



by Timothy Speed  
and Mary LaRoche

**Level:** All  
**Works with:** Domino 5.0  
**Updated:** 11/01/2001

Here's an ID and password recovery fish story:

Cindy HelpDesk answered the phone and heard a timid voice at the other end. "Hello Cindy, this is Bubba Smith. I lost my ID file."

"What happened to your ID file?"

"It's at the bottom of the Gulf of Mexico, with my laptop. . . . I was out fishing with my buddy, Billy JoBob, and I decided to check my e-mail. Then this huge shark swallowed the bait and started a tremendous fight. I dropped my laptop to grab the pole, and the laptop slipped into the water."

"Did you catch the shark?"

Mr. Smith sheepishly said, "Nope, it got away, but I have a new laptop now. I need a Notes ID and password, and I also had an X.509 certificate in my Notes ID file. I don't know how to get a replacement."

"Let me check. Your ID was last harvested two weeks ago. How long ago did you import the X.509 certificate into your ID file?"

"About four months ago."

"Then you should be OK. I'm sending your ID to your manager now. Here is the key to unlock your ID—5829692949294a36. Also I'm e-mailing the procedures on how to unlock the ID file to your manager; it takes just a few steps to unlock the ID and enter a new password. Without the number I've just given you, no one will be able to unlock your ID file, so guard it just as carefully as your password."

Mr. Smith sighed with relief. "Thanks, Cindy. You were a great help!"

Great story with a happy ending. User drowns laptop, user gets a new laptop, and then user gets ID back. All this without getting wet. This success story was brought to you by the ID and Password Recovery (also called ID Recovery) mechanism that is built into Lotus Notes R5. This article explains how to implement ID and Password Recovery for your organization.

## What ID Recovery does for you

The ID Recovery mechanism is basically simple. If an ID has been created with a certifier that has recovery information, the ID file contains at least one recovery password that is randomly generated and encrypted with an administrator's public key. The password is unique for each administrator and user. For example, administrator Cindy HelpDesk has a unique recovery password for user Bubba Smith, and that password is stored in Bubba's ID file.

Before ID Recovery, if a user lost the password to her ID, the administrator had to either get the ID file from an archive or create a new ID file for the user. Both options posed problems:

- If the ID was obtained from the archive, the old ID file might not contain

recent X.509 keys, encryption keys, name changes, or new keys from recertification.

- If the administrator created a new ID file for the user, even with the same user name as before, the user would not be able to read previously encrypted mail or documents.

ID and Password Recovery makes user ID management simpler and better with these new features:

- The ability to "open" an existing ID Recovery-enabled ID file and assign a new password to it.
- The ability for an administrator to unlock an ID over the phone.
- The ability to harvest IDs from R5 clients and back up the IDs in a secure, centralized database.
- The ability to enable any ID to support ID Recovery via Notes mail.
- The ability to automatically archive IDs at the time of new user registration.
- The ability to manage the recovery information in each ID based on the OU level certifier.

These powerful features allow an enterprise Domino installation to securely manage ID files while also providing better service to users.

## How to implement ID and Password Recovery

Here are the basic steps for implementing ID and Password Recovery in your organization:

1. Define your security policies and procedures for ID and password management.
2. Create a recovery database to house each set of IDs per O or OU. Technically, you can place all of the IDs into the same database. Where OUs reflect actual administration boundaries, it is better to create one recovery database per OU.
3. Create a mail-in database record for each ID recovery database.
4. Add recovery information to each O or OU certifier that will be certifying end users.
5. Export the recovery information and send it to all R5 users per O or OU; this is the harvest process.

Let's review each of these steps in more detail.

### 1. Define security policies and procedures for ID and password management

First, before creating recovery policies and procedures, you need to have a basic, organization-wide security policy. If you need help here, several books and Web sites can help you, including *The Internet Security Guidebook*, ISBN:0122374711; "An IT Security Policy: What Every Hacker Does Not Want You To Have in Place," ([THE VIEW](#), November/December 2000); and the National Institute of Standards and Technology (NIST) [Internet Security Policy](#) guidebook. These materials can help you create security policies and procedures to support your security infrastructure.

Then, in relation to ID Recovery, you need to define the following:

- The number of recovery IDs that will be placed into each OU. Currently the maximum value is 8.
- The minimum number of administrator recovery IDs (also called Recovery Authorities) required to unlock a user ID file.
- The naming standard of the administrator recovery ID files that will be used to unlock the ID files.

### Identify the number of Recovery Authority IDs to be placed in certifiers

Here are your options. Which you choose depends on your organization's security policies:

- The most secure practice is to have many recovery ID files, each controlled by a different specific administrator, and to require several of them to work together to recover an ID. That way, no one individual acting alone can steal user IDs, but no one individual being unavailable will prevent recovery of IDs. For example, five top administrators might get the recovery ID files, but you could require that two of them have to participate in the recovery of any ID. However, this can lead to multiple recertifications of user IDs as administrator staff changes.
- An alternative to multiple recovery IDs is a single recovery ID protected by multiple passwords (which can also require two of five passwords). The downside of this is that the administrators would have to be at the same physical location to enter their passwords and unlock the ID, rather than acting independently from different locations connected by phone.
- You might use each administrator's user ID instead of assigned recovery IDs. This should not ordinarily be done because IDs in everyday use are more susceptible to theft than IDs that are kept separate and only used for this specific purpose. Even more so than with their individual IDs, owners of recovery IDs should be reminded to never tell anyone else their password.
- It is not a best practice to use shared administrator and/or recovery ID files. Although this is the easiest approach for administrators, it gives considerable power to individuals and leaves no audit trail.

***Identify the minimum number of administrator IDs (Recovery Authorities) required to open an ID file***

The Lotus recommended minimum number is three. Many organizations follow standard security practice for sensitive IDs and require two. Other organizations have minimal security requirements and only require one, and/or use a shared recovery ID.

***Identify the naming standard of the administrator IDs (Recovery Authorities) that can unlock an ID***

This can be any person that has a Notes public key in the address book. The [Domino R5 Administration Help](#) suggests using existing administrator IDs. You could also create specific ID files for administrators that would be dedicated to opening ID files. For example:

Recovery1/Recovery/TheCompany

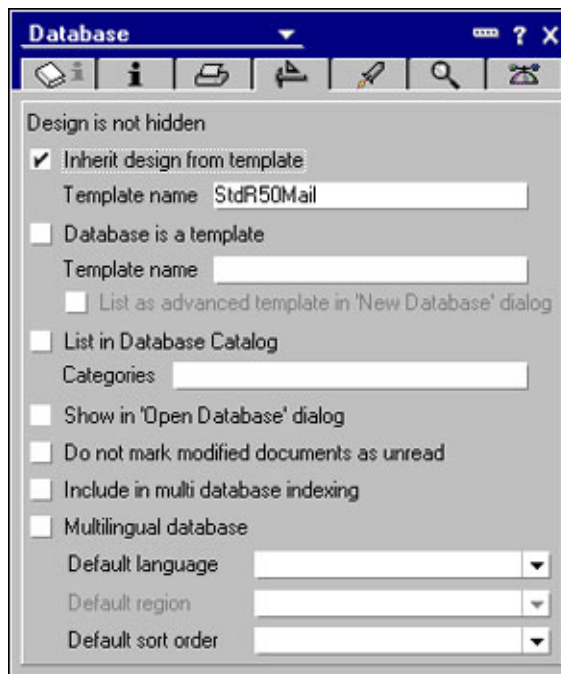
**2. Create a recovery database to house each set of IDs**

As we mentioned earlier, you can use one database for the whole organization or one per O or OU. In either case, you must:

- Create a new database on a server.
- Set the ACL as needed to limit access to only authorized administrators.

We recommend that you also:

- Use the mail50.ntf template (named StdR50Mail) for the database.
- Place the database on an isolated server, and use the Server Access field in the Server document to limit access to this server.
- Use the Design tab of the Database properties box to deselect the "Show in 'Open Database' dialog" and "List in Database Catalog" options:

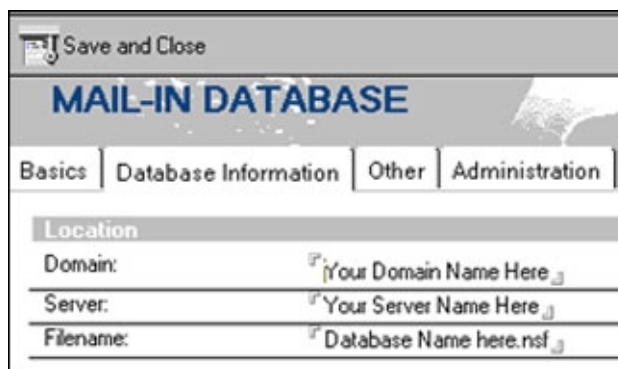


### 3. Create a mail-in database record for each recovery database

Every certifier ID has an internal memory location that lists the name of the mail-in database for the recovery of IDs. The administrator can have a single database for all certifiers or one database for each certifier.

To create a mail-in database record for each recovery database:

1. Open your domain's Domino Directory with the Notes client.
2. Go to the Server/Mail-in-Database view.
3. Click the Add Mail-in Database action button.
4. Fill in the Domain, Server, and Filename fields with the correct domain, server, and database name. It's a good idea to make the database name similar to the OU name so that it's easier to remember.



5. Save and close the document.

### 4. Add recovery information to each OU certifier

Every certifier ID can hold recovery information. This recovery information is "stamped" into each new user ID when that ID is created using an R5 Administrator client. This recovery information can also be exported and imported into R4-based IDs that are on R5 clients.

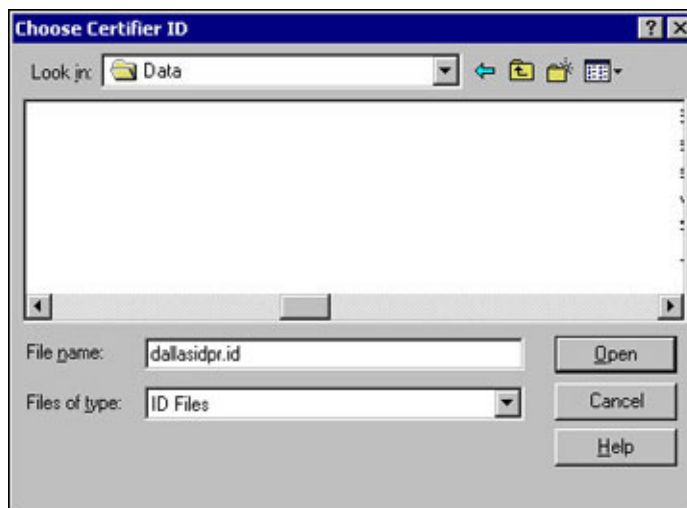
For each OU certifier:

1. From the Administrator client, select the server where you have

- registered the recovery IDs.
2. Make sure your Location document in your address book is also set to this server in the Home/mail server field of the Servers tab.
  3. Go to the Configuration tab for the server, and click Certification under Tools. Then click Edit Recovery Information:



4. In the Choose Certifier ID dialog box that appears, enter the name of the certifier ID file in the File name field. Then click Open.



5. Enter the certifier's password when prompted. The Edit Master Recovery Authority List dialog box appears:



6. Enter the minimum number of administrator IDs (Recovery Authorities) required to open an ID file in the "How many Recovery Authorities do you require" text box.
7. Click the Address button to specify the name of the mail-in database that you created.
8. Click the Add button to add the names of those who will be acting as Recovery Authorities. This opens a name and address dialog box where you select names to add to the list. (You may first have to select the directory where the Recovery Authority names are registered.)

At this point, the Recovery Authority information is complete and will take affect for all new users. For existing users, you will need to export the information and send it to them. This step is covered in the next section.

Here's an example of what a completed Edit Master Recovery Authority List dialog box looks like:



In this case, only one Recovery Authority is required, so either Mike Jones,

Tim Speed, or Tom Smith will be able to recover (unlock) an ID file. The name of the mail-in database is Dallas IDPR. All new and harvested IDs will be sent to this mail-in database for the OU /Dallas/TheCompany.

You repeat this process of adding recovery information for each OU in your organization. All new users will have recovery information in their IDs and their IDs will be automatically mailed to the recovery database. The example below shows how the recovery database looks after registering two new users:

New Memo Reply Forward Delete Folder Copy into Tools				
Who	Date	Size	Subject	
Tim Speed	09/16/2001	5,542	Backup of newly registered ID file for Joe User01/Dallas/Bubba	
Tim Speed	09/16/2001	5,544	Backup of newly registered ID file for Mary User02/Dallas/Bubba	

These messages look like any normal mail message, but they house a backup copy of the user's Notes ID file. Here is what the message looks like:



## 5. Export recovery information and send it to all current R5 users

Now your new users are protected, but any existing R5 users and R4.x users you have migrated to R5 clients and servers still do not have recovery information in their IDs. What do you do to fix this? You can export the recovery information from the certifiers and send it to the users. You need to repeat the following steps for each group of users certified with a specific certifier:

1. Tell the users why it is important for them to accept the recovery information.
2. Export the recovery information and send it to the users certified with that OU.
3. The users accept the recovery information into their ID files.
4. The users accept the option to send the ID with the new recovery information to the recovery database.

Note that this export can happen at any time, but if you are dealing with any type of migration, you will save yourself headaches if you finish the migration before you export the recovery information and send it to the users. The same is true if you are in the process of moving users from one O or OU level certifier to another one.

Now let's go through the process with one user. Suppose Billy JoBob was an R4 user that recently upgraded to an R5 client.

### ***Tell users about ID Recovery***

This is the most important step you can take, because until users accept the recovery information and mail back their IDs, their IDs will not be protected. Use whatever notification methods you normally use, but send the message several times. Explain how important it is. You might even include a button for them to acknowledge the message.

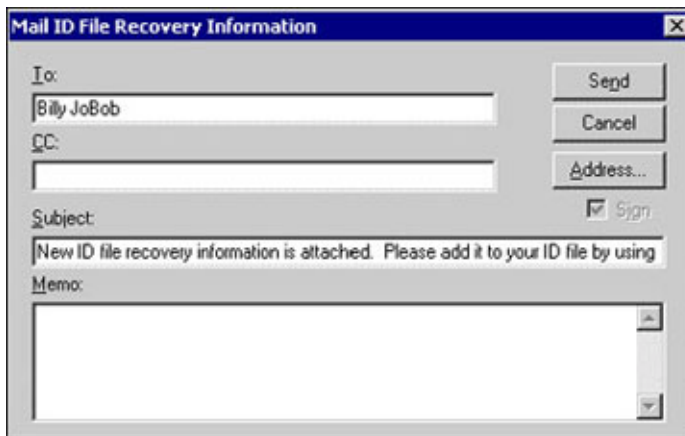
### ***Export the recovery information***



Next, you export the recovery information and send it to the users.

Remember that you have to do this for each certifier used to register users:

1. From the Administrator client, select the server where you have registered the IDs.
2. Go to the Configuration tab for the server, and click Certification under Tools. Then click Edit Recovery Information. You will be prompted for the certifier that you want to edit. Suppose you know that Billy JoBob was registered with the OU called Dallas/TheCompany. After you select the certifier for that OU and enter the password, you will see the Edit Master Recovery Authority List dialog box.
3. Click the Export button in the dialog box.
4. Enter the password for the OU and click OK. The Mail ID File Recovery Information dialog box appears:



The dialog box titled "Mail ID File Recovery Information" contains the following fields and controls:

- To:** A text field containing "Billy JoBob".
- CC:** An empty text field.
- Subject:** A text field containing "New ID file recovery information is attached. Please add it to your ID file by using".
- Memo:** An empty text area.
- Buttons:** "Send", "Cancel", "Address...", and a "Sign" checkbox.

5. In the To and CC fields, enter the user name or group name of those who should receive the recovery information. You can use the Address button to select the user names and/or group names from the Domino Directory.
6. Click the Send button.

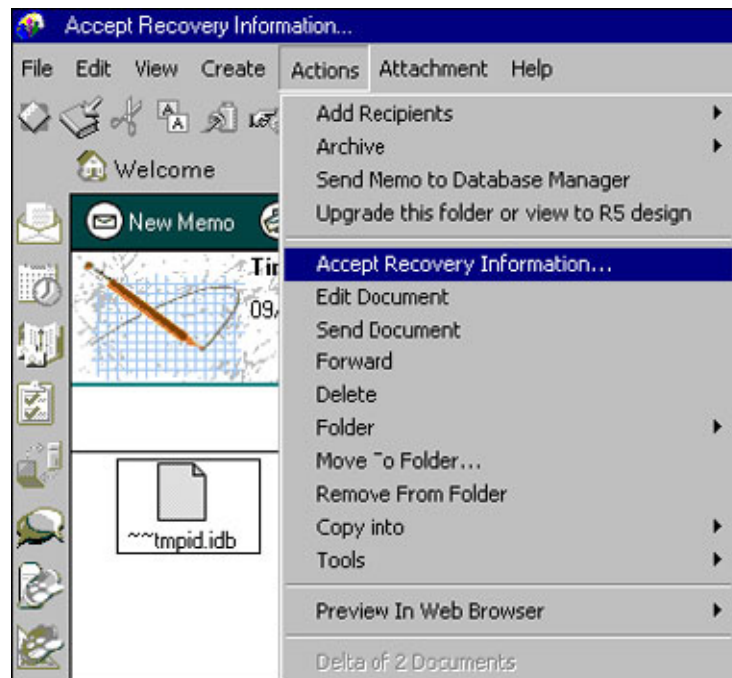
In this example, we have selected Billy JoBob. Once we click the Send button, the message will be delivered to Billy JoBob's mail file. Here's how it looks in Billy's mail file. Notice that the instructions are in the Subject line of the message.



### ***The user accepts the recovery information***

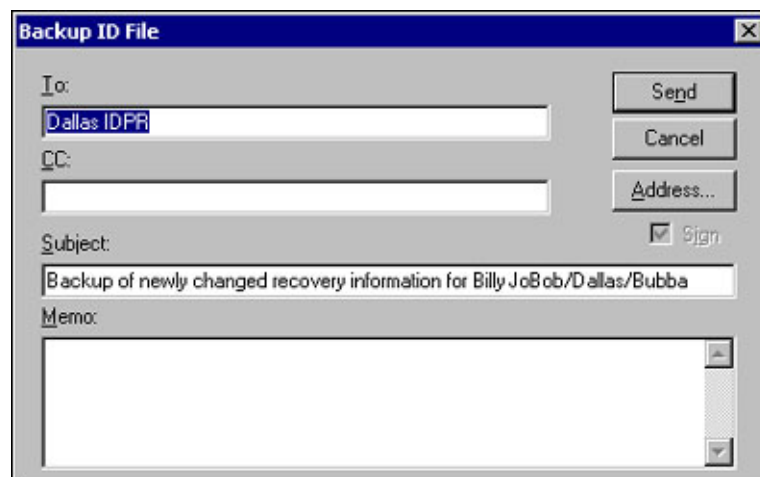
Next, Billy opens the message and follows the directions in the Subject line, choosing Actions - Accept Recovery Information:





***The user sends the ID with the recovery information to the recovery database***

Once Billy has chosen the Accept Recovery Information option, the Backup ID File dialog box appears, prompting Billy to send his ID to the recovery database:



The new recovery information is placed into users ID files once they have accepted it, even if they cancel the dialog box to e-mail a backup copy to the recovery database. But let's review the impact of several different scenarios, based on Billy's actions.

If Billy decides not to bother with another "boring administration message" and doesn't open the message and accept recovery information—in other words, does absolutely nothing—there will be no way to recover his ID file. You will probably need to issue a new ID file to Billy, even if he still has the ID file and has only forgotten the password. This will take time, and Billy will not be happy. If Billy has any encrypted messages or other data, those are permanently lost, and he will be even less happy.

By the way, if Billy is ever under suspicion of illegal activity, your audit department will not be pleased when you tell them that you cannot read his encrypted messages. Of course, an intelligent criminal won't send you the ID file with the private key that she uses for clandestine activity, but at least if you have the ID file in the recovery database, the audit department will know you did everything possible.

If Billy opens the message and chooses Actions - Accept Recovery Information but then cancels out of the Backup ID dialog box, the ID will be recoverable, but a current copy of the ID file will not be in the recovery database. This means that the following information will not be available:

- Current certificates
- Secret keys
- X.509 certificates
- Recovery passwords

In other words, Billy and you are in almost the same predicament as if he hadn't done anything at all. The only advantage is that someone could possibly make a copy of the ID file on Billy's workstation and send it to you and then you could recover it—not an option when the ID file is at the bottom of the Gulf of Mexico.

The moral is that you should never shortcut the first step—telling users about ID Recovery. It's important to impress the importance of ID Recovery on your users and to make sure they follow through. In fact, it's much better for you—and for everyone else—if you keep track of which users have sent in their recoverable IDs and harass the others until they do too.

Also, if people in your organization use S/MIME or other X.509 certificates, it is a good idea to repeat the recovery process every few months to keep this information up-to-date. Otherwise, normal recertification will take care of keeping the stored user IDs current.

## How to recover an ID

So far, we've discussed setting up ID Recovery and showed you that once the recovery was enabled, it would place the recovery data in new user IDs. We also showed you how to harvest and enable IDs that were created before ID Recovery was implemented. Now we can turn our attention to how you actually recover an ID.

Before ID Recovery, it didn't matter whether the user had lost the ID file or had only forgotten the password—in either case, if you had a backup of the ID file with a known password, you could send it to the user, either by sneaker net or by sending the file to the user's local administrator or manager. Otherwise, you would have to give the user a totally new ID file.

With ID Recovery in place, the process of recovering from a forgotten password is different than from recovering from a lost ID. When the user has only forgotten the password, the whole recovery process can take place over the phone, which means that if the administration team is available, the user can be back in business in minutes. If the ID file is at the bottom of the Gulf of Mexico, the physical ID file has to be delivered to the user, but at least all the certificates and private keys are current.

The basic process has four steps:

1. You copy the ID file from the recovery database.
2. You (or whoever is authorized in the certifier file as a Recovery Authority) recovers the ID by using the Administrator client to find your recovery password for that ID. This process is repeated with different administrators who are Recovery Authorities until the minimum number of recovery passwords has been obtained.
3. You give the recovery passwords to the user.
4. You or the user enters the recovery passwords, unlocking the ID file

and making it fully functional.

Here are the steps in detail.

### 1. Copy the ID file from the recovery database

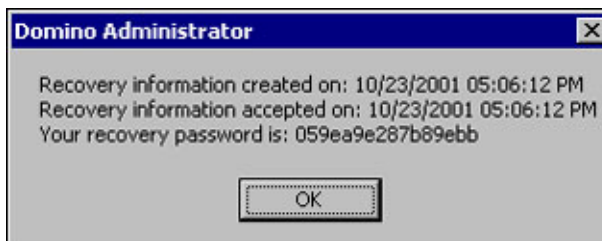
This step is simple. You:

1. Open the recovery database.
2. Open the last message from the user.
3. Right-click the attachment and choose Detach. You should detach the attachment to a local drive.

### 2. Find the recovery passwords for the ID

This step is also straightforward:

1. From the Administrator client, select the server where you have registered the IDs.
2. Go to the Configuration tab for the server, and click Certification under Tools. Then click Extract Recovery Password. You will be prompted for your password and for the ID that you want to recover.
3. Enter your password and then select the ID that you want to recover. If your ID is authorized to recover the ID that you selected—that is, you are listed as a Recovery Authority for that ID—you will see the following information:



If your name was not on the recovery list of the certifier for that ID, you see an error message indicating that you are not authorized to recover that ID file.

4. Different administrators should repeat the process until you have the necessary number of recovery passwords to recover the ID. For example, three recovery authorities must extract their recovery password for the ID if the ID Recovery process was set up to require at least three Recovery Authorities. For best security, the user should deal with each Recovery Authority separately so that only the user has the recovery passwords needed to unlock the ID (and no one intermediary ever has them).

### 3. Give the recovery information to the user

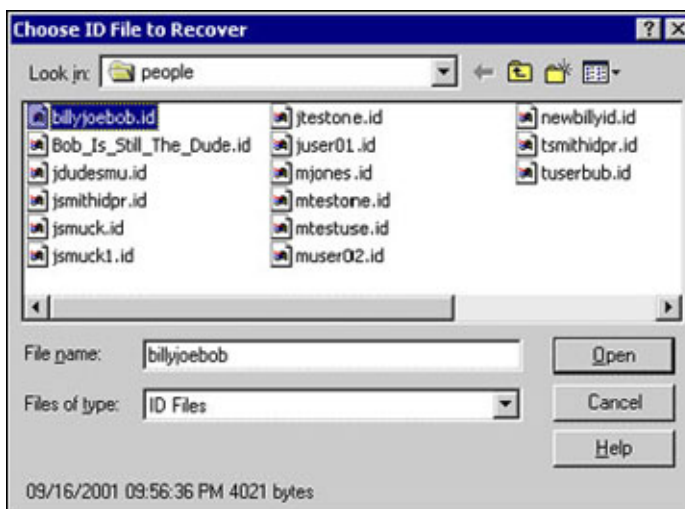
At this point, you have essentially two choices: You can read the recovery passwords to the user over the phone or you can recover the ID yourself, assign an easier password, and send the ID and password to the user's administrator or manager. Some users have so much trouble entering a 16-character random string that they actually prefer to wait and get the ID file itself with an easier password, or your organization may expect local administrators to do the recovery for the user.

### 4. You or the user enter the recovery passwords and recover the ID file

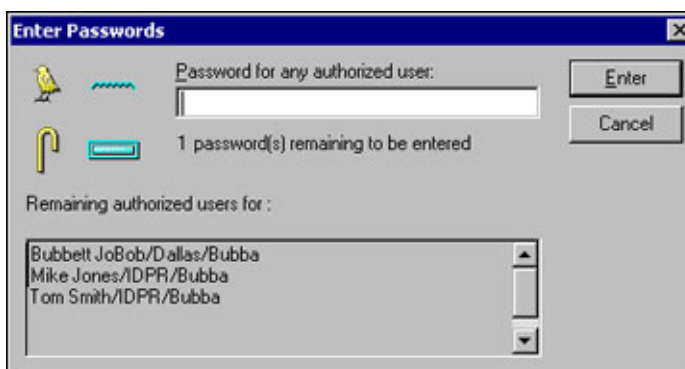
Actual recovery of the ID file can occur under either scenario, with either you recovering the ID yourself or the user recovering the ID with the recovery information you give them.

If you, as an administrator, are going to recover the ID file for the user, you can follow these steps:

1. From the Notes client, select File - Tools - User ID - Recover ID. The Choose User ID to Recover dialog box appears:



2. Select the ID file you want to recover and click Open. The Enter Passwords dialog box appears. It lists the administrators with Recovery Authority status who can recover the selected ID. It also displays the minimum number of Recovery Authorities needed to recover the ID.

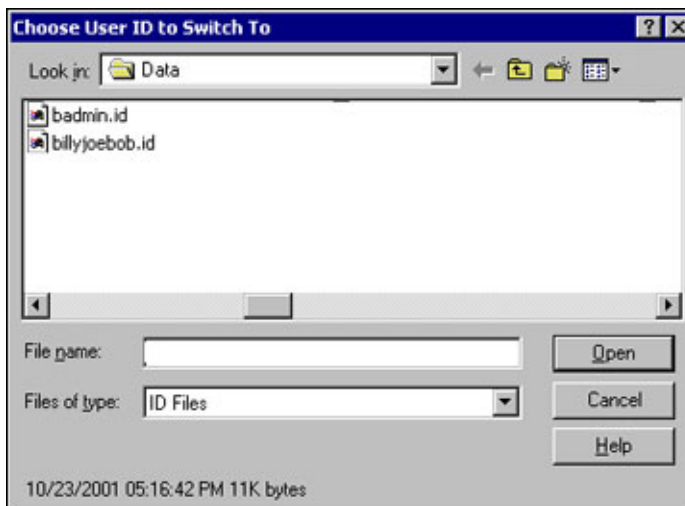


- In this example, one recovery password is needed to unlock the ID, and three administrators are authorized as Recovery Authorities for this ID.
3. Enter the 16-character recovery password for one of the Recovery Authorities listed. The required number of passwords can be entered in any order. Click Enter after typing each one. A message confirms whether the password was valid. The dialog box displays how many more passwords are needed. Once you have entered the appropriate number of recovery passwords, the Set Password dialog box appears.
  4. Enter a new password for the user and click OK. The Set Password verification dialog box appears. As always, you have to enter the password again to make sure there were no typographical errors.
  5. Enter the password again and click OK. The ID file is now fully recovered and functional. You can send the ID file to the user along with their new password, usually via the user's manager.

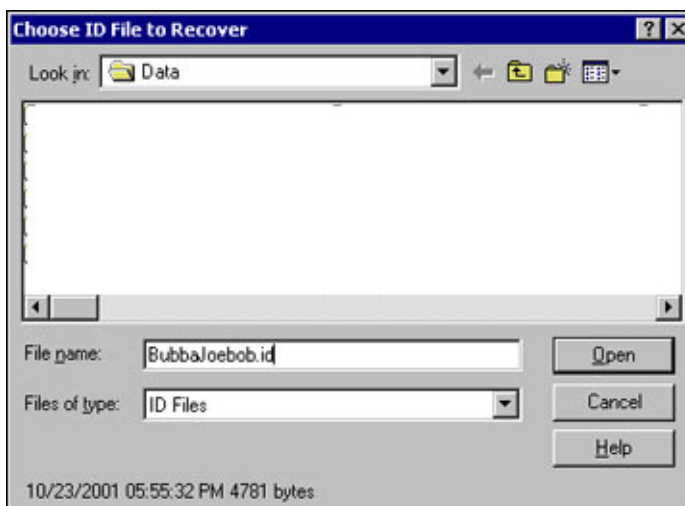
If, on the other hand, the user is going to recover her own ID file, the File - Tools - User ID - Recover ID won't work, because she can't use her Notes client without knowing the password to the ID file. The solution is simple, but not necessarily obvious. To recover an ID file when you can't get into the Notes client:

1. Start Notes.
2. At the Enter Password dialog box, click Cancel. (If you enter the wrong password and click OK, you see the Wrong Password message. Click OK at that message to return to the Enter Password dialog box and then click Cancel.)

3. When the Enter Password dialog box reappears, click Cancel again. The Choose User ID to Switch To dialog box appears:

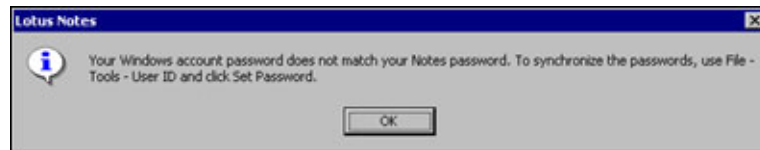


4. At the Choose User ID to Switch To dialog box, click Cancel. This opens the Choose ID File to Recover dialog box:



5. Select the ID file to recover and click Open. The Enter Password dialog box appears with the list of Recovery Authorities. From this point on, the process is the same as that followed by an administrator recovering a user's ID.
6. In the Enter Password dialog box, enter the 16-character recovery ID of one of the Recovery Authorities and click Enter. Repeat this until you have entered the appropriate number of recovery passwords, at which point, the Set Password dialog box appears.
7. Enter a new password, click OK, and then enter the new password again as verification. Then click OK.

Whether you have recovered the user's ID, reset her password, and sent her the ID file or she has done the recovery herself, if she is running Windows NT or Windows 2000 and the Domino synchronization code, there is one more step to take. The user will be prompted to synchronize the Windows and Notes passwords, either right after she finishes setting the recovered ID's new password or when she first uses the recovered ID.



The user should follow the directions in the message to synchronize the passwords.

## The end of the story

That's it; now you know why it was so easy for Cindy HelpDesk to help Bubba Smith with his lost ID. The ID Recovery process is straightforward to set up and use. The only part that takes effort is getting your users to understand how important it is—before they drop their laptops in the Gulf of Mexico. Otherwise, once you have set up the databases and certifiers, sent recovery information to existing users, and retrieved their updated ID files, you have a working recovery system that will make life easier for you and your users.

## ABOUT THE AUTHORS

Timothy Speed is an infrastructure and security architect for Lotus Professional Services (LPS). Tim has been involved in Internet and messaging security for the last nine years. He also participated with the Domino infrastructure at the Nagano Olympics and assisted with the Lotus Notes systems for the Sydney Olympics. His certifications include, MCSE®, VCA (VeriSign Certified Administrator), Lotus Domino CLP Principal Administrator, and Lotus Domino CLP Principal Developer. Tim has also co-authored two books: *The Internet Security Guidebook*, ISBN: 0122374711, February, 2001, and *The Personal Internet Security Guidebook*, ISBN: 0126565619, October, 2001. You can reach Timothy at [Tim\\_Speed@Lotus.com](mailto:Tim_Speed@Lotus.com).

Mary LaRoche is a consulting IT security and infrastructure specialist for Lotus Professional Services (LPS). Mary has been working with messaging security and Notes and organizational security for the last eight years. She recently worked with several Federal agencies to implement secure organization-wide Domino infrastructures. You can reach Mary at [Mary.LaRoche@Lotus.com](mailto:Mary.LaRoche@Lotus.com).