Recipe: Managing users in Domino 4.5 and Windows NT

by Chip Carter and Barbara Burch

[Editor's note: This article resides in "Notes Today", the technical Webzine located on the http://www.notes.net Web site produced by Iris Associates, the developers of Domino/Notes.]

Overview

The Domino 4.5 server builds on a history of making server administration easier and more integrated with Windows NT. Beginning with Notes Release 4, you could include server statistics in the Windows NT Performance Monitor and run the server as a Windows NT service. With Release 4.5, you gain ways to better manage users, applications, events, and more.

One such Domino Release 4.5 feature is called User Synchronization, which enables you to synchronize your Domino/Notes users with your Windows NT user accounts, and vice versa. This means that you can keep both the Domino Public Address Book and Windows NT User Manager current, without having to update them both when making changes. For example, when you need to add or delete users (such as, when a person joins or leaves the company), you can make the change from a single location -- either from Domino or Windows NT.

This article concentrates on helping you, the Domino administrator, get started using the User Synchronization feature. We'll first discuss in detail what the User Synchronization feature is and what options are available. Then, we'll walk through three possible scenarios for how you can actually use the feature in your organization: (1) if you have an existing Windows NT network and are just beginning to deploy Domino and Notes; (2) if you have existing "unsynchronized" users on both Windows NT and Domino/Notes; or (3) if you have already synchronized users and you want to move forward with additions and deletions. The article ends with some answers to common questions.

Note that you can use all of the Lotus Domino/Notes 4.5 features on both Windows NT 3.51 and 4.0, and on both the Intel and Digital Alpha platforms. For more information on any of the features, please see the *Lotus Notes 4.5 Administrator's Guide*.

Synchronizing Domino/Notes user information and Windows NT user accounts

The User Synchronization feature in Domino 4.5 makes managing users easier because you can update users from one location. Entries in the Domino Public Address Book are linked to entries in the Windows NT User Manager for Domains. In other words, Person documents are linked to the Windows NT user accounts. Changes made in one place automatically appear in the other. (The way this is done is by synchronizing the Network account name in the user's Person document to the user account name in Windows NT.)

From the Domino end, when you register or delete a person in the Public Address Book, you can automatically update the Windows NT User Manager. This works for both individual users as well as when you register a group of users from a text file. To register new Domino users, you must be an administrator with the UserCreator role or Editor access in the Public Address Book on the registration server. You can only create Windows NT user accounts while registering Domino users; that is, you cannot create Windows NT users when manually adding a person to the Public Address Book.

Likewise, by using the Notes menu added to the Windows NT User Manager during installation, you can create or delete Windows NT user accounts and automatically reflect the changes in the Public Address Book. You can also add existing Windows NT users as new Domino/Notes users in the Public Address Book. To add user accounts to the User Manager, you must be a member of the local Administrator Group or local Account Operator Group in Windows NT.

Note that to use the User Synchronization features, you must first do a customized installation of Domino and make sure to select the User Synchronization option.

What happens when you use Domino to create user accounts in Windows NT
When you register a new Domino user and choose to create a Windows NT user account, Domino, by default, uses the shortname from the user's Person document as the Windows NT user account name (for example, JSmith). If you want, you can specify a different name for the Windows NT user account. Domino then copies this name to the Network account name field in the Person document. Therefore, the Network account name field will match the Windows NT user account name, and this is how the accounts will stay synchronized in the future.

Domino creates the Windows NT user account with the following information:

- NT User Name (created by default from the user's shortname in the Person document, or it can be a name you specify)
- Full name (created by combining the user's first name, if supplied, and last name)
- Password (created by using the Notes password. If the Notes password exceeds 14 characters, the Windows NT password will consist of the first 14 characters of the Notes password.)
- NT Group Name (created by using a name you specify, or the default Windows NT user group, Users)

If while creating user accounts, Domino encounters a Windows NT error (for example, you are not a Windows NT Administrator or Account Operator), it returns an appropriate error message to the screen. If an error message is encountered that prevents creation of an account in the User Manager, the user is still registered in Domino; Windows NT errors have no effect on Domino registration.

What happens when you use Windows NT to register (create) Domino/Notes users
Unless you modify the Registration Setup or Mail/ID Registration options in the current User Manager session, new Domino/Notes users are registered with the following default information.

- Notes mail files are created immediately using the users' shortnames (for example, JSmith.nsf for John Smith)
- User ID files are saved to the Public Address Book (not to a file) using the users' shortnames. The IDs are created with a North American license and two-year certificate expiration dates. No setup profiles or unique user organizations are specified
- Common passwords (shared by the Domino and Windows NT accounts) are generated and stored in the local database called "New User Passwords"
- The local Domino server is used as the registration server (the server on which Public Address Book entries are created) and the mail server (the server containing the users' mail files).
- The local administrator's ID and certifier IDs are used

If during registration a Domino or Windows NT error is encountered, (for example, a Person record already exists for the user), the User Manager returns an appropriate error message. A failed registration for a single user doesn't prevent pending users from being registered. If a Domino error prevents a user from being registered in Domino, the user account is still added to User Manager (if you chose to create them); Domino errors have no effect on User Manager.

Scenarios for using User Synchronization in your organization

Now, we will discuss the following scenarios for using User Synchronization in your organization:

- You have an existing Windows NT network and are deploying Domino and Notes for the first time in your organization. Therefore, you want to add a whole batch of NT users to Domino at one time.
- You already have Domino/Notes deployed and you have existing users on both Windows NT and Domino. Therefore, you want to get the user accounts synchronized so that if you need to delete a user, for example, when they leave the company, you can just delete the user with a single action.

- You already have Domino/Notes deployed and synchronized with Windows NT. Now, you simply want to add, delete, and rename users as necessary.

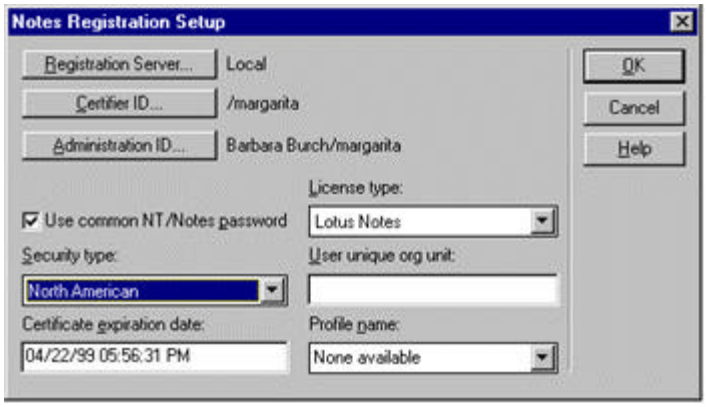
Scenario 1: Deploying Domino and Notes for the First Time in Your Organization
This scenario addresses when you have an existing Windows NT network and are deploying Domino and Notes for the first time in your organization. Before you even get to the synchronization stage, you should have completed the planning for your Domino and Notes deployment. You should have already set up the Public Address Book and servers -- now you're ready to add the users. You should know where the users' mail files will be located (their home server) and to which server's Public Address Book you want to add the users (their registration server). Depending on the loads already on or planned for the servers, the mail server and registration server can be different.

You can add existing Windows NT users to Domino either individually or all at one time. In addition, you can use the default registration information or customize it. For this scenario, we recommend that you save time by customizing the registration and mail information (to make sure users are set up specifically as you want them) and register groups of users at one time (without separate prompts for individual names and passwords). Random passwords will be generated for the users and stored in the database titled "New User Passwords" (NTSYNC45.NSF). After the users are registered in Domino, you can open this database and distribute the passwords to users so they can install their Notes workstations. (After installation, the users can then replace the random passwords with passwords of their own.)

Adding existing Windows NT users to Domino --The following steps will help you customize registration information and then register a group of Domino users with the Windows NT User Manager. The computer upon which you do this must also be a Domino server, although it's not necessary for the Domino server to be running.
Note: To use the User Synchronization features, you must first do a customized installation of Domino and make sure to select the User Synchronization option.

1. From the User Manager for Domains, choose Notes - Registration Setup. Doing this automatically selects the option Enable Notes User Registration, which is required for you to register users in Domino.
2. If necessary, enter your Notes password and the path and password for the appropriate certifier ID.
3. Complete the Registration Setup dialog box. The information you enter applies to all users registered during this User Manager session. Click OK when finished.
    - To specify a server other than the local server as the server on which to create Person documents, click Registration Server and select another server. Users are assigned the same domain as that of the selected server. You must have a properly certified Notes ID and sufficient access to the specified server to register users in Domino.
    - Check that the correct certifier ID and administration ID are displayed. If not, select the correct one.
    - Do not select Use common NT/Notes password. Because you will be generating random passwords for users (by selecting to register users without additional prompts), you probably do not want to overwrite the users' existing Windows NT passwords with random ones. This wouldn't make much sense since users will most likely only use the random password when first installing Notes.
    - Select the correct encryption (North American or International), Notes certificate expiration date (in mm-dd-yy format), and license purchased.

- If necessary, specify a unique organizational unit and/or setup profile for the users.



4. Choose Notes - Mail/ID Registration Options, and complete the dialog box. Again, the information you enter applies to all users registered during this User Manager session. Click OK when finished.
   - To create the users' mail files on a server other than the local server, click Mail Server and select another server.
   - To select a mail type other than Lotus Notes, click Mail Type and select a different mail type. If you select another mail type, the remaining fields in this dialog box disappear.
   - If necessary, specify a directory other than Mail for the Notes mail files.
   - To create a mail file during Domino registration, select Create mail file now. To create a mail file later using the Administration Process, select Create mail file later.
   - To indicate how you want to store the user ID file, select In Address Book or In file or both. If you store the ID in a file, click Set ID path, select a location for the ID file, then click OK.

5. From the Username window, select the user accounts you want to register and choose Notes - Add Selected NT Users to Notes.
6. In the "Choose Registration Options for Selected NT Users" dialog box, select to register selected users at once without additional prompts. (This saves time because you don't need to add name and password information for each individual user.) Notes passwords will be generated and saved in the database "New User Passwords" (NTSYNC.NSF).
7. Click Begin Registration when a prompt appears asking whether you want to register the selected user accounts in Notes. If you click Cancel, the pending registration information remains stored until you exit User Manager (at which time you can either register the users or lose the pending information).

8. (Optional) After registration has begun, click Stop Registration at any time to stop registration after the current user registration is complete. Subsequent user registrations will remain pending until you refresh or exit the User Manager.

After registration is complete, you can open the "New User Passwords" database in Domino and click on any user name to view the password that was generated. Distribute these passwords to users so they can use them when they install the Notes workstation software.

Scenario 2: Synchronizing Existing Users on Windows NT and Domino
This scenario applies to when you have both Windows NT user accounts and Domino users already set up in your organization, and you want to synchronize the accounts to make changes easier later. The method for doing this is actually called "renaming" in the User Manager.

Using Windows NT to synchronize your Domino and Windows NT user information -- The following steps synchronize the user information by changing the username for the Windows NT account and then placing the same name in the corresponding Network account name field in the users' Person document. The computer upon which you do this must also be a Domino server, although it's not necessary for the Domino server to be running.
Note: To use the User Synchronization features, you must first do a customized installation of Domino and make sure to select the User Synchronization option.

1. From the User Manager, choose Notes - Deletion/Rename Options.
2. If necessary, enter your Notes password.
3. Select Enable Notes User Renaming in the lower left corner of the dialog box.
4. Select the name of the server whose Public Address Book will be updated. Click OK.
5. From the Username window, select the user account you want to rename and choose User - Rename. (Windows NT requires that you rename users one at a time.)
6. Specify the new name. The Network account name field in the corresponding Person document for the user will automatically reflect the new name.

Note that this procedure does not change the full Domino user name. You can't rename a user if the user's name is not unique within Domino.

Scenario 3: Adding and Deleting Users as They Join or Leave Your Organization
This scenario involves the ongoing task of using User Synchronization to add and delete users.

When you want to add a user, you have the following options:

- Use the Windows NT User Manager to create a new Windows NT account and simultaneously register the user in Domino. You can register the user by using default information, or by specifying registration and mail options.
- Use Domino to register the person and simultaneously create the Windows NT account. You can also do this when registering a group of users from a text file. The default account name is the same as the Domino shortname. See the *Administrator's Guide* for information.

To delete users, the Notes full name or short name must match the Windows NT full name or user name, respectively. The user name must be unique within Windows NT.

When you want to delete a user, you have the following options:

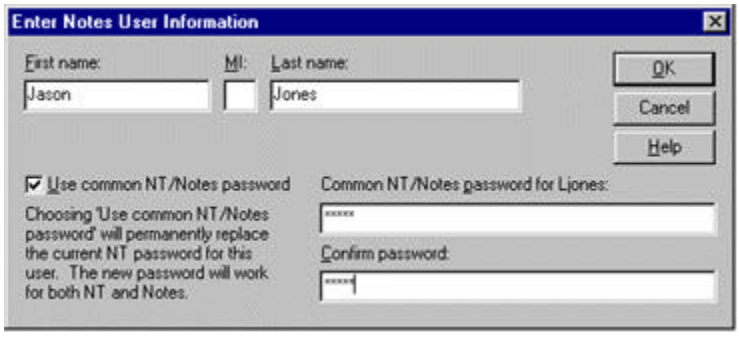
- Use the Windows NT User Manager to simultaneously delete a Windows NT account and Domino user. To delete a user's Windows NT account, the Delete Person request must be made from a Windows NT machine and the initiator must be a Windows NT domain administrator with rights to delete user accounts.

- Use the Domino Administration Process to delete a Domino user and simultaneously delete the Windows NT account. If you delete a person manually within Domino (rather than choosing the Delete Person action), you will also have to delete the user manually in Windows NT. See the *Administrator's Guide* for information.

Adding new users to both Windows NT and Domino at the same time --The following steps walk through how to use the User Manager to add users to both Window NT and Domino. The computer upon which you do this must also be a Domino server, although it's not necessary for the Domino server to be running. If you do not specify Registration or Mail options, the Domino server functions as the registration server (the server on which the Public Address Book entry is created) and the mail server (the server storing the user's mail file). To add a large group of users at one time to both Windows NT and Domino, we recommend using Domino to register the users from a text file. See the *Administrator's Guide* for information.

Note: To use the User Synchronization features, you must first do a customized installation of Domino and make sure to select the User Synchronization option.

1. From the Windows NT User Manager, choose Notes - Enable Notes User Registration.
2. If necessary, specify other Registration and/or Mail setup options. (See Scenario 1 for a description of the options in the Registration Setup and Mail/ID registration dialog boxes.)
3. Choose User - New User from the User Manager menu bar and complete the dialog box. Click OK when finished. (Windows NT requires that you add new users one at a time.)
4. If necessary, enter the password for your Notes ID. Then, enter the path and password for the certifier ID.
5. Complete an Enter Notes User Information dialog box for each new user. Click OK when finished.
    - Accept the default first name, middle initial, and last name to be used in Domino or change the name. The default name is derived from a user's full name in Windows NT.
    - Keep Use Common NT/Notes password selected to provide the user with the same password for both Windows NT and Notes. You can also deselect this option.
    - Enter a password, either a common password or a Notes password, depending on your previous selection. You can also leave this option blank. If you use a common password, it writes over the user's current Windows NT password if one exists; to preserve a current Windows NT password, enter it exactly as it exists.



6. Click Begin Registration when a prompt appears asking whether you want to register the new user account in Notes. If you click Cancel, the User Manager adds the new account to Windows NT and stores the pending registration information until you exit the User Manager (at which time you can either register the users or lose the pending information).

7. (Optional) After registration has begun, click Stop Registration at any time to stop registration after the current user registration is complete. Subsequent user registrations remain pending.

Deleting users from both Windows NT and Domino at the same time
The following steps walk through how to use the User Manager to delete users from both Window NT and Domino. The computer upon which you do this must also be a Domino server, although it's not necessary for the Domino server to be running. The user's full name or shortname in Domino must match the Windows NT full name or user name, respectively.

1. From the User Manager, choose Notes - Deletion/Rename Options.
2. Select Enable Notes User Deletions.
3. Select the name of the server whose Public Address Book will be updated.
4. Select one of the "delete mail file" options. Click OK.
5. From the Username window, select the user accounts you want to delete and choose User - Delete.
6. Click OK when the User Manager warns that a user account cannot be restored once it's been deleted.
7. Click Yes to delete users individually, or click Yes to All to delete several users at once. The corresponding Person document for the user will be automatically deleted from the specified server's Public Address Book. (The Administration Process is actually used by the Domino server to remove all references to the user name in Domino.)

Common Questions

Does using the User Manager with Domino compromise Domino security?
Administrators must have a properly certified Notes ID and appropriate access to make any changes to a Domino server's Public Address Book, even when using Windows NT. When using the User Manager, the same security mechanisms take place as in Domino. Also, an administrator must be a member of the local Administrator Group or local Account Operator Group in Windows NT to add user accounts to the User Manager.

Why doesn't Domino synchronize changes in the Person document back to Windows NT?
The only two changes in the Person document that would have been worth handling in Domino 4.5 would be a change to the Network Account Name and/or a change to the full name (both in the Person document). Of these two changes, only a change to the Network Account Name would really affect user synchronization and Windows NT. Since that Network account name is used only in NT and only changed in NT, it doesn't affect Domino functionality. When changed in NT, the corresponding Person document in Domino gets properly synchronized (that is, the Network Account Name in the Person document gets updated).

Windows NT account generation is quick. Domino takes more time to create a user ID file, because a public and private key for each ID file has to be computed. Do I have to wait for Domino each time I manually create a Windows NT account?
No. Domino registration (which can be time consuming) does not take place with each Windows NT user added. You can choose to wait to begin Domino registration until the end of your User Manager session. User registration-related information is saved for each Windows NT user created, and then you can begin the Domino registration whenever you want. (A Refresh in the User Manager (F5) or exiting the User Manager will trigger the prompt.)

When does the User Synchronization NOT work ?
User synchronization is not available when you open the Public Address Book and add a Person document manually. Nor is synchronization available when you select a Person document and press Delete. Instead, you must click the Delete Person button to synchronize deletions.

ABOUT THE AUTHOR

Barbara Burch has been a technical writer at Lotus since June of 1996. For Release 4.5, she worked on the Install Guides for Notes workstations and Domino servers. She's currently working on the next version of the Administrator's Guide. Before moving to Boston last year, Barbara worked as a technical writer at National Instruments in Austin, Texas.