Using policies in Lotus Domino 6

Presented by the Lotus Developer Domain

http://www.lotus.com/ldd

Table of Contents

If you're viewing this document online, you can click any of the topics below to link directly to that section.

1. Introduction 2
2. Overview of policies 4
3. Working with Policy documents 8
4. Assigning an explicit policy 12
5. Policy hierarchy and inheritance 15
6. Roaming User feature 20
7. Real-world scenario 29
8. Setting up a security policy for the organization 35
9. Setting up a desktop policy for the organization 40
10. Mail archiving policy 46
11. Tutorial summary 47

Section 1. Introduction

What is this tutorial about?

Managing a large network can be a daunting task. Domino 6 has many new features that can make the lives of administrators and users easier, including *policies* -- the subject of this tutorial. Policies allow administrators to define rules or policies that can be implemented and enforced automatically across a Domino/Notes environment to manage the configuration, security, and installation of users and Notes clients. We'll begin the tutorial with an overview of some of the more important elements of policies, such as the Policy and policy Settings documents, and the new Roaming User feature. Then we'll walk you through a real-world scenario that shows how to set up policies on multiple servers.

Policies are a powerful and sophisticated new feature with many capabilities. This tutorial focuses on some of the more useful capabilities of policies and shows you how to get started quickly. It's impossible to cover every detail of such a complex feature in the scope of a tutorial, so additional documentation on policies is provided in the Tutorial resources on page 47 section. The topics covered in this tutorial include:

- Creating Policy and policy Settings documents
- Assigning explicit policies using the Person document and the Assign Policy tool
- Using the Roaming User feature
- Using registration policies for registering users
- Using desktop policies to control and update the user's desktop environment
- Using security policies to manage security and define password-management options

Should I take this tutorial?

This tutorial is for Domino/Notes administrators who want to ease the tasks of administering users and Notes clients, simplify and standardize Notes client installations, and make it easier for end users to use Notes clients.

It is recommended that readers be familiar with the following:

- Domino systems administration
- Notes client installation and configuration

Tools

In order to complete the steps in this tutorial, you'll need to have the following applications installed and running properly:

- Lotus Domino 6.0.1 Server
- Lotus Domino Administrator 6.0.1 client
- Lotus Notes 6.0.1 client

Free trial versions of Lotus Domino 6.0.1 and all clients are available for download.

About the author

Kenneth Adams, a Studio B (http://www.studiob.com) author, has been in the Information Technology field for over 17 years and has been working with Lotus Technologies for over eight years. Ken is a dual Principal Certified Lotus Professional (PCLP), certified in both Lotus application development and systems engineering/administration. He is also a CLP in Collaborative Solutions Administration and is certified in Lotus Domino Messaging Administration/Migration. His development experience includes Domino/Notes Designer, LotusScript, HTML, JavaScript, CSS, and others.

Ken also has a solid foundation in LAN/WAN technology having been network certified with a Master CNE (Certified Novell Engineer) and having many years experience in networking. Ken has worked with Domino & Notes since R2, and with practically every Lotus product, including Sametime, QuickPlace, Discovery Server, Domino.Doc, Enterprise Integrator, and more. Ken was a contributing author on the books "Special Edition: Using Lotus Domino/Notes R5" and "Professional Developer's Guide to Domino". He can be reached at: *kadams@kennethadams.com*, or visit his Web site at: http://kennethadams.com/tutorials.

Section 2. Overview of policies

How policies work

Policies allow administrators to define rules or policies that can be implemented and enforced automatically across a Domino/Notes environment to manage the configuration, security, and installation of users and Notes clients. A policy is defined by a Policy document that specifies a collection of policy Settings documents. Each policy Settings document defines settings that apply to the users and groups to which the Policy document is assigned. Once a policy is in place, you can easily change a setting, and it will automatically apply to those users to whom the policy is assigned.

In this section we'll look at the various types of Policy and policy Settings documents and how they work together.

Policy and policy Settings documents

The policies features of Domino 6 are managed using documents stored in the Domino Directory on your Domino servers. The are two types of documents that are used for policies:

- **Policy document:** A Policy document connects individual policy Settings documents to users. The Policy document can be applied to users, groups of users, all users at a particular level in an organization, or an entire organization. Policy documents can be set up in a hierarchy that can inherit settings from one level to the next.

- **Policy Settings document:** A policy Settings document stores settings that are applied to users and groups via the Policy document. You can easily change a policy setting, and it will automatically apply to those users that are assigned to the policy.

How Policy and policy Settings documents work together

There is something of a host/slave relationship between Policy documents and policy Settings documents in that a Policy document uses a policy Settings document (although a policy Settings document can be used in many Policy documents).

Policy documents are assigned to users either explicitly or organizationally, as described in detail in the next panel. You set up an explicit policy by specifying the policy type as Explicit. Next, you assign the policy to users or groups using the Assign Policy tool (see Assign policies with the Assign Policy tool on page 13) in the Domino Administrator client, or to individual users by editing the user's Person document in the Domino Directory (see Assign policies in Person documents on page 12). You set up an organizational policy by specifying the policy type as Organizational and specifying the organization unit in the policy as Name.

When setting up policies, you can create your policy Settings documents first and then create the Policy documents that use them. Or you can create new policy Settings documents while creating or editing the Policy document.

Types of Policy documents

There are two types of Policy documents: organizational and explicit. Below are descriptions of their purposes.

Organizational policies

You use an organizational policy to automatically apply policies to all users under a particular organizational unit. For example, if you have an organizational unit for the East and West Coast (such as East/KennethAdams.com and West/KennethAdams.com, as you'll see later in the Real-world scenario on page 29 section), and you want to assign different settings to each area, you would create two Organizational Policy documents named */East/KennethAdams.com and */West/KennethAdams.com.

If a user moves from one coast to the other, the organizational policy for */West/KennethAdams.com is automatically assigned to the user. The new policy settings will become effective the first time the user authenticates with his or her home server.

Explicit policies

You use an explicit Policy document to assign settings to individual users or groups. For example, if you want to set up a custom Welcome page as well as specific database bookmarks and replicas for a department, you would:

1. Create an explicit Policy document for the department.
2. Create a desktop policy Settings document defining the Welcome page and the database bookmarks and replicas.
3. Assign the policy to the users in the department.

You can assign an explicit policy in three ways: during user registration in Register Person, by using the Assign Policy tool, or by editing the user's Person document.

Types of policy Settings documents

There are five types of policy Settings documents available. Registration and setup settings are used to register users and set up Notes clients, and are only used for those tasks. The other three types are used after a Notes client is set up, and they are used continuously to enforce policies. Here is a complete list of the five types of policy Setting documents along with descriptions of their purposes.

Registration

These settings set default user registration values including user password, Internet address format, roaming user designation, and mail. A policy that includes registration policy settings must be in place before you register Notes users.

Setup

Setup Profiles was a Domino R5 feature, but in Domino 6 it has been enhanced to support new features like using Policy documents to assign settings. Setup policy settings are used only once during the initial Notes client setup to populate a user's settings. Setup settings include servers, Internet browser and proxy settings, database bookmarks, replicas and directory catalogs, dial-up connections, accounts, name servers, applet security, and user preferences.

As with registration policy settings, policies using setup policy settings must also be in place before clients are set up. To change or enforce these settings after a Notes client is installed you must use the desktop policy settings (see below).

Security

You use security settings to define password-management options, including password expiration and synchronization of Notes and Internet passwords, and to set up administration Execution Control Lists (ECLs). ECLs are significantly easier to manage now because they are administered in one place and automatically deployed. You no longer need to send emails to users with a button to refresh ECLs. The result is more effective security.

Desktop

The desktop policy Settings document is similar to the setup policy settings. You use it to manage and update the user's desktop environment and to reinforce setup policy settings. If you make a change to any of the policy settings, the next time a user authenticates with his or her home server, the desktop policy settings are processed. This allows you to update client settings at any time.

Archive

You use an archive policy Settings document to control mail archiving. Archive settings allow you to control if and when archiving is performed, where the archive is stored, and selection criteria used when archiving.

TIP: Setup and desktop policy Settings documents have almost the same available settings. If you want to enforce settings, use desktop policies. If you want to set defaults on new Notes client installs and allow users to change them, use setup policies. If you want to enforce some settings and only set defaults on others, use desktop policies to enforce and setup policies for defaults.
The next section looks at the details of accessing, creating, and editing Policy and policy Settings documents.

Section 3. Working with Policy documents

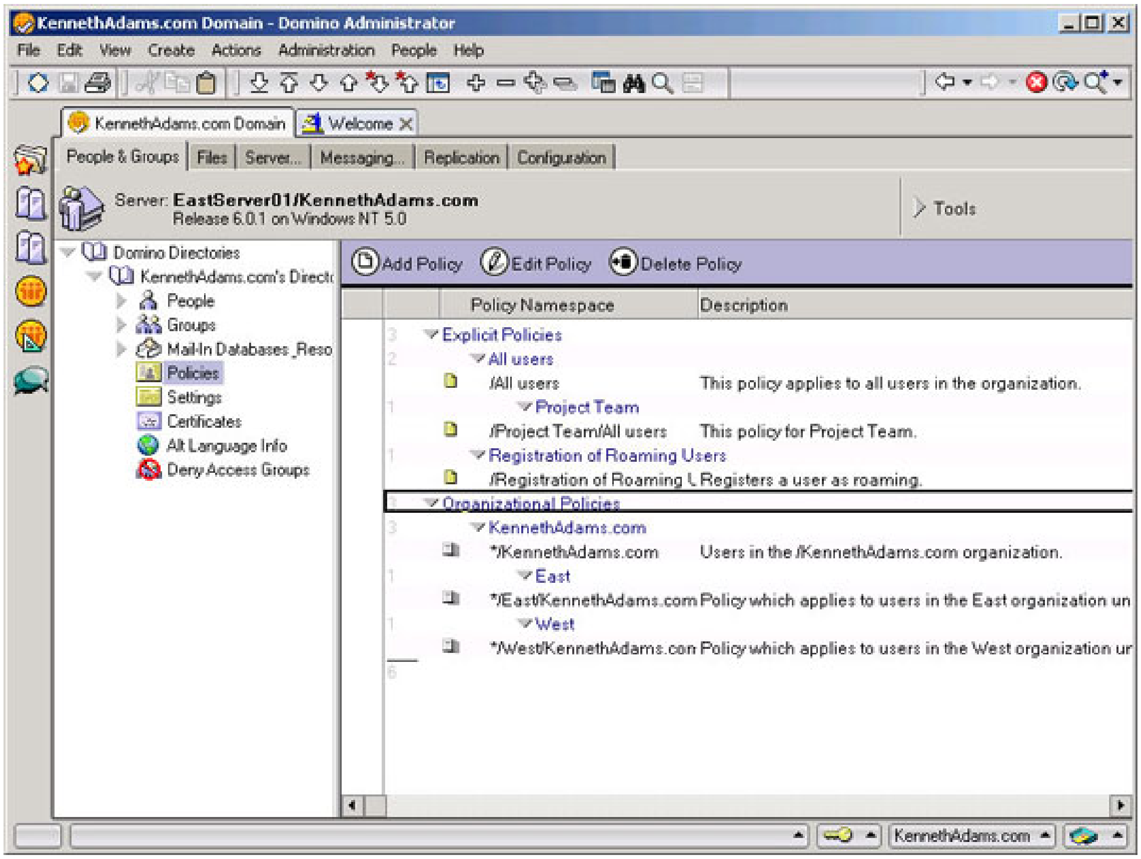
Accessing the Policy documents

All of the Policy and policy Settings documents are stored in the Domino Directory on your Domino servers. You can use either the Domino Administrator client or the Notes client to work with these documents.

Most of Lotus' own product documentation on administration topics is written based on using the Domino Administrator client. Most experienced Domino administrators who have been using Notes for a while (such as old timers like me) use the Notes client for configuration tasks because they can get directly to many administration databases quickly. For the sake of consistency, the examples in this tutorial will use the Domino Administrator.

Follow the steps below to use the Domino Administrator client to access Policy and policy Setting documents:

1. Select a server
2. Click the People & Groups tab
3. Expand the Domino Directories section
4. Expand your directory
5. To display Policy documents, click Policies, or to display policy Settings documents, click Settings



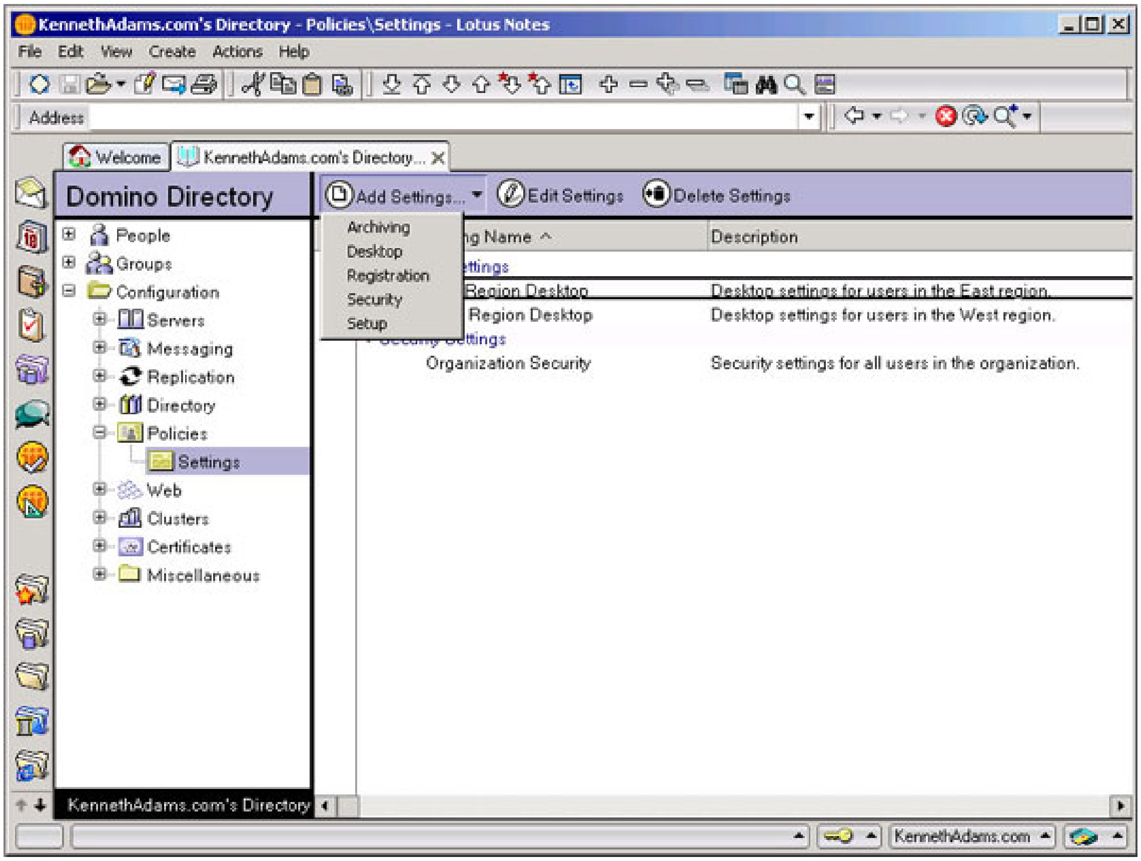
Server: **EastServer01/KennethAdams.com**
Release 6.0.1 on Windows NT 5.0

	Policy Namespace	Description
3	Explicit Policies	
2	All users	
	/All users	This policy applies to all users in the organization.
1	Project Team	
	/Project Team/All users	This policy for Project Team.
1	Registration of Roaming Users	
	/Registration of Roaming U	Registers a user as roaming.
3	Organizational Policies	
3	KennethAdams.com	
	*/KennethAdams.com	Users in the /KennethAdams.com organization.
1	East	
	*/East/KennethAdams.com	Policy which applies to users in the East organization un
1	West	
	*/West/KennethAdams.con	Policy which applies to users in the West organization ur
6		

Creating policy Settings documents

All policy Settings documents are displayed in the Settings view of the Directory, categorized by type (archiving, desktop, registration, and so on). To create a new policy Settings document:

1. Open the policy Settings view in the Domino Directory
2. Click the Add Settings button
3. From the pull-down menu, select the type of policy Settings document you wish to create
4. Fill out the new policy Settings document
5. Click the Save & Close button

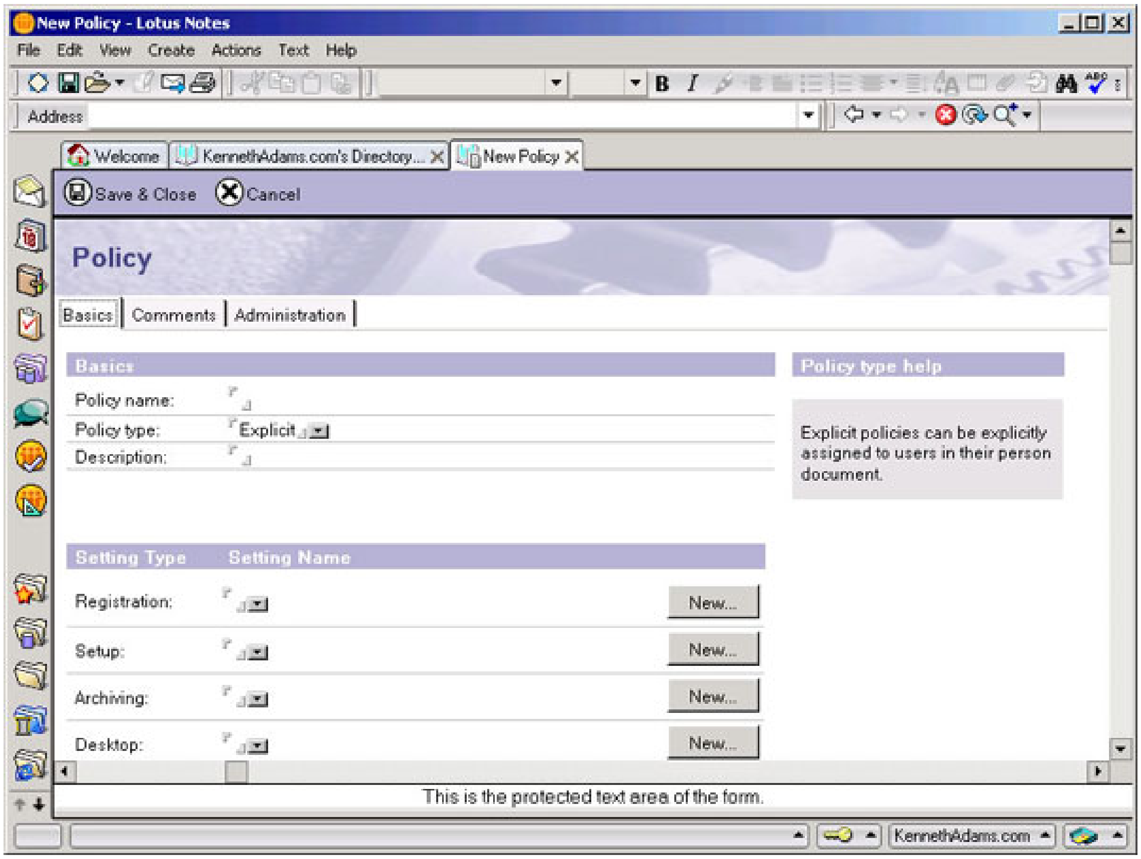


g Name ^	Description
ttings	
Region Desktop	Desktop settings for users in the East region.
Region Desktop	Desktop settings for users in the West region.
ttings	
Organization Security	Security settings for all users in the organization.

Creating Policy documents

All Policy documents are displayed in the Policies view of the Directory. To create a new Policy document:

1. Open the Policies view in the Domino Directory
2. Click the Add Policy button
3. Fill out the new Policy document
4. Click the Save & Close button



Basics

Policy name:	
Policy type:	Explicit
Description:	

Policy type help

Explicit policies can be explicitly assigned to users in their person document.

Setting Type	Setting Name
Registration:	
Setup:	
Archiving:	
Desktop:	

This is the protected text area of the form.

Next, we'll look at the different ways available to assign an explicit policy.

Section 4. Assigning an explicit policy

Assigning an explicit policy overview

As discussed earlier, an explicit Policy document is used to assign settings to individual users or groups.

There are three ways to assign explicit policies manually:

1. During user registration
2. Using the Assign Policy tool
3. Editing the Person document

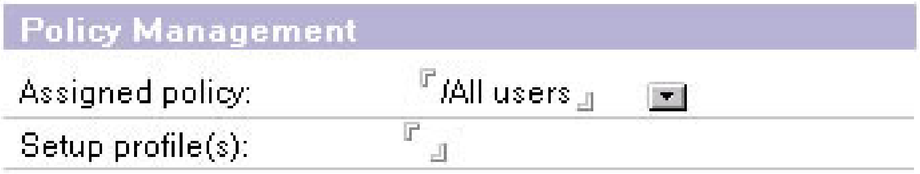
All three methods can be used to assign policies to individual users. You can use the Assign Policy tool to assign policies to groups .

For details on how to assign policies during user registration, see Using registration policy while registering new users on page 32 .

Assign policies in Person documents

You can assign any explicit policy to a specific person by editing their Person document in the Domino Directory. All settings in security, desktop, and archive policy Settings documents will be applied to the user. Remember that registration settings cannot be applied at this point, because the user already exists, and setup settings only apply when the Notes client is set up.

1. Open the Domino Administrator client
2. Click the People & Groups tab
3. Expand the People view
4. Select the name of the person you want to edit
5. Click on the Edit Person button
6. From within the Person document, click the Administration tab
7. Under the Policy Management section, edit the Assigned policy field



Policy Management

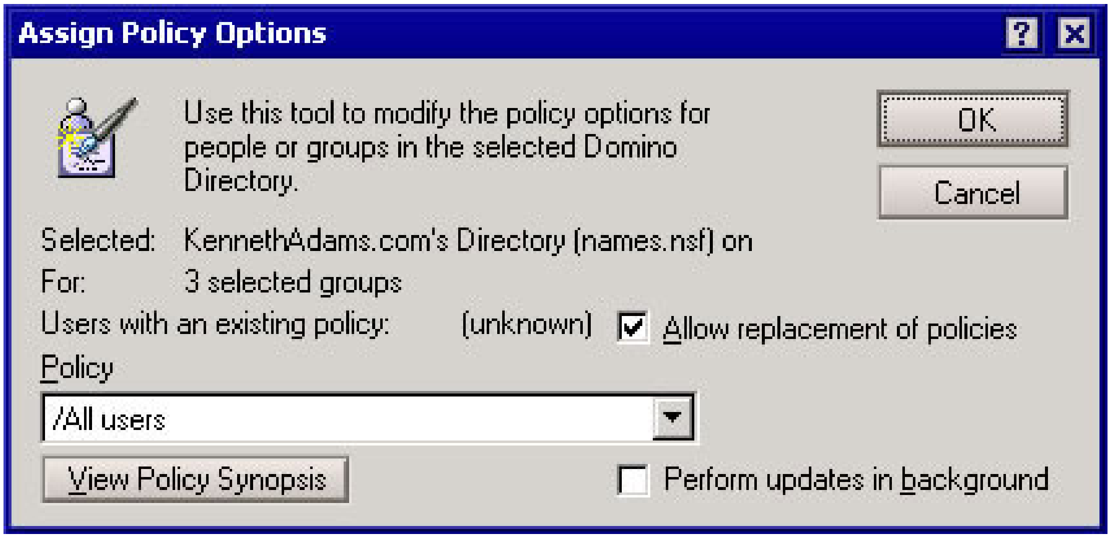
Assigned policy:	/All users
Setup profile(s):	

8. Click the arrow button next to the field to select a policy
9. Click the Save & Close button

Assign policies with the Assign Policy tool

The Assign Policy tool is very useful for making policy changes to multiple users or groups. When you change the explicit policy for a user or a group using this tool, you have the option of viewing the way the policy assignment change impacts the effective policy for that user or group.

1. Open the Domino Administrator client.
2. Click the People & Groups tab.
3. Expand the People or Groups view.
4. Select the name of the people or groups you want to edit.
5. Expand the Tools pane. If you are in the People view, expand the People tools. If in the Groups view, expand the Groups tools.
6. Select the Assign Policy tool.



Assign Policy Options

Use this tool to modify the policy options for people or groups in the selected Domino Directory.

Selected: KennethAdams.com's Directory (names.nsf) on

For: 3 selected groups

Users with an existing policy: (unknown) ☑ Allow replacement of policies

Policy

/All users

□ Perform updates in background

7. If you want to replace an existing policy with a new one, select the Allow replacement of an existing policy checkbox.
8. Select the explicit policy you want to assign from the pull-down list in the Policy field.
9. If you are assigning policies to a large number of users, you can select the Perform updates in background checkbox.
10. To see the new effective policy, click the View Policy Synopsis button. The Choose Organizational Policy dialog box will appear, which will allow you to choose the organizational policy you want to combine with the explicit policy to view the new effective policy.
11. Click the OK button to assign the policy.

The next section looks at policy hierarchy and inheritance.

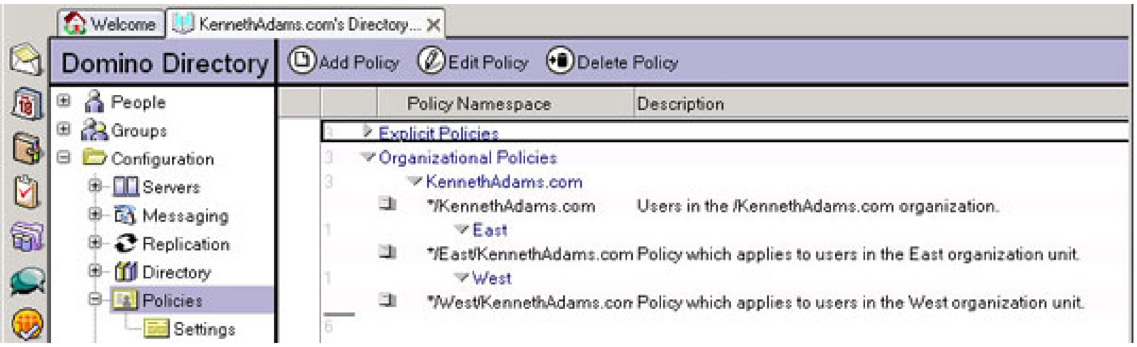
Section 5. Policy hierarchy and inheritance

Policy hierarchy and inheritance overview

Policies can be set up in a hierarchy, using parent-child relationships between Policy documents. In a policy hierarchy, Policy documents build the relationships, and policy Settings documents determine the values of the settings based on their position in the hierarchy.

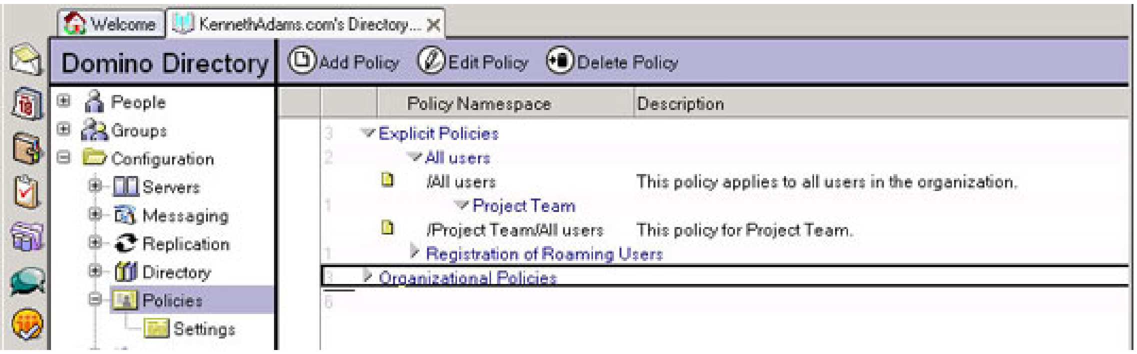
Child policies can inherit the settings of their parent policy, and parent policies can enforce settings in their child policies. You define the inheritance and enforcement in the policy Settings documents. Using inheritance and enforcement, you can control the effective settings that are applied to a user.

With organizational policies, the hierarchy of policies is determined automatically based on the organization's naming hierarchy. You would use the organization naming hierarchy in the Policy Name of the Organizational Policies. For example, the organizational policy named */East/KennethAdams.com is the child of the organizational policy named */KennethAdams.com. Therefore, if a user is named John Doe/East/KennethAdams.com, they will automatically receive the settings of the policy Settings documents in the */East/KennethAdams.com Policy document, and inherit the settings in the */KennethAdams.com policy.



Policy Namespace	Description
Explicit Policies	
Organizational Policies	
KennethAdams.com	
*/KennethAdams.com	Users in the /KennethAdams.com organization.
East	
*/East/KennethAdams.com	Policy which applies to users in the East organization unit.
West	
*/West/KennethAdams.con	Policy which applies to users in the West organization unit.

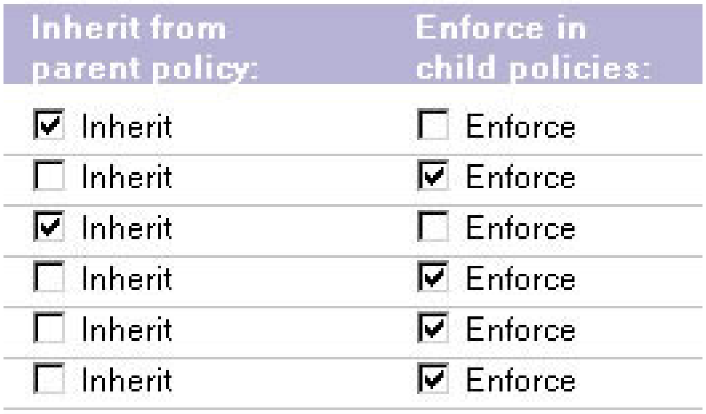
Explicit policies do not follow the organizational structure, so when you create explicit policies, you build in the hierarchy yourself, using the policy names. For example, if you have an explicit policy named /All Users and create another explicit policy named /Project Team/All Users, the /Project Team/All Users policy becomes the child of the /All Users policy.



Policy Namespace	Description
Explicit Policies	
All users	
/All users	This policy applies to all users in the organization.
Project Team	
/Project Team/All users	This policy for Project Team.
Registration of Roaming Users	
Organizational Policies	

Setting inheritance and enforcement in policy Settings

The inheritance from a parent policy and the enforcement in child policies are controlled by settings in the policy Settings documents. Each setting displays checkboxes next to them, which allows you to enable or disable the inheritance or enforcement.



Inherit from parent policy:	Enforce in child policies:
☑ Inherit	□ Enforce
□ Inherit	☑ Enforce
☑ Inherit	□ Enforce
□ Inherit	☑ Enforce
□ Inherit	☑ Enforce
□ Inherit	☑ Enforce

To enable, simply select the option.

The effective policy

The effective policy for a user is a set of policy settings that are dynamically calculated at the time of the execution of the policies. The settings of an effective policy may come from many different policy Settings documents that are assigned based on the policy hierarchy that you have defined.

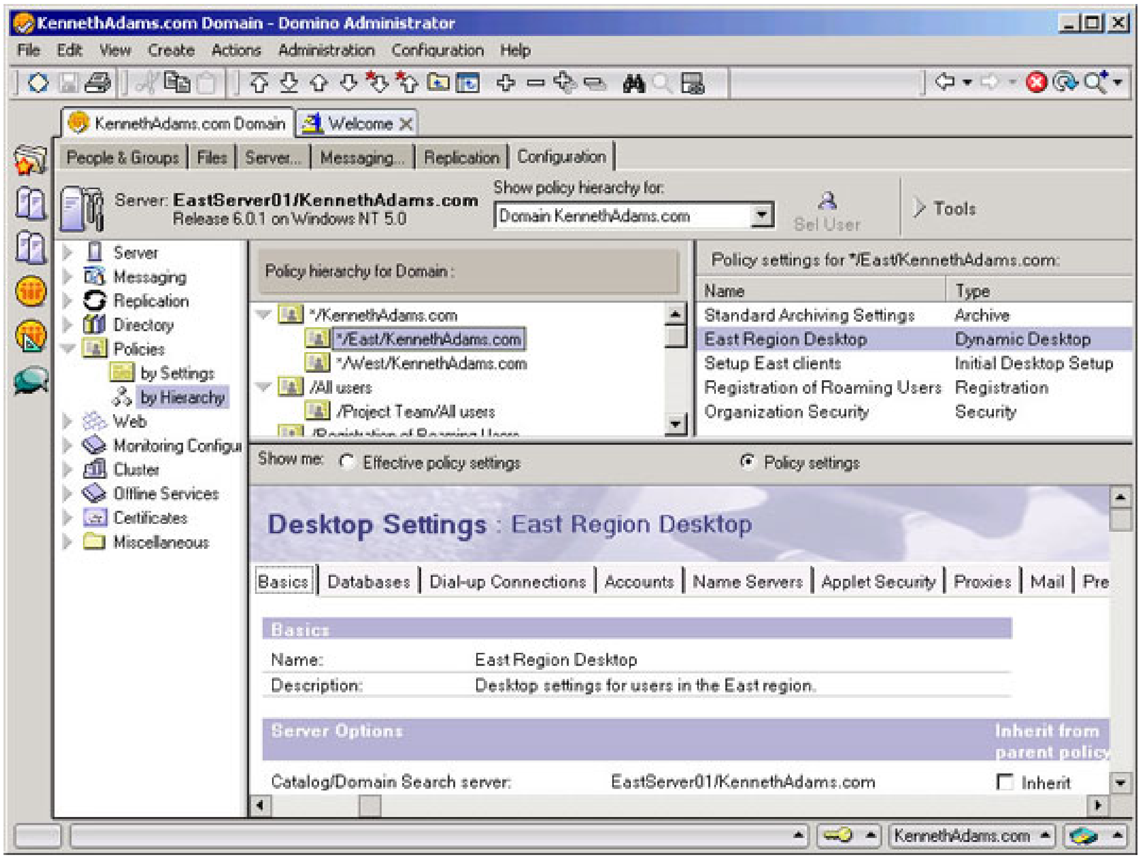
The calculation of each user's settings is determined by stepping through the hierarchy of policies to determine the effective policy for each user.

Using the Policy Viewer

The Policy Viewer tool provides an easier way to view a sophisticated policy implementation. This tool allows you to view the relationships of policies in a hierarchy that you can drill down into, or view by policy settings to see which levels of a hierarchy use them.

To open the Policy Viewer:

1. Open the Domino Administrator client.
2. Click the Configuration tab.
3. Expand the Policies view.
4. Click the By Hierarchy view or the By Settings view.



Server: EastServer01/KennethAdams.com
Release 6.0.1 on Windows NT 5.0

Show policy hierarchy for: Domain KennethAdams.com

Policy settings for */East/KennethAdams.com:

Name	Type
Standard Archiving Settings	Archive
East Region Desktop	Dynamic Desktop
Setup East clients	Initial Desktop Setup
Registration of Roaming Users	Registration
Organization Security	Security

Show me: ○ Effective policy settings ● Policy settings

Desktop Settings : East Region Desktop

Basics

Name: East Region Desktop
Description: Desktop settings for users in the East region.

Server Options — Inherit from parent policy

Catalog/Domain Search server: EastServer01/KennethAdams.com □ Inherit

To view the policy Settings documents or effective policy settings for a particular hierarchical level:

1. Open the By Hierarchy view.
2. Select a level in the Policy hierarchy for Domain pane in the top left.
3. The policy Settings documents for that level will display in the Policy settings for... pane in the top right.
4. To view a policy Settings document, select it in the top right pane. That document will display in the bottom pane.
5. To view the impact of inheritance and enforcement, select Show me Effective policy settings in the bottom pane.

To see which hierarchical levels use which policy Settings documents:

1. Open the By Settings view.
2. Select a policy Settings document in the Policy settings for Domain pane in the top left.
3. The levels that use that document will display in the Policy hierarchy using... pane in the top right, and the document will display in the bottom pane.

Exceptions to policies

You use an exception to allow the user to override a policy setting that would normally be enforced throughout an organization. Exception policies are the way you would give someone in an organization special features and capabilities; perhaps a user's job responsibilities require them to have a different Welcome page or specific bookmarks.

To create an exception policy, you:

1. Create an organizational or explicit Policy document
2. Assign an exception attribute to that Policy document, by selecting the Exception Policy checkbox on the Administration tab
3. Include the policy Settings documents that have the settings to exclude

When you assign the exception policy to a user, it will exempt the user from enforcement of the settings in the assigned policy Settings documents.

In the next section, we'll take a look at one of the more valuable new policy features available in Domino 6.0.1.

Section 6. Roaming User feature

Overview of Roaming User feature

The Roaming User feature allows users to access their customized settings and personal information automatically from any Notes client on any computer. Roaming User is a feature that is new to Domino 6.0.1. The initial Domino 6 release did not include this feature, although the Domino Administrator 6 Help did document it. The feature's release was delayed so that it could be completed and be put through extensive quality testing. To utilize this feature you must first upgrade your home/mail Domino servers and Notes clients to 6.0.1.

What is Roaming User?

In the past, users who needed access to Notes from more than one computer were not able to automatically share their personal files and desktop settings between computers. Some of the possible scenarios where this was a problem included:

- Sharing files among multiple computers in the office: desktop, notebook, terminal server, and so on
- Accessing files from a home computer
- Accessing files from a remote work location like a customer site
- Migrating to new computer hardware

Some of the personal files and settings include that a user might want to access and share include:

- Personal Address Book/Contacts (names.nsf)
- Bookmarks and Welcome pages (bookmark.nsf)
- Personal Journal (journal.nsf)
- Notes ID file (notes.id)
- User Preferences
- User Dictionary

Before the Roaming User feature, it was technically possible to synchronize some of this data between multiple Notes clients, but it was problematic and difficult to set up. Domino 6.0.1's new Roaming User feature completely automates the process and does a thorough job of supporting roaming users.

The Roaming User feature is not only supported on Notes 6.0.1 clients but also on

Web browsers accessing Domino applications that support Domino Off-Line Services (DOLS). The feature is also supported on Domino server clusters.

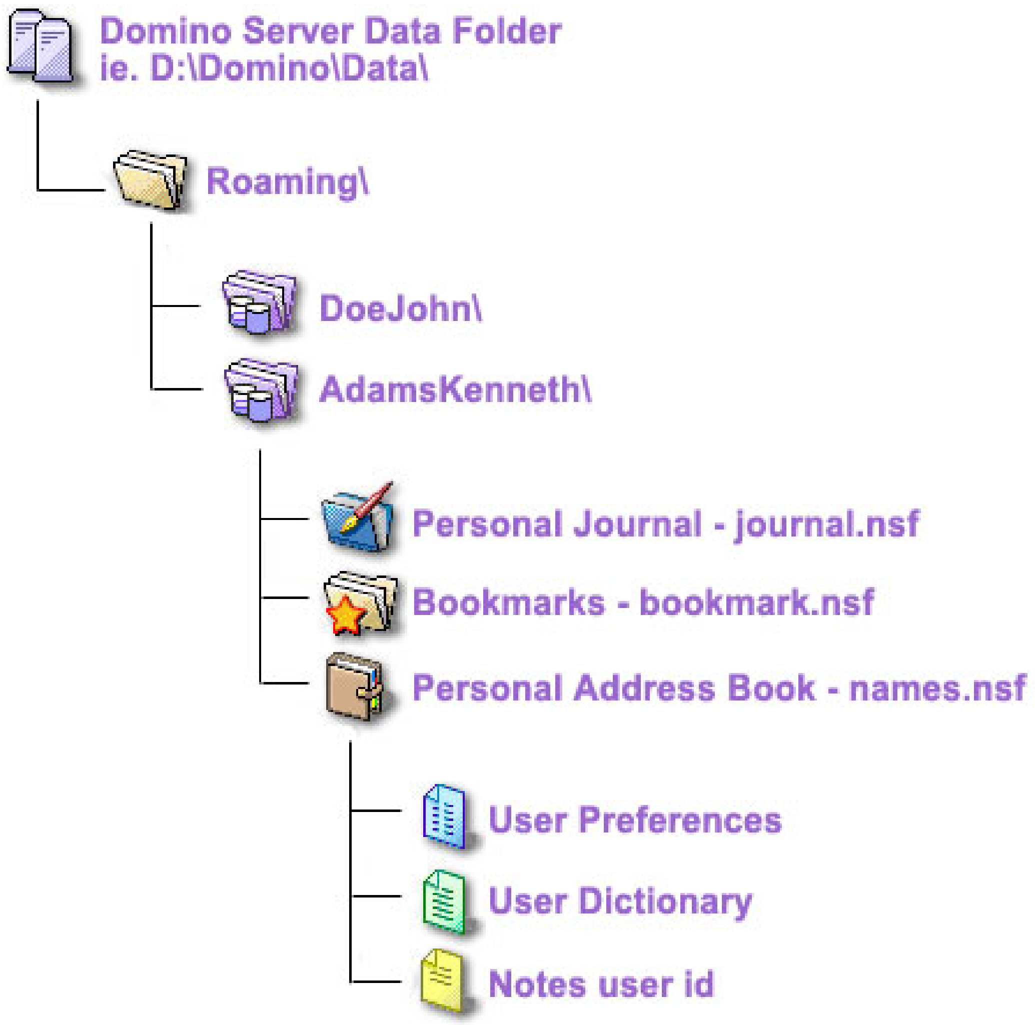
TIP: The Roaming User feature is also useful for providing a method of backing up a user's personal files. Even if the user doesn't need roaming features, it's a good idea to enable it anyway so you always have a backup of the user's personal data in the event of a computer failure or loss. Recovering the user's personal Notes files then becomes as easy as configuring the Notes client.

How Roaming User works

The Roaming User feature can be enabled for specific users in two ways:

- When registering new users, you can use the Register Person tool in the Domino Administrator client.
- With existing users, roaming can be enabled using the Domino Administrator client.

Once enabled for a user, data for the roaming user replicates between the user's computer and a Roaming User server where these files are stored. The administrator determines the folder on the Domino server where the files are stored when roaming is enabled. The administrator can specify the base folder for roaming files (the default is Roaming\) and the naming convention that will be used for user folders under the roaming base folder. For example, some of the naming conventions available for user folders are LastNameFirstNameMiddleInitial, FirstInitialLastName, and so on.



When a roaming user connects from a different Notes client, the Notes client automatically retrieves the user's ID file, Personal Address Book, bookmarks, and journal from the Roaming User server. Changes the user makes in these files replicate to the Roaming User server so that other Notes clients can be kept up to date.

The specifics of the user's Roaming User configuration are stored in the user's Person document in the Domino Directory on the servers. These options cannot be edited in the Person document, except for the Clean-up setting, and can only be changed via the Assign Roaming Profiles tool.

The next few panels walk you through the process of setting up users as roaming users.

Setting up users as roaming users

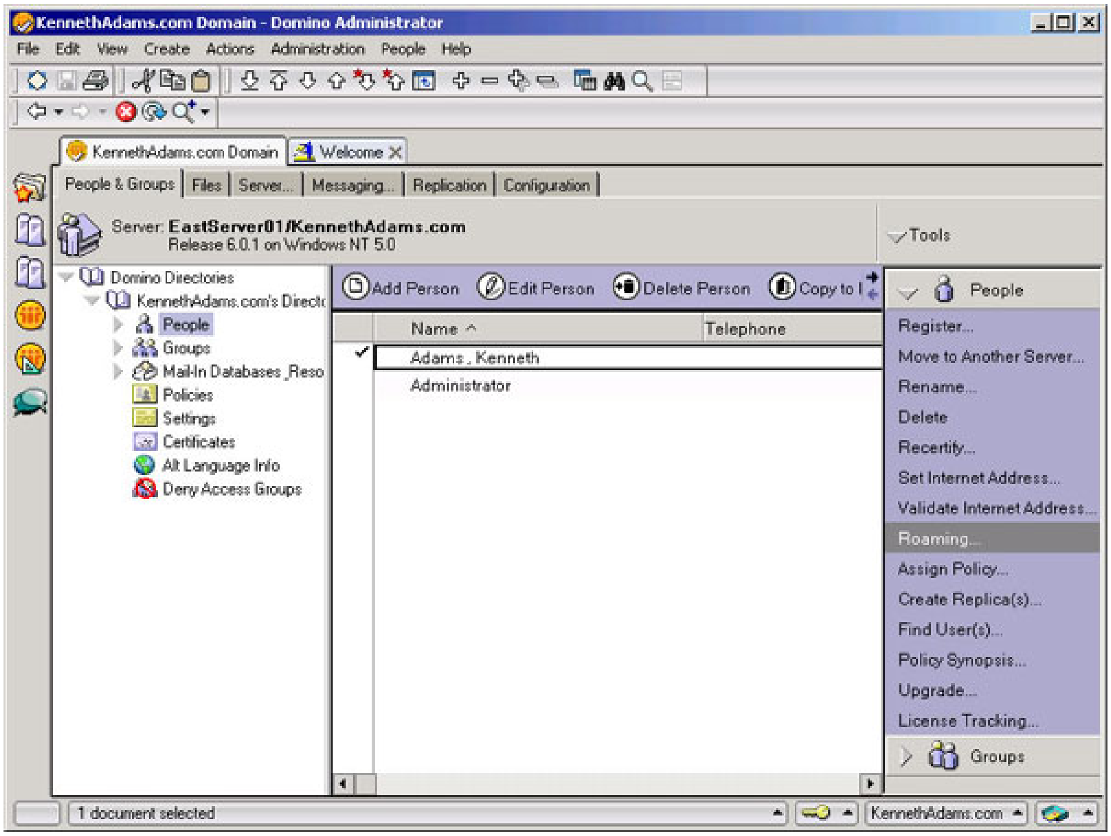
There are two options for setting up a user to use the Roaming User feature of Domino 6.0.1. You can enable roaming during registration, or, if the user already exists, you can use the Domino Administrator client. For general information on the new Roaming User feature, see Roaming User feature on page 20 .

TIP: Enabling roaming for all users during registration is a good practice. Enabling during registration will ensure that all the personal files are created; by default, a Journal is not created on a non-roaming user's computer until the user creates it. It also gives you the advantage of having backups of users' personal files, and allows you to easily set up a new computer with the Notes client for users whenever you need to, without having to manually move the personal databases and Notes.ini and ID files.

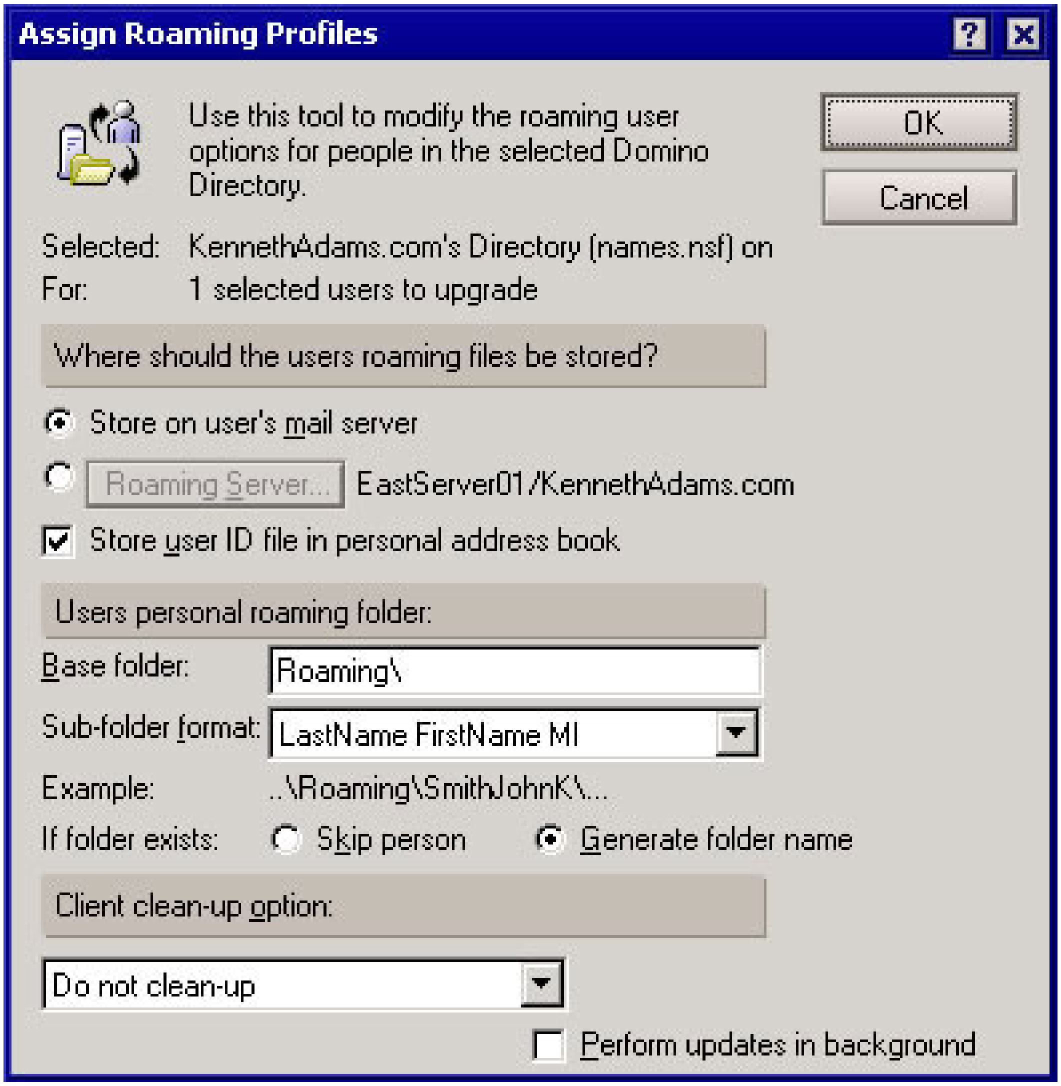
Setting up existing users as roaming users

To enable roaming for an existing user:

1. Open the Domino Administrator client.
2. Select the server you wish to administer.
3. Click the People & Groups tab.
4. Expand Domino Directories and your Directory.
5. Click the People view.
6. Select the user or users for which you wish to enable roaming.
7. Expand Tools, then People, and select the Roaming tool, or select the menu command **People => People => Roaming**.



8. The Assign Roaming Profiles dialog box will appear.



Use this tool to modify the roaming user options for people in the selected Domino Directory.

Selected: KennethAdams.com's Directory (names.nsf) on
For: 1 selected users to upgrade

Where should the users roaming files be stored?

● Store on user's mail server
○ Roaming Server... EastServer01/KennethAdams.com
☑ Store user ID file in personal address book

Users personal roaming folder:

Base folder: Roaming\
Sub-folder format: LastName FirstName MI
Example: ..\Roaming\SmithJohnK\...
If folder exists: ○ Skip person ● Generate folder name

Client clean-up option:

Do not clean-up

□ Perform updates in background

9. Under the Where should the users roaming files should be stored? heading, use the defaults or select your own options as follows:
   - The Store on user's mail server field is checked by default. This stores the user's roaming files on the user's mail server. Generally, using this option is best so that all the user's files are stored on the same server.
   - Click the Roaming Server button to specify the server on which to store the roaming files. This is useful if you wish to use a specific server for all roaming user files.
   - The Store user ID in personal address book field is checked by default. This places the user's ID in their own local personal address book. Storing the ID in the personal address book is a good idea because it can simplify the set up of Notes on additional computers and DOLS.
10. Under the User's personal roaming folder heading, use the defaults or select your own options as follows:

- In the Base folder field, enter the name of the folder in which to store the user's roaming files. The Roaming folder is the default.
- In the Sub-folder format field, enter the format to use when naming the roaming user's personal subfolder, which is created under the Base folder. LastName FirstName MI will provide the most unique name and help avoid name conflicts. It was also allow the folders to be viewed alphabetically by last name.
- In the If folder exists field, check Generate folder name to generate a new folder name. If the folder already exists, checking Skip person will not enable roaming.

11. Under the Client clean up options heading, leave the default Do not clean-up. This will not clean up Roaming User files. For more details see Create the registration policy Settings document on page 30 .
12. Click the OK button. The request to enable roaming on the selected users will be queued in the Administration Requests.

How enabling roaming for existing users is processed

Enabling roaming initiates a sequence of processing steps that are completed by the Administration Process on the servers. The status of the requests can be viewed in the Administration Requests database. The Administration Process works in conjunction with the user's Notes client. When enabling an existing user, the Notes client must complete the replication of the personal files before the roaming enablement process can be completed by the Administration Process.

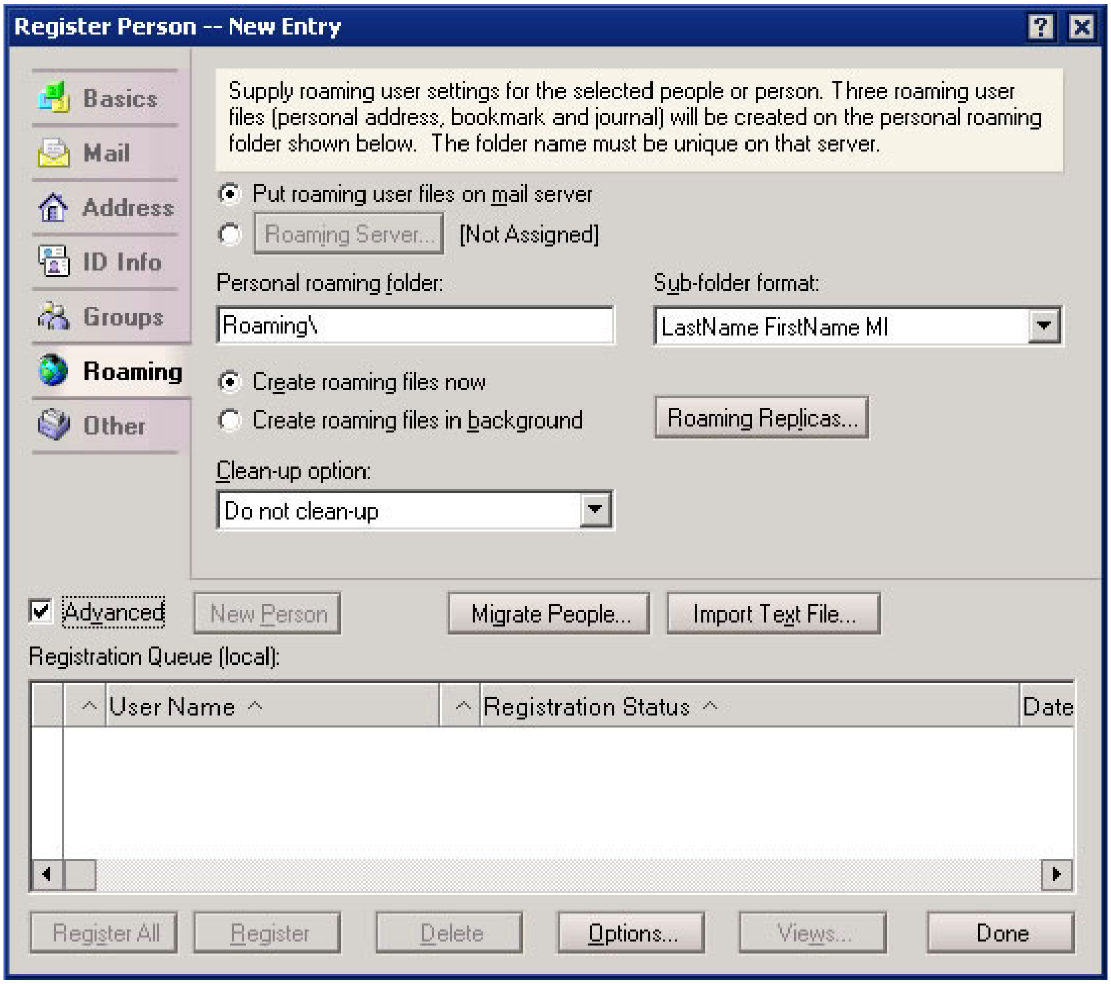
Once enabled, the specifics of the user's Roaming User configuration are stored under the Roaming tab of the user's Person document in the Domino Directory on the servers. These options cannot be edited in the Person document, except for the Clean-up setting, and can only be changed via the Assign Roaming Profiles tool by first completely disabling roaming and then re-enabling it.

TIP: To ensure you have a complete set of roaming files, make sure the user creates a Personal Journal before you enable roaming for them. The user can easily do this by clicking on the Journal icon on the default Welcome page. By default, a Journal is not created on a non-roaming user's computer until the user creates it. If you enable roaming and a Journal does not exist, it will not be set up for roaming. Then, the only way to enable a Journal for roaming is to disable roaming (letting the Administration Process complete all steps) to create the Journal on the user's computer, and then to re-enable roaming.

Setting roaming options while registering new users

When registering users it is important to set the roaming options correctly. To set the roaming options during registration:

1. Start the Register Person process (see Using registration policy while registering new users on page 32 for details).
2. Click the Advanced checkbox to display all registration options.
3. Click the Roaming tab.



Register Person -- New Entry

Supply roaming user settings for the selected people or person. Three roaming user files (personal address, bookmark and journal) will be created on the personal roaming folder shown below. The folder name must be unique on that server.

● Put roaming user files on mail server

○ Roaming Server... [Not Assigned]

Personal roaming folder: Roaming\

Sub-folder format: LastName FirstName MI

● Create roaming files now

○ Create roaming files in background

Clean-up option: Do not clean-up

☑ Advanced

Registration Queue (local):

User Name	Registration Status	Date

4. You can use the Put roaming user files on mail server option or select a specific server by clicking the Roaming Server button.
5. Specify the base folder name for the roaming files in the Personal roaming folder field. The default is Roaming\.
6. Specify the naming convention to use for naming the user folder under the base folder in the Sub-folder format. This is where the Roaming User files will be stored.

TIP: Using LastNameFirstNameMI provides the most unique name and allows the folders to be sorted by last name.

7. To create all files, select the Create roaming files now option.
8. If you want to create replicas of the roaming files on other servers, which you would do if you used a server cluster, for example, click the Roaming Replicas button.
9. Specify a clean-up option for multi-user Notes by selecting it from the clean-up option pull-down list.

TIP: The Clean-up option is the only option that can be changed after roaming is enabled. Change this option by editing the user's Person document.
Next, we'll learn some of the basics of setting up policies by walking through a real-world scenario.

Section 7. Real-world scenario

Scenario overview

In this section, we will learn some of the basics of setting up policies by walking through the creation of some specific policies for KennethAdams.com. KennethAdams.com has an East Coast office and a West Coast office. They have two servers, one in each office.

Here's what we would like to do with policies:

1. Provide support for roaming users for those people that have both a desktop computer and a notebook computer.
2. Create a company-wide security standard to enforce password expiration every 90 days and synchronize Notes and Internet passwords.
3. Ensure that each office has its own Welcome page and database bookmarks on their respective user's Notes clients.

What Policy documents we need

We will need the following documents to support our requirements:

Policy documents needed:

- An explicit Policy document for roaming users
- One organizational Policy document for the entire organization
- Two organizational Policy documents: one for the East region and one for the West region

Policy Settings documents needed:

- A registration policy Settings documents for roaming users
- One security policy Settings document with the password settings
- Two desktop policy Settings documents for East and West, with settings for Welcome page and local databases

---

Setting up a registration policy

In this example, we want to set up registration policies for registering new users. Our requirement for the registration policies is a registration policy that automatically enables the Roaming User feature.

To support this we need the following documents:

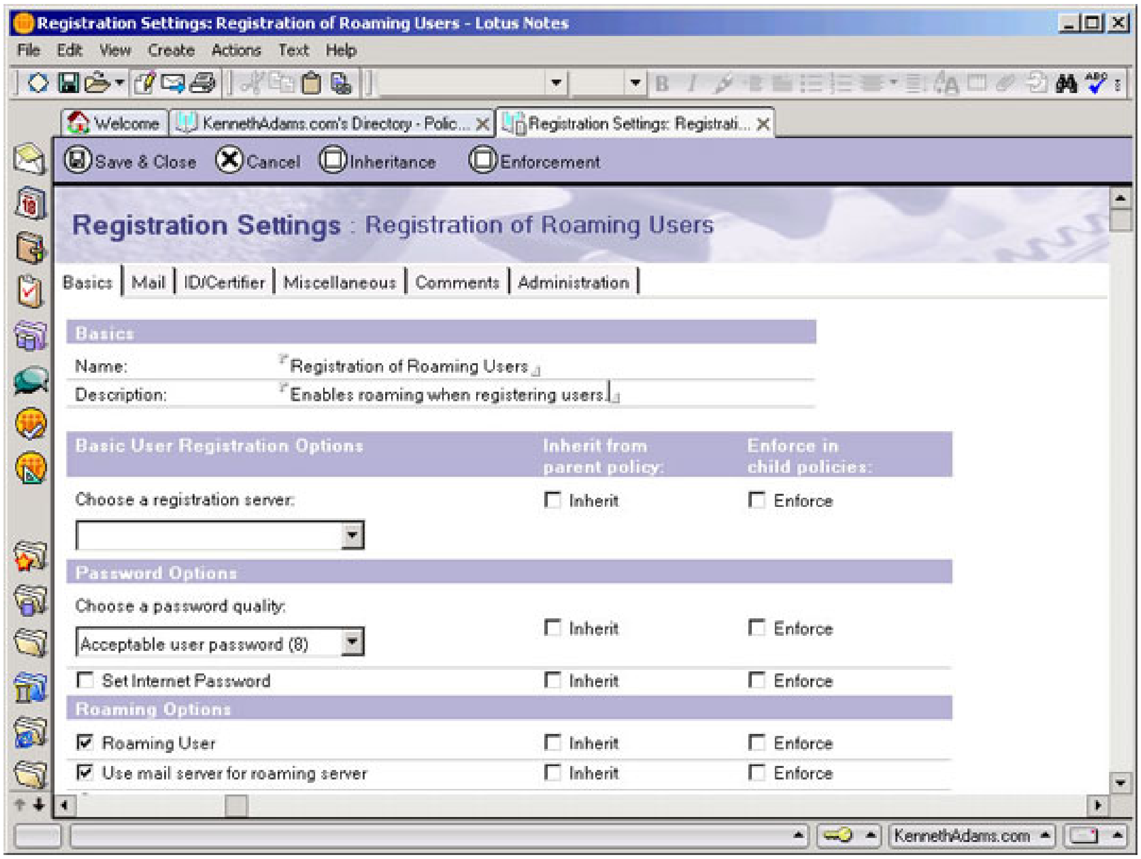
- A registration policy Settings document that will enable roaming
- An explicit Policy document that we will use when registering users

---

Create the registration policy Settings document

First we will create our registration policy Settings document, and then we'll create the Policy document that will use it.

1. Create a registration policy Settings document (see Creating policy Settings documents on page 9 for details)
2. Fill in the Name and Description


Registration Settings: Registration of Roaming Users - Lotus Notes
File Edit View Create Actions Text Help
Welcome
KennethAdams.com's Directory - Polic...
Registration Settings: Registrati...
Save & Close
Cancel
Inheritance
Enforcement
Basics | Mail | ID/Certifier | Miscellaneous | Comments | Administration
KennethAdams.com

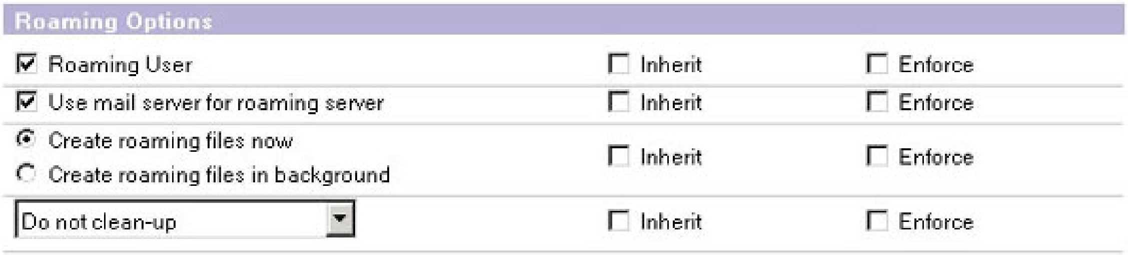
Registration Settings : Registration of Roaming Users

Basics

Name:	Registration of Roaming Users
Description:	Enables roaming when registering users.

Basic User Registration Options	Inherit from parent policy:	Enforce in child policies:
Choose a registration server:	☐ Inherit	☐ Enforce
Password Options		
Choose a password quality: Acceptable user password (8)	☐ Inherit	☐ Enforce
☐ Set Internet Password	☐ Inherit	☐ Enforce
Roaming Options		
☑ Roaming User	☐ Inherit	☐ Enforce
☑ Use mail server for roaming server	☐ Inherit	☐ Enforce

Next, scroll down to the Roaming Options section. Below the figure, you'll find an explanation of the settings in this section.



Roaming Options

☑ Roaming User	□ Inherit	□ Enforce
☑ Use mail server for roaming server	□ Inherit	□ Enforce
● Create roaming files now ○ Create roaming files in background	□ Inherit	□ Enforce
Do not clean-up ▾	□ Inherit	□ Enforce

The Use mail server for roaming server option is checked by default. This will store the user's roaming information on the same server used for mail. If you uncheck it, you can then select the name of the server to store the user's roaming information on from the Choose a roaming server pull-down list.

The Create roaming files now option is checked by default. This creates the user's roaming files during user registration. The Create roaming files in background option will use the Administration Process to create the user's roaming files after user registration, which can save time during registration.

In the Clean-up options drop-down list, the Do not clean-up option is set by default, which means that Roaming User files will not be cleaned up. Clean-up periodically will enable the Clean up every N days field in which you specify the number of days that should pass before Roaming User data is deleted from the Notes client workstation. Clean-up at Notes shutdown will delete Roaming User data from the Notes client workstation immediately upon Notes shutdown. Prompt user will prompt users upon exiting the client as to whether they want to clean up their personal files.

Note: Clean-up will only occur on clients that have been installed and configured for multiple users and therefore does not apply to regular, single-user client installations. There are too many options in registration policy Settings documents to cover them all in this tutorial. For complete details, see Tutorial resources on page 47 .

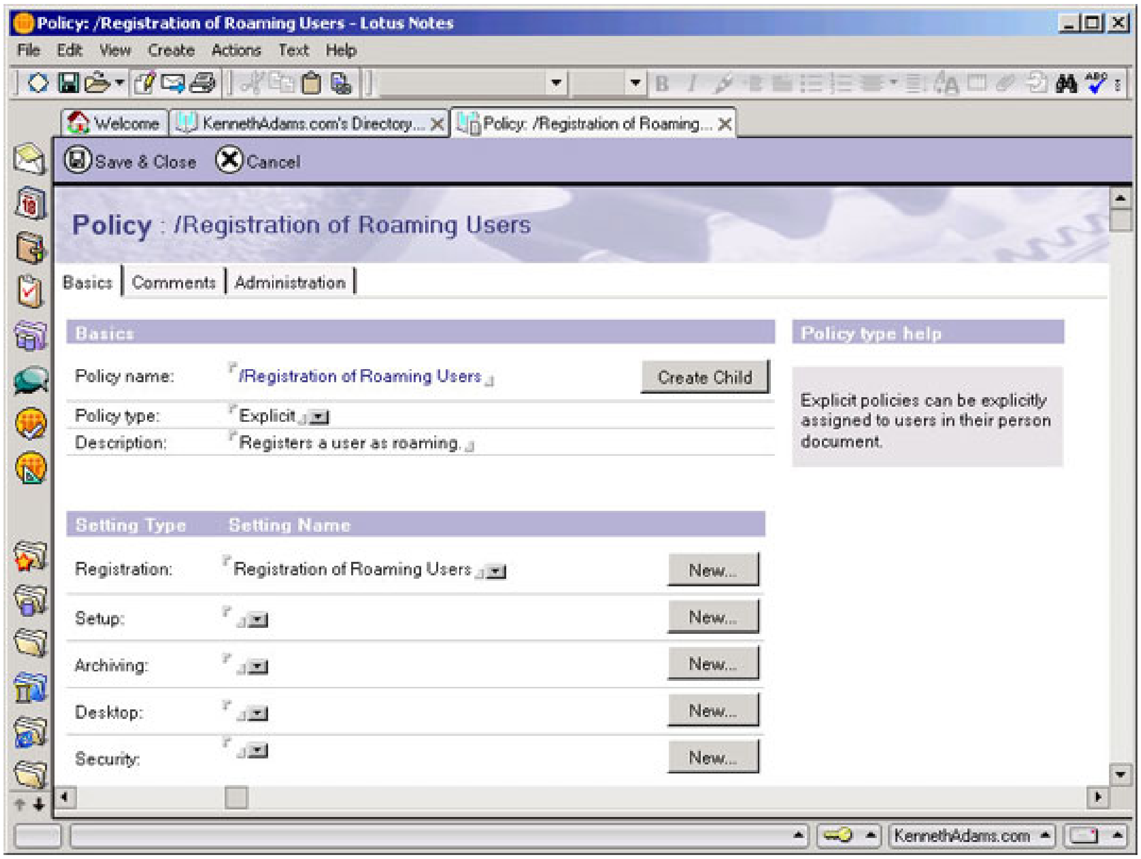
Create the Policy document

Now we will create our Policy document that will use our registration policy Settings document. We will use an explicit Policy document so that we can select the policy while registering new users.

1. Create a Policy document (see Creating Policy documents on page 10 for details).
2. Fill in the Policy Name, which will display in the Register Person tool when we

register new users. Select the Policy Type as Explicit.

3. Fill in the Description.
4. Under the Settings Type section, in the Registration field, select the policy Settings document we already created.
5. Click the Save & Close button.


Policy: /Registration of Roaming Users - Lotus Notes
File Edit View Create Actions Text Help
Welcome
KennethAdams.com's Directory...
Policy: /Registration of Roaming...
Save & Close
Cancel
Basics
Comments
Administration
Create Child
New...
KennethAdams.com

Policy : /Registration of Roaming Users

Basics

Policy name: /Registration of Roaming Users

Policy type: Explicit

Description: Registers a user as roaming.

Policy type help

Explicit policies can be explicitly assigned to users in their person document.

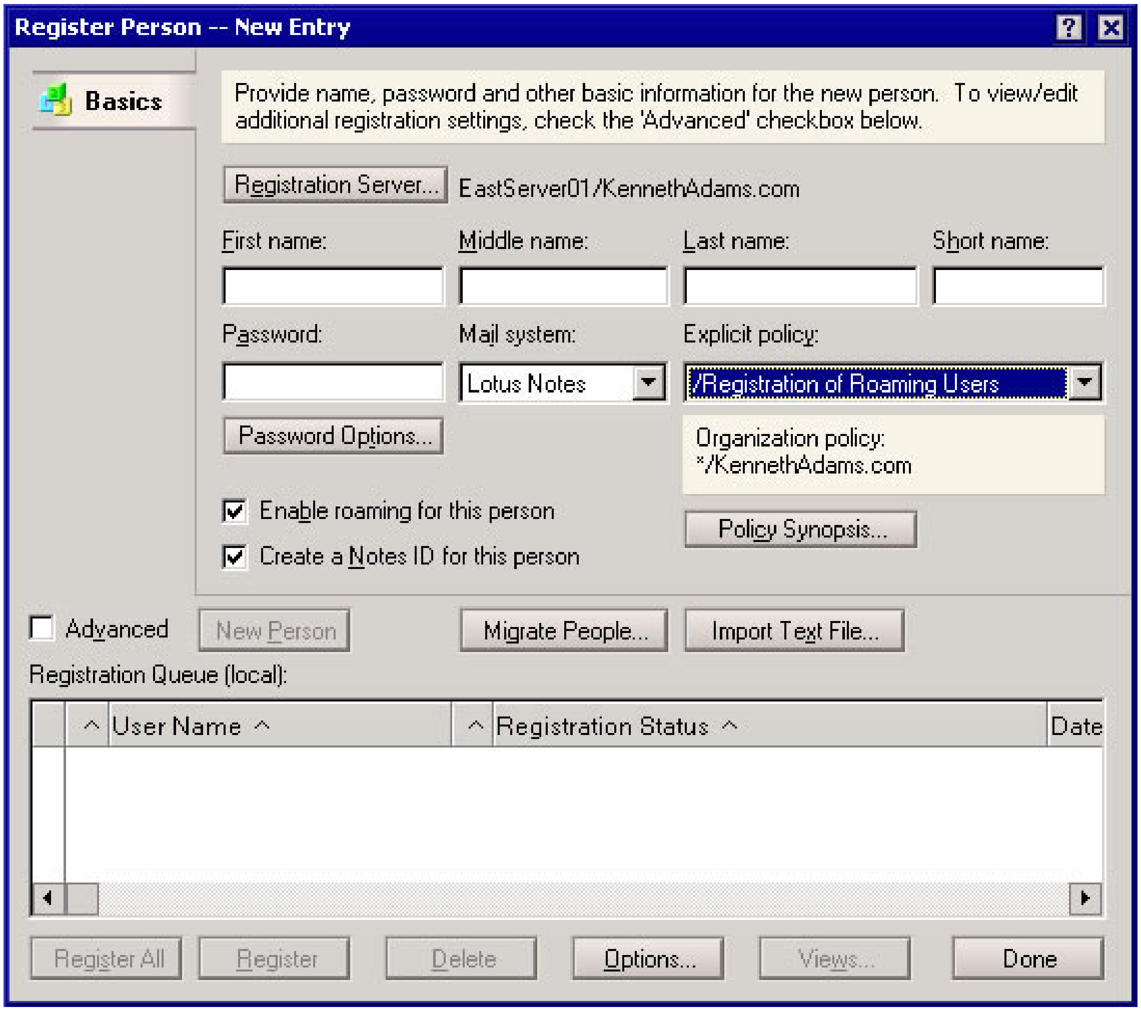
Setting Type	Setting Name
Registration:	Registration of Roaming Users
Setup:	
Archiving:	
Desktop:	
Security:	

Using registration policy while registering new users

When we register new users, we can select our newly created explicit policy by selecting it from the Explicit policy pull-down list in the Register Person tool of the Domino Administrator client. To initiate the registration process:

1. Open the Domino Administrator client
2. Select the server you wish to administer
3. Click the People & Groups tab
4. Expand Tools and then expand People

5. Click the Register... tool
6. You will be prompted for the Certifier ID and password
7. To select a policy when registering, select it from the Explicit policy pull-down list on the Basics tab



Register Person -- New Entry

Provide name, password and other basic information for the new person. To view/edit additional registration settings, check the 'Advanced' checkbox below.

Registration Server: EastServer01/KennethAdams.com

Mail system: Lotus Notes

Explicit policy: /Registration of Roaming Users

Organization policy:
*/KennethAdams.com

☑ Enable roaming for this person

☑ Create a Notes ID for this person

□ Advanced

For more details on roaming, see Setting roaming options while registering new users on page 26 .

Setup policy for Notes client installs

Setup policy Settings documents and desktop policy Settings documents have almost the same settings available on them. The desktop policy Settings document actually has more settings that we can control, and it is continuously enforced. Setup policy

Settings documents are used only once during the initial Notes client installation and are not used by that client again.

In our scenario we have chosen not to use the setup policies, but to instead use desktop policies to set and enforce all client settings. This avoids duplicating the same settings in desktop policy Settings documents and setup policy Settings documents.

If you would like to use setup policy Settings documents, you can create them as you would any other policy Settings document.

The next section looks at setting up a security policy for the organization.

Section 8. Setting up a security policy for the organization

Security policy overview

In this example, we want to set up a security policy for our entire organization. To support this we need the following documents:

- An organizational Policy document for the entire organization
- One security policy Settings document

Our organization's security policy will follow these specifications:

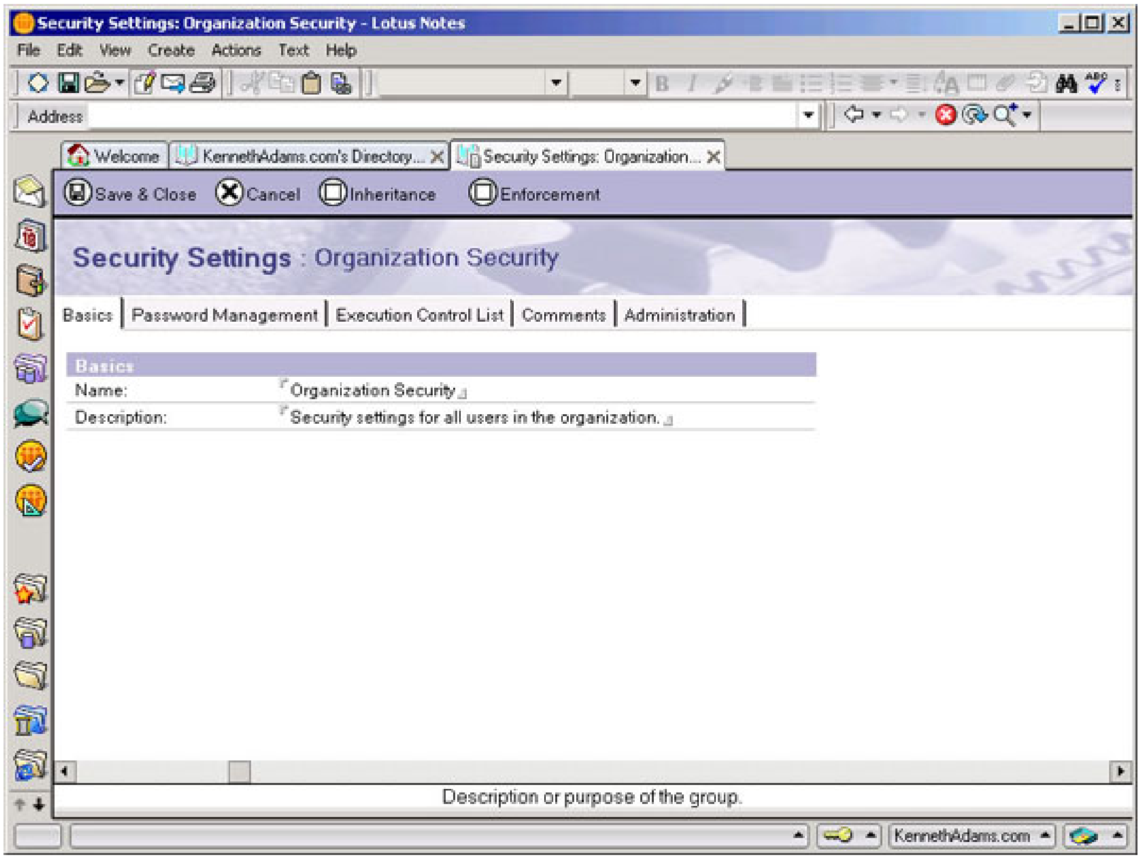
- Notes and Internet passwords are kept synchronized so users don't have to remember two passwords. When the Notes password is changed the Internet password is also changed.
- Passwords will expire every 90 days.
- Passwords are prevented from being reused.
- A grace period of 14 days is allowed for the password to be changed after it expires.
- Reasonably strong passwords are required.

The settings we will select in our security policy Settings document will enforce these requirements.

Create the security policy Settings document

First we will create our security policy Settings document, and then we will create the Policy document that uses it.

1. Create a security policy Settings document (see Creating policy Settings documents on page 9)
2. Fill in the Name and Description


Security Settings: Organization Security - Lotus Notes
File Edit View Create Actions Text Help
Address
Welcome
KennethAdams.com's Directory...
Security Settings: Organization...
Save & Close
Cancel
Inheritance
Enforcement
Security Settings : Organization Security
Basics
Password Management
Execution Control List
Comments
Administration
KennethAdams.com

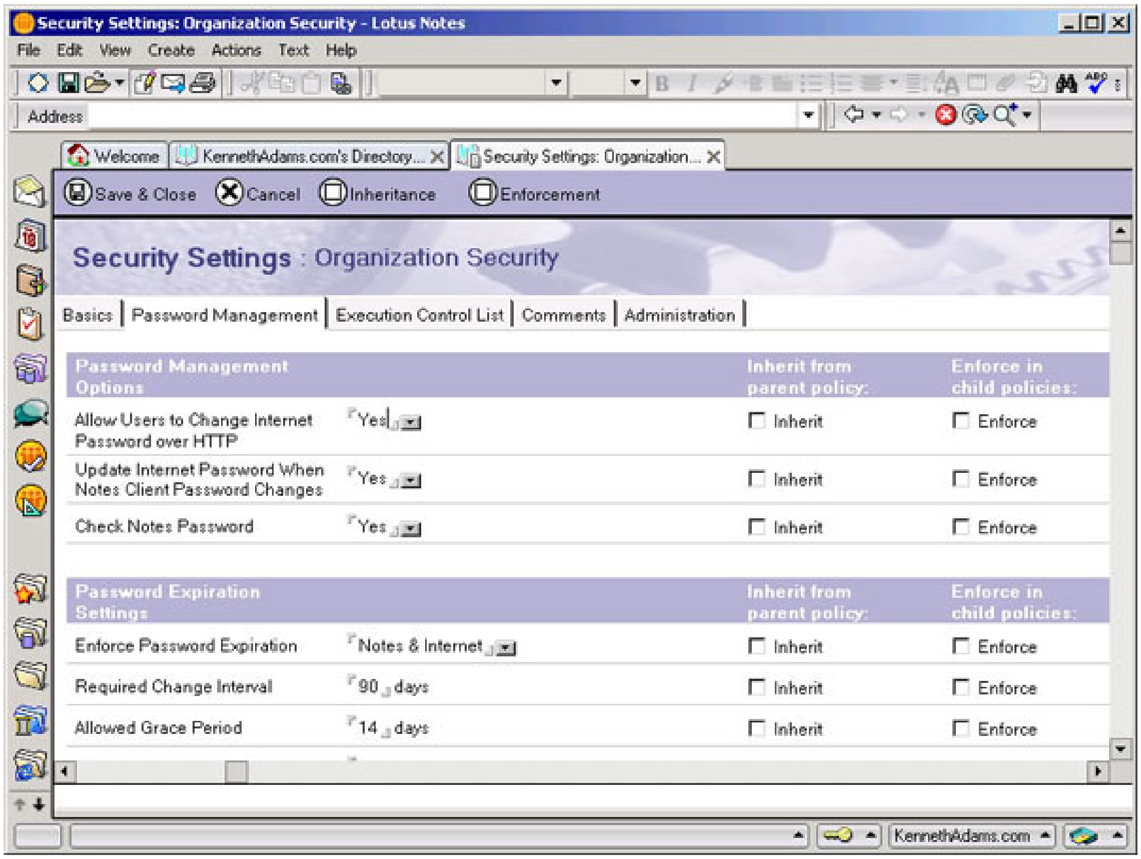
Basics

Name: Organization Security

Description: Security settings for all users in the organization.

Description or purpose of the group.

Next, click on the Password Management tab.


Security Settings: Organization Security - Lotus Notes
File Edit View Create Actions Text Help
Address
Welcome
KennethAdams.com's Directory...
Security Settings: Organization...
Save & Close
Cancel
Inheritance
Enforcement
Basics
Password Management
Execution Control List
Comments
Administration
KennethAdams.com

Security Settings : Organization Security

Password Management Options		Inherit from parent policy:	Enforce in child policies:
Allow Users to Change Internet Password over HTTP	Yes	□ Inherit	□ Enforce
Update Internet Password When Notes Client Password Changes	Yes	□ Inherit	□ Enforce
Check Notes Password	Yes	□ Inherit	□ Enforce

Password Expiration Settings		Inherit from parent policy:	Enforce in child policies:
Enforce Password Expiration	Notes & Internet	□ Inherit	□ Enforce
Required Change Interval	90 days	□ Inherit	□ Enforce
Allowed Grace Period	14 days	□ Inherit	□ Enforce

The default should be selected in the three Password Management Options fields, as follows:

- In the Allow users to change Internet password over HTTP field, the setting should be set to Yes as the default. This allows users to use a Web browser to change their Internet passwords.
- In the Update Internet Password When Notes Client Password Changes field, the setting should be set to Yes as the default. This automatically synchronizes Notes passwords with Internet passwords when the user changes his or her Notes password.
- In the Check Notes password field, the setting should be set to Yes as the default. This setting works the same way as the Check Password option in the Person document. If selected, the password in the Notes user ID will also be stored in the Person document. When the user connects to the server, the passwords will be compared and, if they don't match, the user will be denied access. This is useful in case the user ID is lost or stolen. The user can change his or her password and effectively lock out the user ID with the old password.

In the Password Expiration Settings section, change the settings as follows:

- In the Enforce Password Expiration field, change the setting to Notes and Internet.

This enables password expiration for both Notes and Internet passwords.

- In the Required Change Interval field, change the setting to 90. This enforces the number of days a password can be in effect before it must be changed.
- In the Allowed Grace Period field, change the setting to 14. This enforces the number of days users have to change an expired password before being locked out.
- In the Password History (Notes only) field, change the setting to 50 (this is actually the default when Check Notes Password is enabled). This prevents users from reusing old passwords by storing the number of expired passwords specified here.

In the Password Quality Settings section, you can leave the defaults, which are as follows:

- The Required Password Quality field allows you to choose the quality level required when users create passwords. The default, Strong Password Possibly Crackable by Automated Dictionary Attack (8), should provide sufficient security.
- If you check the Use length instead field, the Require Password Quality field becomes Required Password Length and you can enter a number from 0 to 16 to require that users create passwords of a specific length. You can leave this field unchecked.

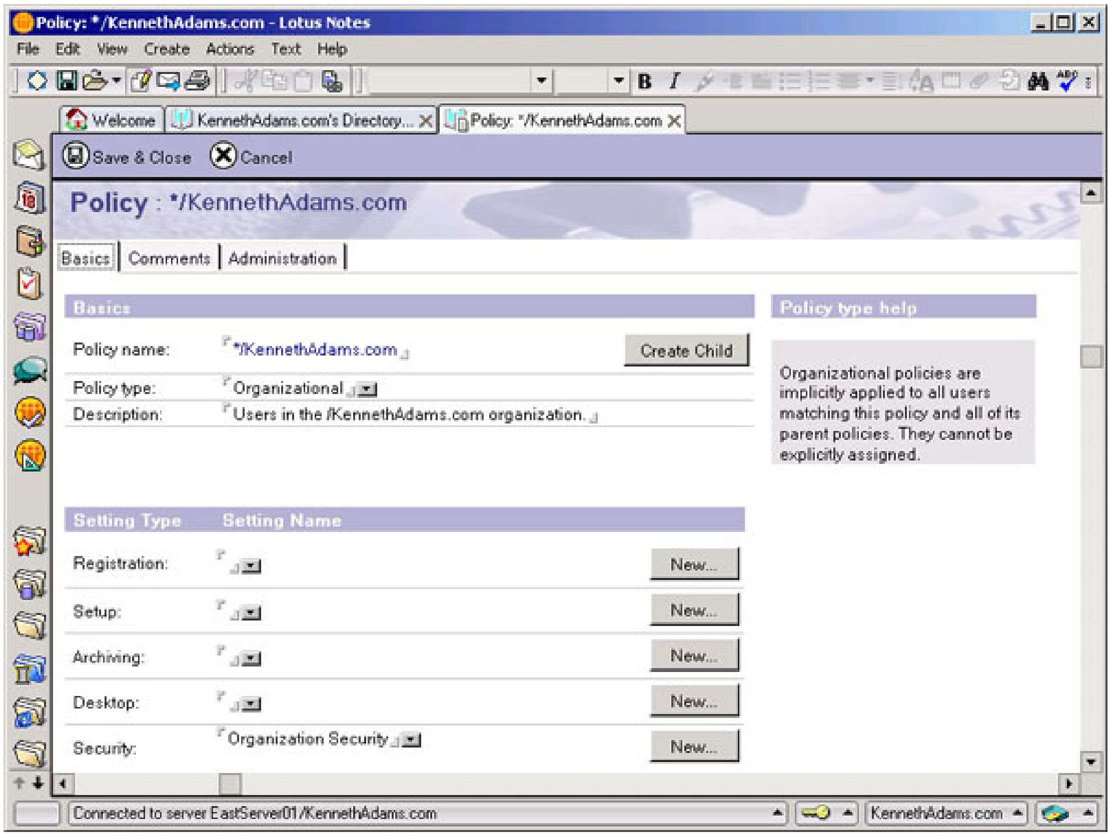
After you've completed these fields, click the Save & Close button.

There are additional options in security policy Settings documents, such as Execution Control Lists, which we will not cover in this tutorial. For complete details, see Tutorial resources on page 47 .

Create the security Policy document

Now we will create our Policy document that will enforce our security policy Settings document. We will use an organizational Policy document because we want our security policy to be enforced across the entire organization.

1. Create a Policy document (see Creating Policy documents on page 10 for details)
2. Fill in the Policy Name using the format */organization unit/organization name (for example, */KennethAdams.com)


Policy: */KennethAdams.com - Lotus Notes
File Edit View Create Actions Text Help
Welcome
KennethAdams.com's Directory...
Policy: */KennethAdams.com
Save & Close
Cancel
Basics
Comments
Administration
Create Child
New...

Policy : */KennethAdams.com

Basics

Policy name:	*/KennethAdams.com
Policy type:	Organizational
Description:	Users in the /KennethAdams.com organization.

Policy type help

Organizational policies are implicitly applied to all users matching this policy and all of its parent policies. They cannot be explicitly assigned.

Setting Type	Setting Name
Registration:	
Setup:	
Archiving:	
Desktop:	
Security:	Organization Security

Connected to server EastServer01/KennethAdams.com

KennethAdams.com

3. Select the Policy Type as Organizational
4. Fill in the Description
5. Under the Settings Type section in the Security field, select the policy Settings document we already created
6. Click the Save & Close button

Next, we'll look at setting up a desktop policy.

Section 9. Setting up a desktop policy for the organization

Desktop policy overview

In this example, we want to set up desktop policies for our organization. Our requirements for our desktop policies are the following:

- We have two offices, an East Coast office and a West Coast office.
- Each office has its own Welcome page and database bookmarks that users wish to have on their respective Notes clients.

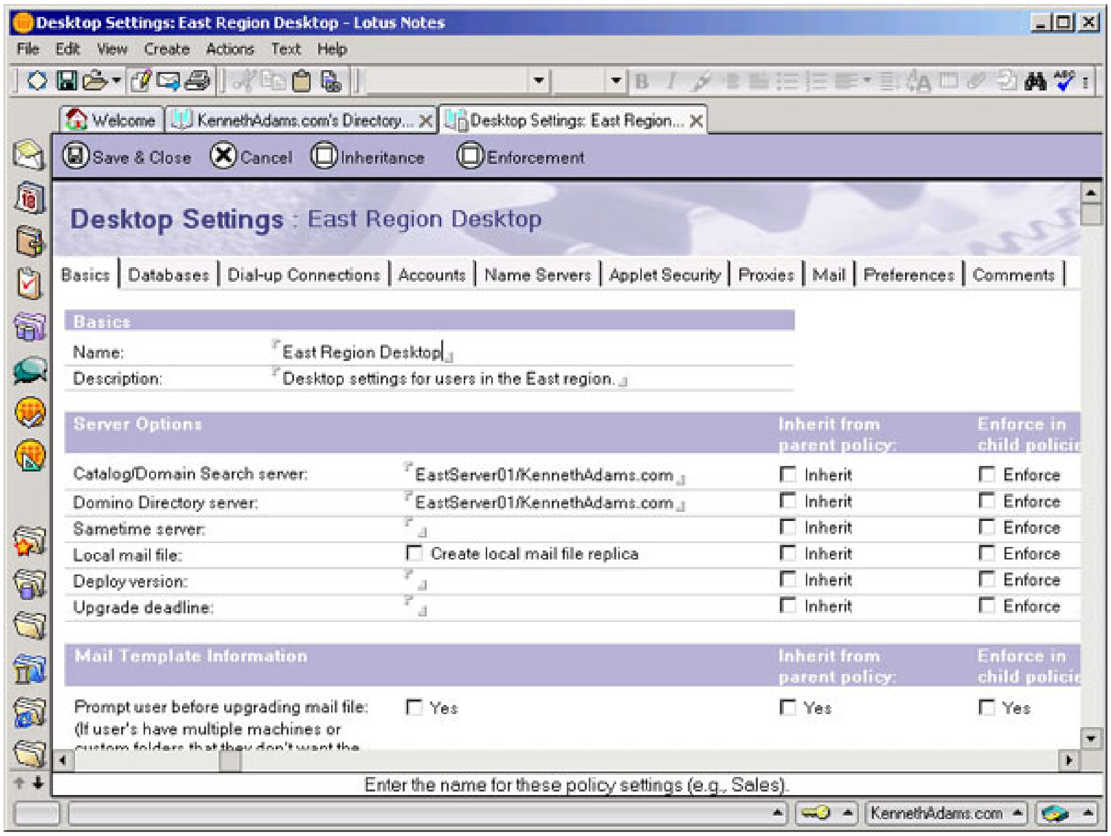
To support this we need the following documents:

- Two organizational Policy documents: one for East region and one for West region
- Two desktop policy Settings documents for East and West, with settings for Welcome page and local databases

Create the desktop policy Settings documents

First we will create our two desktop policy Settings documents, and then we'll create the Policy documents that use them.

1. Create a desktop policy Settings document (see Creating policy Settings documents on page 9 for details).
2. Fill in the Name and Description.


Desktop Settings: East Region Desktop - Lotus Notes
File Edit View Create Actions Text Help
Welcome
KennethAdams.com's Directory...
Desktop Settings: East Region...
Save & Close
Cancel
Inheritance
Enforcement
Basics | Databases | Dial-up Connections | Accounts | Name Servers | Applet Security | Proxies | Mail | Preferences | Comments
KennethAdams.com

Desktop Settings : East Region Desktop

Basics

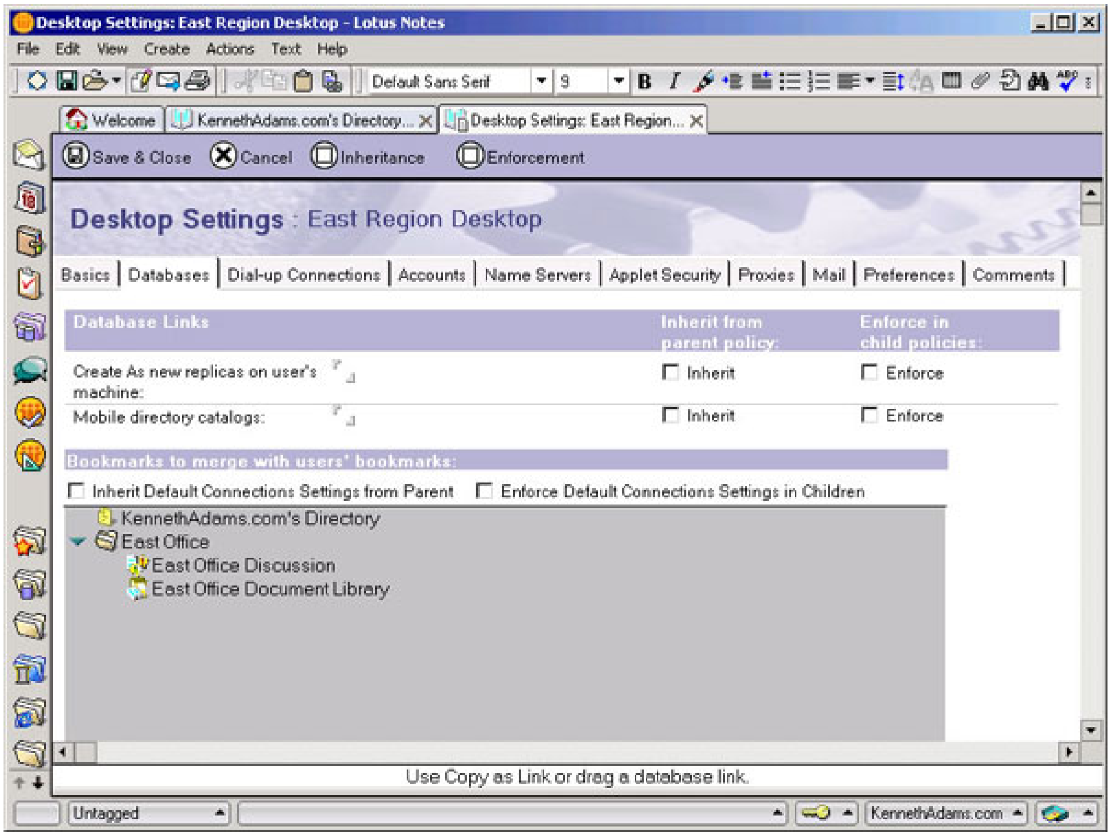
Name:	East Region Desktop
Description:	Desktop settings for users in the East region.

Server Options		Inherit from parent policy:	Enforce in child policie
Catalog/Domain Search server:	EastServer01/KennethAdams.com	□ Inherit	□ Enforce
Domino Directory server:	EastServer01/KennethAdams.com	□ Inherit	□ Enforce
Sametime server:		□ Inherit	□ Enforce
Local mail file:	□ Create local mail file replica	□ Inherit	□ Enforce
Deploy version:		□ Inherit	□ Enforce
Upgrade deadline:		□ Inherit	□ Enforce

Mail Template Information		Inherit from parent policy:	Enforce in child policie
Prompt user before upgrading mail file: (If user's have multiple machines or custom folders that they don't want the	□ Yes	□ Yes	□ Yes

Enter the name for these policy settings (e.g., Sales).

3. Enter the server name EastServer01/KennethAdams.com in the Catalog/Domain Search server and Domino Directory server fields.
4. Scroll down to the Homepage/Welcome Page Options section.
5. Copy a database link from the Welcome Pages database that you intend to use and paste that link into the Corporate Welcome Pages database field. You can then set the other Home/Welcome page settings.
6. Scroll back up to the top of the page and click on the Databases tab.


Desktop Settings: East Region Desktop - Lotus Notes
File Edit View Create Actions Text Help
Default Sans Serif
9
Welcome
KennethAdams.com's Directory...
Desktop Settings: East Region...
Save & Close
Cancel
Inheritance
Enforcement
Untagged
KennethAdams.com

Desktop Settings : East Region Desktop

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

Database Links	Inherit from parent policy:	Enforce in child policies:
Create As new replicas on user's machine:	□ Inherit	□ Enforce
Mobile directory catalogs:	□ Inherit	□ Enforce

Bookmarks to merge with users' bookmarks:

□ Inherit Default Connections Settings from Parent □ Enforce Default Connections Settings in Children

- KennethAdams.com's Directory
- East Office
  - East Office Discussion
  - East Office Document Library

Use Copy as Link or drag a database link.

7. Copy the bookmarks to databases you wish to add to user's Notes client in the Bookmarks to merge with users' bookmarks section. These bookmarks will be merged with the user's existing bookmarks. To set up the bookmarks to be merged, complete the following:
   1. First create the bookmarks in your own Notes client. You can organize the bookmarks into folders.
   2. Drag and drop the bookmarks and bookmark folders into the gray box in the Bookmarks to merge with users' bookmarks section.
8. Click the Save & Close button.

Repeat these steps for the West office so that there are two desktop policy Settings documents.

There are too many options in desktop policy Settings documents to be able to cover them all in this tutorial. For complete details, see Tutorial resources on page 47 . The next panel contains an overview of the settings available under each tab.

Options in desktop policy Settings documents

Here is an overview of the setting available under each tab in desktop policy Settings documents.

Basics

- Name and Description
- Server Options including create local mail replica and smart upgrade options
- Mail Template Info for converting from previous mail template versions
- Homepage/Welcome Page options for deploying custom welcome pages
- Internet browser options

Databases

- Create new local replicas
- Create local replicas of mobile directory catalogs
- Push bookmarks to users

Dial-up Connections

- Default dial-up connections and passthru server
- Accounts
- Internet server accounts (LDAP, SMTP, POP servers, etc.)

Name Servers

- Secondary Domino name servers for finding network addresses of servers
- Applet Security
- Security for Java applets

Proxies

- Settings for Internet proxy servers (HTTP, FTP, SOCKS, etc.)

Mail

- Choose the format to use for mail sent to Internet addresses

Preferences

- Extensive list of settings similar to what's available under User Preferences in Notes clients. Includes sub-tabs for: Basics, Misc, International, Internet, Mail and News, Replication and Network Ports

Comments

- A rich text field for comments

Diagnostics

- Options for diagnostic report collection

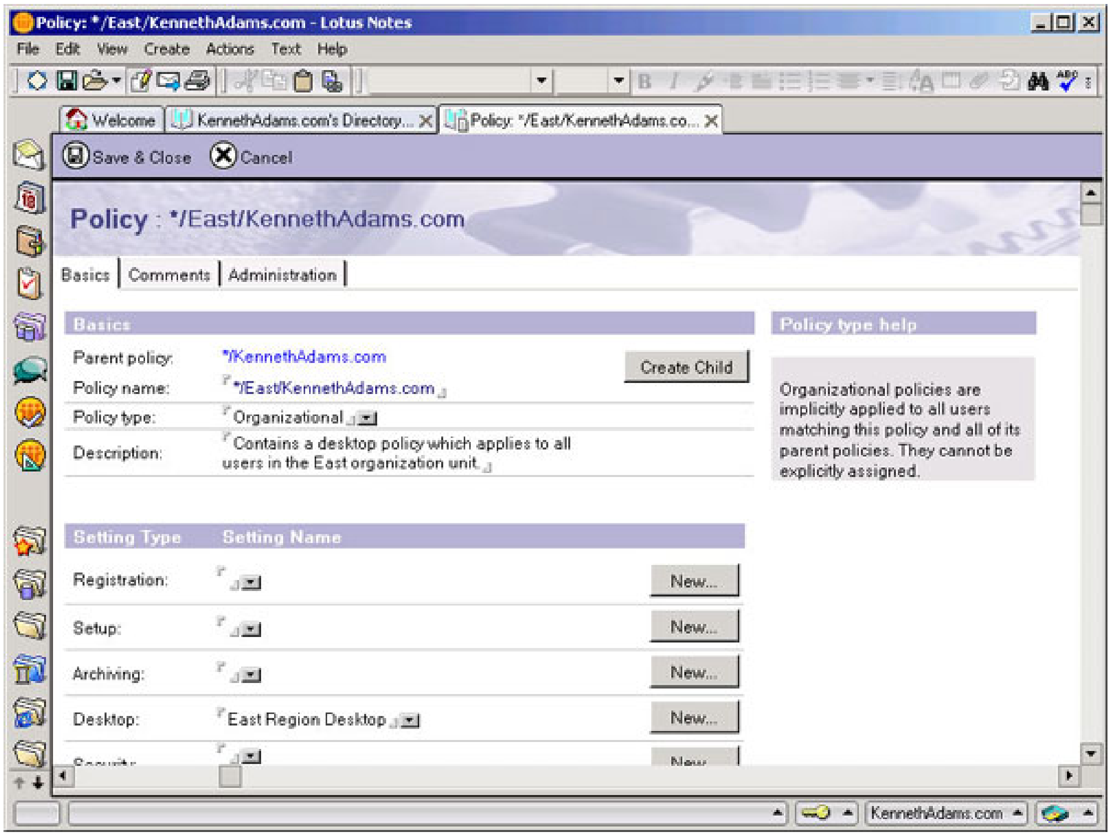
Administration

- Administrators of policy Settings document

Create the desktop Policy document

Now we will create our Policy document that will enforce our desktop policy Settings documents. We will use organizational Policy documents because we want our desktop policy to be enforced across the organization units for East and West.

1. Create a Policy document (see Creating Policy documents on page 10 for details)
2. Fill in the Policy Name using the format */organization unit/organization name (for example, */East/KennethAdams.com)


Policy: */East/KennethAdams.com - Lotus Notes
File Edit View Create Actions Text Help
Welcome
KennethAdams.com's Directory...
Policy: */East/KennethAdams.co...
Save & Close
Cancel
Basics
Comments
Administration
Create Child
New...
KennethAdams.com

Policy : */East/KennethAdams.com

Basics

Parent policy:	*/KennethAdams.com
Policy name:	*/East/KennethAdams.com
Policy type:	Organizational
Description:	Contains a desktop policy which applies to all users in the East organization unit.

Policy type help

Organizational policies are implicitly applied to all users matching this policy and all of its parent policies. They cannot be explicitly assigned.

Setting Type	Setting Name
Registration:	
Setup:	
Archiving:	
Desktop:	East Region Desktop
Security:	

3. Select the Policy Type as Organizational
4. Fill in the Description
5. Under the Settings Type section, in the Desktop field, select the Policy Settings document already created
6. Click the Save & Close button

The next section takes a look at mail archiving policy options.

Section 10. Mail archiving policy

Mail archiving policy overview

Mail archiving policies allow administrators to centrally control and manage mail-file archiving. The mail archiving policy features are very sophisticated and are too vast to cover beyond this overview. See Tutorial resources on page 47 for links to complete details on mail archiving.

You set up a mail archiving policy as you would any other policy, using the archiving policy Settings documents and Policy documents. Here are some of the capabilities of mail archiving:

- Prohibit archiving or prohibit private archiving criteria
- Perform archiving on client or server
- Specify source and destination servers
- Specify multiple sets of archive criteria including:
  - Copy and clean up
  - Clean up without archiving
  - Clean up by deleting or reducing size of documents
  - Clean up by date accessed, modified, or marked expired
  - Archive by view or folder
  - Specify destination directory, file prefix and suffix, and portion of original filename
- Log all archiving activity to specific filenames
- Schedule client-based archiving

Section 11. Tutorial summary

Configuring and deploying policies summary

This tutorial provided an overview of how policies work, and covered a few of the ways you can use policies in a real-world scenario. Policies are an incredibly powerful new feature for Domino and can make the life of administrators and users easier.

Our tutorial covered the following topics:

- How policies work
- How to manage Policy documents
- How to use policy hierarchies and inheritance
- How to use the Roaming User feature to easily support mobile users
- How to set up several types of policy Settings documents

The policies features of Domino 6 have many capabilities, far too numerous to cover completely here, so the following panel contains links to all the details you will need to fully take advantage of all that policies have to offer.

Tutorial resources

Some of the information contained in this tutorial and additional details can be found in these topics from the *Lotus Domino Administrator 6 Help*. You can also find these topic titles using the Search view of Lotus Domino Administrator 6 Help in your Notes client or Web browser:

Policy documents

- Organizational and explicit policies
- Planning and assigning policies
- Assigning an explicit policy

Policy Settings documents

- Policies
- Creating policies
- Managing policies

Roaming User

- Roaming users
- Changing a non-roaming user to roaming
- Changing a roaming user to non-roaming
- Using Advanced Notes user registration with the Domino Administrator
- Update user from non-roaming to roaming user -- lists the Administration Process Requests
- Downgrade user from roaming to non-roaming user -- lists the Administration Process Requests

Registration policy Settings

- Creating a registration policy Settings document

Setup Policy settings

- Creating a setup policy Settings document

Security Policy settings

- Creating a security policy Settings document
- The execution control list

Desktop Policy settings

- Creating a desktop policy Settings document
- Deploying a custom Welcome page

Mail Archiving Policy settings

- Mail archiving and policies
- Using the mail archive log
- Creating an archive policy Settings document
- Creating criteria for mail archiving

Policy hierarchy and inheritance

- Policy hierarchy and the effective policy
- Using the Policy Synopsis tool to determine the effective policy
- Viewing policy relationships

Others

- Any updates to this tutorial, new information, or other useful stuff will be posted on my Web site at: *http://kennethadams.com/tutorials*.

Policies-related resources

- For an excellent introductory article on policy-based system administration, see *Policy-based system administration with Domino 6* an article on the Lotus Developer Domain.

General resources

- The Lotus Developer Domain's *Notes/Domino Product Pages* contain numerous resources on Notes and Domino, including links to articles, documentation, and trial downloads.
- The Lotus Domino 6 server and administrator documentation is *downloadable in a number of formats* including Acrobat PDF and Notes NSF.
- You can view the *Lotus Domino Administrator 6* with a Web browser without having to download it first.

Feedback

Colophon

This tutorial was written entirely in XML, using the developerWorks Toot-O-Matic tutorial generator. The open source Toot-O-Matic tool is an XSLT style sheet and several XSLT extension functions that convert an XML file into a number of HTML pages, a zip file, JPEG heading graphics, and two PDF files. Our ability to generate multiple text and binary formats from a single source file illustrates the power and flexibility of XML. (It also saves our production team a great deal of time and effort.)

You can get the source code for the Toot-O-Matic at www6.software.ibm.com/dl/devworks/dw-tootomatic-p. The tutorial Building tutorials with the Toot-O-Matic demonstrates how to use the Toot-O-Matic to create your own tutorials. developerWorks also hosts a forum devoted to the Toot-O-Matic; it's available at www-105.ibm.com/developerworks/xml_df.nsf/AllViewTemplate?OpenForm&RestrictToCategory=11. We'd love to know what you think about the tool.