where VariableName is the name of the fields you are setting in the location documents. You can add the value to be set into this new field; this value is then assigned to all users' location documents.

Basics Tab

Readers familiar with the desktop policy document's Basics tab will notice that the layout of the sections on this tab has been modified. This was done to accommodate the Allow users to change the settings below this section setting. This option is associated with the new client lock-down feature, described earlier in this chapter. The sections that have client lock down available are:

- Server Options
- Mail Template Information
- Browser Options
- Calendaring and Scheduling

The following screenshot shows this lock-down setting:



A number of other policy document tabs offer lock down sections. These tabs include the Name Server, SSL, Applet Security, Proxies, and Mail tabs, among others.

One other new Domino 7 desktop policy setting (Location Options | Do not allow private location docs) prevents end users from creating private location documents.

Smart Upgrade Tab

The only new feature on the desktop policy document's Smart Upgrade tab is the ability to control the number of days to keep smart upgrade files. The default value is 365, but you can set this lower. (We talk more about smart upgrade in Chapter 6.)

Preferences | Basics Tab

The Preferences | Basics tab is another tab that includes a lock-down section. In addition, this tab includes the new features Save state on exit (which allows end users to save the state of the window's tabs on exiting Notes so that these tabs will be display the next time they start Notes) and AutoSave every N minutes: (which controls how often AutoSave processes a document save).

Preferences | Miscellaneous Tab

There are five new selections available in the desktop policy document's Preferences | Miscellaneous tab. Each of these allows policy administrators the ability to impose specific policies on the end user desktop. The following five items show some of the new policy options in Domino 7. These are the same new settings that are described in the *Setup Policy* section.

- Disable View updates as a background
- Enable MS Office 97 SendTo to Notes
- Enable Icon Popup Help in View
- Expand Names field contents when printing
- Do not prompt when marking all documents read or unread

Preferences | Internet Tab

As with the setup policy, this tab includes a new startup policy setting: Lotus Notes should check on startup to see that it is my default email program. This allows administrators to disable this prompt for a group of users or a complete organization.

Preferences | Instant Messaging Tab

New features for Domino 7 on this tab include:

- Show instant messaging status for names: This Notes client feature (also found in Notes/Domino 6.5) can be enabled or disabled to display the Lotus Instant Messaging (Sametime) status of any users that are online.
- Log onto IBM Lotus Instant Messaging using Single Sign-On (SSO): This client feature allows a user to save an instant-messaging password, to be used during instant-messaging authentication.

Preferences | Diagnostics Tab

There are a few differences between Notes/Domino 6 and Domino 7 for this tab. These differences include:

- Maximum size of diagnostic message including attachments (in MB)
- Maximum size of NSD output to attach (in MB)
- Maximum amount of console output file to attach (in KB)
- Diagnostic file patterns

Mail Archiving Policy

Mail archiving is another feature that first appeared in Notes and Domino 6. Mail archiving policy documents are easy to set up. First, create an archive settings document. Then open the archive setting document and create an archive 'criteria' document. Each archive policy settings document requires at least one archive criteria policy settings document. Let's review each of these documents using Domino 7 as a base example.

First, create the base policy document, organizational or explicit. Then create the mail archive policy setting document. The following example shows an archive policy setting document called Sales - Archive - Mail:

Archiving Settings : Sales - Archive - Mail

Basics	Selection Criteria	Logging	Schedule	Advanced	Comments	Administration
--------	--------------------	---------	----------	----------	----------	----------------

Basics

Name: Sales - Archive - Mail

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:

<input checked="" type="radio"/> User's local workstation	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="radio"/> Server		

Archiving source database is on:

Source Server:

<input type="radio"/> Local	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="radio"/> Specific server		
<input checked="" type="radio"/> Mail server		

Destination database is on:

Destination Server:

<input checked="" type="radio"/> Local	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input type="radio"/> Specific server		
<input type="radio"/> Mail server		

The next step is to create a criteria document. Click the Selection Criteria tab, and create a criteria document:

Archiving Settings : Sales - Archive - Mail

Basics	Selection Criteria	Logging	Schedule	Advanced	Comments	Administration
--------	--------------------	---------	----------	----------	----------	----------------

☐ Inherit Selection Criteria ☐ Enforce Selection Criteria

Currently Selected Criteria

Click the New Criteria button to create the new selection criteria. The trick here is that once you create the criterion, you must click Add Criteria to display and use it in this document. The following is an example of a criteria document:

Archive Criteria Settings : Criteria Two

Basics | Destination | Comments | Administration

Basics

Name: Criteria Two

Description:

☒ Enable archive criteria

How should documents be archived?

☒ Copy old documents into archive database; then clean up database
☐ Clean up database without archiving

How should documents be cleaned up?

☒ Delete older documents from the database
☐ Reduce the size of documents in the database

Which documents should be cleaned up?

not modified after 365 days

Archive By View/Folder:

Server: Domino7B2/ND7B2
Template: Extended Mail (R7)
Change template server: Domino7B2/ND7B2
Choose template: Extended Mail (R7)

☒ In views or folders:

<input checked="" type="checkbox"/> To Do	<input checked="" type="checkbox"/> Drafts	<input checked="" type="checkbox"/> Sent
<input checked="" type="checkbox"/> All Documents	<input checked="" type="checkbox"/> Inbox	<input checked="" type="checkbox"/> Trash
<input checked="" type="checkbox"/> Calendar	<input checked="" type="checkbox"/> Meetings	

After you create and add all the criteria documents, you will see a list of the criteria that have been selected:

Archiving Settings : Sales - Archive - Mail

Basics | Selection Criteria | Logging | Schedule | Advanced | Comments | Administration

☐ Inherit Selection Criteria ☐ Enforce Selection Criteria

New Criteria Add Criteria Remove Criteria

Currently Selected Criteria

- Criteria One
- Criteria Three
- Criteria Two

Domino 7 includes all mail-archiving features that were introduced in Notes/Domino 6. There are a few changes in the mail-archiving settings document. The following features are new in the Advanced tab:

- **Maximum document retention selection is:** This setting specifies the number of days, months, or years that is the maximum retention period for deleting and archiving documents.
- **Use customer generated expiration field:** This allows administrators to define their own field name for an archive document expiration date.
- **Specify a field name for the expiration date of archived documents:** If Use customer generated expiration field is selected, then this field will be displayed so that an administrator can place a name in this field.

Archiving Settings : Domino 7

Basics | Selection Criteria | Logging | Schedule | **Advanced** | Comments | Administration

Advanced Settings	Inherit from parent policy:	Enforce in child policies:
<input checked="" type="checkbox"/> Don't delete documents that have responses	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Maximum document retention selection is: 99 Years	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<input checked="" type="checkbox"/> Use customer generated expiration field	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Customer generated expiration field name:	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Security Policy

The security policy document controls Notes and internet passwords as well as the Administration ECL. In Domino 7, policy administrators can also manage internet passwords and public key requirements for Lotus Notes ID files.

The new Domino 7 settings include the following:

- **Minimum Allowable Key Strength:** This setting has three options: No Minimum, Maximum compatible with all releases (630 bits), and Compatible with Release 6 and later (1024 bits).
- **Maximum Allowable Key Strength:** This setting has three options: Minimum (512 bits), Maximum compatible with all releases (630 bits), and Compatible with Release 6 and later (1024 bits).
- **Desired Default Key Strength:** This has the same three options as the Minimum Allowable Key Strength setting.
- **Maximum Allowable Age for Key (in days):** This setting specifies the maximum age a key can reach before needing to be rolled over. The default is 36,500 days (10 years).
- **Earliest Allowable Key Creation Date:** This specifies that a key created prior to this date will be rolled over to a larger key size.
- **Spread new key generation for all users over this many days:** This setting specifies the time period for new keys to be generated for all users to whom this security settings policy document applies. User keys are randomly rolled over during the configured time period. The default is 180 days.
- **Maximum number of days the old key should remain valid after the new key has been created.**

Security Settings : Sales

Basics | Password Management | Execution Control List | **Public Key Requirements** | Comments | Administration

User Public Key Requirements	
Minimum Allowable Key Strength:	No Minimum
Maximum Allowable Key Strength:	Compatible with Release 6 and later (1024 bits)
Desired Default Key Strength:	Compatible with Release 6 and later (1024 bits)
Maximum Allowable Age for Key (in days):	36500
Earliest Allowable Key Creation Date:	08/01/77
Spread new key generation for all users over this many days:	180 days
Maximum number of days the old key should remain valid after the new key has been created:	365

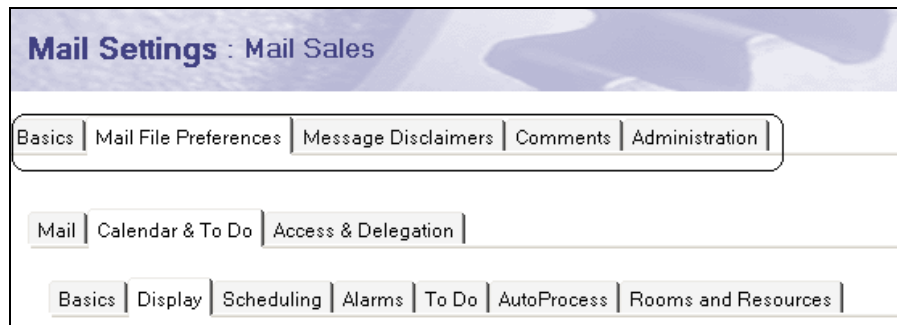
Domino 7 has a process known as **key rollover**. This can be used to update the set of Lotus Notes public and private keys that are being stored in user and server Notes IDs. There are times when the keys will need to be replaced, for instance, when a Notes. id file has been compromised. Another reason to force a key rollover is to move to a large key set.

Administrators will configure triggers to start a key rollover in the Domino directory. Both user and server ID files can be triggered for a key rollover. Triggers include existing key size, the issue date of the existing key, and the age of the existing key.

Mail Policy

Mail policy settings are a new and very powerful feature in Domino 7. Mail policy settings let you set and enforce client-based mail settings and mail-related preferences. You can use policies to manage mail features as well as calendaring and scheduling features.

The mail policy document consists of five tabs: Basics, Mail File Preferences, Message Disclaimers, Comments, and Administration.



Basics Tab

The Basics tab includes two fields:

- Name: The name of the policy setting (Mail Sales in the preceding screenshot example)
- Description: A description of this particular policy setting

Mail File Preferences | Mail | Basics Tab

This tab has four categories, each with a single setting:

- User Configuration includes the setting Allow users to change mail file ownership. This determines whether the user can change mail file ownership. This setting is controlled with the Allow checkbox under Allow User to Change.
- Spell Checking includes the setting Automatically check mail messages for misspellings before sending. This setting is enabled/disabled via a checkbox. You can also choose when this action will be executed. Choices are Never, Always, and Initially.
- The Delete/Remove Preference for Sent View setting determines whether the user will be prompted to delete messages from the Sent view. Options are Always Ask (the Notes client will always ask in the event that the user wants to save each message when it is sent; if the policy administrator selects Yes, then the Notes client will save the message in the Sent view), Always Delete (the Notes client will delete the mail message after it is sent), and Always Remove (Notes will remove the mail message from the current view after sending the message, but the message will not be deleted). Also, there is a choice of *when* this action will be executed. Options are Never, Always, and Initially.
- Soft Delete includes the setting Soft Delete expire time in hours. This allows the policy administrator to set the time for the soft deletions.

Mail Settings : Mail Sales

Basics | **Mail File Preferences** | Message Disclaimers | Comments | Administration

Mail | Calendar & To Do | Access & Delegation

Basics | Letterhead

User Configuration		When to apply this setting:	Allow user to change:
Allow users to change mail file ownership:			<input checked="" type="checkbox"/> Allow
Spell Checking		When to apply this setting:	Allow user to change:
Automatically check mail messages for misspellings before sending: <input type="checkbox"/> Yes		Never	<input checked="" type="checkbox"/> Allow
Delete/Remove Preference for Sent View		When to apply this setting:	Allow user to change:
Delete/Remove Preference for Sent View: Always Ask		Never	<input checked="" type="checkbox"/> Allow
Soft Delete		When to apply this setting:	Allow user to change:
Soft Delete expire time in hours: 48		Never	<input checked="" type="checkbox"/> Allow

Mail File Preferences | Mail | Letterhead Tab

This tab includes the option Set default Letterhead. This allows policy administrators to define the letterhead that will appear on outgoing user messages. If you select Yes, an additional dialog box will appear, showing the various letterheads available.

Mail Settings : Mail Sales

Basics | **Mail File Preferences** | Message Disclaimers | Comments | Administration

Mail | Calendar & To Do | Access & Delegation

Basics | Letterhead

Your letterhead will appear at the top of your outgoing mail messages

Set default Letterhead: ☒ Yes

Letterhead:

- Bouncy Earth
- Buck Rogers Mail
- Computer Chip
- Decco
- Falling Spheres
- Frank Lloyd

Mail File Preferences | Calendar & To Do Tab

The mail policy document's Mail File Preferences | Calendar & To Do tab consists of seven tabs: Basics, Display, Scheduling, Alarms, To Do, AutoProcess, and Rooms and Resources:



Basics Tab

The Basics tab has three options that the policy administrator can set:

- Double clicking on a time-slot in Calendar creates a gives the policy administrator the option to select a default selection for a particular explicit or organizational group of users. Options include Meeting, Appointment, All Day Event, Anniversary, and Reminder.
- Duration of a new Appointment or Meeting (in minutes) specifies a time in minutes as a default setting for a meeting duration. The default for this setting is 60 minutes.
- Anniversaries repeat for (in years) defines a time for which anniversaries will be created for users who have this policy applied. The default is ten years.

Display Tab

The Display tab provides a considerable amount of control for the policy administrator.

Mail Settings : Mail Sales

Basics | **Mail File Preferences** | Message Disclaimers | Comments | Administration

Mail | **Calendar & To Do** | Access & Delegation

Basics | **Display** | Scheduling | Alarms | To Do | AutoProcess | Rooms and Resources

How the Calendar View is Displayed	When to apply this setting:	Allow user to change:
Beginning of the work day: 07:00 AM	Never	<input checked="" type="checkbox"/> Allow
End of the work day: 07:00 PM	Never	<input checked="" type="checkbox"/> Allow
Each time slot lasts: 60 minutes	Never	<input checked="" type="checkbox"/> Allow
Start monthly view with current week: <input type="checkbox"/> Yes	Never	<input checked="" type="checkbox"/> Allow
Days displayed in a work week: <div> <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday </div>	Never	<input checked="" type="checkbox"/> Allow

Displaying Calendar Entries in Mail Views	When to apply this setting:	Allow user to change:
Put C&S documents into a special New Notices MiniView for processing: <input type="checkbox"/> Yes	Never	<input checked="" type="checkbox"/> Allow
Hide new calendar entries and notices in All Documents view of Mail: <input type="checkbox"/> Yes	Never	<input checked="" type="checkbox"/> Allow
Hide new Meeting invitations in the Sent view of Mail: <input checked="" type="checkbox"/> Yes	Never	<input checked="" type="checkbox"/> Allow
Remove Meeting invitations from your Inbox after you have responded to them: <input type="checkbox"/> Yes	Never	<input checked="" type="checkbox"/> Allow
Types of Meeting notices to be shown in your Inbox: All	Never	<input checked="" type="checkbox"/> Allow

The Display tab consists of two basic subsections.

How the Calendar View is Displayed lets you control how each time field is displayed by default. Each of these is shown below with its default setting:

- Beginning of the work day: 07:00 AM
- End of the work day: 07:00 PM
- Each time slot lasts: 60 minutes

- Start monthly view with current week: This is enabled when Yes is checked. By default this is unchecked.
- Days displayed in a work week: Monday; Tuesday; Wednesday; Thursday; Friday.

Displaying Calendar Entries in Mail Views consists of a series of checkboxes. These provide a mechanism to control how each calendar entry displays, as well as a choice of *when* these actions will be executed (Never, Always, or Initially). Options include (with their default settings):

- Put C&S documents into a special New Notices MiniView for processing: By default this is unchecked.
- Hide new calendar entries and notices in All Documents view of Mail: By default this is unchecked.
- Hide new Meeting invitations in the Sent view of Mail: By default this is checked.
- Remove Meeting invitations from your Inbox after you have responded to them: By default this is unchecked.
- Types of Meeting notices to be shown in your Inbox: Choices are All, All Except for Responses, and None. All by default.

Scheduling Tab

This tab has two categories: Your Availability and When Adding an Entry to your Calendar. You can choose when each of these actions is executed (Never, Always, or Initially).

Your Availability

The choices in this section drive the user's default availability. For instance, imagine that a group of users work during a second shift. In this case, the policy administrator can set a default set of availability times for this group via policies. The following screenshot shows the default settings for a new mail policy in this section:

<input type="checkbox"/> Sunday	
<input checked="" type="checkbox"/> Monday	09:00 AM - 12:00 PM, 01:00 PM - 05:00 PM
<input checked="" type="checkbox"/> Tuesday	09:00 AM - 12:00 PM, 01:00 PM - 05:00 PM
<input checked="" type="checkbox"/> Wednesday	09:00 AM - 12:00 PM, 01:00 PM - 05:00 PM
<input checked="" type="checkbox"/> Thursday	09:00 AM - 12:00 PM, 01:00 PM - 05:00 PM
<input checked="" type="checkbox"/> Friday	09:00 AM - 12:00 PM, 01:00 PM - 05:00 PM
<input type="checkbox"/> Saturday	

When Adding an Entry to Your Calendar

This section manages scheduling conflicts, and shows how the scheduler will manage the details for each participant. There are two default choices for this section and one additional choice based on selection criteria. Check for conflicts when adding appointments, accepting meetings, scheduling a new meeting is a self-explanatory checkbox, and is by default unchecked. When this option *is* checked, the option Note a conflict if entry occurs outside available hours described above appears. This is checked by default. When this option is selected, the field For new meetings, the Scheduler initially shows appears. This allows you to control the schedule details for each participant. Options are Schedule Details for each participant (this is the default setting for a new mail policy) and Suggested best times for meetings.

Alarms Tab

The Alarms tab includes one default section (or two, if alarms are enabled). This tab allows the administrator to set up default alarms based on each calendar-entry type. As with a number of other mail policy settings, this section lets you decide when these actions will be executed (Never, Always, or Initially). The default choice displayed for this section is Enable/Disable Alarms. If the alarms are enabled, the Default Alarm Settings When Creating a New Entry (On/Off) How Far in Advance section appears. This consists of the following fields:

- Appointments/Meetings: Default is 30 minutes in advance
- Reminders: Default is 0
- Events: Default is one day in advance
- Anniversaries: Default is one day in advance
- To Do: Default is one day before the due date

The following screenshot shows an example of the Alarms tab:

Mail Settings : Mail Sales

Basics | **Mail File Preferences** | Message Disclaimers | Comments | Administration

Mail | **Calendar & To Do** | Access & Delegation

Basics | Display | Scheduling | **Alarms** | To Do | AutoProcess | Rooms and Resources

Enable/Disable Alarms		When to apply this setting:	Allow use change:
Enable the display of alarm notifications:	<input checked="" type="checkbox"/> Yes	Never	<input checked="" type="checkbox"/> Allow
Default Alarm Settings When Creating a New Entry (On/Off)		When to apply this setting:	Allow use change:
<input checked="" type="checkbox"/> Appointments/Meetings	30 minute(s) in advance	Never	<input checked="" type="checkbox"/> Allow
<input checked="" type="checkbox"/> Reminders	0 minute(s) in advance	Never	<input checked="" type="checkbox"/> Allow
<input checked="" type="checkbox"/> Events	1 day(s) in advance	Never	<input checked="" type="checkbox"/> Allow
<input checked="" type="checkbox"/> Anniversaries	1 day(s) in advance	Never	<input checked="" type="checkbox"/> Allow
<input checked="" type="checkbox"/> To Do	1 day(s) in advance of due date	Never	<input checked="" type="checkbox"/> Allow

To Do Tab

The next tab on our tour of the mail policy is the To Do tab. This tab provides policy administrators the ability to manage the working of to-do functions in a user's mail file.

There is one section, To Do, with two field settings:

- Hide To Do entries in the Calendar: By default unchecked
- Allow Notes to update To Do status and dates for incomplete entries: By default unchecked

The screenshot shows the 'Mail Settings : Mail Sales' dialog box. The 'Mail File Preferences' tab is selected. Within this tab, the 'Calendar & To Do' sub-tab is active. The 'To Do' section is expanded, showing two settings: 'Hide To Do entries in the Calendar:' with a checked 'Yes' option, and 'Allow Notes to update To Do status and dates for incomplete entries:' with a checked 'Yes' option.

Mail Settings : Mail Sales	
Basics Mail File Preferences Message Disclaimers Comments	
Mail Calendar & To Do Access & Delegation	
Basics Display Scheduling Alarms To Do AutoProcess	
To Do	
Hide To Do entries in the Calendar:	<input checked="" type="checkbox"/> Yes
Allow Notes to update To Do status and dates for incomplete entries:	<input checked="" type="checkbox"/> Yes

AutoProcess Tab

The AutoProcess tab provides the option to enable auto-processing of new calendar invites delivered into a user's mail file. This tab also controls automatic Inbox management. This tab has two primary categories, and one optional section:

- **Automatic Processing of Meeting Invitations:** This section has only one field: Enable automatic responses to meeting invitations. This field allows Notes users to automatically process meeting invitations. This is unchecked by default.
- When a meeting invitation is received from anyone, automatically accept only appears if Automatic Processing of Meeting Invitations is enabled. This section contains the field Perform the following action. This is a drop-down list. Choices are If time is available and Even if time is not available. If you select If time is available, two additional radio button fields appear: Automatically decline if time is not available and Let me decide if time is not available.
- Automatic Inbox Management consists of a single field, When you delete a Calendar Notice from your Inbox or a Mail folder/view. Options are Prompt to confirm deletion and Remove from this view/folder without prompting.

Basics Mail File Preferences Message Disclaimers Comments Administration		
Mail Calendar & To Do Access & Delegation		
Basics Display Scheduling Alarms To Do AutoProcess Rooms and Resources		
Automatic Processing of Meeting Invitations		
Enable automatic responses to meeting invitations: <input checked="" type="checkbox"/> Yes	When to apply this setting: <input type="text" value="Never"/>	Allow user to change: <input checked="" type="checkbox"/> Allow
When a meeting invitation is received from anyone, automatically accept:		
Perform the following action: <input type="text" value="even if time is not available"/>	When to apply this setting: <input type="text" value="Never"/>	Allow user to change: <input checked="" type="checkbox"/> Allow
Automatic Inbox Management		
When you delete a Calendar Notice from your Inbox or a Mail folder/view: <input type="text" value="Prompt to confirm deletion"/>	When to apply this setting: <input type="text" value="Never"/>	Allow user to change: <input checked="" type="checkbox"/> Allow

AdminP and mail policies:

Domino administrators can force mail policy to be applied. Overall, the mail policy settings document are applied to all users' mail files on a specific server by the administration process (AdminP). The administration process runs every six hours by default, so changes will not take effect until the next time the administration process executes. An administrator, with the correct access, can force the administration process to process new information in the mail policy settings document, by using the following command:

```
tel | AdminP process mail policy
```

Room and Reservations Tab

This is the last tab in the Calendar & To Do set of tabs in the mail policy document. This tab controls the defaults for rooms and reservations. This tab has three sections: Default Reservation Settings for choosing Site, Default Meeting Settings for Rooms, and Default Meeting Settings for Resources.

Default Reservation Settings for choosing Site contains three fields:

- Preferred Site defines a preferred site.
- Use preferred site as the default site in the Find Room and Find Resource dialog is checked by default.

- Prompt to reset your preferred site when scheduling within a site that is not your current preferred site is also checked by default.

Default Meeting Settings for Rooms has a radio button field with three choices:

- Prompt me to add rooms to my list when scheduling meetings
- Always add rooms to my list when scheduling meetings
- Never add rooms to my list when scheduling meetings

Default Meeting Settings for Resources is another section with three radio button choices:

- Prompt me to add resources to my list when scheduling meetings
- Always add resources to my list when scheduling meetings
- Never add resources to my list when scheduling meetings

Access to Your Mail & Calendar Tab

This tab allows policy administrators to control whether or not users can grant others users access to their email and calendars.¹ This tab consists of a single section that contains one field: Allow users to setup delegates to their mail file. By default, this is unselected. If you select this option, you are given the choice of when to apply it (Never, Always, or Initially) and a checkbox to specify whether the user can change this setting.

¹ In Notes/Domino terminology, this is referred to as delegating access to your mail file; a common scenario is when an executive delegates access to an assistant so the assistant can review and respond to the executive's email, schedule executive meetings, and so on.

Access to Your Schedule Tab

This tab determines how much leeway users have when granting others access to their schedule information. (In most situations, users grant some type of access to their calendars, for instance, so that others can see their free time and schedule meetings with them.) This tab has one primary section and one optional section. The primary section is Who is allowed to see your schedule information (when you are busy or available). The section contains a single radio field called Who is allowed to see it, with two options; one allows everyone to see the user's schedule information, and the other allows no one to see it.

If you select the first option, a second section called What schedule information they can see appears on this tab. This also contains a single field, with two options. Only information about when you are busy or available (in other words, another person can see whether the user is available at a given time, but cannot gain access to more detailed information such as what meetings the user is attending and with whom), and Detailed information about your calendar entries (users can see detailed calendar information). As with other menu choices, you can select when these settings apply (Never, Always, or Initially) and whether users are allowed to change this setting.

The screenshot shows the 'Mail Settings : Mail Sales' window. It has a navigation bar with 'Basics', 'Mail File Preferences', 'Message Disclaimers', 'Comments', and 'Administration'. Below this is a sub-navigation bar with 'Mail', 'Calendar & To Do', and 'Access & Delegation'. The 'Access & Delegation' section is active, showing 'Access to Your Mail & Calendar' and 'Access to your Schedule'. The 'Access to your Schedule' section contains two main settings:

Who is allowed to see your schedule information (when you are busy or available)	When to apply this setting:	Allow user to change:
Who is allowed to see it: <input checked="" type="radio"/> Everyone may see your schedule information <input type="radio"/> No one may see your schedule information	Never	<input checked="" type="checkbox"/> Allow

What schedule information they may see	When to apply this setting:	Allow user to change:
What schedule information they can see: <input checked="" type="radio"/> Only information about when you are busy or available <input type="radio"/> Detailed information about your calendar entries	Never	<input checked="" type="checkbox"/> Allow

Message Disclaimers

The ability to add message disclaimers has been enhanced in Notes/Domino 7. This feature provides a mechanism to add messages to the end of outgoing messages. These can be added by the server or by the client.² An example of a message disclaimer could be legal information about the company, or a particular department in the company. Policy administrators can enable or disable message disclaimers from the Domino server and/or the Notes Client.

Server Disclaimers

On the server, policy administrators enable message disclaimers by creating a policy document. To do this, the policy administrator must first create a policy document and add the disclaimer text. The policy administrator must then enable or disable the message disclaimer in the Server Configuration settings document. The following screenshot shows an example configuration document:

The screenshot shows the 'Configuration Settings : Domino7B2/ND7B2' document. The 'Router/SMTP' tab is selected. Within this tab, the 'Message Disclaimers' sub-tab is active. The settings are as follows:

Message Disclaimers	
Message disclaimers:	Enabled
Add disclaimer to S/MIME signed or encrypted messages:	Enabled
Logging level:	Informational

Client Disclaimers

A policy administrator can also enable message disclaimers on the Notes client. Once again, the policy administrator must create a mail settings policy document, make the appropriate policy settings, and add the message-disclaimer text.

² Note that users can also add disclaimers in earlier Notes/Domino releases. For instance, Domino Web Access (iNotes) has the ability to add disclaimers. You can also add a disclaimer to your messaging signature via a Notes client. Also, some customers have added disclaimers into the Notes mail template directly.

The Message Disclaimer tab contains five fields:

- Notes Client can add disclaimers can be enabled or disabled.
- Disclaimer text is the actual value of the text; for example, This is not to be shared outside Acme Corporation. Use the Modify button to edit this text field.
- Disclaimer text format can be HTML or plain text.
- Disclaimer position is either Append (add the disclaimer after the email message body) or Prepend (add the disclaimer before the body).
- Multilingual Internet Mail can be Use Best Match or Use Unicode (UTF-8).

The screenshot shows a web-based configuration window titled "Mail Settings : Mail Sales". It has a tabbed interface with five tabs: "Basics", "Mail File Preferences", "Message Disclaimers" (which is selected and highlighted with a dashed border), "Comments", and "Administration". Below the tabs is a section titled "Message Disclaimer" with a light blue header. This section contains five rows of settings, each with a label and a dropdown menu:

Message Disclaimer	
Notes client can add disclaimers:	Enabled
Disclaimer text:	This is a disclaimer Modify
Disclaimer text format:	HTML
Disclaimer position:	Append
Multilingual Internet mail:	Use Unicode (UTF-8)

The last two tabs (Comments and Administration) are common to all policy documents.

SMTP

There are three major SMTP features new in Domino 7:

- DNS Whitelists
- Private Blacklists
- Private Whitelists

Let's start our discussion of unwanted mail with junk mail.

Junk Mail

This type of mail can actually arrive into your email box due to some action on your part. Imagine that last week you went out on site and registered to access some information about the site, or you filled out an information card to receive a free magazine. Now you are receiving email as a result of your actions. Some of this mail may be information you want to read. However, after a while these mail messages start to add up, especially if you're on more mailing lists than you would like. To minimize this, you can request that your address be removed from the sender's distribution list. But this may not always fix the problem, especially if the sender isn't particularly meticulous about honoring such requests, or shares your address with others.

In addition, users often send each other lots of long non-work-related emails with attachments, such as holiday-greeting messages. The end result is you have a clogged email system with messages to and from known users or companies. Many corporations would consider this junk mail; at a minimum, this should be classified as non-business use of your workplace messaging environment.

Spam

The worst type of junk mail consists of messages that you have no desire to receive. This is commonly referred to as spam, and virtually every email user in the world has encountered it. With a seemingly endless number of spammers out there, asking to be removed every time you receive one of their messages can be hopelessly time-consuming, and may in fact result in receiving even more spam.

To help minimize the impact of spam, it would help if you understand how spammers got your address in the first place. They often purchase a list of names from various sources. Most reputable e-commerce companies that have your email address will place some type of banner or disclaimer stating that they will not sell your address to an external vendor. But not all companies will offer this disclaimer. Spammers can also get a list right off the Internet itself from anonymous sources, especially if you post an entry on an online service or internet bulletin board, or spend time in chat rooms on an online service.

Now, on with Restrictions and Controls:

Edit Server Configuration ✕ Cancel	
Basics Restrictions and Controls Message Disclaimers Message Tracking Advanced	
Restrictions SMTP Inbound Controls SMTP Outbound Controls Delivery Controls Transfer Controls Rules	
<div> <div>Inbound Relay Controls</div> <div>Inbound Relay Enforcement</div> </div>	
Allow messages to be sent only to the following external internet domains:	Perform Anti-Relay enforcement for these connecting hosts:
Deny messages to be sent to the following external internet domains: (* means all)	Exclude these connecting hosts from anti-relay checks:
Allow messages only from the following internet hosts to be sent to external internet domains:	Exceptions for authenticated users:
Deny messages from the following internet hosts to be sent to external internet domains: (* means all)	Allow all authenticated users to relay
<div> <div>DNS Blacklist Filters</div> <div>DNS Whitelist Filters</div> </div>	
DNS Blacklist filters: Disabled	DNS Whitelist Filters: Disabled
DNS Blacklist sites:	DNS Whitelist Sites:
Desired action when a connecting host is found in a DNS Blacklist: Log only	Desired action when a connecting host is found in a DNS whitelist: Silently skip blacklist filters
Custom SMTP error response for rejected messages:	
<div> <div>Private Blacklist Filter</div> <div>Private Whitelist Filter</div> </div>	
Private Blacklist Filter: Disabled	Private Whitelist Filter: Disabled
Blacklist the following hosts:	Whitelist the following hosts:
Desired action when a connecting host is found in the private blacklist: Log only	Desired action when a connecting host is found in the private whitelist: Silently skip blacklist filters
Custom SMTP error response for rejected messages:	

DNS Whitelist Filters

Domino messaging administrators can now enable DNS whitelist filters. This new Domino 7 feature provides the ability to identify legitimate email. Whitelists contain addresses from which you will accept incoming messages. When a DNS whitelist filter is enabled, the SMTP listener task determines (via the SMTP `helo` commands) whether the connecting hosts are listed in the DNS whitelist entries. If the connecting host is not listed in the DNS whitelists, then normal processing will continue via the DNS blacklist filters. If the host name is listed in the blacklist filter, then that host name will not be allowed to continue SMTP processing on the server.

DNS whitelist filtering applies only to hosts subject to inbound relay enforcement.

Whitelists are enabled or disabled via the Configuration document. From the Domino Administrator:

1. Click the Configuration tab and expand the messaging section.
2. Click Configuration.
3. Select Configuration settings for the server on which you would like to enable or edit the DNS whitelist filters.
4. Select Router/SMTP | Restrictions and Controls | SMTP Inbound Controls.
5. Edit each field as needed (see the example below for a definition of each field):

DNS Whitelist Filters	
DNS Whitelist Filters:	Disabled
DNS Whitelist Sites:	
Desired action when a connecting host is found in a DNS whitelist:	Silently skip blacklist filters

- DNS Whitelist Filters: Select Enabled or Disabled. Disabled by default.
- DNS Whitelist Sites: Specify the DNS whitelist sites that the SMTP listener task will use to perform DNS analysis. This analysis occurs when Domino receives an SMTP connection request.
- Desired action when a connecting host is found in a DNS whitelist: There are three options available when the connecting host is found in a DNS whitelist:
 - Silently skip blacklist filters: All whitelist actions skip blacklist filters. This action will not execute any logging.
 - Log only: This action will record the host name and IP address of the connecting server, and the name of the site where the server was listed.
 - Log and tag message: This action will add the Note item \$DNSWLSite to each message accepted from the whitelisted analysis. This action will also record the host name and IP address of the connecting server, and the name of the site where the server was listed.

Private Blacklist Filters

Next up with our new list of Domino 7 SMTP features is the private blacklist. Private blacklists can be enabled by a Domino messaging administrator to specify hosts and/or Internet domains that are responsible for sending unnecessary, unwanted mail into your messaging environment.

Private blacklists are stored in the Domino directory. This helps simplify the process of maintaining the distribution of blacklist information between servers. Private blacklists are processed after the SMTP listener task compares the name of the hosts that are subject to relay enforcement first; then the listener tasks will compare the private blacklist entries listed in the Configuration document. If a match is found in the private blacklist, the specified actions will be executed. If a match is not found, normal processing of the message will continue, with the DNS whitelist filters and then the DNS blacklist filters.

To enable private blacklists, do the following from the Domino Administrator:

1. Click the Configuration tab and expand the messaging section.
2. Click Configuration.
3. Select Configuration settings for the server on which you would like to enable private blacklists.
4. Select Router/SMTP | Restrictions and Controls | SMTP Inbound Controls.
5. Edit each field as needed, as shown in the following screenshot:

Private Blacklist Filter	
Private Blacklist Filter:	Disabled
Blacklist the following hosts:	
Desired action when a connecting host is found in the private blacklist:	Log only
Custom SMTP error response for rejected messages:	

- Private Blacklist filter: This field has two options, Enabled and Disabled (the default). Choose Enabled to allow the SMTP listener task to determine if connecting hosts have been blacklisted.
- Blacklist the following hosts: Enter IP addresses or the host names of the systems to be blacklisted. Note that IP address ranges and masks are supported.
- Desired action when a connecting host is found in the private blacklist: There are three choices:
 - Log only: This is the default setting. This records the host name and IP address of the connecting server found in the private blacklist.
 - Log and tag message: This setting will log and then tag the message by adding the Note item \$DNSBLSite to each message accepted from the blacklisted host. A value of PrivateBlacklist is assigned to this field.

- Log and reject message: This setting will log and then reject each message by returning an error response to the blacklisted host.
- Custom SMTP error response for rejected messages: You can enter custom error-message text to be sent when the connecting host's name is found in the private blacklist. For example, using a format specifier %s, you can return the IP address of the connecting host back to it in an error message. In this field you enter: Your host %s was blacklisted. Then, when Domino rejects a message from the blacklisted host 127.0.0.1, the following error message appears: Your host 127.0.0.1 was blacklisted.

Private Whitelist Filters

Domino 7 now offers private whitelist filters. The whitelist filter is used to identify exceptions to entries listed in blacklist filters. Entries that are listed in the private whitelists are exempt from each blacklist check. As a result, the whitelisted hosts will bypass blacklist filters checks.

Members of the private whitelists are reviewed by the relay, sending, and recipient controls.

The processing for a private whitelist filter is controlled by the SMTP listener task. The listener task will compare the inbound host information against the entries in the whitelist. If a match is found, then action is taken, based on selections entered.

When private whitelists are enabled, the SMTP listener task compares hosts that may be subject to relay enforcement against the defined private whitelist. If there is a match, the private blacklist, DNS whitelists, and DNS blacklists are skipped. Otherwise, processing continues, beginning with the private blacklist.

You can configure private whitelists in the Private Whitelist Filter section of the Configuration document:

Private Whitelist Filter	
Private Whitelist Filter:	Disabled
Whitelist the following hosts:	
Desired action when a connecting host is found in the private whitelist:	Silently skip blacklist filters

- Private Whitelist Filters: Disabled by default. When this option is enabled, the SMTP listener task will review each message to determine whether the

connecting host has been whitelisted. If so, it will be allowed to continue processing within the confines of the overall SMTP relay rules.

- Whitelist the following hosts: Enter the IP addresses or the host names of the systems to be added to the whitelist. IP ranges and masks are supported.
- Desired action when a connecting host is found in the private whitelist: Options are:
 - Silently skip blacklist filters: This is the default setting. This selection will allow actions to skip blacklist filter checks. No logging occurs, and all actions skip blacklist filters.
 - Log only: This selection will record the host name and IP address of the connecting server found in the private whitelist.
 - Log and tag message: This selection will allow logging to occur, similar to the Log only option. This will tag the message by adding \$DNSWLSi te to messages accepted from whitelisted hosts. The value of \$DNSWLSi te is Pri vateWhi tel i st.

Statistics

Each of these settings now provides a series of statistics that can be reviewed under server statistics or statrep. nsf (via the collector). Each of these statistics can be reviewed by typing show stat SMTP at the server console.

These statistics include DNS whitelist, private blacklist, and private whitelist data.

DNS Whitelist Statistic

The SMTP listener task will maintain a statistic called SMTP. DNSWL. Total Hi ts to keep a running count of the number of connections accepted from DNS-whitelisted hosts. You can determine the number of times a particular IP address is listed in one of the configured DNS whitelists by reviewing this statistic: SMTP. DNSWL. <Whi tel i stSi te>. IP address. Hi ts.

To collect the expanded information, set the NOTES. I NI variable SMTPExpandDNSWLStats =1.

Private Blacklist Statistic

The SMTP listener task will maintain a running count of the number of connections accepted from blacklisted hosts, and stores that count in the SMTP. Pri vateBL. Total Hi ts statistic. The SMTP. Pri vateBL. Total Hi ts statistic is part of the total SMTP statistics package.

Private Whitelist Statistic

The SMTP listener task also maintains a statistic to keep a running count of the number of connections accepted from whitelisted hosts. The statistic is SMTP.PrivateWL.TotalHits.

Summary

This chapter reviewed policy management in Notes/Domino 7. We reviewed the basics of policy management, and how you can take advantage of this powerful tool to help reduce the time and effort required to maintain a functioning and healthy Notes/Domino environment. We then examined new policy-management features introduced in Notes/Domino 7, including the new mail policy, as well as enhancements to existing policies such as security and archiving.

6

Smart Upgrade

The IBM Lotus Notes Smart Upgrade process notifies the end user that their client will be upgraded. The Smart Upgrade feature is not new with Domino 7—Lotus Notes/Domino 6 offered this automated upgrade process with its first code release. Lotus Notes Smart Upgrade works with the Lotus Notes 6 and 7 upgrade kits or incremental installers that can be downloaded from developerWorks: Lotus at <http://www.lotus.com/idd/smartupgrade>.

With Domino 7, the Smart Upgrade server can fail over within clustered servers. This is executed when a Notes client user logs on; the user's home server's Configuration Settings document is checked to access the link to the Smart Upgrade database. If the server containing the Smart Upgrade database is down, then Smart Upgrade searches (via replica ID and database name) for a replica on a server within the cluster, and tries to open the replica database on the server. After Smart Upgrade locates a replica, it opens the database so that the Smart Upgrade database on that replica server is used.

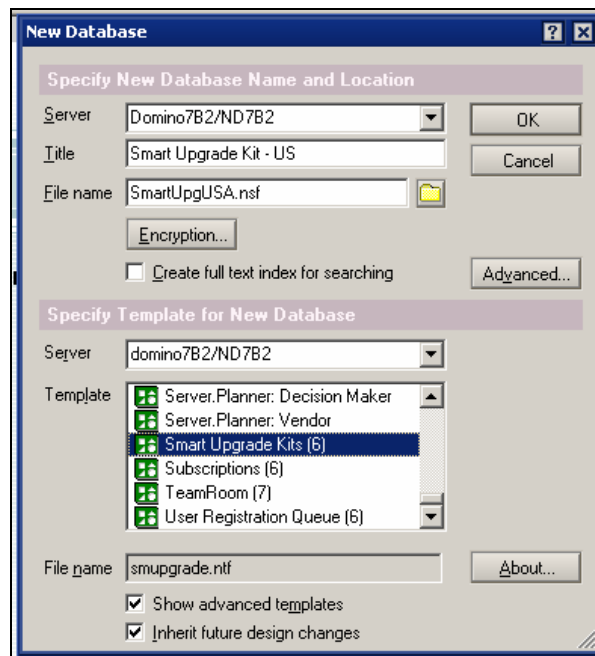
Smart Upgrade Process

The overall Smart Upgrade process is very simple. A combination of policy and Smart Upgrade settings are used to enable and configure Smart Upgrade. There are five basic steps to enable Smart Upgrade:

1. Create the Smart Upgrade Kit database using the Smart Upgrade Kits template from your server.
2. Create or modify a Server Configuration document and add a link to the database created in step one.
3. Create a kit document in the Smart Upgrade database.
4. Create or modify a desktop policy document and apply this policy via an organizational or explicit policy to the end users that you want to upgrade.
5. Create the Smart Upgrade Tracking Database. This is where data is stored about the status of the Smart Upgrade.

Create the Smart Upgrade Kit Database

The first step is to create an update database. The ACL of this database needs to be set so that users have read access (default Reader or */O = Reader). Using your Notes 7 client, select File | Database | New. This displays the New Database dialog:



Complete the New Database dialog fields as shown in the preceding illustration, and select OK to save the database.

Create or Modify a Server Configuration Document

Next, create or modify a Server Configuration document. Just open (or edit) a Server Configuration document and select the Smart Upgrade tab. This tab has been introduced in Domino 7. (Notes/Domino 6 has a single field on the Basics tab of the Configuration document.) This new tab has two categories and three fields:

Configuration Settings : Domino 7B2/ND7B2

Basic | **Smart Upgrade** | Router/SMTP | MIME | NOTES.INI Settings | Domino Web Access | IMAP | SNMP | Activity Logging | Diagnostics | Administration

Smart Upgrade

Smart Upgrade Database link:

Smart Upgrade Governor

Limit Concurrent Smart Upgrade:

Maximum Concurrent Downloads:

The Smart Upgrade category includes the field Smart Upgrade Database Link. This field was available in Notes/Domino 6 as well. This is the field where a server administrator places the database link to the Smart Upgrade Kit database.

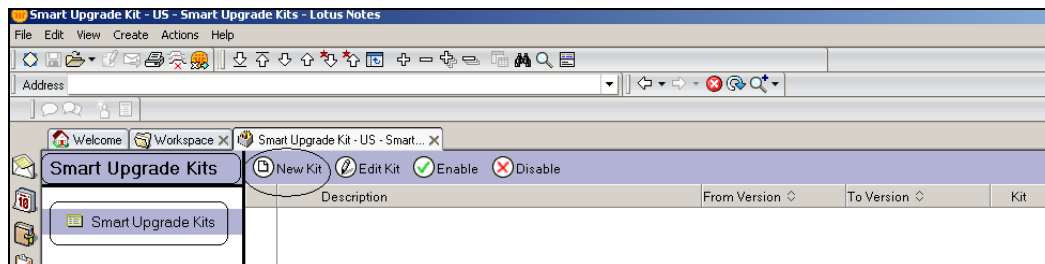
The Smart Upgrade Governor category helps limit the number of Smart Upgrade connections that process against the server at the same time. Two fields control these functions:

- Limit Concurrent Smart Upgrade: Either enabled or disabled
- Maximum Concurrent Downloads: A numeric value

Note that the example setting of 40 shown in the preceding screenshot is not a recommendation.

Create a Kit Document

Next, use the action button New Kit in the Smart Upgrade Kit database to create a new kit document.



Open the Smart Upgrade database and press the New Kit Action button. A new kit document will open. This document has two tabs, Basics and Administration.


Basics Tab

The Basics tab has five different categories:

- Basics:
- This Smart Upgrade kit can be used to update the following versions of Lotus Notes:
- After applying this kit, the client will be running this version of Lotus Notes:
- Location of update kit:
- Optional message to end users (appears in update prompt):

The following screenshot is an example of a completed kit document Basics tab:

The screenshot shows a window titled "Smart Upgrade Kit : This kit is used to upgrade the USA IT Team to Notes and Domino 7". The window has a tabbed interface with "Basics" and "Administration" tabs. The "Basics" tab is active and contains the following fields:

- Kit description:** This kit is used to upgrade the USA IT Team to Notes and Domino 7
- Enable this kit for use:** ☒ Enabled
- This Smart Upgrade kit can be used to update the following versions of Lotus Notes:**
 - Source versions: *
 - Operating system: Windows/32
 - Localization: English
- After applying this kit, the client will be running this version of Lotus Notes:**
 - Destination version: 7.0
 - Restart Notes after update: ☒ Restart
- Location of update kit:**
 - Location:
 - ☐ On a shared network drive
 - ☐ Attached to this note
 - ☒ Shared network drive & attached kit
 - Full path to update kit: f:\lotus\newnotesclient.exe
 - Optional arguments for shared network drive kit:
 - Attach update kit here:  Notes7client.exe
 - Optional arguments for attached kit:
- Optional message to end users (appears in update prompt):**
 - Message text: This will upgrade you to the new and most cool Notes 7 client! Enjoy the new great features !

Basics

This category has two fields:

- Kit description: This is where you enter a short description of the upgrade kit.
- Enable this kit for use is a single checkbox: Select Enabled to enable the kit for use.

This Smart Upgrade kit can be used to update the following versions of Lotus Notes

This category has three fields:

- Source versions: This is where you enter your current Notes client release. Optionally, you can also enter a series of Notes client releases. (See the tip below for a quick discussion of expression rules.)
- Operating system: This lets you enter and/or select the operating system for which the kit is targeted.
- Localization: There is a large list of languages that you can select from. Enter or select the language of the Notes client in this field.

Expression rules for use with the Smart Upgrade document

Smart Upgrade in Domino 7 includes a code-release version comparison. For example, suppose some Notes clients in your environment will continue to run release 6.5.3 due to some custom API. In this case, you would not enable this group to be upgraded. In other cases, you might have a specific release you would like to upgrade. This is where 'expression rules' can be used. The Smart Upgrade process compares these various code releases and then effectuates an upgrade based on these releases. The expression rules control how the upgrades are executed.

Here are a few examples of the basic rules (see the Domino 7 administrator's online help for a full list matching parameters). Note that "D" in the following list denotes any specified character:

- * (asterisk) matches any string.
 - D matches a single specified non-special character; in this case *D*.
 - \D matches a single specified character, even for special characters.
 - ? matches any single character.
 - {ABC} matches any character in the set (*A,B,C*).
 - {!ABC} matches any character not in the set (*A,B,C*).
 - +D matches any number of occurrences of the pattern *D*.
 - | performs a logical OR on two templates.
 - & performs logical AND on two templates.
-

To determine which Notes releases are being used in your environment, consult your Domino directory. The Administrator process (commonly called AdminP) is managed by a combination of a server task, a database, and proxy actions. (A more detailed description of AdminP is included in Chapter 4.) AdminP tracks which releases of Notes clients are using your Domino servers. A document containing this data is entered into the AdminP database (admi n4. nsf) and processed by the AdminP sever task. This sever task will update the Domino directory with the client information. The following table shows an example of an AdminP entry from admi n4. nsf:

*Action: (Proxy action) 46)	Update Client Information in Person Record
*Server(s) to perform the action:	Administration Server for the Domino Directory
*Name(s) to perform the action on:	Domino Admin7/ND7B2
*Action requested by:	Domino Admin7/ND7B2
*Name of process to perform action:	AdminP
Client type:	4; 3
Client's machine name:	BASEVMWAREONE
Client's platform type:	Windows/2000 5.0 Intel Pentium
Client's build number:	Release 6.5.3

This AdminP example entry shows how AdminP updates each person document. AdminP takes information from this document and updates the Domino Directory with it. This includes client platform type and client build number. One great feature is that this works not only for Domino 7 but also for Notes/Domino 6. Here is a comparison of how this data looks in a Domino 6 and in a Domino 7 directory (person documents).

Domino 6

This example shows data for client license, machine names, client platforms used, Notes client build, network account name, and change request:

Notes client license:	Lotus Notes Administration, Lotus Notes Designer
Notes client machine:	WorkStationA, WorkStationB, WorkStationC
Notes client platform:	Windows/NT 5.0 Intel Pentium, Windows/NT 5.0 Intel, Windows/NT 5.0 Intel Pentium
Notes client build:	Release 6.0, Release 6.5, Release 6.0.2CF1
Network account name:	(Network Account Name here – if used)
Change request:	None (used for other AdminP Activities)

Domino 7

Along with all the information shown in Domino 6, Domino 7 includes some DB2 account name information as well.

Notes client license:	Lotus Notes Administration, Lotus Notes Designer
Notes client machine:	VMWAREONE, BASEVMWARE, BASEVMWAREONE
Notes client platform:	Windows/2000 5.0 Intel Pentium, Windows/2000 5.0 Intel Pentium, Windows/2000 5.0 Intel Pentium
Notes client build:	Build V70_M4_12162004 Beta 3, Build V70_M4_12162004 Beta 3, Release 6.5.3
Network account name:	(Network Account Name here – if used)
Change request:	None (used for other AdminP Activities)
DB2 account name:	(If used)

As you can see with each example, this is where you can identify each build release. Now you can use the matching rules to provide an upgrade path for Smart Upgrade.

Now let's use the data (thanks to AdminP) from the Domino Directory and upgrade these clients. Here are the clients we have identified that we would like to upgrade to Notes 7:

- Release 6.0
- Release 6.5
- Release 6.0.2CF1
- Build V70_M4_12162004 beta 3
- Release 6.5.3

Next, you must build a list of potential matching patterns; for example:

Example Pattern	Comments
*	This is a wild card that will match any release. Use this to upgrade all clients found.
Release 6.0	This will upgrade any Notes client code that is listed as Release 6.0.
Release 6.5.{1-3}	This will upgrade any Notes client at Release 6.5.1, 6.5.2, or 6.5.3 to the target release.
Release 6.0.?	This will upgrade clients listed at 6.0.x (x being any release).

After applying this kit, the client will be running this version of Lotus Notes

This category has two fields, Destination Version and Restart Notes after upgrade:

- Destination Version has limited effect on the client upgrade process. Many administrators will place a 'V' in front of the target upgrade number. In some cases, administrators have noticed that the Smart Upgrade process will interpret 6.5.3 and 6.5.3FP1 as the same version, and will not update the client.
- Restart Notes after upgrade is a single checkbox. If Restart is checked, the client will restart Notes after the upgrade has completed.

Location of update kit

This category has five fields that you can set up:

- Location is the location of the actual upgrade kit. There are three options: On a Shared network drive, Attached to this note, and Shared network drive & attached kit. Note that the Smart Upgrade process checks whether a Full Path kit is available. If the Full Path kit is available, it is used; otherwise, the attachment kit is used.
- Full path to update kit is the drive or UNC path to the location of the upgrade kit. The Universal Naming Convention (UNC) is a naming convention for files that provides a machine-independent means of locating the file. A UNC name will include a reference to a shared folder and file accessible over a network, rather than a folder and file specified by a drive letter and path. A UNC name for the install kit provides a less specific path requirement in case users have different mappings based on their business unit or division.
- Optional arguments for shared network drive kit: You can use optional arguments when launching the Smart Upgrade kits. (See the note opposite for information about these arguments.)
- Attach update kit here is where you can place an attachment for executing the upgrade.
- Optional arguments for attached kit also contains optional arguments when launching the Smart Upgrade kits. (See the note that follows.)

Optional Arguments

There are two places to use optional arguments as part of the setup process: from the pointer to a full path of the kit (mapped drive or UNC), and directly in the kit document (if the setup file is attached). These optional arguments are used when launching Smart Upgrade. Examples of the various arguments are listed below:

Optional command line argument	Description and use
/a	Administrative installation.
/s	Silent mode.
/v	Pass arguments to MSiexec. All arguments entered to the right of the argument /v apply to MSiexec.
q	Sets the interface level. For example, /qn indicates that no user interface displays during the upgrade.
qn+	Displays no user interface except for a message box at the end of the upgrade.
qb+	Displays the basic user interface and a message box at the end of the upgrade.
/px	Web Kit installations—sets a path to the default program directory and the default data directory.

Use the following format to run the upgrade in silent mode without a progress bar:

```
Setup.exe /s/v"/qn"
```

Use the following format to display a message when the upgrade is complete or it has failed. Use the + parameter as follows:

```
Setup.exe /s/v"/qn+"
```

Use this format to display a progress bar during the upgrade, in addition to displaying the message indicating that the upgrade is complete or it has failed. Use the b parameter as follows:

```
Setup.exe /s/v"/qb+"
```

Optional message to end users (appears in update prompt):

This category has only one field: Message text. This is where you can enter a message that will appear when Smart Upgrade prompts users to upgrade their Notes client.

Administration Tab

The second tab in the kit document is the Administration tab. This tab has one category with four fields:

- **Allowed Users & Servers:** This is where you can enter (or select) the users or servers allowed to upgrade their Notes clients. You can use O- and OU-level entries to include all users in a particular organization.
- **Owners:** This is the typical 'owners' field that you would find on most Administration tabs. Enter or select the persons who own this document.
- **Administrators:** This lets you enter or select the users who administer the document.
- **Comments:** This field is optional; it lets you enter comments such as the update history for the document.

The following is an example of a completed kit document Administration tab:

Smart Upgrade Kit : This kit is used to upgrade the USA IT Team to Notes and Domino 7

Basics Administration

Administration:

Allowed Users & Servers:	Mike Smith Bubba Jones LocalDomainServers	This is a reader names field - be careful so you don't lock yourself out of this document
	Note: If you enter any names in this field, you will also want to add the group LocalDomainServers so that this document will replicate.	
Owners:	Domino Admin7/ND7B2	
Administrators:	LocalDomainAdmins	
Comments:	This is the upgrade Kit for USA IT Team	

Create or Modify a Desktop Policy Document

We now return to the desktop policy document. This time, we will focus on just the Smart Upgrade Tab. This tab has two categories: Smart Upgrade and Smart Upgrade Tracking Options.

One of the big advantages of using policies is that you can now assign various Notes code releases to specific departments and groups.

Smart Upgrade

This category has three fields:

- **Deploy version** is where you place information about the target release that will be sent out to each user.

- Upgrade deadline is a date selection that the policy administrator can enable. Use mm/dd/yyyy format to enter the date by which users must upgrade. If users do not accept the upgrade by this date, the upgrade takes place automatically.
- Remind me every hour after "upgrade deadline" has passed: This is an optional field. If a date is selected, then end users can be reminded every hour or so to upgrade. (Try this with the executives in your company!)

Smart Upgrade Tracking Options

This category has the following fields:

- Mail-in Database for Smart Upgrade Tracking reports: This is where the policy administrator can enable Smart Upgrade Tracking by selecting the mail-in database name. When Domino firsts starts, it will create a mail-in database named Lotus Notes/Domino Smart Upgrade Tracking reports database (l ndsutr. nsf). This database is created using the database template l ndsutr. ntf. Domino will also create the corresponding mail-in database document for the Smart Upgrade Tracking reports database. Smart Upgrade Tracking reports are automatically created each time Smart Upgrade runs on a Notes client.
- Remove Smart Upgrade Tracking files after a specified number of days: The policy administrator will have two choices. Yes means this option will automatically remove the Smart Upgrade Tracking files when the day setting is reached; if Yes is selected, then an optional field Number of Days to keep Smart Upgrade Tracking files is displayed, where you can specify the number of days. If you select No, the Smart Upgrade tracking files are not deleted.

The following is an example of a completed Smart Upgrade tab:

The screenshot shows the 'Smart Upgrade' tab within the 'Desktop Settings' window. The window title is 'Desktop Settings : Desktop Sales'. The 'Smart Upgrade' tab is selected, showing the following configuration:

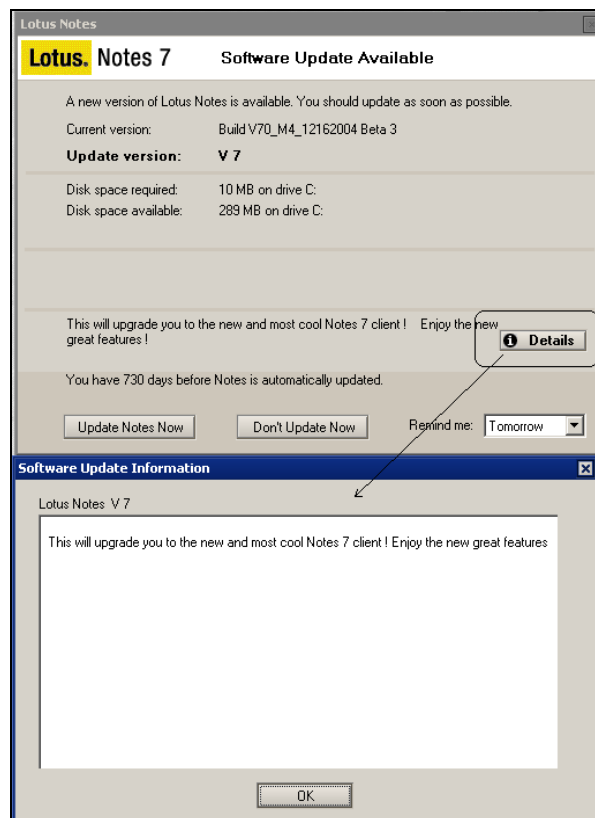
- Smart Upgrade**
 - Deploy version: v7
 - Upgrade deadline: 04/07/2007 16
 - Remind me every hour after "upgrade deadline" has passed: ☒ Remind me every hour
- Smart Upgrade Tracking Options**
 - Mail-in Database for Smart Upgrade Tracking reports: Lotus Notes/Domino Smart Upgrade Tracking Reports - ND7B2
 - Remove Smart Upgrade Tracking files after a specified number of days: ☒ Yes
 - Number of days to keep Smart Upgrade Tracking files: 365

Smart Upgrade Tracking Database

Smart Upgrade Tracking database was a feature that was introduced in Notes/Domino 6. This is the location for storing Smart Upgrade Tracking reports. These reports contain detail information about the status of each attempt to run Smart Upgrade on each Notes client. Smart Upgrade Tracking reports are automatically created each time Smart Upgrade runs on a Notes client. Policy administrators can use the Smart Upgrade Tracking reports database to monitor the Notes clients' upgrade status. This database can also be used to monitor for upgrade issues.

The End-User Experience

Overall, the upgrade process is very easy for the end user. As mentioned previously, the Domino administrator will enable Smart Upgrade to send out a notification to each end user via a set of policies. After the end user logs into his or her Domino home server, the comparison process will execute, and (if needed) a notification will be sent out to the user starting the upgrade process. An example of the initial process is shown in the following screenshot:



A few things to keep in mind before we end this chapter:

- For the 'automatic' update notification to work properly, the mail location in the location document must be set to **On Server**. Also, the home mail server must match verbatim (it is case-sensitive) and should use the fully hierarchical convention as in the server document.
- The tracking report does not work properly if the **Restart** option is selected.
- Prior to Notes/Domino 6.5.4, there was *one* field in the form for optional parameters; in 6.5.4 and later, there are *two* (one for share network and one for attached). Only the Notes 6.5.4 and later client code can interpret both fields. Older clients can not comprehend the optional parameters for attached upgrade procedures. To work around this issue, create the Smart Update kit as usual, but for backwards-compatibility, provide the optional parameters in the network drive selection. Make sure to attach the kit before saving the document, or you'll receive an error message.

Summary

In this chapter, we discussed the enhancements made to the Smart Upgrade process in Domino 7. We reviewed Smart Upgrade basics, how it works, and how you can use it. The Smart Upgrade process allows you to know when your users need software upgrades, without having to rely on them to notify you (or having to keep in constant contact to monitor their desktops).

7

Performance Aspects and Additional Standards

Performance

If there is one area where you can start a fight between computer geeks, it is with the word *performance*. For this discussion, we will define two basic types of performance: measured and perceived:

- **Measured performance** involves using a formal set of metrics to determine the ability of a system to provide a specific service within a certain set of criteria. Note that one of the more important of these criteria is time.
- **Perceived performance** is how the end user reports the ability of a particular system or service to execute a series of tasks.

Both types of performance definitions can be used to determine how a particular system or service is performing. Normally, measured performance is used to determine whether the end-user perceived performance adequately meets service levels. In the real world, you may be on the fastest system in the universe, yet the end user will tell you it is slow. Again, formal metrics can come to the rescue.

Domino 7 delivers better performance than previous releases. This has been true with each release; the impact for you is that you need to determine how each of these improvements really plays out in your organization.

When upgrading, there seem to be two basic philosophies:

- Upgrade all of your servers and users, and see what happens. ☹
- Build a formal test plan and a set of metrics, and determine what steps you need to execute before you upgrade. ☺

Can you guess the method we recommend?

When building metrics, here are the basic steps to get started:

1. Identify monitoring tools for your particular operating systems (in this section, we will be showing Perfmon for Windows 2000).
2. Identify some type of testing tool so you can set up a performance test (we will be using Lotus Domino Server.Load).
3. Document a current IT-production architecture of your Notes and Domino environment.
4. Create a test environment that statistically represents your production environment.

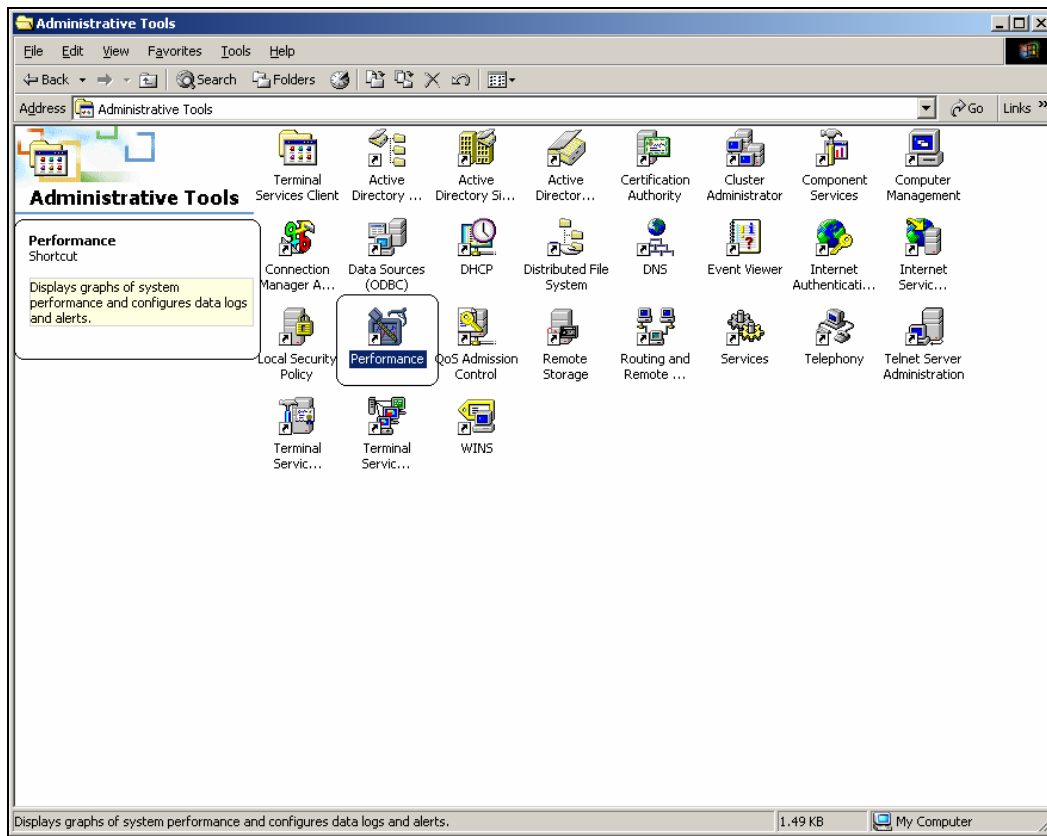
Identify Monitoring Tools

Most operating systems have some type of monitoring system. Windows 2000 has a program called Microsoft **Performance Monitor (Perfmon)**. Also, there are many different commercial 'off-the-shelf' programs that you can use.

Perfmon is a native operating system tool included in many Microsoft products. This tool provides the ability to view the internal operating of the operating system, and the various tasks that are running. Perfmon provides several interfaces that can be used to monitor system real-time activities. Perfmon lets you:

- Monitor CPU, memory, and disk activities.
- Display data in a variety of charts and graphs.
- Provide a real-time export of data (we will be using this one).
- Issue alerts, and execute specific actions based on those alerts.
- Acquire data over all extended time frames.
- Save monitoring configurations for later use.

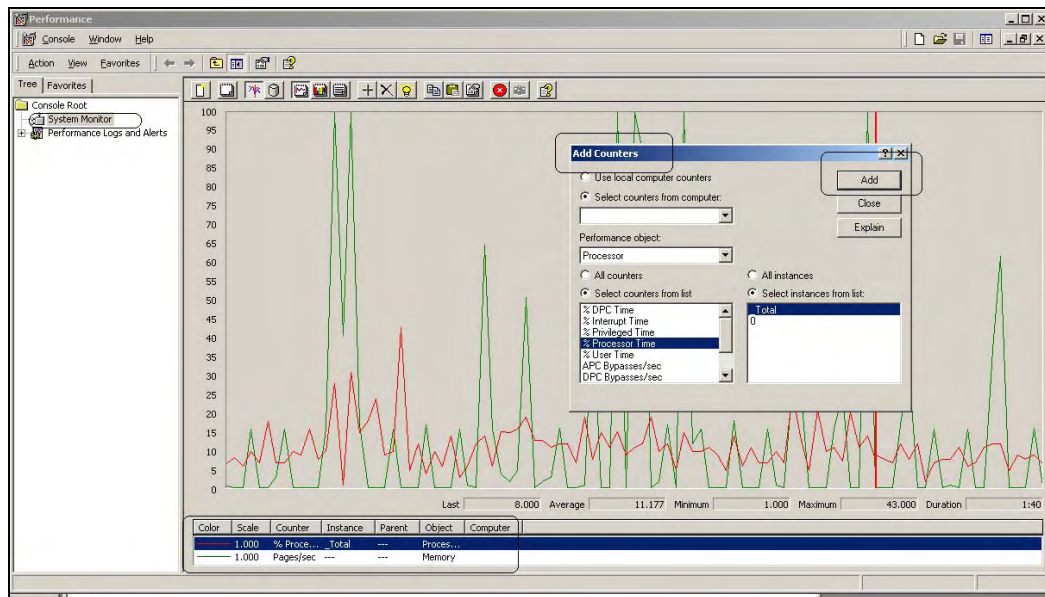
There are several methods to launch Perfmon. You can open the Start menu, select Run, type Perfmon, and press *Enter*. Or, open Administrative Tools, shown opposite, and select Performance:



When you start Perfmon, a chart appears. This chart will allow you to track various operating system, hardware, and application activities. This chart will allow you to extract real-time data, as well as allow you to review captured data.

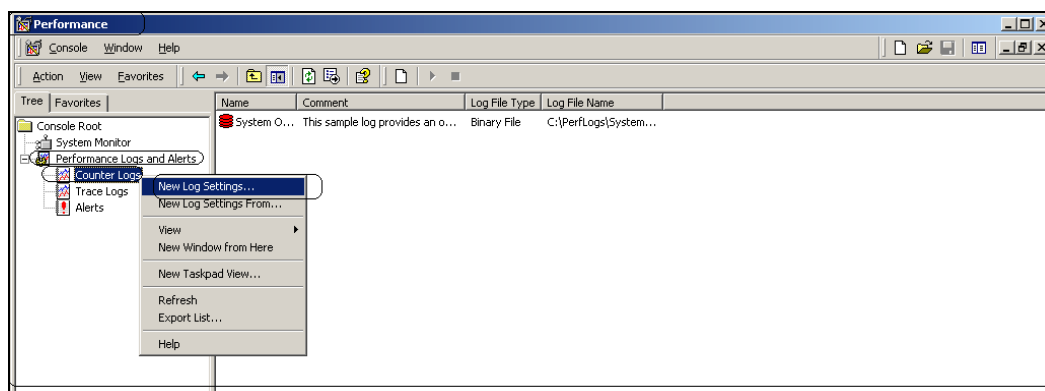
The screenshot that follows shows how you can add various objects that you can monitor. The first area is the main graph, where a plot line is displayed for each counter. Under the graph area, a counter shows details, including averages, minimum and maximum values for the selected counters, etc. At the bottom of the window is a list of added counters defined as the legend. This list displays the counters added to the Chart view, and indicates their plot line colors and their display scales.

Performance Aspects and Additional Standards

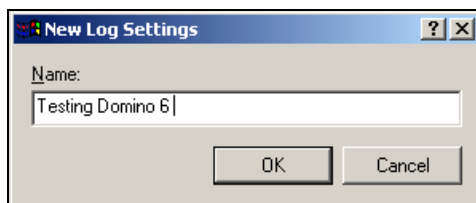


Perfmon can also track data and export it to a variety of log files. Our testing examples will be using CSV files. Overall, it is a simple process to enable this tracking. Use the following steps:

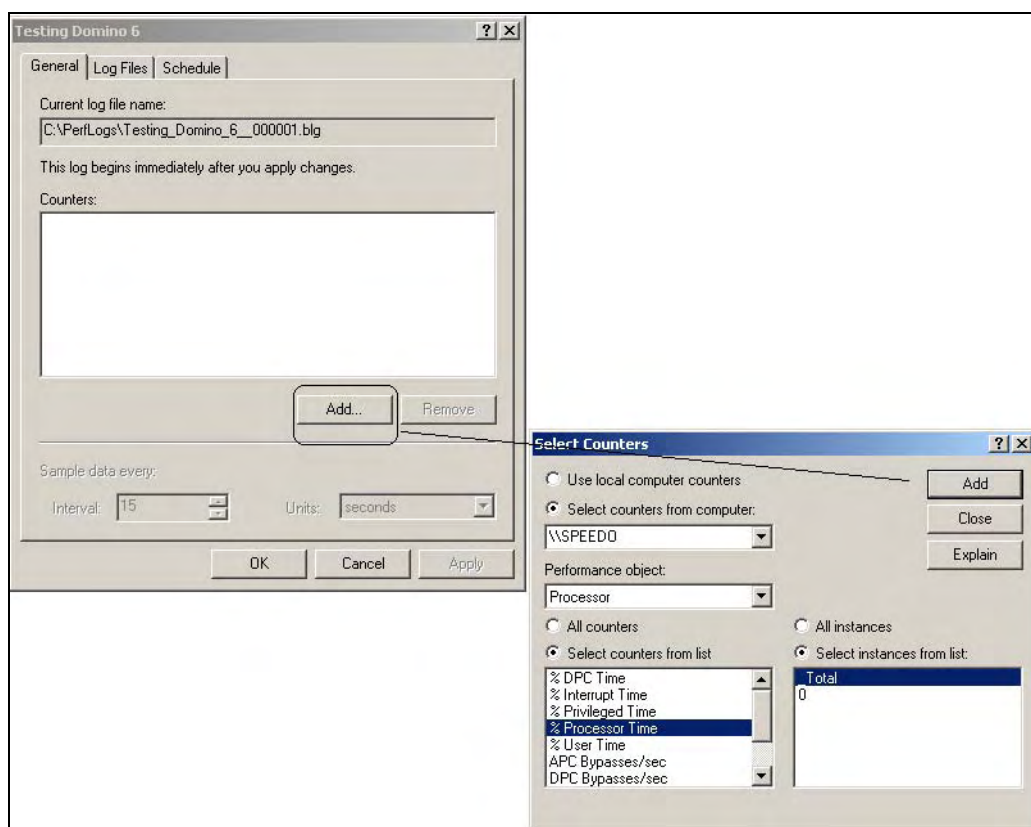
1. Launch Perfmon.
2. Expand Performance Logs and Alerts.
3. Select Counter Logs.
4. Right-click on Counter logs. From the dialog box that appears, select New Log Settings:



After you select New Log Settings, you will see the following dialog. Enter a name for the new log file.



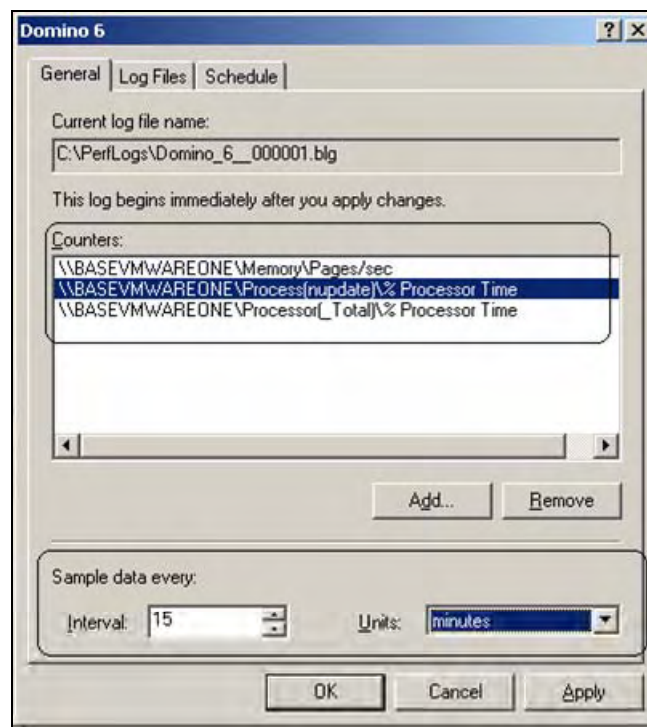
Another dialog box will display, with three tabs: General, Log Files, and Schedule. The General tab will allow you to add each counter. The following screenshot shows you how to start that process:



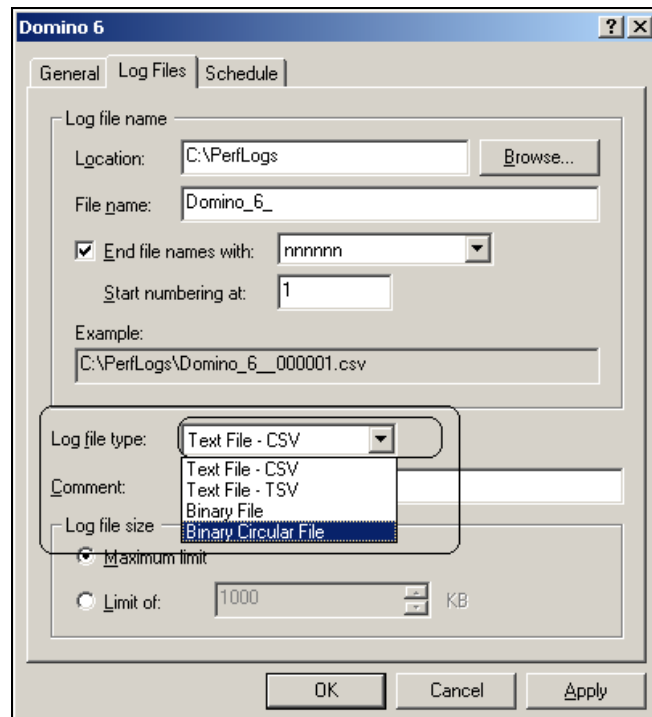
Next, you must add each counter. There are some basic items that should be reviewed with any Domino performance test. These include pages per second, total CPU time, and Updater tasks. The screenshot below shows how you can add each one. Each counter is added one at a time. The counters are located as follows:

- You will find Memory pages per second in the Memory section.
- You will find Total Processor time under Processor.
- You will find Nupdate under Process.

When each counter has been added, set the unit sample time as needed. The example below shows an interval of 15 minutes.



The next step is to enable the type of logging you will need. The examples shown in this chapter use a CSV format. The following screenshot shows how you can set this:



The final step is to set the schedule and enable the collection process. Once the collection process is started, a CSV file will be created. Once this is done, you will be able to use this file to determine the performance results of each test.

Server.Load

You have now seen one method (based on Windows) for how to collect data from a test. The next step is to set up a process to execute a test. To help you do this, Domino provides a tool known as Server.Load. This tool is used as a capacity-planning mechanism that you use to run various scripts. Using both Server.Load and monitoring tools like Perfmon, you can collect and analyze various metrics about each test. Server.Load runs via a Notes Administration client. As part of any single set of tests, you could configure several clients (Server.Loads) to put a performance test on a target server. The Server.Load process is based on an executable and a series of scripts. Server.Load includes a set of built-in scripts that can be customized to accommodate a particular test and environment.

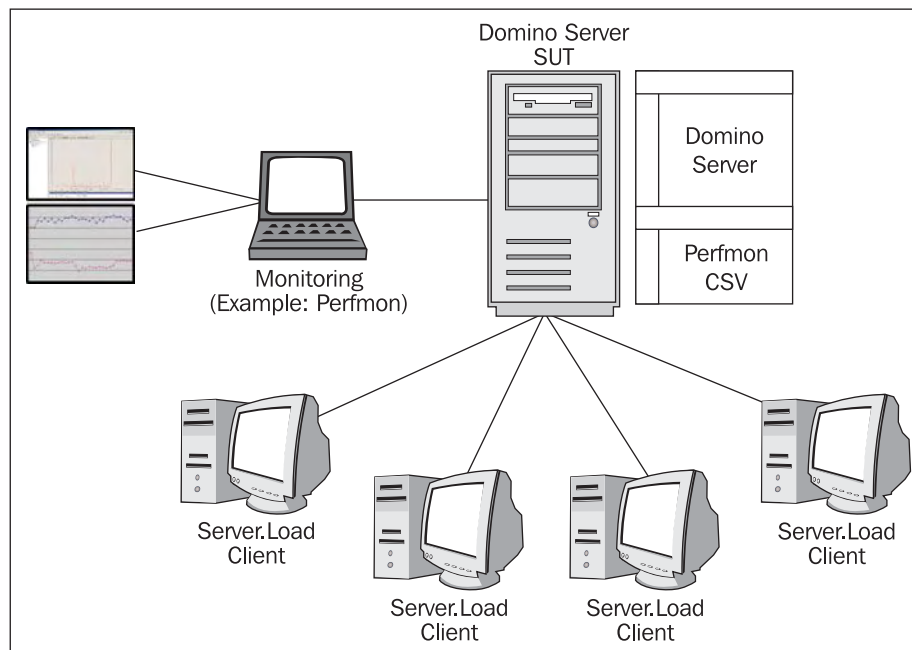
One great feature of Notes and Domino is the extensive help files. Just open the Administration help database, and you will find all you need to know about Server.Load. Also, to run Server.Load, you need to install it as part of the Administration client installation process. Once installed, it is ready to use.

The basic testing architecture includes the following elements:

- A target test server (this is known as the server under test, or SUT)
- Test clients running Server.Load
- Scripts (built-in or customized)
- Monitoring and data collection (note that Server.Load will collect many statistics)

The Server.Load client tests and generates the activities that are presented to the server. A typical Server.Load configuration has one or more client systems driving the server under test. Each client running Server.Load executes a simulated user load of Notes transactions against the server under test. A set of statistics is also generated back to the Server.Load tool. These statistics can be reviewed and analyzed to help determine the server performance.

Overall, the testing and the use of Server.Load are intended for a test environment. In most cases, it is not a good idea to stress-test a production server. This could have adverse effects, especially when you need to have a server available during production times. So please consider carefully what servers you test, and if possible, use a system in an isolated test environment that emulates your production architecture.



To set up Server.Load, do the following:

1. Identify the server under test.
2. Verify that you have Administrator access, create-database access, and access to run unrestricted LotusScript and Java agents. Also verify that the server, replicator, router, and update tasks are running.
3. There is a series of agents that will need to be copied into the test Domino directory. You will find these agents in the namagent.nsf database.
4. Create NotesBench Mail person documents. To do this, refresh all documents. Then set the following:
 - Set HTTPPassword to NotesBench
 - Set Message Storage Format = MIME
 - Set Message Storage Format = No Preference
 - Set Message Storage Format = Notes
5. Update the ACL of mail databases to include Owner (mail1, mail2, ...).

Next, you must set up each Server.Load client:

1. Verify that the Domino Administration client with Server.Load installed is configured on each client that you want to run it with.
2. Each client may need be able to use and access mail templates. Verify that you have access to each of these templates. In general, the more the RAM, the better, with each client (at least go for 512 KB per simulated user/thread).
3. Edit and configure the location document on each client. Edit the following fields: Mail File Location and Mail file name.
4. Open the Server tab in the location document and make sure that the home and mail server sections have the name of the server under test. (You should be using a Notes.id that has administration access to this server.)
5. After all connectivity has been tested and verified, you are ready to proceed.

Next is to review the various internal scripts. These include:

- Idle workload
- Cluster Mail workload
- R5 IMAP workload
- R5 Simple Mail Routing
- R5 iNotes workload
- R6 Mail workload
- R6 iNotes workload

- R6 IMAP workload
- R5 Shared Database
- SMTP and POP3 workload
- Web Idle workload
- Web Mail workload
- Workload Data Collection
- Workload Data Rollup
- Cluster Mail Initialization workload
- R5IMAP Initialization workload
- R6IMAP Initialization workload
- iNotes Initialization workload
- NRPC Mail Initialization workload
- SMTP and POP3 Initialization workload
- Web Mail Initialization workload

Each of these tests can be run as is, or can be modified to run a customized test.

All of these various tests will have some type of configuration settings. The following table describes the settings available, based on each test type. Not all parameters are used with all tests.

Variable	Action
MailServer	Enter the canonical name of the mail server; for example, CN=MailServerA/O=ND7.
nb_dbdir	Enter a database directory relative to the Notes data directory; for example, 'mail'.
MailTemplate	Enter the name of the mail file template.
Message storage format	2 (MIME).
Mail system	0 (SMTP/POP3).
NumMailNotesPerUser	Number of specific notes used to populate a test mail file when the mail file is created.
NormalMessageSize	Enter the size of the body of the message.
Max No. of Users	Enter the number of targeted simulated users (1 by default).

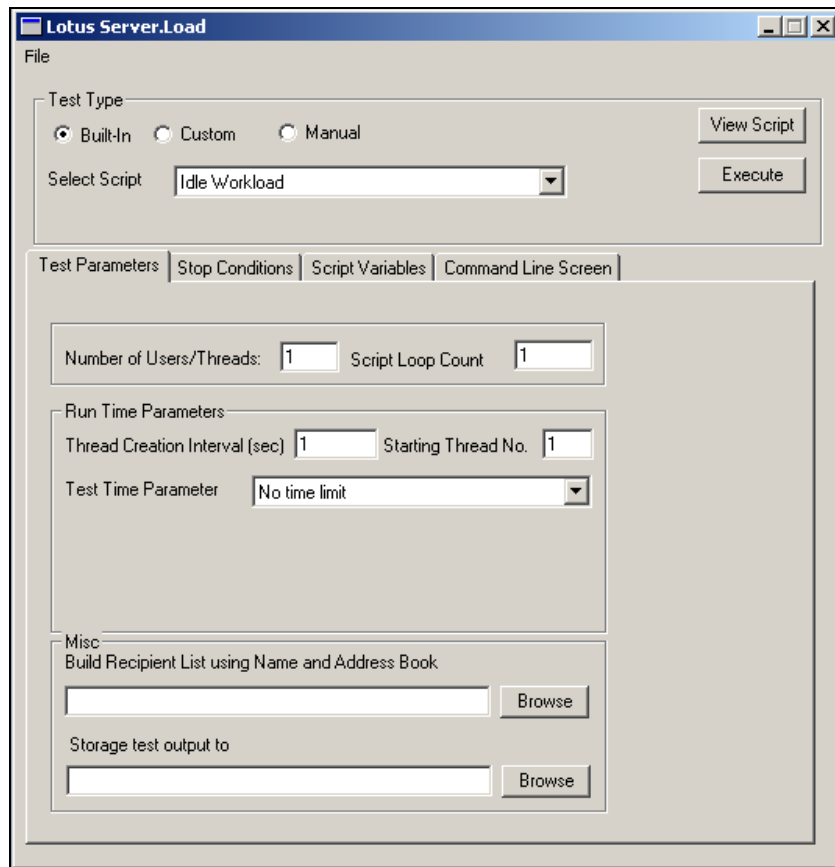
Variable	Action
Script Loop Count	Enter the number of times the script runs per targeted simulated user (1 by default).
Thread Creation Interval (in seconds)	Enter the interval at which the simulated users are created, in seconds (1 by default).
Starting Thread No.	Enter the thread number that will start the test (1 by default).
Test Time Parameter	Choose one of the following: No time limit: This will run the test indefinitely. (This is the default option.) Run between two time periods: This runs the test between start and stop times that you enter, in standard format (3:00 PM) or military format (15:00). Specify Total Test Time: This runs the test for the specified number of minutes.
Build Recipient List using Name and Address Book	Click Browse and select the Domino Directory or Personal Address Book to use when building a list of recipients to be used for testing.
Storage test output to	Click Browse and choose the location to store test output data.
NormalMessageSize	Enter the size of the body of the message.
MessageLineSize	Enter the number of characters per line.
RecipientDomain	Enter the name of the domain containing the intended recipients; for example, thecompany.xyz.
SMTPHost	Enter the fully qualified domain name of the Domino server that is running the SMTP Listener task; for example, example:theserver.thecompany.xyz.
ClientHost	Enter the fully qualified domain name of the client; for example, theclient.thecompany.xyz.
NumMailNotesPerUser	Enter the number of documents to populate the mail file when it is created.
NBTestReset	Enter one of the following to control how to handle existing documents at the start of the test: 0 = To ignore existing documents 1 = To delete existing documents

Variable	Action
HTTPHost	Enter the TCP/IP address or host name of the Domino Web server.
Domain	Enter the name of the Notes mail domain.
DiscussionDB	Enter the name of a test discussion database.
DiscTemplate	Enter the name of the template used for the test discussion database.
MaxDocToDelete	Enter the number of documents to delete when the test starts. After deleting documents, the initial document count is reset.
NumMailNotesPerUser	Enter the number of documents to create for each user to populate the database initially.
DiscDbAddDocRate	Enter the number of documents to add for each user.
MaxSessions	Enter the thread capacity of the client.

Also available are some NOTES.INI settings; for example:

NOTES.INI Setting	Description
NB_SteadyStateTime	Enter the number of minutes to disregard, in order to ensure you are getting steady-state data. The default is 30 minutes.
NB_MeasureTime	Enter the number of minutes after steady state that the rollup should read data. The default is 60 minutes.
NB_SaveCMDConsole	Set this value to 0 (zero) prior to running the Workload Data Rollup script. The default is 1.
NB_Rollup	Enter 1 to enable the Data Rollup Workload to run.

There are several methods to get Server.Load started. One quick way is to select Start | Run on the installed Notes Administration client, then select: C: \Program Files\Lotus\notes\sl oad. exe. Once Server.Load is started, the following screen will be displayed:

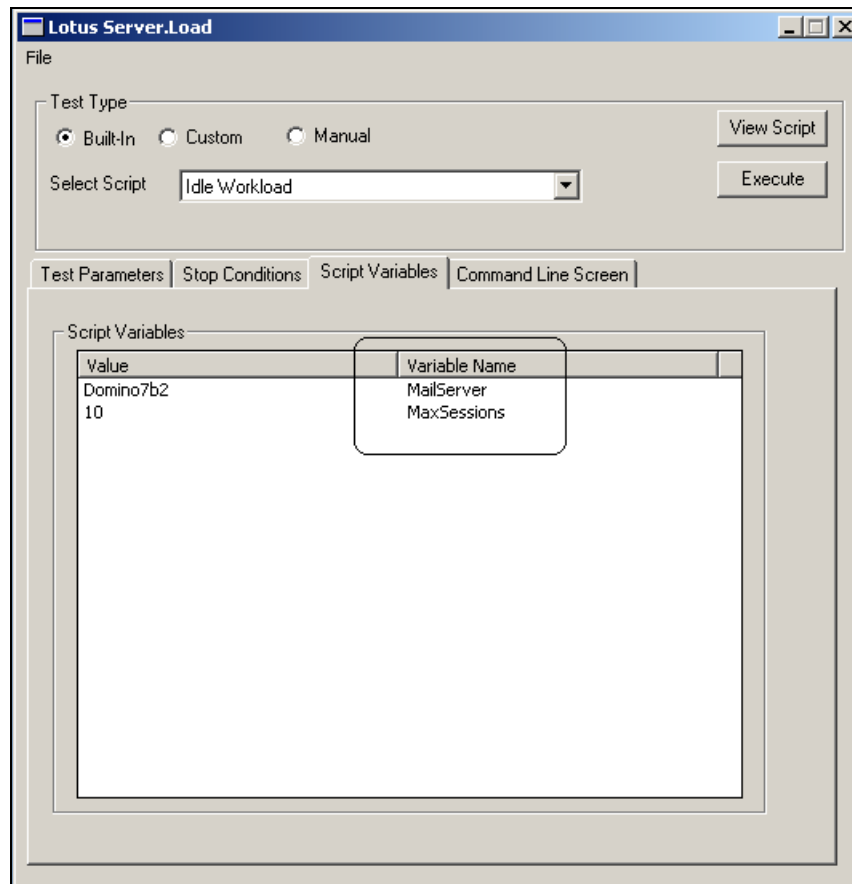


The example script shown is Idle Workload. This script can be viewed by clicking the View Script button. An example of this script is shown below:

```
* Wait for other scripts to finish initialization
* pause 0-3min
pause 0-180000
* Open the desired number of sessions
sessionsopen "[Mail Server]" [MaxSessions]
* Wait for other systems (if any) to open additional sessions
pause 2h
* Close all opened sessions
sessionsclose
```

A description of these commands can be found in the Notes Administration help database.

In the following example, we are running the Idle Workload test. Compare the script just listed and the following screenshot. You will see variables named MailServer and MaxSessions. These parameters are used by Server.Load to configure the test and what server to run on.



After you have set up the test and entered all of the variables, you will be ready to execute and test the server.

The following screenshot shows the dialog box that displays when you press **Execute**. This box allows you to add various metrics and statistics that can be monitored during the test. Also, you can monitor server statistics via the Collector process by typing `show stats` at the server console. After you have configured your metrics, press **Start Test**.

Lotus Server.Load

Script Metrics
SESSIONSOPEN

Server Stat Metrics
Database.DbCache.CurrentEntries

Add Metric

Delete Selected Metric

Metric	Min	Max	Avg	Total Operations
SESSIONSOPEN	0	0	0	0
Database.DbCache.CurrentEntries	0	0	0	0

Start Test

Stop Test

View Output

Close

Server to receive Console Commands: Domino7b2

Store the Metrics to this File: Browse

Per Minute Thread Stats

Min. Trans (Per Thread)

Max. Trans (Per Thread)

Avg. Trans (Per Thread)

Total Trans (All Threads)

Running Threads

Agg. Replications:

Avg. Rsp Time (ms)

Running Time (min)

Server Errors

Server Not Resp.

Session Timeout

Sem Timeout

Start Date/Time:

End Date/Time:

Waiting for Start of Test...

When the test has completed, you can choose View Output to see the results of each test activity. You can also review the various metrics that were updated during the test.

The following test and results are listed here to show how you can run Server.Load and interpret results. These results are *not* scientific, and should not be used as part of any architecture planning. The results cannot be used to make any assumptions or correlations about the performance of Domino 7.

The authors do recommend that you set up your own test environment and conduct your own tests.

For fun, the authors set up a simple test with Server.Load on a Windows server. The test was configured using the following parameters and variables:

- Dual Processor server (450 MHz each)
- 1 GB of RAM
- Domino 7 (Beta 4 version)
- DB2 not enabled
- Windows 2000
- Windows Perfmon (running on the server under test) was used to collect process and operating system data. The parameters collected were Nserver (process), pages per second (memory), total CPU (both CPUs), and processor.
- Server.Load, executed on an IBM Thinkpad T40 (2 GB RAM).
- Test executed 24 hrs total (only a limited amount of data extracted to show results).
- A custom Server.Load script was used.
- A private home network based on 100 MHz was used for access into the server.

The custom Server.Load script is listed below:

```
* Wait for other scripts to finish initialization
* pause 0-3min
pause 0-180
* Open the desired number of sessions
sessionsopen "[MailServer]" [MaxSessions]
* Wait for other systems (if any) to open additional sessions
pause 1-150
* Close all opened sessions
* Pause a random interval so multiple processes are staggered well
pause 0-22
* Start the part of the script, which loops.
*****
beginloop
*****
* Access an icon on the server
webget -url [httphost]/
* Wait 1 minute
pause 1-16
*** Repeat entire sequence all over again (go back to beginloop
statement)
*****
rewind
*****

sessionsclose
```

The test was executed, and the CSV file was extracted. The following data was analyzed using a simple average function in Excel. The averages for Notes/Domino 6 and Domino 7 are shown in the table. Basically, the Domino 7 server used a bit more memory, but the Nserver task and the total processor time were lower.

ND6		
\\PE2300\Memory\ Pages/sec	\\PE2300\Process(nserver)\ % Processor Time	\\PE2300\Processor(_Total)\% Processor Time
76.70391885	2.890554585	82.34269523

Domino 7		
\\PE2300\Memory\ Pages/sec	\\PE2300\Process(nserver)\ % Processor Time	\\PE2300\Processor(_Total)\% Processor Time
115.532763	0.759714033	75.71121849

Whether you will see similar results in your own environment depends on a number of factors, including end-user activity levels, size of mail files, server configuration, and network configuration.

Be sure to set up a test environment that emulates part or all of your production environment. Execute the testing, and then determine whether you need to make any system changes to your architecture.

LEI

Lotus Notes and Domino has a long history of data integration tools and techniques. Looking back at Lotus Notes 3, you will find Open Database Connectivity (ODBC) connectivity¹ options using @DBColum and @DBLookup. These functions provided some simple connectivity. Later, Lotus purchased a product known as NotesPump. This product provided a series of connectors that allowed a developer (via LotusScript) to extract data from various stores (including Structured Query Language).

Over time, IBM/Lotus developed additional integration methods, including:

- Domino Enterprise Connection Services (DECS)
- LotusScript Data Objects (LS:DO)

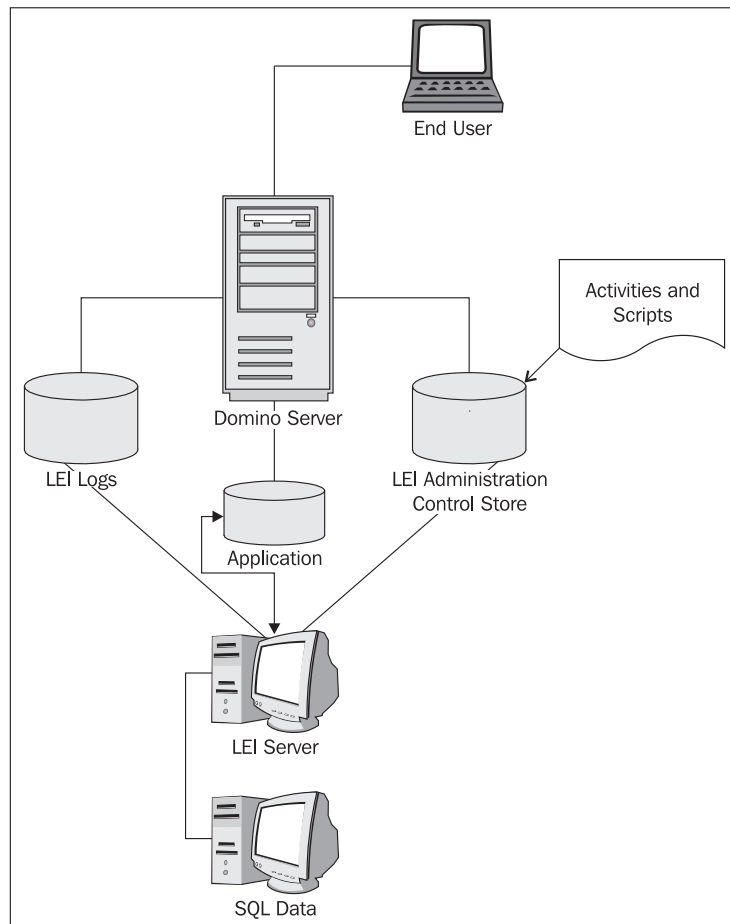
After several iterations and improvements, the **Lotus Enterprise Integration (LEI)** was developed. LEI provided many of the features of each of the preceding connectivity products. LEI also provided additional features with Domino 6. One very cool feature is

¹ ODBC is a database access method developed by the **SQL Access Group (SAG)** in 1992. ODBC provides the ability to access data from most supported relational database management systems. A 'middle layer' was introduced via a set of drivers. This layer provided a mechanism to translate commands and queries into the native language of the target system.

virtualization. This new feature provides the ability for a Domino database to act as a front end to relational data. This allows a developer to create a single Notes database with no data in the actual NSF. Each form, view, and agent processes data directly from the external data source.

LEI is a separately acquired Lotus product for the Domino server. It provides the ability to perform high-volume data transfers, synchronize disparate data sources, and perform real-time integration with back-end data sources.

The following diagram shows a simple use of LEI. The LEI server is configured to access data from a SQL data source, and to provide it to a Domino-based application. The LEI server uses a control store to determine what activity and scripts are executed. Once the activity completes, information is stored in a log file.

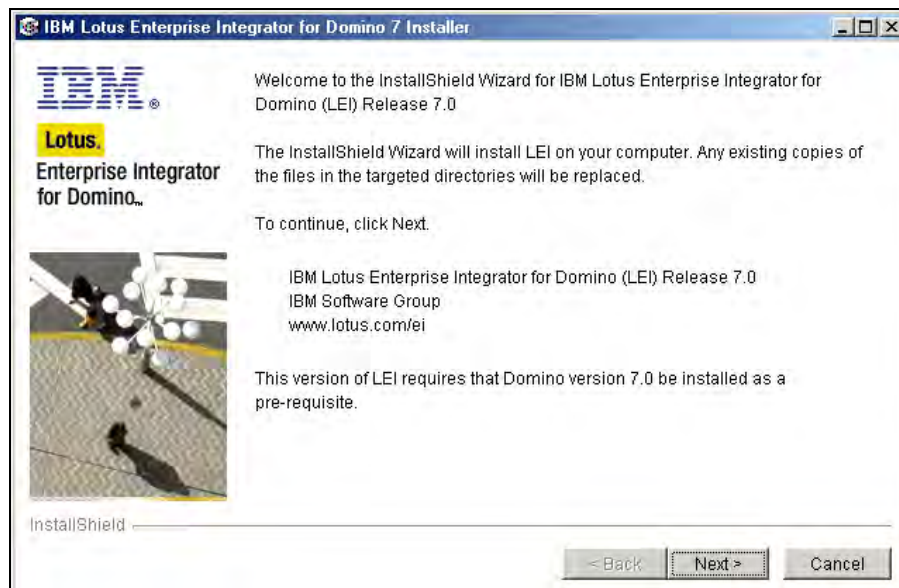


Domino 7 now provides us with a new release of LEI—Lotus Enterprise Integration 7. LEI release 7 contains the following new features and enhancements:

- Improved LEI user interface.
- Sametime awareness.
- LEI and DECS can be configured for Domino memory management, by including the `EI UseOSMemory=1` setting in the `NOTES.INI` file.
- All selection options (document, field, and view) in the Notes connection document have been grouped under a single tab called Selection Options.
- You can browse ODBC data sources that are available on the server.
- Safeguards have been added to avoid errors when creating connection and activity documents.
- Connection documents offer the new feature: Test Connection. This lets you test the connection before putting it into use.
- Failover mode lets data-management activities run on one of a designated set of servers.

The LEI installation process is relatively simple. Obtain your license from IBM, and run the install program. Open the LEI readme file, and review the system requirements. Also, verify that all of your database software is current with all available maintenance releases and fix packs.

The screen that follows shows the starting point:



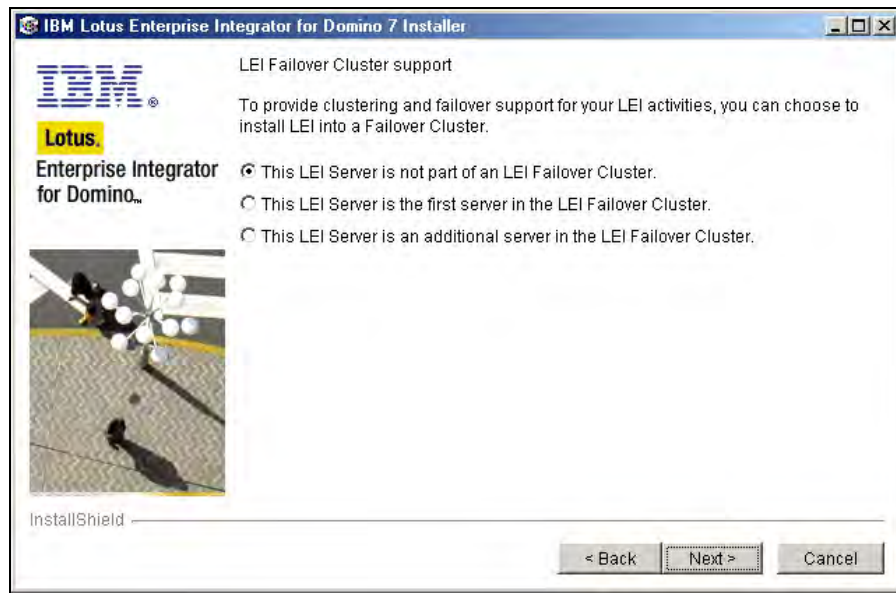
Next is the famous IBM License Acceptance Panel (no pirates allowed). Click Accept.

As noted earlier, Domino 7 must be installed first. The next screen asks you for the location of the NOTES.INI file for that server:



The next screen is another information screen. Review this so you can understand the security requirements for the server. i d.

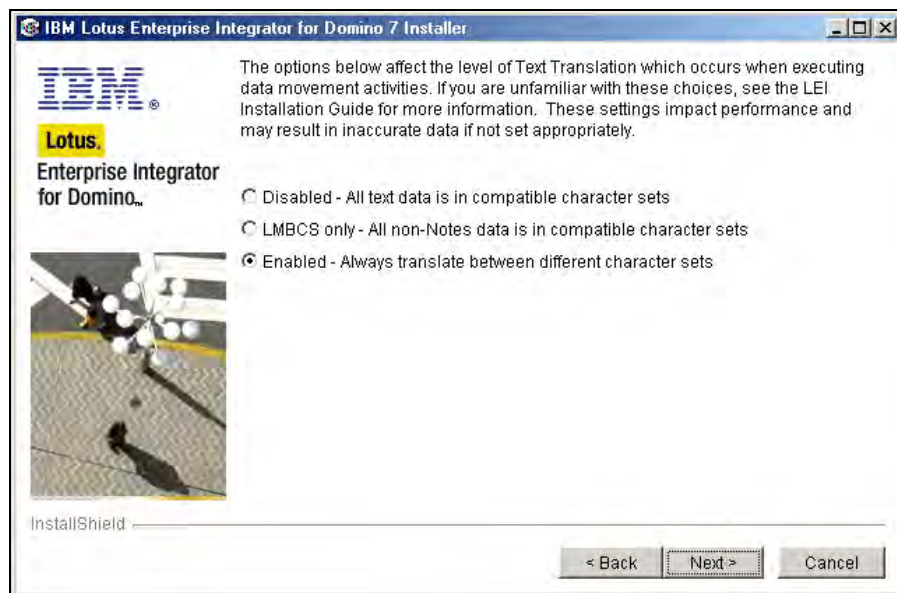
The screen that follows provides you the ability to select what type of server is being installed. This example shows This LEI Server is not part of an LEI Fail over Cluster. As a result, you will only see installation screens that apply to this option.



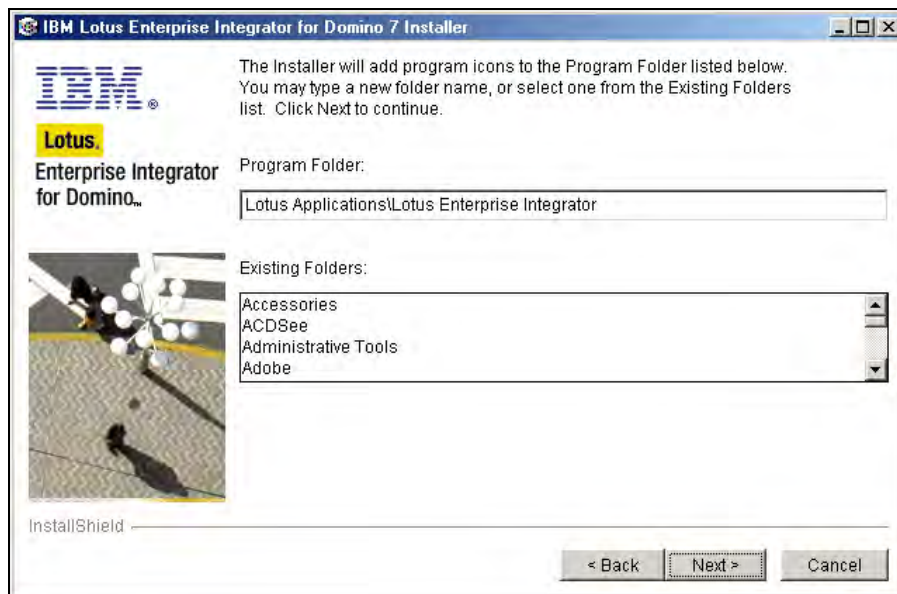
The next screen provides an opportunity to add additional managers to the LEI server. (Note the warning about default access to databases listed in this dialog box.)

The screen after this provides you with the ability to configure real-time access activities. This is followed by a screen of settings to enable the server to run as an add-in task. This can provide the ability to automatically start up when the operating system boots.

The next screen provides control over the level of text translation that occurs during data movement activities. Make sure you understand how these features work; as noted in the screenshot, these features can impact on overall performance.



Next up is a screen with icon selection dialog boxes:



The next question is for sample database installation. We find these to be very useful.

The screen that follows this is informational—a good screen to capture so that you know where everything was placed as part of this installation.

After you press **Next**, the actual placement of code starts. When this is complete, you are done—LEI is installed and ready to use.

Let us now move to some additional standards and tools.

Automatic Data Collection and Fault Analyzer

One feature introduced in Notes/Domino 6.0.1 was the Automatic Diagnostic Data Collection tool, also known as automatic data collection, or ADC for short. ADC provides a mechanism that, when a Notes client or Domino server crashes, will gather data to debug the crash, and send it to a mail-in database when a client or a server restarts. This provides Domino administrators with a single location (per domain) in which they can review all the crashes that have occurred for all clients and servers.

ADC has the ability to 'know' which diagnostic files were created corresponding to a server crash. ADC will also identify where each file is located after the collection process has been executed. This is known as the **diagnostic directory**. The types and names of each diagnostic type log entry are stored in a file called `di agi ndex. nbf`. This file is unique to each crash, and is renamed and saved as a new file after each ADC execution.

Once a server restarts after a crash, the platform-specific version of the **senddiag** program runs (on Windows platforms, this program is `nsenddi ag. exe`). This program is responsible for processing the `di agi ndex. nbf` file that relates to each server crash. The program searches through the index, and extracts each diagnostic file that was generated. Additionally, this program parses out (from the NSD) the Notes name, Notes/Domino version, operating system version, start time, crash time, and error message. Once all of this has been completed, the program will create a mail message containing this information, and send it to the mail-in database that has been configured to receive this information.

A lot of data is potentially created with each crash. Domino administrators have the ability to configure how long to keep these diagnostic files (via a policy setting for clients and the Server Configuration document for servers). Also, each time a Domino server boots, a file called `fi l e r e t` executes. This file scans the diagnostic directory for files that exceed the configured number of days for which diagnostic files are to be kept (the default is 365 days), and then removes them. Here is a list of files that can be found in the diagnostic directory:

- NSD output
- memcheck output
- Core files
- Memory dump
- `notes_chi l d_pi d` (UNIX servers only)
- `semdebug. txt`

Below is an example of documents found in the IBM_TECHNICAL_SUPPORT directory:

- 37,073 configall_Domino7B2_2005_01_04@19_05_49.dxl
- 36,372 configspecific_Domino7B2_2005_01_29@22_25_30.dxl
- 1,024 console.log
- 1,024 console_Domino7B2_2005_07_23@20_35_18.log
- 233 diagnosis_BASEVMWAREONE_2005_04_11@16_48_50.nbf
- 1,657 kill_W32I_Domino7B2_2005_07_23@20_42_14.log
- 11,118 nsd_W32I_BASEVMWARE_2005_01_29@23_16_06.log
- 39,159 serverdoc_Domino7B2_2005_07_24@14_08_27.dxl
- 219,251 sysinfo_Domino7B2_2005_07_24@17_59_53.log

In Domino 6.5 and 6.0.3, a new feature known as the **Configuration Collector** was introduced to provide snapshots of how a Domino server is configured, and to allow an analysis of any recent changes that may have impacted on the performance of the server.

During the normal operation of the Domino server, Configuration documents and Server documents are read during initialization. The respective views (\$Servers, \$ServerConfig, and \$ServerAccess) are polled every five minutes for changes, and if the view has been modified, the associated documents are reread. Up to four documents within the Domino directory can be used to set the basic operational parameters for a Domino server. These consist of the Server document, and three types of Configuration documents:

- Server Config All: configall
- Server Config Group: configgroup
- Server Config Specific: configspecific

When a document is read, a filename is constructed based on the document's modification time and date, and the server name.

With Domino 7.0, autonomic diagnostic collection will now evaluate call stacks generated from a Notes client or Domino server crash, using the automatic diagnostic collection functionality.

Autonomic diagnostic collection, introduced in Lotus Notes/Domino 6.0.1, extends the capability of automatic data collection by analyzing call stacks located in the fault report mail-in database, and then evaluating this data to determine whether other instances of the same problem have occurred. The ADC tool will also check the server to determine whether it is run under the Domino Controller. In such a case, the automatic diagnostic collection will use the Controller logs. Also, Domino administrators can define wild cards to determine which files are being collected.

One new setting with Domino 7 is the ability to set the server shutdown timeout. With a default of 300 seconds, this setting will force a server to shut down after a quit or exit has been issued. You can disable this feature with the new `NOTES.INI` setting `SHUTDOWN_MONITOR_DISABLED=1`.

Also with Domino 7, the ADC tool collects diagnostic data after server and client crashes, and sends the collected data to a mail-in database when the server reboots. Administrators can then analyze the collected data to determine the root cause of the crash. A single mail-in database can be configured per domain, and the data stored in fault report defined documents.

Domino 7 also provides a process to analyze server issues. The **Fault Analyzer process (FAP)** is a new server add-in task that processes all new crashes as they are delivered to the ADC mail-in database. The FAP searches the mail-in database that contains the fault report documents, and then determines whether the stack data matches a crash that has already been identified. The ADC database lists all fault reports, along with response documents for any duplicate occurrences of the same crash. The ADC will also identify whether the duplicate occurrence is a partial match or an exact match of the original crash. Each duplicate occurrence response document is defined as an "Exact Match Fault Report" or a "Partial Match Fault Report" document.

The steps to enable automatic data collection and the fault analyzer are easy. Domino administrators will edit a Domino Directory configuration document. The configuration document includes a series of fields that enable/disable each diagnostic feature. Domino reads the Server Configuration Settings documents and desktop policy documents in the Domino Directory at server startup. Domino determines whether the database resides on the local server, and if so, adds it to its list of databases to monitor. Every ten seconds, the Fault Analyzer process determines whether the data modified time of any of the monitored databases has changed. See the tip on `NOTES.INI` below on how to manage this setting.

NOTES.INI setting: `Debug_Fault_Analyzer = value`

Usage: Once the Fault Analyzer task has been enabled, configuration documents will be read and processed at server startup. Fault process reports, via the monitored databases, are reviewed every ten seconds to determine whether any action is required. This `NOTES.INI` setting will modify the monitoring of the process activities.

Use `Debug_Fault_Analyzer` to provide debug information for the Fault Analyzer as follows:

- 1—List errors
 - 2—List errors and also show the progression of the code
-

The following list shows each setting for automatic server recovery. Most of these features are new; features introduced in Notes/Domino 6.x are noted by the identification (*ND6*):

- Mail-in database for diagnostic reports (*ND6*): This field identifies the name of the mail-in database, via a drop-down list from the Domino directory, to which the reports for server crashes will be mailed.
- Maximum size of diagnostic records including attachments (in MB): Server initialization will create several diagnostic documents. The number of files collected can be limited too; the default limit is a maximum of ten documents and files of each type.
- Maximum size of NSD output to attach (in MB): This field will specify the maximum size of the diagnostic output.
- Maximum amount of console output file to attach (in KB) (*ND6*): This field shows the amount of CONSOLE. LOG that will be sent. The default value is 10240.
- Diagnostic file patterns: This field can be used to specify a file name pattern that Domino will search for. di agi ndex. nbf is used as a source for the pattern search. If the pattern is located, and it is listed in this file, then the diagnostic message is sent to the specified mail-in database. Note that the di agi ndex. nbf file contains a list of files associated with the particular crash instance of the server.
- Remove diagnostic files after a specified number of days (*ND6*): This setting has two options. Select No to accept the default of never automatically deleting the diagnostic files created on the server. Select Yes to enter the number of days after which the diagnostic files on the server are to be deleted. If Yes is selected, then the field Number of days to keep diagnostic files is displayed. The default is 365.

Fault Analyzer Settings

The following list show each setting available for the Fault Analyzer process:

- Run Fault Analyzer on Fault DBs on this server: Two choices are available. Yes enables the Fault Analyzer task on this server. No disables the Fault Analyzer task.
- Run Fault Analyzer on: Two choices are available. All mail-in databases on this server instructs the Fault Analyzer process to run on all mail-in databases on this server. Specific mail-in databases displays the field Databases to run Fault Analyzer against. In this case, the fault reports will be posted to the specified databases.

- **Databases to run Fault Analyzer against:** Select the databases against which you want Fault Analyzer to run. The Fault Analyzer task will search the listed databases for fault report documents. The Fault Analyzer task will also determine whether the stack matches a crash that has already been seen by a user or server at that customer site.
- **Remove attachments from duplicate faults:** This setting instructs the Fault Analyzer to look for and analyze duplicate fault reports. Each new crash is reported as a response to the original crash, and attachments are either removed from the response document to save space in the database, or are saved with the response document. Two options are available. **Yes** specifies that attachments are removed from the response document to save space in the database. **No** saves attachments with the response document.

Configuration Settings : Domino7B2/ND7B2

Basics | Smart Upgrade | Router/SMTP | MIME | NOTES.INI Settings | Domino Web Access | IMAP | SNMP | Activity Logging | **Diagnostics** | Administration

Diagnostic Collection Options

Mail-in Database for diagnostic reports:

Maximum size of diagnostic message including attachments (in MB):

Maximum size of NSD output to attach (in MB):

Maximum amount of console output file to attach (in KB):

Diagnostic file patterns:

Remove diagnostic files after a specified number of days:

Fault Analyzer

Run FaultAnalyzer on Fault DBs on this server:

Run Fault Analyzer on:

Remove attachments from duplicate faults:

IPv6

Lotus Notes is a client/server based technology that can communicate using a variety of network protocols. Today, one of the most common protocols used is TCP/IP. This particular network-communication process is actually two protocols: TCP (Control Protocol) and IP (Internet Protocol). Each section of this dual protocol controls various parts of a network-communication process. TCP is responsible for verifying the delivery of data from a client to a server—in our case, a Lotus Notes client accessing a Domino server (or server to server communication). IP is responsible for moving network packet data from one computer to another. One very important aspect, in relation to Domino 7, is that the IP address is based on a four-byte address (for a total of 32 bits).

TCP and IP were developed by a Department of Defense (DOD) research project to connect various networks, designed by different vendors, into a series of networks. This 'network of networks' eventually evolved into today's Internet.

The newest iteration of IP is known as IPv6 (version 6), short for Internet Protocol version 6. The previous version of the Internet Protocol was version 4 (referred to as IPv4). IPv6 is designed to be the next evolutionary step from IPv4. A total of up to 32 addressable bits are available with IPv4. In the case of IPv6, there are a potential of 128 addressable bits. The following table shows the basic IPv6 header:

0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version				Traffic Class								Flow Label																			
Payload Length																Next Header								Hop Limit							
(IPv6) Source address 0,1,2,3																															
(IPv6) Destination address 0,1,2,3																															

Version is four bits in length, and contains the IPv6 version number.

- Traffic Class is eight bits, and contains the Internet traffic priority delivery value.
- Flow Label is 20 bits, and is used for specifying special router handling from source to destination.
- Payload Length is 16 bits (unsigned), and specifies the length of the data in the packet.
- Next Header is eight bits, and specifies the next encapsulated packet.
- Hop Limit is eight bits. For each router that forwards the packet, the hop limit is decremented by one. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header.
- Source address is 16 bytes (128 bits). The table shows a QTY of four 32-bit addresses. The table shows addresses 0,1,2,3 for a total of four sets of 32 bit addresses. This contains the IPv6 address of the sending node.
- Destination address is 16 bytes (128 bits). This is the IPv6 address of the destination node.

IPv6 addresses strings can be used any place an IPv4 address is used. There are a few limitations. For instance, a sample IPv4 address looks like this: 192. 9. 200. 33. A sample IPv6 address, on the other hand, looks like: fa80: 292: 27bb: fa66: ac16.

One common use with IPv4 addresses is to add a service port to the end of the IP address; for example, 10. 11. 12. 13: 1352.

As you can see, IPv6 uses colons as numeric separators. The service port cannot be directly used with IPv6. If you need to include the service port address with IPv6, then the base address will need to be enclosed in square brackets; for example, [fa80: : 292: 27bb: fa66: ac16]: 1352.

Domino 7 provides the ability to support both IPv4 and IPv6. By design, it is backward-compatible with IPv4, so if an IPv6-enabled packet receives an address in the IPv4 format, Domino will still be able to service that request. The Domino support for IPv6 protocol includes support for the following services: SMTP, POP3, IMAP, LDAP, NRCP, and HTTP.

To enable IPv6 on Notes and Domino 7, just add the setting TCP_ENABLE_IPV6=1 to the NOTES. INI file on both the Notes client and the Domino server. Domino will evaluate each IP address, and will determine how to service each request. The following table shows the various responses for each type of request:

IP address style format	Domino server response
IPv4	Resolves to an IPv4-style connection.
IPv4 address mapped to IPv6	Domino will attempt to make an IPv6 connection, and then will wait for the TCP/IP software to make either an IPv6 or IPv4 connection.
IPv6	Resolves directly to the IPv6 style.
Domino server name	Uses DNS to resolve the name. If only an A record is found, connects over IPv4. If only an AAAA record is found, connects over IPv6, or waits for the TCP/IP software to make the connection. If an A record and AAAA record are both found, uses the AAAA record.

One big assumption with IPv6 is that the operating systems will need to support it. So, before you get too far into enabling IPv6, you need to check and enable IPv6 for each operating system. The first step is to contact your software vendor and determine whether IPv6 is available on your particular operating system (both server and client). Also, check the Domino release notes. After you have enabled/installed IPv6 on your operating system, you can verify whether it has been installed, using the following commands:

- `ipconfig/all` (Windows platforms)
- `ifconfig -a` (most other platforms)

DNS and Resource Records

Domain Naming System (DNS) is a distributed database that maps usernames and host names to IP addresses, and vice versa. The DNS system can also store information about your company's organizational structure, which will include how many computers with IP addresses are in each DNS-based domain.

Domain names are described in terms of a fully qualified domain name. A fully qualified domain name includes all higher-level domains relevant to the entity named. So, for a Domino server (any TCP/IP-based supported Notes/Domino release), the fully qualified domain name would include the string that identifies the particular device, plus all of the domains of which the host is a part, up to and including the top-level domain.

For example, serverA.dallas.thecompany.xyz is a fully qualified domain name for the host at 10.11.12.13. In addition, dallas.thecompany.xyz is the fully qualified domain name for the Dallas Data Center for the company, and thecompany.xyz is the base address for TheCompany, Inc. Basically, the domain name identifies some type of node—in our case a server or a client. Each of these nodes will have defined resource information that is associated with a particular name and is then associated with an IP address.

DNS will track several sets of attributes in various records. These include:

- **Owner:** This is information about the DNS domain.
- **Type:** This value specifies the type of the resource record. Examples include the host address, the CNAME (identifies the canonical name of a defined alias), MX (identifies a mail exchange for the domain; this is used for SMTP mail routing), and AAAA (new for IPv6; this is the IPv6 equivalent for the IPv4 A record).

A few comments about these examples

As you've probably noticed, .xyz is not an Internet-defined suffix. We used it here because we did not want to use potentially real addresses when showing test URLs and addresses, although someday this suffix could be valid. (The suffix .xyz can resolve on a private network if you want to use it, but there's no real value in doing that.)

The original Internet-defined suffixes were .com, .org, .net, .edu, and .gov. Today many more are available; as far as we know, .xyz is not one of them.

TheCompany is not a real company (we hope).

You will also notice that we are also using IPv4 addresses that start with 10. The reason is that originally, the architects of the Internet, the **Internet Assigned Numbers Authority (IANA)**, reserved three blocks of the IP address space for private networks: 10. 0. 0. 0 through 10. 255. 255. 255, 172. 16. 0. 0 through 172. 31. 255. 255, and 192. 168. 0. 0 through 192. 168. 255. 255. So we reference the use of these as 'test', or non-resolvable, addresses.

Zones

The IPv6 standard specifies that link-local address and site-local address can be used; in this case an additional parameter can be enabled to specify the interface on which the address is valid. This additional parameter is called the `scope_id`. This parameter is defined as the **zone**. Domino 7 uses the format address string, followed by the percent sign (%), followed by the zone.

The zone is an integer index into the interface list in Microsoft Windows. The first interface is defined as zone one.

Note the following information regarding zones:

- Zones are mandatory on Linux for link-local addresses.
- AIX and Solaris do not require zones.
- Zones are mandatory on Windows for link-local addresses.
- You should not attempt to put a zone into DNS, in a hosts file, or in a global data store such as the Domino directory—the zone is not a characteristic of a particular *target* system, but is a characteristic of the *source* system.

Also, if any of your computers are on a single network interface, then you can use the `NOTES.INI` variable `TCP_DEFAULTZONE` to provide a default zone for all link-local addresses.

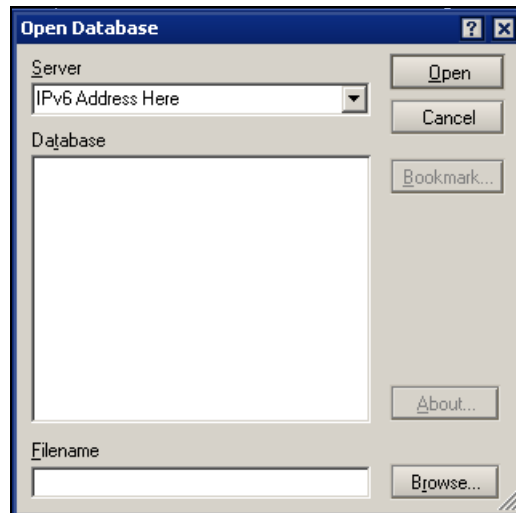
Enabling IPv6 on Domino 7 Servers and Notes 7 Clients

This process starts with installation Domino 7 servers and/or the Notes 7 clients.

1. To enable IPv6 on both the client and the server, set the `NOTES.INI` variable as `TCP_ENABLEIP6=1`. This variable is added to both the server(s) and the clients.
2. Next, you need to configure a zone on both the Notes client and the Domino server.

The first challenge to use IPv6 is to enable IPv4 and IPv6 to work at the same time. This can be an issue with Windows/Intel configurations. In the case of Microsoft Windows, the operating system is not capable of receiving incoming IPv4 and IPv6 connections both on the same socket. UNIX provides more flexibility because UNIX platforms have the ability to receive both IPv4 and IPv6 incoming connections on the same socket. To receive IPv4 and IPv6 connections on Windows, you will need to define two ports, one bound to an IPV4 address, and another bound to an IPv6 address.

3. Next, configure a port for IPv4 and a port for IPv6 on the Domino server.
4. Launch one of your Notes clients. Using the Notes client, connect to a server using an IPv6 address using **Notes remote procedure call (NRPC)**. When the address is entered and the server is 'opened', a low-priority Connection document will be added to the local Name and Address book (names.nsf). Note that a DNS-enabled server name will also resolve a connection.



Summary

This chapter discussed the performance monitoring and optimization tools available to you in Notes/Domino 7. We also outlined our recommendations for how you can plan for performance, starting with an assessment of available performance tools (including Server.Load), and how you can plan your environment in a way that anticipates future performance requirements and ensures that you meet them.

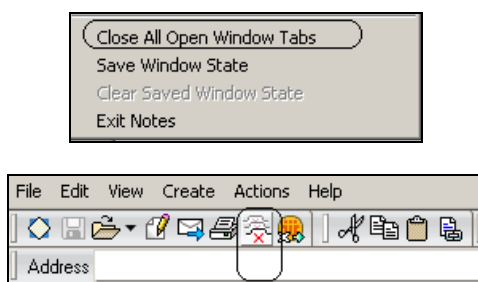
8

Client Features

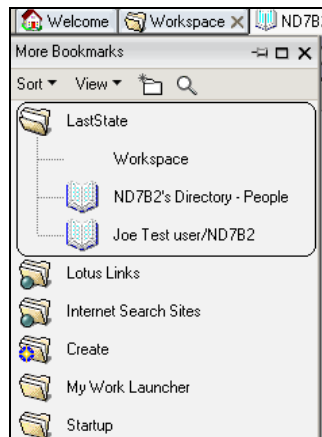
In this chapter, we discuss new features introduced in the Notes 7 and Domino Web Access 7 clients.

Notes 7

In Notes 7, there are several new features to help you with window management. For example, every time you open a document or database, a new window tab appears beneath the toolbar (or beneath the main menu bar if the toolbar is hidden). In the following illustration, there are four window tabs: one for the Welcome page, and one each for Pat Wilkins' Inbox, to do list, and database application. The following option(s) will close *all* of open tabs at once.

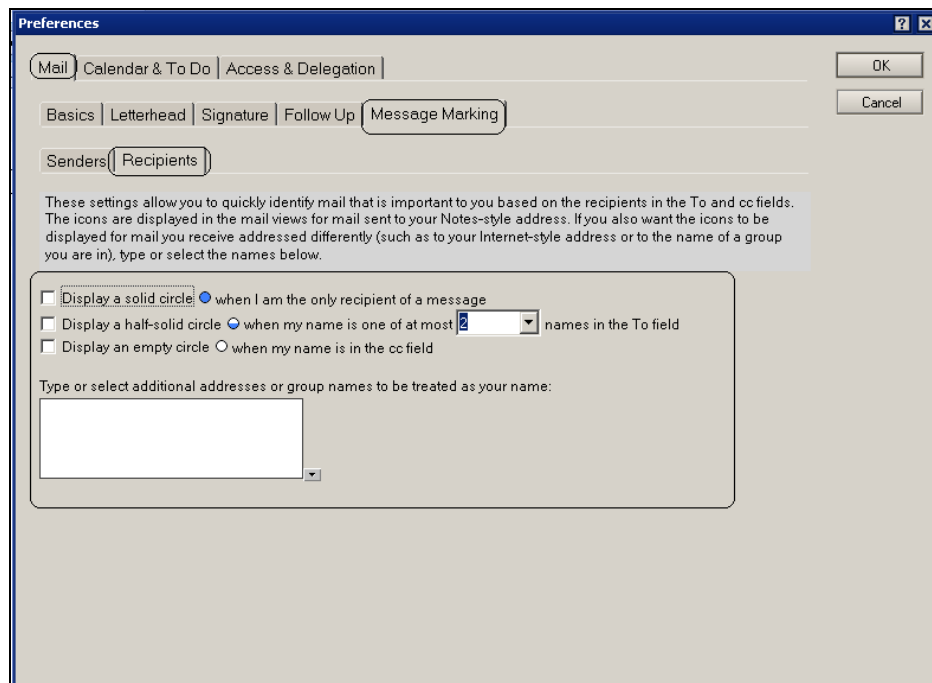


Another new feature is saving window states. This lets you save the state of your Notes environment. Saving the state allows you to see the same open window tabs the next time you start Notes. To save the same window tabs every time you use Notes, use the menu command File | Save Window State to permanently save a window state. Notes saves the open windows as bookmarks in the LastState folder within More Bookmarks. Once the last state has been saved, you can select any of these saved states. The screenshot overleaf shows how these can be selected:

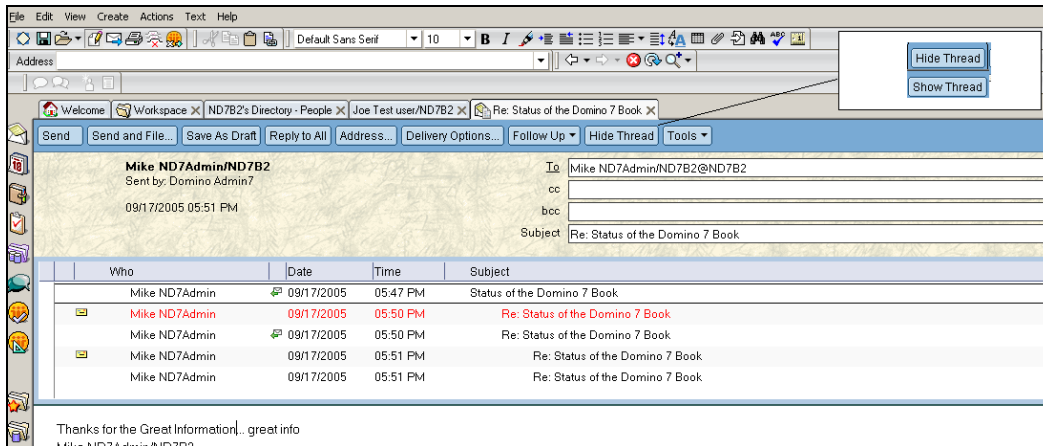


New Mail Features

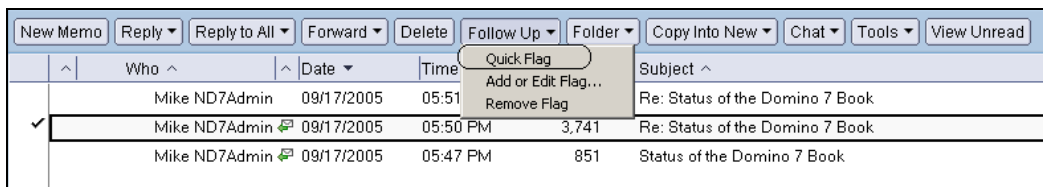
New Notes 7 features in the mail file and the directory include **message marking**. This will help identify whether your name is in To or cc fields. This feature can visually display whether you are likely to need to respond to the message personally, or whether it is a larger distribution. The following screenshot shows how you can enable this feature in Mail preferences:



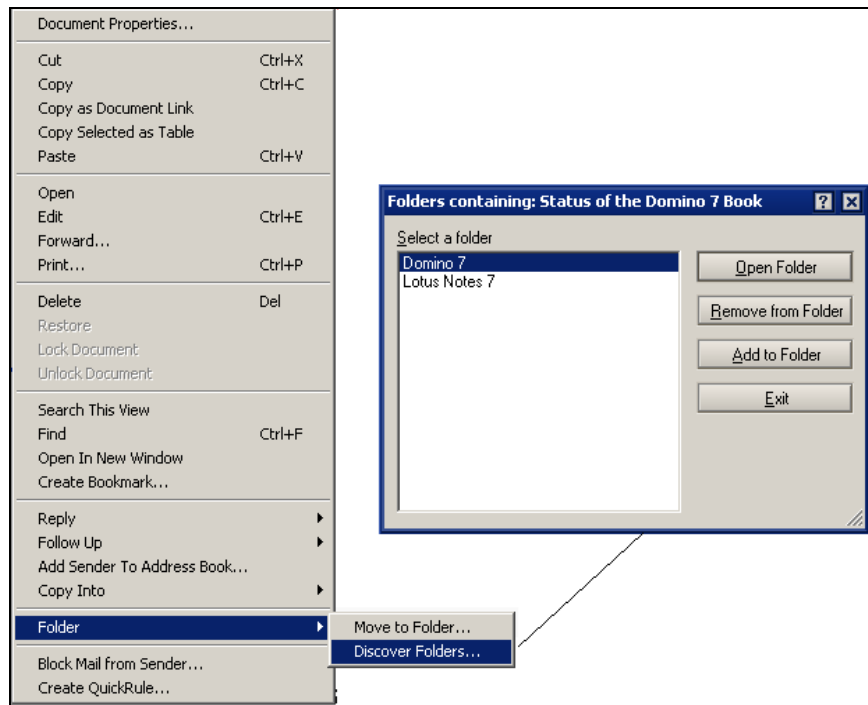
You can sort messages in most mail folders and views by clicking the headings of the columns that contain an up or down arrow. To return to the original sorting method, click the relevant heading again. Mail threads can now be displayed as part of the Memo header. This feature helps you to locate where the current message belongs within a message thread, and also allows navigation to other messages in the thread directly. The following screenshot shows an example of this feature:



Quick Flag follow up lets you flag a document (or a set of documents) for follow up. You can flag a mail message with an icon to indicate whether the message requires urgent, normal, or low-priority action. Flagging a message also places it in the Follow Up view.



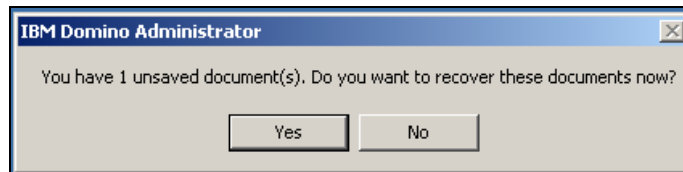
Discover Folders is a new folder option. When a document is selected in the view, and the Folder | Discover Folders action is selected, a dialog box will be displayed, showing which folders the selected document is in:



Autosave

Autosave provides the ability to automatically save work in process into a local Notes database. This can be executed automatically or on a predetermined schedule. Then, if Notes crashes, you can recover the work that was done before the crash. Users can override the default location for autosave. nsf by setting the NOTES. INI variable `auto_save_db` to the file location of their choice.

Documents are removed from the autosave database after they have been saved, sent, or discarded. In the event of a client crash or a power outage, the documents can be recovered easily. You will be prompted to recover documents from the autosave database upon restart of the Notes client, as follows:



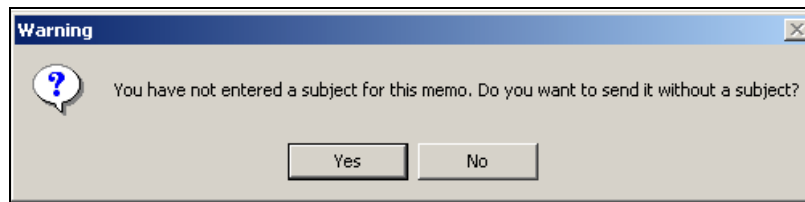
You can select File | Autosave | Recover AutoSaved Documents for this purpose as well. You can also view the contents of the autosave database:

Autosave	Server ^	Database ^	Document ^	Save Time ^
Autosave	Domino7B2/ND7B2	CN=Domino7B2/O=NL	This is an autosave example - Number 2	09/17/2005 09:27:21 PM

Other Mail Features

Lotus Notes 7 and XP provide a mechanism to recognize certain types of text in Microsoft Office XP documents, and then provide related functions and commands. For this, Microsoft Word must be configured to use Smart Tags.

If you attempt to send a message without a subject line, you will receive the following dialog box asking if you really want to send this message:

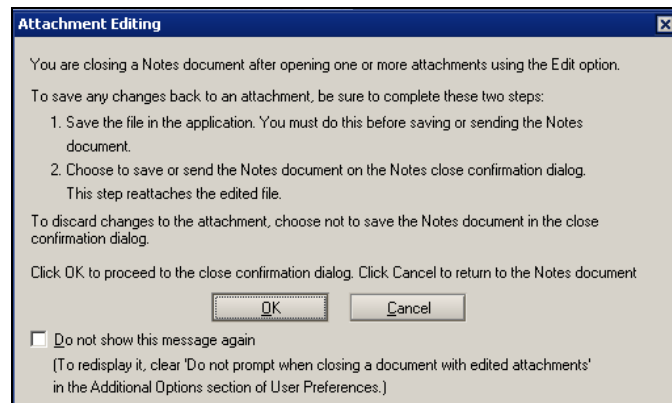


An icon will display the encryption status of an opened document. These statuses include:



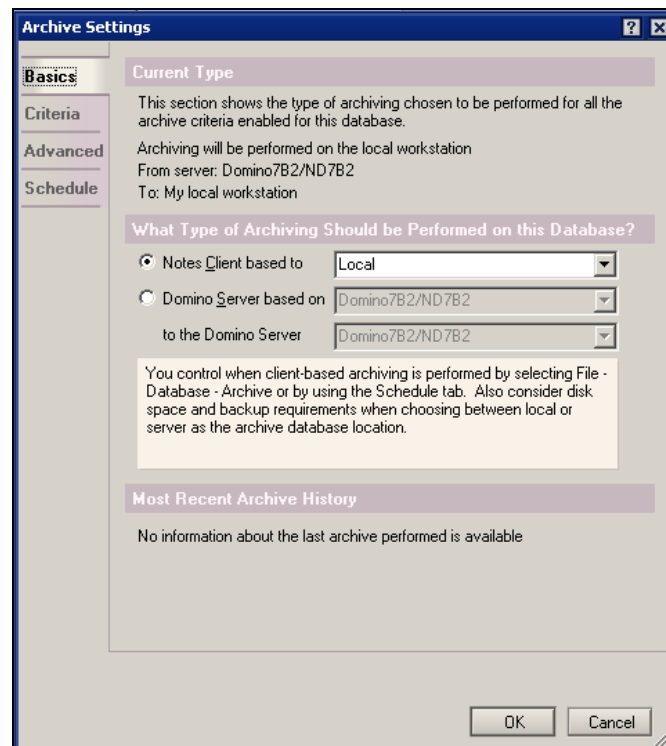
Notes 7 provides a new feature for managing attachments. When you open an attached file, you can open it with the software program it was created in, or with an alternative program.

End users will receive warnings if an attachment is not saved in the event the hosting document is closed, but not saved. The following screenshot shows an example:



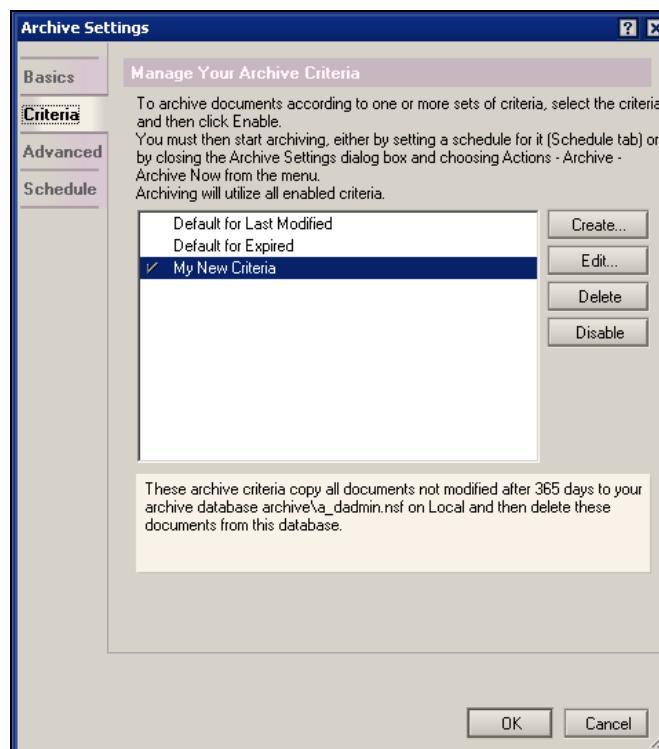
Archiving

A mail archive is a database copy that can be created to store information that is not needed on a daily basis, but that you would like to keep. An archive contains documents and design elements from the original database. Notes 7 offers improved archiving capabilities. The screenshot that follows shows how you can set up archiving. This dialog is accessed by Actions | Archiving | Settings.



There are four tabs that will need to be configured:

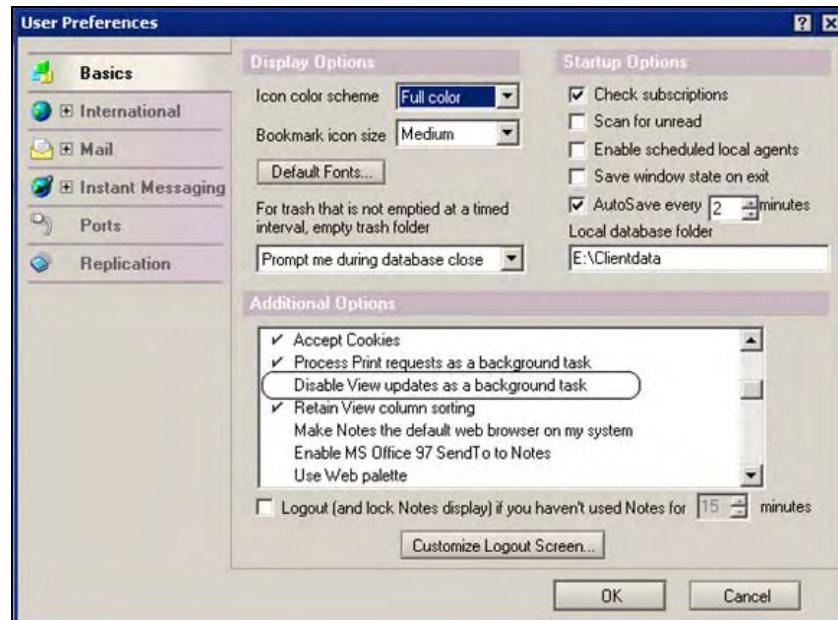
- **Basics:** This tab defines the computer where archiving runs, and the one where the archive is stored. You can set the archive process to be performed either by your mail server or by the Notes client. If the Notes client performs archiving, you can store the archive database locally, or on any server to which you have access. If a mail server performs archiving, you can store the archive database only on a server to which you have access.
- **Criteria:** This tab provides the ability to create and enable a set of archive-based criteria that will instruct the archiving program on what to archive. The following screenshot shows how you can create custom criteria:



- **Advanced:** This tab provides a way to change the manner in which archiving handles documents that have responses, and create an archive log.
- **Schedule:** This tab shows scheduling options for client-based archiving.

Background View Indexing

This feature provides view updates as a background task. You no longer need to wait while a view that needs updating is being opened. During this time, you can work in other views and documents while the view update is being processed. The view will display the following messaging while it is indexing in the background: This view is being updated. It will display as soon as the update completes. You can continue working with other Notes windows while the view is updating. This feature can be disabled via User Preferences, shown in the following screenshot:



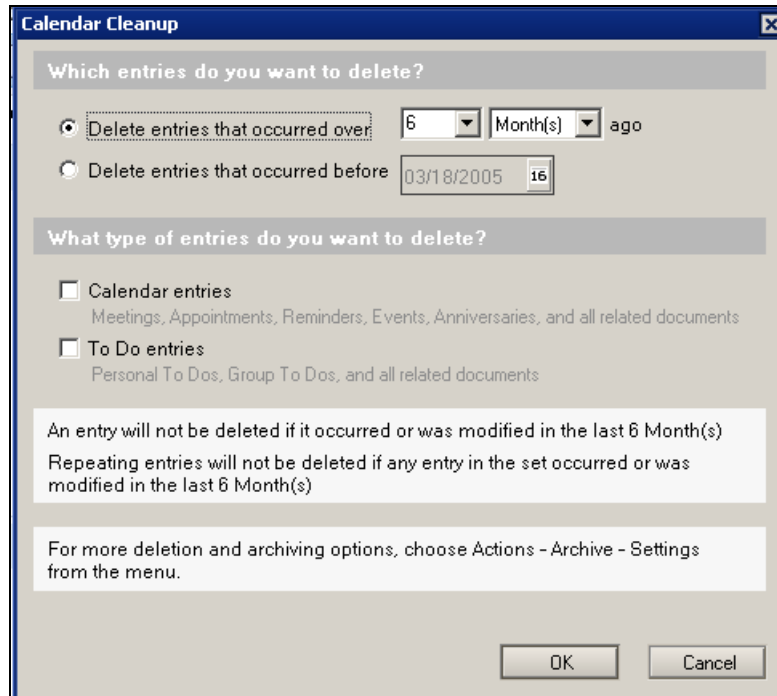
Mail Rule Processing

A new processing rule that provides a processing 'stop' is available with Notes 7. This stop-processing rule action will stop the processing of all rules following the rule that contains the 'stop processing' action. The 'stop processing' action can be used alone, or can be used with another action in a rule. The 'stop processing' rule is especially useful when more than one rule could apply to a message, but you want execution of mail rules to stop after the first action is executed.

You can also use mail rules to help filter spam. The Domino server can be configured to use blacklists to specify hosts or domains responsible for sending unwanted email to end users. When blacklist filters are enabled, any email from a host on the blacklist is tagged. You will not be able to see or identify these tags directly, but you can create mail rules to act on messages that have one of these blacklist tags.

Calendar and Scheduling

Notes 7 and Domino 7 have improved the calendaring and scheduling (C&S) functions. There are many new features (this section will cover only a few of the more important ones). For example, there's a new feature called Calendar Cleanup, which you can enable by opening the calendar and then choosing Tools | Calendar Cleanup. Calendar Cleanup lets you delete calendar entries older than a specified time interval or calendar date.



Notes 7 provides the ability to manage another user's calendar, without the user having to give you full access to his or her mail file. Calendar management is set up in the person's calendar that you are managing, as well as in your calendar. The calendar manager can schedule meetings for the calendar owner, and receive notification for all of the meeting notices the owner receives.

Add People/Groups

1 Enter the name of the person or group to whom you want to grant access to your mail file

☒ Enter or choose a user/group ☐ Access is for everyone

Linda Admin/Dallas/Domino7

2 Choose how much of your mail file to delegate to this person or group

☐ All Mail, Calendar, and To Do ☒ Only Calendar and To Do ☐ None

3 Choose how much access you want to give to this person or group

Read any Calendar Entry or To Do

4 Automatically forward to this person calendar notices sent to you

Enabling auto-forwarding makes it easier for someone to manage your calendar if they do not normally keep your calendar open and on display.

☒ Forward notices where you are the invitee of the meeting

☒ Forward notices where you are the chair of the meeting

If the message is marked as private: Do not forward

Note: this setting affects all auto-forwarded messages

OK Cancel

You can now set up a 'quick access' to other calendars. This feature is configured in the preference setting, and is used by a quick-access dropdown in the calendar.

C&S filters provide the ability to display various C&S entries based on a set of filters.

Filter options include:

- By Chair to see only meetings chaired by a certain person.
- By Type to select which calendar-entry type you want to see (meetings, appointments, all-day events, and so on).
- By Status to see only invitations you have accepted, for example.
- By Private to see entries that cannot be seen by others who have access to your calendar.

There are two methods to activate filters: via Actions | Filters, and via the drop-down dialog box.

New Right Mouse Button Selections

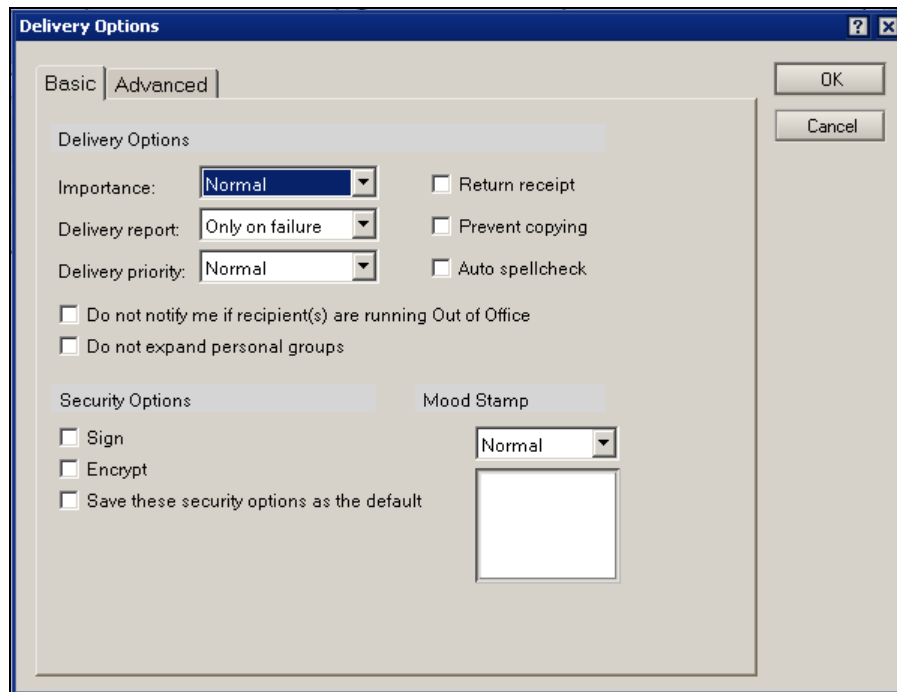
When you right-click the mouse while in the Calendar, you'll see a number of new options. Here is a comparison of right-click options in 6.5.4 with those in 7.0:

Right Mouse - 6.5.4	Right Mouse - 7.0
Document Properties...	Document Properties...
Cut Ctrl+X	Cut Ctrl+X
Copy Ctrl+C	Copy Ctrl+C
Copy as Document Link	Copy as Document Link
Copy Selected as Table	Copy Selected as Table
Paste Ctrl+V	Paste Ctrl+V
Open	Open
Edit Ctrl+E	Edit Ctrl+E
Forward...	Forward...
Print... Ctrl+P	Print... Ctrl+P
Delete Del	Delete Del
Restore	Restore
Lock Document	Lock Document
Unlock Document	Unlock Document
✓ Search This View	Search This View
Find Ctrl+F	Find Ctrl+F
Open In New Window	Open In New Window
Create Bookmark...	Create Bookmark...
	Reply ▶
	Follow Up ▶
	Add Sender To Address Book...
	Copy Into ▶
	Folder ▶
	Block Mail from Sender...
	Create QuickRule...

Another new C&S feature is the ability to automatically accept a calendar event, even if there is a schedule conflict.

Preventing Expansion of Personal Groups

You can control whether the recipient of a mail message sees the membership of a personal mailing group. This is controlled by a new delivery option, on a message-by-message basis. To enable this, create a message and choose Actions | Delivery Options. On the Basic tab, select Do not expand personal groups.



One advanced option for end users (actually, this would more likely be used for troubleshooting by the help desk or administrator) is to enable **status-bar logging**. If this feature is enabled in the NOTES.INI file, then status-bar messages can be written to the local log.nsf. Also, these messages can be written to an external file by using Debug_outfile = Filename. The syntax for this setting in the NOTES.INI file is as follows:

- LOGSTATUSBAR=1 enables status-bar logging
- LOGSTATUSBAR=0 disables status-bar logging

This works with all Notes 7 clients.

Rooms and Resources

Resources and rooms are managed in the Resource Reservations database, a feature introduced in an earlier release of Notes and Domino. Resources can include conference rooms and meeting room accessories, such as projectors, TVs, or even specialized phones. You can use this database to reserve rooms and equipment. A Resource Reservations database contains three types of documents: Site Profile, Resource, and Reservation.

- **Site Profile document:** This identifies a particular location where rooms and resources are located.
- **Resource document:** This identifies each conference room by name. Using the Site Profile and the Resource documents, you will know that you will be using the Eisenhower room in London, and not the Churchill room in Dallas.
- **Reservation document:** You can either use a reservation document in the database, or the document will be created automatically for you if an invitation requests the use of a resource or requests a reservation.

After the creation of the database and the Site Profile and Resource documents, the Schedule Manager tracks the free time of a resource in the same way that it tracks free time for users.

The Rooms & Resources (R&R) functionality in Domino 7 has been updated with the ability to prevent overbooking of rooms or resources. A new server task, **RnRMgr** (Rooms & Resources Manager), is responsible for both, processing all reservation requests and updating the information in the busytime system for rooms and resources. Room and resource reservations will not be processed unless the RnRMgr task is loaded on the server where the R&R database is hosted. You can edit the NOTES.INI to ensure that the RnRMgr task is added to the ServerTasks= line. A less effective method is to manually load the task using the `load RnRMgr` console command.

In Notes/Domino 6, the **SchedMgr** (Schedule Manager) task was responsible for updating the busytime data for rooms or resources. Also note that all console commands previously used by the SchedMgr task can be used with the new RnRMgr. The AdminP Administration Server setting for each resource database needs to be set before any administrative changes can be made to it.

Sametime Integration

Notes 7 provides many new features supporting Sametime instant messaging and associated services. With Notes 7 Sametime integration, you can see instant person awareness (who is online) not only in your Inbox, but also in your calendar, Personal Address Book, Teamrooms, to-do lists, discussion databases (based on Notes 7 templates), and the Notes 7 Room and Resource reservation.

Let's look at an example of Sametime online awareness. Just open your calendar and, if the person whose name appears is online, you will see the name with an awareness icon next to it:








Save and Send Invitations		Find Room or Resource ▾		Delivery Options...		Actions ▾		Chat ▾	
Calendar Entry									
Meeting									
Subject		meeting							
When		Starts		Mon 09/26/2005	16	09:00 AM	🕒	1 hour	
		Ends		Mon 09/26/2005	16	10:00 AM	🕒		
		<input type="checkbox"/> Specify a different time zone							
Invitees		Invited The following invitees have been invited							
		Required (to)		Tim Speed/Dallas/IBM@lotus					
		<input type="button" value="Remove Invitees"/> <input type="button" value="Add Invitees"/> ▸							
Scheduler		Click to see Invitee status							
Description		Click to append attachment(s)							

There is also a dropdown titled Chat, which offers four options:

Chat with Chair...
Chat with All...
Show/Hide Instant Contact List
Add Chair to Instant Contact List...

Meetings now allow you set up the online portion of the meeting to restrict attendees to only those on the invite list, and to provide a password for the online meeting. The screenshot that follows shows the various fields that can be set on the invitation:

- The This is an Online Meeting checkbox.
- The Type dropdown offers three choices: Collaboration (the default), Moderated presentation/demo, and Broadcast meeting.
- Place is a selection from the Domino directory (based on data from the Resources.nsf database).
- The Restrict only to meeting invitees checkbox.
- Meeting Password.
- Online Meeting Attachments.

Chair	Mike ND7Admin/ND7B2	
Where	Location	<input type="text"/>
	Rooms	<input type="text"/> 
	Resources	<input type="text"/> 
	Online	<input checked="" type="checkbox"/> This is an Online Meeting
	Type	Collaboration 
	Place	Online meeting Place One/Dallas 
	Restrict Attendance	<input checked="" type="checkbox"/> Restrict only to meeting invitees
	Meeting Password	meetingpasswordhere
Online Meeting Attachments	 graphic.gif 	
Categorize		

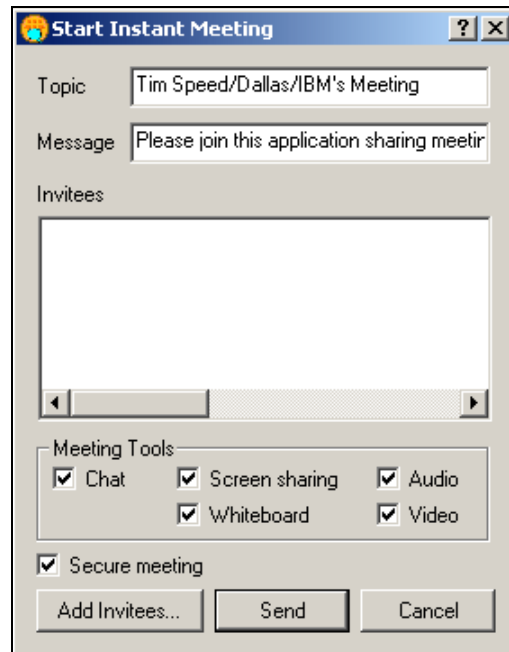
Notes 7 also offers Sametime instant chat/meeting features. New features include:

- Start Instant Audio Meeting
- Start Instant Video Meeting
- Start Instant Shared Meeting
- Start Instant Collaboration Meeting
- Edit Current Status Message

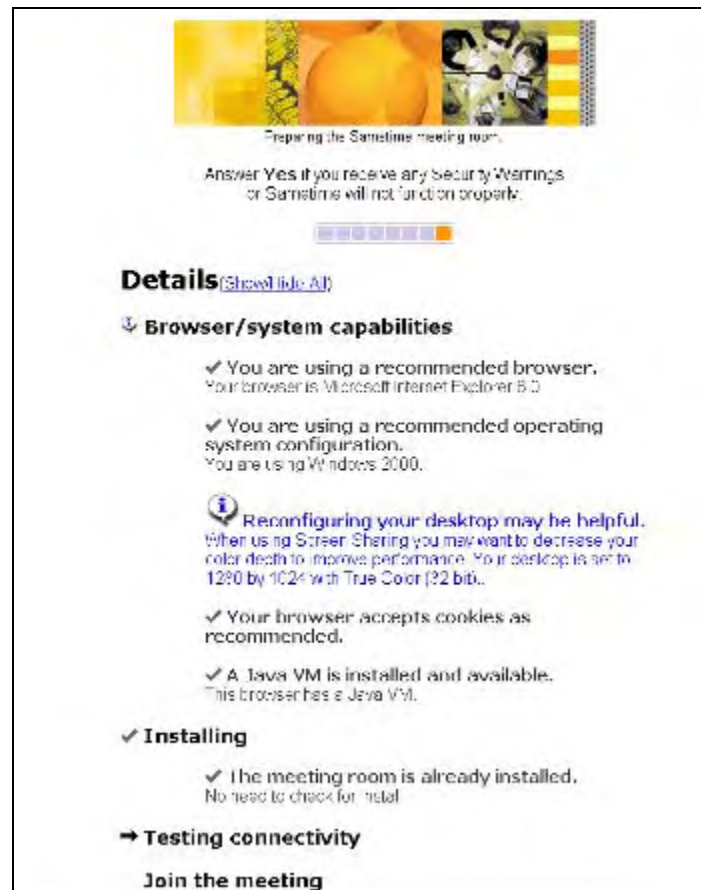
Here's a screenshot of the features:

Chat...	
Start Instant Chat Meeting...	
Start Instant Audio Meeting...	
Start Instant Video Meeting...	
Start Instant Shared Meeting...	
Start Instant Collaboration Meeting...	
Add to Instant Contact List...	
Show/Hide Instant Contact List	Ctrl+Shift+C
Preferences...	
✓ I Am Active	
I Am Away	
Do Not Disturb Me	
Edit Current Status Message...	
Log Off Instant Messaging	

The same basic dialog box is displayed for each selection. The difference is *how* the box is displayed with each selection. For example, if you select 'chat', then the following dialog box appears. If you select 'collaboration', then all checkboxes will be displayed.

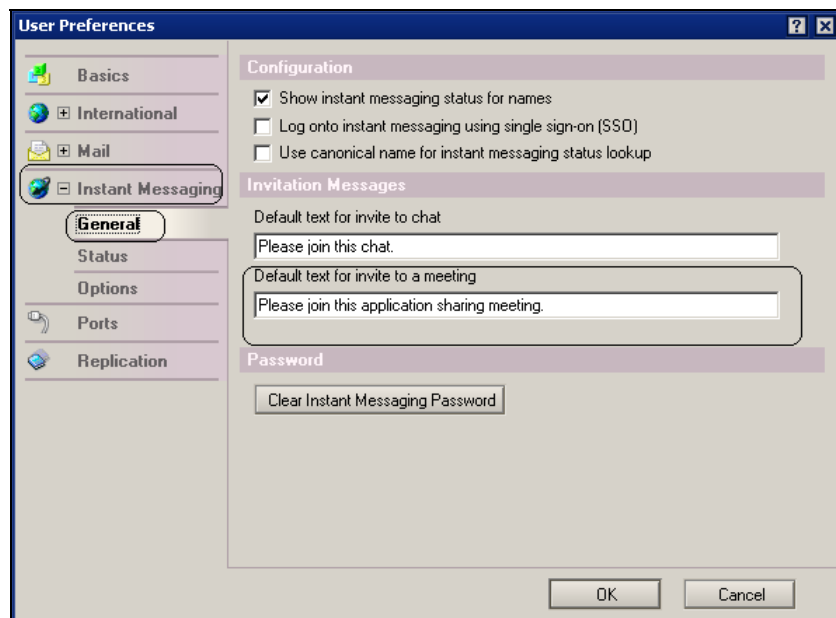


As soon as you add invitees, the following screen will display, showing the status of each meeting setup step:



The next new feature is the ability to set preferences that control the appearance in the Sametime contact list. This feature is found in the Notes 7 client, under File | Preferences | User Preferences. This displays the standard User Preferences dialog box. In this box, you will see the Instant Messaging selection tab. This tab offers three choices: General, Status, and Options.

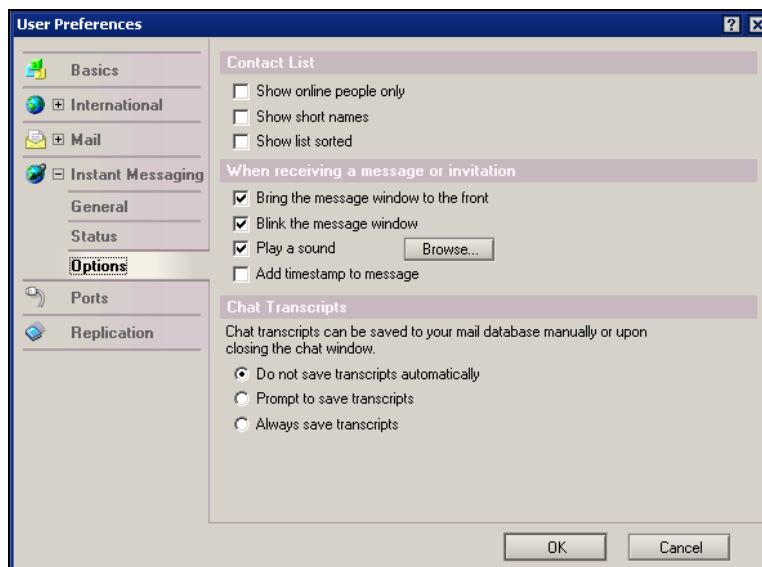
Although the General and the Status tabs are not new with Notes 7, some new features have been introduced to the General tab in this release. One example is the option Default text for invite to a meeting.



Another place to set instant-message preferences is via the status bar.



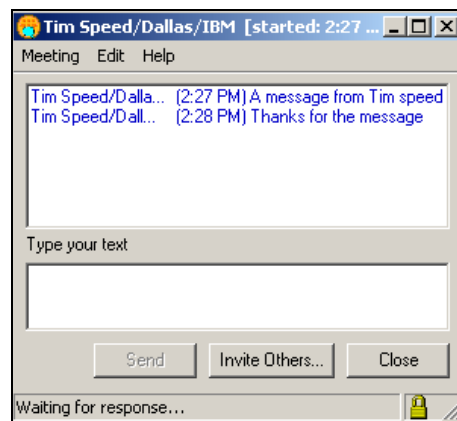
The Options tab, however, is new. The following screenshot shows the new options. The Options tab has three categories: Contact List, When receiving a message or invitation, and Chat Transcripts.



The Contact List category includes three options: Show online people, Show short names, and Show list sorted.

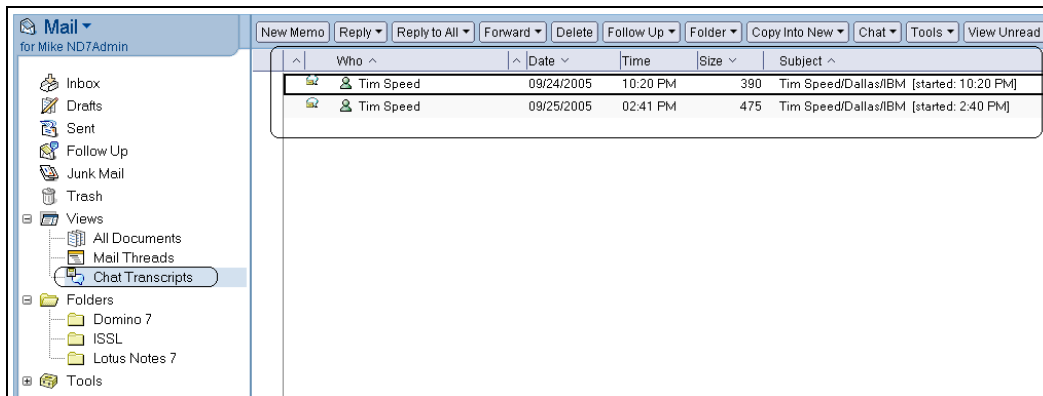
The When receiving a message or invitation category includes the following options:

- Bring the message window to the front brings the message box to the front of the screen.
- Blink the message window causes the message window to blink when a new message arrives.
- Play a sound plays a distinctive sound when a new message is received. You can browse the file list for the name of the sound you want to play.
- Add timestamp to message adds a timestamp prefixed to each message:



The next category is Chat Transcripts. In Notes 7, you save a transcript of your chat sessions to your mail database, manually or upon closing the chat windows. You have three options: Do not save transcripts automatically, Prompt to save transcripts, and Always save transcripts.

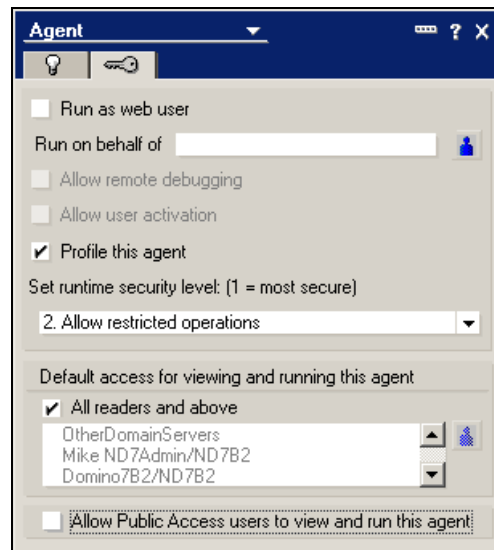
To save a transcript, select Meeting | Save to Database while in the chat window. If a transcript is saved manually or automatically, it will be saved to your mail file. If you are using a Notes 7 template, a special view is available to review the saved transcripts. The following screenshot shows an example of this view and sample transcripts:



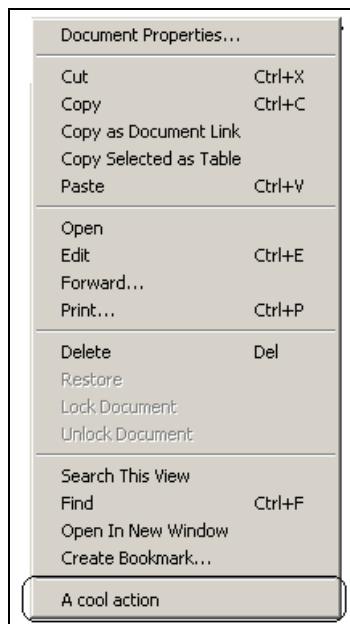
Domino Designer 7

This section describes some of the new and updated features offered in Domino Designer 7. For example, design lists have been redesigned for better display of information. Also new with Domino Designer 7 is the ability to edit forms from the design-view level.

The **Java debugger** allows you to prepare design elements that contain Java code for debugging, by using the checkbox provided for agents, web services, and script libraries. A remote Java debugger (for example, Eclipse) can then be attached to the Notes client JVMs, to debug these design elements. Also, agents can now be enabled for agent profiling, and the results of the profiling can be viewed from Designer. For example, calls to Domino Objects in agents that were created in LotusScript or Java can be monitored. You can also monitor the agents elapsed times reported. And if you want to view the profiling results for the latest run, select the agent and choose Agent | View Profile Results.



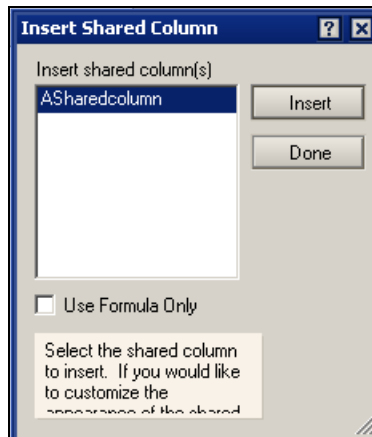
Another new feature is the ability to add custom actions to the right mouse button. All you need to do is create an action or insert a shared action. The action's properties box will include a checkbox labeled **Include in Right Mouse Button Menu**. When this is selected, you can open the view where you added the action (or shared action). Right-click the mouse, and you will see your action in the list.



Shared Columns

With shared columns, you can create a shared column that can be inserted into several views in the same database. The major advantage of this is that you can create a single column, add it to several views, and make changes to only one copy of the column for all views. The change you make to the single shared column will be propagated to all the views in which it appears.

To create a shared column, open Domino Designer 7 and select the Column icon. Select the New Shared Column button. Edit the column as you normally would; add formulas and titles. After the shared column has been created, you can add it to a view. To do this, open the view, right-click on the column, and select Insert New Shared Column or Append New Shared Column. The following screenshot shows the Insert Shared Column dialog box. This shows a list of pre-created shared columns. Select a column, or select a formula to select the column. Press the Insert button to complete the action.



When an existing shared column is saved and edited, all views containing the shared column will be updated. These views are resaved with the current user ID. Where Use Formula Only is checked, only the formula is updated. After the shared column is saved, you will see a dialog box that prompts you with the following: Upon saving, all views and folders that use this shared column will be updated. You now have three choices: Yes, No, and Cancel.

To delete a shared column, select the shared column design element. Then press Delete. You can even choose Edit | Delete. Note that when a shared column is deleted, the shared column is changed to an unshared column in all views containing the defined column. Another nice feature is the ability to use shared columns in DB2 views.

After you have created a shared column and added it to several views, select the shared column. You will see a button labeled Who is using this Shared Column. Select this button; this displays the list of views that have that shared column.

Administration Client

The Domino 7 Administration client provides many new features, including:

- Domino Domain Monitoring (DDM)
- Improved policy-based management
- Serviceability, including autonomic data collection
- Linux/Mozilla Web Administration client
- Improved email management
- Administration event scripting
- Rename reversion approval

When you open the Domino 7 Administration client, you will notice a new splash screen. After this, by default, an information page is displayed. This briefly discusses new features and where to get help on them.

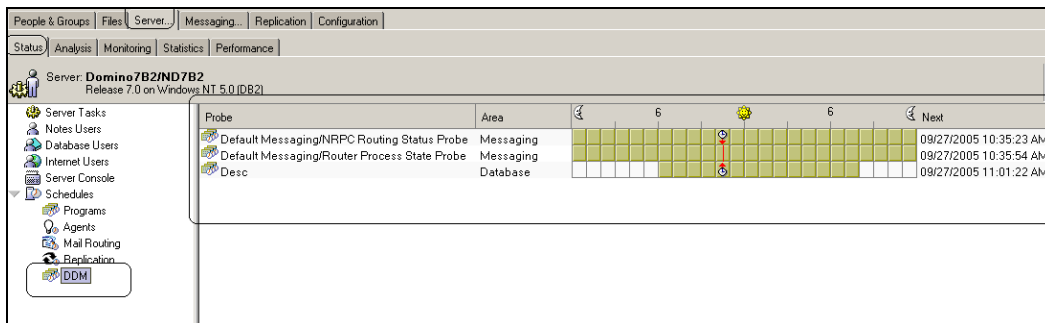


One great new feature is integration with the **Tivoli Autonomic Monitoring Engine (TAME)**. This provides event-reporting capabilities to other Tivoli interfaces, including the **Tivoli Enterprise Console (TEC)**. Also, this integration provides a framework for third-party resource-module plug-ins. Third parties can create resource modules to manage server events and add-in tasks.

Another powerful feature is probes. Probes can perform the following:

- SMTP probes verify that mail can be delivered to a particular SMTP recipient, via a **Delivery Status Notification (DSN)** report.
- Replication probes check for replication errors and conditions.
- Security probes can verify a database ACL against a predetermined configuration and check for inconsistencies in security configurations across multiple servers.
- Agent probes report the total number of agents run, agent security errors, time-out errors, and other agent-related information.
- A database probe ensures that a database can be opened. Another database probe monitors key locations in the database software layer, and generates events for errors.
- Directory probes check the health of a number of directory-related tasks and processes.
- Mail probes verify local mail routing, by sending a message to a known destination and verifying its delivery.

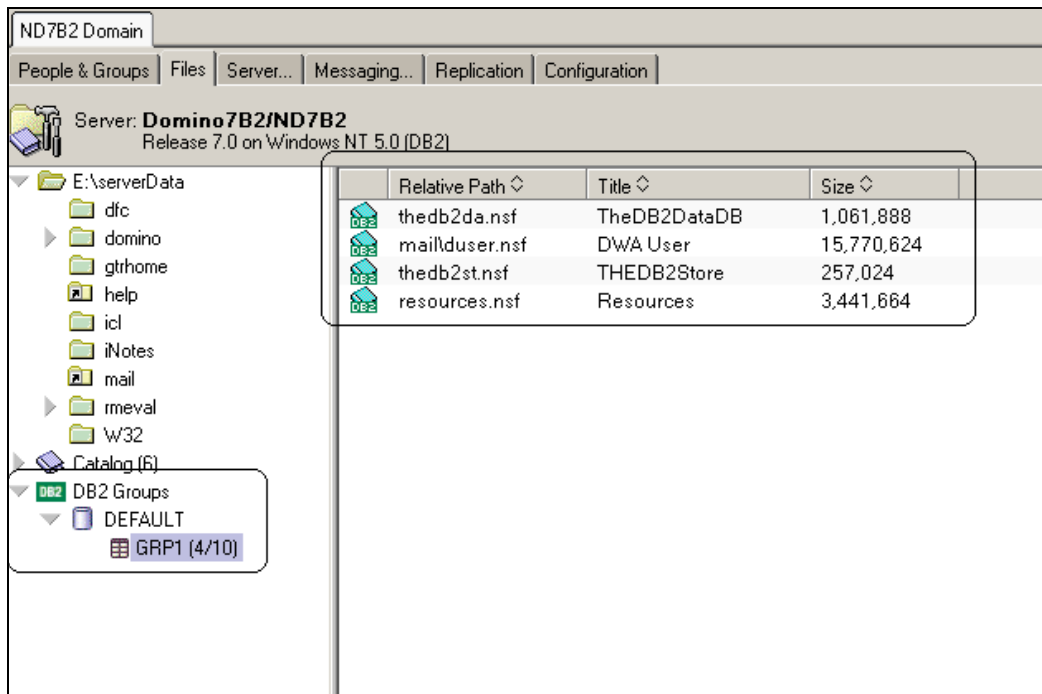
After probes are configured in the events4.nsf database, all you need to do is open the Domino 7 Administrator and select **Server | Status**, and then select **DDM** from the list. The following screenshot shows the monitoring screen:



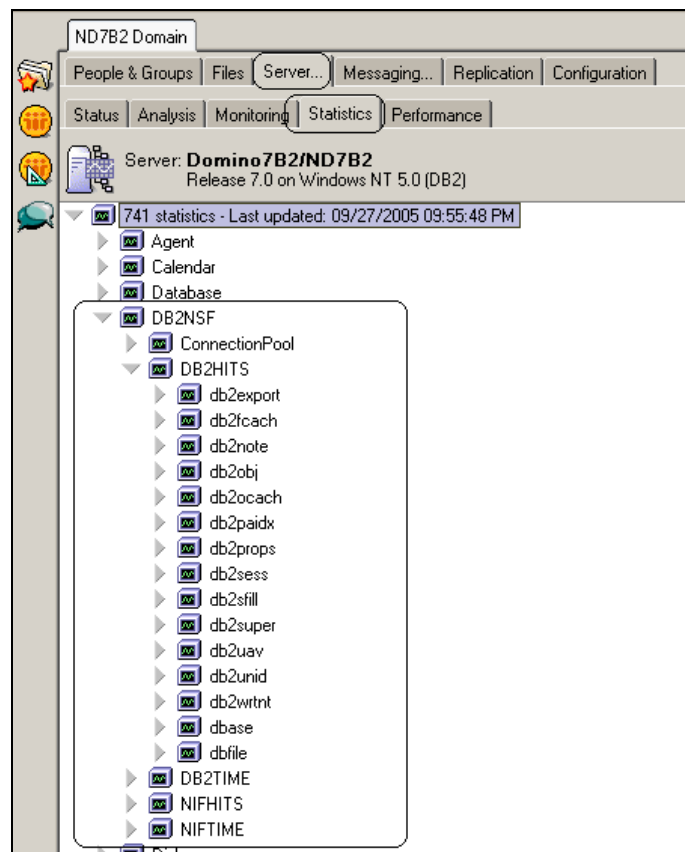
Other features include the Domino 7.0 Web Administration client from the Mozilla Web browser on a Linux system, enabling an end-to-end Linux deployment of Domino and Domino Web Access, with no need for Windows in the environment.

Domino 7 also supports rename reversion approval. The Administration process (also known as AdminP) no longer automatically reverts name changes. It now requires the administrator to either approve or reject the name change reversion.

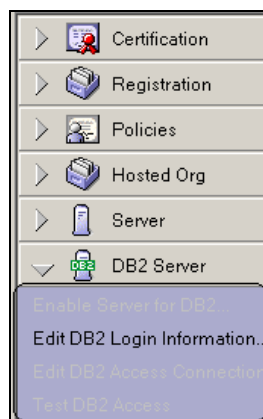
Lotus Notes 7 has administration support for DB2, including an enablement tool to set up Domino to run with a DB2 data store. An integrated API has also been added—to allow for management of DB2 users and passwords—as well as a tool to monitor DB2 groups. Domino uses DB2 groups to manage database storage in a Domino DB2 system. Groups allow multiple DB2-enabled Notes databases to share a DB2-based schema. This includes DB2 tablespace. The following is an example of DB2 management in the Domino 7 Administrator.



You can also monitor DB2 statistics in the Notes 7 Administrator client.

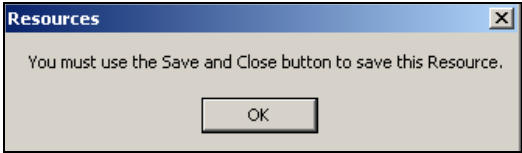


The Notes 7 Administration client also includes a set of tools to enable and test for DB2 connectivity. See the following screenshot for an example:



Hotkeys

Overleaf is a short list of client hotkeys (Windows commands shown). Let's start out with a few of our favorites. (Be sure to check out the client help file for a longer list.)

Press	To do this
<i>Ctrl+M</i>	This will create a new mail memo. This is also a quick method to test the location document settings. If your location document is set incorrectly for the server name, and file name of your mail file, then this command will fail.
<i>Ctrl +O</i>	This will open a new open database dialog box.
<i>Esc</i>	This is an old stand-by. This will close forms, views, date picker, time picker, and many other Notes dialog boxes.
<i>Ctrl+S</i>	This saves the current open document.
<i>Ctrl+E</i>	This edits a document. Note that this does not always work; for example, if you do this in a resource document, you will see a prompt asking you to use the Save and Close button.
	
Arrow keys	<p>This can be different, based on the context of where you are in Lotus Notes. You can use arrows almost anywhere in Notes. Here are a few examples:</p> <ul style="list-style-type: none"> • In some cases to select different documents • In a Calendar to select different days • With the space bar to select docs in a view
<i>Delete</i>	This will delete a document and/or select a document for deletion.
<i>Ctrl+W</i>	This will close the current document window.
<i>F9</i>	Refresh views.
<i>F6</i>	Move focus to next pane or frame in the Notes client.
<i>F5</i>	Logout.
<i>F1</i>	Context-sensitive help.
Return	Close the current document and open next document.
Return	Open a selected document or view.
Backspace	If you are in a document, this will take you to the previous document in the view.

Summary

This chapter discussed the new features introduced in the Notes 7, Domino Designer 7, and Domino Web Access 7 clients. We began with a review of the major enhancements in Notes 7. These include better window management, new mail features, background view indexing, Calendar and Scheduling (C&S) improvements, expanded Rooms and Resources (R&R) capabilities, and better Sametime integration. We then reviewed release 7 enhancements to the Domino Designer (such as upgraded design lists and Java debugger), and the Domino Administration client.

9

Domino Web Access

Domino Web Access (previously iNotes Web Access) provides Lotus Notes users with browser-based access to Notes email and calendar and scheduling. **Domino Web Access (DWA)** lets you send and receive mail, view calendars, invite people to meetings, create to-do lists, keep a notebook, and work offline. After the Domino administrator enables you for Domino Web Access, you can use the standard Notes client *and* a web browser to access your mail files. Read and unread marks will remain up to date since both the Notes client and Domino Web Access operate on the same basic user mail file. Users can also synchronize contact information in their Lotus Notes Personal Address Books with information in their Contact List in Domino Web Access.

Security

Domino Web Access requires user login and logout security. When you log in to Domino Web Access, you must enter your name and internet password, as specified in your Person document. The login names that the server accepts as valid depend on the setting in the Internet authentication field on the Security tab of the Server document. When you log out, Domino Web Access closes the browser and removes your login credentials and private data from the browser's cache. By deleting this data, Domino Web Access prevents unauthorized users from using cached information to access the user's mail file.

Using browser cache management, you can improve the client-side performance and security of Domino Web Access sessions on Internet Explorer by controlling which entries are stored in the cache and which ones are removed when the Domino Web Access session ends. The removal of private data from the browser's cache and more secure data clearing capabilities are available only if the user accepts the Domino Web Access control.

Domino Web Access will not remove some personal data unless the user explicitly selects Logout for Shared PCs or Kiosk Users. With this selection, users can choose one of two secure logouts:

- **Secure:** This deletes all traces of your personal use of Domino Web Access and any web pages that you may have browsed, but keeps Domino Web Access program elements. This boosts performance when the next person logs on.
- **More secure:** This deletes all traces of Domino Web Access and all other web pages in the Temporary Internet files folder.

You can also redirect users to a specific web page after they log out.

Integration with DOLS and Instant Messaging

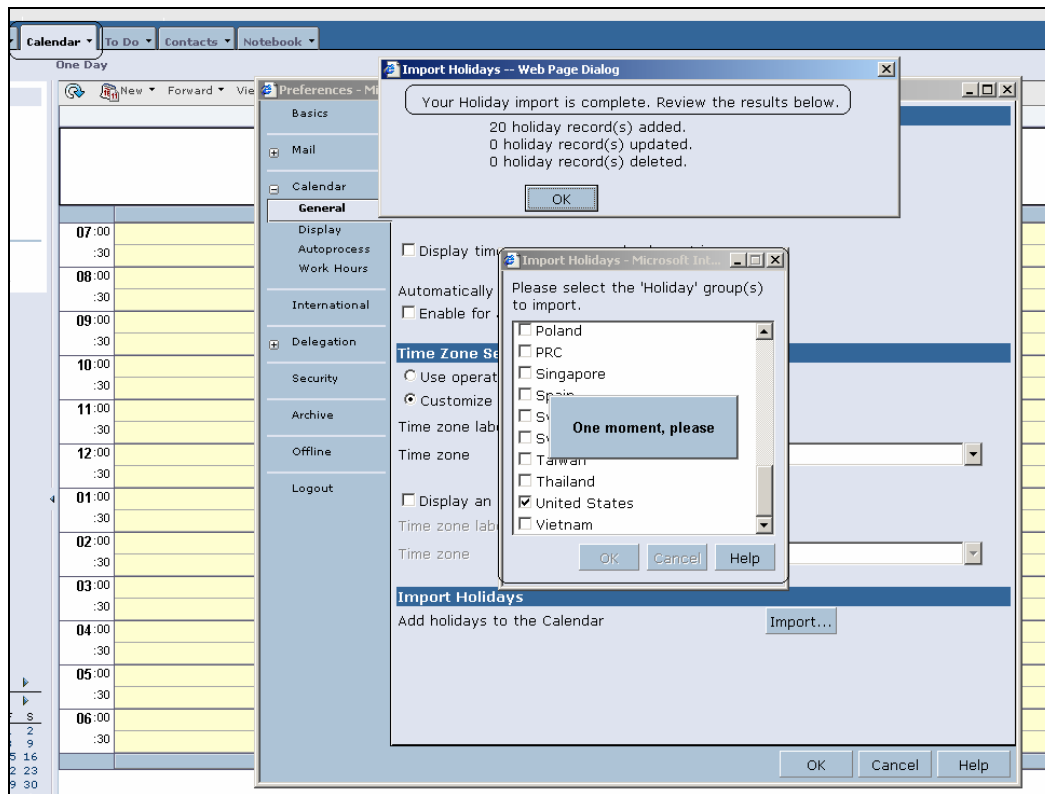
To provide users with the ability to work offline and use instant messaging, you can integrate Domino Web Access with **Domino Off-Line Services (DOLS)** and Sametime. DOLS enables users to work offline, disconnected from the network, and provides many replication features that Notes users expect when working in the Notes client. Sametime provides integrated, real-time instant-messaging and chat features for Domino Web Access users. Neither DOLS nor Sametime Messaging is required for Domino Web Access use.

Instant Messaging

The integrated Sametime instant-messaging feature is much more robust and more closely mirrors the Lotus Notes client-awareness features. Name awareness has been added in views such as contacts, calendar and scheduling, and meetings, with right-click menus available for each of the views. In Notes/Domino 7, Domino Web Access users will be able to use the Lotus Sametime Connect 6.5.1 contact-list manager, and will be able to share contact lists with the Lotus Notes client.

Import Corporate Holidays

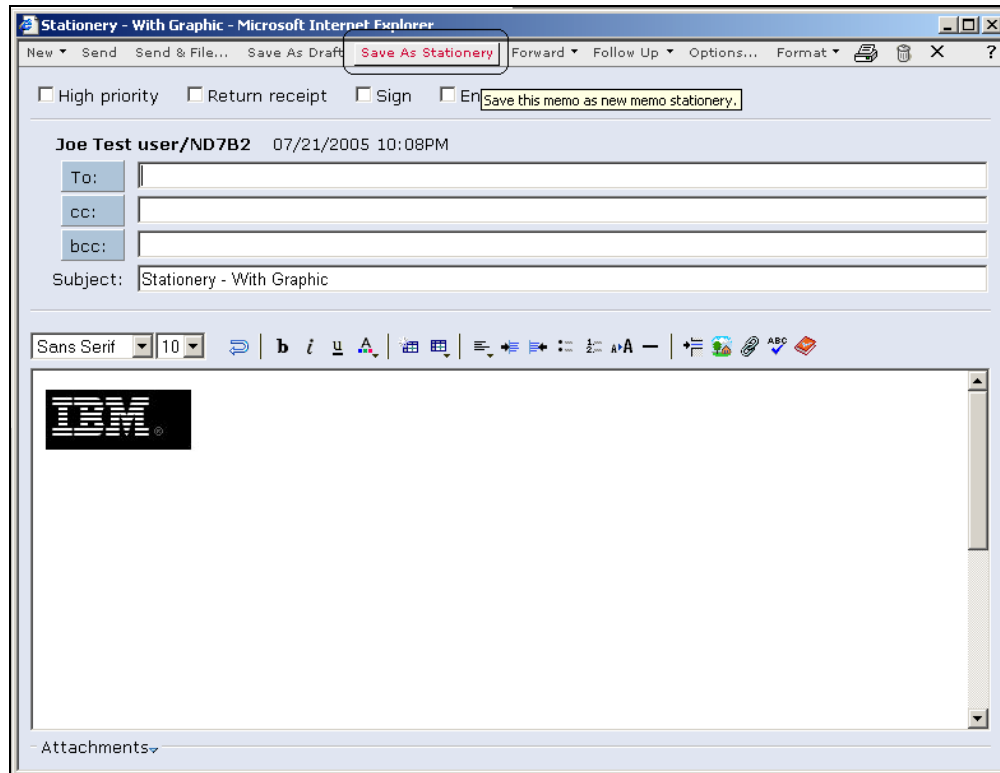
In Notes/Domino 7, DWA users have the ability to import holidays into their calendar via DWA preferences. You can now import holidays into your calendar using predefined country-specific sets. The following screenshot shows how Domino 7 DWA clients can import Holidays into a DWA client:



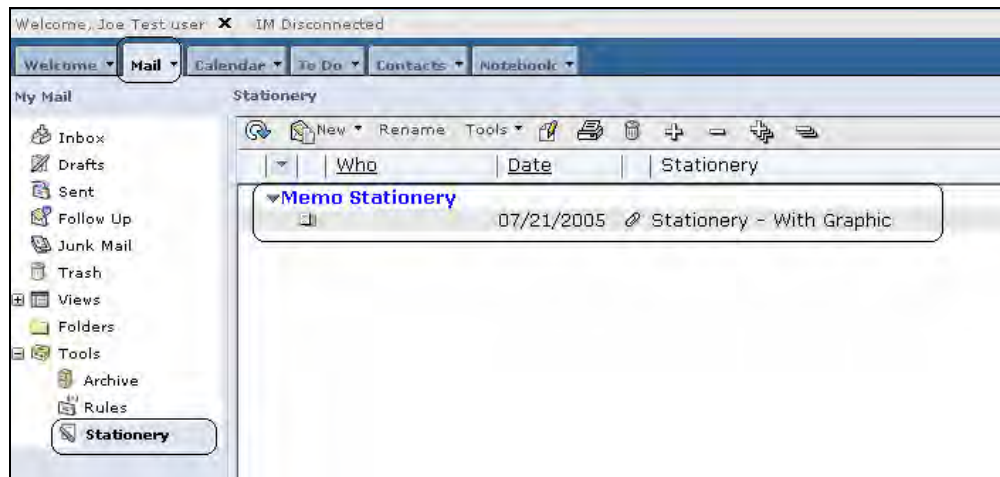
Stationery

You can also create stationery that you can reuse for your mail messages. Stationery can include text and graphics, and other information such as mail-delivery options. You can create standard stationery that includes recipients. This is useful for messages that routinely get mailed to the same group of people. You can also create personal stationery that includes personalized text or graphics.

Here is a sample of stationery with an embedded graphic:



The following screenshot shows how user Joe can use the Memo Stationery, which was created in DWA:



Mail Threads

With Domino 7, users can now view mail threads. A mail thread groups a message together with the responses to it. Mail threads can be viewed from the DWA Mail Threads view. Mail threads can also be viewed when reading mail. To view mail threads when reading mail, DWA users select the Mail | Display user preference.

S/MIME Support

In Notes/Domino 7, DWA now includes the same level of S/MIME support that the Notes client offers. S/MIME is the standard encryption technology used to secure Internet-based (SMTP) email.

Mail encryption protects messages from unauthorized access. Basic mail encryption is not new with Lotus Notes and Domino. The Notes client has the ability to encrypt both Notes mail messages (via PKCS RSA encryption) and Internet-based email (via S/MIME). Notes users can encrypt mail sent to other Notes users or to users of mail applications that support S/MIME, including Netscape Communicator and Microsoft Outlook.

Public-Key Cryptography Standards (PKCS) are specifications produced by RSA Laboratories, in cooperation with secure systems developers worldwide, for the purpose of accelerating the deployment of public-key cryptography. First published in 1991, the PKCS documents have become widely referenced and implemented. Contributions from the PKCS series have become part of many formal and de facto standards, including ANSI X9 documents, PKIX, SET, S/MIME, and SSL.

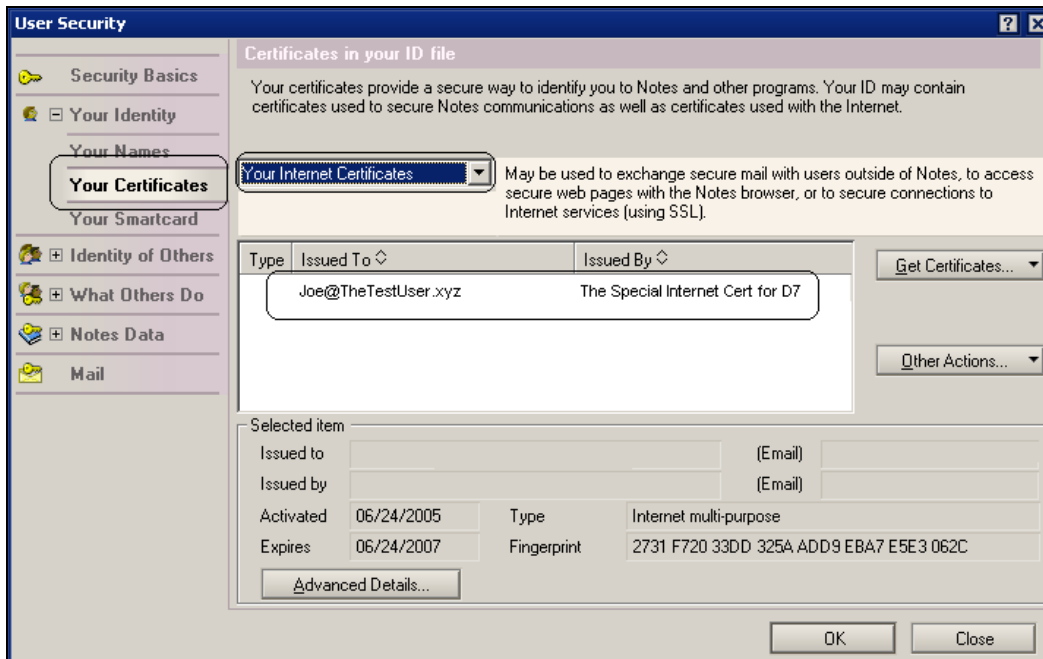
Internet email is based on a standard known as SMTP. The initial SMTP specification is a standard (RFC821) first published in 1982 before the Web as we know it even existed. If you send a message on the Internet, you use SMTP. Notes/Domino fully supports SMTP messaging, providing many powerful mechanisms to keep the message secure.

At about the same time SMTP was defined, **Public Key Infrastructure (PKI)** was developed. PKI is a secure system for a trusted third party (known as a Certificate Authority or CA) to provide digital identities to users and servers and to publish those identities using X.509 V3 digital certificates. The identity consists of an asymmetrical key pair: a public key that anyone can use (thus the name), and a unique private key known only to the user. This digital identity can then be used to exchange text securely by encryption using the key pair.

Lotus Notes supports the use of X.509 V3 certificates. To enable your Notes/Domino site to use these certificates, each user must have the X.509 certificate in their Notes. id file. With Notes/Domino 7, there are many different mechanisms available to import these certificates into a Notes. id file. These include:

- Manually importing the certificate. This is known as a PKCS 12 extract. Normally the certificate is housed in a file with a . p12 extension.
- Using the Lotus Domino Certificate Authority (CA) process to place the certificate into the Notes. i d file.
- Using the Domino Administrator to place the certificate into the Notes. i d file.
- Using Domino Web Access to manually import the certificate into the Web-hosted Notes. i d file.

After the certificate has been placed into the Notes. i d file, you can view it using the Notes client by selecting File | Security | User Security, clicking on Your Certificates, and selecting Your Internet Certificates:



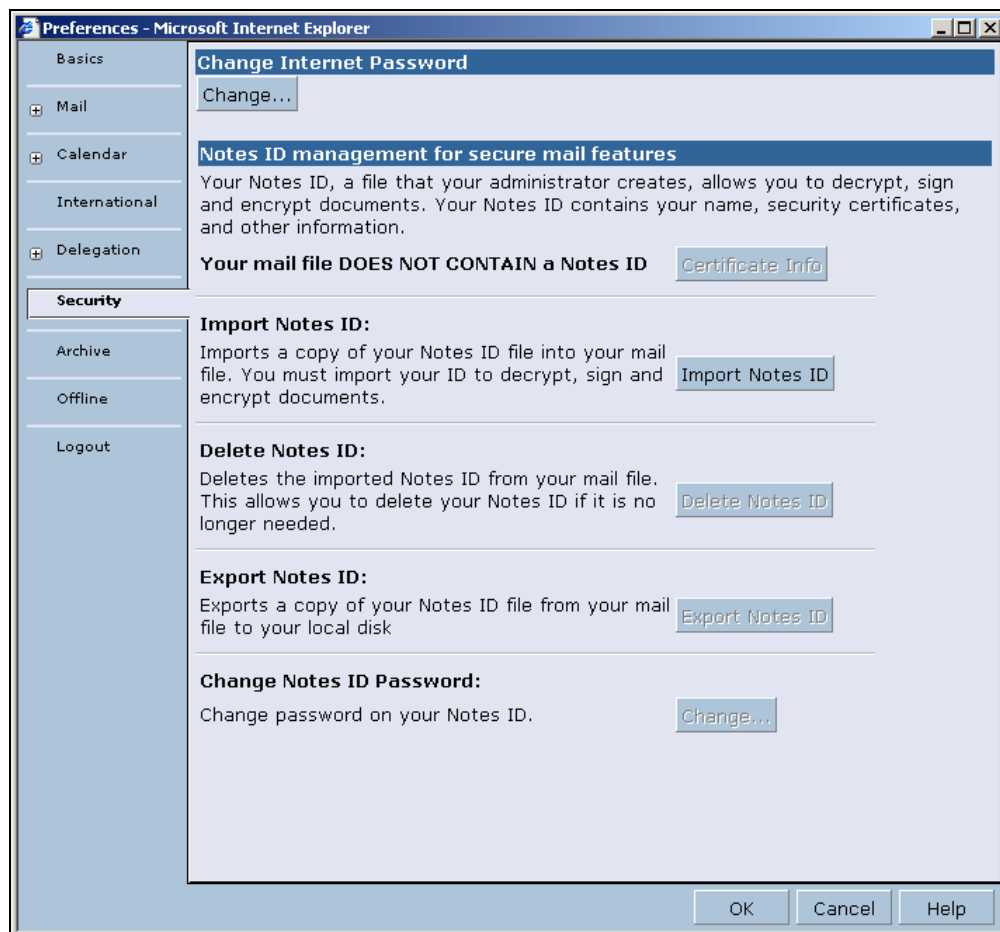
The preceding screenshot showed the certificate was issued to Joe@TheTestUser. xyz, and was issued by The Special Internet Cert for D7.

As mentioned previously, DWA with Notes/Domino 7 provides several mechanisms to import an X.509 certificate into the DWA mail file. These methods are described in the following sections.

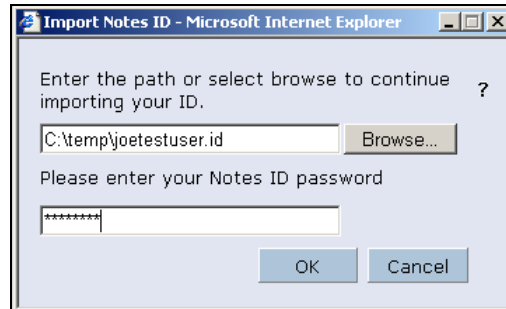
Importing a Notes ID

You can import a copy of a Notes ID (Notes. i d) file into a mail file. This imported ID file can be used to digitally sign, encrypt, and decrypt Notes documents. Also new with Domino 7, you can sign and encrypt Internet documents. This is possible if an X.509 certificate is hosted in the Notes. i d file that is imported.

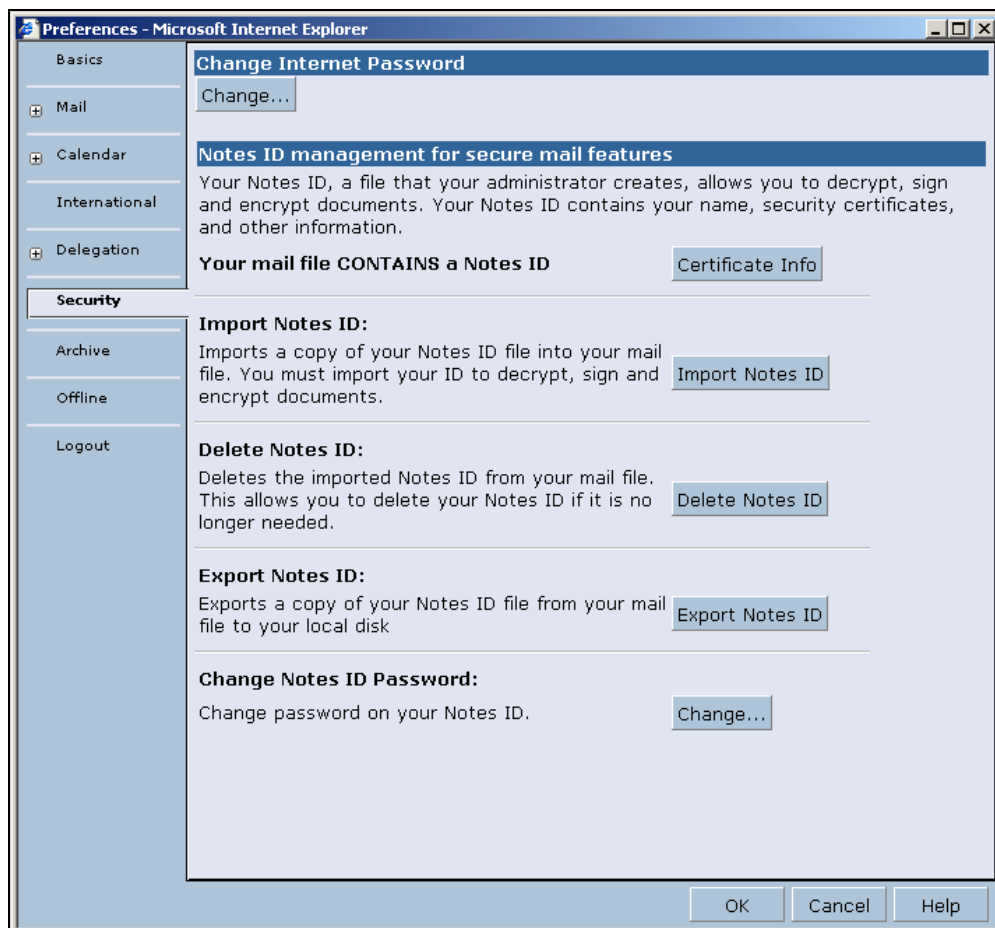
Importing a Lotus Notes ID file into the client is easy. Just select Preferences | Security | Import Notes ID. The following screen is displayed:



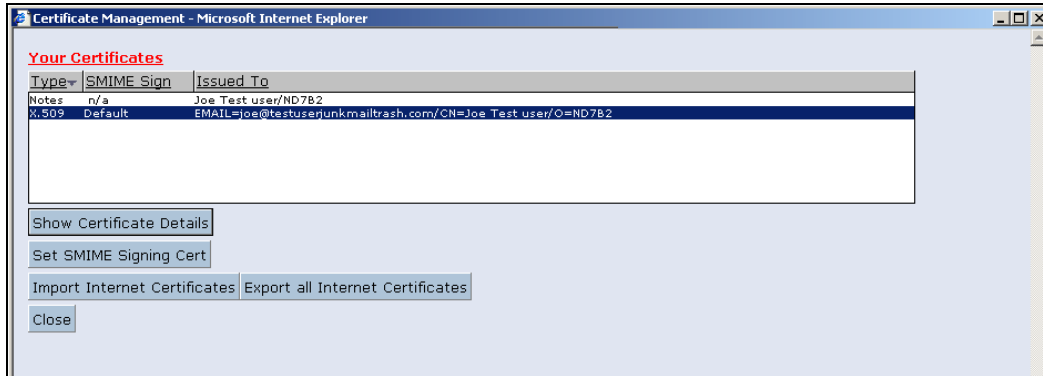
Clicking Import Notes ID displays the following dialog:



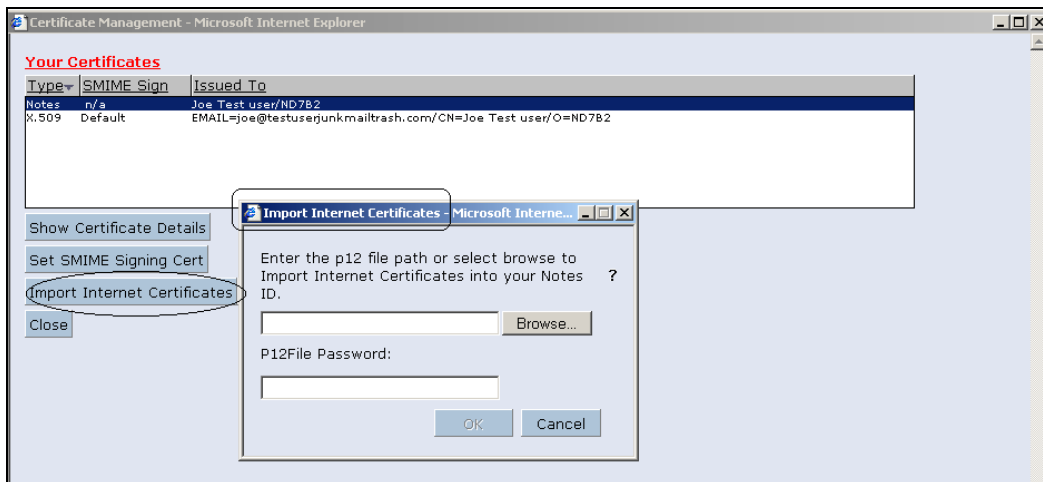
Enter the path and name of the Notes .id file, as well as its Lotus Notes password. The following screenshot shows that a Notes ID file has been added into the DWA mail file:



After the ID has been imported, you can view your Lotus Notes certificate and your Internet certificates. You can host several X.509 certificates, for example one for digital signature and one for encryption.



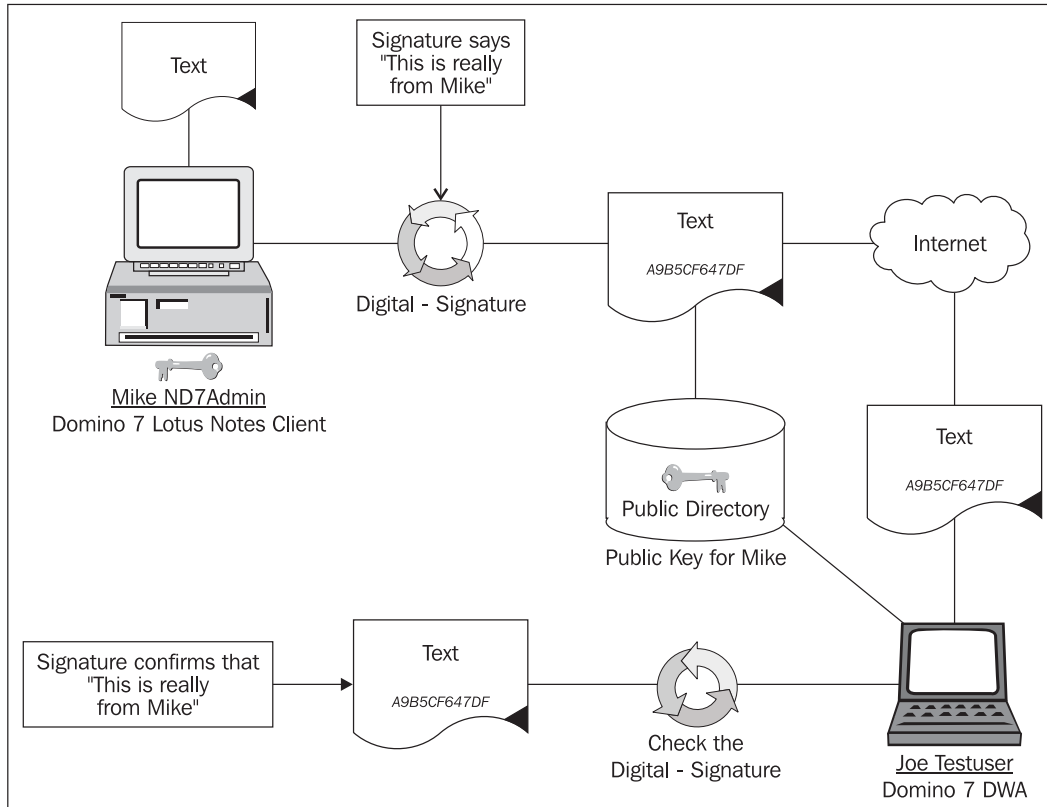
Support for hosting a Notes ID in your DWA mail file was introduced in release 6.5. So, as part of your Notes/Domino 7 upgrade process, you may want to import a P12 X.509 extract into the Notes ID contained in your DWA mail file. This feature will be available after you have upgraded the server to Domino 7 and have also upgraded the mail file to a Domino 7 template. The following screenshot shows how you can add an X.509v3 certificate into an upgraded Notes/Domino 7 DWA mail file:



Let us now look at a real example of using the Notes 7 client and the Domino 7 DWA client to send and receive signed and encrypted S/MIME messages. In our simple scenario, we have two users. One user is Mike ND7Admin (email address

MikeND7Admin@TheD7Company.xyz) using Notes 7 client. The other user is Joe Testuser (email address JoeTestuser@test.xyz) running the DWA 7 client. In this example, we are using two different Internet certificates. As a result, cross-certificates will be required, and/or you will need to accept untrusted certificates (see the discussion on DWA configuration setting after the figure).

The following diagram shows both the users.



After the public keys are accepted, each user can send an encrypted message to the other. To do this, the following two steps will be executed:

The users send each other a signed message and accept the signature into their address (contract list) book.

As each message is accepted, the other person's public key is placed into the address book.

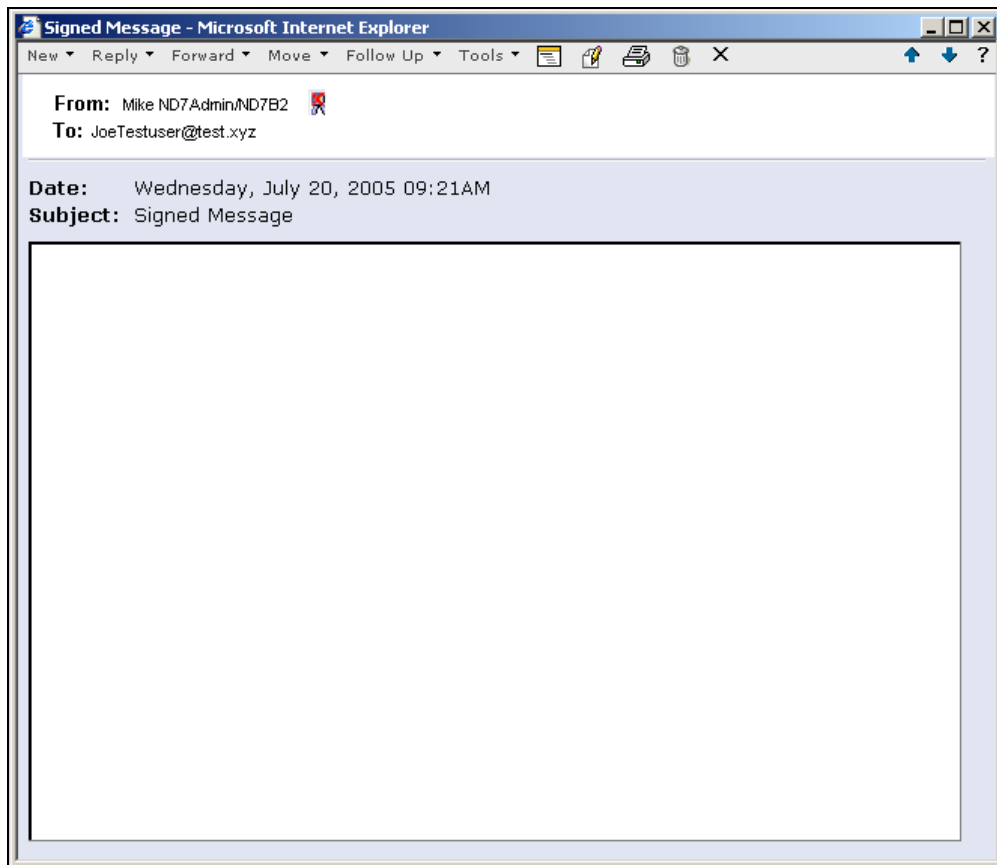
So let's start this process by having Joe Testuser send a signed message from a Domino 7 DWA client to Mike ND7Admin. When Mike receives and opens this message, he is prompted to accept a cross-certificate. The reason for this is that certificates will have some type of ancestral certifier or a common root certificate. In each case, trusted is defined and/or implied. If the root certificate is not in common with each user, then a cross-certificate will need to be issued. Lotus Notes provides a system to generate cross-certificates. DWA provides settings that allow you to accept untrusted certificates. To send an encrypted message, the sender needs to have the recipient's public key. In our example, Mike sends a signed message to Joe. So in this case, it is important that Joe accepts the message from Mike and adds Mike's public key into Joe's personal contact list. After this process is completed, Joe can send an Internet-based encrypted message to Mike.

After the entry has been added into Mike's address book, Joe's public key will be listed as **Present** in the Internet certificate field of Joe's Person record. An example of this information is shown in the following screenshot:

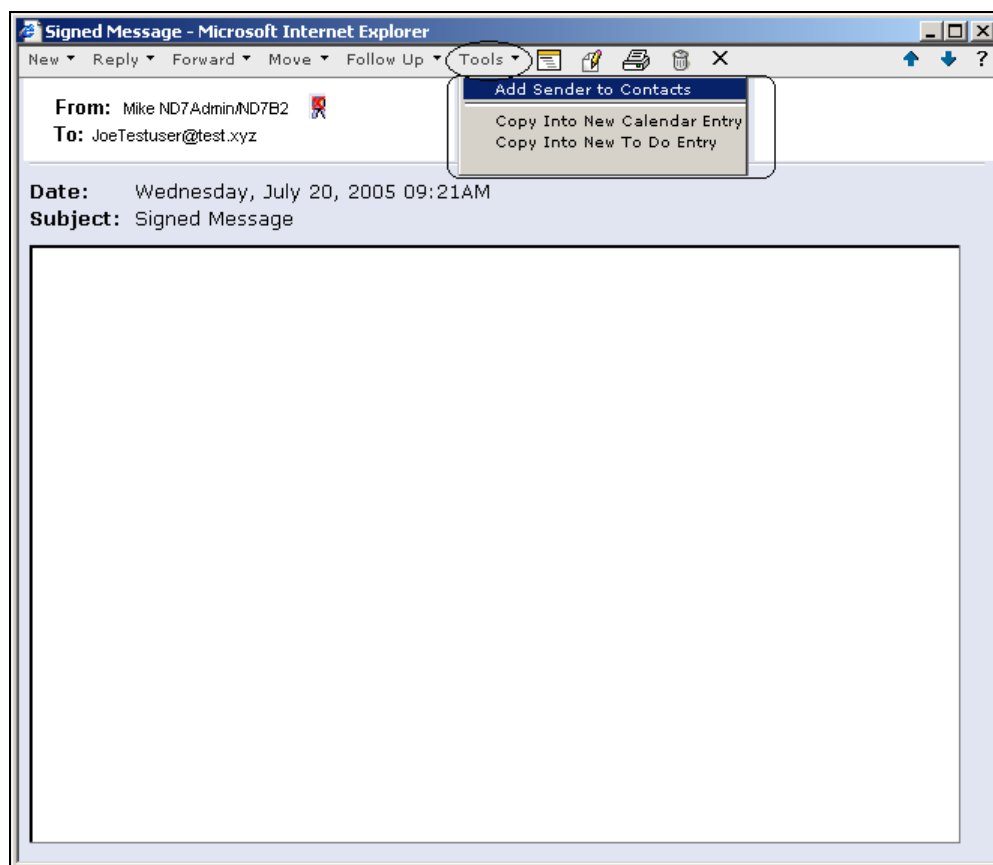
The screenshot shows the 'Joe user' entry in a Lotus Notes address book. The entry is titled 'Joe user • Joe Testuser/ND7B2'. The main form has tabs for 'Business', 'Personal', 'Briefcase', and 'Advanced'. The 'Business' tab is selected. The form is divided into several sections:

- Name:** Fields for First (Joe), Middle (Test), Last (user), Title (dropdown), Suffix (dropdown), and Email (Joe Testuser/ND7B2).
- Organize:** Fields for Categories, Display name format (Firstname Lastname), and Show in preview pane (Business data).
- Internet certificate:** A section with a table showing the status of the Internet certificate. The 'Internet certificate' column shows 'Present' and the 'Internet certificate issuers' column shows '1. CN=Bubba The Duck/OU=Dude/O=The Bubba/L=Denton/ST=Texas/C=US'.
- Notes certificates:** Fields for Certified public key and Flat name key.

Now Mike, via his Notes client, can send a signed message to Joe. Joe receives the message and notices there is a certificate symbol associated with the message. This symbol tells the user that there is a digital signature assigned to the message, and whether the certificate is a 'trusted' certificate. Use the mouse over to display the trust status:

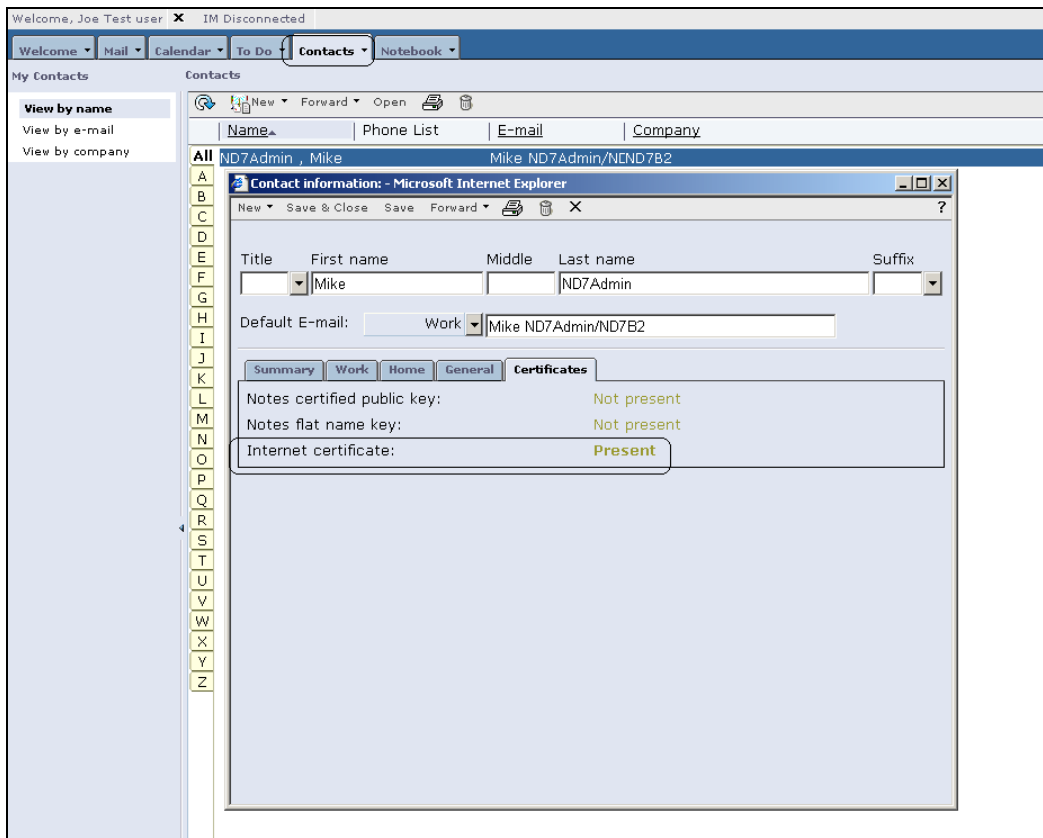


After Joe receives the message, all he needs to do is to Add Sender to Contacts:

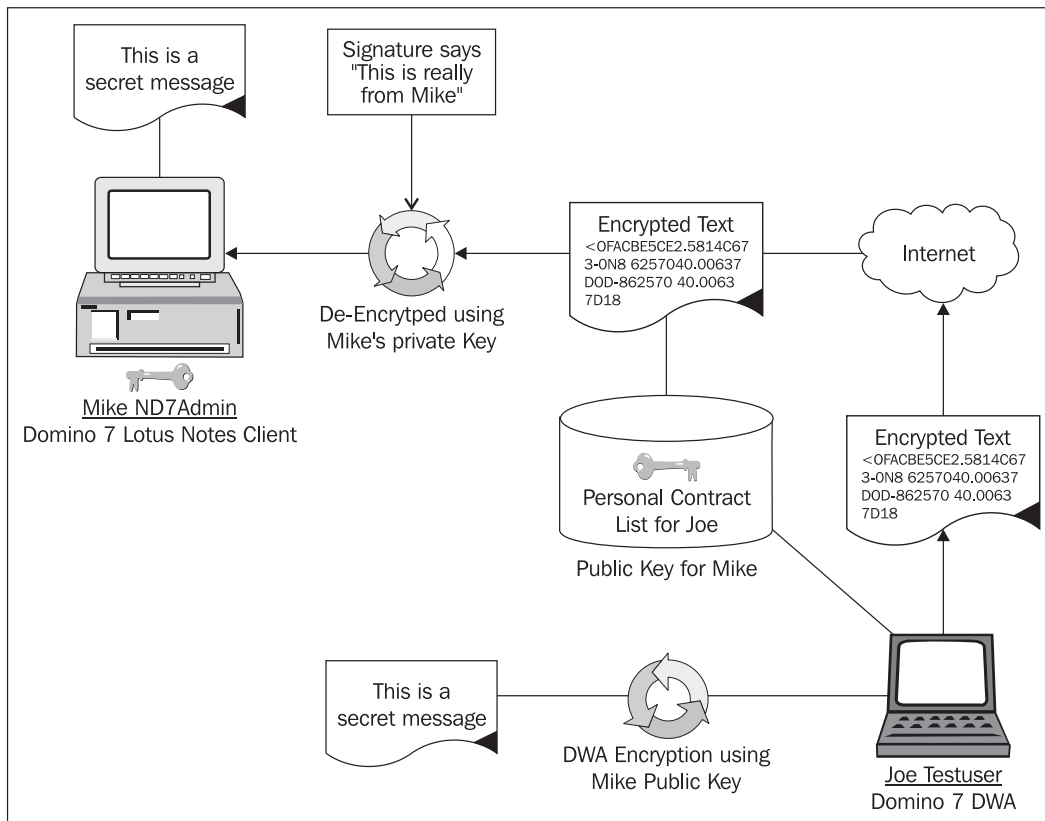


At this point, Mike's certificate is available to Joe. All Joe needs to do is to save this contact and then reopen the contact entry. After he reopens the contact, the certificate will show as being present:

Domino Web Access

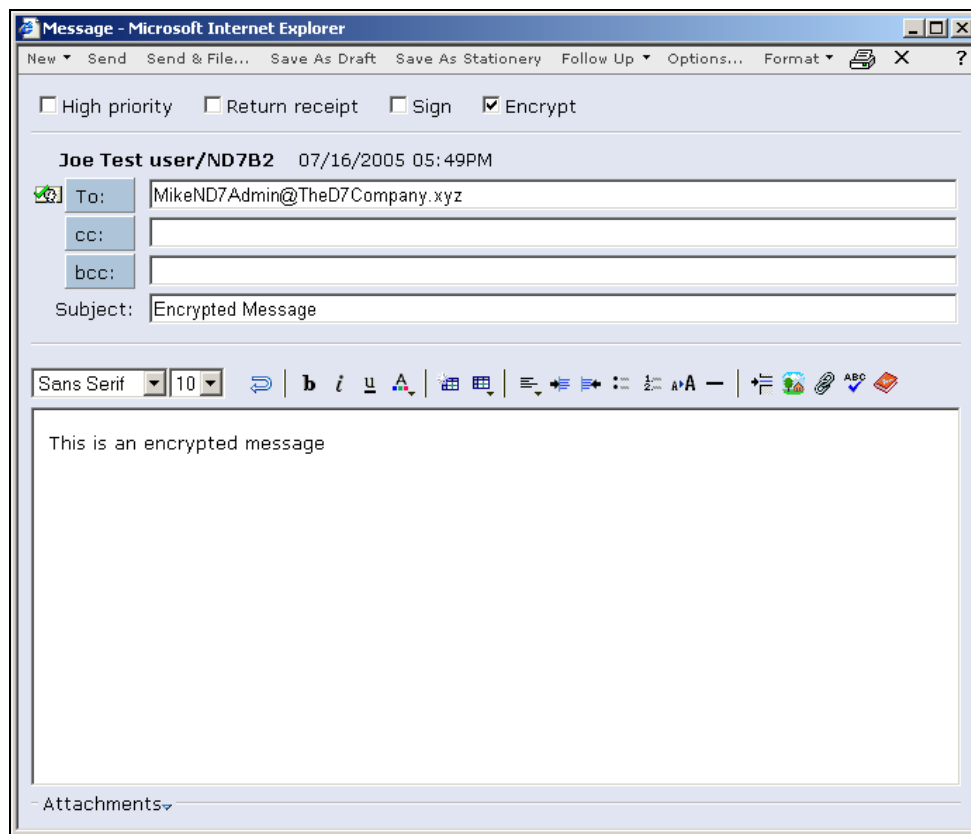


Now Joe and Mike are ready to send and receive encrypted messages with DWA. The following diagram shows the process:



A message is created with either DWA or Lotus Notes. The message is then encrypted using the target (recipient) person's public key. Remember that Mike and Joe exchange their public keys via signed messages. Joe creates a message to Mike, and selects Encrypt this message. The DWA client finds Mike's public key in the DWA contact list. The message is encrypted and sent, via SMTP, to Mike. Using Notes, Mike will read and decrypt the message using his X.509 certificate.

The following screenshot shows the DWA 'new memo' page, which now includes the Encrypt checkbox:



Domino Web Access Configuration

Now let's discuss Domino Web Access configuration, which in Notes/Domino 7 has been modified to accommodate new Web-related features and changes. To work with Domino Web Access configuration information, open the configuration settings document and select the Domino Web Access tab:



The first noticeable update is the Mail section in the Domino Web Access tab. A new field, Mail Threads, is available. If Enabled (which it is by default), this will allow users to set a Domino Web Access user preference to view mail threads.

Mail	
Minimum mail polling time	5 minutes
When sending mail, set format to:	Let user decide
Name resolution and validation:	Enabled
Maximum attachment size (kb):	50000
Mail threads:	Enabled

Mail Encryption

To allow Domino Web Access users the ability to encrypt and digitally sign email messages, you must enable both the Encrypted mail support and the Name Resolution and Validation fields in the Domino Web Access tab of the server's configuration settings document, as shown in the following:

Mail Encryption	
Encrypted mail support:	Enabled
Allow user to delete their Notes ID from their mail database:	Disabled
Allow user to export their Notes ID:	Disabled
Require SSL when reading encrypted mail:	Client
Use JavaScript for SSL-redirection requests:	Enabled
Allow untrusted Internet certificates to be used for S/MIME encryption:	Disabled

Another setting that impacts on the new DWA S/MIME settings is Allow untrusted Internet certificates to be used for S/MIME encryption (see the preceding illustration). This is enabled in the Mail Encryption section in the Domino Web Access tab. Domino administrators can enable this setting to allow users to use an untrusted Internet certificate for S/MIME encryption. Note that this setting is disabled by default.

Instant Messaging

Another new Domino 7 feature for web management in the configuration settings documents is the Instant Messaging tab. This tab includes the options shown in the following screenshot:

Instant Messaging	
Instant Messaging features:	Enabled
Online awareness:	Enabled
Allow secrets and tokens authentication:	Enabled
Set an Instant Messaging server hostname for all DWA users (useful for clustered configurations):	
Loading lstlinks from Domino application server:	Enabled
Prefer "Sametime Java Connect for browsers":	Enabled
Set to use pass the current user's O= part of their name as the organization to Sametime:	Enabled
Allows adjusting the format of the name which is passed to Sametime for login:	

Instant messaging options include:

- **Instant Messaging features:** When set to Enabled (the default), this turns on Sametime features such as chat and online-presence awareness (live names). (Note that you also need to assign a Sametime server for these features to be available to clients.)
- **Online awareness:** When set to Enabled (the default), this setting turns on online-presence awareness for any users that also have awareness enabled via their user preferences.
- **Allow secrets and tokens authentication:** When set to Enabled (the default), this setting will use secrets and tokens authentication, if available. When set to Disabled, if an LTPA token is present, Domino will use the LTPA token instead.
- **Set an Instant Messaging server hostname for all DWA users (useful for clustered configurations):** Enter the name of the Sametime Instant Messaging server that will set a Sametime hostname for all Domino Web Access users. This feature removes the need to populate the Sametime server field value within every user's Person document.

- Loading \stlinks from Domino application server: When set to Enabled (the default), this loads \stlinks (Sametime Links) from the Domino application server. When set to Disabled, this loads the \stlinks directory from the Sametime server defined in each user's Person document. This should be used if you are running different versions of Sametime servers within your organization and are using a version of Domino prior to 6.5.2.¹
- Prefer "Sametime Java Connect for browsers": When set to Enabled (the default), this feature loads the Sametime Connect for browsers (6.5.1 or later) as the chat client. When set to Disabled, this will use the Domino Web Access Chat client.
- Set to pass the current user's O= part of their name as the organization to Sametime: For xSP users only (see the following section for more information about xSP). The default for this setting is Disabled. If Enabled, this will include the user's organization as part of the name format (for example, CN=Bubba Smith/O=Domino7).
- Allows adjusting the format of the name which is passed to Sametime for login: This has four settings;
 - Sametime using Domino Directory (or blank) can be used if the Sametime server and Domino Web Access server both use the Domino Directory.
 - Sametime using Domino LDAP can be used if the Sametime server uses the Domino LDAP directory and the Domino Web Access server uses the Domino Directory.
 - Sametime using another LDAP can be used when the Sametime server and the Domino Web Access server both use an LDAP directory other than Domino LDAP.
 - Sametime using xSP Domino LDAP (xSP servers only) is for when the Domino Web Access xSP server uses the Domino Directory and the Sametime server uses the Domino LDAP server.

¹ Sametime Links is a toolkit that allows web developers to Sametime-enable their web pages and applications with **aware names**. A simple HTML JavaScript API allows web developers to turn existing names into Sametime links by simply adding a few lines of HTML code, without impacting the layout of the page.

xSP

The generic term xSP can refer to many different types of service providers—application, Internet, storage, and management, to name just a few.

A Domino service provider delivers services to small-to-medium-sized businesses, or multiple hosted organizations from a single Domino domain. To those hosted organizations, the service provider offers IP-based access to a specific set of applications running on Domino servers. By using a service provider, a company can outsource the administration of applications and services that were formerly run on the company's computer infrastructure.

The responsibilities of a service provider administrator include maintaining both, the server environment at the host site, as well as (to varying degrees) the hosted organizations.

First and foremost, the service provider administrator is responsible for setting up and maintaining xSP servers (that is, protocol and database servers) as well as any Domino clusters and network routers.

Although the hosted organization administrator can perform some of the user and group maintenance, the service provider administrator performs a significant amount of the administrative tasks required to maintain a hosted organization. At a minimum, the service provider administrator is responsible for registering and maintaining hosted organizations and controlling which applications the hosted organization uses. In addition, the service provider administrator must create and maintain a mechanism that the hosted organization's administrators use to communicate problems and issues that require the intervention of the service provider administrator.

International

The Server Configuration document for Web Access also includes a section labeled International:

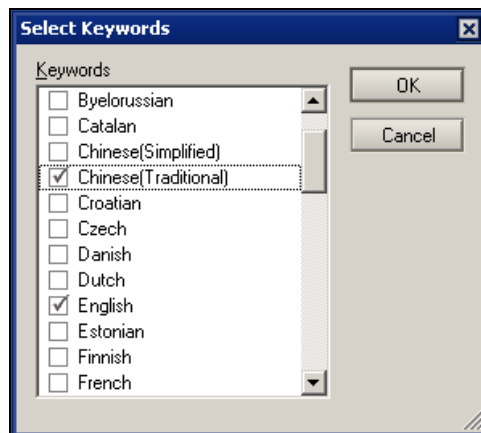
International	
Alternate name support:	Enabled
Preferred alternate name languages:	English
Allow user to choose alternate name display:	Disabled

Alternate name support is not new with Domino 7; it was first introduced in release 5. Nonetheless, we probably should spend a little time discussing how alternate names work. The alternate naming feature allows you to assign two names—a primary name and an alternate name—to an end user. The primary name is normally internationally recognizable. The alternate name is recognizable in the user's own native language. Alternate names allow users to use their native languages and also use a native language character set to display their names. Each alternate name can be associated with a specifier that identifies the native language to be used in the user's .id file.

The Enable option for Alternate Name Support enables alternate names. By default, this setting is enabled to allow Domino Web Access users to display alternate names in a native language. Domino administrators can also disable this feature to prevent Domino Web Access from displaying alternate user names in a native language. If disabled, users see alternate names in English only.

Other International options include:

- Preferred alternate name languages: This setting overrides the preferred language for an alternate name set in user preferences. You can select the list of languages from a drop-down list:



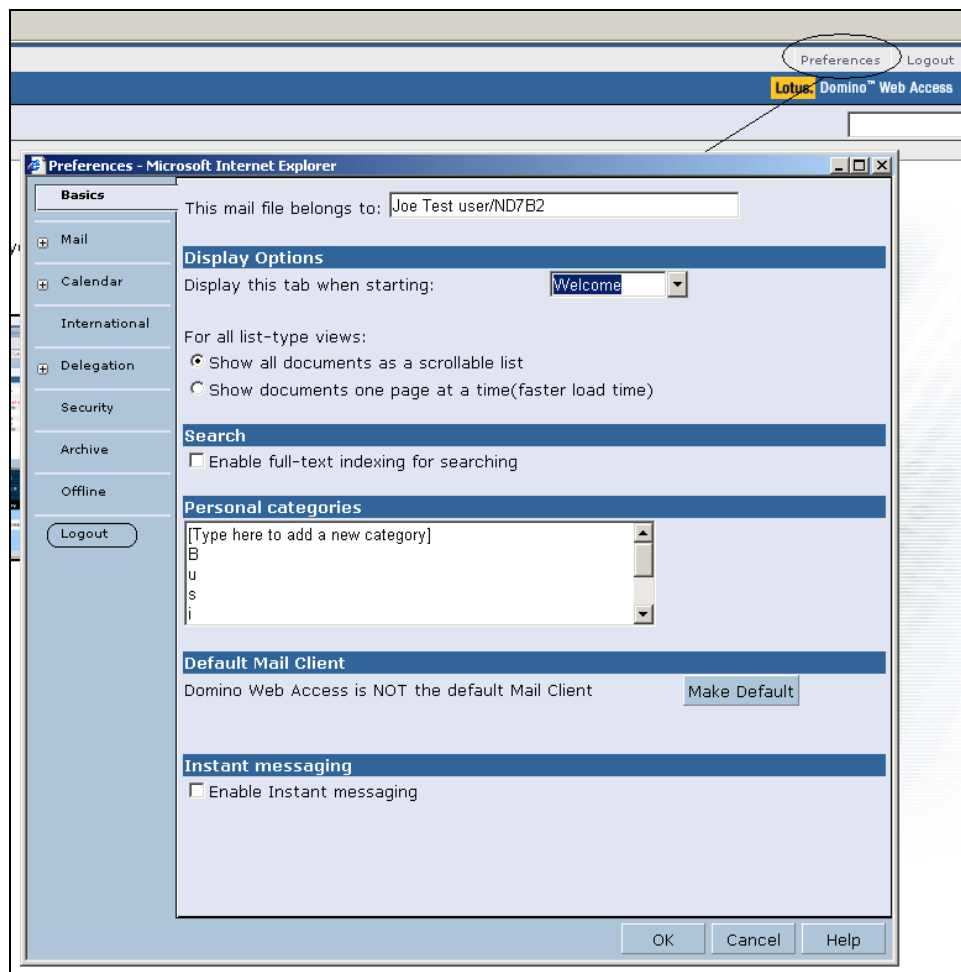
- Allow user to choose alternate name display: This setting allows end users to choose the preferred language for an alternate name. This setting is disabled by default, thus preventing users from using alternate name support.

Browser Cache Management

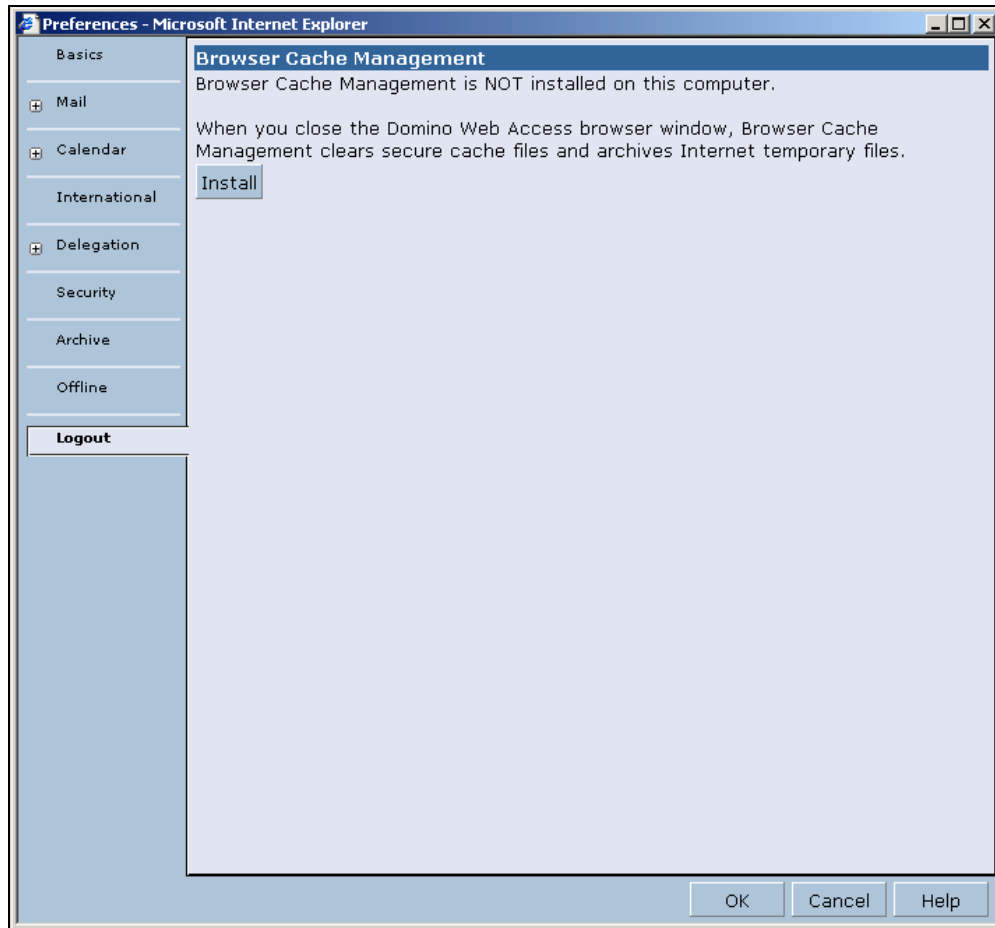
Browser Cache Management (BCM) improves Domino Web Access client security and performance. Browser Cache Management manages the cache processing in Internet Explorer; this process controls the entries that are stored in the browser cache. If

configured correctly, these cache entries can be removed from the client browser when the Domino Web Access session terminates. Domino administrators (via the Web section in a Server Configuration document) can set various levels of cache scrubbing. Domino administrators can either install Browser Cache Management on Domino Web Access clients automatically, or give users the option of installing it. If the automatic feature is enabled, then a Browser Cache Management system confirmation displays when a user loads the Domino Web Access client for the first time. This will prompt the user to close all browser windows for Browser Cache Management to take effect.

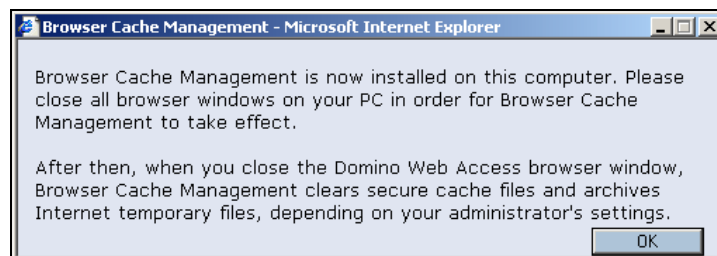
The Domino Administrator can also enable Browser Cache Management but not have it installed automatically. Users can then install and/or uninstall Browser Cache Management using a Domino Web Access preference. End users will be able to enable or disable Browser Cache Management (if allowed) by selecting Preferences and then Logout:



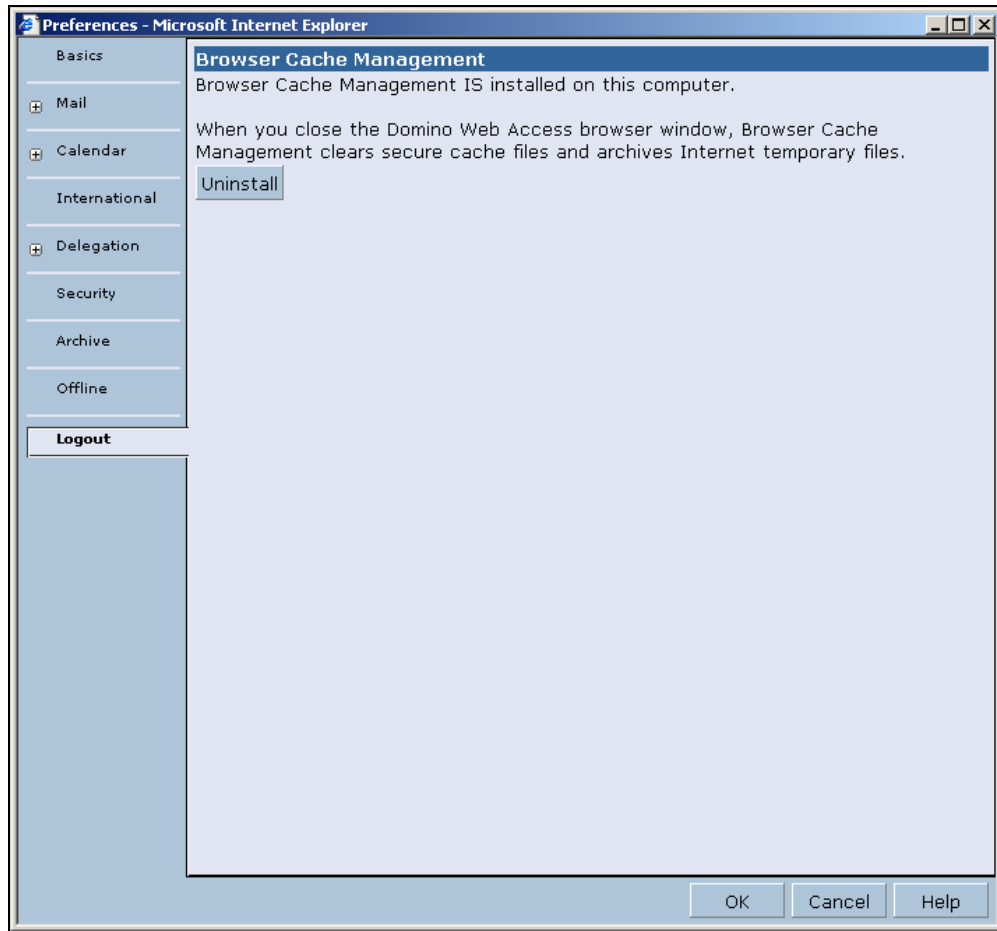
The Browser Cache Management end-user screen appears when the user is allowed to install/uninstall Browser Cache Management:



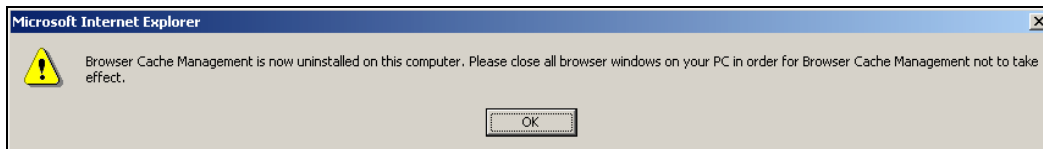
Once the client installs the Browser Cache Management, the following prompt will be displayed.



The administrator will be able to control whether BCM is installed automatically. If the BCM is installed automatically, then the end user will not be able to install or uninstall the BCM. If the administrator provides control of the BCM to the user, then the end user may uninstall the BCM if he or she wants to. The following screenshot shows how the end user can uninstall the BCM:



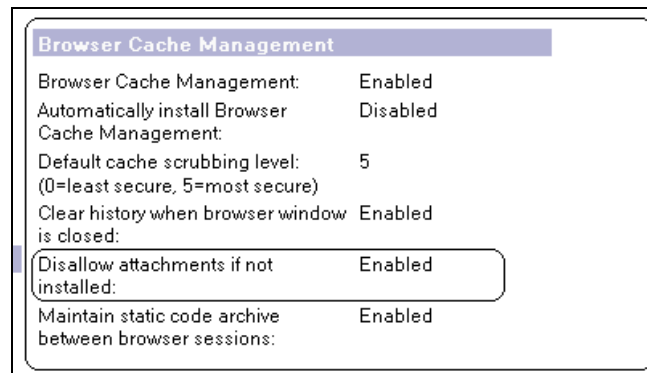
If the Browser Cache Management is uninstalled, you will see the following message:



If you as the administrator have not enabled Browser Cache Management, then this preference is not visible.

As an additional security measure, you can prevent users who have not installed Browser Cache Management from adding or accessing email attachments.

This can also be set via the Disallow attachment if not installed option in the Browser Cache Management section in the Domino Web Access tab of the Server Configuration document:



After the Browser Cache Management feature has been installed on a user's system, the cache cleanup occurs based on the cache scrubbing level set in the server's Configuration Settings document. The user cannot change this. If this has not been installed, then users can manually clear the cache at logout by clearing the history, and selecting one of two logout options:

- **Secure:** This option will delete all entries in the cache except Domino Web Access design elements. Domino Web Access design elements are archived locally when the last instance of Internet Explorer is closed, and then restored back into the browser cache when the browser is opened again.
- **More Secure:** This option will delete all entries in the cache.

Browser Cache Management Settings

The Browser Cache Management section of the Domino Web Access tab in the Server Configuration document includes the following options:

- **Automatically install Browser Cache Management:** If enabled, this setting will automatically install Browser Cache Management the first time a user accesses Domino Web Access. If it is disabled, the user can install Browser Cache Management manually from Preferences. This is Disabled by default.

- **Default cache scrubbing level:** This sets the automatic cache-clearing level for the Domino Web Access server. There are six options:
 - **Option 0:** Deletes the cache, including personal information related to the mail database.
 - **Option 1:** Deletes all URLs that begin with the mail file path.
 - **Option 2:** Deletes all URLs in the cache that originate from the server hostname, except for URLs that contain /i Notes/Forms7.nsf (the current forms file) or /i Notes/Forms6.nsf.
 - **Option 3:** Deletes all URLs in the cache that originate from the server hostname.
 - **Option 4:** Deletes all URLs in the cache except for URLs that contain /i Notes/Forms7.nsf or /i Notes/Forms6.nsf.
 - **Option 5:** Deletes all URLs in the cache.
- **Clear history when browser window is closed:** If enabled, this clears the browser history when the window is closed. This setting prevents unauthorized users from accessing previously displayed pages. This is Disabled by default.
- **Disallow attachments if not installed:** If enabled, this prevents users from adding or accessing attachments in email if Browser Cache Management is not installed. This is Disabled by default. The advantage of this feature is that it will prevent users who have not installed Browser Cache Management from using attachments at an unsecured workstation. (Domino administrators can also use a new NOTES.INI setting to prohibit access to attachments in calendar and scheduling documents, online meetings, and email.)
- **Maintain static code archive between sessions:** This setting (which is enabled by default) will move static Domino Web Access design entries from the cache to a folder on the local machine so that they can be restored to the browser cache when the browser is started again.

Other Domino Web Access Settings

The Other Settings section of the Domino Web Access tab has only one new option, Rooms and Resources. If enabled, this prevents access to the room and resource database when scheduling meetings. By default, this setting is disabled.

Other Settings	
Archiving on server:	Enabled
Full-text indexing:	Enabled
Modification of Internet password:	Enabled
Calendar printing:	Enabled
Domino Web Access ActiveX file attachment utility:	Enabled
Compress HTTP response data	Enabled
Rooms and Resources	Enabled

Another new Notes/Domino 7 option is the ability to support XML services. In Domino 6.x, you must update the NOTES.INI file on your Domino mail server to include the setting HTTPDomWSAppSpace=1. This enables Domino XML services on the Domino server. In Domino 7, you just edit the Server document. To do this, open the Server document and select the Web Engine tab. At the bottom of the document, you'll find the setting XML Services. You can enable or disable this setting (the default is Disabled).

Domino XML Services	
XML Services:	Disabled

Summary

In this chapter, we reviewed Domino Web Access 7, the latest release of the tool that allows you to work with Notes mail from within a web browser. Domino Web Access has been significantly enhanced in release 7, to raise the user experience to be more like the functionality expected while working in the Notes client. Among the many improvements are better security, integration with DOLS and Sametime, personalized stationery, mail threads, S/MIME support, the ability to import a Notes ID, and enhanced configuration options.

10

Programming

Notes/Domino 7 continues to improve developer productivity with a new set of programming enhancements. In this chapter, you will learn how to use the latest programming features to improve your application development environment, and to integrate more closely with server administrator functions, the new IBM Workplace, and DB2. This chapter covers the following topics:

- AutoSave
- Enhanced Java Support
- New formula language commands
- New LotusScript elements

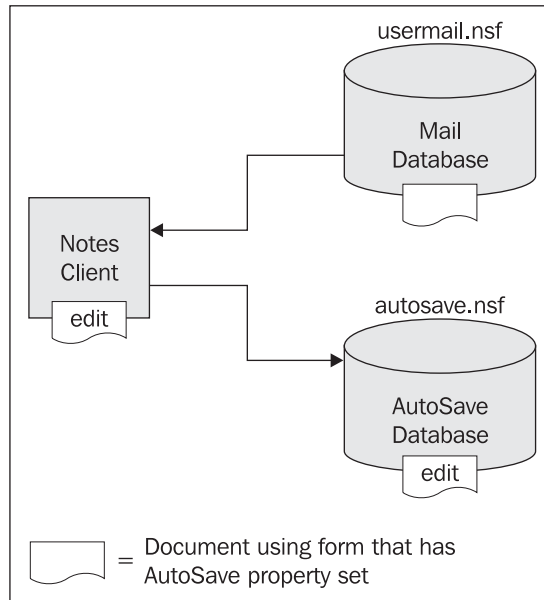
AutoSave

Application designers can create forms that include a new AutoSave feature. When a form specifies the AutoSave feature, documents being edited with that form are saved locally based on a user-specified time. They are then available after a system failure/crash. Users have the option to save documents that use that form to a local database in the event the server they are working on goes down.

The following process describes the flow when AutoSave is enabled:

1. At startup (first time use), Notes creates a database called `autoSave.nsf` with medium encryption.
2. When a user has a document open for editing, and its form is enabled for AutoSave, modifications to the document are periodically saved to the local database.
3. Once a document is saved by the user, it is removed from the database until modified again.

4. If a crash (system or Notes) occurs while the document is being edited, on restart the user is presented with a dialog box to recover any unsaved documents. The user can then continue editing or can discard their modifications.



Designers can enable AutoSave in a number of ways:

- User preference to enable AutoSave: File- Preferences | User Preferences | Startup Options | AutoSave every x minutes checkbox
- New menu to access AutoSave options: File | AutoSave
- NOTES.INI parameters:
 AUTO_SAVE_ENABLE = 1 (feature is on)
 AUTO_SAVE_ENABLE = 0 (feature is off)
 AUTO_SAVE_INTERVAL = 15 (sets AutoSave interval)
- Via Policy | Desktop Setting | Preferences tab.

Recovering Documents Saved with the AutoSave Feature

Users can recover documents when Notes starts up, or at any other time they like. Under some circumstances (after a crash or a power loss, for example) users are prompted with the message You have x unsaved document(s). Do you want to recover these documents now?

If a user selects Yes, the Recover Unsaved Documents dialog box appears. This lists the documents that can be recovered.

From the Recover Unsaved Documents dialog box, users have the following options:

- Recover recovers the selected document.
- Recover All recovers all documents without prompting for each one.
- Remove deletes the selected document from the AutoSave database.
- Remove All removes all documents from the local database.

Alternatively, the user can press No at the recovery prompt, and recover the autosaved documents later by selecting File | Autosave | Recover Autosaved Documents. The Recover Unsaved Documents dialog box appears and users can recover or delete documents as described previously.

After a document has been recovered from the AutoSave database, it is automatically removed from that database. This helps keep the AutoSave database from becoming too big.

Enhanced Java Support

Domino release 7 enhances Java integration by supporting Sun Java 2 Platform, Technology Edition, version 1.4.2, but perhaps more importantly; it also provides support for debugging your Java applications remotely. You can embed Java code in agents, web services, and script libraries. To use the new debug features, you must:

- Enable debugging on your server.
- Connect your preferred debugger (Eclipse or RAD/WSAD, for example).
- Choose to Compile Java code with debugging information on the design element you want to debug.

To enable debugging (in this case, the Eclipse debugger) on your server, start up the Notes client, with Java debugging enabled on the agent or web service you want to debug. Then do the following:

1. Start the debugger, and create a Java project. Then switch to the Java perspective. For example, select File | New | Project, select Java in the Project window; and enter a name for the project. Select Finish, and switch to the Java perspective. (If the project already exists, you can simply open it.)
2. Import the source Java files. You can do this by right-clicking the project folder in the left-hand pane. Select Import; browse to the source files, and then select and import them. Note that source code that is not imported is not available to the debugger. You can see the execution thread and can access variables, but you cannot see the source code and set breakpoints.
3. Return to Notes and start the agent or web service to be debugged.

4. In Eclipse, attach the debugger to the Notes JVM. For example, choose Run | Debug, enter a name for the debug configuration, and select the Connect tab. Then select the project, enter the host name or address of the Notes computer, and enter the Java debug port number on the Notes client. Select Apply if this is the first time you are specifying this, or if you change the configuration. Then select Debug. The host address is 127. 0. 0. 1 if the Notes client and Eclipse are on the same machine.

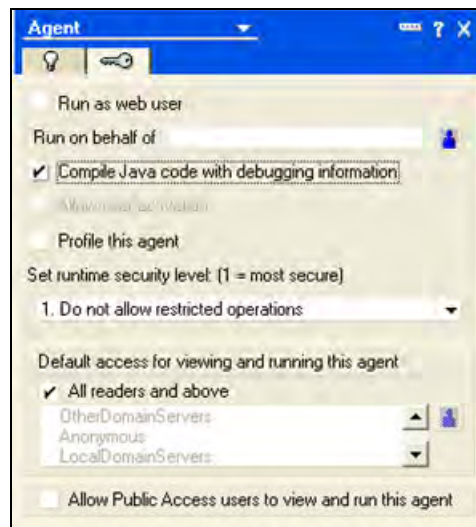
After you attach the debugger, you can see the execution threads for the JVM. An agent's thread looks something like this:

Thread(AgentThread: JavaAgent) (Runni ng)

You can suspend the agent's thread to gain control of it. The usual debugger features now become available.

The Java agent must run long enough for you to attach the debugger to the JVM. You can delay execution at the beginning of the procedure.

You can now allow the debugger to run on the element (an agent, in this example) that you want to debug.



New Formula Language Commands

Domino developers implement business logic through the use of Notes Formula Language. Many of the powerful legacy Notes applications are based entirely on Designer. To support the existing users of the formula language, and the new, enhanced features of the product, Domino Designer 7 introduces several new formula language commands:

- `@AdminECLIsLocked`: Checks the current status of the Administration Execution Control List (ECL) in the name and address book. Use this `@Function` to determine whether the Administration ECL document in the Domino Directory is locked. If the document is locked, then it cannot be edited.
- `@DB2Schema`: Returns the DB2 schema of a Notes database that is DB2 enabled.
- `@IsDB2`: Given a server and filename, indicates if the specified database is DB2 enabled. This Boolean function returns 1 for 'true' and 0 for 'false'.
- `@IsEmbeddedInsideWCT`: Indicates whether any part of the current Notes session is embedded inside IBM Workplace Client Technology. This new `@Function` will most likely only be used in 'hide-when' formulas and will determine whether the current Notes session is being accessed using the IBM Workplace Client. This is also a Boolean function that will return 1 for 'true' and 0 for 'false'.
- `@PolicyIsFieldLocked`: Indicates whether a field is locked by an administration policy and cannot be modified. Domino 7 administrators now have the ability to lock fields, such as client settings, using policy documents. As a developer, you may want to know whether a field is locked by a policy. This function almost certainly would be used in a 'hide-when' formula.
- `@Command([DiscoverFolders])`: Opens a dialog box indicating which folders contain a specified document.

New LotusScript Elements

The LotusScript language has also been enhanced in several key areas. Developers can now access one new Admin function, two new document properties, and multiple new ways to work with XML data in the Domino context, and work within the IBM Workplace client.

Admin Support

`NotesAdministrationProcess.ApproveHostedOrgStorageDeletion` is a new method to continue a previously initiated Administration request that is pending approval.

General Document Support

- `NotesAgent.GetPerformanceDocument` is a new method to return the latest profiling results for an agent.
- `NotesDatabase.GetModifiedDocuments` is a new method to get from a database the documents that have been modified since a specified time.

XML Support

LotusScript in release 7 also adds several new elements to manage the use of XML namespaces. These new elements will assist in the management of unique terminology within specified XML domains.

- NotesDOMNode. NamespaceURI
- NotesDOMDocumentNode. CreateAttributeNodeNS
- NotesDOMDocumentNode. CreateElementNodeNS
- NotesDOMDocumentNode. GetElementsByTagNameNS
- NotesDOMElementNode. GetAttributeNodeNS
- NotesDOMElementNode. GetAttributeNS
- NotesDOMElementNode. GetElementsByTagNameNS
- NotesDOMElementNode. RemoveAttributeNS
- NotesDOMElementNode. SetAttributeNodeNS
- NotesDOMElementNode. SetAttributeNS

The following new properties enhance Domino XML schema management:

- NotesDXLExporter. SchemaLocation is a new property to indicate where an exported schema should be placed.
- NotesDXLExporter. ValidationStyle is a new property to indicate the schema-validation style.

IBM Workplace Client Support

IBM Workplace Client Technology is a user interface that was originally designed to work with IBM Workplace Collaboration Services. It offers a new paradigm for building server-managed clients that support flexible and cost-effective access to data about people, business processes, applications, and content.

IBM Workplace Client Technology can be extended, via a Notes plug-in, to allow access to any standard Notes application, including mail and calendaring. To support this, release 7 has added a new property to determine whether an application is running inside the IBM Workplace Client:

- NotesUIWorkspace. IsEmbeddedInsideWCT

Summary

This chapter explained the latest programming features in Notes/Domino7. These features are designed to improve your application development, and to integrate with server administrator functions. We also discussed new programmatic support for IBM Workplace and DB2, AutoSave, enhanced Java support, and additions to the formula language and LotusScript.

11

Security

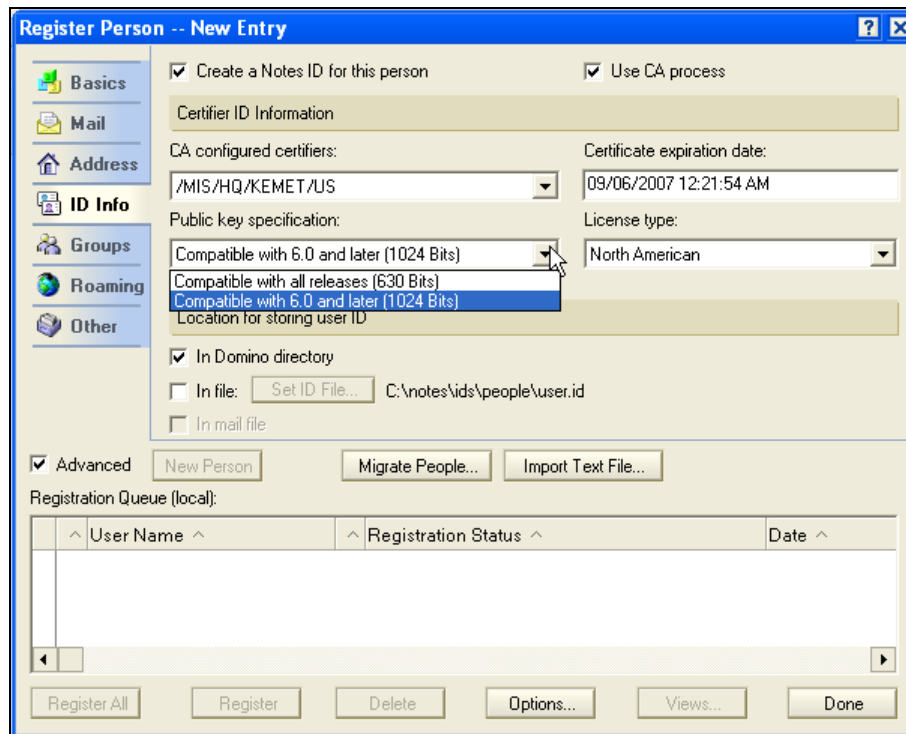
Many security features have been added and improved in Notes and Domino 7. These features include enhanced encryption options, larger Notes keys, Smartcard support, new security APIs, ID recovery enhancements, and new custom password policies. This chapter looks at each of these additions and improvements.

New Encryption Options

First, let's take a look at the new encryption options in Lotus Notes and Domino 7. Encryption for Domino is available first when creating a Notes ID file. Stored in the Notes ID file is the Internet key, used for S/MIME. Support for large Internet keys has been available since release 4. Prior to version 5.0.4, key lengths were restricted for encrypting data, but authentication and signing could have different lengths—you had to choose between a North American key and an International key. Anything over a 512-bit RSA and 56-bit symmetric key was considered 'strong' encryption. Now that the US government has relaxed regulations for export of cryptography, all of the encryption levels have been combined into one global release.

When you use release 5.0.4 or later, the ID encryption is automatically upgraded to strong encryption. Now Notes and Domino 7 bring 1024-bit RSA as well as 128-bit RC2 encryption to the table. The Notes client and Domino server both support 1024-bit RSA and 128-bit symmetric key for S/MIME and SSL. The Notes proprietary protocols support the use of 630-bit and 1024-bit keys for key exchange, and use 64-bit and 128-bit keys for bulk data encryption.

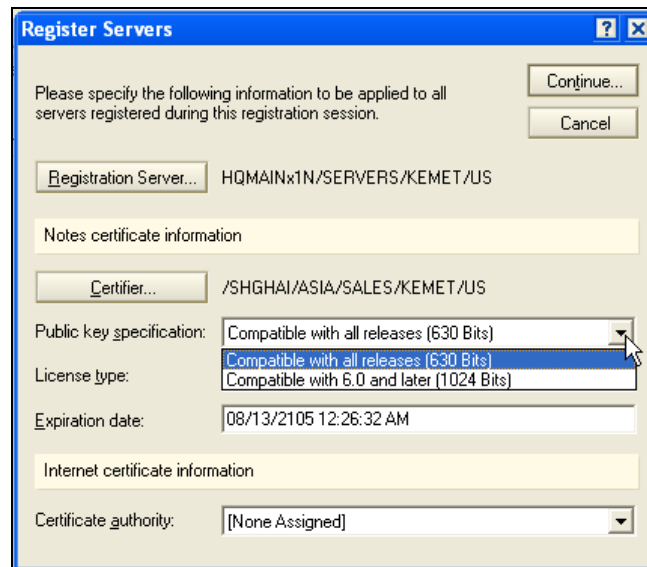
In addition to these new larger keys, Notes/Domino 7 includes several new encryption-related tools. In the Administrator client, there are now options to specify key size during registration. When registering a person, you can specify 630 bits or 1024 bits (more on this later).



The "Register Person -- New Entry" dialog box is shown. It has a left sidebar with tabs: Basics, Mail, Address, ID Info, Groups, Roaming, and Other. The "ID Info" tab is selected. The main area contains the following fields and options:

- ☒ Create a Notes ID for this person
- ☒ Use CA process
- Certifier ID Information**
- CA configured certifiers: /MIS/HQ/KEMET/US
- Certificate expiration date: 09/06/2007 12:21:54 AM
- Public key specification: Compatible with 6.0 and later (1024 Bits) (selected)
- License type: North American
- Location for storing user ID: (empty)
- ☒ In Domino directory
- ☐ In file: Set ID File... C:\notes\ids\people\user.id
- ☐ In mail file
- ☒ Advanced
- Buttons: New Person, Migrate People..., Import Text File...
- Registration Queue (local): (empty table with columns: User Name, Registration Status, Date)
- Buttons at bottom: Register All, Register, Delete, Options..., Views..., Done

For a server, you can specify the same key specifications.



The "Register Servers" dialog box is shown. It has a title bar with a question mark and close button. The main area contains the following fields and options:

- Please specify the following information to be applied to all servers registered during this registration session.
- Buttons: Continue..., Cancel
- Registration Server...: HQMAINx1N/SERVERS/KEMET/US
- Notes certificate information**
- Certifier...: /SHGHAI/ASIA/SALES/KEMET/US
- Public key specification: Compatible with all releases (630 Bits) (selected)
- License type: Compatible with 6.0 and later (1024 Bits)
- Expiration date: 08/13/2105 12:26:32 AM
- Internet certificate information**
- Certificate authority: [None Assigned]

You can also initiate the process of generating new keys for existing users via a policy-settings document. The document is referred to as a security settings document and can be found under the Keys and Certificates tab. You can use this tab to set minimum and maximum allowable key strengths, preferred key strength, maximum allowable age for the key, and earliest allowable key creation date. You can also specify the number of days over which to spread the new key generation for all users.

Security Settings : Global Security	
Basics Password Management Execution Control List Keys and Certificates Comments Administration	
Default Public Key Requirements	
<input type="checkbox"/> Inherit Public Key Requirement Settings from Parent	<input type="checkbox"/> Enforce Public Key Requirement Settings in Children
User Public Key Requirements	
Minimum Allowable Key Strength:	No Minimum ▼
Maximum Allowable Key Strength:	Compatible with Release 6 and later (1024 bits) ▼
Preferred Key Strength:	Compatible with Release 6 and later (1024 bits) ▼
Maximum Allowable Age for Key:	36500 days
Earliest Allowable Key Creation Date:	08/01/1977
Spread new key generation for all users over this many days:	180 days ▼
Maximum number of days the old key should remain valid after the new key has been created:	365 days

You can also set the public key requirements in the server document's Administration tab. Here you can set the minimum and maximum allowable key strength, as well as the maximum age and the earliest allowable key creation date. You can also specify a date before which the server will not automatically generate a new key. The maximum number of days an old key should remain valid after the new key has been created is available as a setting as well.

Basics	Security	Ports...	Server Tasks...	Internet Protocols...	MTAs...	Miscellaneous	Transactional Logging	Shared Mail	DB2	Administration
Administration										
Owner:		Sysadmin ▾								
Administrators:		Sysadmin ▾								
Public Key Requirements										
Minimum Allowable Key Strength:		No Minimum ▾								
Maximum Allowable Key Strength:		Compatible with Release 6 and later (1024 bits) ▾								
Preferred Key Strength:		Compatible with Release 6 and later (1024 bits) ▾								
Maximum Allowable Age for Key:		36500 ▾ days								
Earliest Allowable Key Creation Date:		08/01/77 ▾								
Don't automatically generate a new key before:		03/17/2105 ▾								
Maximum number of days the old key should remain valid after the new key has been created:		365 ▾ days								

Interoperability

With all these new options, you need to consider which versions of which clients and servers work together. Release 5 will fail cleanly when presented with a large key. Notes/Domino 6 can use 1024-bit RSA keys, but cannot generate them. In addition, Notes/Domino 6 can use 128-bit RC4 keys but cannot use 128-bit RC2 keys. Specifically, Notes/Domino 6.0.4/6.5.1 can use 1024-bit RSA keys or 128-bit RC2 keys, but cannot generate either of them. Release 7 can use and generate both 1024-bit RSA and 128-bit RC2 keys. Release 7 also adds latent support for 2048-bit RSA keys.

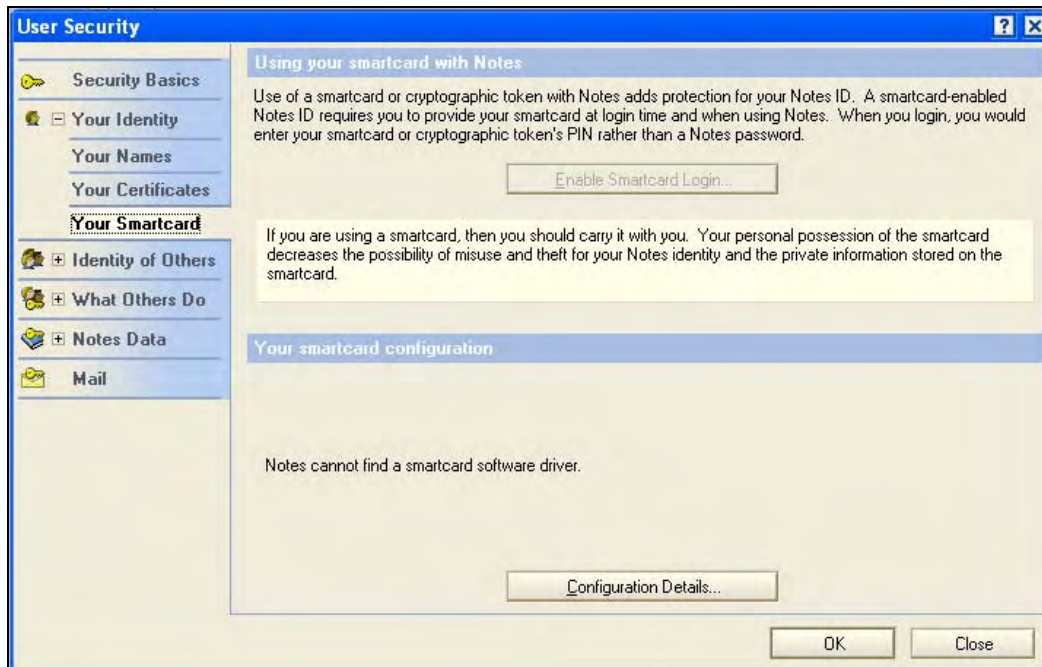
Key Rollover

As mentioned earlier, Notes/Domino 7 allows the administrator to enforce creation of new key pairs via a policy. Both key age and key width can be specified. The release 7 client will automatically generate a new key pair and submit it for certification. You can also control the load on the server by setting a time period for key rollover throughout a domain.

Smartcards

Notes/Domino 7 adds significant support for Smartcards. There are two standards for Smartcards: MS CAPI and PKCS #11. Notes supports PKCS #11. Starting with Notes/Domino 6, many Smartcard features were available. Basically, release 6 could lock an ID with a token object and perform password-equivalent functions. Smartcard support has increased with each point release of Notes/Domino 6. Check the release notes of each version for a complete list of what is available.

Notes/Domino 7 added the ability to lock an ID with an RSA key or token. This is now configurable in the User Security dialog. You can enable Smartcard login and set this lock here. Minimal Smartcard support is required.



To lock an ID with an RSA key wrapped with a symmetric key, you will need the API to configure this. This is the highest level of ID security, and the token must support symmetric encryption (AES, 3DES, or RC2) and key wrapping, in addition to basic RSA cryptographic functionality.

You can now also select a Smartcard slot on the User Security dialog. This is found in the Smartcard Configuration Details screen when you select the Your Smartcard option.



Security APIs

Notes/Domino 7 offer several new security APIs. These are as follows:

- SECKFMOpen, SECKFMClose for opening and closing the ID file
- SECAccessIDFileToDB, SECEXtractIDFileFromDB for storing the ID file
- SECRFreshIDFile for refreshing the ID file
- NSFNoteCopyAndEncryptExt2 for encrypting a note
- NSFNoteDecryptExt2 for decrypting a note
- NSFNoteSignExt3 for signing a note
- NSFNoteInspectSignatureExt2 for verifying a note

Examples and more detailed explanation of these APIs will be available in the Lotus C API toolkit.

ID Recovery Enhancements

Notes/Domino 7 brings a complete solution for allowing ID recovery to be seamless and a smooth experience for the end user.

Configurable Password Length and Recovery Message

First, Notes/Domino 7 adds a configurable password length and recovery message. From the Domino 7 administration client, you can edit the recovery information (in the Configuration tab in the Certification section) and specify the length of the recovery password and customize the message that will be displayed to the end user.

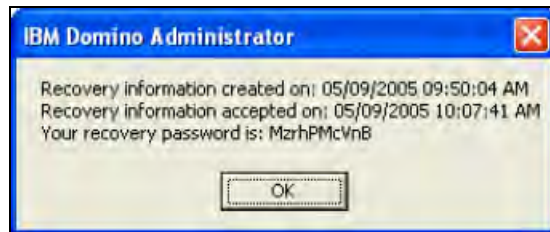
The screenshot shows the 'Edit Master Recovery Authority List' dialog box. It has a blue title bar with a question mark and close button. The main area is light beige. At the top, there's a small icon of a document with a red ribbon and a text box that says: 'Add or change recovery authority names to allow ID and password recovery for IDs created with the certifier /SHGHA/ASIA/SALES/KEMET/US.' Below this is a section titled 'Specify the names of Recovery Authorities'. It contains a text input field, a label 'How many Recovery Authorities do you require?' with a value of '1' and a note '(At least three are recommended)', and a label 'Length of recovery password' with a dropdown menu set to '16'. Below these is a section titled 'Current Recovery Authorities' with a large empty text area and 'Add...' and 'Remove' buttons. Further down is a section titled 'New/modified IDs will be mailed to the address below'. It has two radio buttons: 'I want to use an existing mailbox.' (selected) and 'I want to create a new mailbox.' Below these is an 'Address...' button and the text 'Asia Notes Password Recovery'. At the bottom is a section titled 'Custom Recovery Message :' with a large text area containing 'Call 1-800-Help Desk'. At the very bottom are 'Export...', 'OK', and 'Cancel' buttons.

Suppression of Standard Export Recovery Message

Next, Notes/Domino 7 adds the ability to suppress the standard export recovery message. This is set via a NOTES.INI variable `ID_RECOVERY_SUPPRESS_RECOVERY_MSG=1`. This will remove the standard message sent to a user during export of password-recovery information.

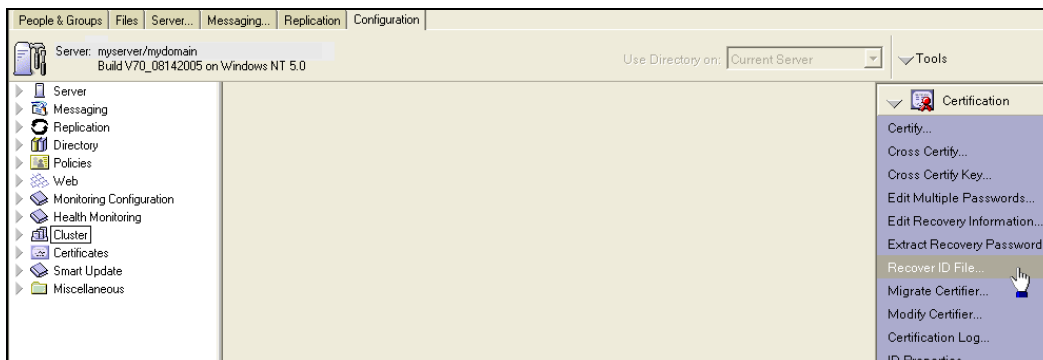
Timestamps

Notes/Domino 7 adds timestamps for extracting a password as well as for the recovery of the ID file password prompt.



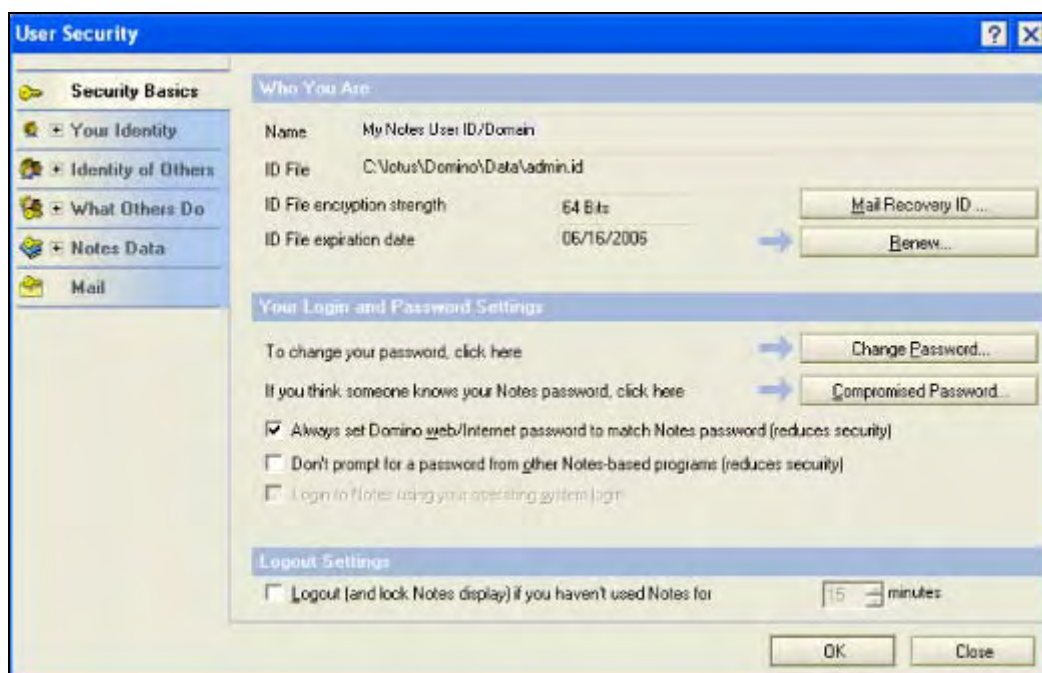
Recover User IDs from the Administration Client

The Domino 7 administration client now has a menu option that lets you recover an ID file. The new menu option is available by choosing Configuration | Tools | Certification. You can click on Recover ID File..., and you'll be prompted with a file dialog box with which you can select the ID file to recover. This allows you to avoid using the Switch Users option in the Notes client to recover a password.



Mail ID Recovery

In the Notes User Security dialog, you now have the option to mail the recovery ID for immediate backup of the ID file.



Expanded Logging

It's now possible to log the following information to the Notes log in Notes/Domino 7: any time an ID file is marked for backup, recovery information timestamps when accepting new recovery information, signature failures when accepting new recovery information, and success or failure of ID file backup.

Obsoleting Recovery Passwords

In Notes/Domino 7, after the recovery password has been used, the next authentication will generate new backup passwords. The current set becomes obsolete and cannot be used.

Password Management

One of the most useful new features for security in Notes and Domino 7 is in the area of password management. An administrator can now specify a custom password policy. The custom password settings can be found in the Security Settings policy settings document.

After you select Yes under Password Management | Password Management Basics, you will see a new tab labeled Custom Password Policy appear.

Security Settings : Global Security		
Basics Password Management Execution Control List Keys and Certificates Comments Administration		
Password Management Basics Custom Password Policy		
Password Management Options	Inherit from parent policy:	Enforce in child policies:
Use Custom Password Policy for Notes Clients	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

The Custom Password Policy tab allows you to change just about everything you can imagine about a password. This includes the minimum number of alphabetic, uppercase, lowercase, numeric, and special characters, among other things.

Security Settings : Global Security		
Basics Password Management Execution Control List Keys and Certificates Comments Administration		
Password Management Basics Custom Password Policy		
Custom Options	Inherit from parent policy:	Enforce in child policies:
Change Password on First Notes Client Use	<input type="checkbox"/> No	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Allow Common Name in Password	<input type="checkbox"/> Yes	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Password Length Minimum	<input type="checkbox"/> characters	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Password Length Maximum	<input type="checkbox"/> characters	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Password Quality Minimum	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of Alphabetic Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of UpperCase Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of LowerCase Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of Numeric Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of Special Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of Non-LowerCase Characters Required	<input type="checkbox"/> characters of <input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Maximum Number of Repeated Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Minimum Number of Unique Characters Required	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Password May Not Begin With	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce
Password May Not End With	<input type="checkbox"/>	<input type="checkbox"/> Inherit <input type="checkbox"/> Enforce

Summary

We have discussed several of the major new security-related features that can be found in Notes/Domino 7. You can learn more about these features by referring to the Notes/Domino release notes, online help, and product documentation (which you can download from the developerWorks: Lotus website at <http://www.lotus.com/idd/ocweb>). Be sure to explore the new encryption options, larger Notes keys, Smartcard support, new security APIs, ID recovery enhancements, and the new custom password policies.

12

Upgrading to Domino 7

After you have decided to upgrade to Domino 7, you need to start building an upgrade plan. Most companies are not able to upgrade all users and servers at once. There are several areas that you need to consider before you upgrade; this chapter explains these areas.

This chapter is divided into two main sections. In the first, we look at the Notes/Domino upgrade process in general, discussing concepts and steps that should be considered whenever you upgrade to any major release of Notes/Domino. In the concluding section, we look at upgrade issues that are specific to Notes/Domino 7.

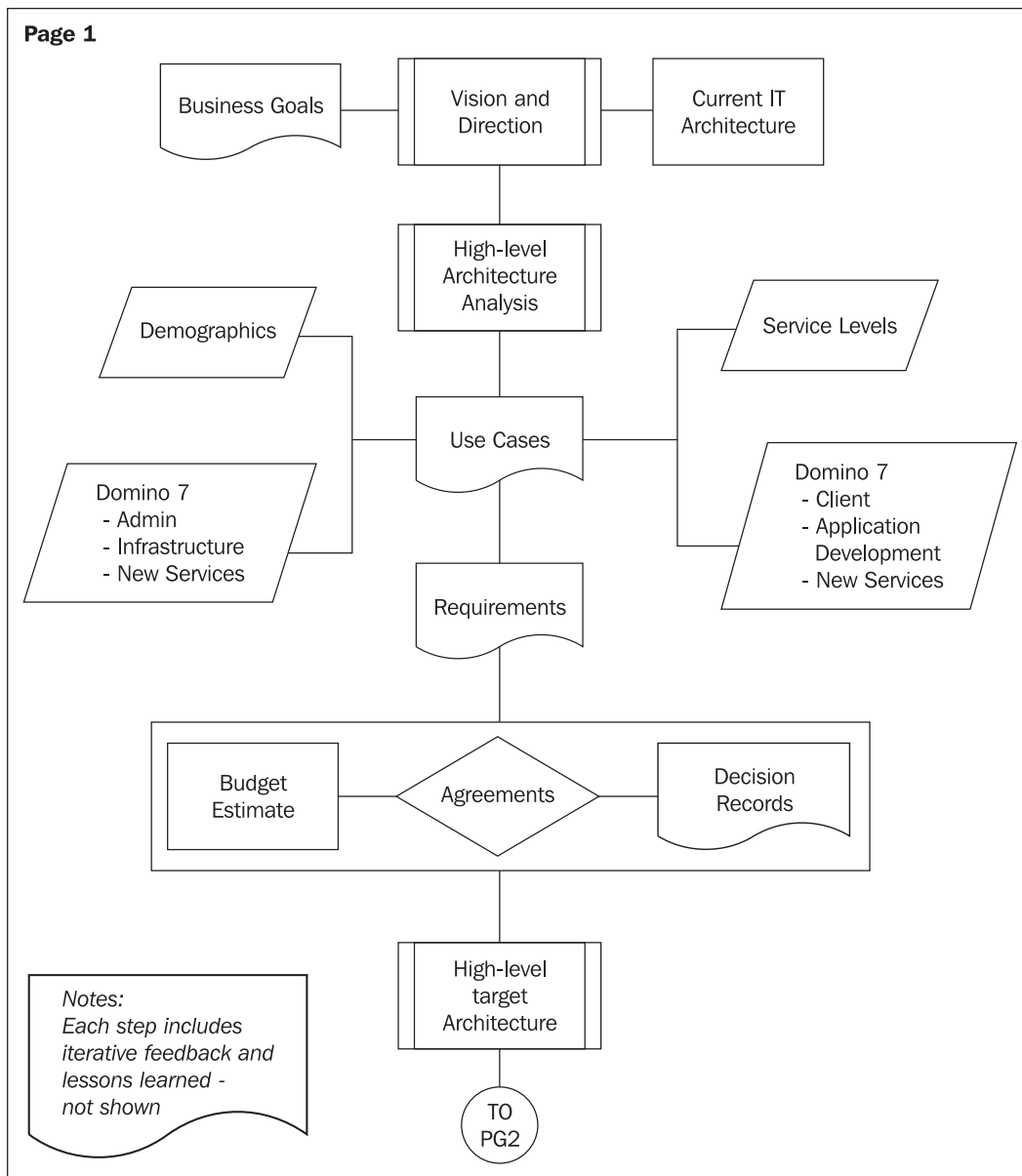
Use Cases

The upgrade process all starts with a technique known as an architectural use case. A use case, in our context, is a statement and description of a system/service that define the use and behavior of an environment. A basic use case should include the following elements:

- A sequence of actions
- Description of requirements
- Goals to help target requirements
- Identification of 'actors' (the people using the system: users, administrators, operators, and so on)
- Identification of associations between use cases and actors

The flowchart overleaf shows each of the basic steps that you will use to upgrade your architecture to Domino 7.

Page 1



Let's review the major steps involved:

Vision and direction: This is where you define your goals for the upgrade. These goals can include your business needs, a basic identification of your current IT architecture, and some rough timelines for the upgrade. This vision charter may read something like this:

The Company will upgrade its ND6 architecture to Domino 7 in eight months, taking advantage of new Domino 7 features, and will also consolidate several servers during the upgrade.

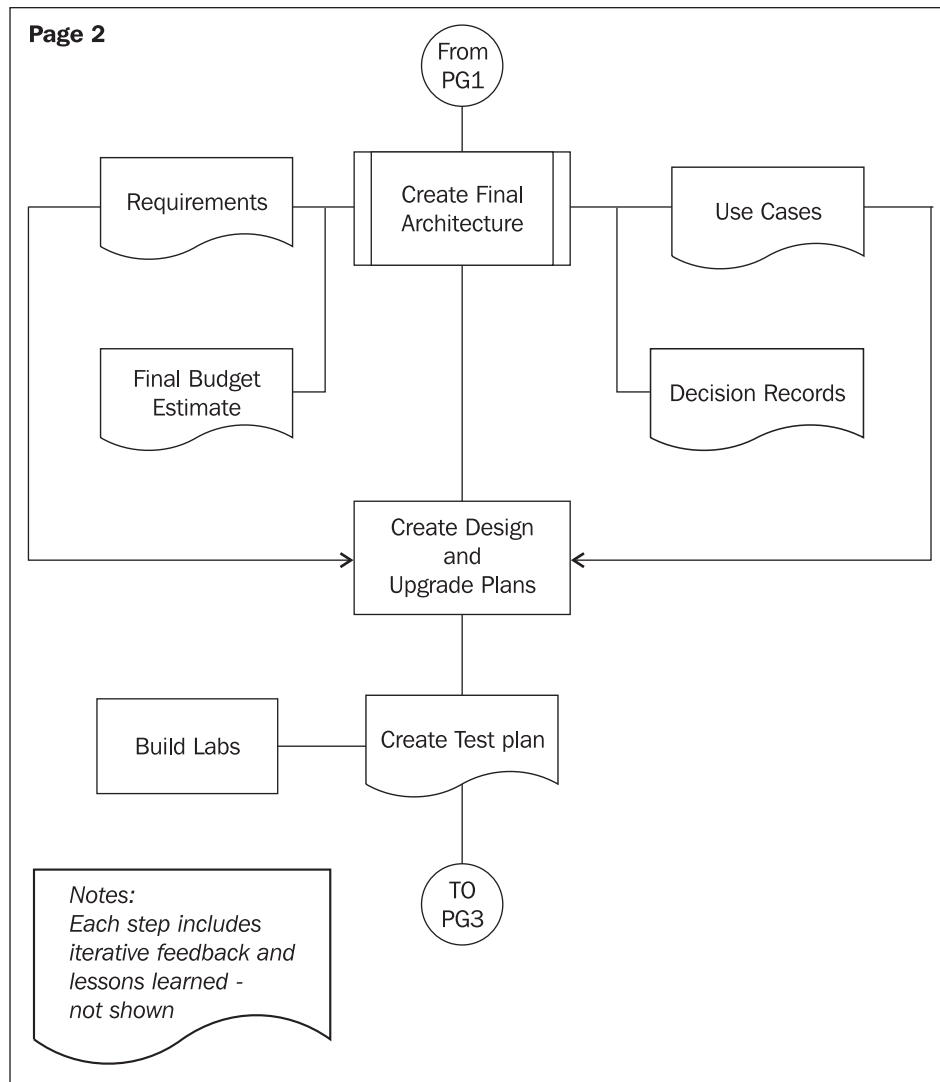
High-level architecture analysis: Before you upgrade, make sure you know what you have. Experience tells us that you cannot identify 100% of everything in your environment. A good review is prudent to keep surprises to a minimum. Take the time to obtain a list of applications, email applications, custom applications, backup systems, virus scanners, and web-based services and appliances. Build an inventory of all things that 'touch' Domino. This will help you identify any items that may be impacted on by the upgrade.

Use cases: These documents will help you build a set of requirements. A sample use case is attached at the end of this chapter. In each use case, you should also identify various states of the upgrade. Examples include upgrading the server, but only enabling the new mail policy feature once all of the clients and server have been upgraded. A use case can include:

- Client upgrade
- Server upgrade
- Communications and transformation management
- Application upgrade
- Custom API upgrades
- Administration tool upgrade
- SMTP service upgrade
- Security impacts
- Directory impacts
- Process upgrade
- Help desk

Requirements: When all the use cases have been created and agreed on, you can summarize the use cases into a total list of requirements. These use cases and requirements can be used to determine upgrade steps, use of new features, systemic impacts, budgets, and timelines. These requirements will be used to create the 'draft' target architecture.

Agreements: This is where you will build out your budgets, build out decisions records, and obtain agreements from all concerned parties in your organization. After all of the agreements have been reviewed, signed, and approved, then your target architecture can be finalized.

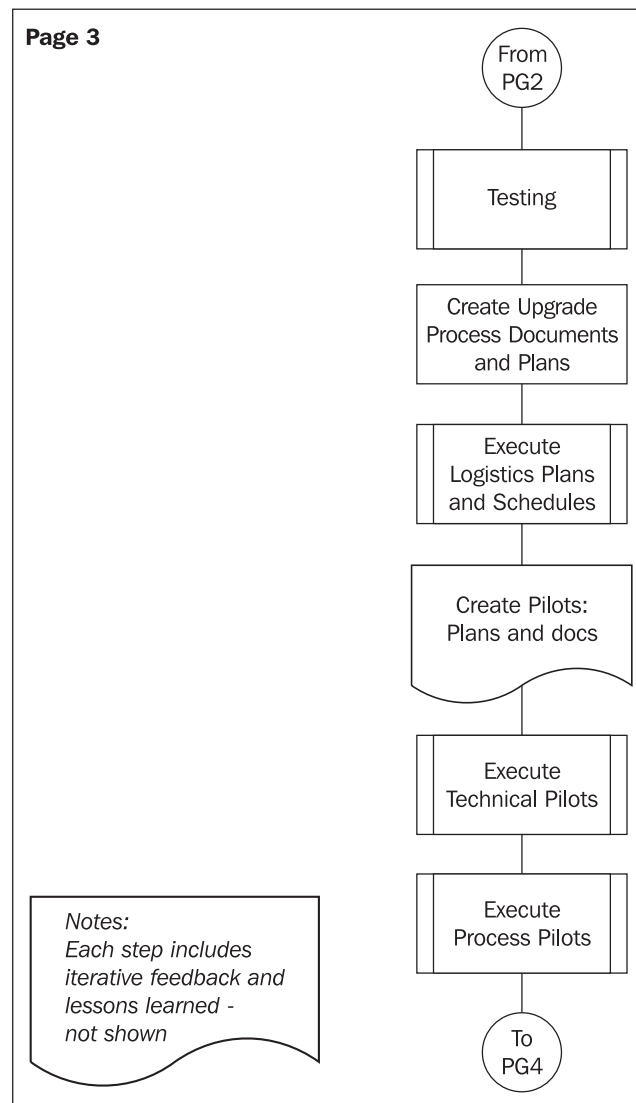


Final target architecture: Note that this is a 'final' architecture. In most organizations, there will normally be a phased approach. It can take several iterations to get to this final architecture. One example would be new Domino 7 programming functions. In order to take advantage of these, you would need to have both servers and clients upgraded before the new functions are enabled.

Create the design and upgrade plans: This step is where you start the process of detailing the upgrade process. Also, you begin documenting the process that will be used as a step-by-step upgrade guide.

Create test plan: Remember the identification of new features and requirements? This is where you create a test plan to test each of the upgrade elements:

- Server
- Clients
- Applications
- Custom tools
- Other stuff



Testing: The previous flowchart shows the testing and pilot process. Each part of the upgrade should be tested before you actually put any new technology into a production environment. Most companies execute what are known as **unit** or **component tests**. These tests involve the basic components of the new technology. In our case, you would test the Notes 7 client on a sampling of your current PCs. This particular test verifies that Notes 7 will run on your existing hardware, and will not impact any other applications and/or the PC environment. As testing progresses, you will start to include each other element into the environment; for example:

- Notes 7 on the network
- Notes 7 on applications
- Notes 7 via a Domino 6 or 7 server

The goal is to test Notes/Domino in a holistic test environment that replicates various parts of your production environment.

One very important step is to contact vendors of any third-party tools and utilities that might have been used. The upgrade process will make changes to the directory, and then to each server. Be sure to contact every vendor and determine whether Domino 7 (or any new release of Notes/Domino) is supported by that vendor. Double-check to verify that APIs have been recompiled (as needed) by the vendor, and that the new directory is supported. Then do your own testing, to make sure everything is working as advertised by the vendor.

Create upgrade process document and plans: Create all of the upgrade steps, procedures, schedules, training, and frequently-asked-questions documents. Some of these documents will be the actual upgrade steps and checklists. If you are upgrading a large number of servers and users, then you can use a tracking database and/or spreadsheet. The results of the testing will be manifest in the upgrade process. Also, communications plans should be created at this time.

Execute logistics plans and schedules: This is the where you order any equipment, hire any additional staff, and start the overall upgrade process. Included in the scheduling process will be the execution of the pilots (see the following step).

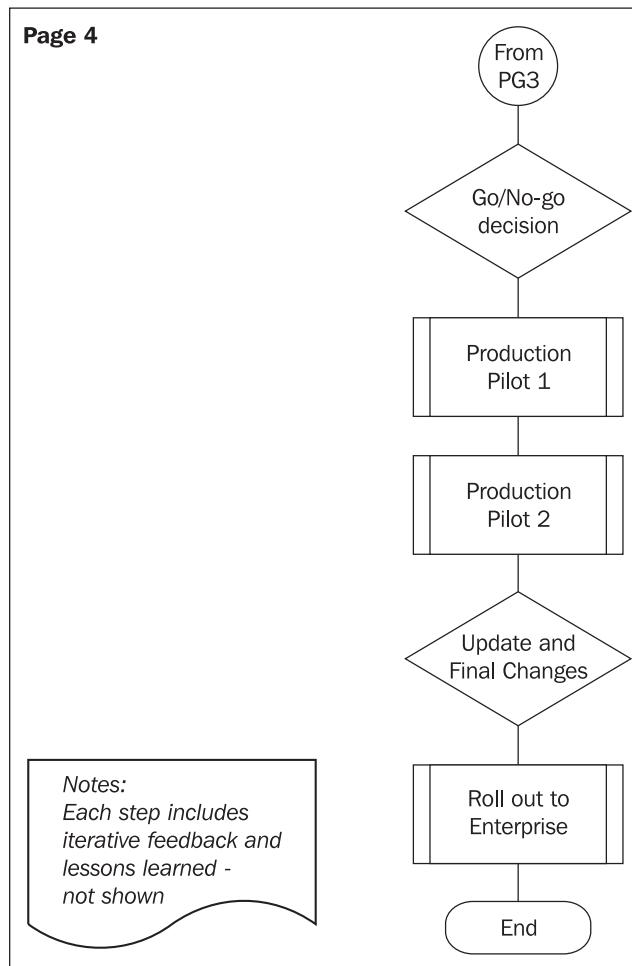
Create the pilots: Next, create and document each pilot needed. You will need two pilot types: non-production pilots (technical pilots, process pilots), and production pilots (shown on page 4 of the diagram).

As we mentioned earlier, you should test as much as possible in a test environment before executing a production rollout. The non-production pilots are an opportunity to test each step of a process. These should include:

- Upgrade steps
- Training and education
- Communications
- Help desk testing and FAQ
- Executive help staff

One important step of the pilots is gain 'lessons learned'. Each pilot is an opportunity to modify upgrade steps and processes.

Non-production pilots are normally separated into two types, technical pilots and process pilots. Technical pilots verify that each holistic step of the upgrade works correctly. Process pilots verify that the actual checklists and documents are correct.



A **Go/No-go decision** is made before the production pilots are executed. This decision will be based on the results of the testing of technical and process pilots. If all have been successful, then the next step will be the production pilots.

Once all of the pilots had been completed, then you need to start the actual upgrade process. Use a set of 'friendly' users (never use executives!) for the first pilot. The previous diagram showed two production pilots. In reality, you will execute as many as needed. Each pilot will provide lessons learned to be used in the next pilot.

Update and final changes: After all pilots have been executed, and you have an opportunity to update the processes and make any final changes to the overall upgrade process, you are ready to roll out the upgrade to your enterprise.

Notes/Domino 7 Upgrade

So far we have discussed a generic upgrade process. At this point in the upgrade process you have completed the pilots and testing. Next are the actual upgrade steps for Notes/Domino 7.

Review the Current Infrastructure

Before you upgrade, you will need to identify the components and systems that will be impacted on by this upgrade.

- **Servers:** Identify any existing issues, such as crashes, sick servers, slow access, and so on. Your servers should be tested before you process the upgrade. Be sure to set up similar servers in a test environment, and use Server.Load to test the performance capabilities of your servers. Also, make sure that your servers are not sick; you should *not* upgrade a server that is crashing or is having hardware issues. Fix issues and problems before you upgrade.
- **Monitoring systems** (Tivoli, BMC, and so on): There are many new monitoring features with Domino 7. Be sure that your current monitoring systems work with Domino 7, and that there are no conflicts with any new features.
- **Directory architecture** (directory analysis, directory customization): This is a big step. Analyze your directory, and check whether there is any customization. Determine whether any custom design features (views, forms, and so on) need to be moved into a new directory. In some cases, you may find these customizations are no longer needed in Domino 7.

- **Clients:** Test your clients and make sure that your current hardware and software configuring will support Notes 7.
- **PDA and/or other wireless systems.**
- **AdminP status:** This is a great opportunity to make sure that admin4.nsf is replicating to all servers, and that all AdminP ACL database assignments are correct.
- **Application analysis:** This includes any issues with applications being upgraded, custom templates, and API analysis. Be sure to test your applications with Domino 7. In general, upgrading to Domino 7 should not result in any issues to existing applications, but it's always a good idea to test with any upgrade. Make sure that your custom APIs still work as needed with Domino 7. In some cases, you may need to recompile some of these APIs, and in other cases, you may no longer need the APIs.
- **Custom templates:** Check for customization to system templates. Compare this customization to any new features in Domino 7, and determine whether you need to move this customization into the templates and applications.
- **Messaging architecture,** including NRPC services, SMTP services, messaging tracking, enterprise-wide communications (mass mail, corporate communication), and co-existence with other messaging systems and other tools: NRPC rarely causes problems during or after upgrades, but it's never a bad idea to test this anyway. Make sure that NRPC Notes Name Networks, a.k.a. NNN or Domino Named Networks (DNN), work as before the upgrade. Test each SMTP Services feature that is enabled. Test each Domino message tracking feature you have enabled in your current environment. A wide variety of mass-mailing tools and other customization may be installed in your environment. Be sure to test each of these tools. Large enterprise organizations can have several varieties of mail systems and servers; test any custom interfaces, software, and SMTP connectivity.
- **Other services and servers:** There are a large number of Lotus/IBM products. All of these need to be tested. Examples include Quickplace, Sametime, LEI, SMTP gateways, virus scanners, backup services, and provisioning systems. Ensure that these products (and the versions you have installed) are supported with Domino/Notes 7. A useful tool for this is the following table from IBM/Lotus TechNote #1163573:

Product Name	Dom.Doc 3.5, 3.1	Doc Mgr 6.5.1	Doc Mgr 7.0	ST 3.1	IM & WC 6.5.1	ST 7.0
Domino 5.0.12	Supported	Supported	Unsupported for Server run on	Unsupported for Server run on	Unsupported for Server run on	Unsupported for Server run on
Domino 5.0.13	Supported	Supported	Unsupported for Server run on	Unsupported for Server run on	Unsupported for Server run on	Unsupported for Server run on
Domino 6.0.3	Supported	Supported	Supported	Supported	Supported	Unsupported for Server run on
Domino 6.5.x	Unsupported	Supported	Supported	Supported during upgrade only	Supported	Unsupported for Server run on
Notes 6.5.x	Supported	Supported	Supported	Supported	Supported	Supported
Domino 7.0	Unsupported	Supported	Supported	Unsupported for Server run on	Supported during upgrade only	Supported
Notes 7.0	Unsupported	Supported	Supported		Supported	Supported

Product Name	QP 3.0.1	TW 6.5.1	QP 7.0	WF 3.0.1	WF 6.5.1	WF 7.0
Domino 5.0.12	Supported	Unsupported for Server run on	Unsupported for Server run on	Supported	Supported	Unsupported
Domino 5.0.13	Unsupported for Server run on	Unsupported for Server run on	Unsupported for Server run on	Supported	Supported	Unsupported
Domino 6.0.3	Unsupported for Server run on	Unsupported for Server run on	Unsupported for Server run on	Supported	Supported	Unsupported
Domino 6.5.x	Unsupported for Server run on	Supported	Unsupported for Server run on	Unsupported	Supported	Supported
Notes 6.5.x	not applicable	not applicable	not applicable	Supported	Supported	Supported
Domino 7.0	Unsupported for Server run on	Unsupported for Server run on	Supported	Unsupported	Supported	Supported
Notes 7.0	not applicable	not applicable	not applicable	Unsupported	Supported	Supported

The Upgrade Process

After you have diligently checked your infrastructure, it is time to start your upgrade. The following steps show the basic upgrade path. This path can vary, based on your research and the use cases you created.

Upgrade the Domino Administrator clients: Upgrade all of your Domino Administrator clients. Verify that all features and functions run in the current environment before you upgrade your first server.

Upgrade the Domino directory: This step can be executed before you upgrade your first server. Remember the use case? Use that to drive the upgrade of the directory, making any customizations and changes. Be sure to work with IBM/Lotus support to make sure that the directory is backward-compatible with your current directory. (You should have done this in the testing phase of the upgrade.)

Upgrade the administration server: This is a very important server. AdminP requires that you assigned an administration server to the Domino directory (names.nsf).

The AdminP server task runs on all Domino servers. This task loads when the Domino server is first started, and is controlled through the NOTES.INI variable ServerTasks. The AdminP server task wakes up on periodic time intervals (specified in the Administration Process section of the Server document), and executes commands waiting in the Administration Request database. Each command placed in the Administration Request database has an assigned proxy action. These proxy actions are essentially the Opcode that runs the Administration Process. Each command placed in the Administration Request database is represented by a document. Each document has a number of fields, including one called Proxy Action. After each action has completed on a server, a response document is created to indicate the status of that request.

Carefully evaluate your administration server. Due to the new complexities of Domino 7 and some new proxy actions, you may need to have a dedicated administration server. AdminP can generate a large number of proxy actions as your architecture grows.

Upgrade utility servers: This step can be different with each customer. In some cases, the hub server can be upgraded first, followed by the utility servers. Utility servers are defined as SMTP, support, tools, and other servers. In some cases, vendors may not be ready with their updates to support a new release of Domino.

Upgrade hub servers: Upgrade each server, and then monitor the 'normal' operations between each upgrade. Verify that replication is still working, agents are still executing, and that mail is still routing.

Upgrade spoke/messaging servers: After the hub servers have been completed, upgrade your spoke and messaging servers.

Upgrade specialized servers: In some cases, these may be some of the first servers you upgrade. One example would be specialized backup software. Once again, you need to contact your vendor before you upgrade your first server and/or upgrade the directory. The issue is backward compatibility. Verify with each vendor that the tools or utilities will work with each release.

Application servers: Upgrade the application servers, but make little or no change to the applications. One important step is to test the applications before you upgrade. There are several tools listed in the reference section of this book, to help you.

Upgrade Notes clients: Finally, you are at the point where you can upgrade the Notes clients. Smart Upgrade can be used if you have Notes/Domino 6 installed. If not, you can use a MSI/MST-type install process to roll out the code.

New Domino 7 features: When all servers and clients have been upgraded, you can implement the new Domino 7 features. Each feature should be tested, and in some cases you may need to build an architecture/design for each feature. One new feature that you should consider is mail policies. This is a new policy that can be enabled after you have upgraded both servers and clients.

Applications: When your architecture is pure Domino/Notes 7, you can start to implement new Domino 7 features into your applications. Use the same testing methodology as listed earlier.

Use Case: Domino Server Upgrade

Use case	Domino Server Upgrade
Subject area	This use case identifies the basic steps needed to upgrade the messaging servers from Notes/Domino 6.x (or 5.x) to Domino 7.
Business event	The upgrade will provide new TCO and management features to your company.
Actor(s)	Architecture team End user ISSL Administration team Operations

Use case overview	<p>This use case deals with the architecture needed to upgrade the servers to Domino 7.</p> <ul style="list-style-type: none"> • Server upgrade steps • Administration impact • End-user impacts
Preconditions	<p>Get approval from various team members on all decision documents.</p> <ul style="list-style-type: none"> • Agreement for the upgrade process • Operations support • Architecture team support • Management support
Use case associations	<p>Use cases:</p> <ul style="list-style-type: none"> • Client upgrade • Communications and Transformation Mgt • Application upgrade • Administration tool upgrade • SMTP service upgrade • Security impacts • Directory impacts • Process upgrade • Help Desk
Business rules	<p>The goal of this upgrade is zero-impact to the end-user community and to overall service levels.</p> <p>Upgrade the Domino messaging servers to Domino 7.</p>
Use case notes	<p>Reference to the LotusSphere upgrades presentation.</p>
Information Sources for use case	<p>Workshops, meetings, data from IBM, and architecture team.</p>

Summary

In many ways, the concepts we have discussed in this chapter form the 'heart' of this entire book. We reviewed the process involved in developing an upgrade plan, an essential step you should always take before embarking upon the actual Notes/Domino 7 upgrade. We began with a look at the Notes/Domino upgrade process in general, discussing concepts and steps that should be considered whenever you upgrade to any major release of Notes/Domino. This included detailed examples of how to develop use cases. We concluded the chapter with a discussion of upgrade issues specific to Notes/Domino 7.

13

Domino and the Web

In this chapter, you will learn how to integrate Lotus Domino and IBM WebSphere Portal, and how to take advantage of WebSphere Portal to present your Domino data and applications on the Internet, on your corporate intranet, or on an extranet. This chapter covers the following topics:

- An introduction to IBM WebSphere Portal
- Advantages of integrating Lotus Domino and WebSphere Portal
- Server integration
- Application integration
- IBM Workplace Managed Client and the Notes Application plug-in

Integrating Lotus Domino and WebSphere Portal gives you one more way to present your Domino applications and data on the Internet or intranet. By integrating these two systems, you enable collaboration in WebSphere Portal, bringing such features as Domino messaging into a portal environment, and you make your Domino applications and data available to portal users, who may use almost any web browser to access Domino data. WebSphere Portal, based on J2EE, provides scalability for your Domino applications, so you can reach even more users without the Notes client.

IBM WebSphere Portal for Beginners

For those unfamiliar with WebSphere Portal, let's review some basics. WebSphere Portal lets you build custom portals for your organization's users, for your customers, for your business partners, or for anyone else. A portal is similar to a desktop. It presents users with a unified workspace in which they can access data and applications that reside on the Internet, on a corporate intranet, or on a company's network. No portal is complete without portlets. **Portlets** are portal applications that display your data and other applications, such as email. Each portlet has a title bar and Minimize, Maximize, Edit, and

Help buttons similar to a desktop application. Portlets are included on a portal page. If you have more than one page, their collection is known as a place. You can build places with different portlets for different users.

WebSphere Portal is available in a number of different flavors that support many of the operating systems supported by Lotus Domino, including iSeries. WebSphere Portal for Multiplatforms has two editions:

- **Portal Enable** provides document management for creating, editing, and storing rich-text files, spreadsheets, and presentations; personalization; and workflow functionality for review and approval of content.
- **Portal Extend** offers the Collaboration Center portlets and extended search functionality that allows you to search even your Domino applications.

WebSphere **Portal Express** is a simpler version of WebSphere Portal for Multiplatforms, which is easier to install. It comes with WebSphere Application Server, on which all WebSphere Portal offerings run. It also provides document management for creating, editing, sharing, and storing documents; collaborative portlets for email, calendar, and so on; and the Portal toolkit for portlet creation. A plus offering of Express includes more collaborative features, such as instant messaging, document libraries, group calendar, and so on.

You can build portals for your mobile devices with WebSphere Everyplace Mobile Portal. Then there is WebSphere Commerce Portal for sales, marketing, customer service, and so on, which combines both WebSphere Commerce and WebSphere Portal.

Advantages of Lotus Domino and WebSphere Portal Integration

WebSphere Portal offers several advantages to Lotus Notes users. For starters, users can open more than one Domino application at a time in a portal and can work with *all* open applications at the same time. In the Notes client, you can open more than one application, but you can work with *only one* application at a time. Domino applications and portlets can share a one-to-one relationship (one Domino application per portlet), or they can share a one-to-many relationship (one Domino application to many portlets). This enables you to present different parts of the same application—for instance, different forms and views—to different users.

Another advantage of WebSphere Portal is that it allows users to personalize their workspaces by arranging portlets to suit their needs. Users can drag and drop portlets anywhere on their workspaces. They can minimize unused portlets to save on-screen real estate, or maximize portlets to fill their workspaces. The Edit button lets users select portlet settings, which may be unique to the portlet application or data it displays. With the proper permissions, users can also choose which portlets to include on their

workspaces. This feature, enabled by the portal administrator, allows users to personalize their workspaces with the applications that they use most often or the data that they access most frequently.

Administrators can also customize workspaces for different users, and can also add themes or skins to the portal for a unique look and feel. Workplaces may contain applications and data for specific users or groups based on role or job function. For instance, your company's administrative assistants need access to email, calendar, instant-messaging, and word-processing applications, while your company's human resource representatives need access to employee data, the corporate directory, email, and web conferencing. You can customize workspaces to provide these two different sets of users with the right data and applications needed for their jobs. This doesn't mean, of course, that these users don't need access to other applications or data, just that you can take the guesswork out of choosing which portlets each group needs by customizing their workspaces. By enabling them to add and remove portlets, you let them personalize their workspaces even further.

Workspace customization increases productivity by displaying the applications and data that each of your users needs to get his or her job done, and by eliminating anything unnecessary from cluttering the workspace. Beyond personalization and customization, there is the ability for users to access their workspaces from anywhere at anytime. Users only need a web browser to access WebSphere Portal. Before you purchase a Lotus Notes license for every user in your organization, ask which ones need a rich client to access your Domino applications and data, and which ones can use WebSphere Portal. If you think that your users must be connected to the Internet, intranet, or company network to use WebSphere Portal, later in this chapter, we will introduce you to the Notes Application plug-in available with Lotus Notes 7. This plug-in works with the IBM Workplace Managed Client, a rich client that you can provision from IBM Workplace Collaboration Services—a WebSphere Portal application—and that users can use to access applications and data off-line.

In addition, when you integrate the two systems, you can benefit from features such as single sign-on, a single, shared LDAP directory between Lotus Domino and WebSphere Portal, and separation of content from presentation.

Lotus Domino and WebSphere Portal

Lotus Domino serves as both a data repository, storing content created in a portlet, *and* a data source, serving content to a portlet. To use Lotus Domino as a repository, you must use Domino LDAP, which looks up specific user values and attributes, for example, for email. Later in this chapter, we describe how to configure Domino LDAP for WebSphere Portal. To use Lotus Domino as a data source, you must enable the HTTP,

Domino IIOP (DIIOP), and LDAP tasks. The HTTP task lets Domino access Domino data through Domino XML or DXL. The DIIOP task pulls in data from Lotus Domino to populate certain lists. Later in this chapter, we describe how to enable both the HTTP and DIIOP tasks.

Server Integration

Integration has two parts: server integration and application/portlet integration. Here are a couple of ways in which you can integrate the Lotus Domino server and WebSphere Portal:

- Install Lotus Domino and WebSphere Portal on the same machine. All Domino applications that you want to make available in the portal must reside on this machine. If you use WebSphere Portal Express, then this is the typical setup. Accessing the applications and data locally is faster than accessing them remotely, but you sacrifice scalability with this configuration. For hardware requirements and performance aspects, see Chapter 7.
- Install Lotus Domino and WebSphere Portal on separate machines. In this configuration, WebSphere Portal can either access Domino applications and data from one Domino server or from more than one Domino server. You can dedicate a server or even a Domino cluster to this configuration or use more than one server in a non-clustered environment for load balancing and failover. Remote access configurations require either HTTP or DIIOP; performance may be an issue, so adequate bandwidth is required.

One of the features that you should consider implementing is single sign-on. This allows your users to access a Domino application through a portlet without having to sign in twice: once to WebSphere Portal to access the portlets and again into Lotus Domino to access the application. Single sign-on is preferred for Domino applications that do not have anonymous web access. Lotus Domino can implement single sign-on in one of two ways:

- If WebSphere Portal and Lotus Domino share a common LDAP directory, then use LTPA token authentication. This type of authentication is temporary; it lasts for the duration of the session and expires when the user closes his or her web browser. The LTPA token stores and encrypts all credentials. Both Lotus Domino and WebSphere Portal share secret keys. WebSphere Application Server creates and exports an LTPA key that Lotus Domino imports.
- If you have different directories for WebSphere Portal and Lotus Domino or if the two systems reside in different domains, then use the **credential vault**, which serves as a credential repository against which Lotus Domino can authenticate a user. There are two types of credential vaults: passive and

active. The passive credential vault lets a portlet extract the credentials, while the active credential vault submits the credentials to Lotus Domino using HTTP or basic authentication.

In this chapter, we focus on integration between Lotus Domino and WebSphere Portal Express. We chose Portal Express because it is the easiest product in the WebSphere Portal family to install, and requires a single server installation. If you are piloting this integration for the first time, then the single server installation is recommended for test purposes. We assume that you already have Lotus Domino and WebSphere Portal Express installed. If you have not installed WebSphere Portal Express, refer to the WebSphere Portal Express InfoCenter at [http://www. i bm. com/devel operworks/websphere/zones/portal /proddoc. html](http://www.ibm.com/devel operworks/websphere/zones/portal /proddoc. html) for instructions.

Lotus Domino 7 supports WebSphere Portal Express 5.x.

First, we configure Lotus Domino settings in the Server document, and then configure the Domino IIOP task. After that, we configure WebSphere Portal.

Configuring Lotus Domino for WebSphere Portal

Before you configure Lotus Domino for WebSphere Portal, there are a few things to consider:

- Will you be integrating with Lotus Sametime and Lotus QuickPlace as well as WebSphere Portal to enable additional services in the portal environment?
- Will the Domino Directory serve as the Portal LDAP directory? A shared LDAP directory will make single sign-on easier to configure.

After you answer these questions, you are ready to get started on configuring Lotus Domino for WebSphere Portal. The first task that you need to perform is to configure the Domino Directory for WebSphere Portal. Here we assume that the Domino Directory will serve as the WebSphere Portal LDAP server.

Configuring Domino LDAP

You have to configure Domino LDAP so that WebSphere Portal can access certain attribute types. When you configure Domino LDAP for WebSphere Portal, you have two choices: You can bind users to LDAP to enable authenticated LDAP or you can configure anonymous access for users. We do the latter in the following procedure, but if you prefer authenticated LDAP, modify the `CSEnvi ronment. properti es` file.

To configure anonymous access, you must extend the Domino LDAP schema with the HTTP-HostName attribute, which is where we start.

1. In the Lotus Notes client, open the Domino LDAP Schema database (schema.nsf) on your Domino Directory server.
2. Open the All Schema Documents view.
3. Click the New Document button and select Add Attribute type from the button menu.
4. On the Basics tab of the LDAP Schema attribute type document, do the following:
 - Enter HTTP-HostName in the LDAP name field.
 - Enter xxx in the OID field.
 - Enter Directory String in the Syntax name field.
 - Select Yes in the Single valued field.
 - Select No in the Collective field.
 - Select No in the No user modification field.
5. Save and close the document. The document is saved as a draft document that requires approval before it takes effect.
6. Open the Draft Documents | Draft Attribute Types view to find your new document.
7. Select the HTTP-HostName document, click the Approve button, and select Approve Selected Drafts from the button menu.

Now if you open the All Schema Documents view, you should see the HTTP-HostName document in the view. Next, we modify the LDAP schema settings in the Domino Directory.

1. In the Domino Administrator client, open the Domino Directory (names.nsf) on the Domino Directory server.
2. Select the Configuration tab, and then open the Server | Configurations view.
3. Select the All Servers Configuration document, and then click the Edit Configuration button.
4. In the Configuration document, select the LDAP tab.
5. Click the Select Attribute Types button.
6. In the LDAP Attribute Type Selection dialog box, select the asterisk (*) in the Object Classes drop-down field, and then click the Display Attributes button.
7. Select the following attribute types from the Selectable Attribute Types:
 - AltFullName
 - dominoCertificate
 - givenName

- HTTP-HostName
 - Location
 - mail
 - mailaddress
 - MailDomain
 - MailFile
 - MailServer
 - member
 - NetAddresses
 - PublicKey
 - sn
 - uid
 - userCertificate
8. Click the Add button to add the attributes to the Querable Attribute Types window.
 9. Click OK to save your changes and to close the dialog box.
 10. On the LDAP tab, select Yes in the Allow LDAP users write access field if it's not already selected. This option allows WebSphere Portal users to use the self-registration feature in Portal Express.
 11. Save and close the Configuration document.

Now that you have anonymous access configured for your users, don't forget to add your Portal administrators group, `wpsadmin`s, to the Access Control List of the Domino Directory. See the Chapter 4 for details on modifying the ACL.

Enabling LDAP for SSL

If you want to secure the data between WebSphere Application Server and WebSphere Portal and the Domino Directory, enable WebSphere Application Server and WebSphere Portal LDAP to use SSL. Enabling SSL protects passwords that are passed between the different systems. This chapter gives you an overview of the process, but does not include step-by-step details for setting up SSL. Refer to the WebSphere Application Server and WebSphere Portal product documentation for more information.

When you enable LDAP to use SSL, Domino is forced to present either a self-signed certificate or a certificate signed by a Certificate Authority (CA). For more information about the Domino Certificate Authority, see the Chapter 9. To set up SSL, you need to import the Domino certificate into the WebSphere Application Server and WebSphere Portal keystores. Self-signed certificates are imported as signer certificates into the WebSphere Application Server Java Key Store and into the `cacerts` file for WebSphere Portal. For CA-signed certificates, the CA certificate chain is imported as the signer certificate into the WebSphere Application Server Java Key Store and into the `cacerts` file for WebSphere Portal.

Domino self-signed certificates are GSKIT-compatible, which is not supported by WebSphere Application Server. Both WebSphere Application Server and WebSphere Portal support ARM files. The ARM format is a Base64encoded-ASCII data format. The IBM HTTP Server, which provides the HTTP service to WebSphere Application Server, and therefore to WebSphere Portal, includes IKeyMan, a key-management utility that can convert GSKIT-compatible certificates to the ARM format.

You must configure WebSphere Application Server and WebSphere Portal to allow LDAP over SSL, but before doing so, make sure that LDAP is working without SSL. Also make sure to have the Domino Directory working over SSL. The basic procedure is as follows:

1. Generate the certificates, either self-signed or CA-signed, in Lotus Domino. Certificates must be in the ARM file format before you can export them. Use IKeyMan to generate ARM files.
2. Move the certificate into the WebSphere Application Server. You can move the file by network transfer or some other file sharing means.
3. Import the certificate into the WebSphere Application Server using IKeyMan.
4. After importing the certificate into WebSphere Application Server, make it accessible to WebSphere Portal by importing it into a WebSphere Portal keystore (cacerts). Again, use IKeyMan to import the certificate.

If you use Lotus Domino only as an LDAP directory, and not as a datastore, you must configure `wpsconfig.properties` to enable WebSphere Portal to use Domino LDAP. This chapter assumes that Lotus Domino serves as a datastore, so we do not cover how to modify `wpsconfig.properties`. For more information on how to configure Lotus Domino as an LDAP directory only, see the WebSphere Portal product documentation.

Setting the Domino Server Document for WebSphere Portal

There are several fields on the Domino Server document that you should set to support WebSphere Portal:

- On the Security tab, in the Agent Restrictions and Java/COM Restriction fields, enter the names of the users and/or groups who may access Portal.
- On the Internet Protocols | HTTP tab, make sure that the fully qualified host name is entered in the Host Name field and that the Allow HTTP clients to browse databases field is set to Yes. This property allows users to select servers and databases when editing the Lotus collaborative portlets properties. On the same tab, you can set the fields in the Character Set Mapping section to allow non-western languages.

- On the Ports | IIOp tab, make sure that the TCP/IP port is enabled and that Authentication Options name and password are set to Yes.

Enabling the DIIOP Task

To communicate with Lotus Domino, the collaborative portlets that ship with WebSphere Portal Express use Java APIs. To connect with Lotus Domino, the Java APIs use DIIOP, so enabling the DIIOP task is required. You can enable the DIIOP task in the server's NOTES. INI file. Stop the Domino server before making any modifications to the NOTES. INI file. Using a text editor such as Notepad, open the NOTES. INI file and add di i op to the ServerTasks variable. Save the NOTES. INI file and restart the server.

To verify that the DIIOP task is running on the server, open the Domino server console and look for the line: DIIOP Server: Started.

Application Integration

WebSphere Portal lets you reuse your existing Domino applications and data, so you don't need to create new applications specifically for a Portal environment. However, how much programming is required to integrate your existing Domino applications with WebSphere Portal depends on your method of integration. WebSphere Portal provides out-of-the-box collaboration portlets that integrate with Lotus Domino, Lotus Sametime, and Lotus QuickPlace with no or little programming required. More sophisticated methods of integration, including the Domino JSP tag libraries, Java, and IBM Application Portlet Builder, are available.

When we discuss application integration, there are two aspects to take into consideration: the type of integration, and the integration technique. There are more factors to consider, but this chapter concentrates on these two.

Application Integration Types

You can integrate portlets with Domino applications in several different ways. Linking to the Domino application is the simplest and easiest way to integrate the two systems. In this case, you include a link to a Domino application from a portlet. When the user clicks the link, Lotus Notes is launched to display the application. This type of integration does not present content and provides no functionality, but if you need to display application links as bookmarks, you may find this type of integration helpful.

If you want to provide content without functionality, you can display read-only data in the portlet. This type of integration may be useful if you want to push data to your users, for example, if you want to present your users with news, announcements, or other important information that they need to be aware of, but do not need to interact with.

To manipulate the Domino data, users must use either a Notes client or a web browser to access the application because functionality is not built into the portlet. If users need or want to interact with the data, you can provide a link in the portlet to launch the application in Lotus Notes.

A more robust option is to fully integrate an application with the Portal environment, eliminating the need for a separate client to manipulate data. When you fully integrate the two systems, users can create data and perform other functions that they are allowed to perform according to the application ACL (short of changing the application design). In this case, the application and the portlet cooperate to transfer data entered into the portlet to the Domino back end. This type of integration requires the most significant development investment of all integration types, but in return, provides the most functionality in addition to content.

Application Integration Techniques

Now that you understand the different types of integration available to you, let's discuss the different techniques for integration. The simplest technique is an existing portlet. Existing portlets include out-of-the-box portlets that ship with the WebSphere Portal family of products, IBM-developed portlets (such as the Domino Application Portlet) that you can download, and third-party portlets that you can use with Lotus Domino and WebSphere Portal. The IBM Workplace Solutions Catalog located at <http://catalog.lotus.com/wps/portal/workplace> provides many portlets for different industries, solutions, and products, and many of the portlets are free to download. Here are some of the more common out-of-the-box and ready-to-use portlets already available.

Collaboration Center

Both WebSphere Portal Extend and WebSphere Portal Express ship with a set of collaborative portlets that you can integrate with Lotus Domino. With WebSphere Portal Extend, you get Collaboration Center, a set of portlets that includes:

- People Finder for locating others in your corporate directory. You can search for others by employee name and find contact information as well as their place in the organizational hierarchy.
- My Lotus Team Workplaces (QuickPlace) for a list of all QuickPlaces to which you belong. You can search across all QuickPlaces, and join or create a QuickPlace.
- Web conferencing for online meetings. You can manage your web conferences and join or schedule an online meeting.

The Collaboration Center also provides presence awareness for instant messaging. The Team Workplaces and Web Conferencing portlets require Lotus QuickPlace and Lotus Sametime installations.

Domino Application Portlet

The Domino Application Portlet can integrate any Lotus Domino 5 or later web application with WebSphere Portlet with minimal configuration. Your Domino application developers are not required to change their Web-enabled Domino applications to function in WebSphere Portal with this portlet. All Notes formula language, LotusScript, Java, and JavaScript should function as intended for the Web in Domino Application Portlet. WebSphere Portal administrators do not require an in-depth knowledge of Domino applications to make them available from a portal, and Domino developers do not require extensive knowledge of WebSphere Portal to create their applications.

The usual portlet configuration is required to use the Domino Application Portlet with parameters specific to that portlet. The portlet uses reverse proxy to map the Domino URLs to WebSphere Portal. The portlet also supports single sign-on and SSL for security. Users interact with the Domino data in the Domino Application Portlet just as they would through a web browser, so no additional client is required to manipulate data. All web application functionality is preserved by the portlet.

Lotus Domino Extended Products Portlets

The Lotus Domino Extended Products Portlets describes a group of Lotus collaborative portlets that includes Domino Web Access, Domino Document Manager, Lotus Sametime, and Lotus QuickPlace portlets to name just a few in this bundle. These ready-to-use portlets require that you have the appropriate back-end products (Lotus Sametime, Lotus QuickPlace, and so on) to enable the portlets to work. The Domino Extended Products Portlets work with WebSphere Portal Extend and WebSphere Portal Express Plus.

Common Personal Information Management (PIM) Portlets

The Common Personal Information Management Portlets, usually referred to as the **Common PIM Portlets** or by the acronym **CPP**, let you access your messaging and personal information management features, such as personal calendar, from a variety of back-end sources. The Common PIM Portlets support Lotus Domino, Microsoft Exchange 2000, IMAP, and POP3. Currently, the Common PIM Portlets consist of the Common Mail and the Common Calendar portlets. You can configure these portlets to work with any of the support back ends.

With most out-of-the-box portlets, the development is already done for you, so Java skills and WebSphere Portal knowledge isn't required to implement these portlets. Conversely, because most of the programming has been handled by the portlet developers, the

Domino application developers can do little to no customizing of the portlet. For more flexibility, developers may want to consider the Domino JSP tag libraries.

Portlet Builders

Portlet builders are applications that let you create customized portlets quickly and with little programming. Portlet builders are viable options for any developer or organization that needs a customized portlet, but lacks either the resources or skills to create them with the Domino JSP tag libraries or Java. They bridge the gap between existing portlets and more advanced integration techniques.

There are several portlet builders available today from both IBM and third-party vendors. As an example, we focus on IBM Portlet Builder for Domino to show what a portlet builder can do for you. As part of WebSphere Portal Application Integrator, the IBM Portlet Builder for Domino is available as a free download from the IBM Workplace Solutions Catalog referenced earlier. Using an existing Domino application, you can create a customized portlet to display the application with Portlet Builder for Domino without having to alter the Domino application in any way. The Portlet Builder for Domino can connect with any Domino application using IIOP.

Portlet Builder for Domino lets you choose the view columns and form fields to display. It supports file attachments, view search, column resizing, and column sorting. Presence awareness is also available if you have a Lotus Sametime installation. The Portlet Builder for Domino includes a document viewer portlet, so when users select a Domino document for viewing in WebSphere Portlet, you can choose to render the document in the same portlet or in the document viewer portlet. The document viewer portlet has the capability to display Domino documents in an iFrame. Users can interact with existing documents or create new documents through the iFrame.

Generally, portlet builders enable you to build portlets quickly, easily, and inexpensively, but they have their limitations, which is why two more options exist: Domino JSP tag libraries and Java programming.

Domino JSP Tag Libraries

With the Domino JSP tag libraries, you can incorporate Domino data and functionality on a JavaServer Page (JSP). Because of WebSphere Portal's J2EE environment, you can surface Domino data and functionality to WebSphere Portal through a portlet (the JSP). You can use the Domino JSP tag libraries to create any one of the different types of integration (link-only, read-only, or full integration).

The Domino JSP tag libraries were first introduced in Lotus Domino 6. They are part of the Lotus Domino toolkit for WebSphere Studio, which Lotus Domino customers can

download from <http://www.lotus.com/products/product4.nsf/wdocs/toolkitwstudio>. The Domino JSP tag libraries are available with Lotus Domino Designer 6.0.2 and later. The toolkit is actually a plug-in for WebSphere Studio 5.0, and provides not only the custom JSP tag library but also a Domino view in WebSphere Studio navigator for dragging and dropping tags onto a JSP.

The JSP tags appear as XML on the JSP. They provide access to Domino objects, such as forms, views, and so on, using the Domino Java API. However, knowledge of Java or even the Domino Java API isn't required. The Domino JSP tag libraries simplify creation of a JSP.

There are two JSP tag libraries for Lotus Domino: `domtags.tld` and `domutil.tld`. In the first library, you will find all the collaborative tags necessary for accessing Domino data and objects. The tags in `domtags.tld` let you access, input, and manipulate Domino data. The second library, `domutil.tld`, provides the tags that are common to the J2EE containers, such as `if` and `else`.

WebSphere Portal reportedly does not support the Domino JSP tag libraries, and some input tags may not work at all in the Portal environment because of URL translation; however, that does not mean that they are not an option for creating your own portlets from JSPs. You must test the portlet thoroughly in WebSphere Portal to ensure that the Domino functionality works as expected. Another downside to using the Domino JSP tag libraries is performance. Because each remote server request that the JSP executes with the JSP tag libraries opens a new DIIOP session, server performance may suffer as the number of users increases. If a large number of users will be accessing the Domino data, then you may want to consider another option: Java.

Java Programming

The last option available for integrating Lotus Domino and WebSphere Portal is Java programming. You can create sophisticated, customized portlets to access Domino data and to present Domino functionality in WebSphere Portal and avoid the limitations of the previous integration techniques. All of the advantages inherent to Java—multithreading, platform independence, and so on—are available to you when you code portlets using Java. The major disadvantages of this integration option are:

- The advanced skills required to program Java
- Longer development time than the other available options
- Knowledge of the Domino Java API is required

If you are considering this option, then likely you have the skills and the know-how to program Java, and the benefits of a customized Portlet far outweigh the disadvantages.

The Notes Application Plug-In

Most of this chapter has been focused on integrating the Lotus Domino server and WebSphere Portal, and integrating Domino applications and data with portlets. There is a new tool in Lotus Notes 7 that may make integration easier: the Notes Application plug-in. But before we describe this plug-in, you need to know about IBM Workplace Collaboration Services and the IBM Workplace Managed Client because without the Workplace Managed Client, the Notes application plug-in would not exist.

IBM Workplace Collaboration Services

IBM Workplace Collaboration Services is a WebSphere Portal application. It is to WebSphere Portal what Domino Web Access is to Lotus Domino; without their respective platforms—WebSphere Portal and Lotus Domino—these products can't operate.

Workplace Collaboration Services began as a group of products known as Lotus Workplace Messaging, Lotus Workplace Team Collaboration, and Lotus Workplace Collaborative Learning. Lotus Workplace Messaging provided a low-cost messaging alternative for organizations whose employees lacked a dedicated workstation. A Workplace Messaging account could be accessed from almost any web browser at any time. Administrators could auto-provision mail accounts to their users, who could self-register with the system to create accounts that included a mailbox, personal calendar, and personal address book.

Lotus Workplace Team Collaboration offered features similar to what is available in Lotus QuickPlace and Lotus Sametime. It provided instant messaging, web conferencing, discussion forums, and file creation and sharing. Lotus Workplace Collaborative Learning was similar to the Lotus Learning Management System and prior to that Lotus LearningSpace. It allowed you to manage online course offerings, import courseware, and create a curriculum. Users could self-enroll in courses that they could take at anytime from anywhere. Eventually, another product was added: Lotus Workplace Documents for document management, file sharing, and document creation.

Shortly thereafter, the Lotus Workplace products evolved into IBM Workplace Collaboration Services. These services included all of the previous services available: messaging, instant messaging, web conferencing, Team Spaces, and so on.

All the services offered by Workplace Collaboration Services are accessible through a web browser.

A subset of these services—messaging, documents, and instant messaging—are also available through the IBM Workplace Managed Client.

IBM Workplace Managed Client

The IBM Workplace Managed Client, formerly known as the IBM Workplace Client Technology, rich edition, is a server-managed rich client that you can use online or off-line. The Workplace Managed Client is provisioned by the Workplace Collaboration Services system administrator, who can not only provision the client to users, but also provision updates for both clients and applications.

The Workplace Managed Client was built with Java and based on the Eclipse framework. It provides a platform on which you create your own client applications. It even provides tools to help you get started:

- The IBM data access tool lets you create database applications using IBM Cloudscape on the back end to store data. The data access tool includes data access designer for developing your database application and data access viewer for entering data into your application.
- Activity Explorer is a collaboration tool that helps teams to manage their projects. With it, teams can share files, share their screens, chat online, and send broadcast messages, known as shared notes.

Because the underlying structure for the Workplace Managed Client is the Eclipse Standard Widget Toolkit (SWT) framework, you can create plug-ins for the client just as you would for Eclipse. (In fact, any Eclipse plug-in should work with the Workplace Managed Client because of their common platform.) Plug-ins are components that let you extend the client to work with other applications and data. With the right tools, anyone can build a plug-in for the Workplace Managed Client. That extensibility is one of the greatest strengths of the client.

While you could build a Notes plug-in for the Workplace Managed Client, Lotus Notes 7 has already done that for you with the Notes Application plug-in. This plug-in enables you to work with your Notes applications—standard and custom applications—in the Workplace Managed Client, so you have one more way in which to access your Domino applications and data.

The plug-in requires you to install both Lotus Notes 7 and Workplace Managed Client 2.5 or later. Most of the functionality available in Lotus Notes is available to you in Workplace Managed Client with the Notes Application plug-in, including bookmarks, Notes menu options, document links, database links, and so on.

Custom applications built with LotusScript or the Notes formula language will run the same in Workplace Managed Client as they do in Lotus Notes. No special programming is required to build Notes applications for the managed client.

Once you integrate your Notes applications and Workplace Managed Client, you can take advantage of the tools in the managed client to work with Lotus Notes. For instance, you can save Notes file attachments to a document library in Workplace Documents to share with other team members.

Deploying the Notes Application plug-in is as simple as checking a box. The Allow Notes Application plug-in option is available on the default user policy. As with other user options, you can determine which groups or individuals are allowed to use the plug-in in case you don't want to allow all users that option.

Almost anything that you do in Lotus Notes will take effect in Workplace Managed Client, and likewise, what you do in the managed client will take effect in Lotus Notes. For example, if you create a new bookmark in the managed client, it will appear in Lotus Notes.

To avoid having to log in to the managed client and separately into Lotus Notes, enable single sign-on in the Notes client.

Despite having two different clients, you can open only one instance of an application at a time, so if you open an application in Lotus Notes, you can't open the same application in Workplace Managed Client.

Summary

In this chapter, we described how to integrate Domino and WebSphere Portal, to take advantage of WebSphere Portal's ability to present your Domino data and applications to web browser users (both internal and external). We started with a brief review of WebSphere Portal, and the ways in which integrating WebSphere Portal and Domino integration can enhance your environment. We then explained how WebSphere Portal and Domino can be integrated (both at the server level and the application level). We concluded with an overview of the Workplace Managed Client and the Notes Application plug-in.

14

Directories

Every email sent uses directories. Lotus Notes uses at least one directory, and often several. The directory is more than just a list of names; it can provide information and act as a service. Some of the information is obvious: names, addresses, and phone numbers. Complex directory services can include automatic look-up and referrals, and can act as a binding agent for authentication.

Here is one example of how directories simplify your life. Let's say you need to send an email to your friend Mike. Mike's email database is located at:

- ServerA
- IP Address 10. 10. 10. 2
- In the directory mai l 01
- Database name Mi keBubba. nsf

To send a message, you would need to create an address: something like
mai l /ServerA/mai l 01/Mi keBubba. nsf @10. 10. 10. 2.

But what if Mike moves to another server, with all of the settings changed? And how about other people who you need to communicate with during the course of a year? Can you remember all of those addresses? Not to worry; directories to the rescue!

Using your Notes address book (yes, this is a directory), all you need to know is 'Mike Bubba'. The address book will put the actual email address into the **Send To** field. After the message is sent, a DNS (a directory) would help route the message to the right server. When the message arrives at the server, another directory then delivers the message to the correct database.

Imagine that your company has 7000 employees working in 12 different countries. To execute an effective business, everyone in the company shares their personal address book with every other employee. Also, each employee has address entries that have customer information and email addresses. You could have each employee send or copy their address, and send it to all other employees as they get new contacts. For 7000 employees, this would be a massive mess. In this case, an 'enterprise directory' would

help out. The enterprise directory acts as a central repository to hold information about the other employees and customers in the company. You can also store information about other resources, such as conference rooms and projectors. With a single enterprise directory, you can easily support 7000 people (or even 700,000), and all that your end users would need to do is open the address bar on their email client.

Directories have grown from just a repository of names and passwords into a required ubiquitous systemic-infrastructure component. Today's directories contain not only user information, but also security and access policies. Directories are now an integral part of the business-to-business enterprise. The Internet connects enterprises into a global economy. Directories hold the Internet together, and TCP/IP ties them together. This interaction of directories is critical to the success of the current Internet-based economy.

Directory Uses

Many readers may conclude that all they need is a single directory. But many large enterprise companies have many different directories. The reason for this is the complexity of large companies; in many cases, there can be hundreds of directories. Some examples would be:

- Directory for messaging (several if there are several systems)
- Payroll directories (again, in some cases, several)
- DNS directories
- Phone directories
- Customer directories
- Special application directories

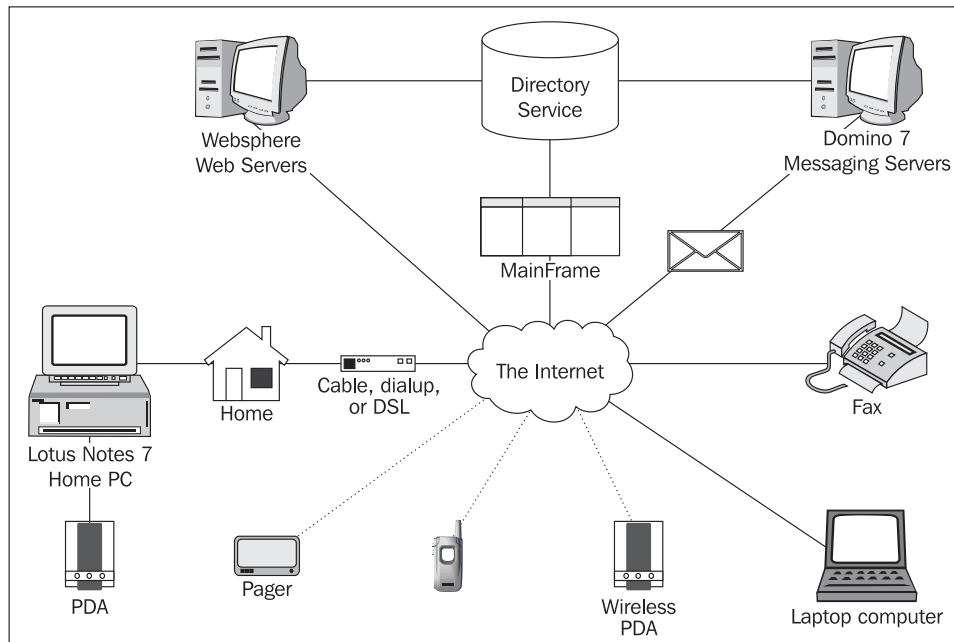
You may have heard the term **authoritative directory**. The simple idea behind this term is that a corporate enterprise will have just one 'authoritative' directory. This single directory will be the central source for all activities within the company. The reality is that large enterprise companies will have several authoritative directories. Due to the complexity of today's business environment, and the fact that many companies cross geographical boundaries, these different directories are required. Every merger and joint venture can create several directories.

The Domino Directory can support many different services and requirements. Depending on the needs and size of the company, Domino Directories can support a large variety of requirements. In today's e-enterprise, you must be able to contact another member within your team, or virtual team, quickly. Directories enable unified messaging. The Domino 7 directory can play very well in this consolidated enterprise.

In a global enterprise, people will have several tools that they will use for messaging. These include:

- **Phone:** In the office or when working at home, most employees have a phone. The enterprise directory contains information about users, the locations where they work, and their phone numbers.
- **Paging service:** With the advent of two-way paging, the directory is now very important.
- **SMS messages.**
- **Home or office email:** Directories have been a part of email since it was developed.
- **Mobile email:** There are many different types of mobile email, from proprietary systems to generic standards-based systems.
- **Instant messaging (IM):** This is another messaging technology that has grown virtually ubiquitous in recent years. With IM, you can contact team members quickly, host and attend meetings, and even share applications. A directory is needed to help establish the connection between users.
- **Wireless:** Wireless technologies are now widely used to connect IM, email, and SMS. In every case, a directory is needed.
- **Fax:** Even the old fax service might use a directory. This directory can be via DID (to find users and delivery the fax directly to the desktop), or can be just a simple directory embedded into the fax machine itself.

The following diagram illustrates a directory service in action:



There are many different types of directory services available on the market. One example would be the IBM Tivoli Directory Integrator. Directory Integrator provides LDAP, directory integration, and directory interfaces. Directory Integrator can also serve as a flexible synchronization layer between a company's identity structure and the application sources of identity data. Using Directory Integrator can eliminate the need for a centralized data store.

Directories are also starting to be integrated into policy management. Domino 7 provides a mechanism to help manage end users' desktops; all of this data can be entered into the Domino directory via policies.

One of the most promising developments in the directory arena was the emergence of the Lightweight Directory Access Protocol (LDAP). LDAP is quickly becoming a standard that can provide a single universal interface for information retrieval across enterprise directories. Many products, including Notes, Domino, Microsoft Active Directory, and Novell NDS, support LDAP.

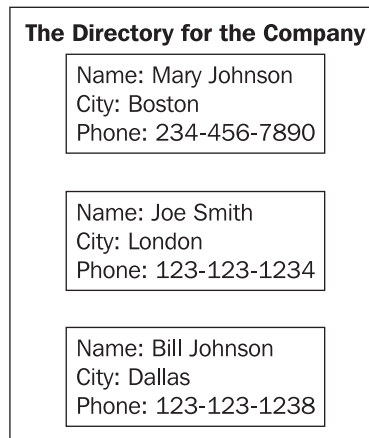
Directory Architecture

Modern directory architecture is based on a set of objects. A directory object is normally a pre-set data structure that represents some type of entry in the directory. These entries can be users, groups, servers, resources (such as conference rooms, printers, or projectors), policies, and so on. Each object has some type of definition assigned to it. These object definitions include properties (also known as attributes). A directory object will, in most cases, have some type of unique identifier. This will provide uniqueness within the directory structure. This value can be a number, a name, or a combination of properties. Object properties can include name, phone number, email address, and so on. Typically, each property has a data type associated with each value. For example, a phone number can be data type 'number', and its name can have a data type of 'string' or 'text'.

A directory can also have a defined schema. The schema is basically the 'definition' of the internal directory structure. The schema can define the basic structure of all directory objects in a particular directory. The schema defines what properties can be assigned to an object, and the specific syntax of the values that can be assigned. Once the directory schema is defined, then you can start to build the various components of a directory. The components include the namespace. A namespace is a collection of objects that reside within a common directory environment. You can also create an object that contains other objects. This is called a container. A container has a set of rules; sets of objects that follow these rules are said to "exist within that namespace". There are basically two types of namespaces: flat and hierarchical.

Flat names are those in which the objects are held below a single authoritative object, or in a common container. An example is Mary Johnson. In this case, Mary could appear in

the directory as Mary or Johnson, or even Mary Johnson. In a small company, this would not be a problem. But what if you have a Mary Johnson in Boston, another in Dallas, and a third one in London? In the following example, there are three names in a single container. This represents a flat directory structure.



Hierarchical namespaces are logically organized in a directory to facilitate management of the directory. Names can be provisioned via a directory tree that includes unique criteria for each name. Unique criteria can include operations-type data; for example Sales, Marketing, and so on. Another example would be to set up names based on geography; for instance, UK, Dallas, EMEA, and so on. In each example, each person is unique. The common names can be the same; the unique qualifications provide the information about each person so that they can all exist in one hierarchal directory.

Notes and Domino have supported hierarchical naming since release 3. As you provision users and servers, you use hierarchical names. Notes uses a concept of certifiers as the mechanism to create users. A hierarchical name reflects a user's or server's place in the hierarchy. In Notes, the names and certificates are also used to control each user's and server's access in different organizations, and can control organizational units that communicate with each another. A Notes hierarchical name can include the following components:

- **Common name (CN)** corresponds to the user's name or server's name. All names must include a common name component.
- **Organizational unit (OU)** identifies the location of the user or server in the organization. Domino allows a maximum of four organizational units in a hierarchical name. Organizational units are optional.
- **Organization (O)** identifies the organization to which a user or server belongs. Every name must include an organization component.
- **Country (C)** identifies the country in which the organization exists. The country is optional.

X.500

Our next stop on our tour of directories is a discussion about X.500. This is the name given to the standard produced by the International Telecommunications Union (ITU at <http://www.itu.int/>). Headquartered in Geneva, Switzerland, the ITU is an international organization within which governments and the private sectors coordinate global telecom networks and services. ISO/ITU-T defined the protocols for a global directory service that is independent of computing application and network platforms. The X.500 standard was first released in 1988. This standard defines a specification for a distributed directory, based on hierarchical names.

One part of the X.500 protocol is the Directory Access Protocol (DAP). DAP provides a comprehensive protocol for accessing directory servers. A significant part of the X.500 specification addresses the data and information model, and the protocols needed to provide a fully distributed service based on a model for a directory service. In a distributed directory, each server is responsible for a section of the overall Directory Information Base (DIB). All these various sections of a distributed directory are linked together, providing a single logical directory.

LDAP

One term we've already mentioned is LDAP (Lightweight Directory Access Protocol). LDAP emerged several years ago as a subset the X.500 DAP specification. The idea was to use a lightweight client to access an 'X.500-like' directory. LDAP was originally conceived of as a way to simplify access to a directory service, modeled according to the X.500 standards.

LDAP is increasingly being adopted as the Internet directory standard. The LDAP protocol provides a system for passing text-based queries from a client to an LDAP server over a TCP/IP network.

The newest releases of LDAP provide new features, improve compatibility with X.500 (1993), and also specify how LDAP can be used with non-X.500 and standalone directories. The major new features of LDAP are in the areas of:

- Referrals
- Security
- Support for Unicode characters
- Extensibility

The LDAP version 3 core specifications contain protocol specification, attribute syntax definitions, string representation of distinguished names and search filters, LDAP URL format, and X.500 schema definitions. LDAP version 3 also defines a number of

improvements to enable the client/server access model to be more efficiently implemented and more suitable for the new Internet model. Examples of this include support for extended character sets, and support for referrals to facilitate the hand-off from one server to another.

One way to look at LDAP is that it is a simplification of the X.500 Directory Access Protocol. LDAP is this and much more. The LDAP directory service model is based on specific and unique entries. An entry is a single collection of attributes with a single key (a parameter that can be used to look up something, and *not* a key for encryption). In each entry, there is a name. The Distinguished Name (DN) is used as a unique value that represents each collection or entry.

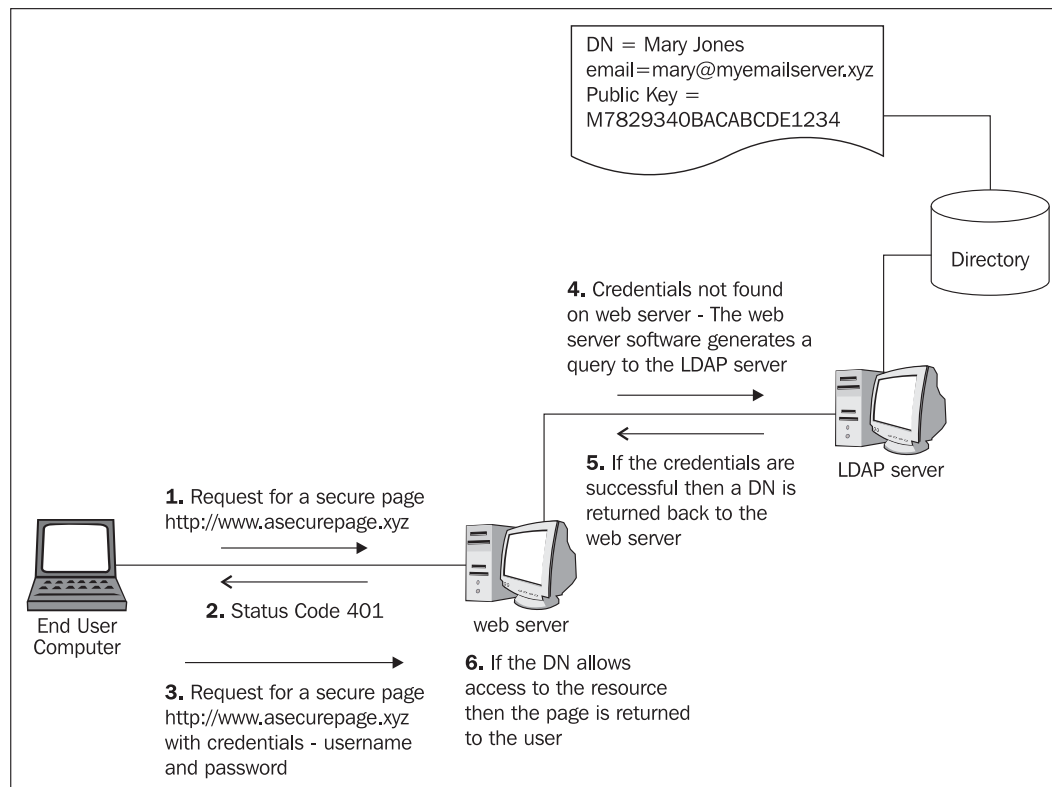
The LDAP directory service is based on a client/server model. An LDAP server offers the directory data via TCP/IP port 389, and SSL encrypted port 636. Clients access the LDAP server via a set of queries. The results of the queries can be used in messaging, applications, and authentication.

Notes/Domino 7 supports LDAP in the client *and* in the Domino server. The client provides access via a set of account documents, and the server provides a wide range of LDAP services and features. The Domino 7 LDAP service supports these features:

- LDAP search, add, modify, compare, and delete operations
- Two methods for schema extension, and support for schema publishing and schema checking
- LDAP language tags to support LDAP searches in alternative languages
- LDAP v3 and v2 clients
- Anonymous access, name-and-password authentication, secure sockets layer (SSL) connections and X.509 certificate authentication, and Simple Authentication and Security Layer (SASL) protocol
- LDAP operations extended beyond the primary Domino Directory to secondary Domino Directories, and to directory catalogs
- LDAP referrals to remote LDAP directories
- LDAP searches of document text in databases configured in a Domain Catalog

Another great feature is the ability to import and register users via an export from an LDAP directory (using LDIF), or import directly from LDAP.

LDAP can also be used to store X.509 certificates for authentication. The certificates are placed into the directory, and then accessed via a web server or service. The following figure shows how an end user with a browser can access a web server. This particular web server is using LDAP as the authentication source.



In the preceding example, the web server returns a status code of 401 when the user attempts to access a protected resource. Once the user's browser receives the status code, it prompts the user for credentials (this is an example of "basic" authentication; form-based authentication works differently). Next, the user sends his or her credentials back to the web server. The web server checks if the user directory information is local; if the information is not local, then it executes a bind operation on an LDAP server and then connects to it. The web server then sends a query to the LDAP server, checking whether the credentials are valid. If the credentials are valid, a Distinguished Name (DN) is returned to the web server. At this point, the user is authenticated, but not authorized. So the web server checks whether the DN has access to the resource being requested. If the request is valid, then the page is returned to the browser. Domino 7 (as well as Domino 6) supports remote LDAP authentication via directory assistance (discussed later in this chapter).

New Directory Features in Domino 7

Domino 7 offers a number of new features related to directories. This section briefly reviews some of these features.

LDAP UNID

The integrated Domino LDAP service task now supports Universal Notes IDs (UNID) through 32-character values of the `dominoUNID` operational attribute. The UNID is a 32-character combination of hexadecimal digits (0-9, A-F) that uniquely identifies a Notes document. This feature is provided for use with advanced LDAP applications. With this feature, you can uniquely identify documents in the Domino Directory, even when the directory objects change. Some of these objects are:

- LDAP: DN Notes: FullName/LastName
- LDAP: UID Notes: ShortName

Directory Assistance

Notes/Domino provides a technology known as **directory assistance (DA)**. This is a feature where a server can look up information in a directory other than just the local primary Domino Directory (`names.nsf`). The Domino Directory is a directory created from the `pubnames.ntf` template. Servers can use DA technology to execute lookups in either local or remote replicas of a Domino Directory. Domino directory assistance can be configured to enable and support Notes mail addressing, LDAP service searches or referrals, client authentication, and group lookups for database authorization.

Domino 7 supports an LDAP concept known as **dereferencing**. An alias entry in an LDAP directory is an entry that points to another entry. Looking this up is known as dereferencing an alias. Support for dereferencing is enabled via the Domino 7 directory assistance database. There are four choices for dereferencing for searches of the remote LDAP directory: Never, Only for subordinate entries, Only for search base entries, and Always.

If aliases aren't used in the LDAP directory, then set this field to Never. This can help improve LDAP search performance. The following screenshot shows how to enable dereferencing. In the DA database, create a new Directory Assistance document. On the Basics tab, set the Domain to LDAP. The LDAP tab, as shown overleaf, will be displayed. The Dereferencing alias on search field appears as a drop-down list. Fill out the form and save it. The final step is to enable directory assistance in the server document.

DIRECTORY ASSISTANCE

Basics | Naming Contexts (Rules) | **LDAP**

LDAP Configuration

Hostname:

Optional Authentication Credential:

Username:

Password:

Base DN for search:

Channel encryption:

Port:

Accept expired SSL certificates:

SSL protocol version:

Verify server name with remote server's certificate:

Advanced Options

Timeout: seconds

Maximum number of entries returned:

Dereference alias on search:

Preferred mail format:

Attribute to be used as Notes Distinguished Name:

Type of search filter to use:

LDAP Connections and Domino 7

As we noted, directory assistance can be enabled for Domino to provide support for LDAP services. Directory assistance uses and retains LDAP search results for a period of time. This can eliminate the need to obtain refreshed information from the LDAP servers. Domino 7 allows directory assistance to detect whether entries in certain LDAP directories have changed. This feature provides the ability for Domino to flush stale search results and execute another search for up-to-date LDAP information. Be sure to check with Notes help and/or readme.nsf for status on supported and tested LDAP services.

LTPA

Lightweight Third-Party Authentication (LTPA) is an authentication technology used in IBM WebSphere and Domino. An IBM WebSphere server or a Domino server configured with LTPA will challenge a web user for a name and password. After the authentication has been validated, the browser receives a session cookie. This cookie is available for just that session. This session cookie stores an LTPA token. This token

includes the name of the user who was authenticated. When Domino creates an LTPA token, it places the Domino-distinguished name in the token by default. This lets you use the LTPA token as a single sign-on mechanism.

With Domino 7, you can now map the username that appears in a Domino-created LTPA token to a name expected by WebSphere. This allows you to ensure that the name is recognized in a mixed Domino and WebSphere environment. The reason for this is that Domino and WebSphere do not share the same directory. There are several implementation options:

- If Notes user information is contained only in a Domino Directory, specify the username mapping in the Person document.
- If Notes user information is contained in a corporate LDAP directory, configure the username mapping in directory assistance.
- If the organization uses both Domino and LDAP directories, configure both the Domino Person document and the directory assistance SSO information.

The Domino Directory

As part of an upgrade to Domino 7, you will need to refresh the design of the Domino Directory. This can be done automatically, or before the first server upgrade. One of the issues that you will need to deal with is directory backward compatibility. Overall, this will not be much of an issue with standard Domino 6. Issues arise if you have added custom elements. Each of these custom design elements will need to be reviewed to determine whether you need to move/modify these elements into the new Domino 7 directory.

The authors executed a simple analysis via a design refresh between a Domino 6.5.4 and a Domino 7 template. What follows is a list of the results of that refresh design.

There are seven new elements that were added to the Domino Directory:

```
' Pol i cy'
' Server\DB2'
' $Certi fi catel nfo'
' $DPLocked'
' $Publ i cKeyRequi rements'
' ($Di scl ai mDi g)'
' ($vwServersByMaj Ver)'
```

There are 272 elements that were updated. Due to the size of this list, only a subset of the elements is shown below.

' Group'	' \$scalendarInheritanceSchema'
' Groups	' \$CatalogerSubform'
' Groups'	' \$CCMAILMTAConnectionFormSubForm'
' hbLoad'	' \$CCMAILMTAServerFormSubForm'
' HiPriorityReplacement'	' \$CertifierExtensionSchema'
' People'	' \$certifierInheritanceSchema'
' Person'	' \$CharacterSetSettings'
' Policies\Policies'	' \$ClientPreferenceSubform'
' Policies\Settings'	' \$ConferencingPersonFormSubform'
' Policy'	' \$ConFormRLANSubform'
' PolicyManagement'	' \$countryExtensionSchema'
' Policy\Archive'	' \$countryInheritanceSchema'
' Rules'	' \$GroupExtensionSchema'
' Schedule'	' \$GroupInheritanceSchema'
' Server\Certificates'	' \$HTMLAttributes'
' Server\Certifier'	' \$IMAP'
' Server\Clusters'	' \$iNotesWebAccess'
' Server\Configuration'	' \$IntegratedMessagingPersonFormSubform'
' Server\Configurations'	' \$InternetSecurity'
' Server\Connections'	' \$InternetSite'
' Server\Connections'	' \$LDAPConfiguration'
' Server\Domain'	' \$localityExtensionSchema'
' Server\Domains'	' \$localityInheritanceSchema'
' Server\Holiday'	' \$LotusFaxLocationSubform'
' Server\Holidays'	' \$LotusFaxPersonSubform'
' Server\Internet'	' \$LotusFaxServerSubform'
' Server\Licenses'	' \$MailInDatabaseExtensionSchema'
' Server\Networks'	' \$MobileServicesPersonSubform'
' Server\Parameter'	' \$MobileServicesServerSubform'
' Server\Program'	' \$MTAConnectionFormSubform'
' Server\Programs'	' \$organizationalUnitExtensionSchema'
' Server\Resource'	' \$organizationalUnitInheritanceSchema'
' Server\Server'	' \$organizationExtensionSchema'
' Server\Servers'	' \$organizationalInheritanceSchema'
' wMainFrameset'	' \$OTPPP'
' wOutline'	' \$PersonExtensionSchema'

'\$PersonGeneral Info'	' (Publ i cDi rectoryProfi l e)'
'\$PersonI nheri tabl eSchema'	' (Real m)'
'\$Pol i cyl FPI tems'	' (RLANLi st)'
'\$Pol i cyPOI tems'	' (Rul esDI g)'
'\$Pol MdTm'	' (Sameti meProxyAuthenti cati on)'
'\$Pol Rdrs'	' (ServerConfi gDi al ogWeb)'
'\$Repl i cati onSubform'	' (ServerConfi gDi al og)'
'\$RouterSMTPSetti ngs'	' (SetPasswordFi el ds)'
'\$ServerI nternetProtocol s'	' (SSLCi pherDi al og)'
'\$ServerTasks'	' (Upgrade)'
'\$SMTPServerFormSubForm'	' (Vi rtual)'
'\$Templ ateBui l d'	' (wAuthenti cate)'
'\$X400Connecti onFormSubForm1'	' (WebDI gAddressMul ti)'
'\$X400ServerFormSubForm'	' (WebDI gAddressSi ngl e)'
'\$\$ReturnGeneral Error'	' (WebDI gLi stboxMul ti)'
'\$\$SearchTempl ateDefaul t'	' (WebDI gLi stboxSi ngl e)'
'\$\$Vi ewTempl ateDefaul t'	' (WebSSOConfi g)'
' (46Group)'	' (wEncrypted)'
' (46Person)'	' (wQSAggregati onConfi gurati on)'
' (Al l Vi ews)'	' (wQSGroup)'
' (Del eteCertDi al og)'	' (wQSPol i cy)'
' (Del eteUserOpti ons)'	' (wQSSi tes)'
' (Di spl ayCerti fi erNotesCerti fi cates)'	' (wReadAddressData)'
' (Di spl ayUserNotesCerti fi cates)'	' (wReadData)'
' (Enrol l CADi al og)'	' (wSetAdmi nOwnFi el ds)'
' (External Domai nNetworkAddresses)'	' (wSetPol i cyFi el ds)'
' (Fi l eProtecti onDi al ogWeb)'	' (\$ACPDi al og)'
' (Fi l eProtecti onDi al og)'	' (\$ACPEmbedded)'
' (Fi ndName)'	' (\$ACPLookup)'
' (LDAPAttri buteTypeLi stWeb)'	' (\$Admi np)'
' (LDAPAttri buteTypeLi st)'	' (\$Catal ogerSetti ngs)'
' (Mappi ng)'	' (\$Certi fi cateAuthori ti es)'
' (Modi fyCCSDi al og)'	' (\$Certi fi ers)'
' (Parts)'	' (\$Cl usters)'
' (Pol i cyComputePOI temLi st)'	' (\$Connecti ons)'
' (POP3)'	' (\$CrossCertByName)'
' (ProxyAuthenti cati on)'	' (\$CrossCertByRoot)'
' (ProxyDi al og)'	' (\$Di rcatConfi g)'
' (ProxyHel p)'	' (\$Di rectori es)'

' (\$Domai ns)'	' (\$Pol i ci esExpl i ci t)'
' (\$External Domai nNetworkAddresses)'	' (\$Pol i ci es)'
' (\$External Domai nNetworkConfi gurati ons)'	' (\$Profi l es)'
' (\$Fil el denti fi cati ons)'	' (\$Programs)'
' (\$Groups)'	' (\$Regi sterGroups)'
' (\$Hol i days)'	' (\$Repl i cati on)'
' (\$I nternetSi tes)'	' (\$Resources)'
' (\$LDAPCN)'	' (\$Rooms)'
' (\$LDAPG)'	' (\$ServerAccess)'
' (\$LDAPHi er)'	' (\$ServerConfi g)'
' (\$LDAPRDNHi er)'	' (\$ServerGroups)'
' (\$LDAPSetti ngs)'	' (\$ServerParameters)'
' (\$LDAPS)'	' (\$ServersLookup)'
' (\$Locati ons)'	' (\$Servers)'
' (\$Mai l Groups)'	' (\$Users)'
' (\$Messagi ngSetti ngs)'	' (\$VI MGroups)'
' (\$NamesFi el dLookup)'	' (\$VI MPeopl eAndGroups)'
' (\$Networks)'	' (\$VI MPeopl eByLastName)'
' (\$Onl i neMeeti ngPl aces)'	' (\$VI MPeopl e)'
' (\$Peopl eGroupsByLang)'	' (\$WebSSOConfi gs)'
' (\$Peopl eGroupsCorpHi er)'	' (\$XACL)'
' (\$Peopl eGroupsFI at)'	' (_Locati ons)'
' (\$Peopl eGroupsHi er)'	' _Add'
' (\$Peopl e)'	' _Peopl e'
' (\$Pol i ci esByHi er)'	' (\$LDAPAI as)'
' (\$Pol i ci esBySetti ngs)'	

Our point is this: take the time to review any custom changes in your directory before you upgrade. Here is an example: Let's say that you use (\$Users) as a lookup in some of your applications. As you can see in the preceding list, this view has been modified. In most cases, these modifications will not be an issue. But due diligence tell us that you should check and make sure that you don't have any issues.

Summary

This concludes our detailed tour of how and why Notes/Domino 7 uses directories to store and maintain the information it needs. We started with a look at the various uses of directories in the Notes/Domino world, including messaging, DNS, data (such as lists of customers and employees), application directories, and so on. We examined typical directory architecture, and looked at directory standards such as X.500 and LDAP. We then turned our attention to new directory-related features added to Notes/Domino 7. These included support for the LDAP UNID, enhanced directory assistance, and upgrades to the Domino Directory itself.

15

Domino Access for Microsoft Outlook

Why would a book on Lotus Domino have a chapter on Microsoft Outlook? Well, Domino Access for Microsoft Outlook (DAMO for short), is a feature that comes out of the box with Lotus Domino. DAMO allows you to use Microsoft Outlook as a client for Notes/Domino mail. This chapter takes a look at all the aspects of DAMO, from installation to client use, highlighting the many new DAMO features found in Notes/Domino 7.

Requirements

Domino Access for Microsoft Outlook allows Microsoft Outlook 2000, 2002 (XP), or 2003 users to connect to a Domino server. Here are the system requirements:

- Windows 2000 Professional Edition and Windows XP Professional Edition with Service Pack 3; 128 MB RAM required (256 MB or more recommended)
- Microsoft Outlook 2000 or Outlook XP with SP3, and (recommended) Outlook 2003 with SP1 (consult the Outlook online help to ensure SP1 is installed)
- Domino 6.5.1 or higher
- Mail databases created using the Mail7.ntf, Mail7ex.ntf, or DWA7.ntf template
- 275 MB disk space

Installing Domino Access for Microsoft Outlook

The installation program in Domino Web Access for Microsoft Outlook 7 is a standard Windows MSI installer and is compatible with SMS.

Upgrading from DAMO 6.5.x to 7

You can upgrade from DAMO 6.5.x to release 7. However, if you are upgrading from DAMO 6.5.3 or earlier, the upgrade will continue to use a single data directory that allows multiple users to have profiles sharing that directory. To take advantage of the multi-user installation capabilities of DAMO 7, in which each user can have his or her own data directory, you must first uninstall DAMO 6.5.x, and then install DAMO 7. Before doing this, back up your existing .nsf, .pst, and .ost files as a precaution. These should be in your Microsoft Outlook directory. The initialization process of the new installation will recreate the mail files locally.

During the upgrade, you will be asked whether you want to create a profile at the end of the upgrade process. If you choose No, you can create a new profile at any time in the future by choosing Create New MAPI Profile from the Start | Programs | IBM Lotus Domino Access for Microsoft Outlook shortcut. This is the only way to create a DAMO profile; you cannot create a profile using the Outlook Setup Wizard.

Setting Up Condensed Directories for Working Offline

With DAMO, you can create a local replica of an address book to use when working offline, disconnected from the network. Using Domino Preferences in Microsoft Outlook, you can select an address book to take offline. We strongly recommend that a condensed directory catalog is available for users to conserve space and improve the time it takes to replicate.

Keeping Your Mail File Secure

As mentioned earlier, DAMO 7 allows multiple users to share the same installation. This type of installation, however, allows access to other users' .pst files because the .pst and .nsf files are local. Typically, in both a standard Notes environment and a standard Outlook environment, the mail file is on the server, and the server controls access. If a user travels, typically he or she is the only user that has access to the laptop containing the local replica. However, since DAMO requires all files to be on the local workstation, you need to protect your local mail data file (*.pst) from others by assigning a password to your local mail data file. You would also want to be sure your DAMO data is in your private folder hierarchy, for example, C:\Documents and Settings\<user>\DAMO_Data. Check your Outlook documentation for the procedure to assign a password to your local files; it is different for each version of Outlook.

Installation Notes for Administrators

The Domino Access for Microsoft Outlook 7 installation program can be found in the data directory under `domino\html\DA0`. You will find one 35.2 MB `setup.exe`.

Before running the `setup.exe` to install DAMO, you must be a registered Domino user and have your `Notes.id` file available. Also, you need to know your username as defined in the Domino directory, and the IP address of your mail server.

Administrators can install Domino Access for Microsoft Outlook without end-user involvement, or end users can install it on their workstations. All of the information about the different kinds of installations (including silent installations, using the wizard, and end-user installation) can be found in the Notes 7 Administrator help under Domino Access for Microsoft Outlook. This information is also available in the *Lotus Domino Access for Microsoft Outlook Installation and Setup Guide* on www.lotus.com/lotus/doc.

It is important that any existing or new user has the `mail7.ntf`, `mail7ex.ntf`, or `dwa7.ntf` as the template used to create his or her mail database. If you have single sign-on enabled or you plan to install it as an option, do *not* move the `user.id` file to the DAMO install data directory when prompted. Windows security is in play when installing DAMO, so be sure the user has the necessary rights to the local PC to create Outlook profiles before beginning the installation. More information on creating the users' profiles is in the Notes 7 Administrator help.

It is important to configure your Microsoft Outlook client as the default mail program and to be sure the Outlook installation is completed before running DAMO. More information can be found under 'Configure Microsoft Outlook' in the Notes 7 Administrator help.

The basic steps to installing DAMO, found in the Notes 7 Administrator help, are as follows:

1. Start the DAMO setup program, and choose whether to install Domino Access for Microsoft Outlook for a single user (which creates a single mail box) or multiple users (each with his or her own mail box). Note that these choices are only available to Windows administrators.
2. You can optionally select the 'single logon' feature to synchronize your Notes ID and Windows passwords. With this option enabled, changing either password changes the other.
3. You must then create a DAMO profile. To do this, use the Create New MAPI Profile shortcut on the Start menu, by selecting Start | Programs | IBM Lotus Domino Access for Microsoft Outlook | Create New MAPI Profile.
4. At the Your Name prompt, enter your Domino common username (*not* your fully qualified name).

5. At the Domino server name prompt, enter the name or the IP address of your mail server.
6. If you installed the multi-user version of DAMO, and you want your Data directory to be in a directory different from your program files, enter a path for your mail files in the Data Directory field. For instance, enter C:\Documents and Setting\leejones\DAMOData or C:\DAMO leejones. (To secure these folders, you can use Windows' folder-security settings.)
7. If DAMO cannot find your Notes ID in your Person document on the Domino server, you may be prompted for one now. Enter the path to the ID file (or browse to it and select it). Optionally, you can also copy your Notes ID file to your data directory (which we recommend doing as a backup). Do not do this, however, if you have single sign-on enabled.

Your DAMO profile will be created. Note that during the creation of the user profile, you will be prompted to wait while the profile is being processed. If you are an existing mail user with a large mail database (500 MB or higher), this can take an hour or more. You must let this process complete before moving on or trying anything with DAMO in the Outlook client. The status will update you as to what the setup is doing and what percentage is complete.



It is also important to ensure that the Notes client is installed on the same PC that DAMO is being installed on, and that the client is already configured and is not currently running while installing DAMO.

DAMO Performance

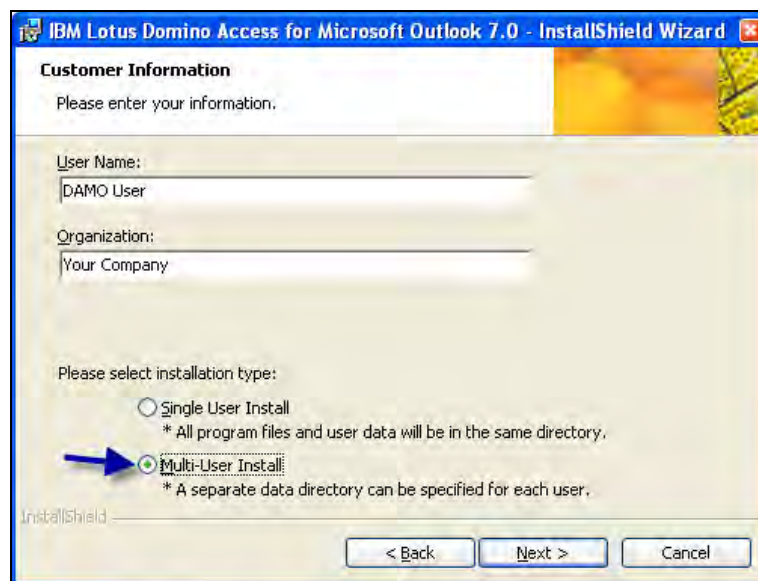
After you have DAMO installed and the profile created, you will want to begin using DAMO. One major thing you will notice in using DAMO 7 is its launch time compared to pre-6.5.3 versions. Using Outlook XP, you can get up to 48 times faster launch speeds!

DAMO 7 Improvements and Enhancements

Domino Web Access for Microsoft Outlook 7 offers many new features and enhancements over previous releases. The following sections briefly discuss some of the more important new DAMO features offered in this release.

Option for Separate Program and Data Directories

As we mentioned earlier, when installing DAMO, you will be prompted for either a Single User Install or a Multi-User Install. Selecting Multi-User Install allows you to separate the program and the data directories.

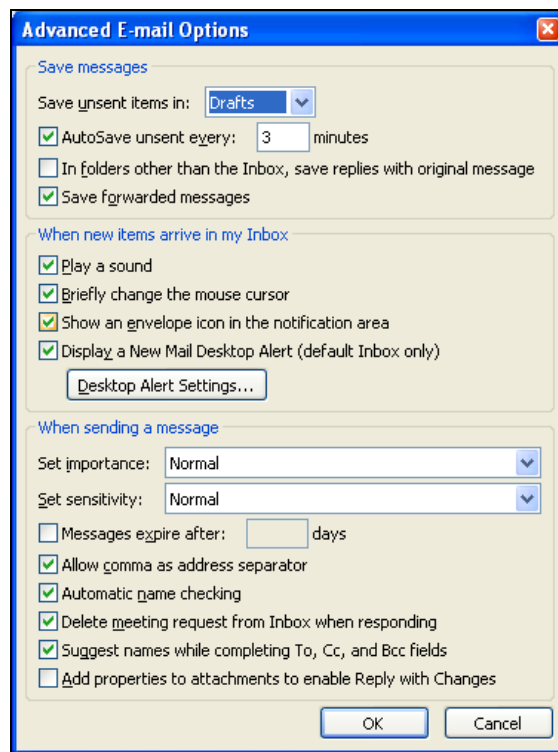


Productivity Enhancements

Several new productivity options have been added to DAMO 7.

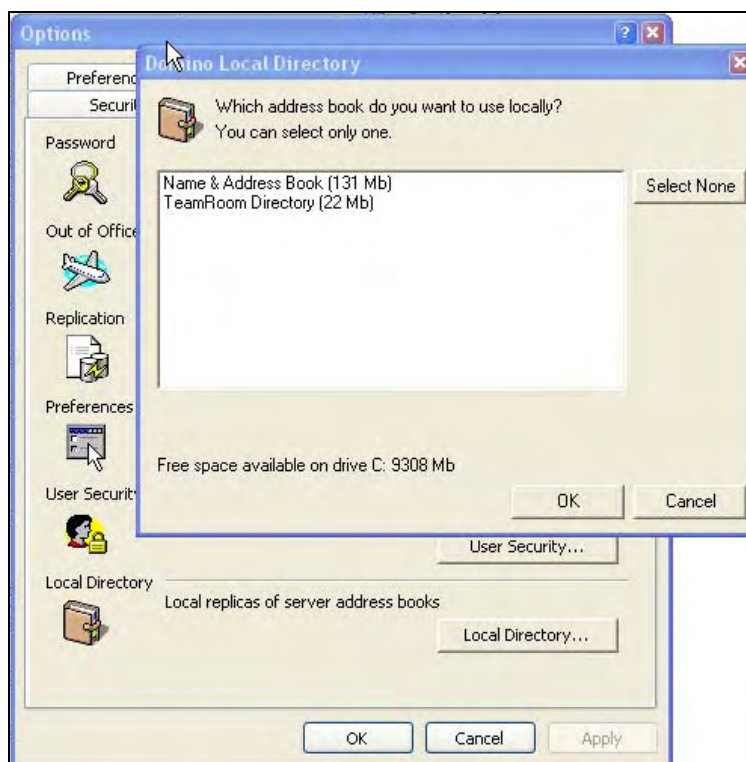
New Mail Notification

Mail notification functionality, similar to Notes mail, has been added to DAMO 7. You can play a sound, briefly change the cursor, or show an envelope in the notification area. You configure this feature through the Advanced E-mail Options dialog:



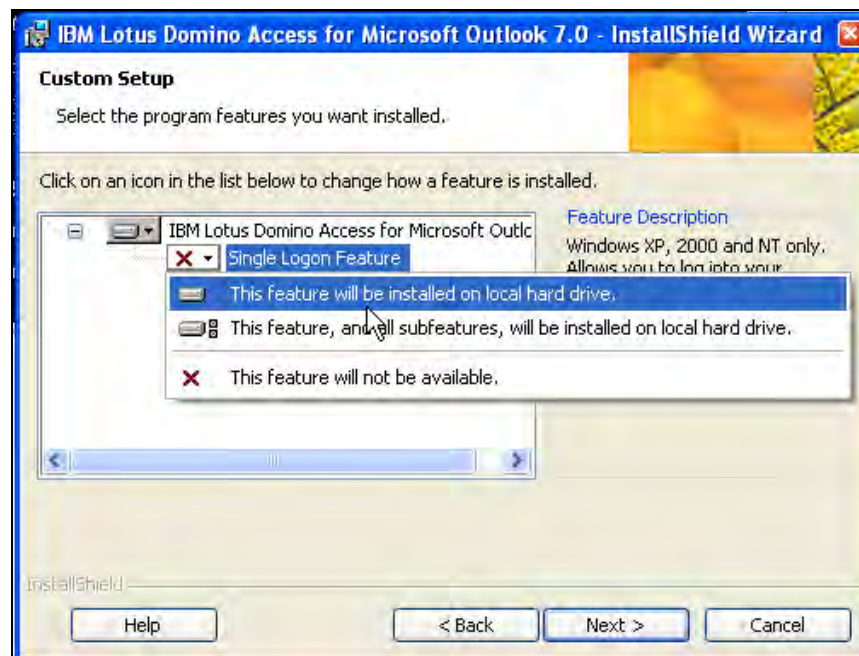
Offline Address Book Support

As mentioned in the installation section earlier, an offline Notes address book can now be maintained in DAMO 7. The only caveat is that you can only have one directory as a local copy.



User Security

DAMO 7 offers single sign-on (SSO) to allow your Windows account password to be used to automatically log in to DAMO. When installing DAMO, you have an option to install SSO; select this option to set up SSO for DAMO:



X.509

DAMO 7 supports X.509-based encryption. You can send and receive X.509-encrypted messages from external recipients outside the Domino domain.

Notes Encryption

DAMO 7 allows an incoming encrypted Domino email to be automatically decrypted. Currently, Notes encryption is not available when sending email using DAMO.

Out-Of-Office Management

Although this feature is not new to DAMO 7, we thought we'd mention it anyway because of its usefulness: DAMO offers the ability to set up an out-of-office message. The DAMO Out of Office feature is very similar to the native Notes client out-of-office functionality. You can enable or disable it, and specify different options about the text of the message that is received while you are away. Enabling the out-of-office functionality in DAMO turns on the agent on the Domino server so the DAMO client does not have to be running.

Out of Office

☐ Enable
☒ Disable

Domino can automatically reply to incoming mail while you are away. To use the Out of Office agent, fill out the dates you will be gone, and "Enable".

Dates

First day out of the office: 8/31/2005

First day back in the office: 9/1/2005

Message

Using the dates entered above, the Out of Office agent will automatically reply only once to each sender with the following message:

To: Whomever

Subject: DAMO User is out of the office

Message: I will be out of the office starting 08/31/2005 and will not return until 09/01/2005.

I will be out of the office through Tuesday, May 31.

Agent status

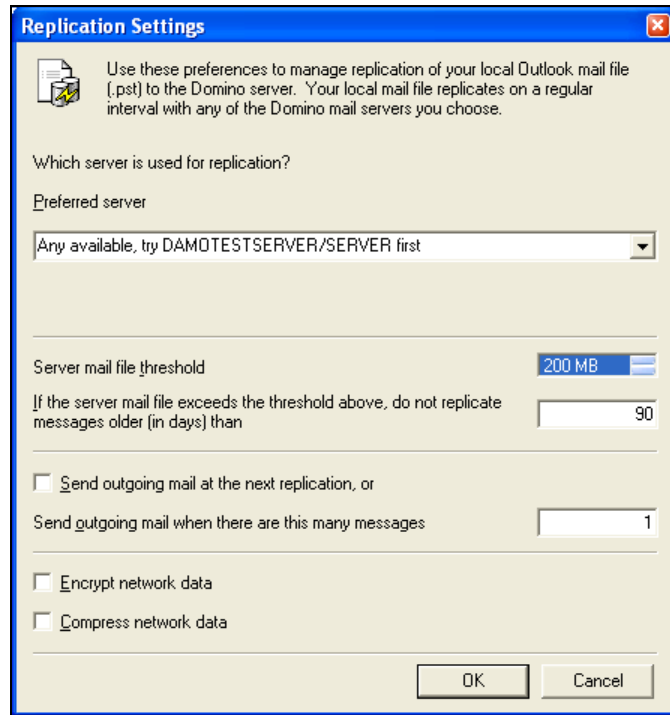
OK Cancel

Replication Management

In DAMO 7, replication is used to 'move' data between the Domino server and the local Outlook files. DAMO replication can be divided into three areas:

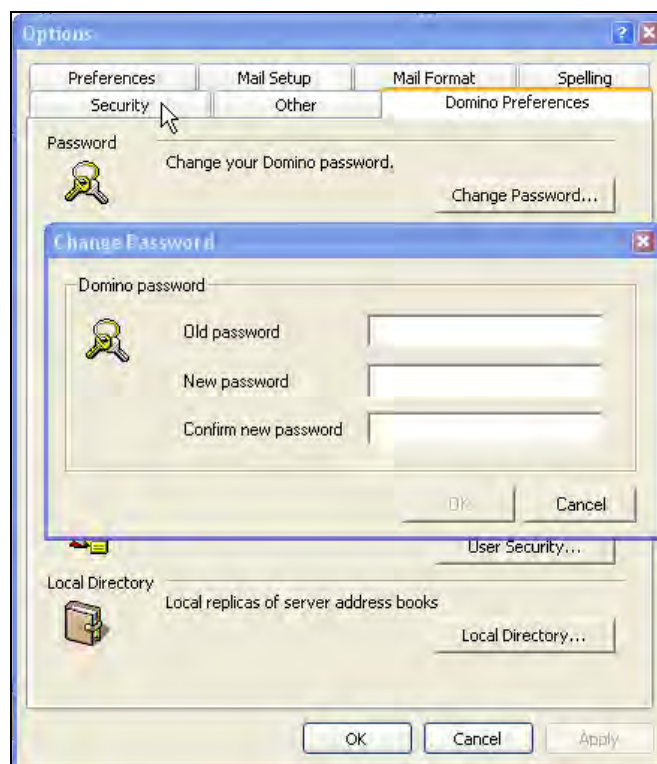
- **Regular replication:** Sends pending mail, replicates any changed documents, updates folder contents, and synchronizes unread mail. These tasks are done in this order. When you click on Send/Receive in Outlook, this type of replication is invoked.
- **'On Demand' replication:** Sends new mail and calendar entries to Outlook immediately.
- **Hourly replication cycle:** During the hourly cycle, additional processes are performed to ensure that the server and local mail data are in sync.

The replication settings options can be accessed via Domino Preferences and allow you to change the preferred server and mail threshold, and to control when outgoing mail is sent:



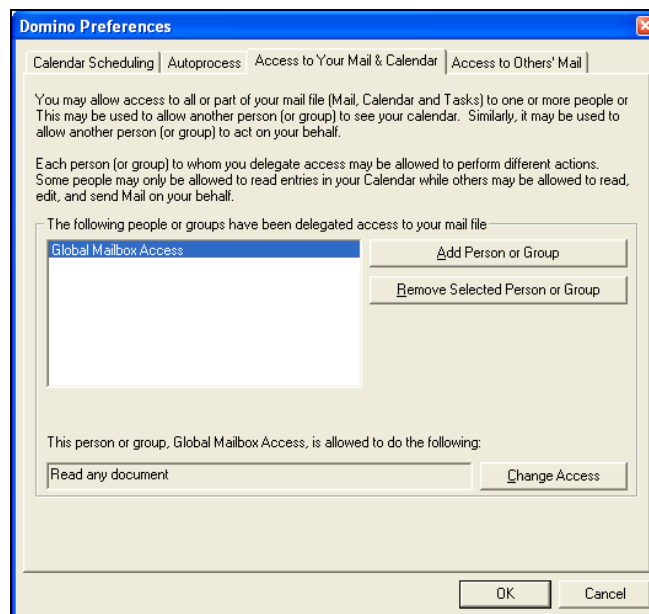
Password Management

DAMO 7 allows you to change your password from within Outlook. Under Outlook's options, select Domino Preferences and then click on Change Password. You need to supply your old password along with your new password, and a confirmation of the new password. Keep in mind that this password change isn't 'connected' to the AdminP process within Domino. This only changes the password in the locally stored Notes user ID.



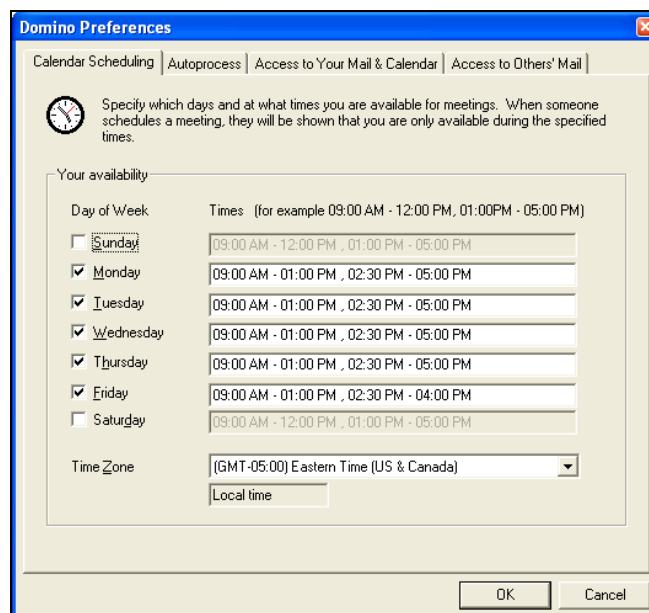
Mail File Ownership

DAMO 7 allows you to access Domino preferences for your mail, calendar, and more. These are very similar to their counterparts within the Notes client. You can change who can access your mail and calendar, and what other Domino mail databases you have access to.

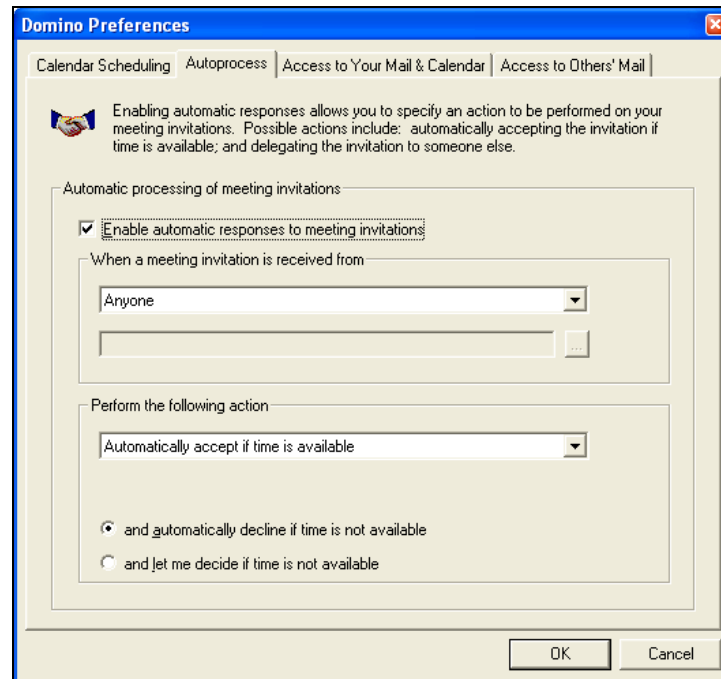


Calendar and Scheduling

Calendar and scheduling is available in DAMO 7. Also, under Domino Preferences from within Outlook's options, you can set up your free-time schedule.

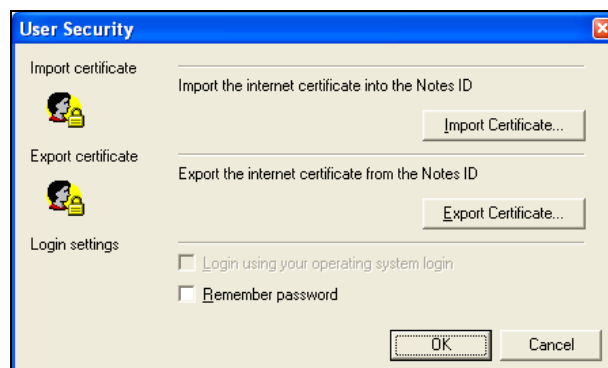


You can also set up how meeting invitations are responded to. The features available here are similar to (but not necessarily completely on par with) all the options available in the Notes client.



S/MIME

S/MIME is available in DAMO to send, read, and receive messages. Under Common security procedures from within the Domino preferences, you import or export Internet certificates into your Notes ID. Keep in mind that these are stored with your Notes ID file, and a plan to keep this backed up and in sync with an installed Notes client should be in force.



Issues

As users of both products know, Outlook and Notes have many differences. Refer to the release notes for Notes and Domino 7.0, specifically in the area Domino Access for Outlook, and then the section titled Domino Access for MS Outlook issues. These notes will outline in detail the interaction between the two software clients, especially in the area of calendar and scheduling.

Read the release notes online at <http://www.lotus.com/idd/doc>. Be sure you completely understand the section on DAMO and Outlook issues before attempting to use the capabilities of DAMO in a production environment.

Summary

This chapter discussed Domino Web Access for Microsoft Outlook (DAMO), a feature that allows you to use Microsoft Outlook to work with Notes mail. We began with a quick review of DAMO basics, and how you can upgrade to DAMO 7. We then reviewed the new features and functionality introduced in the release 7 version of DAMO 7, such as offline address book support, out-of-office management, replication management, calendar and scheduling, and security enhancements.

16

Troubleshooting

Even the best software can have problems. To help fix issues, Notes and Domino provide a systemic set of tools and techniques that can be used for troubleshooting.

Domino Domain Monitoring

Domino Domain Monitoring (DDM) gives administrators the ability to monitor a Domino environment. DDM can also be used to help predict issues before they occur. DDM provides the following features:

- An active monitoring capability that utilizes more than 50 probes.
- Automatic problem determination and analysis.
- Sets of visual indicators that display the most critical problems. Also, there are indicators that display issues that have been resolved.

log.nsf (Server Log File)

Log files have been part of Notes for a very long time. The `log.nsf` file provides many different elements, including views that inform you about databases' size and usage, and others that log replication and mail-routing events.

Events Monitoring (events4.nsf and Event Monitor Task)

The `events4.nsf` database provides you with a set of tools to provide information when problems occur. Here are some of the processes available to manage these problem events.

Event Generator

Event generators gather information by monitoring a Domino task or a system statistic. Events can be generated with DDM integration or can be generated by a specified threshold. Once the event is created, it will be passed to the Event Monitor task.

Event Handler

Once the event is passed into the Domino event task, a handler takes actions. If an event handler has not been defined, the Event Monitor task does nothing. If an event handler has been defined, then the Event Monitor task carries out the operations code (instructions) in the event handler. The Event Monitor task can be started when you start the server, by setting the NOTES.INI variable ServerTasks. Once the task executes, you can set up an Event Notification method.

Event Notification Method

The following list describes some of the notification options available:

- Broadcast reports the event to all users logged onto the server or to a pre-determined group of users according to the option selected.
- Log to a database logs events to a database; statrep.nsf is commonly used.
- Mail mails the event to a mail-in database or a person.
- Log to NT Event Viewer reports the event to the Windows NT event viewer.
- Log to UNIX System Log reports the event to a UNIX system log.
- Run an agent runs a specified agent based on a configured event.
- Run Program runs an add-in program or a specified command. The idea here is to automatically correct problems based on specific or known events.
- Send a console command to the server sends a console command to a server according to a specified event. For example: SHOW TASK, SHOW SERVER.
- Send Java Controller command sends a Java Server Controller command, based on a pre-selected event. The commands that can be sent include 'restart Domino', 'start Domino', and 'shutdown Domino'.
- SNMP Trap sends the event as an SNMP trap.

Domino Web Logging

There are two different web-logging mechanisms that can be used to track web server activity:

- Domlog.nsf
- Text logging

Domlog.nsf tracks various web activities via a Notes database. This is great if you want to log and track data in a Notes database. The downside to this selection is a performance impact on the server. Also be careful; the Domlog.nsf file can get really big, and this can impact on Domino indexer performance.

Text logging can be set up in two modes:

- Extended Common
- Common

The most commonly used Access log format is Extended Common, which logs all web server information to a single text file.

Mail Tracking

Domino provides tools to monitor mail messages:

- **Mail routing event generators:** To monitor a mail network, you can configure mail routing event generators to monitor and gather statistics on mail routes.
- **Tracking mail messages:** Users and Domino administrators can both track mail via a mail-tracking system built into Domino. If enabled, the Mail Tracker Collector (MTC) task reads special mail tracker log files produced by the router. The MailTracker Store database (MTSTORE.nsf) is created automatically when mail tracking is enabled. You can access mail-tracking reports using the Administrator client.
- **Generating mail usage reports:** The Domino MailTracker Store database accumulates information about mail-routing patterns and activities on the server. Reports can be generated into a database, Reports.nsf. Mail usage reports can provide mail-routing information that can be used to resolve problems.



The Server's mail.box Database

There are several tools in the mail.box database (mail.box.ntf) to help you manage email. For example, you can check mail.box for undelivered mail. If you have a large amount of undelivered mail, then there may be a routing problem in your architecture.

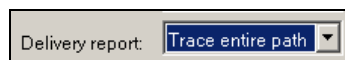
Administrators can edit messages in the mail.box to specify the destination address for resending the original message. The Subject line can also be edited to insert additional information about the status of the message to be sent back to the sender.

Using the following options, you can release dead messages:



Mail Trace

This is a simple tool that anyone can use. Create an email to the address you want to test. Select Delivery options, and the Delivery options dialog box will display. You will see an option for Delivery report. Select Trace entire path. After you send the message, you will receive reports on the path of the email, and whether or not it was successful.



Maps Tool

Do you remember the old NotesView program? This provided a graphical view of mail routing and replication for a particular Notes domain. The Maps program provides many of these features. The Maps program is a server task that you can load to display mail-routing and replication configuration. You can view the Maps program via the Domino Administrator.

TCP/IP Connection Logging

Notes and Domino supports several network protocols. The protocol of choice today is TCP/IP. Notes NRPC base connectivity communicates on TCP port 1352. There are some basic Windows tools that you can use to troubleshoot Notes network issues. Each operating system has a similar set of tools.

Ping provides the ability to test whether another computer is available via TCP/IP. The `Ping` command uses the **Internet Control Message Protocol (ICMP)** echo request to execute each ping request. The `Ping` command syntax is as follows: `Ping Address`, where `Address` can be an IP address or DNS address.

Tracert traces the path taken by TCP/IP packets from a source computer to a target computer. One example would be to trace a path from a Notes client to a Domino server, or even test the basic routing path from one Domino server to another. Tracert uses the ICMP echo request, similar to a `Ping` command: `Tracert Address`

Netstat displays protocol statistics and current TCP/IP network connections. A commonly used syntax is `netstat -n`.

NSlookup returns an IP address for a DNS name. You can use this directly from a command line, or you can just type the name in a command window, and then enter `NSlookup` commands. This is a very powerful utility that can be used to determine an IP address, and can also be used to troubleshoot SMTP routing issues.

SMTP Troubleshooting Examples

SMTP routes mail, based on the TCP/IP protocol. The default port for SMTP mail routing is TCP port 25. SMTP mail routing can work via a point-to-point connection or via a set of DNS Mail Exchange (MX) Records. This is where Notes native mail routing differs from that of Internet standards-based mail routing (SMTP). Notes routes mail based on set of algorithms that includes Notes domains, a network protocol (not just TCP/IP), connection docs, and Notes Named Networks. SMTP works based on TCP/IP, point-to-point connections, DNS, and DNS with MX Records. The following are some simple methods to troubleshoot SMTP mail routing.

- Send an email to your Domino server via a POP client. Yes, it is just that easy. Edit the configuration for your POP email client, and send a message. Look at the logs and/or the target mail box to determine if the message was received.
- Use DNS to find what the MX record is pointing to. For example:

```
c: \> NSlookup
>Set type = MX
```

Enter the name of an email address, for example: `ServerA.TheCompany.xyz`. This will return the name of the target listening server.

- Another method to check a server is via Telnet. The commands are as follows:

```
c: \telnet [Servername.DNS or IP address]
```

You can use the following example for a simple SMTP test on a Domino server with SMTP enabled:

```

Telnet DomainName.com SMTP
HELO TheDomainname.xxx
MAIL FROM: Name@Sourcename.domain.xxx
RCPT TO: areanameinyourdirectory@yourdomainname.xxx
DATA
[Enter data here]
end with a .
QUIT

```

After you enter **QUIT**, the message will be sent. The success of the message acceptance and delivery will depend how the address resolves, whether the target name (**RCPT TO**) is in the directory, whether the SMTP service is listening, and how the SMTP filters are configured in any configuration documents.

NOTES.INI Logging and Debug Parameters

The following is a short list of **NOTES.INI** settings to help troubleshoot various parts of Notes and Domino:

- **Log_AgentManager** specifies whether agent execution is recorded in the log file.
- **LogStatusBar** controls the logging of client status bar messages. This setting is used by developers for debug purposes. The messages can be viewed in the client **log.nsf**.
- **SMTPDebug10** enables the logging of all data received by the SMTP task.
- **Log_Console** enforces logging of server console command output.
- **SMTPDebug** controls the level of console logging performed by the SMTP task.
- **Log_DirCat** logs information about the Directory Catalog task to the Miscellaneous Events view in **log.nsf**.
- **No_Force_Activity_Logging** controls the Statlog task. **Servertasksat5** automatically enables activity logging on all databases.
- **Log_Replication** specifies the level of logging of replication events performed by the current server.
- **HTTPLogUnauthorized**, if enabled, causes the web server to log HTTP 401 (status code) error instances to the server console.
- **Mail_Log_To_MiscEvents** determines whether or not all mail event messages are displayed in the Miscellaneous Events view of the log file.
- **Log_Sessions** specifies whether individual sessions are recorded in the log file.
- **Log_View_Events** specifies whether messages generated when views are rebuilt are recorded in the log file.
- **DIIOPLowLevel** provides additional logging for the DIIOPL task.

- WebAuth_Verbose_Trace can be used to troubleshoot problems with web server user authentication.
- Log_Tasks specifies whether the current status of a server task is recorded in the log file.
- Debug_Roaming, along with Debug_Outfile, collects processing status information to troubleshoot a roaming user problem.
- Log_Update specifies the level of detail of Indexer events displayed at the server console and in the log file.
- Debug_Smart_Upgrade enables all Smart Upgrade status messages.
- Log_Connections reports the TCP/IP status when a session is opened or closed on a Domino server.

There are a large number of Debug parameters that can be used to troubleshoot various issues and problems in a Notes/Domino environment. Some of these include:

- Debug_amgr
- Debug_btree_errors
- Debug_capture_timeout
- Debug_MIMEConversion
- Debug_outfile=C:\debug.txt
- Debug_show_timeout
- Debug_threadid=1

In most cases, it is best to work with IBM/Lotus support before you use any of these parameters. Also, once you have solved your particular problem, work with IBM/Lotus support to determine whether you still need any debug parameters. Many debug parameters will impact on server performance, so be careful if you use these parameters.

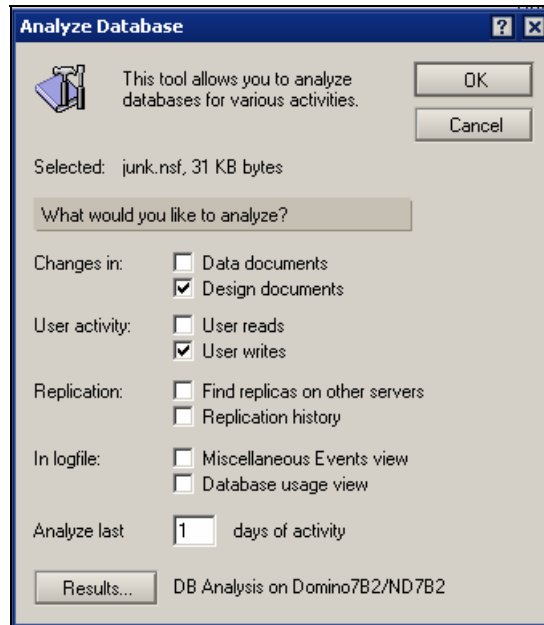
Database Analysis

Using the administrator client, you can perform an analysis on a particular database, to collect database information. Some of this information includes:

- Replication history
- User reads and writes
- Document creations
- Design changes
- Replication additions
- Mail messages delivered by the Domino mail router

Once this data has been collected, it is written into a database based on the Database Analysis template (dba4.ntf).

To use the tool, open the administration client and select the Files tab. Select the database from the list, right-click on it, and then select Analysis. The following dialog box will display:

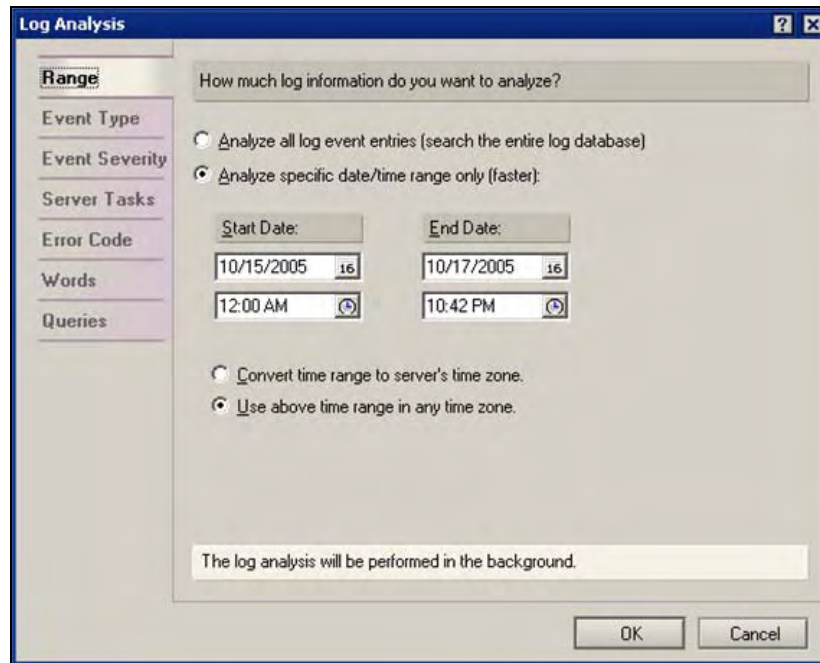


Log Analysis

As stated previously, the server log file (log.nsf) has a lot of important information that can be used for troubleshooting. The downside of the log.nsf database is that it can be really big, and can contain a lot of information. The Domino Administrator includes a tool to help you analyze the log.nsf database. Using this tool, you can analyze the log.nsf database and search for summary data on the following elements:

- Status of particular events
- Type of events
- Severity of the events
- Time the particular event occurred
- A description of the event you are looking for

It is easy to use the log analysis tool. Open the Domino Administrator, and select the Server | Analysis tab. On the right-hand side of the screen will be a dropdown for Analyze. Select Log. The following dialog box will appear:



Click on OK. The analysis will be executed in the background of the Lotus Domino Administration client. The following status bar will appear:

Analyzing Log on Server Domino7B2/ND7B2...

You can use the Administration client to review the log analysis results.

Cluster Analysis

Domino lets you cluster servers. Clusters provide high availability for both Notes and web clients. It is important to analyze the health of a cluster on a regular basis. The Domino Administrator provides the ability to execute a cluster analysis. You can access this tool by opening the administrator client, and selecting the Server | Analysis tab. Then, from the drop-down list on the right side of this screen, select Cluster. A cluster analysis executes, and then presents the results in the Cluster Analysis database (clusta4.nsf) or in a database that you specify. The following data elements can be analyzed and reported:

- **Number of cluster members** reports the number of servers in the cluster.
- **Consistent domain membership** checks that all servers are members of the same domain.
- **Consistent protocols** checks that servers are running the same protocols. Cluster members cannot communicate if they are running different protocols.
- **Required server tasks** checks the ServerTasks setting in the NOTES.INI file for required server tasks.
- **Consistent ACLs** compares the ACLs of replicas throughout the cluster, to check if the ACLs are consistent.
- **Disabled replication** checks if cluster replication is enabled for the databases on the server.
- **Consistent replication formulas** checks for inconsistent replication formulas among replicas that share the same path.
- **Replicas exist within cluster** checks whether databases on the current server have replicas in the cluster.

Predictive Activities Using Server Health Monitor

The Server Health Monitor provides the ability to automatically monitor and calculate the health status of a particular Domino environment. The health-monitoring tools will calculate a set of health statistics. These statistics can then be compared to a set of thresholds. A set of reports will then be made available, using a set of server health ratings. These reports and ratings are stored in the Health Monitoring Database (Dommon.nsf). With Domino 7, the Server Health Monitor is incorporated into the Domino server monitor, which is now part of the Domino Administration client.

Using the Server Health Monitor, the domain administrator can now perform the following activities:

- Modify threshold values for server components
- Create health reports
- Specify which server components to monitor
- Change the purge interval for historical health reports
- Improve the performance of the Server Health Monitor
- Enable statistic alarms
- Exclude a server from being monitored by the Server Health Monitor

Notes System Diagnostic (NSD)

Notes System Diagnostic (NSD) is a Lotus tool designed to gather information about a Notes workstation or a Domino server. NSD was originally designed to be run on various Unix systems, and has been enhanced for use with Unix Services on the other platforms. NSD contains configuration data, as well as a snapshot of server activity at the time it is executed. The NSD program (`nsd.exe` for Win32 platforms, `nsd.sh` for Unix platforms) creates a set of diagnostic files that are placed into a specified directory on a Domino server or a Notes client. NSD will collect and create various data elements.

Domino administrators have the ability to configure how long to keep these diagnostic files (via a policy setting for clients and the Server Configuration document for servers). The `IBM_TECHNICAL_SUPPORT` directory contains data that has been collected using the Domino Configuration Collector and the Automatic Diagnostic Data Collection tool. System information files are automatically generated each time Domino starts when Domino issues an NSD command. Domino collects a variety of information about the system configuration, as opposed to the configuration collector, which collects information about the Domino server configuration. Information such as available memory, available disk space, operating system version, and other related data is collected to determine what has changed when the server begins to have problems.

Server Commands

There are many server console commands that you can use to troubleshoot server issues. The following is short list of various commands that you can use:

- `Show Server` is a simple and powerful command that displays information about the server.
- `Show users` shows how many users are online.
- `Show All ports` displays the configuration for all enabled and disabled ports.
- `Show Cluster` displays the local server's cluster name cache.
- `Show Configuration [notes.ini variable name]` displays the current value for a particular `NOTES.INI` setting.
- `Show Disk space` displays the amount of space available on a disk drive.
- `Show Heartbeat` indicates whether the server is responding.
- `Show Performance` displays per-minute user/transaction values when the Domino server is running.
- `Show Transactions` displays information about NRPC transactions when the Domino server is running.
- `Show Schedule` shows the next time that a server task will run.

- Show Stat shows all of the current server statistics on the console.
- Show Stat *statistic*. * shows a list of statistics by name, and each sub-category of these statistics.
- Show Stat Platform displays individual and cumulative platform statistics for a particular operating system.
- Show Local e displays the region, collation, and CSID (character set ID) settings used by Domino.
- Show Directory lists all database files in the data directory. This is a powerful command and you can use it with the switch unread. This switch will show the status on unread mark replication.
- Show OpenDatabase displays a list of open databases on the server, and gives detailed information for the listed databases.
- Show Port *PortName* displays traffic information about a particular port.
- Show Xdir provides information about each directory a server uses for name resolution.
- Show Dbs displays performance information about a database, such as the number of times a database has been opened, whether the database has been modified, and the number of times a user has had to wait for a lock on the database.
- Show Stat Sem. Timeouts displays the total count and type of Sem.Timeouts messages that occurred since the start of the Domino server.

There are many more commands. Check the Domino Administration help database for the full list.

Summary

This chapter presented information you can use to help troubleshoot your Notes/Domino 7 environment. We listed the diagnostic tools you have at your disposal (such as DDM, event monitoring, and logging), and how each of them can help you analyze, identify, and fix issues that you may encounter. This information is intended more as a handy reference, rather than a detailed explanation of how to address every possible problem or malfunction that you may encounter. For more detailed troubleshooting information, consult the Domino 7 administrator help.

The first step before you upgrade any server is, of course, to check the status of fixes and updates. Open the readme.nsf from each new release of Domino. This database will show the list of fixes and the status of each fix. Also, take the time to check out support issues at <http://www-306.ibm.com/software/lotus/support/>.

17

Case Study

In this chapter, we look at how one site planned for and deployed Notes/Domino 7. The site in question was IBM's own developerWorks Lotus website (<http://www.ibm.com/developerworks/lotus/>). The developerWorks Lotus site (formerly called the Lotus Developer Domain, and even earlier, Notes.net) is the premier web source for information about all Lotus/IBM products, including Lotus Notes and Domino.

developerWorks Lotus

The developerWorks Lotus site provides:

- Discussion forums for asking questions and exchanging ideas about Lotus/IBM products. These include the heavily used Notes/Domino 6 and 7 discussion forum (<http://www.lotus.com/ldd/nd6forum.nsf/>) as well as the still-active Notes and Domino 4 and 5 forum (<http://www.lotus.com/ldd/46dom.nsf/>). The site also offers discussion forums for other Lotus/IBM products, including Sametime, QuickPlace, and SmartSuite. All these discussion forums are built on Notes/Domino technology—the forums themselves are Domino databases, and can be accessed both via the Web and in 'native' Notes/Domino form, via the Notes client.
- Beta forums for pre-release Lotus/IBM products. Beta forums support both public and private programs. As with the discussion forums, the beta forums are hosted by Domino.
- Product pages for all Lotus/IBM products.
- Technical articles covering a wide range of topics of interest to users of Notes/Domino and other Lotus/IBM products.
- The Sandbox for sharing developer code and examples.
- Product showcases and other programs.

Much of the developerWorks Lotus site is powered by Notes/Domino. This demonstrates the power of Notes/Domino as the foundation of a heavily trafficked, '24/7' website. It also gives the Notes/Domino development team an excellent opportunity to deploy early versions of in-progress releases, to help identify issues that arise in large-scale environments (and hopefully fix these issues before they release the product to customers).

developerWorks Lotus often serves as one of the first test sites for new Notes/Domino releases. At any one time, the site is likely running multiple versions of Notes and Domino (to test for compatibility issues), on every major platform supported by Notes/Domino. This can make administering the site very complex (probably more complex than most customer sites), but does allow for thorough testing of all aspects of the Notes/Domino products. At the same time, this testing must be done in a way that presents little or no impact to the large community that depends on the site daily.

Notes/Domino Upgrade Process

Over the years, the developerWorks Lotus team has rolled out many major new releases of Notes/Domino. The team has developed a standard procedure for handling deployments, to help ensure that deployment goes smoothly and quickly, while minimizing the possibility of downtime. The major steps involved in the procedure are as follows.

Plan

This should be rather self-evident, but isn't always the case in all environments (some of which seem to employ a 'ready-*fire*-aim' approach). The team initiates regular meetings well in advance of the actual deployment, to make sure all those involved understand the goals, tasks, and schedules required for the deployment. It is important to understand the new release and the functionality it introduces, and to take full advantage of this capability on the site. It is also important to identify all requirements and prerequisites, along with any known issues (which early in the development cycle can be numerous) and how to work around them.

Deploy on a Non-Production Test Server

The developerWorks Lotus infrastructure includes at least one server dedicated to running test builds. This server does not host any user-visible programs, so any problems it encounters will not impact on the site. This is the first server that Notes/Domino is typically installed upon. If the new release can run on the test server with reasonable reliability, it is ready for wider deployment.

Set Up a Forum to Discuss Issues Found

This is a critical step, one that we highly recommend for all sites in the process of deploying Notes/Domino 7. After all, you have at your disposal the finest communication and collaboration tool in the industry—why not take full advantage of it? This discussion database serves as the central point for exchanging information and resolving issues encountered during the deployment.

Start Small (Deploy on a Cluster Member and Expand)

A cluster member can serve as an important 'baby step' towards full Note/Domino deployment. The cluster member is an actual production, customer-facing server. At the same time, if the cluster member crashes or hangs, failover will immediately relocate user activity to another cluster member. In this way, the new release of Notes/Domino can perform useful, production work, but still with minimal risk of site downtime.

Deploy on One Platform (Win32) and Gradually Move Out to Others (Unix Dialects)

After the new release appears stable on the cluster member, developerWorks Lotus typically upgrades all servers running on a particular platform (usually Windows, initially). As mentioned previously, developerWorks Lotus runs Notes/Domino on all supported platforms. So if the Windows version of the new release performs well, the team can then deploy on other platforms, such as Unix.

Work Closely with Application Designers

Many of the programs offered on developerWorks Lotus, including the discussion forums and Sandbox, are at the core of Notes applications. As the new release of Domino servers is deployed, the administrators work very closely with the application developers to ensure that all site programs continue to run normally. In addition, application designers can begin to incorporate new features offered in the new release.

Watch for Issues, Trends, and Assorted Weirdness

All such issues are immediately recorded in the discussion database, and are brought to the attention of the development team as appropriate.

Document Everything!

For developerWorks Lotus, this often takes the form of an article published on the site, detailing how the team performed the upgrade. In this way, the developerWorks Lotus team can share its experience with customers, to help them avoid some of the problems the developerWorks Lotus team may have encountered. We recommend that you follow a similar process at your site, keeping a running record of all the processes used in the deployment, as well as issues and resolutions. This can help you plan and execute your further upgrades.

Summary

This chapter offered a high-level overview of the process the administrators of the developerWorks Lotus site took when upgrading their hosting environment (which depends largely on Domino technology) to Domino 7. We began with a quick review of the developerWorks Lotus site, and the content and programs it offers. We then described the major steps involved in upgrading the developerWorks Lotus servers to a newer Domino version.

A

Tools and References

Binary Tree Migration Tools for Lotus Notes 7 and Domino 7

For over ten years, Binary Tree has been one of the leading providers of messaging and migration products for Lotus Notes and Domino. Binary Tree's **Common Migration Tool (CMT)** family of products has been used by thousands of companies to migrate several million mailboxes, as well as to migrate, consolidate, and/or enhance existing Lotus Notes and Domino infrastructures.

Migration to Notes/Domino 7

CMT for Notes is a state-of-the-art data-migration product that supports the migration to Notes/Domino 7 from the majority of competitive email environments, specifically Microsoft Exchange and Outlook, Novell Groupwise, Netscape, and other environments supporting IMAP and POP3. CMT has been widely acknowledged as the industry standard for data migration to Lotus Notes. CMT for Notes lets you migrate all mail messages with subject, recipient, date, and body information, and also migrate all attachments. Administrators can choose server mail or local mail (or both); migrate the default profile or let the user choose the profile and message classes to migrate as mail. Users can migrate address books, and view progress in a dialog box. CMT also lets you:

- Migrate repeating appointments
- Migrate meetings, which can then be scheduled after the migration for attendees that have also been migrated to Notes.
- Migrate personal information from Exchange Global Address Lists to Notes Address Book/Directory
- Filter distribution lists from Exchange
- Migrate Exchange data within date ranges to multiple database targets.

CMT for Notes Domains, Servers, Users, and Desktops (CMT for Domains) is a highly advanced all-in-one Lotus Notes and Domino infrastructure migration, consolidation, and enhancement product that has been used by hundreds of organizations of various sizes and profiles to dramatically reduce the complexity, effort, and cost normally associated with Notes/Domino enhancement projects. This tool, a member of Binary Tree's award-winning CMT Suite, allows seamless migration of Domino Servers and Notes Domains, renaming and/or recertification of user names and ID files (including automated upgrade of flat users to hierarchical format), moving and upgrading mail files, and complete update of end users' desktops, including database icons and bookmarks. All activities are performed and monitored from a central administrative database, eliminating the need for any end-user workstation visits!

Coexistence Solutions for Notes/Domino 7 and Microsoft Outlook/Exchange

The most popular and highly functional connectivity solution between Microsoft Exchange and Lotus Notes environments is the Notes Connector for Microsoft Exchange. This solution addresses email, calendar and scheduling, task data exchange, automated directory synchronization, and free/busy lookup between Microsoft Exchange and Lotus Notes environments.

To overcome issues reported by many customers using the Microsoft/Notes connector, Binary Tree's solution greatly enhances fidelity of mail exchange and improves connectivity reliability allowing the two messaging environments to coexist with the highest amount of reliability and fidelity.

For more information, contact Carl Baumann (Carl . Baumann@bi narytree . com).

DNA Network Analysis for IBM Lotus Domino

DNA Network Analysis specializes in efficiency improvement of IBM Lotus Domino/ICT infrastructures and supports customers in implementing technical choices, where topics such as availability, scalability, manageability, and billing all play an important role. As a niche player in the area of Domino infrastructures, DNA is gaining recognition for its success in serving IBM and its customers. It has built up an impressive track record over the past years. (For more information, please visit <http://www.dna-portal.net>.)

DNA Network Analysis for IBM Lotus Domino provides an immediate insight into every Lotus Notes and Domino environment and identifies opportunities that will reduce TCO and boost performance. By utilizing the powerful DNA Network Analysis solution from IBM Lotus Software strategic business partner Trust Factory, IT departments are able to take advantage of a revolutionary new insight into the wellbeing of a Domino infrastructure.

DNA delivers a comprehensive management report along with observations, conclusions, and recommendations in four areas of interest: user demand, system activity, platform health, and deployment integrity. The management report is tailor-made by certified Lotus professionals, and focuses on the specific needs indicated by the customer. All conclusions in the report are supported by pre-formatted Microsoft Excel spreadsheets, available for download through a secure customer login at the DNA portal.

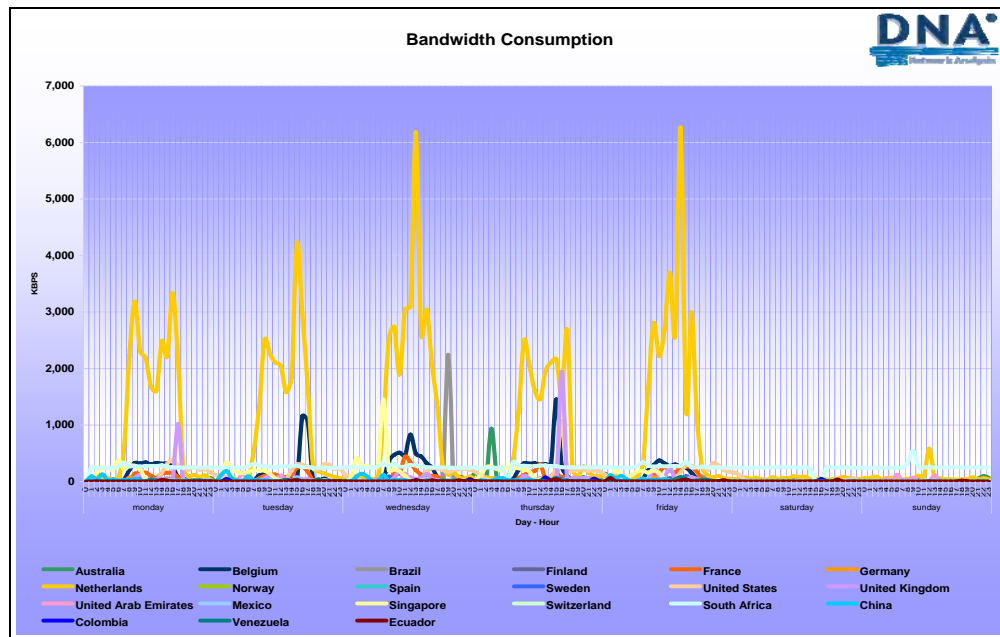
DNA Network Analysis enables customers to clean up and optimize the existing Domino environment, prior to upgrading to Release 7. DNA can produce upgrade and consolidation scenarios that enable customers to take fact-based decisions without room for assumptions. Of course, DNA supports all versions of Domino, from release 4 through 7.

The following are just a few examples of DNA's capabilities. For a complete list of examples, please visit the DNA Portal at <http://www.dna-portal.net>.

End-User Demand

Understanding user demand is of vital importance to an upgrade or consolidation project. Knowing what it is that users are doing, where, when, how much and at which performance levels, allows you to predict the consequences of the changes you are about to make. With this, you can guarantee that users will experience better performance against lower cost, while DNA reports support your efforts with hard evidence.

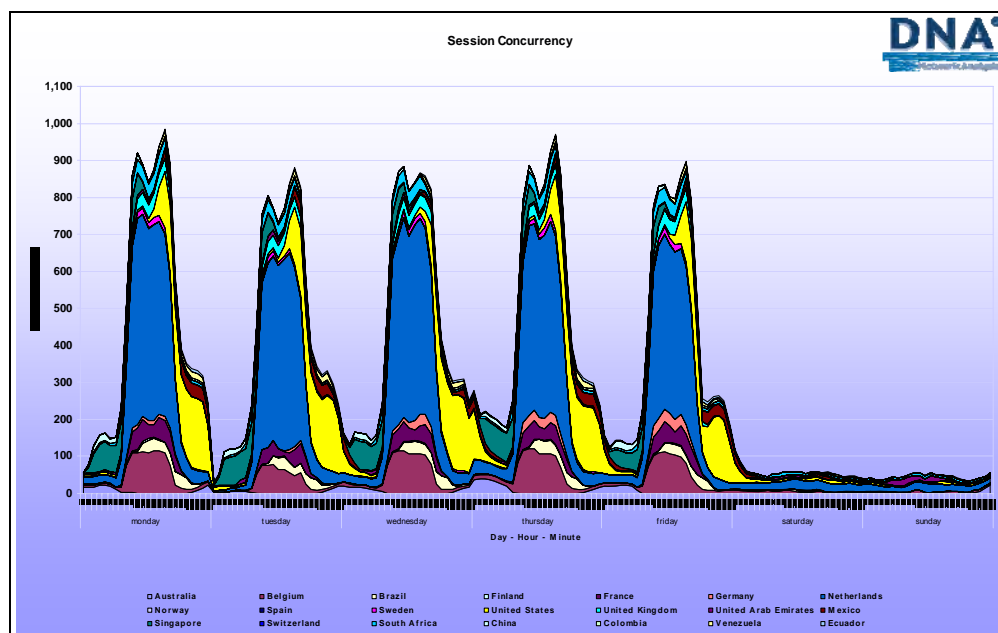
Regarding network infrastructure, for instance, the available capacity to individual office locations is generally known. DNA analysis of traffic generated by end users working with Lotus Notes gives you complete insight into the bandwidth-consumption levels of your network links, as shown in the following graph:



DNA has determined that the average bandwidth consumption per end user can vary anywhere from 4 KB/s to 25 KB/s, with an average of 8 KB/s (server to client). DNA also determined how poorly configured agents and databases can cause exceptionally high consumption levels. DNA spreadsheet reports identify such 'large' consumers, allowing you to take corrective action.

Session Concurrency

How many sessions do users carry out on the Domino servers? When do these sessions take place, and does this result in shortage or surplus server capacity? In the following graph, the session concurrency of an arbitrary organization is shown. Pay particular attention to the fact that some servers receive traffic to process from less than 50 concurrent users (indicating over-capacity).



With Domino release 7 offering higher efficiency on server hardware, these servers could be regarded as candidates for consolidation. DNA produces this concurrency report, while the spreadsheets allow you to calculate the future session concurrency for any consolidation scenario.

Deployment Integrity

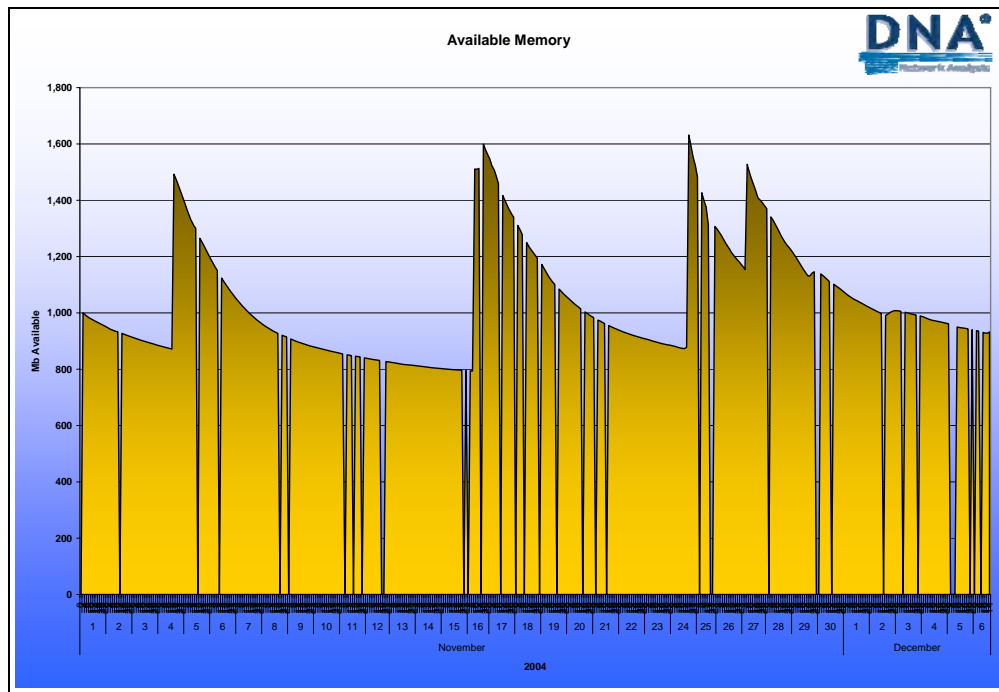
DNA produces standard reports that help you identify cleanup opportunities. Solving such issues not only reduces the workload for support and administrative operations, but also considerably reduces the risks involved in upgrades and consolidation. DNA performs deployment integrity checks, not only to verify all address book documents, but also to verify the deployment of all databases on servers, along with their attributes in terms of configuration and design.

Possible unwanted network and/or replication behavior will be identified, and the background will be found. Possible database deployment issues such as inheritance will be found, including server name, file path, and file name:

Count of replica_id	
error_msg	Total
Duplicate Replica on Same Server	153
Duplicate Template on same Server	30
Replicas acting as different Template	55
Same Replica but Different Inheritance	213
Grand Total	451

Server Platform Health

DNA Platform Health reports provide you with strong, fact-based evidence of how Domino 7 reduces resource utilization for memory, CPU, and disk I/O inside your server park. Perhaps one of the best examples is the evidence that DNA finds regarding memory leaks inside a specific combination of operating system and Domino release:



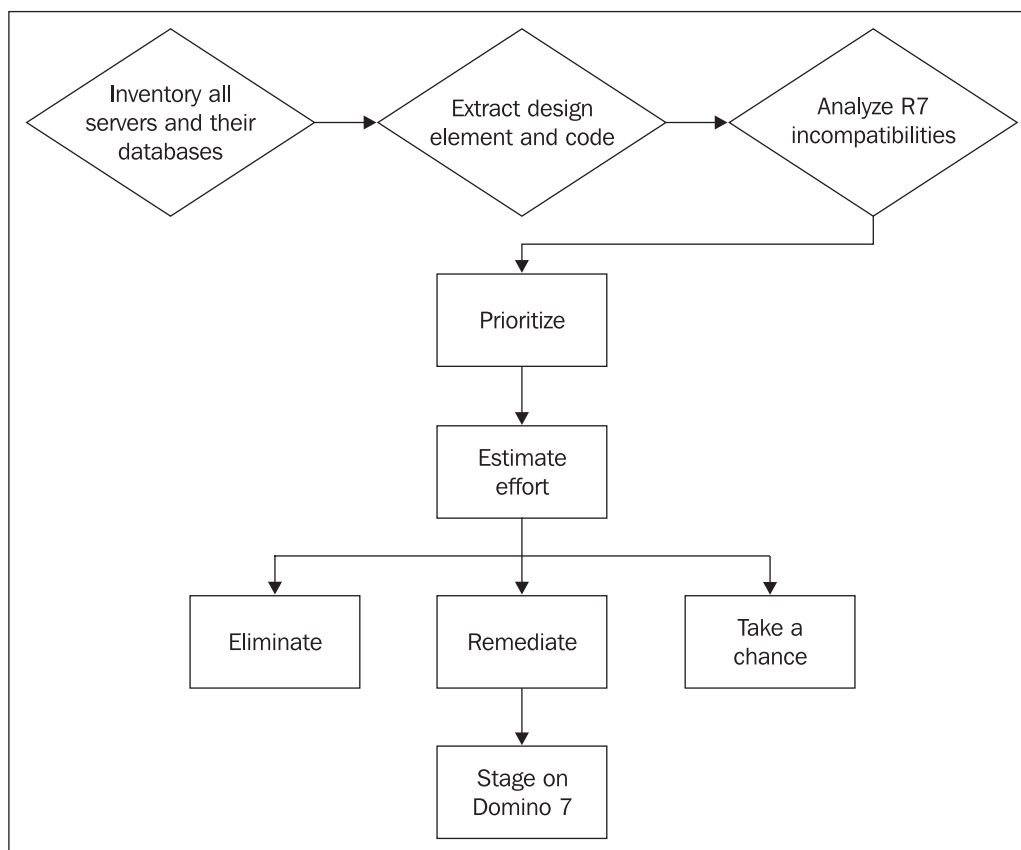
Notice how the server is rebooted on November 4, and loses memory over every 11 days before requiring a new reboot.

Angkor

Since release 2, Lotus/IBM has ensured compatibility when upgrading, but does not guarantee it. The official position is to test what matters. Angkor has found that release 5 and Notes/Domino 6 upgrade-incompatibilities exist, with varying degrees of impact. In its analysis of several large enterprises, Angkor found less than a tenth of one percent incompatibilities among millions of design elements.

Reaching 100% confidence—and avoiding breaking a few hundreds of potentially critical applications in large enterprises—requires thorough testing, an impractical proposition sometimes. This may explain why some companies are still running release 4.

Finding the proverbial needles in the haystack of Notes code requires the use of automated tools such as Angkor, executing release 5, Notes/Domino 6, and some release-7 incompatibility rules against millions of lines of code in a matter of days rather than months. The approach is illustrated by the following:



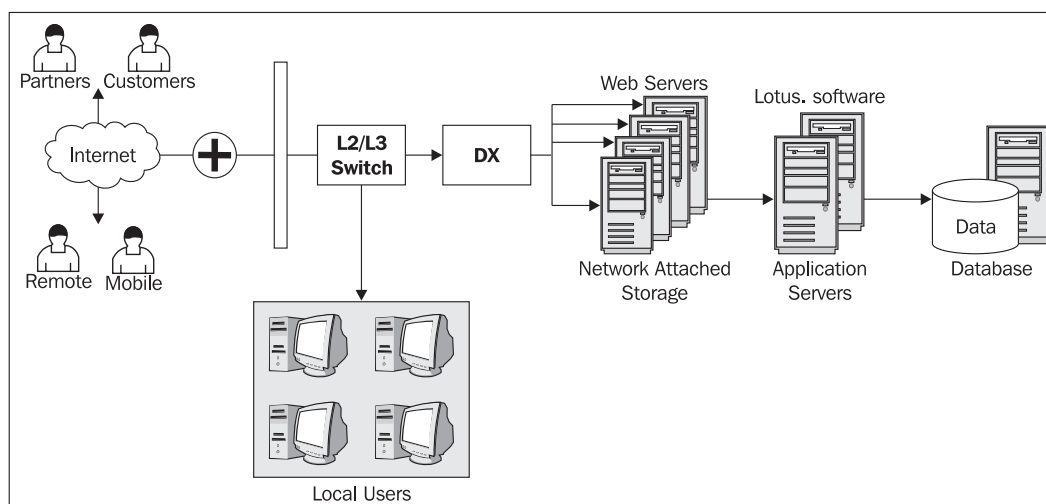
An example of an upgrade incompatibility for release 7 would be code that writes items in the LotusScript Save and PostSave events. If the form uses the new AutoSave feature, code may need to be added in the QueryOpen event to set the default values. Similarly, it would be useful to know all the databases that contain forms with encrypted or authors/readers fields prior to exposing view documents to DB2 queries.

For more information about Angkor, please contact angkor@ad-usa.com.

Securing and Assuring Delivery of Lotus Domino Web Applications

The growing migration toward web-enabled applications and data center simplification is driving the need for a new class of multi-function devices—**application front ends (AFE)**. By incorporating critical functionality to offload web server processing, accelerate web browser sessions, and secure the 'web tier', the Juniper Networks DX series of application acceleration platforms (<http://www.juniper.net/products/appaccel/index.html?from=HomePage-to=ApplicationAcceleration>) delivers unprecedented application performance, security, and availability in an easy-to-manage, flexible platform. Deployed in front of web, application, and database servers, the DX platform replaces multiple point products to deliver a cleaner, more scalable solution that dramatically reduces the complexity of the data center.

The DX integrates multiple functions such as transport connection multiplexing, SSL termination and acceleration, server load balancing, ultra-fast object caching, adaptive compression, and TCP slow-start mitigation to streamline application delivery from the data center. By multiplexing TCP connections, the DX platform reduces thousands of incoming client connections down to just a few, relieving the connection-management burden on back-end servers and allowing them to do what they do best: serve content. By taking over resource-intensive tasks such as session setup and teardown, and SSL termination, the DX platform frees up considerable CPU cycles on the servers, allowing them to process four times the normal number of incoming requests and deliver much faster response times for all users, whether they are local or dialing in over a 56k line.



Juniper is an IBM Business Partner and is continually working with IBM and Lotus to deliver value-added solutions to their joint customers. The IBM Lotus Domino applications benefit greatly from the DX platform, particularly the SSL acceleration capability and the OverDrive feature, which make it possible to define and dynamically apply changes to application behavior "on the fly" without manually rewriting any code. The OverDrive feature delivers an unprecedented level of "application fluency", giving IT the business agility to transform content in order to improve performance, modify workflows, and reduce or eliminate errors.

For more information, contact Juniper Networks at:

Address: 1194 N. Mathilda Ave., Sunnyvale, CA 94089

Phone number: 888-JUNIPER or 408-745-2000

Index

A

ADC, automatic data collection tool.

- about, 137
- data, collecting, 137
- diagnostic directory, 137
- enabling, 139
- working, 138, 139
- See also* FAP, Fault Analyzer Process

admin4.nsf

- administrative requests, 51
- proxy actions, 62
- releases, tracking, 106
- replica ID, 63

Administration process. *See* AdminP

AdminP.

- administration, 49
- administration requests, 62
- administration server, 51
- administration server, primary, 60
- administration server, spoke, 61
- application on a server, updating, 51
- certification log, 51
- clients, upgrading, 107
- components, 49
- mail policies, 88
- name-change management, 64, 171
- proxy actions, 49, 52-60
- releases, tracking, 106, 107
- server task, 49
- See also* admin4.nsf

Angkor

- checking Domino version compatibility, 305

Application Code probe, 24

application integration, Domino on the Web.

- See* WebSphere Portal

architectural use cases, 223

Automatic Diagnostic Data Collection tool.

- See* ADC, automatic data collection tool

autosave, Notes feature, 150

- document recovery, 204
- enabling, 204
- forms, creating, 203
- working, 203

B

browser cache management

- about, 195
- enabling, 196
- installing, 197
- options, 199, 200
- security, 199
- uninstalling, 197, 198

C

calendar and to do settings

- alarms, 85
- basics, 82
- calendar entries in mail views, 84
- calendar invites, autoprocessing, 87
- calendar, managing others', 155
- calendar, right-click options, 157
- display, 83
- features, 155
- filters, 156
- holidays, importing, 176
- room and reservations, 88
- schedule, 90
- todo, 86

certlog.nsf, log database, 51

chat. *See* Sametime

chat transcripts, 166

client policy lock down, 66, 72

cluster analysis, 291

Configuration Collector, 138

CPP, Common PIM Portlets, 247

criteria document, archiving settings, 75

D

DAMO, Domino Access for Microsoft Outlook

- about, 269
- calendar, 280
- encryption, 276
- enhancements, latest, 273
- installing, 270, 271, 272
- issues, 282

- mail file, 279
- new mail notification, 273
- out-of-office management, 276
- password management, 278
- replication management, 277
- S/MIME, 281
- scheduling, 280
- system requirements, 269
- updating to DAMO 7, 270
- user security, 275
- data.** *See* **ADC, automatic data collection tool,**
See also **FAP, Fault Analyzer Process**
autosave
- database event generator, 46**
- Database probe, 25**
- DB2**
 - administration support in Notes, 171
 - management tools, 15
 - statistics, monitoring, 171
- DDM, Domino Domain Monitoring, 15**
 - about, 20
 - filters, 23
 - probes, 22, 170
 - working, 20, 21, 170
- dereferencing, 261**
- desktop policy**
 - basic settings, 72
 - client lock down, 72
 - diagnostics, 74
 - instant messaging, 74
 - Internet preferences, 74
 - Notes client desktop updates, 72
 - preferences, 73, 74
 - Smart Upgrade, 73, 110
- developerWorks Lotus, 295**
- diagnostic directory, automatic diagnostic data collection, 137**
- directories.**
 - architecture, 256
 - Domino Directory, 263
 - Domino Directory, elements, 263
 - features in Domino, 261, 262, 263
 - namespace types, 256
 - uses, 254
 - See also* X.500
 - See also* LDAP, lightweight directory access protocol,
- directory assistance, 261**
- Directory probe, 26, 28**
- DNA Network Analysis**
 - about, 300
 - deployment integrity, 303
 - end-user demand, 301
 - Platform Health, 304
 - session concurrency, 302
- DNS**
 - about, 144
 - uses, 144
- DNS whitelist filters, 94**
- document recovery with AutoSave, 204**
- DocumentContext method, 45**
 - syntax, 45
- DOLS, Domino Off-line Services integration, 176**
- Domino**
 - application integration, 245
 - compatibility tools, 305
 - Configuration Collector, 137
 - configuring for WebSphere, 241
 - configuring for WebSphere Portal, 241
 - DAMO, 269
 - data, presenting on the Internet, 237
 - diagnostic data, automatic collection, 137
 - Domino Designer, 8
 - Domino Web Access, 175
 - enabling IPv6, 145
 - event notification, 35
 - features, 92, 239, 261
 - history, 7, 8, 9
 - internationalization, 194
 - IPv6, enabling, 145
 - Java debugging, 205
 - Java support, 205
 - JSP tag libraries, 248
 - LDAP support, 259
 - mail tracking, 285
 - Microsoft Outlook, 269, 300
 - migration tools, 299
 - name-change management, 63
 - password management, 220
 - performance monitoring, 116
 - policy management, 65
 - rooms and resource manager, 159
 - security, 211
 - Server document, setting for
WebSphere Portal, 244
 - server integration, 240
 - server upgrade use case, 234
 - Smart Upgrade, 101
 - SMTP features, 92
 - troubleshooting, 283
 - upgrading, 101

- upgrading to Domino 7, 223
- web logging, 284
- WebSphere portal, integrating with, 237
- XML services, 201
- Domino Access for Microsoft Outlook.**
See **DAMO, Domino Access for Microsoft Outlook**
- Domino Administrator.**
 - blacklist, 96, 97
 - browser cache management, 196
 - DB2 management, 171
 - event generators, 36
 - features, 15, 169
 - hotkeys, 173
 - log analysis, 291
 - probes, 170
 - TAME integration, 15, 170
 - whitelist filtering, 95, 97*See also* DDM, Domino Domain Monitoring
- Domino Application Portlet, 247**
- Domino Designer**
 - custom actions, 167
 - features, 8, 13, 166
 - history, 8
 - Jave debugger, 166
 - programmability enhancements, 14
 - shared column, 168
 - views, DB2-enabled databases, 13
- Domino Directory.** *See* **directories**
- Domino security.** *See* **security**
- Domino server**
 - enhancements, 16
- DWA, Domino Web Access**
 - browser cache management, 195-199
 - browser cache management, settings, 199, 200
 - configuring, 190
 - Domino Off-Line Services, 176
 - holidays, importing, 176
 - instant messaging, 176, 191
 - instant messaging, options, 192, 193
 - internationalization, 194
 - internationalization, option, 195
 - mail threads, viewing, 179
 - mail, encrypting, 191
 - messages, creating, 189
 - Notes ID, importing, 181-184
 - rooms and resources, 200
 - S/MIME messages, encrypting, 188
 - S/MIME messages, sending, 183,-187
 - S/MIME support, 179, 180
 - security, 175
 - stationary, 177, 178

E

- encryption.** *See* **security**
- ERC, event resolution center, 24**
- event notification**
 - database event generator, 46
 - event generators, 36
 - event handler, creating, 37-47
 - event handler, testing, 47
 - event, creating, 37
 - event, examples, 35
 - severity, event document, 37
 - tracking database, creating, 44, 45
- event resolution center.**
See **ERC, event resolution center**
- events4.nsf**
 - database event, generating, 46
 - event handler, creating, 47
 - probes, 170
- expression rules, Smart Upgrade document, 105,**
See also **Smart Upgrade**

F

- FAP, Fault Analyzer Process, 139**
 - about, 139
 - enabling, 139
 - settings, 140
- filters, DDM**
 - about, 23
- flat names, 256**

H

- heirarchical names, 257**
- hotkeys, 173**

I

- IBM WebSphere Portal.** *See* **WebSphere Portal**
- IBM Workplace Collaboration Services, 250**
- IBM Workplace Managed Client, 251**
- ID recovery**
 - logging, 219
 - mail ID recovery, 219
 - password length, 217
 - password, managing, 220
 - password, obsoleting, 219

- recovery password, 217
- user ID, recovering from
 - administration client, 218

iNotes Web Access.

See DWA, Domino Web Access

instant messaging. *See Sametime*

integrating Domino with WebSphere Portal.

See WebSphere Portal

IPv6

- about, 141-143
- DNS, 144
- Domino, support for IPv6, 143
- enabling on Notes Domino 7, 143, 145
- header, 142
- resource protocols, 144
- zones, 145

J

Java debugging, 205

Java support in Domino, 205

Jave debugger, 166

JSP tag libraries, WebSphere Portal

integration, 248

Juniper Networks, 306

junk mail, 93

K

key rollover, 79, 214

keys, 211

- generating, 213
- public key requirements, 213
- requirements, 213
- specifying, 212

kit document, Smart Upgrade. *See Smart Upgrade*

L

LDAP service, 259

LDAP UNID, 261

LDAP, lightweight directory access protocol

- about, 258
- authentication certificates, storing, 259
- directory service, 259
- Domino support, 259
- features, 258

LEI, Lotus Enterprise Integrator

- about, 17, 131
- features, 133
- installing, 133-137
- real-time access, configuring, 135
- using, 132

lock down, client policy, 66

Lotus Enterprise Integrator.

See LEI, Lotus Enterprise Integrator

Lotus Notes. *See Notes*

LotusScript elements

- admin support, 207
- document support, 207
- IBM Workplace Client support, 208
- XML support, 208

LTPA, lightweight third-party authentication, 262

M

mail archiving policy

- about, 74
- advanced settings, 77
- criteria document, 75-77

mail features, Notes 7

- archiving, 152, 153
- attachments, managing, 151
- autosave, 150
- miscellaneous, 151
- rule processing, 154

mail file ownership, DAMO 7, 279

mail ID recovery, 219

mail policy.

- calendar and todo settings, 82-90
- client disclaimers, 91
- letterhead, 81
- mail preferences, 80
- message disclaimers, 91
- server disclaimers, 91
- See also* calendar and todo settings

mail stationary, 177

mail tracking, 285

mail.box, email management, 286

message marking, 148

Messaging probe, 28

Microsoft Outlook, Domino access.

See DAMO, Domino Access for Microsoft Outlook

N

name reversion, 171

names.nsf

- connection document, adding, 146
- replica ID, 63

namespaces, 256

new mail notification, DAMO, 273

Notes

- administration, 50, 171
- administration, DB2, 171, 172
- calendar and scheduling, 12, 155
- client, 11
- DB2 administration support, 171
- directories, 253
- Domino Web Access, 175
- enabling IPv6, 145
- features, 6, 7, 8, 147, 148
- heirarchical name, 257
- history, 5, 6, 7, 8, 9
- IPv6, enabling, 145
- mail features, 148-154
- NRPC, 146
- password management, 220
- PLATO Group Notes, 5
- policy management, 65
- proxy actions, 52
- Sametime integration, 159
- security, 211
- Smart Upgrade, 101
- status-bar logging, 158
- upgrading, 101
- window management, 147
- window states, saving, 147

Notes Application plug-in

- integration, 250

Notes Formula Language, 206

Notes remote procedure call, 146

Notes security. See security

Notes System Diagnostic, 293

Notes.id file

- certificates, 179
- hosting, 183
- importing, 181-183

NOTES.INI

- auto_save_db variable, 150
- configuration settings,
 - performance testing, 126
- HTTPDomWSAppSpace, 201
- logging parameters, 288, 289

ServerTasks, 49, 233

status-bar logging, 158

TCP_ENABLEIPv6 variable, 145

NRPC, Notes remote procedure call, 146

O

offline address book, DAMO, 274

online awareness, 159

Operating System probe, 29, 30

out-of-office management, DAMO, 276

P

password management, 220

password management, DAMO, 278

Perfmon tool. See also Server.Load

- about, 116
- data, tracking, 118
- logging, 120
- performance, testing, 120
- working, 117

Performance Monitor tool.

See Perfmon tool

See also performance monitoring

performance monitoring.

- data, collecting from a test, 121
- Perfmon, 116
- testing, 120
- testing, collecting data, 121
- tools, 116
- See also Server.Load, See also Perfmon tool*

pilots, 228

PIM, Personal Information Management, 247

policy lock down, 66

policy management, Notes/Domino

- about, 65
- desktop policy, 72
- mail archiving policy, 74
- mail policy, 79
- policy documents, 65
- policy lock down, 66
- registration policy, 67
- security policy, 78
- setup policy, 68
- working, 65

portal integration. See WebSphere Portal

portlet builders, 248

portlets, 237

primary administration server, 60

private whitelist filters, 97

probe, DDM

- about, 22
- application code probe, 24
- configuring, 22
- database probe, 25
- directory probe, 26
- messaging probe, 28
- operating system probe, 29
- replication probe, 30
- security probe, 32
- server probe, 34
- types, 24
- web probe, 35

probes

- configuring, 170
- function, 170

proxy action, 49

- primary administration server, 60

public key requirements, 213

public key requirements, Domino 7 security policy, 78

R

recovery with AutoSave, 204

registration policy

- key length, 67
- settings, 67

replica ID, 63

replication management, DAMO, 277

Replication probe, 30, 31

resource and room management. *See* RnRMgr

RnRMgr

- about, 158, 159
- DWA settings, 200
- loading, 159

room and reservations,

- calendar and todo settings, 88

S

S/MIME support, 179, 183

See also DWA, Domino Web Access

Sametime

- chat options, 161, 162
- chat transcripts, 166
- contact list, 163, 164, 165
- features, 161
- instant messaging, 176, 191

meetings, 160

meetings, setting up, 162

online awareness, 159

options, 161, 162, 191-193

transcripts, 166

SchedMgr, 159

security.

- APIs, 216
- DAMO, 275
- encryption, options, 211
- ID encryption, 211
- ID recovery, enhancements, 217-220
- keys, 211-214
- password management, 220
- security APIs, 216
- Smartcard support, 214, 215
- See also* ID recovery

security policy

- about, 78
- key rollover, 79
- public key requirements, 78

Security probe, 32-34

Server Health Monitor, 292

server integration, Domino on the Web.

See WebSphere Portal

Server probe, 34

Server.Load.

- about, 121, 122
- client, setting up, 123
- configuration settings, 124, 125
- NOTES.INI settings, 126
- scripts, reviewing, 123
- setting up, 123
- starting up, 126
- test, customizing, 124
- test, example, 130, 131
- See also* Perfmon tool

session concurrency, 302

setup policy

- AutoSave, 69
- basics, 69
- instant messaging, 71
- Internet, 70
- mail and news, 70
- miscellaneous, 69
- windows state, 68

shared column design element, 168

Smart Upgrade

- administration, 110
- desktop policy, 73
- desktop policy, modifying, 110, 111
- end-user experience, 112

- end-user message, 109
- enhancements, 15
- expression rules, 105
- kit database, creating, 102
- kit document, administration, 110
- kit document, creating, 103-109
- kit, applying, 108
- kit, location, 108
- process, 101
- server configuration document, creating, 102
- tracking database, 112
- tracking options, 111
- tracking reports, 112
- update database, creating, 102
- working, 101

Smartcards, 214-216

SMTP features

- DNS whitelist filters, 94
- private blacklist filters, 95
- private whitelist filters, 97
- statistics, 98, 99
- troubleshooting, 287, 288

spam, 93

spoke administration server, 61

stationary, mail feature, 177

statrep.nsf, 98

status-bar logging, 158

T

TAME integration, Domino 7, 15, 170

todo list. *See* calendar and todo settings

tracking database, event notification, 44

tracking database, Smart Upgrade, 112

troubleshooting

- database analysis, 289
- DDM, 283
- event monitoring, 283, 284
- log analysis, 290, 291
- log file, server, 283
- mail tracking, 285
- server commands, 293, 294
- server health, monitoring, 292
- TCP/IP connection logging, 286
- web logging, 284

U

upgrade kit document. *See* Smart Upgrade

upgrading to Domino 7

- component tests, 228
- infrastructure, reviewing, 230, 231
- pilots, 228
- process, 233, 296-298
- steps, 233, 234
- use case, 223-230, 234, 235

user IDs, recovering from administration client, 218

W

Web probe, 35

WebSphere Portal

- about, 237
- application integration, techniques, 246-249
- application integration, types, 245
- Domino LDAP, configuring, 241-243
- Domino, configuring, 241
- Domino, integration advantages, 238
- Domino, integration with, 238
- editions, 238
- integration with Domino, advantages, 238
- integration with Domino, parts, 240
- LDAP, enabling to use SSL, 243, 244
- multiplatform, 238
- server integration, 240-245

whitelist filters, 94, 97

- configuring, 95
- statistic, 98

window states, 147

windows state preference, 68

X

X.500.

- about, 258
- LDAP, 258-260
- See also* directories

X.509 support, DAMO, 276

xACL, 66

XML services, 201

xSP, 194

Z

zones

- about, 145
- IPv6, 145