Redbooks Paper

Billy Boykin
Tommi Tulisalo

Active Directory Synchronization with Lotus ADSync

The Active Directory Synchronization tool, or ADSync, allows Active Directory administrators to manage (register, delete, and rename) users and groups in both Active Directory and the Domino Directory as a unified operation from the Active Directory Users and Computers Console.

In this paper, we describe some of the capabilities of the Domino 6 server and the new feature that enables you to synchronize the Domino Directory with Active Directory. This paper assumes you have a Domino server up and running and Active Directory installed. To use Lotus Active Directory Synchronization, the Domino Administration client *must* be installed on the same workstation used to manage users and computers within your Active Directory.

We describe in detail how to install and set up the ADSync tool. Detailed instructions for creating users in Domino Directory using Active Directory Users and Computers Console are given. We also show how to register users into Active Directory from Domino.

Active Directory synchronization

Domino administrators working in a Windows 2000 environment with Active Directory can now administer users and groups from a single administrative interface of their choice: the Domino Administration client or Windows 2000 Active Directory Users and Computers. This new feature of the Domino 6 server, ADSync lets you keep both the Domino Directory and Active Directory current without having to manually update both with changes. This synchronization feature allows a Domino administrator to securely and precisely delegate the responsibility for Domino user and group management to the network administrators who manage these details in Active Directory.

You can create new users and groups in Active Directory and have those changes reflected in the Domino Directory, including the creation of person or group documents, Notes IDs, passwords, and mail files for the users. In order to accomplish these tasks, the Active Directory administrator must have a properly certified Notes ID and appropriate access to make changes in the Domino Directory. The registration server must be Domino 6 or later and the Domino Administration client must be a 6 or later client. Additionally, policies must be created that contain subpolicies, either implicit or explicit, for all Domino certifiers where users will be created. Finally, you must have the appropriate rights in Active Directory to add users and groups, and synchronize passwords.

Note: Refer to the Lotus Domino Administrator 6 Help for information on policies and subpolicies.

For demonstration purposes, you may install Active Directory, Domino Server, and the Domino Administration client on a single workstation. In a production environment, the Domino server and the Active Directory will likely be installed on separate servers.

Note: If you install all components on a single workstation for demonstration purposes, you must change the LDAP port settings for either Active Directory or Domino. By default, both will be listening on port 389; therefore, one of the two will fail to function properly.

For this document we used a Domino server running on Linux and a separate Windows 2000 Server with Active Directory and the Domino Administration Client installed.

The only requirement for utilizing the ADSync tool is to work from a workstation that administers the Active Directory and that also has the Domino 6 Administration client installed.

Note: Active Directory synchronization will work regardless of the platform Domino Server is running on.

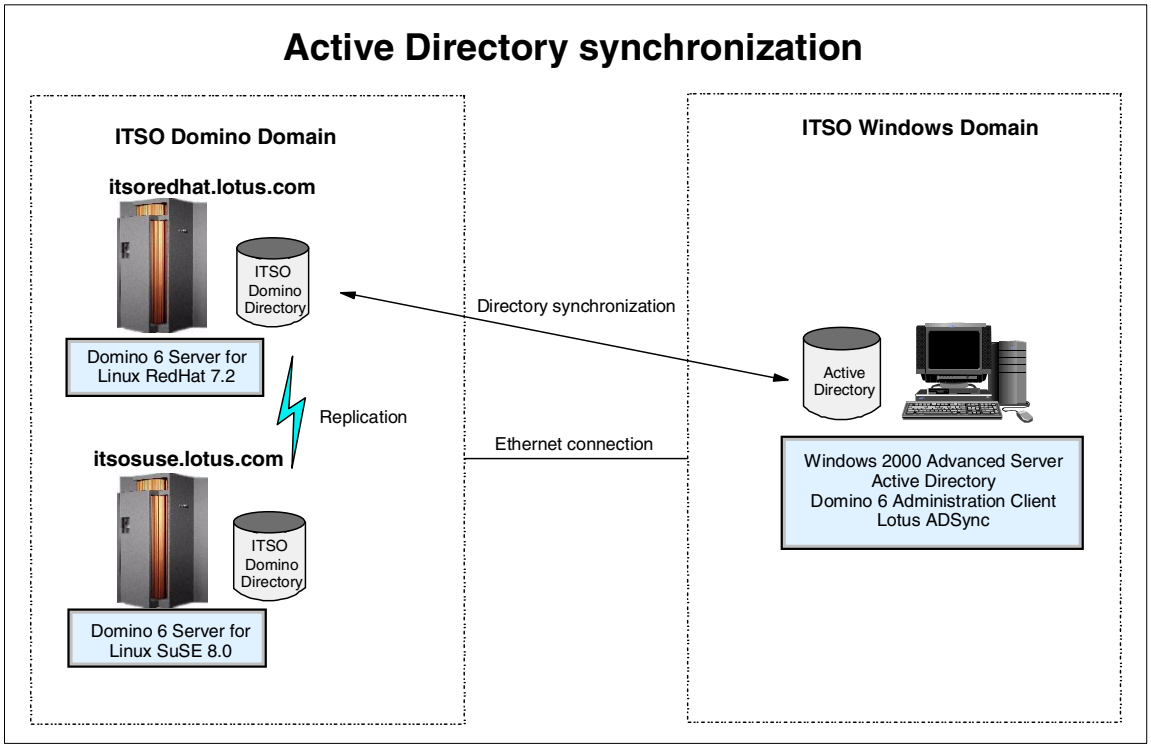

Figure 1 Active Directory synchronization: Server diagram

Active Directory synchronization in our demo environment is illustrated in Figure 1.

Installing the Lotus ADSync tool

In order to use the ADSync tool, you must turn on Domino Directory W2000 Sync Services during the installation of the Domino Administration client. This option is *only* available with the customize button during the Domino Administration client installation.

The synchronization option is not selected by default; therefore, check the appropriate box.

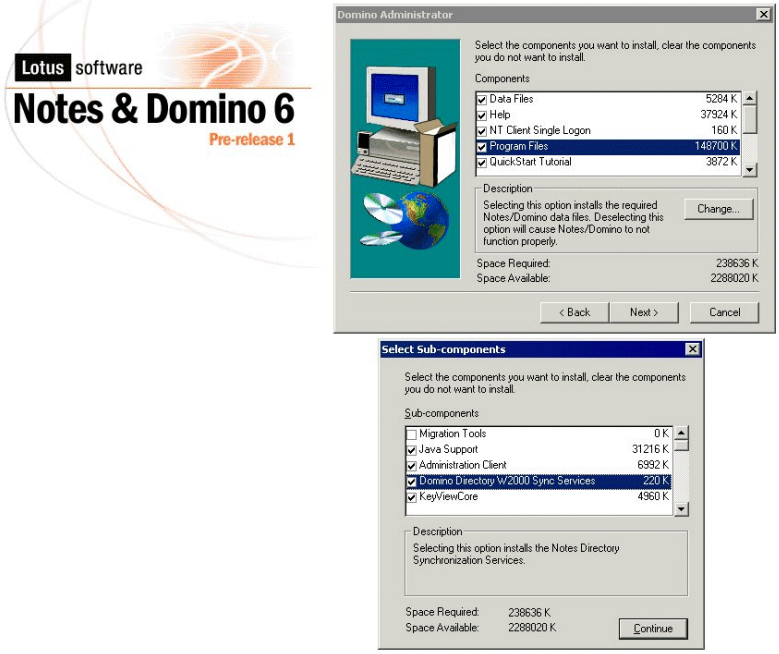

Figure 2 Domino Administration Client Installation: Customize

After installing the Domino Administration client, start a DOS command prompt window, and navigate to the directory where you installed the client. Enter the following command and press Enter:

```
$c:\Program Files\Lotus\Notes> regsvr32 nadsync.dll
```

The command adds a container entry for Lotus Domino Options to the Active Directory Users and Computers management screen and returns the confirmation shown in Figure 3.

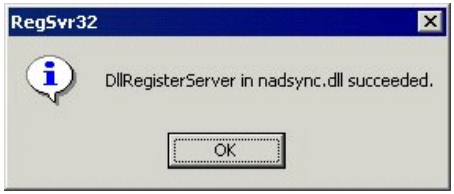

Figure 3 ADSync: RegSvr32

You are now ready to administer users and groups in Active Directory.

Creating users and groups in Active Directory

To access Active Directory Users and Computers from your Windows workstation click **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers.** You may initiate Active Directory “actions” in the right-hand results pane, or in the left-hand navigation pane. Domino users and groups are created by either of two methods:

- In the left pane, right-click an entry and choose your action from the pop-up menu.
- In the results pane, select one or more users and groups, then select “Register in Domino” from either the context menu, the toolbar, or by right clicking the entry and using the pop-up menu.

Note: Refer to your Windows 2000 documentation for more information about working with Active Directory Users and Computers.

Before you start registering users and groups from Active Directory, you must enable the Lotus Domino Option. Use the following steps to do this.

1. From the Active Directory Container shown in Figure 4, double-click the Lotus Domino entry.

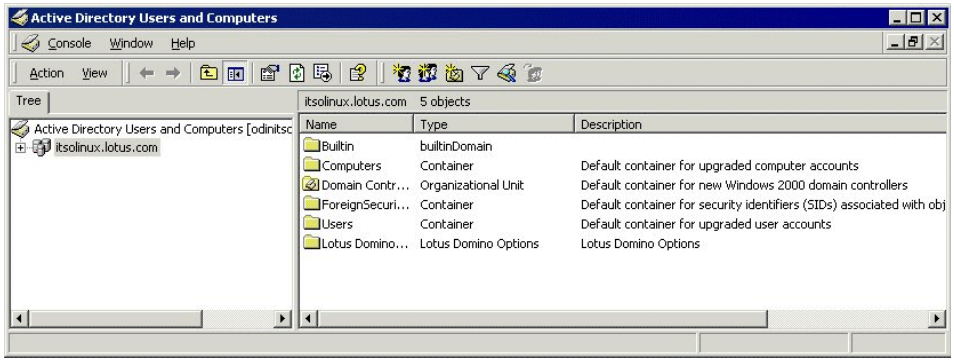

Figure 4 Active Directory Users and Computers

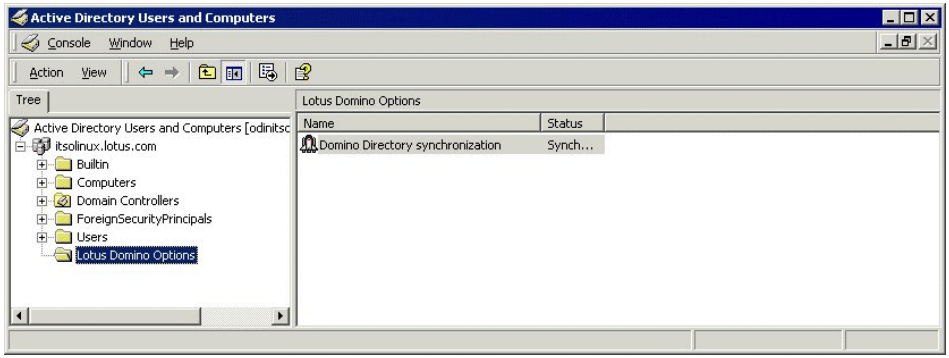

Figure 5 Active Directory Users and Groups: Lotus Domino options

2. Double-click the entry for Domino Directory synchronization in the results pane shown in Figure 5 to initialize the Lotus ADSync tool. This will require the password for the Domino administrator working from the Active Directory Users and Groups console.

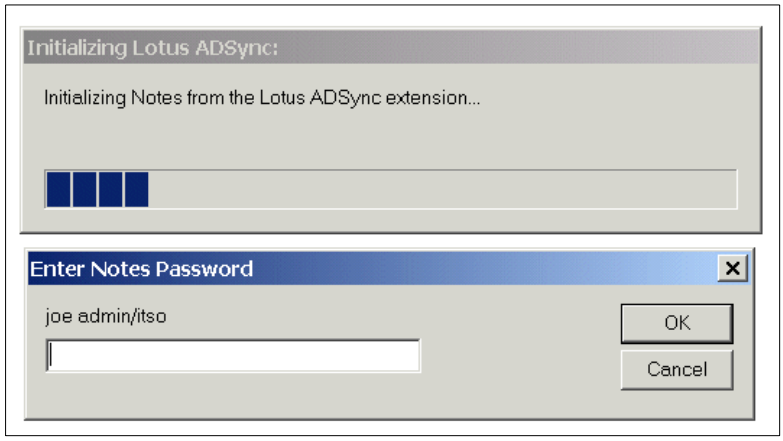

Figure 6 Initializing Lotus ADSync

3. You are then prompted to select a Domino server for all Active Directory/Notes user synchronizations (Figure 7). Select the appropriate Domino server from the drop-down selection box.

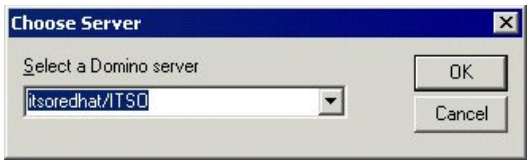

Figure 7 Lotus ADSync: Choose Domino Server

4. If the initialization was successful you should see the window shown in Figure 8.

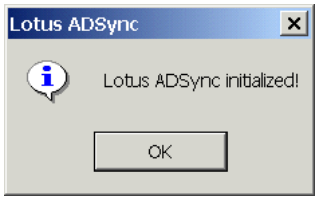

Figure 8 Lotus ADSync initialized

With ADSync initialization complete, you have the opportunity to choose several synchronization options, as shown in the next four windows.

Note: Refer to the Help files available from the Lotus ADSync Options window shown in Figure 9. This window is accessible by right-clicking the Domino Directory Synchronization entry and choosing Options.

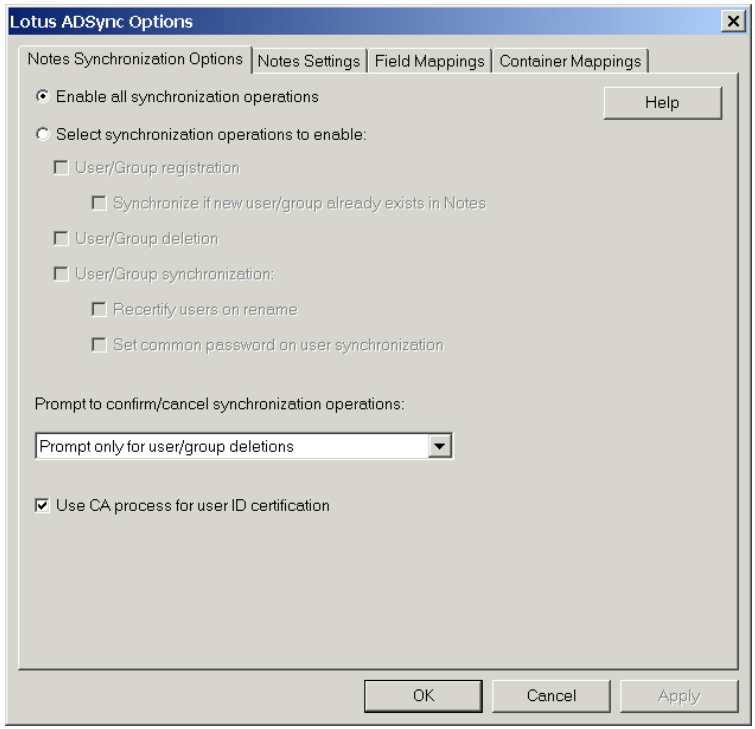

Figure 9 Lotus ADSync- Notes synchronization options

From the Notes Synchronization Options tab you can:

- Enable or disable all synchronization operations
- Customize synchronization options with “Select synchronization operations to enable.”
- Configure prompting options from the drop-down selection box
- Choose to use the CA process for user registration

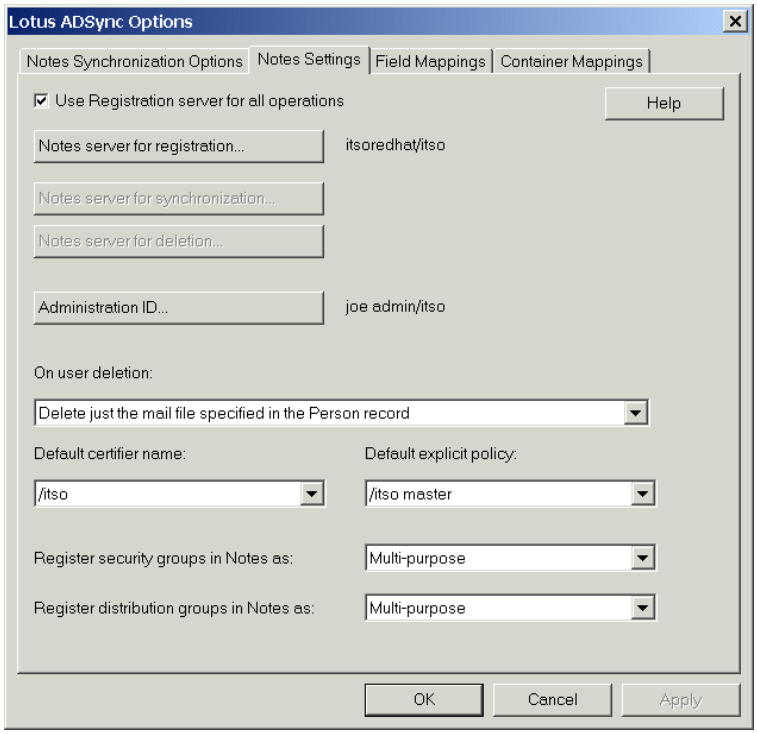

Figure 10 Lotus ADSync: Notes settings

On the Notes Settings tab you can specify:

- Registration server (which Domino server will be used for registration)
- Administration ID (which user ID will have administrative privileges)
- User deletion options (From the drop-down selection box, choose which actions should take place when a user is deleted.)
- Default certifier and policy
- Group type mappings

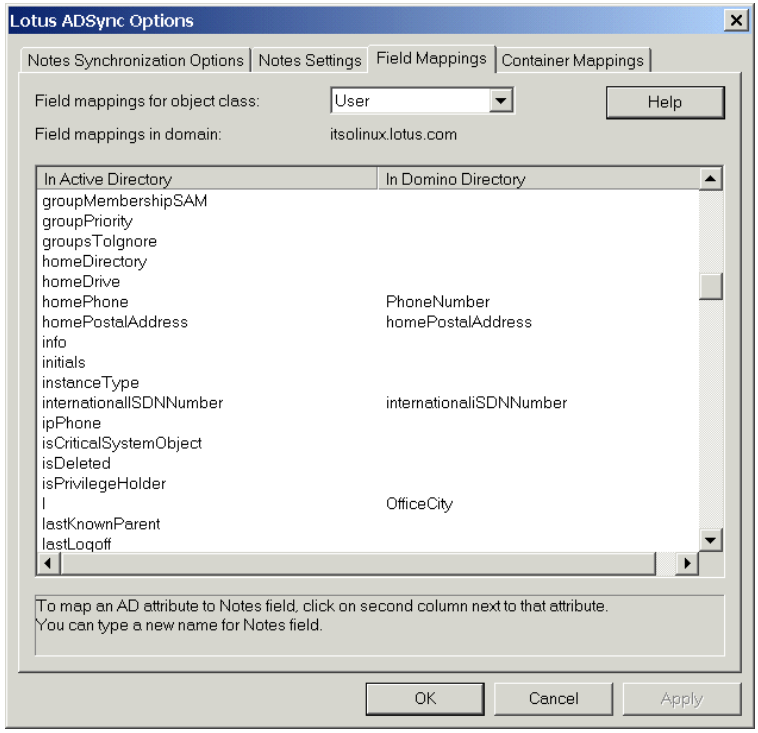

Figure 11 Lotus ADSync: Field mappings

The Field Mappings tab is where you select which Active Directory fields are to be mapped to Domino Directory fields. During ADSync tool initialization, the schemas from Active Directory and Domino are mapped based on default settings. If additional field mappings are needed, left-click in the right column under “In Domino Directory” and a drop-down selection box with Domino directory fields is presented.

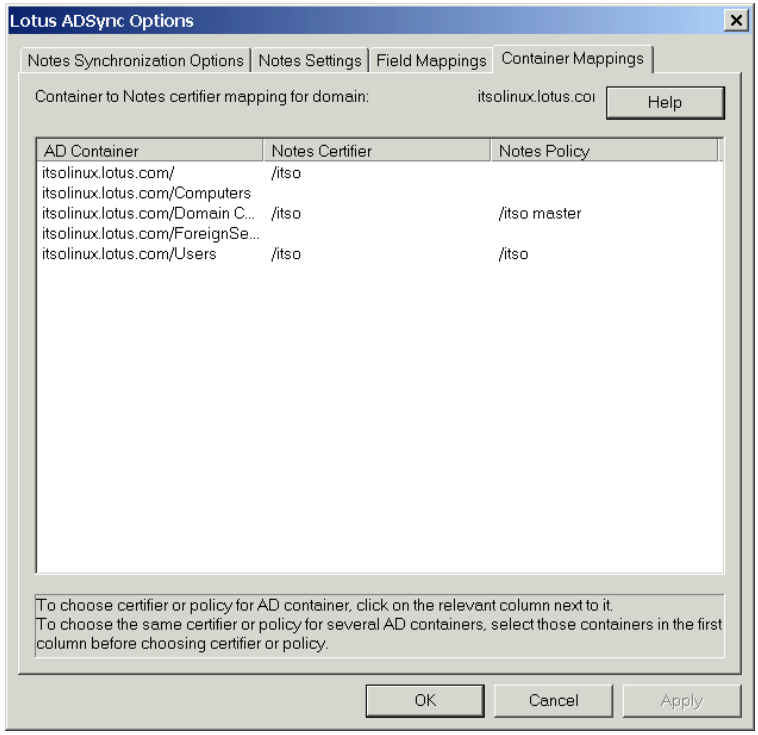

Figure 12 Lotus ADSync: Container Mappings with Notes Certifier

The Container Mappings tab is where you can map Active Directory containers to Notes Certifiers and Policies. Active Directory containers are a special class that has both a namespace and attributes. The container does not represent anything real or concrete, but rather holds one or more objects. Objects, on the other hand, are the underlying principle of everything in the Active Directory. Servers, workstations, printers, users, documents, and devices all represent objects. Each object has its own access control list (ACL) and attributes.

By design, the synchronization tool allows you to preserve the hierarchies in Active Directory and Domino using mapping. You can select a specific container to map to a certifier and/or a policy. You may restrict access to a directory structure (container, object, etc.) with group policies in Active Directory just as you can use the extended access control list in Domino to issue restrictions. An extended ACL is an optional directory access control feature available for the Domino Directory, an Extended Directory Catalog, and the Administration Requests database.

Note: Refer to the Domino Administrator 6 Help document for additional information on setting up and managing extended access control lists.

The main point here is that a user can have certain rights in either directory and not the other. ADSync does not ensure that Active Directory group policies and Domino extended access control lists are synchronized. Therefore, the administrator is responsible for ensuring no security settings are bypassed in either directory.

In the lab, we selected the container root, the domain controllers, and the Users container. Beside the container you wish to associate with a certifier, double-click in the Notes Certifier column to see your selection choices. Select the appropriate certifier and click OK to continue.

Registering users in Domino from Active Directory

Now that your certifiers have been associated to your Active Directory containers, you can register users and groups. You have the ability to register existing Active Directory users and groups in Domino.

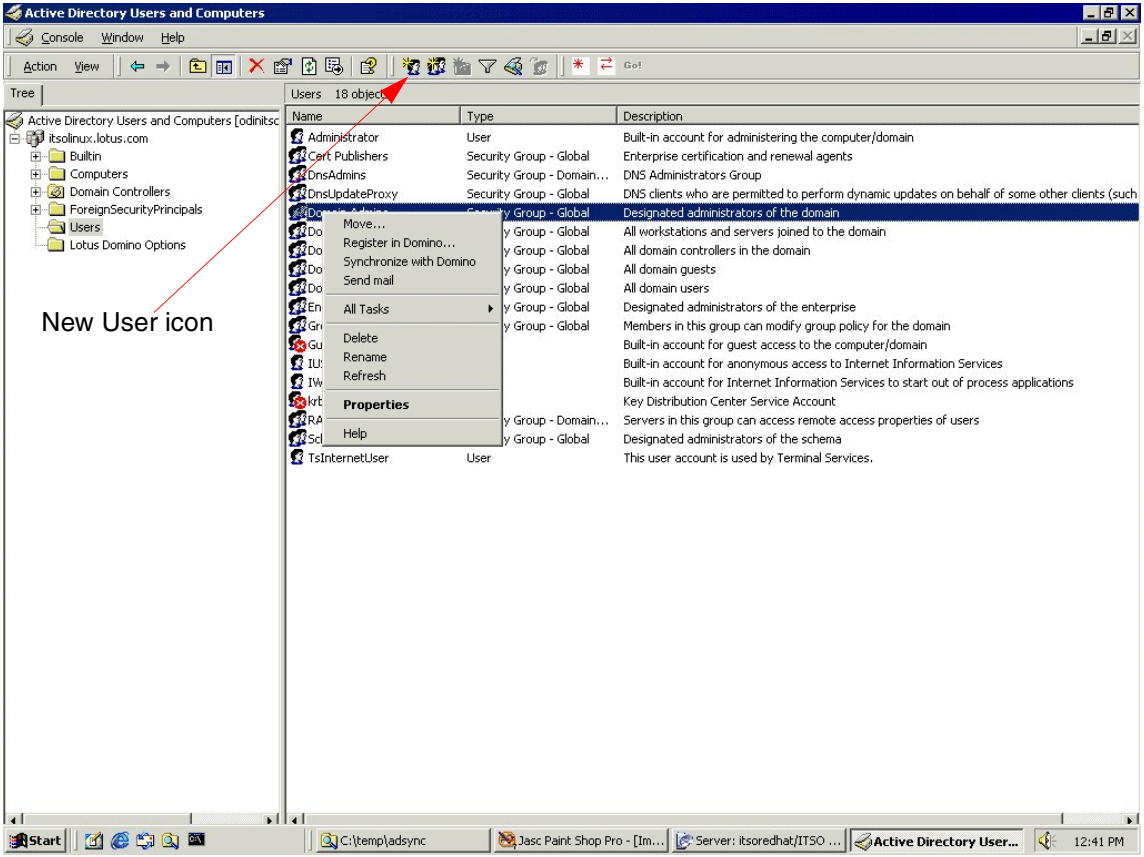

Figure 13 Active Directory Users and Groups: Register in Domino

To register users, select the appropriate container in the left-hand pane, then choose which user or group to register in the right-hand pane. Right-click the selected entry. A pop-up window is presented with Register in Domino as one of the options. This is shown in Figure 13.

You may also create new users and groups in Active Directory and choose to register them in Domino at the same time. To illustrate this, we created a new user account in Active Directory by clicking the New User icon in the Active Directory toolbar. You can also use the Action drop-down menu for this option.

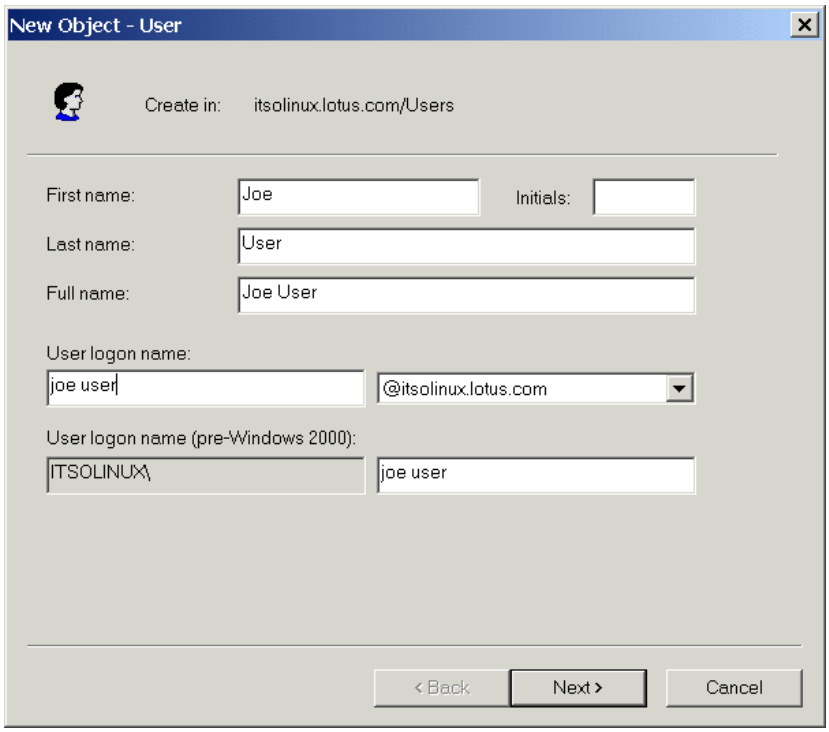

Figure 14 Active Directory New Object: User information

The first window for New Object - User will be returned, as shown in Figure 14. After entering the data for the appropriate fields, click Next to continue.

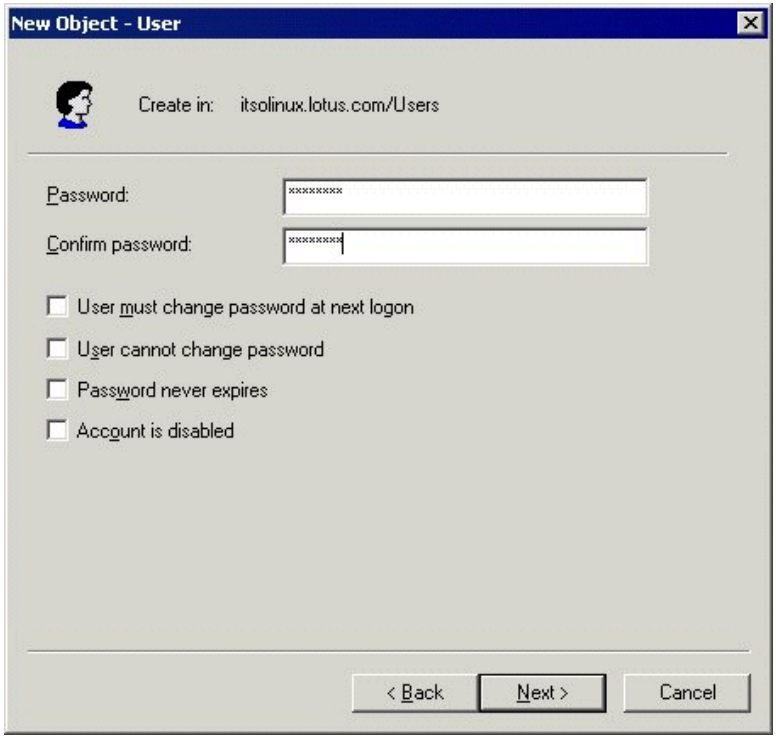

Figure 15 Active Directory New Object: User password

Enter the information for the password fields and click Next to continue. Your choices for password expiration and modification, as well as disabled accounts, are based on your company's security policies.

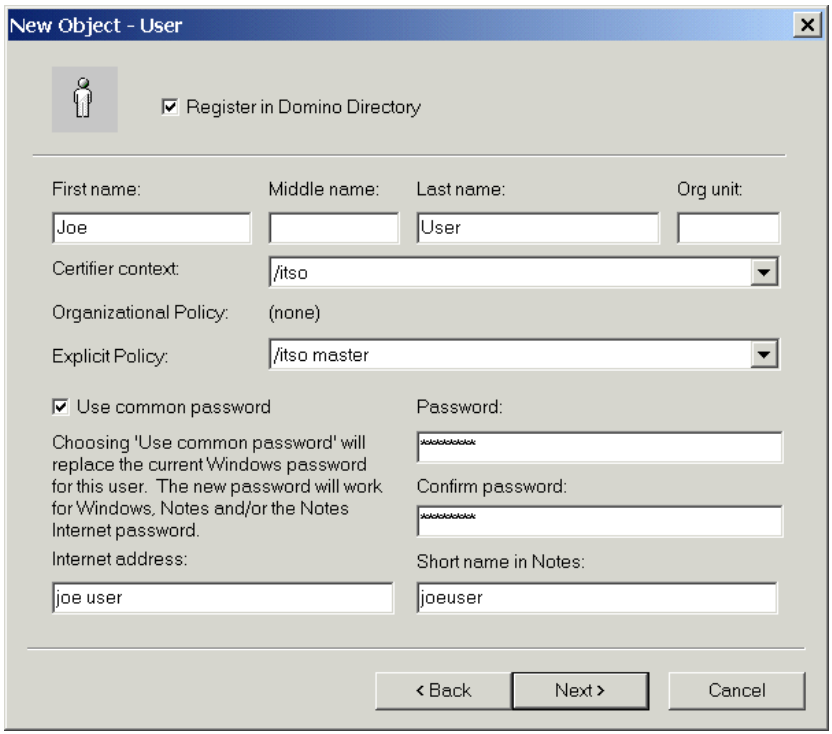

Figure 16 Active Directory New Object - Domino information

In the window shown in Figure 16 you will notice an option to register this user or group in the Domino Directory. This window also provides fields for choosing the certifier context, an explicit policy, password fields for Domino, Notes short name, internet address and the ability to enable the use of common passwords. Once you have supplied the necessary information, click Next to continue.

The new user creation process then presents you with a summary of the user object you are about to create. Click Finish and the system will generate the Active Directory object, the new person document in the Domino Directory, a Lotus Notes ID file, and user mail file.

That's it! You have successfully created a new user from within Active Directory and in doing so, you generated new objects for that person in both Domino and Windows 2000.

Registering users to Active Directory from Domino

In addition to registering users and groups from the Active Directory Users and Groups console for both the Windows 2000 and the Domino environments, you can register them from the Domino Administrator client.

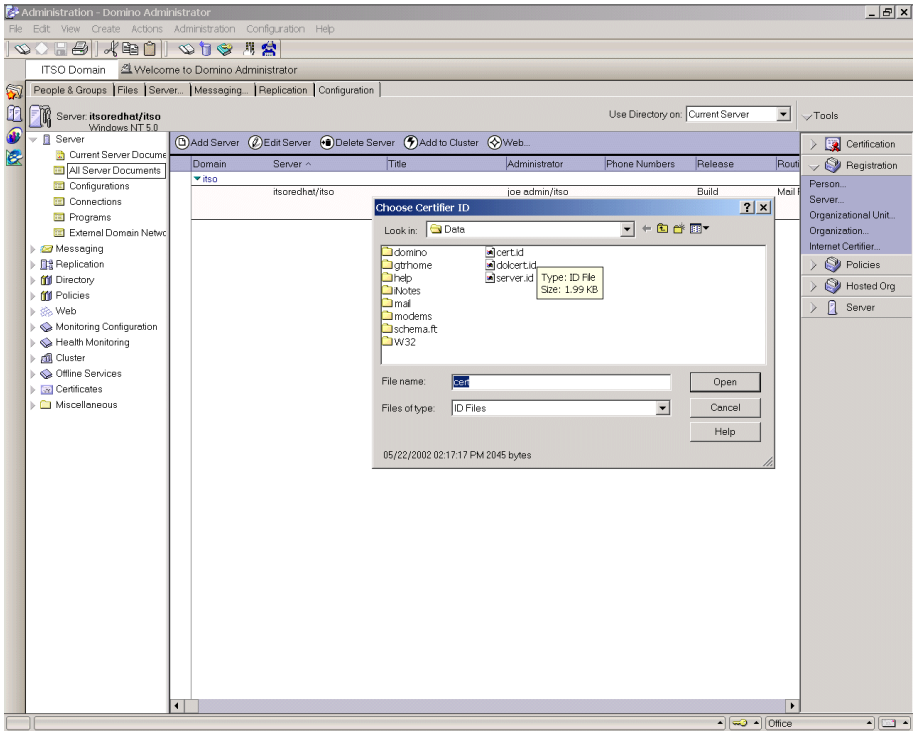

Figure 17 Domino Administration client: Choose certifier

Using the Domino Administration client, select the server to be used for registration and select the Configuration tab. On the right side of the screen, select **Tools -> Registration -> Person**. The administration client then prompts you for the Notes Certifier ID file. Select the appropriate certifier file to be used, supply the certifier password and click OK.

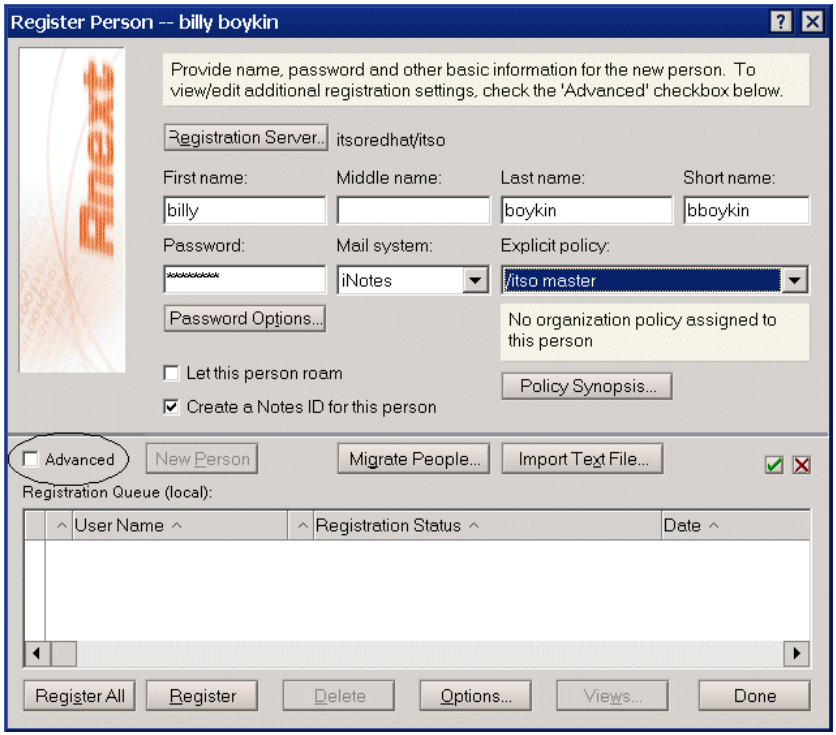

Figure 18 Domino Administration client: Register Person screen

The Domino Administration client then presents you with a Register Person window. Complete the registration fields in this window, then click the check box for Advanced options.

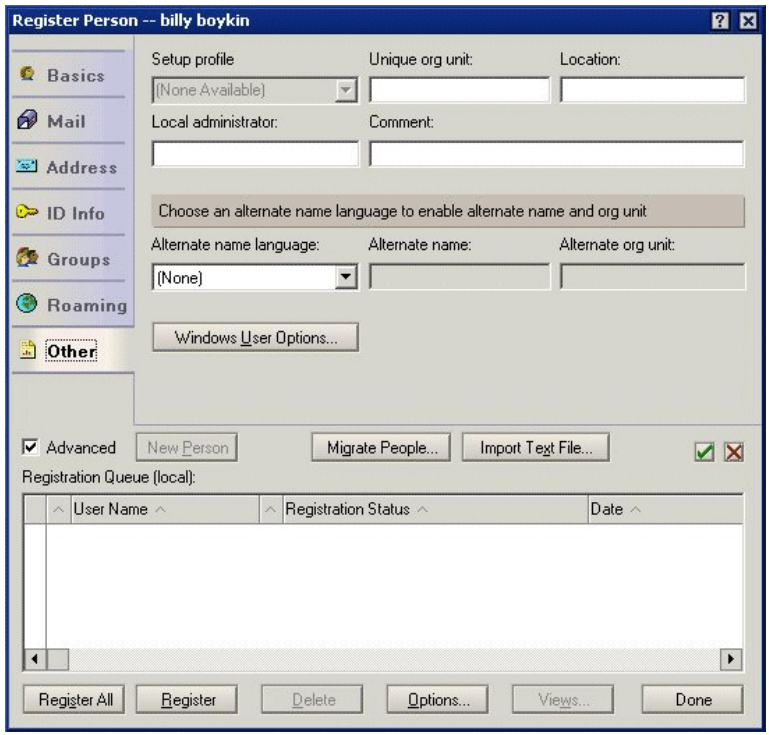

Figure 19 Domino Administration Client - Register Person (Advanced)

Complete the information appropriate for your organization in the Mail, Address, ID Info, Groups, and Roaming sections. Click the tab for the Other section; click the Windows User Options button to add this person to Windows 2000.

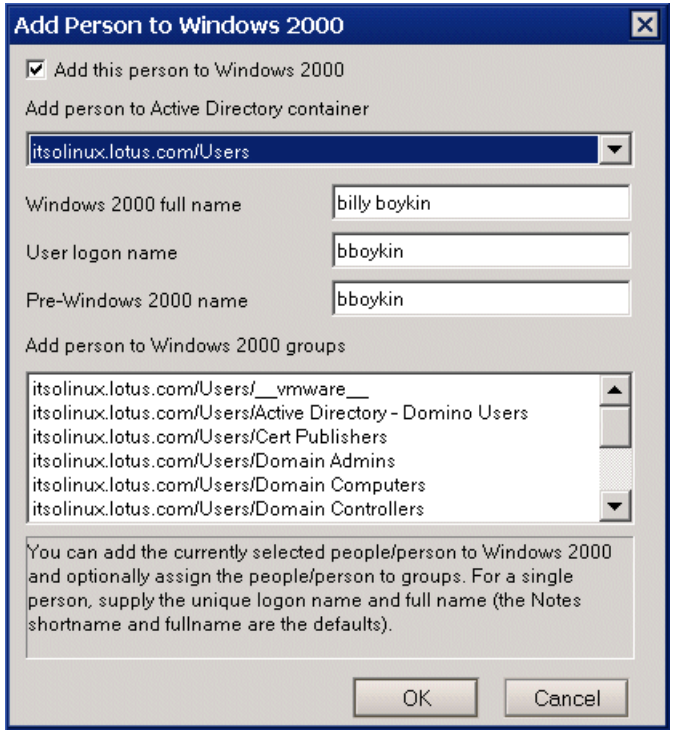

Figure 20 Domino: Add Person to Windows 2000

In this window, select the Active Directory container and Windows 2000 groups to add this person to, then click OK when finished. This particular account was placed in the Users container. We could have placed the user in any container appropriate for that account's security rights.

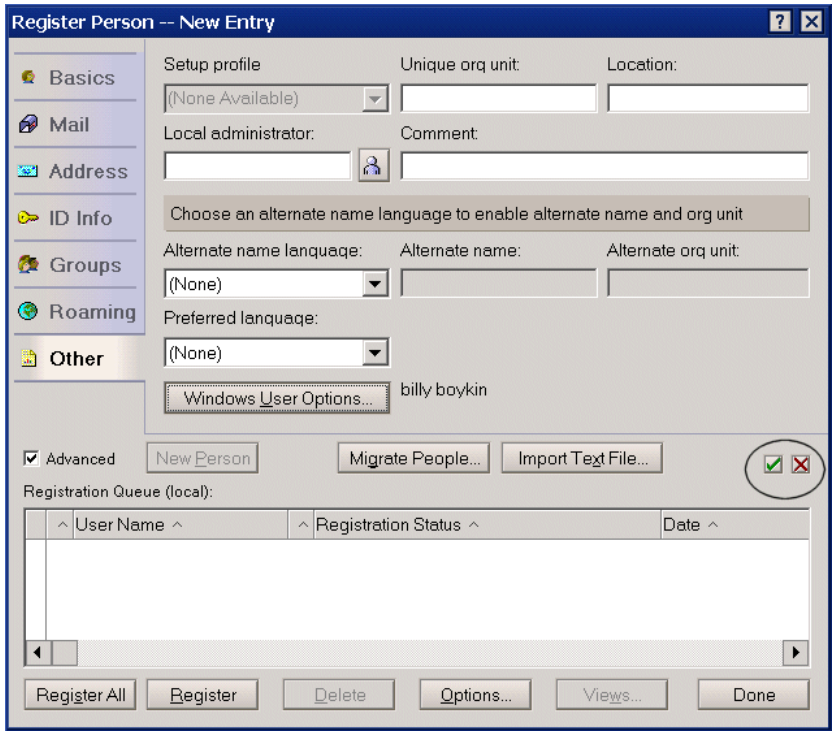

Figure 21 Domino Administration client: Confirm person registration

Click the check mark box in the Register Person window to confirm you have finished entering all necessary data for this person. This box is located on the right-hand side of the Register Person window and is circled in Figure 21.

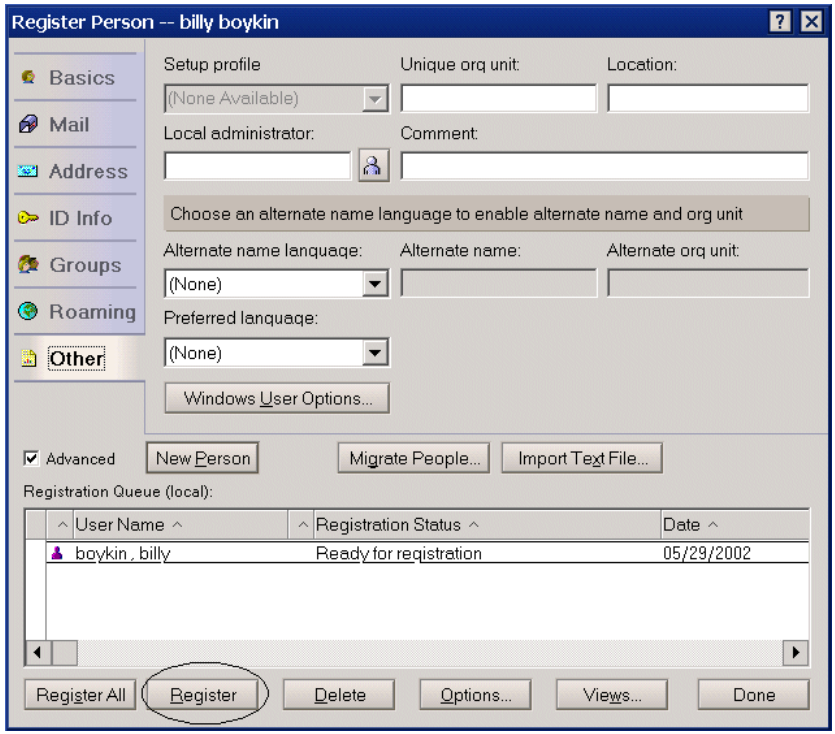

Figure 22 Domino Administration client: Register person

The entry will then be added to the Registration Queue window at the bottom of the screen. Click Register to initiate the registration process.

Once the registration process completes, this person will exist in both the Domino Directory and Active Directory.

Notices

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

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

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

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

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

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

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

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

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

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

This document created or updated on June 26, 2002.

Send us your comments in one of the following ways:

- Use the online **Contact us** review redbook form found at:
  ibm.com/redbooks
- Send your comments in an Internet note to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. THQ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 02142-1245 U.S.A.

Trademarks

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

Redbooks(logo)™  IBM®

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

Lotus®	Lotus Notes®	Domino™
Word Pro®	Notes®	

The following terms are trademarks of other companies:

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

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

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

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

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

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

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