CHAPTER 6

Using Domino Administrator to Manage Client Settings

Managing client settings for the Lotus Notes client can be a daunting task. This chapter provides an insight into managing the settings via the Lotus Domino Administrator through the use of policy profiles.

The intent of this chapter is to provide some basic guidance into the setup and management of client settings through the use of Domino policy and settings documents. These documents can help ensure a consistent user configuration and can reduce the administrative overhead in managing client settings. The chapter provides a basic introduction to the setup process specifically for the Notes client.

You will learn the basic concept of policy-based management of client settings through the use of profiles. Key topics covered include

- Policy-based administration
- Policy documents
- Settings documents
- The six primary types of settings documents
- Inherit and Enforce settings
- Organization and explicit policies
- Exception policies
- How to manage the user's client configuration through the use of Setup, Registration, Mail, Desktop, Security and Archive settings documents

It's important to understand that this chapter is intended to be an introduction on how to manage client settings through the Domino Administrator client. Clearly entire publications could be and are dedicated to using the client. This chapter highlights some of the function that is specific to the support of the Lotus Notes client.

The ability to implement the items described herein will depend on how roles and responsibilities are separated within your company. You might or might not have authority (or the responsibility) to perform the instructions within this chapter. The chapter is for those readers who are responsible for both the Lotus Notes client as well as the administration of the infrastructure.

Readers must have the Lotus Domino Administrator client installed with the appropriate authority level in order to perform the instructions outlined in this chapter. Additionally, readers should have a fundamental understanding of the Administrator client and how to navigate through the various client screens.

Finally, readers should note the information presented in this chapter is based on the version 8 Domino Administrator client. You will notice variances in the screen layout and policy preference settings if you are running and supporting an alternate version of the client.

What Are Policies?

What are policies? Policies allow greater control over the management of the end user's Notes client configuration settings. Let's face it, the sheer number of Lotus Notes client settings can be mind-boggling. There are preference settings, mail template settings, execution control lists (ECLs), and access control lists (ACLs) just to name a few. Using policies, you can create a common, centralized set of rules that govern the end user's client setup.

The policy-based approach to managing user settings has been around for quite some time and was significantly enhanced in the Domino release 6. Since then, the feature has been enhanced with each subsequent release as a means to provide both better concentric control and to reduce the administrative overhead of managing user settings. Using policies you can control a great many settings, including the ability to

- Define a common set of user preference settings for all users
- Define a common set of user preference settings unique to certain groups
- Automatically keep all user settings synchronized across the organization
- Control connection settings
- Set and manage mail database size quotas
- Define default database, catalog, and domain servers
- Determine mail archive settings
- Disable the ability for users to modify certain preference settings
- Establish rules for managing unwanted mail (also known as "spam")
- Manage password duration and rules for creation

If you're new to the concept of policies, this chapter will help orient you, and with a little hands-on experience, you'll find they are quite easy to set up and manage. **Policy documents** allow you to define a common set of configuration settings.

Domino allows you to define one or more policy documents. Contained within each policy are a number of configuration settings that govern the user's Lotus Notes client environment settings. In other words, each policy contains a group of settings. These settings are called **settings documents**. We'll talk more about the settings documents later in the chapter. At this point, just recognize the concept of policies and settings.

How Are Policies Implemented?

There are two primary considerations when implementing policy documents: what the settings are and which users the settings apply to. First, you need to determine all the configuration settings to be applied to the Lotus Notes client.

Once you have identified these settings, your second task is figuring out how to apply the settings to the user community. You need to determine which users or groups of users should be assigned a particular policy, which subsequently contains a number of configuration settings known as settings documents.

Although settings documents might sound complicated, implementing them is actually much simpler than it sounds on paper. Once you've become familiar with the configuration settings, you merely need to determine the settings for a particular group of users and assign the policy.

As with most projects or tasks, the key to successful implementation will be thorough understanding of the application and planning. Having a clear understanding of your user community and a well-defined implementation plan is a crucial step in the planning process and for creating a policy-based architecture. So, let's take a closer look at the approach. Key implementation tasks should include

1. Review the configuration settings and determine the comprehensive list of settings to be applied.
2. Determine all users and groups of users within your community.
3. Organize the configuration settings. In this step you need to identify the configuration rules to be applied to general registered users and those to be applied to each group of users.
4. Create a policy document for general users and for each group of users as identified in the previous step.

Now that you understand the general approach to implementing policies, let's take a look at each type of settings documents that you can create and associate with a policy. Be aware that a policy might contain one or more settings documents. In short, the settings documents associated with a policy will depend on the user group to which they will be applied.

TIP

As part of the Redbook series, IBM has published a Domino server best practices guide. This publication contains a wealth of information, including a section on how to implement policy-based management. You can find this information in Chapter 2 of the guide. All IBM Redbooks are available free of charge. Visit the following Web site to view this publication: www.redbooks.ibm.com/abstracts/SG246937.html?Open.

What Are Settings Documents?

The five primary types of settings documents are Setup, Registration, Archive, Desktop, and Security. Each type of document serves a unique purpose and is utilized at different points in time by the Lotus Notes client. In some cases, the settings are applied one time, such as during the installation of the Notes client, whereas others are dynamically applied. Using dynamic settings, the configuration settings are "refreshed," so to speak, each time the user accesses his Notes client. As you consider the configuration settings, you'll need to organize them in accordance with the various types. These policy documents consist of the types shown in Table 6.1.

Table 6.1 Types of Settings Documents

Document Type	Document Description	Primary Use
Setup	Controls the settings as new users are registered as well as general preferences for the Notes client. Settings are applied only one time during the installation of the Notes client. Changes to the Setup document do not affect clients that have already been installed. Most of the configuration options in the settings document are also included in the Desktop settings document.	Location documents Browser default Preferences Proxy settings
Registration	Controls the registration settings of users. Settings are applied only one time during the registration of the Notes client. Changes to this document do not affect clients that are already connected and currently using the Notes client.	Mail template default Certificate expiration Internet mail address format

Document Type	Document Description	Primary Use
Archive	Controls the archive settings for the user's mail database. This policy document allows you to enable or disable archive and to control settings from a server or user perspective.	Notes client–based archive of folders Server-to-server-based archive Server-to-local-based archive
Desktop	Controls the user's Notes client desktop and environment settings. These settings are dynamic and are applied to the Notes client each time the user starts the client.	Default bookmarks Upgrades Welcome page
Security	Controls the password settings; that is, length, expiration, and creation requirements. This settings document also manages execution control list (ECL) settings and the synchronization of Internet and Notes passwords.	Passwords Security settings

As you research and identify the settings to be implemented, you will need to organize them into one of these policy documents. One method is to start by determining the various user groups and then decide on the settings that should be applied to each group. Once you know the groups and settings, you can create a policy with one or more settings.

Note

Policy documents were introduced in Lotus Notes version 6. Prior to the presentation of policy documents, Lotus Notes 5 utilized **"setup profiles."** As a best practice, eliminate the use of setup profiles and convert them to policy documents as you migrate to version 6 or later of the Notes client.

If you are running a mixed environment consisting of version 5 and higher-level clients, the policy document will only apply to those users running version 6 or higher of the Notes client.

Until all version 5 clients are upgraded, you will need to maintain both setup profiles and policy documents.

Understanding each type of settings document is fundamental to implementing a policy-based system for administration of client settings. Let's take a deeper look at the relationship between the policy and settings documents as it's important to understand the configuration options for both of these documents (see Figure 6.1).

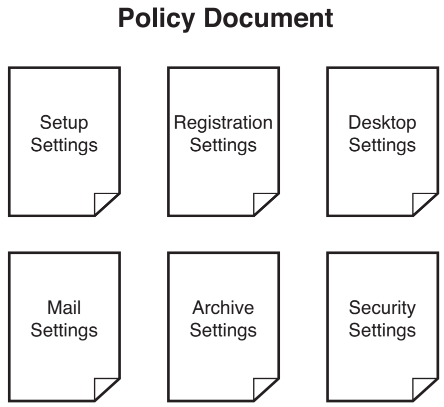


Figure 6.1 A policy document contains a number of settings that you can apply to the client environment to ensure consistent implementation across the company.

As previously stated, each policy document includes a number of settings. These settings are hierarchical in nature and can be implemented in a parent-child-like relationship. In this type of relationship, there is a parent or primary document that has one or more subordinate documents. The parent document setting always takes precedence and overrules a child setting. These policy documents can then be assigned to users or groups. Using this approach you can apply top-level settings across the organization and unique settings based on the group.

In addition to the parent-child relationship you can also **Inherit** and **Enforce** settings within the policy hierarchy.

An **Inherited Setting** is one in which the setting is automatically obtained based on another policy document. This keeps settings consistent from policy to policy.

An **Enforced Setting** is one where the parent document always overrules the child setting. Enforced settings are typically implemented when you want to implement a consistent setting across the organization. That said, here's how they are applied:

- An inherited setting can only be used or implemented in a child settings document. When the Inherit option is selected, the child policy document takes the setting from the parent policy document.
- If a child settings document contains a value and the Inherit setting option is selected, then the child setting is ignored and the parent policy setting takes precedence.
- An enforced setting can only be used or applied at the parent policy level. When selected, the parent policy setting is enforced and the child setting is ignored (if one has been specified).
- If a parent policy document has one or more child policy documents and neither the Inherit nor Enforce option has been selected, then the child setting takes precedence over the parent setting in the event of a conflict between settings.

- When multiple child-level policies are associated with a parent policy, the top-level (or first) child policy document has precedence over sibling policy documents in sequential order.

Table 6.2 shows how these rules are applied. It illustrates the parent-child relationship and the setting that will be implemented based on the Inherit and Enforce setting. The first column shows the parent document value. The second column shows the child document value. The third column represents how Domino manages these settings, based on the Inherit and Enforce setting, and the value to be implemented.

Table 6.2 Inherit and Enforce Value Precedence

Parent Document Setting	Child Document Setting	The Implemented Setting
Setting A	(No setting specified)	Setting A (Parent Value)
Setting A	Setting B, Inherit	Setting A (Parent Value)
Setting A, Enforce	Setting B	Setting A (Parent Value)
(No setting specified)	Setting B	Setting B (Child Value)
Setting A	Setting B	Setting B (Child Value)

NOTE

Lotus has issued a technical bulletin regarding the implementation of policy settings when using the Inherit and Enforce options. This bulletin, entitled "Policy settings not being applied correctly," provides additional information on how policies are applied when the Inherit and/or Enforce options are selected and a child document exists. To review this technical note, visit the following IBM Lotus Web site: www.ibm.com/support/docview.wss?uid=swg21307321.

Now let's review each of the policy documents. After reviewing the documents, you'll learn how to set up and configure these documents.

Archive Policy Document

The Archive document, as the name implies, is used to manage mail archive settings for the organization. Implementation tends to vary from company to company. Some choose to set up an archive policy whereas other companies rely on third-party software or the employee to archive mail to another medium (such as compact disc, shared network drive, or flash drive). Regardless of the method, you'll probably want to implement some method or process to manage archiving. Conversely, if you're working with sensitive information you might also want to disable the ability to archive information. When working with the Archive document, you'll want to have a clear understanding of and be able to answer the following questions:

- Should documents be archived?
- Which documents should be archived?
- When should documents be archived?
- What happens to the documents after being archived?

Using the Archive policy document you can fine-tune the archive process. The numerous settings allow you to

- Enable or disable archiving
- Specify the location of the archive—server or local
- Determine the archive selection criteria
- Record or log archive history
- Schedule the frequency in which archiving will occur
- Define what action to take after the document has been archived

The combination of these options offers great flexibility in the setup and administration of the archive process. Archiving works by removing mail files that meet certain criteria, such as date or age of the document, into a separate database. This subsequently frees up storage space and data management costs on both the server and the user's workstation.

The Basics Tab

Let's start with the Basics tab where you specify a name and provide a brief description of the Archive document. From here you can enable or disable the archive process and define the source and destination settings for archived documents. Table 6.3 describes the various fields of the Archive Policy.

Table 6.3 Basics Tab Field Descriptions

Field Name	Description
Prohibit archiving	A universal setting to completely prohibit all archiving.
Prohibit private archiving criteria	Disables the ability for users to define separate or private archive criteria.
Archiving source database:	The source location of the database to be archived. Archiving can occur at the server level or at the user (or local database) level.
Destination database:	The destination location for where to store all archived documents. Here you can elect to archive documents to a local workstation, Domino server, or mail server.

The Selection Criteria Tab

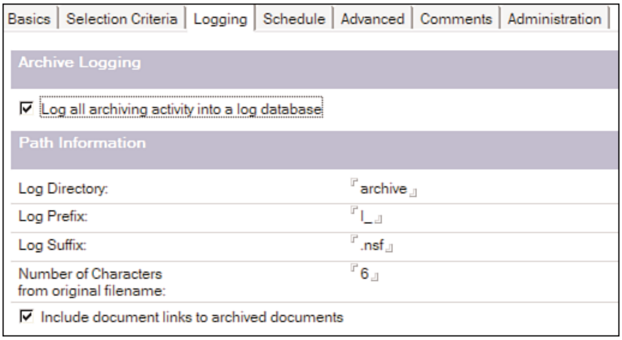
On the Selection Criteria tab, you specify one or more rules to govern what documents are archived. Multiple rules can be established. This allows you to create multiple archive settings documents to manage how and which documents are archived. For example, you might have a rule to manage the server-based archives and another for client-based archives. When taking this approach, you will need to create new selection criteria and then add them to the archive settings document. Table 6.4 outlines the fields associated with an archive rule.

Table 6.4 Selection Criteria Tab Field Descriptions

Field Name	Tab	Description
How should documents be archived	Basics	Administrators have the choice to "copy old documents into the archive database and then clean up the database" or to simply "clean up the database"
How should documents be cleaned up	Basics	When cleaning the database you can either "delete the document from the database" or "reduce the size of the document" to around 40k in size. If you decide to implement the "40k" size restriction, the e-mail will be trimmed to 40k. Any character that exceeds this threshold will be removed from the user's mail database. In other words, a partial message will be displayed. However, users will be able to view the entire message in the archive database.
Which documents should be cleaned up	Basics	Allows users to define which documents are archived based on the age or expiration date of the document.
Archive Directory	Destination	The destination tab allows you to set the default archive database filename and directory. The default directory path and name is "Archive."
Archive Prefix	Destination	A prefix can be appended to the filename to signify the database is an archive. Best practices recommend using "a_" as the prefix for all archive databases.
Archive Suffix	Destination	The suffix indicates the file type extension for the archive database. You will most likely want to keep the default value ".nsf" to allow access from the Notes client.
Number of characters from the original filename	Destination	The number of characters that will be taken from the original database and included in the archive database filename. For example, if the user's mail filename is "harryjones.nsf" and the value is set to 6 characters, then the archive filename would be "a_harryj.nsf" when using the default values.

The Logging Tab

The Logging tab in the “Archive settings” document allows you to record the history or log file information associated with the archive process (see Figure 6.2). This tab enables you to define whether logging is enabled and the name of the log file database.



Archive Logging

☑ Log all archiving activity into a log database

Path Information

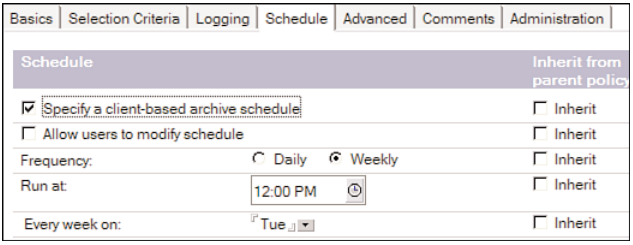
Log Directory:	archive
Log Prefix:	l_
Log Suffix:	.nsf
Number of Characters from original filename:	6

☑ Include document links to archived documents

Figure 6.2 The Logging tab allows you to define if and where to record archiving activities.

The Schedule Tab

The Schedule tab allows you to schedule when archiving will occur for client-based archives (see Figure 6.3). With this option enabled, you can set the frequency, start time, and day of the week to run.



Schedule		Inherit from parent policy
☑ Specify a client-based archive schedule		□ Inherit
□ Allow users to modify schedule		□ Inherit
Frequency:	○ Daily ● Weekly	□ Inherit
Run at:	12:00 PM	□ Inherit
Every week on:	Tue	□ Inherit

Figure 6.3 The Schedule tab allows administrators to set if and when client-based archives will occur.

The remaining three tabs—Advanced, Comments, and Administration—are self-explanatory and only contain one or two fields. For example, the Advance tab allows you to set the retention period in terms of years. The Comments tab is a free-form field and is blank by default. The Administration tab allows you to specify the owners and administrators for the document. These are, for the most part, standard tabs.

Tip

You can find additional information on how to create and manage archive policy settings on the IBM Web site. The article located at www.ibm.com/support/docview.wss?uid=swg27010310 includes step-by-step instructions and a free video presentation regarding the archive settings. It also includes links to the other settings documents.

Note

You should consider the performance impact to the Domino server and/or client when establishing an Archive Settings policy. To learn more about the potential impacts, read the IBM technical bulletin available at www.ibm.com/support/docview.wss?uid=swg21193740.

Registration Policy Document

The Registration policy document contains settings that are applied as new Lotus Notes users are created. These settings are applied when new users are registered in the Domino Directory and do not apply to existing users who have already been registered. Using this document you can manage the settings for

- Home mail server
- Internet address format
- Mail database quota size
- Mail template
- Password options and settings

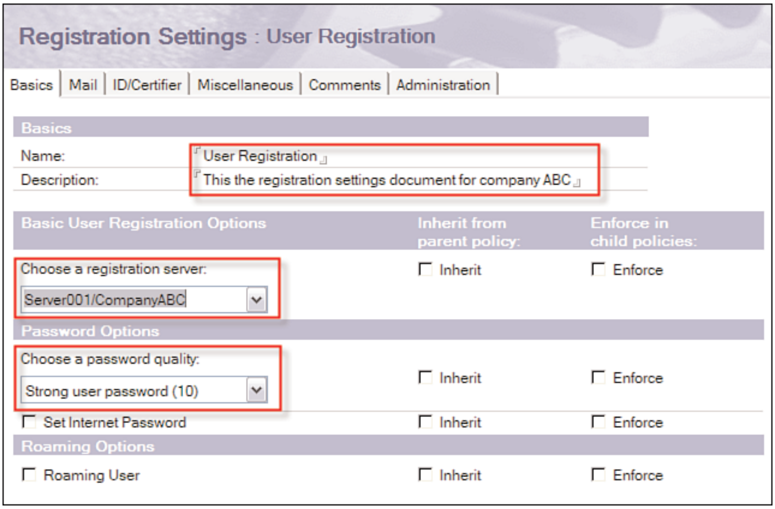
If your company utilizes both the Lotus Notes client and iNotes™, you can create a separate registration document for each type of user—one containing settings for those using the Notes client and another for those who access iNotes through a browser. However, where possible, best practices recommend a single registration document that contains all the settings in a single location. This will simplify management and administration of settings across the organization.

Having a registration document will also reduce the time and effort needed for setting up new users. Instead of having to add similar information and settings during the "registration" process, these settings will automatically be applied to the new user based on the registration policy document. The policies will be applied in a consistent manner, but will be based on the current settings document. So, changes made to the registration document will not be applied to users that were previously registered.

There are several ways to create a registration document: by navigating to the **Settings** view located on the **People & Groups** tab in the Administrator client or by choosing **Policies > By Settings** in the Domino Directory.

The Basics Tab

Let's take a closer look at the registration settings document and some of the associated options, starting with the Basics tab (see Figure 6.4). When creating a registration document you first need to provide a name and general description of the policy. You'll also need to specify the Domino server that's used for user registration and the password strength. Optionally, you can also specify to set the Internet password if users will access Notes from the browser.


Registration Settings : User Registration
Basics | Mail | ID/Certifier | Miscellaneous | Comments | Administration

Basics

Name:	User Registration
Description:	This the registration settings document for company ABC

Basic User Registration Options	Inherit from parent policy:	Enforce in child policies:
Choose a registration server: Server001/CompanyABC	□ Inherit	□ Enforce
Password Options		
Choose a password quality: Strong user password (10)	□ Inherit	□ Enforce
□ Set Internet Password	□ Inherit	□ Enforce
Roaming Options		
□ Roaming User	□ Inherit	□ Enforce

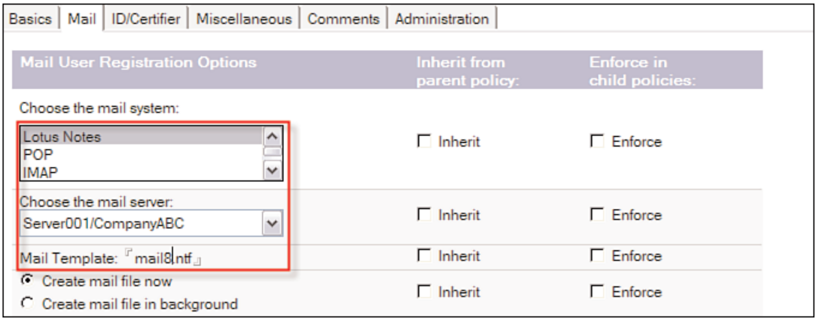
Figure 6.4 The Basics tab of the Registration Settings document.

The Mail Tab

Next, the Mail tab contains three primary sections: Mail user registration options (shown in Figure 6.5), Internet address options, and Advance Mail options. Start by selecting the mail system type. This option governs what subsequent options are displayed.

In most cases, you'll want to select "Lotus Notes" as the primary mail system along with the designated mail server. There's also an option to designate a default mail template file. As users are registered, this template will be used as the basis to create their mail database.

If your company uses consultants who have their mail hosted on another system, it might be beneficial to create a setting that has Other Internet as the mail system. This option can be very useful in organizations with large numbers of consultants.


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

Mail User Registration Options	Inherit from parent policy:	Enforce in child policies:
Choose the mail system: Lotus Notes POP IMAP	☐ Inherit	☐ Enforce
Choose the mail server: Server001/CompanyABC	☐ Inherit	☐ Enforce
Mail Template: mail8.ntf	☐ Inherit	☐ Enforce
● Create mail file now ○ Create mail file in background	☐ Inherit	☐ Enforce

Figure 6.5 In the first section of the Mail tab you select the mail system, mail server, and default mail template for user registration.

Note

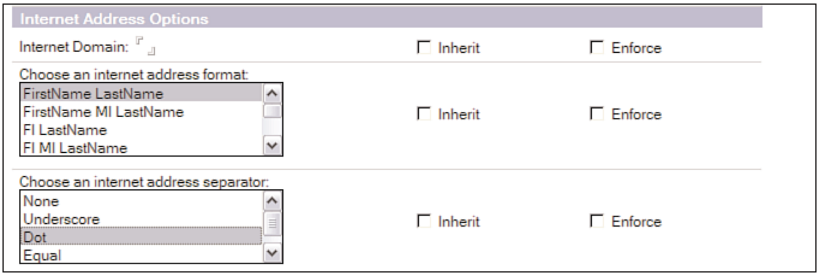
The Registration Settings document allows you to specify how new mail files will be generated: either “Create Mail File Now” or “Create Mail File in the Background.” The default option is to immediately create the mail file. It’s important to understand how these options will impact your Domino Administrator client.

Using the default option, “Create Mail File Now,” your Domino Administrator client will be locked (that is, waiting on the hourglass) as the new mail file is generated. If you find the time required to generate the new mail file is longer than desired, you can select the “Create Mail File in the Background” option. This selection will free up your Administrator client and generate the mail file in the background. This setting is especially important for administrators who access the system from a dialup (or non-broadband) connection.

Tip

You can find additional information on how to create a Mail Settings policy document on the developerWorks Web site. The article, entitled “Creating Mail policies in Lotus Notes/ Domino 7” was written by Timothy Speed and Terry Fouchey. This document focuses specifically on how to manage calendar and mail settings for users. Visit www.ibm.com/ developerworks/lotus/library/domino7-mail-policy to view this document.

The Internet Address Options section allows you to apply a consistent format to the Internet address (see Figure 6.6). There are multiple format options. You should give careful consideration to the format so that a consistent format is established from the onset of the user registration process. You can also specify the delimiter that will be used to separate values, such as the “dot” or "underscore." For example, the Internet addresses could be John.Doe@companyABC.com or John_Doe@companyABC.com.



Internet Address Options

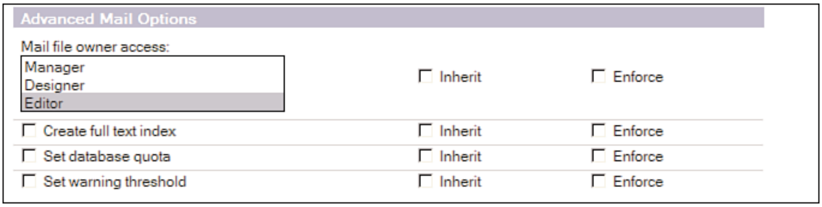
Internet Domain: □ Inherit □ Enforce

Choose an internet address format: □ Inherit □ Enforce
FirstName LastName
FirstName MI LastName
FI LastName
FI MI LastName

Choose an internet address separator: □ Inherit □ Enforce
None
Underscore
Dot
Equal

Figure 6.6 The Internet Address Options section enables you to apply a common address format to all newly registered users.

The last section of the "Mail tab" contains the Advanced Mail options (see Figure 6.7). This section enables you to set the default access level of the user for the mail database, establish a full text index, set a database size quota, and set the warning threshold as users approach the size quota. At a minimum, you should consider which users will have the Manager, Designer, or Editor authority to the mail database.



Advanced Mail Options

Mail file owner access: □ Inherit □ Enforce
Manager
Designer
Editor

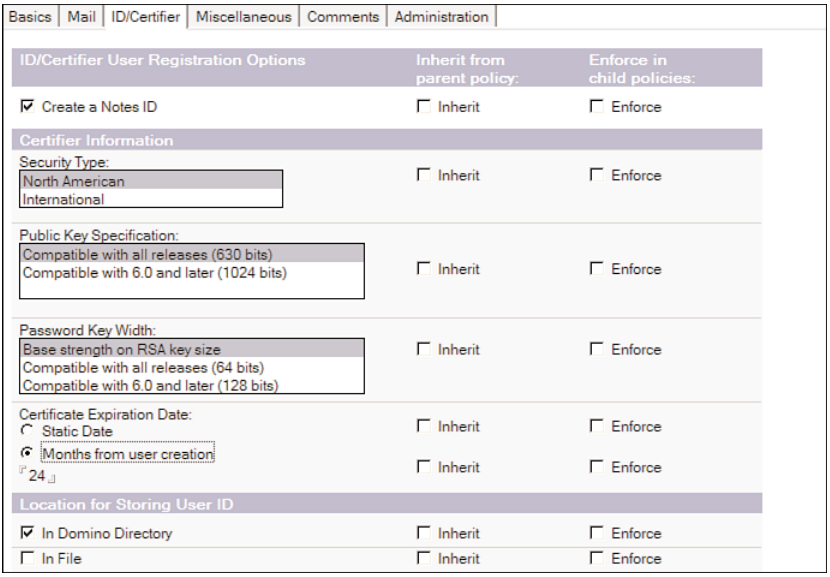
□ Create full text index □ Inherit □ Enforce
□ Set database quota □ Inherit □ Enforce
□ Set warning threshold □ Inherit □ Enforce

Figure 6.7 The Advanced Mail Options section of the Mail tab allows you to set the default access, index, quota, and threshold value pertaining to the user's mail database.

By default, users will be granted **Editor** access to their mail database. Alternatively, you can select **Designer** or **Manager** access. Users who have Editor access will be able to create, modify, or delete any document created in the mail database. Users with Designer authority will have the ability to perform the same actions as Editors plus the ability to modify the design of the mail database, but they cannot modify the ACL permissions. Finally, users with Manager access can perform all the same transactions available to lower access levels, plus they have the ability to modify the ACL, encrypt the database design, modify replication settings, and compact and/or delete the mail file database.

The ID/Certifier Tab

The ID/Certifier tab of the Registration Settings document enables you to specify several key aspects of the users' ID and Certifier, both of which pertain to user ID security (see Figure 6.8). Start by determining whether an ID file will be created. In general, companies running Lotus Notes clients will want to create and store the ID file. By default this file will be stored in the Domino Directory.



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

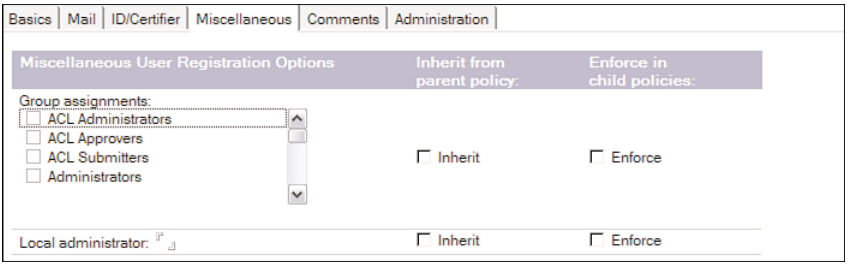
ID/Certifier User Registration Options	Inherit from parent policy:	Enforce in child policies:
☑ Create a Notes ID	□ Inherit	□ Enforce
Certifier Information		
Security Type: North American International	□ Inherit	□ Enforce
Public Key Specification: Compatible with all releases (630 bits) Compatible with 6.0 and later (1024 bits)	□ Inherit	□ Enforce
Password Key Width: Base strength on RSA key size Compatible with all releases (64 bits) Compatible with 6.0 and later (128 bits)	□ Inherit	□ Enforce
Certificate Expiration Date: ○ Static Date	□ Inherit	□ Enforce
● Months from user creation 24	□ Inherit	□ Enforce
Location for Storing User ID		
☑ In Domino Directory	□ Inherit	□ Enforce
□ In File	□ Inherit	□ Enforce

Figure 6.8 The ID/Certifier tab contains security settings associated with the users' Notes ID.

From an administrative perspective, you'll want to determine the storage location that is most appropriate for your company. Finally, you can set the security type and the certificate expiration date. Using a static date means the ID will expire on a specific date. The default is two years from the date of registration. Alternatively, you can state an arbitrary duration in terms of months for when the ID will expire. These values can affect the employees' ability to access their Notes client. Be sure to review the Domino Administrator online help for supplemental information.

The Miscellaneous Tab

The Miscellaneous tab contains miscellaneous settings pertaining to groups (see Figure 6.9). Here you can automatically assign users to groups that have been defined in the Domino Directory as part of the registration process. In many cases, no action will be needed here.



Miscellaneous User Registration Options	Inherit from parent policy:	Enforce in child policies:
Group assignments: □ ACL Administrators □ ACL Approvers □ ACL Submitters □ Administrators	□ Inherit	□ Enforce
Local administrator:	□ Inherit	□ Enforce

Figure 6.9 The Miscellaneous tab allows you to add the user to one or more groups as part of the registration.

The Comments and Administration Tabs

The remaining tabs, Comments and Administration, are straightforward. The Comments tab contains a freeform text field where you can add any personal notes or other information regarding the Registration document. The Administration tab allows you to specify all persons who have the authority to modify the document. Specifically, you can specify the owner and administrators associated with the registration settings.

> **Note**
>
> You might notice after reviewing the Registration Settings document that some Notes settings cannot be managed from a policy document. Some of these settings include the Unique Organization Unit, Location, Comment, Preferred Language, and Alternate Name Language, just to name a few.

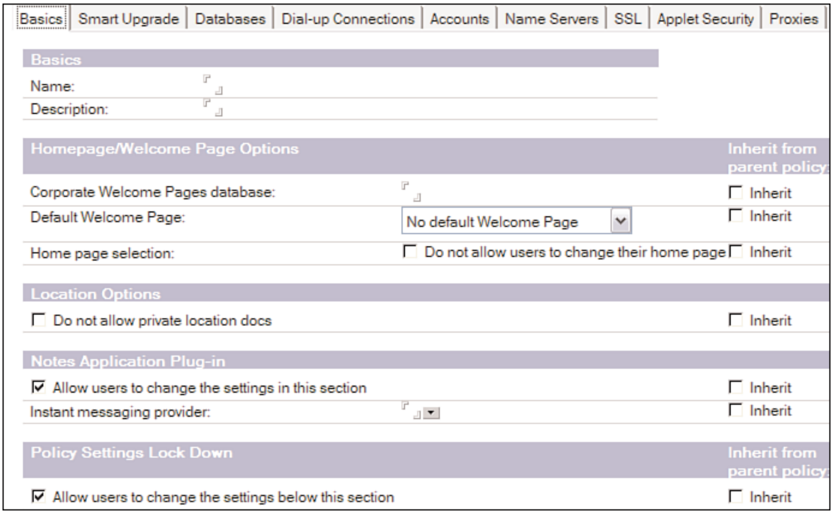
Dynamic Desktop Setting

The Dynamic Desktop setting (previously called the Desktop policy document) manages various aspects of the Notes Desktop for users. The settings affect all users in the Notes community—which is different from the Registration settings document. If you recall, Registration settings only affect users at the time of registration and do not affect existing (already registered) users. However, with the Dynamic Desktop document, these settings are dynamic. Changes to these settings will migrate down to all Notes clients.

When you open this document you'll notice a rather significant number of options. Some of these options extend beyond the general settings associated with the client desktop. Other settings, such as those on the Smart Upgrade tab, are covered in Chapter 5, "Managing Upgrades." So, for the purposes of this chapter, we'll focus on key areas that affect management of the user's desktop rather than all options and settings associated with the Dynamic Desktop policy.

The Basics Tab

The Basics tab contains general settings associated with the Notes client (see Figure 6.10). As with all policy and settings documents, start by specifying a document name and description in the Basics tab. Next you can optionally specify a default welcome page.



Basics

Name:

Description:

Homepage/Welcome Page Options — Inherit from parent policy

Corporate Welcome Pages database: □ Inherit

Default Welcome Page: No default Welcome Page □ Inherit

Home page selection: □ Do not allow users to change their home page □ Inherit

Location Options

□ Do not allow private location docs □ Inherit

Notes Application Plug-in

☑ Allow users to change the settings in this section □ Inherit

Instant messaging provider: □ Inherit

Policy Settings Lock Down — Inherit from parent policy

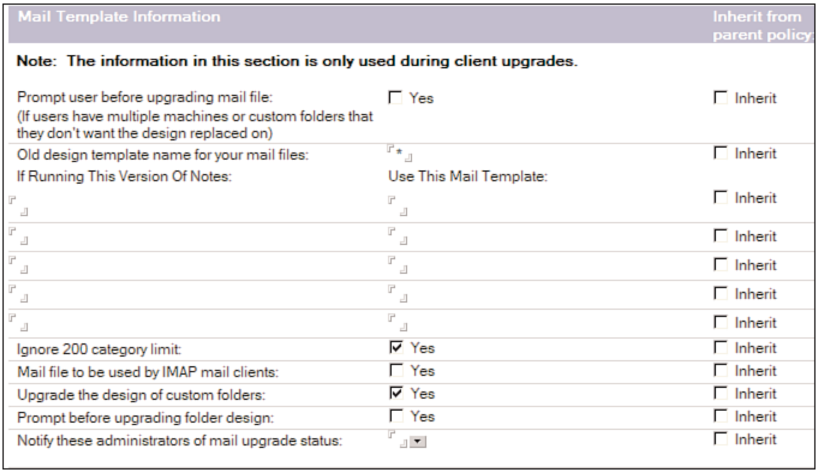
☑ Allow users to change the settings below this section □ Inherit

Figure 6.10 The Basics tab for the Dynamic Desktop document.

The Location Options section enables you to control whether users have the ability to create Location documents on their workstation where the Notes client resides. This option, along with countless other options within the document, enables you to control whether users have the ability to modify, create, or change settings from their client application. For example, you can control whether users have the ability to manage "plug-ins," the default Domino server directory, Instant Message server, default browser to launch, and so forth.

Many readers will find the "Create Local Mail File Replica" option of particular interest. This option allows a local instance of the mail file to be created on a user's workstation. Generally speaking, most administrators will want to enable this option to permit replication.

In the Mail Template Information section (see Figure 6.11), you choose how to communicate with the user and how mail templates are managed during client upgrades. You can prompt users before upgrading their mail file. This option works in conjunction with the Smart Upgrade. You can also elect to automatically upgrade the design of their custom folders. See Chapter 5 for more information.



Mail Template Information		Inherit from parent policy
Note: The information in this section is only used during client upgrades.		
Prompt user before upgrading mail file: (If users have multiple machines or custom folders that they don't want the design replaced on)	□ Yes	□ Inherit
Old design template name for your mail files:	*	□ Inherit
If Running This Version Of Notes:	Use This Mail Template:	
		□ Inherit
		□ Inherit
		□ Inherit
		□ Inherit
		□ Inherit
Ignore 200 category limit:	☑ Yes	□ Inherit
Mail file to be used by IMAP mail clients:	□ Yes	□ Inherit
Upgrade the design of custom folders:	☑ Yes	□ Inherit
Prompt before upgrading folder design:	□ Yes	□ Inherit
Notify these administrators of mail upgrade status:	▾	□ Inherit

Figure 6.11 Using the Mail Template Information settings you can control how upgrades are applied to users' mail database design.

The Databases Tab

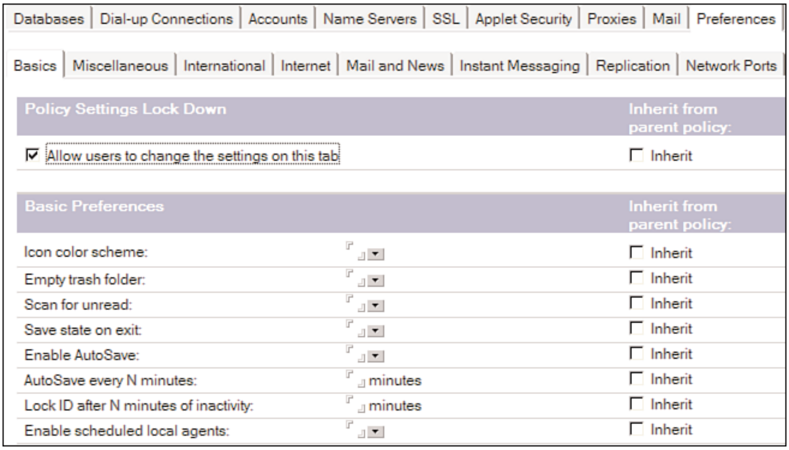
If you have a common set of databases that all employees should have access to, you can add them in the "Database Links" section of the Databases tab. Simply drag and drop the database into the "Default Databases Added to Bookmarks" field. All database links will then appear in the user's bookmarks database.

The Preferences Tab

The "Preferences" tab is another section that you should review when creating a Dynamic Desktop settings document (see Figure 6.12). By default, users will have the ability to modify some of their settings from the Notes client. By going to the appropriate section in the client preferences, users can modify certain values associated with the Notes client. On the Preferences tab you can define certain default values and settings, or if you do not want users to be able to modify settings, you can disable the ability for users to modify their client settings.

Tip

A technical bulletin has been issued that describes how to set values in the notes.ini file and Location document using the Dynamic Desktop settings policy. To learn more about how this works, read the technical note located at www.ibm.com/support/docview.wss?uid=swg21196837.


Databases | Dial-up Connections | Accounts | Name Servers | SSL | Applet Security | Proxies | Mail | Preferences
Basics | Miscellaneous | International | Internet | Mail and News | Instant Messaging | Replication | Network Ports

Policy Settings Lock Down		Inherit from parent policy:
☑ Allow users to change the settings on this tab		□ Inherit

Basic Preferences		Inherit from parent policy:
Icon color scheme:	▾	□ Inherit
Empty trash folder:	▾	□ Inherit
Scan for unread:	▾	□ Inherit
Save state on exit:	▾	□ Inherit
Enable AutoSave:	▾	□ Inherit
AutoSave every N minutes:	minutes	□ Inherit
Lock ID after N minutes of inactivity:	minutes	□ Inherit
Enable scheduled local agents:	▾	□ Inherit

Figure 6.12 You can fine-tune the preference settings for the user's client in the "Preferences" tab.

Initial Desktop Setup

The Initial Desktop Setup (previously called a Setup policy document) is used to control the initial setup settings. These settings are applied as part of the installation process and are applied only one time. You'll also notice that many of the settings found in the Initial Desktop Setup document are also found in the Dynamic Desktop document.

In fact, the Initial Desktop Setup document is a subset of the Registration document. So, you can apply the settings once during the initial setup and then manage them long term using the Registration document. Just remember the Initial Desktop Setup policies only apply once during the installation process.

If you modify the Initial Desktop Setup settings document, the settings will only apply to new software installations that are performed subsequent to the modification. No changes will be applied to existing Notes clients.

From an implementation perspective, you'll probably want to keep the Initial Desktop Setup document and Registration document synchronized. Or, alternatively, primarily use the Registration document as the primary method for managing client settings.

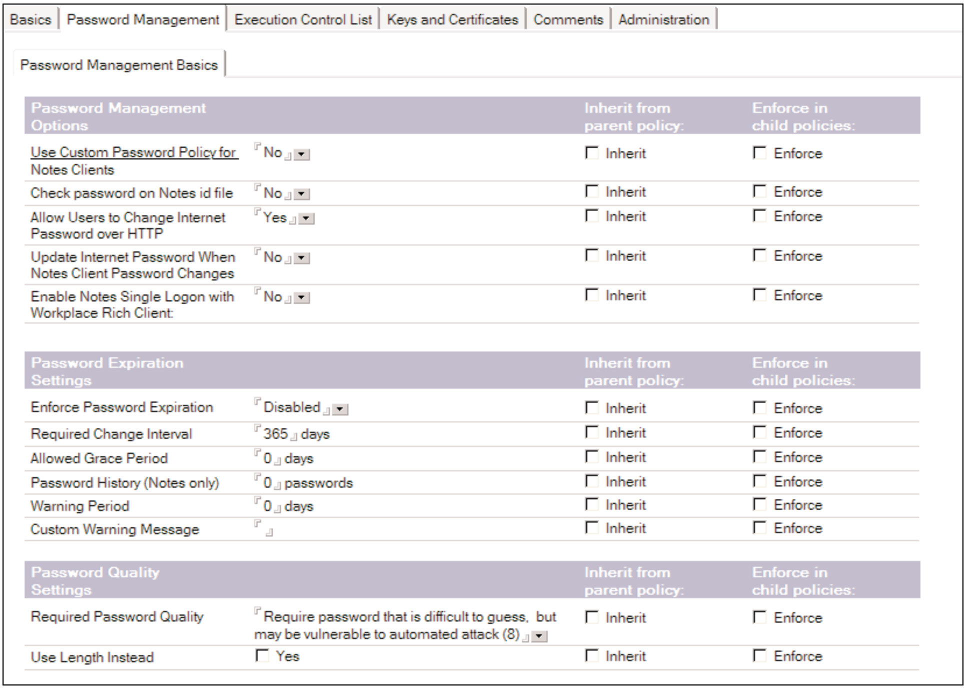
The settings specified in the Initial Desktop Setup document will be applied after the client has been installed and connects to the Domino server for the first time. This is the last step in the install process. Once the settings are applied to the client, a pop-up message will appear stating the "Notes Setup Is Complete."

Tip

You can use the Initial Desktop Setup document to implement mail replicas. If you are considering implementing a standard for mail replicas across the company, you can use the Initial Desktop Setup policy to manage a consistent implementation. You can learn more about how to implement such an approach in the article "Understanding and Implementing Local Mail Replicas for IBM Lotus Notes," by Joseph Anderson and Peter Burkhardt. You can find it at the following developerWorks Web site: www.ibm.com/developerworks/lotus/library/local-mail-replicas.

Security Policy Document

The primary focus of the Security policy document is password management. You can find the majority of the settings on the "Password Management" tab (see Figure 6.13). Here you can define the settings for three areas—Password Management, Password Expiration, and Password Quality.



Password Management Options		Inherit from parent policy:	Enforce in child policies:
Use Custom Password Policy for Notes Clients	No	□ Inherit	□ Enforce
Check password on Notes id file	No	□ Inherit	□ Enforce
Allow Users to Change Internet Password over HTTP	Yes	□ Inherit	□ Enforce
Update Internet Password When Notes Client Password Changes	No	□ Inherit	□ Enforce
Enable Notes Single Logon with Workplace Rich Client:	No	□ Inherit	□ Enforce

Password Expiration Settings		Inherit from parent policy:	Enforce in child policies:
Enforce Password Expiration	Disabled	□ Inherit	□ Enforce
Required Change Interval	365 days	□ Inherit	□ Enforce
Allowed Grace Period	0 days	□ Inherit	□ Enforce
Password History (Notes only)	0 passwords	□ Inherit	□ Enforce
Warning Period	0 days	□ Inherit	□ Enforce
Custom Warning Message		□ Inherit	□ Enforce

Password Quality Settings		Inherit from parent policy:	Enforce in child policies:
Required Password Quality	Require password that is difficult to guess, but may be vulnerable to automated attack (8)	□ Inherit	□ Enforce
Use Length Instead	□ Yes	□ Inherit	□ Enforce

Figure 6.13 Password management should be a key consideration when creating policy settings for the Notes client.

The first section, Password Management, allows you to determine how passwords are implemented for the Lotus application. Table 6.5 describes each of the fields along with the default and recommended settings.

Table 6.5 Password Management Field Descriptions

Field Name	Description	Default	Recommend
Use Custom Password Policy for Notes Clients	Uses custom password requirements for Notes password checking. Using custom password parameters enables you to enhance security to ensure they are not predictable. An additional configuration tab appears after you change the default value to "Yes." This secondary tab allows you to define all the rules a user must follow when generating a password. Some of the settings include • Minimum password length • Minimum number of alphabetic characters • Minimum number of numeric characters • Number of unique characters • Allow common name • Number of uppercase characters • Number of lowercase characters	No	Yes
Check password on Notes ID file	Requires all copies of the user ID to have the same password.	No	No
Allow Users to Change Internet Password over HTTP	Allows users to use the browser to change their Internet passwords. If you do not use the Internet to access Notes, you can set this value to "No."	Yes	Yes, if iNotes is used. No, if not used.
Update Internet Password When Notes Client Password Changes	Synchronizes the users' Internet password with their Notes client password.	No	No
Enable Notes Single Logon with Workplace Rich Client:	Allows workplace users to use the same password for Notes and Workplace™ Rich client. Setting this value to "Yes" enables a single logon between the Notes client and the IBM Workplace Rich client.	No	No

The "Password Expiration Settings" section allows you to control how long a password can be used and the frequency in which the password must be changed. The default values are set rather loosely and many administrators will want to change the values to enforce a tighter level of security. Table 6.6 describes the Password Expiration Settings options.

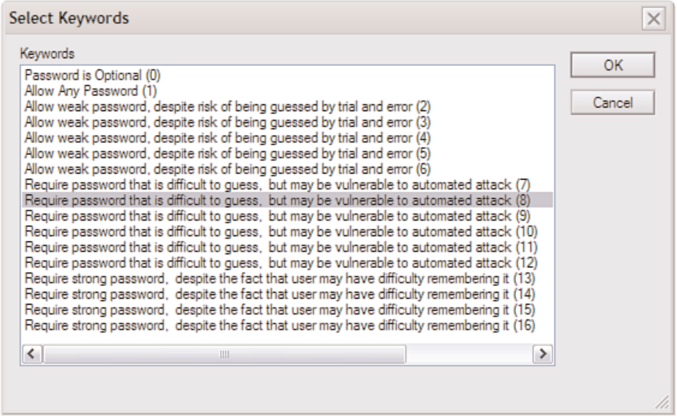
Table 6.6 Password Expiration Settings Field Descriptions

Field Name	Description	Default	Recommend
Enforce password expiration	Requires password expiration. The default is set to Disabled. As a general best practice, users should be required to change their password on a regular basis. WARNING: Do not enable password expiration if smart cards are used to log in.	Disabled	Notes only, Internet only, or Notes & Internet (based on your setup).
Required change interval	The interval in which users must change their password. The default setting is one year. Many administrators will want to change the interval to a more frequent basis, such as Quarterly. Be careful not to set the interval too low as changing the password on a weekly basis could frustrate users and impede work.	365	120
Allowed grace period	The number of days the user is allowed to continue using the Notes client after the expiration date has been reached. Setting this value to 0 will force users to change their password once their password has expired.	0	0
Password history (Notes only)	The number of expired passwords to be tracked. The user can only reuse a password after the specified number has been reached. This prevents the user from reusing the same password over and over. The higher the number the less frequently a user can reuse the password.	50	50

Field Name	Description	Default	Recommend
Warning period	The number of days before a password expires to notify the user. Notes will automatically calculate when to send a notification if this value is set to a value less than 30. Password expiration must be enabled in order to use this field.	0	0
Custom warning message	If you desire, you can specify a custom warning message to be sent to the users when their password is about to expire. This field only applies to the Notes client password.	<Blank>	This is an optional field setting.

The final section in the Password Management tab allows you to manage the quality settings. The higher the password quality, the less likely an intruder will be able to gain access via a password.

When looking at this section, you'll notice there are two fields and approaches to managing password quality, as shown at the bottom of Figure 6.13. The default approach allows you to select a quality level based on a scale of values. It is called the "Required Password Quality" and is set to "Require Password That Is Difficult to Guess, But May Be Vulnerable to Automated Attack (8)." You can select the password quality that is implemented by clicking on the dropdown and selecting a new value, as shown in Figure 6.14.


Select Keywords

Keywords

Password is Optional (0)
Allow Any Password (1)
Allow weak password, despite risk of being guessed by trial and error (2)
Allow weak password, despite risk of being guessed by trial and error (3)
Allow weak password, despite risk of being guessed by trial and error (4)
Allow weak password, despite risk of being guessed by trial and error (5)
Allow weak password, despite risk of being guessed by trial and error (6)
Require password that is difficult to guess, but may be vulnerable to automated attack (7)
Require password that is difficult to guess, but may be vulnerable to automated attack (8)
Require password that is difficult to guess, but may be vulnerable to automated attack (9)
Require password that is difficult to guess, but may be vulnerable to automated attack (10)
Require password that is difficult to guess, but may be vulnerable to automated attack (11)
Require password that is difficult to guess, but may be vulnerable to automated attack (12)
Require strong password, despite the fact that user may have difficulty remembering it (13)
Require strong password, despite the fact that user may have difficulty remembering it (14)
Require strong password, despite the fact that user may have difficulty remembering it (15)
Require strong password, despite the fact that user may have difficulty remembering it (16)

Figure 6.14 The Password Quality Settings area enables administrators to choose the password strength to be implemented across the organization.

An alternative approach that you can use to set the password quality is based on the length of the password. From an implementation perspective, the password is accepted or rejected entirely based on the length of the password as opposed to the quality of the password. To use this approach, simply select YES in the "Use Length Instead" field and specify a numeric value.

The Execution Control List tab, starting with release 6, allows you to specify how updates to the Execution Control List (ECL) are distributed to the user. The default values allow Notes to automatically manage the user's ECL. These settings are sufficient for most companies. You can find additional information on ECL administration in the Domino online help database.

NOTE

IBM has issued a technical bulletin regarding ECL alerts and custom mail templates. In certain circumstances, users may receive alert messages for the person who signed the Mail template. The bulletin, which provides additional information on how to resolve the issue, is at the following Web site: www.ibm.com/support/docview.wss?uid=swg21224814.

TIP

You might be interested to know there is an IBM Redbook called the "Lotus Security Handbook." This free publication is available online. It provides detailed information on all aspects of Domino security, including Execution Control Lists (ECL). It is available on the IBM Web site at www.redbooks.ibm.com/abstracts/SG247017.html?Open.

What Is a Policy Architecture?

What is a policy architecture? A policy architecture is a collection of policy documents, with associated settings documents, that are applied to a group of users. In order to create a policy document, you first need to create the settings to be applied to a particular policy. Next you need to understand there are two types of policy documents—explicit and organizational.

What Is an Organizational Policy?

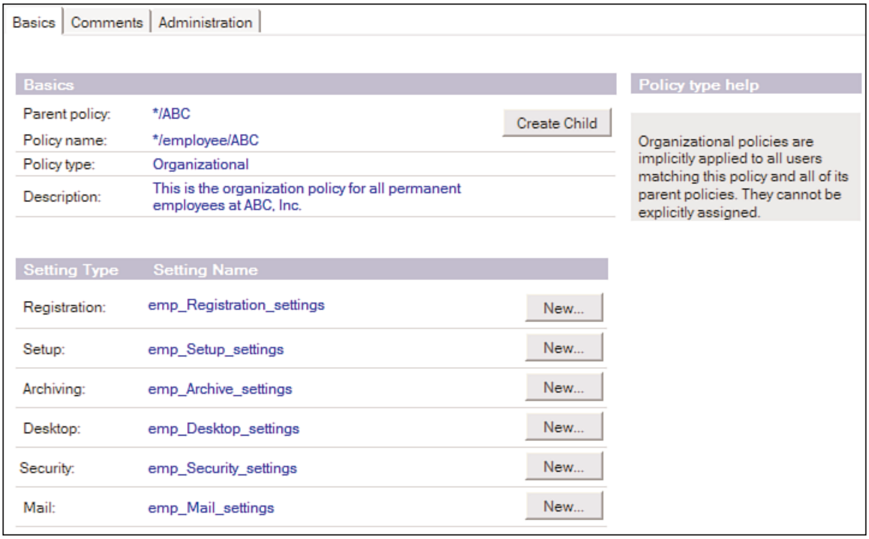
An **organizational policy** is one in which all settings are applied, or inherited, by all members of a specific organization. Using this approach allows you to automatically apply settings based on the organization unit in which users are a member.

For example, let's say your company—called ABC—retains both permanent employees and part-time interns, and that all registered users belong to either the */employee* or the */intern* organization unit. You could then create an organizational policy where all users in **/employee/ABC* automatically inherit its settings. You could then apply a second policy that would apply to all users in the **/intern/ABC* organizational policy.

By creating separate policies, you allow employees to have greater flexibility and control over their Notes client environment and, conversely, restrict the ability of part-time interns to modify their environment settings. Thus all employees are governed by a common set of configuration settings based entirely on the organizational unit (which is defined when the user created or registered in the Domino Directory).

The organization-based policy is generally considered to be the easiest method for managing client workstation settings. Furthermore, this approach provides flexibility to accommodate changes to organization structure. So, if a part-time intern graduates from college and subsequently becomes a permanent full-time employee, all you need to do is update the user's organization unit. The user will then automatically inherit the new policy settings the next time she authenticates with her Domino server (following the status change to the organization unit value).

Figure 6.15 depicts a sample organizational policy for full-time employees. You'll notice that the settings documents all start with *emp_* to help identify the settings that are specific to employees.



Basics

Parent policy:	*/ABC
Policy name:	*/employee/ABC
Policy type:	Organizational
Description:	This is the organization policy for all permanent employees at ABC, Inc.

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:	emp_Registration_settings
Setup:	emp_Setup_settings
Archiving:	emp_Archive_settings
Desktop:	emp_Desktop_settings
Security:	emp_Security_settings
Mail:	emp_Mail_settings

Figure 6.15 A sample organizational policy for all full-time employees.

An organizational policy for the intern employees would look similar to this form except the policy name would be **/intern/ABC* and a different set of settings documents would be defined and selected. Using this same approach, you could prefix all intern settings documents with *intern_* to distinguish them from the employee settings.

Warning

Do not include spaces in the policy name. Domino will interpret the space as a separate policy. In other words, Domino will consider the space to be one policy name and the characters immediately following to be a second policy name. As a best practice, the policy name should contain characters and no spaces. Also note that all policy names must be unique. Duplicate policy names can cause Domino implementation problems. For additional information, you can view the technical bulletin posted on the IBM Web site at www.ibm.com/support/docview.wss?uid=swg21245914.

What Is an Explicit Policy?

An explicit policy, on the other hand, is one in which the policy applies only to specified users or user groups. Using this approach you must explicitly define the users who are associated with the policy. While it's true this approach does require more time and effort to administer, the policy does have advantages. To be specific, this type of policy is frequently used for users who require custom configuration settings. It can also be used for groups that encompass multiple organization units.

Similarly to the organization policy, an explicit policy will contain a collection of settings documents. However, using the explicit policy, you must perform additional setup in order to implement it. If you recall, users automatically inherit the settings as members of an organizational policy. However, when creating an explicit policy you must take an additional step and update users' Person document with the assigned policy. For those of you familiar with "Setup Profiles" in version 5, this process is similar to that one; however, only one explicit policy can be assigned in the Person document.

For example, let's revisit company ABC. We've already learned it has both full-time employees and part-time interns. Continuing with this example, the company also employs a number of subcontract employees. These specialty employees typically come onsite for a short duration as technical experts in a certain field. The contract employees may reside in multiple organizations. Using the explicit policy you could manage the contractors and customize their settings.

Tip

Using an explicit policy you can create a custom welcome page when users first launch the Lotus Notes client. To learn more about this feature and for step-by-step instructions, you can read the article "Rolling out a Corporate Web Welcome Page" by Cara Haagenson. This article is available at the developerWorks Web site at www.ibm.com/developerworks/lotus/library/ls-WelcomePage/.

Just to summarize for a moment, most companies will utilize a combination of both organizational and explicit policies. Organizational policies are automatically applied settings based on the organizational unit. Explicit policies, on the other hand, are created in advance and assigned as part of the user registration. The combination of these policies provides a centralized approach to managing and controlling Lotus Notes client settings. As discussed earlier in this chapter, there are six primary settings documents that you can define for a policy. These settings include Setup, Registration, Desktop, Mail, Archive, and Security. The Setup and Registration settings are applied one time. The remaining are dynamically applied. Policy documents are hierarchical in nature. This means that some settings trump other settings based on the Inherit and Enforce options and the parent-child relationship.

Creating Settings and Policy Documents

You should now have a rudimentary understanding of the settings document and policy document types. You should also have a thorough understanding of the organizational groups that comprise your company and user community. And, you will need to know the settings to be applied to each of the organizational units within your company. Finally, you will need to have the Domino Administrator client installed with the appropriate access level to create policies.

To get started, you must be listed in the Domino Directory ACL and assigned, at a minimum, the **[Policy Creator]** and **[Policy Modifier]** roles. Complete the following steps to check your authority level. If you do not have this authority, you will need to work with a Domino administrator to obtain these roles.

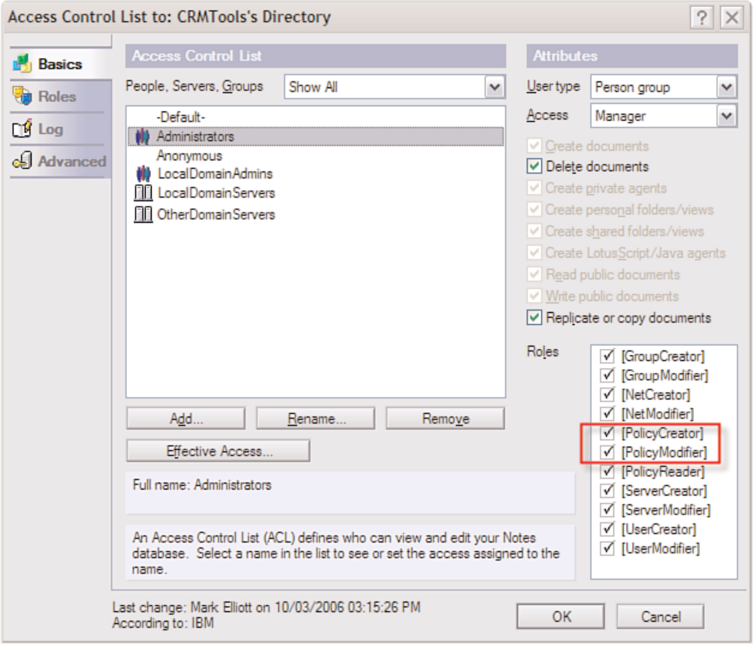
Step 1. Locate the Domino Directory icon from your Notes client.

Step 2. Select the **File > Application > Access Control** menu option.

Step 3. Locate and click on your name. Verify you have the **[Policy Creator]** and **[Policy Modifier]** roles assigned to your ID, as shown in Figure 6.16. Note: Some companies use group names to manage access. If your name does not appear in the ACL, you will need to review the group names by opening the Domino Directory and manually checking the groups listed in the ACL.

Step 4. Click **OK** to save the settings.

You're now ready to start creating the policy documents.



Access Control List to: CRMTools's Directory

Access Control List

People, Servers, Groups: Show All

-Default-
Administrators
Anonymous
LocalDomainAdmins
LocalDomainServers
OtherDomainServers

Attributes

User type: Person group

Access: Manager

☑ Create documents
☑ Delete documents
☑ Create private agents
☑ Create personal folders/views
☑ Create shared folders/views
☑ Create LotusScript/Java agents
☑ Read public documents
☑ Write public documents
☑ Replicate or copy documents

Roles:
☑ [GroupCreator]
☑ [GroupModifier]
☑ [NetCreator]
☑ [NetModifier]
☑ [PolicyCreator]
☑ [PolicyModifier]
☑ [PolicyReader]
☑ [ServerCreator]
☑ [ServerModifier]
☑ [UserCreator]
☑ [UserModifier]

Full name: Administrators

An Access Control List (ACL) defines who can view and edit your Notes database. Select a name in the list to see or set the access assigned to the name.

Last change: Mark Elliott on 10/03/2006 03:15:26 PM
According to: IBM

Figure 6.16 You must be assigned the Policy Creator and Policy Modifier roles in the ACL in order to manage policies.

Creating Policy Documents

Before you create a policy document you'll need a clear understanding of the settings and policy type to be associated with a particular user group. Once this has been determined, and you have sufficient authority via the Domino Administrator client, you're ready to go. The following steps provide a general overview on how to create a policy document.

Step 1. Launch the Domino Administrator client.

Step 2. Navigate to the **People & Groups** tab.

Step 3. Select the **Policies** view.

Step 4. Select the **Actions > Add Policy** menu option or select the **Add Policy** action button.

Step 5. If a warning message appears, review the message and verify you are in compliance. Click **OK** to continue.

Step 6. Specify a **Policy Name** (for example, */employee/ABC).

Step 7. Select the **Policy Type**.

Step 8. Provide a short descriptive abstract for the document (e.g. "This is the Organization Policy document for permanent employees.").

Step 9. Configure the settings associated with the policy. For each setting that's applicable, you'll need to click the **New** button and complete the related document. Note: You can also create these settings documents by navigating to the Settings view, which is also found in the People & Groups tab.

After all settings have been defined, save and close the document. The policies will then be applied as new employees are registered in the Domino Directory. The Notes configurations settings will be applied the user's client based on the settings document type. If you recall, settings are applied during installation, registration settings are applied the first time the user connects to the server, desktop settings are applied dynamically, and so forth.

Registering a New User Using an Explicit Policy

If you recall, an additional setup step is required in order to implement an explicit policy. With this type of policy you must update the Person document in addition to the creation of the Policy and Settings documents. This section illustrates how to go about applying an explicit policy when registering a new user.

As a reminder, you will need to have the appropriate roles assigned to your Lotus Notes ID in order to proceed with these steps. Start by completing the instructions outlined in the section titled, "Creating Policy Documents."

When creating the policy document, be sure to select "Explicit" as the policy type. Once this is complete, continue with these instructions:

Step 1. Launch the Domino Administrator client.

Step 2. Navigate to the **People & Groups** tab.

Step 3. Select the **People** view.

Step 4. Locate the **People** navigation pane along the right side of the Domino Administrator client and select the **Register** action (see Figure 6.17).

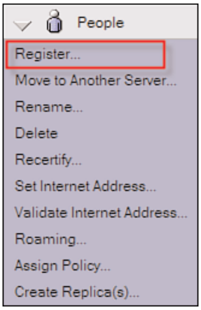
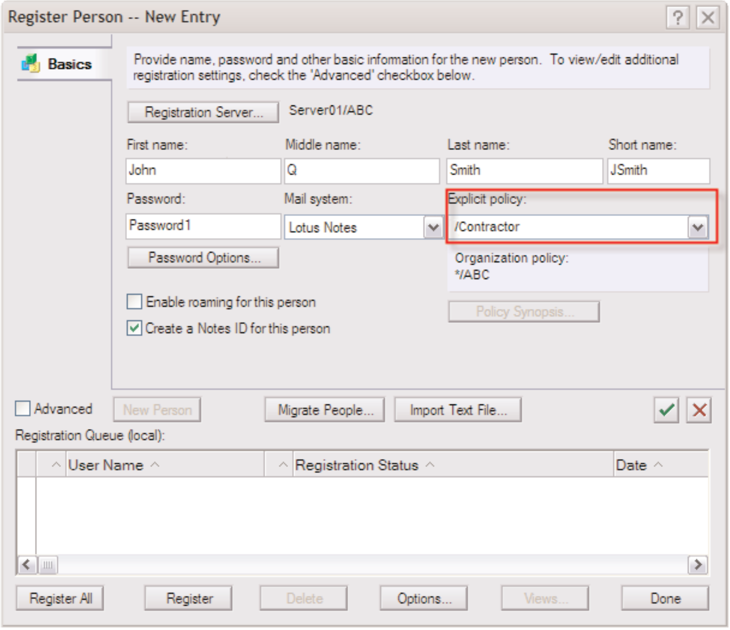


Figure 6.17 The Register action is used to register users in the Domino Directory.

Step 5. Complete the registration form as normal, paying careful attention to select the appropriate explicit policy from the list box (see Figure 6.18).

Step 6. Click the **Register** button to complete the task.



Register Person -- New Entry

Basics

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

Registration Server... Server01/ABC

First name:	Middle name:	Last name:	Short name:
John	Q	Smith	JSmith

Password: Password1

Mail system: Lotus Notes

Explicit policy: /Contractor

Organization policy: */ABC

□ Enable roaming for this person

☑ Create a Notes ID for this person

□ Advanced

Registration Queue (local):

User Name	Registration Status	Date

Figure 6.18 To assign an explicit policy, you must first create the policy and then select it as part of the new user registration process.

Assigning an Explicit Policy to an Existing User or Group

You can apply explicit policies when the user is registered or by updating the Person document for users who already exist in the Domino Directory. Start by completing the instructions outlined in the section titled, “Creating Policy Documents.”

When creating the policy document, be sure to select “Explicit” as the policy type. Once you’ve completed this policy document, you can assign it to existing users or groups.

You can assign an explicit policy to a single user, multiple users, a group, or a collection of groups listed in the Directory. This flexibility enables you to easily apply new explicit policies to many users and groups.

In addition to assigning the explicit policy to a user base (such as a group of contractors), you can also combine it with an organizational policy. For example, your explicit policy may have settings that cause the user’s certificate to expire in three or six months whereas the organizational policy may govern general workstation client settings that should be applied to both employees and contractors. The combination of these two policies can build a much stronger and more effective policy for the company. Both types of policy must be in place, however, before you start the following steps.

Step 1. Launch the Domino Administrator client.

Step 2. Navigate to the **People & Groups** tab.

Step 3. Select the **People** view.

Step 4. Select one or more users or groups from the Directory.

Step 5. Locate the **People** navigation pane along the right side of the Domino Administrator client and select the **Assign Policy** action (see Figure 6.19). The "Assign Policy Options" dialog box appears.

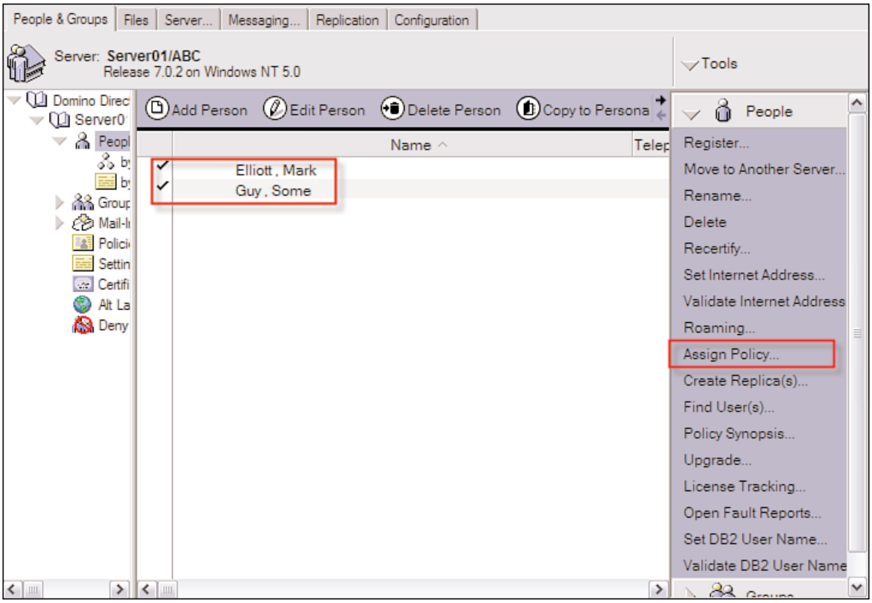
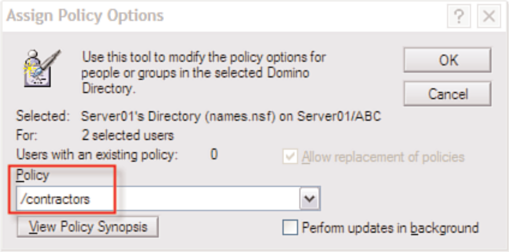


Figure 6.19 You use the Assign Policy function to designate explicit policies to users in the Domino Directory. This action updates their Person document.

Step 6. Select the desired explicit policy from the "Assign Policy Options" dialog, as shown in Figure 6.20.

Step 7. (Optional) If you have an existing organizational policy to govern general workstation configuration settings, you can combine it with an explicit policy to make a more effective policy. The organizational policy must already exist in order to continue with this step. Click the **View Policy Synopsis** button to select the organizational policy. The "Choose Organizational Policy" dialog appears (see Figure 6.21).



Assign Policy Options

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

Selected: Server01's Directory (names.nsf) on Server01/ABC

For: 2 selected users

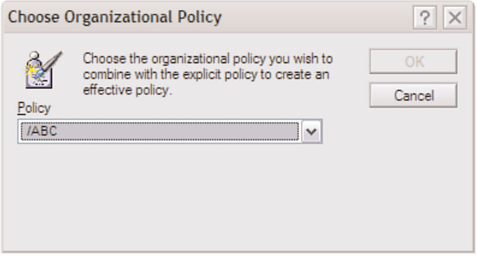
Users with an existing policy: 0

☑ Allow replacement of policies

Policy: /contractors

□ Perform updates in background

Figure 6.20 The Assign Policy Options dialog allows you to select an explicit policy as well as combine it with an organizational policy.



Choose Organizational Policy

Choose the organizational policy you wish to combine with the explicit policy to create an effective policy.

Policy: /ABC

Figure 6.21 Use the Choose Organizational Policy dialog to select the desired organizational policy.

Once you've selected the policy, click the **OK** button to return to the "Assign Policy Options" dialog.

Step 8. (Optional) You can select the "Perform Updates in Background" feature to have the updates performed in the background, which frees up your Administrator client.

Step 9. Click the OK button to complete the process. Domino updates all Person documents with the selected explicit policy (and optional Organization policy if defined).

Using Exception Policies

At the start of the chapter it was stated there were two types of policies—organizational and explicit. However, as with most things these days, there's often the need for an exception to the rule. These exceptions are managed through the use of exception policies. An **exception policy** allows you to create a set of configuration settings that completely ignore all other policies.

Warning

Administrators should use extreme caution when considering and implementing exception policies. When created, an exception policy ignores all settings associated with the primary policies that are implemented. Creating too many exception policies can cause a policy management nightmare—making it virtuously impossible to determine the policy settings and order of precedence.

At this point, you might be asking yourself, “When would I use an exception policy?” First, just to reiterate a previous point, exceptions policies should be *rarely* used. However, that said, they are used when a user needs special treatment or a custom set of policy settings.

An exception policy is actually an attribute associated with an existing organizational or explicit policy. When enabled, it allows the user to override any setting enforced by the policy. With an exception policy, you only specify the setting that will *not* be enforced. Exception policies can be created when a person performs a special job and requires the additional flexibility in policy settings.

For example, you might have a policy that enforces a mail database size quota of 100MB. Using an exception policy, you could allow an exemption to the mail file size and permit a larger size quota of 500MB, perhaps because the user transmits and receives large graphic files. In this case, the person has a very specific need and job responsibility.

While it’s important to understanding this policy type should be used sparingly, it’s equally important to understand the implications associated with this setting. In other words, you want to experiment with this field setting. The following steps outline creating an exception policy.

Step 1. Launch the Domino Administrator client.

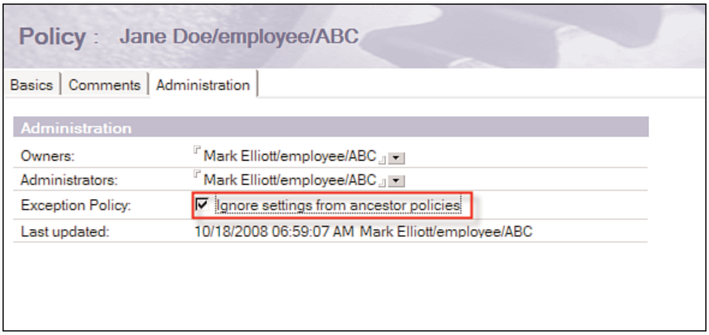
Step 2. Navigate to the **People & Groups** tab.

Step 3. Select the **Policies** view.

Step 4. Create or select the policy.

Step 5. Navigate to the **Administration** tab.

Step 6. Select the **Ignore settings from ancestor policies** option, as shown in Figure 6.22.



Policy : Jane Doe/employee/ABC

Administration

Owners:	Mark Elliott/employee/ABC
Administrators:	Mark Elliott/employee/ABC
Exception Policy:	☑ Ignore settings from ancestor policies
Last updated:	10/18/2008 06:59:07 AM Mark Elliott/employee/ABC

Figure 6.22 Use the **Ignore settings from ancestor policies** option to create an exception policy. Use caution when selecting this option. Generally speaking, you should avoid creating this type of policy.

Viewing Your Policy Settings

Once your policies are set in place, from time to time you may find the need to review your policy settings. Viewing your settings allows you to see the application of policies for a user in the Domino Directory. This is known as the effective policy.

The **effective policy** provides a synopsis of the settings and policies that are associated with a user or group. This feature allows you to view all the inherited and enforced settings based on the policies that apply to the user or group. In other words, if there are multiple organizational policies, the synopsis will show the hierarchical view of policies and settings for the selected users.

Using the Policy Synopsis function of the Domino Administrator client, you view the effect policy. The Policy Synopsis can produce two types of reports—Summary Only and Detailed. These reports are, by default, stored in the policy log database (policysyn.nsf). Each time the synopsis is run, the report is logged in the database.

The summary report provides a list of the policies assigned to the selected user. The detailed report shows all policies and settings for the user. The following steps outline how to produce a policy synopsis and to display the effective policy for a person listed in the Domino Directory.

Step 1. Launch the Domino Administrator client.

Step 2. Navigate to the **People & Groups** tab.

Step 3. Select the **People** view.

Step 4. Select one or more users or groups from the Directory.

Step 5. Locate the **People** navigation pane along the right side of the Domino Administrator client and select the **Policy Synopsis** action (see Figure 6.23). The "Policy Synopsis" dialog appears.

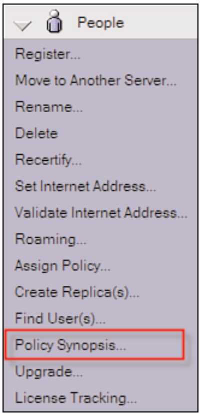
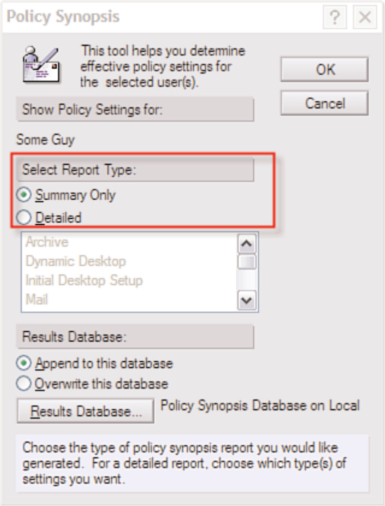


Figure 6.23 The Policy Synopsis action is located in the right pane in the People action menu.

Step 6. Select the report type—either Summary Only or Detailed (see Figure 6.24).



Policy Synopsis

This tool helps you determine effective policy settings for the selected user(s).

Show Policy Settings for:

Some Guy

Select Report Type:

● Summary Only

○ Detailed

Archive
Dynamic Desktop
Initial Desktop Setup
Mail

Results Database:

● Append to this database

○ Overwrite this database

Results Database... Policy Synopsis Database on Local

Choose the type of policy synopsis report you would like generated. For a detailed report, choose which type(s) of settings you want.

Figure 6.24 In the Policy Synopsis dialog, you can select to generate the summary or detailed effective policy report for a particular user.

With the Summary Only option, Domino will generate a hierarchical synopsis of the policies that apply to the user. The Detailed option, on the other hand, enables you to refine the report.

Using the Detailed option, you can select which settings documents should be included in the report, such as Archive, Desktop, Mail, Registration, Setup, or Activities, along with a number of additional settings. One or more of the settings document can be included in the detailed report.

Step 7. (Optional) All synopsis reports are stored in a database on the Domino server. By default, reports will be appended to the database. However, you can optionally change the setting such that new reports overwrite previous reports.

Step 8. Click **OK** to generate the effective policy for the selected user(s). Domino generates the synopsis report and automatically launches the policy report database.

The new report will appear as a document in the database. To view the synopsis, simply select and open the document.

Also note that a separate report document will be generated for each person selected from the Directory. So if you select 100 persons to be included in the synopsis report, Domino will generate 100 separate documents. Each document will contain the unique effective policy for the individual user.

Note

Generating policy synopsis reports can take time to generate from the Domino Administrator client. The response time will depend on the number of users selected from the Directory, server performance, and so on.