Many Lotus customers use Lotus messaging and/or applications on Windows and manage Microsoft server/client environment via Microsoft Active Directory. There are two important business requirements in this architecture, centralised user management and one step login.

Centralised user management

In Lotus – Microsoft environment there are at least two directory, Microsoft Active Directory to manage Microsoft environment and Lotus Domino Directory to manage Lotus environment. Both of them handle users, groups and passwords. Without using any integration tools administration has to manage users in both environment (for exaple name change request, password request, password reset, etc.). It means additional cost and efforts.

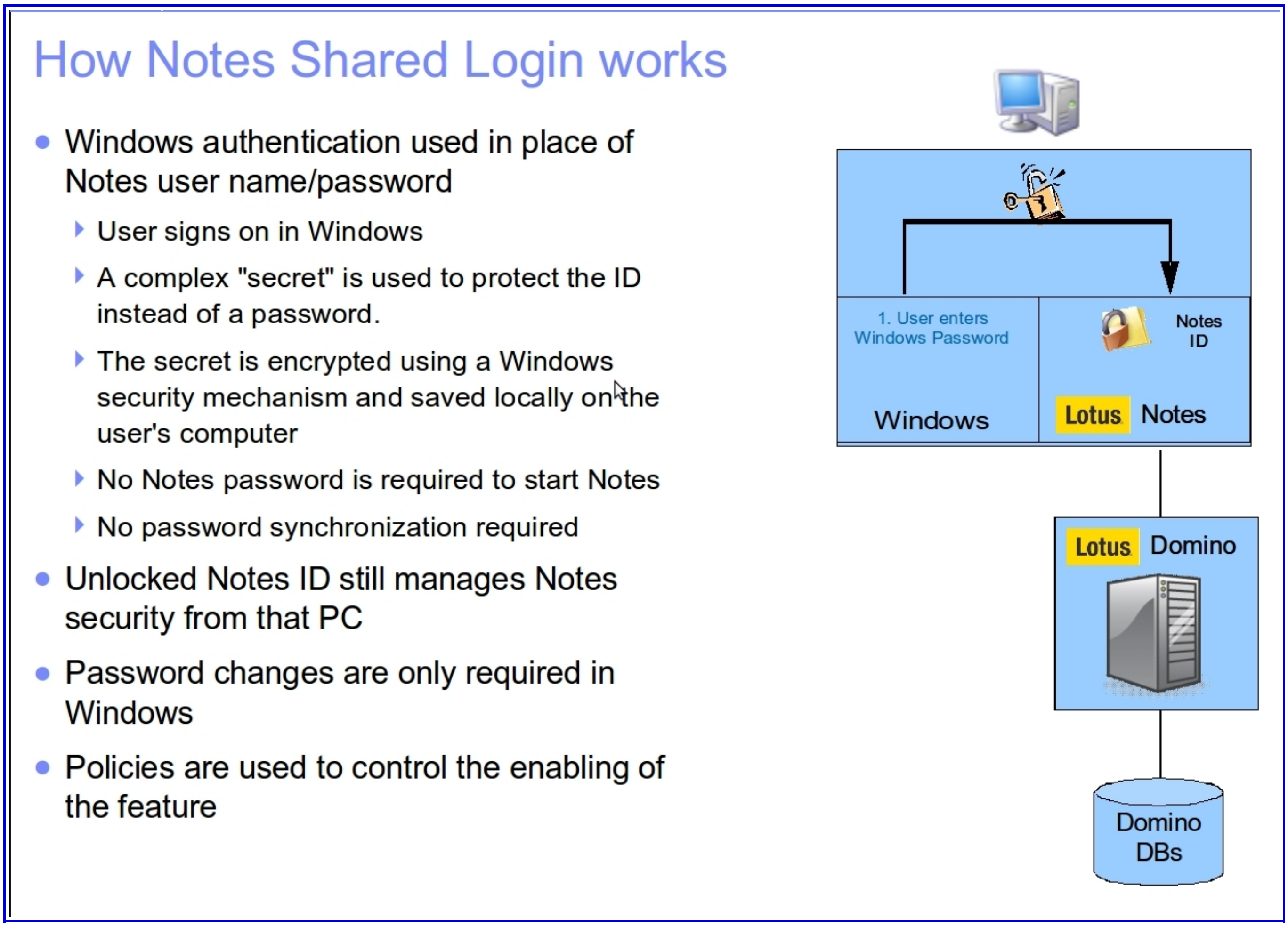
Solutions:

Domino Active Directory sync: Customers with Lotus Domino/Notes licences are eligible to implement this tool without additional licence cost. It provides features&functions to manage users and groups in Microsoft Active Directory and sychronise them with Lotus Domino Directory (setting up Domino Active Directory synchronisation). Lotus Domino and Microsoft experts can implement this solution.

IBM Tivoli Directory Integrator **(TDI)**: The basic goal of data synchronization is to detect changes in one data source and then propagate these to one or more targets. Discovering and then applying changes is not as easy as you might think. Some systems provide change event notifications, most do not. Many maintain some sort of modifications list, but the level of detail available here varies greatly. A few systems allow you to incrementally modify the values of selected attributes. However, the majority require you to build a full data entry with all updates in place and then write this in a single operation. **TDI** gives you a framework for handling all issues at a comfortably abstract level.
TDI video tutorials found here: http://www.tdi-users.org/twiki/bin/view/Integrator/LearningTDI.
Customer has to have licence and Tivoli experts are required to implement this solution.

One step login

End users has to login to Windows first, then login to Lotus Notes client. If there are no policies and other restrictions, many users use different passwords. It is really hard to manage password related issues. Via policies, Lotus Domino provides password management tools like remote password change, password reset, password expiration, etc. but without integration administration has to manage all issues in Microsoft Active directory, too.
Lotus Domino **Shared Login** and **ID Vault** tools are built-in services (no additional charge) and solves most of the ID issues in MS Windows environment. With Shared login feature Microsoft Windows users do not need to login to Lotus Notes client anymore, without loosing the market leader security features. User names and passwords are being managed in Microsoft Active Directory. For example, MS administrators can reset end user password. ID Vault manages ID files on the end user's computer. It solves broken, lost ID issues. Lotus Domino administrators and MS AD administrators can implement Shared login and ID vault via Lotus Domino security policies (enable/disable feature) without going to every machine.



How Notes Shared Login works

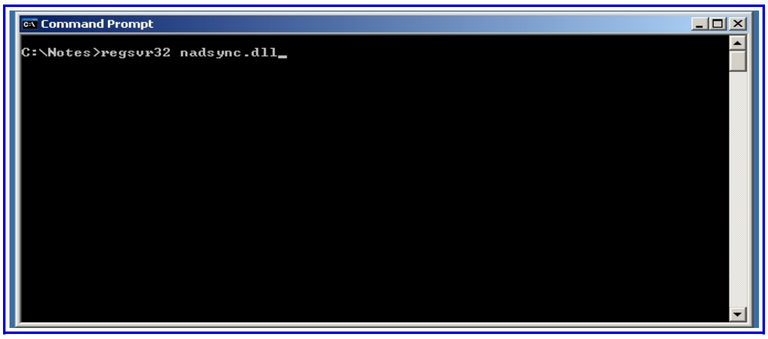
- Windows authentication used in place of Notes user name/password
  - User signs on in Windows
  - A complex "secret" is used to protect the ID instead of a password.
  - The secret is encrypted using a Windows security mechanism and saved locally on the user's computer
  - No Notes password is required to start Notes
  - No password synchronization required
- Unlocked Notes ID still manages Notes security from that PC
- Password changes are only required in Windows
- Policies are used to control the enabling of the feature

Domino Active Directory synchronisation

Install the Active Directory domain controller, the Domino server, and the Domino Administrator on separate computers to improve performance and enhance security. However, if necessary you may install the Domino server on the same computer as the Active Directory domain controller.

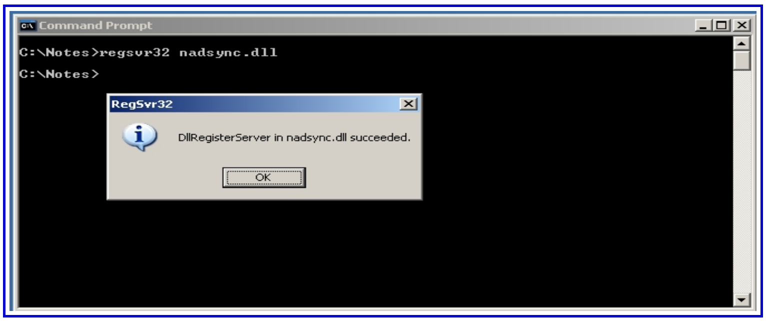
1. Open a command prompt. From your Notes install directory, type:

```
regsvr32 nadsync.dll
```



```
C:\Notes>regsvr32 nadsync.dll_
```

2. A message box appears indicating that registration is complete. This can take up to one minute.

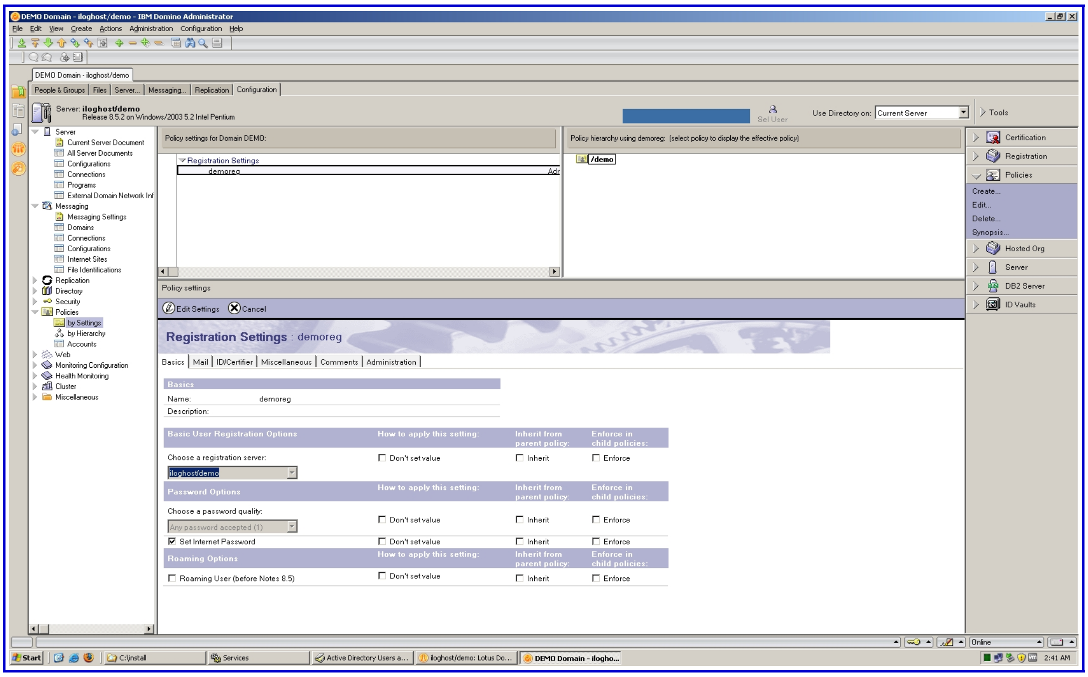


```
C:\Notes>regsvr32 nadsync.dll

C:\Notes>
```

DllRegisterServer in nadsync.dll succeeded.

3. From the Domino Administrator, create an organizational policy or an explicit policy and a Registration policys settings document. You must have at least one policy to use with ADSync.



DEMO Domain - iloghost/demo - IBM Domino Administrator

DEMO Domain - iloghost/demo

Server: **iloghost/demo**
Release 8.5.2 on Windows/2003 5.2 Intel Pentium

Use Directory on: Current Server

Policy settings for Domain DEMO:

Registration Settings
demoreg

Policy hierarchy using demoreg: (select policy to display the effective policy)

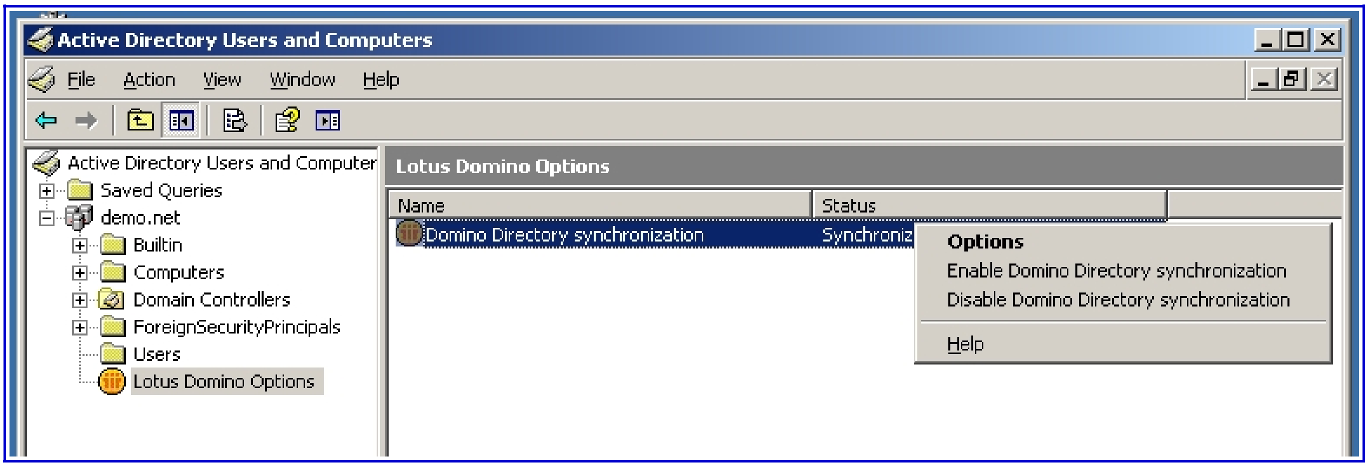
/demo

Policy settings

Registration Settings : demoreg

Basics			
Name: demoreg			
Description:			
Basic User Registration Options	**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
Choose a registration server: iloghost/demo	☐ Don't set value	☐ Inherit	☐ Enforce
Password Options	**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
Choose a password quality: Any password accepted (1)	☐ Don't set value	☐ Inherit	☐ Enforce
☑ Set Internet Password	☐ Don't set value	☐ Inherit	☐ Enforce
Roaming Options	**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
☐ Roaming User (before Notes 8.5)	☐ Don't set value	☐ Inherit	☐ Enforce

4. From the Start menu, click Programs - Administrative Tools - Active Directory Users and Computers. Click the Lotus Domino Options folder.

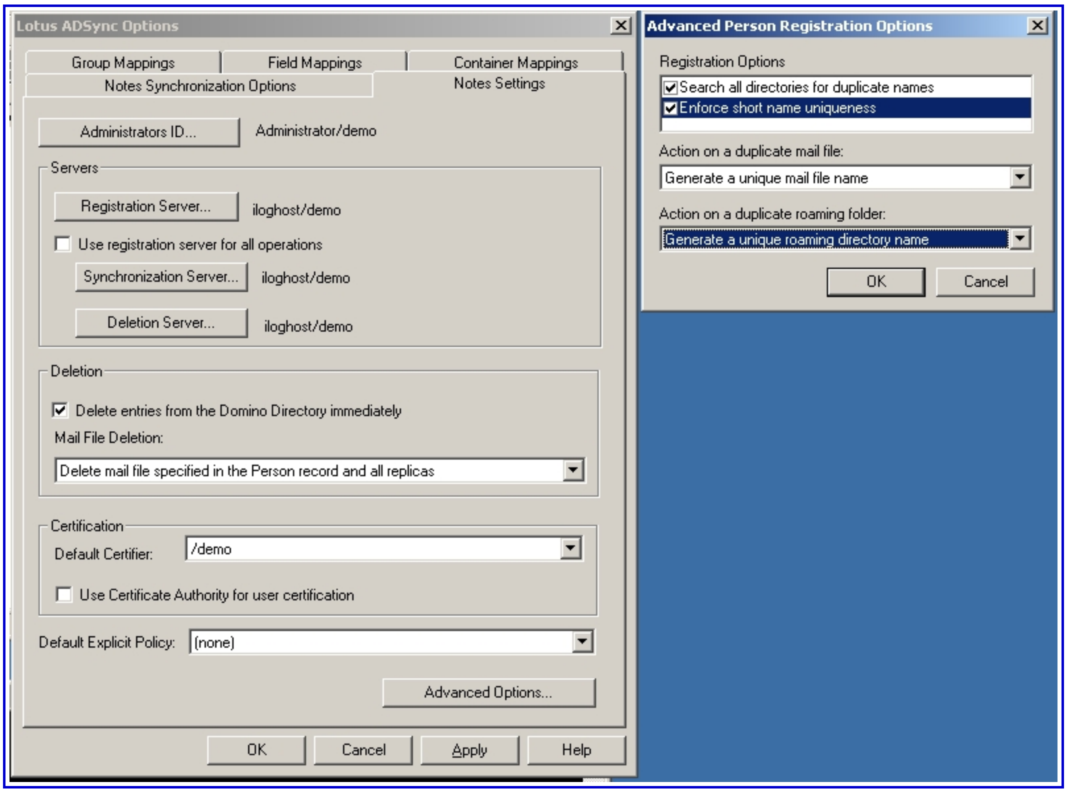

Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computer
Saved Queries
demo.net
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Lotus Domino Options
Lotus Domino Options
Name
Status
Domino Directory synchronization
Synchroniz
Options
Enable Domino Directory synchronization
Disable Domino Directory synchronization
Help

5. Right-click Domino Directory synchronization, and then choose Options.

6. Enter your Notes password.

7. Click the Notes Settings tab.

8. Click the Notes Server for Registration button and specify a registration server. This is typically the administration server of the Domino Directory.



Administrators ID... Administrator/demo

Servers

Registration Server... iloghost/demo

☐ Use registration server for all operations

Synchronization Server... iloghost/demo

Deletion Server... iloghost/demo

Deletion

☑ Delete entries from the Domino Directory immediately

Mail File Deletion: Delete mail file specified in the Person record and all replicas

Certification

Default Certifier: /demo

☐ Use Certificate Authority for user certification

Default Explicit Policy: (none)

Registration Options

☑ Search all directories for duplicate names

☑ Enforce short name uniqueness

Action on a duplicate mail file: Generate a unique mail file name

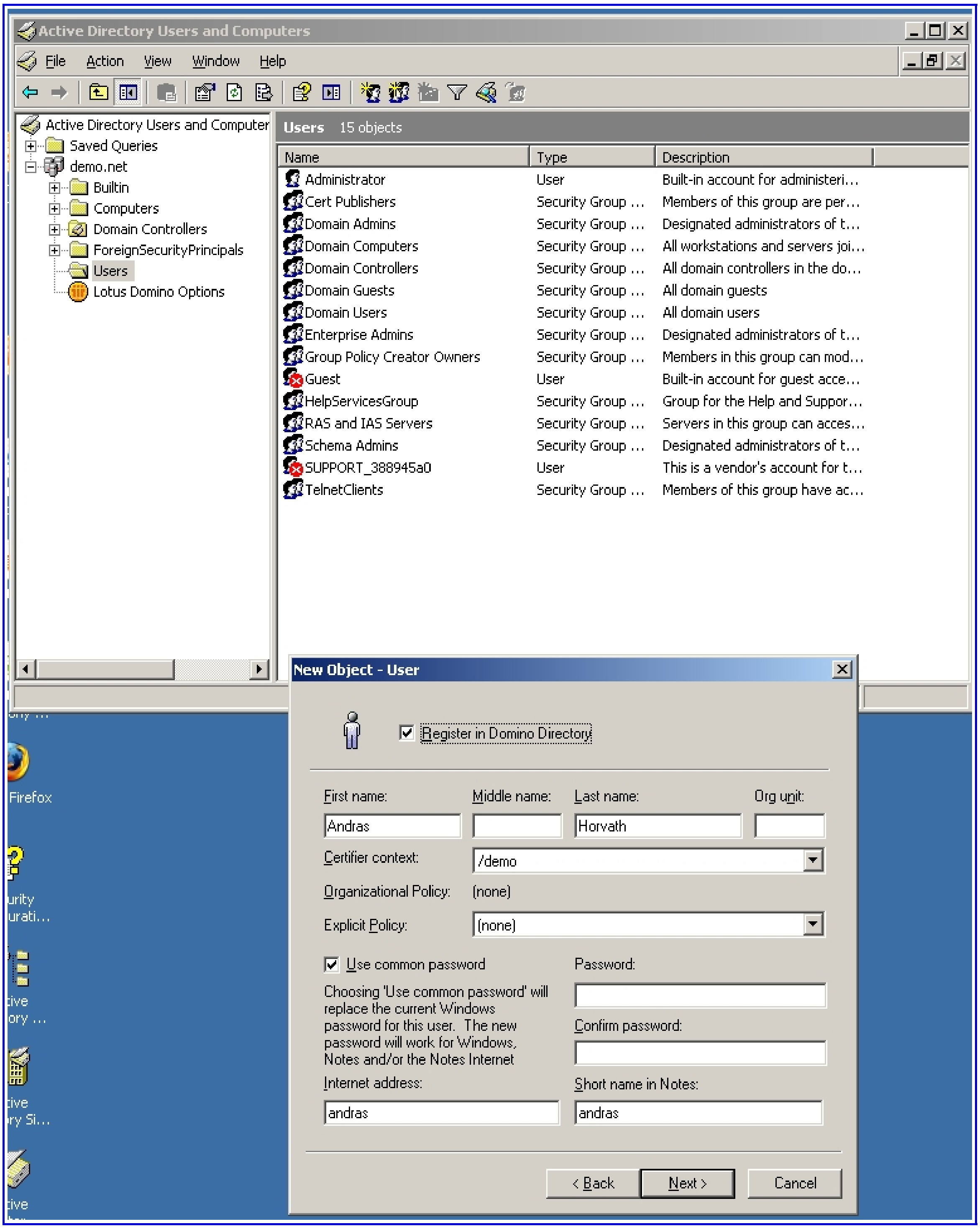
Action on a duplicate roaming folder: Generate a unique roaming directory name

9. Click OK.

10. Close and restart Active Directory Users and Computers to allow these changes to take effect.

11. Register new user in Active Directory and synchronise it with Lotus Domino Directory

12. Create a new user in the current container


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
demo.net
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Lotus Domino Options
Users 15 objects
Firefox

Name	Type	Description
Administrator	User	Built-in account for administeri...
Cert Publishers	Security Group ...	Members of this group are per...
Domain Admins	Security Group ...	Designated administrators of t...
Domain Computers	Security Group ...	All workstations and servers joi...
Domain Controllers	Security Group ...	All domain controllers in the do...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators of t...
Group Policy Creator Owners	Security Group ...	Members in this group can mod...
Guest	User	Built-in account for guest acce...
HelpServicesGroup	Security Group ...	Group for the Help and Suppor...
RAS and IAS Servers	Security Group ...	Servers in this group can acces...
Schema Admins	Security Group ...	Designated administrators of t...
SUPPORT_388945a0	User	This is a vendor's account for t...
TelnetClients	Security Group ...	Members of this group have ac...

New Object - User

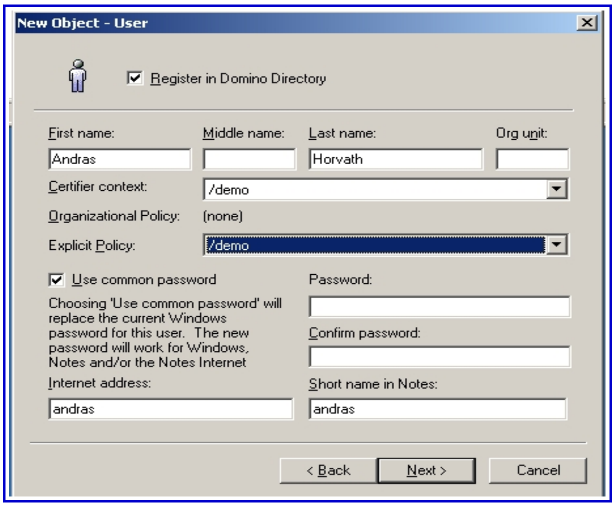
☑ Register in Domino Directory

First name: Andras
Middle name:
Last name: Horvath
Org unit:
Certifier context: /demo
Organizational Policy: (none)
Explicit Policy: (none)

☑ Use common password

Choosing 'Use common password' will replace the current Windows password for this user. The new password will work for Windows, Notes and/or the Notes Internet

Password:
Confirm password:
Internet address: andras
Short name in Notes: andras



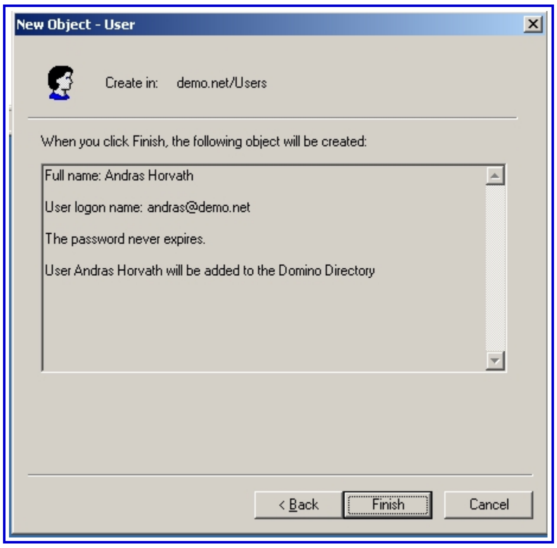
☑ Register in Domino Directory

First name: Andras
Middle name:
Last name: Horvath
Org unit:
Certifier context: /demo
Organizational Policy: (none)
Explicit Policy: /demo

☑ Use common password

Choosing 'Use common password' will replace the current Windows password for this user. The new password will work for Windows, Notes and/or the Notes Internet

Password:
Confirm password:
Internet address: andras
Short name in Notes: andras



Create in: demo.net/Users

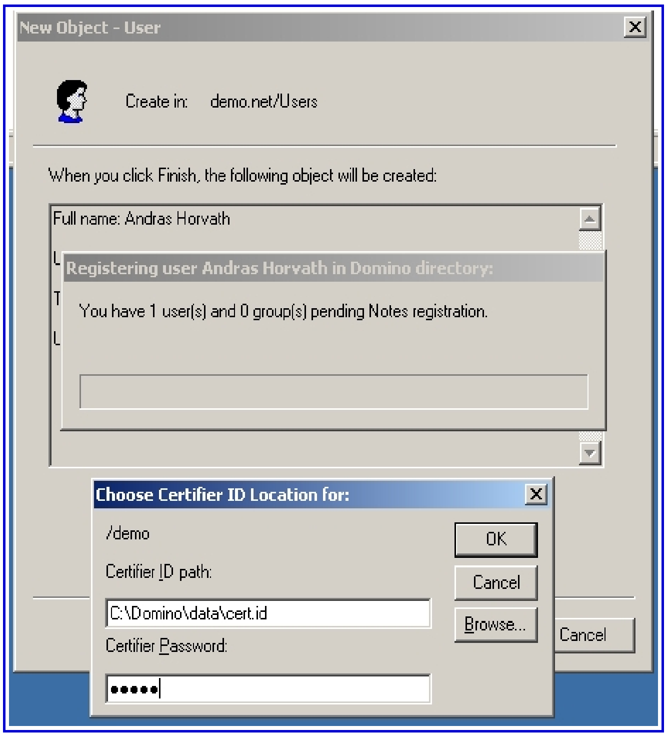
When you click Finish, the following object will be created:

Full name: Andras Horvath

User logon name: andras@demo.net

The password never expires.

User Andras Horvath will be added to the Domino Directory



Create in: demo.net/Users

When you click Finish, the following object will be created:

Full name: Andras Horvath

Registering user Andras Horvath in Domino directory:

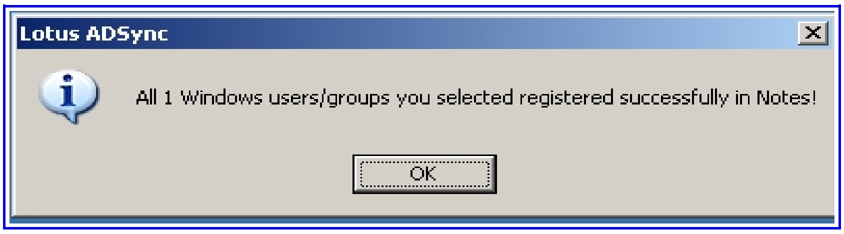
You have 1 user(s) and 0 group(s) pending Notes registration.

Choose Certifier ID Location for:

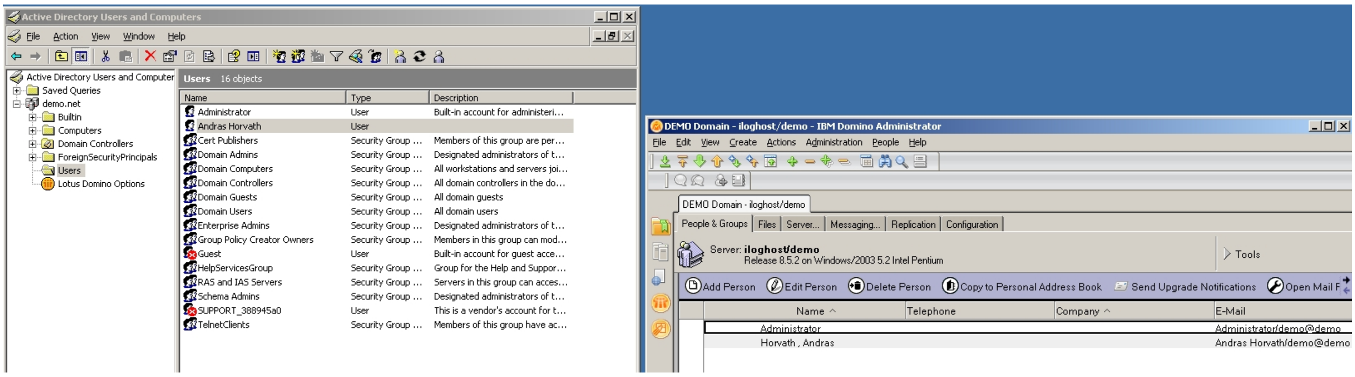
/demo

Certifier ID path: C:\Domino\data\cert.id

Certifier Password: •••••



All 1 Windows users/groups you selected registered successfully in Notes!


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
demo.net
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Lotus Domino Options
DEMO Domain - iloghost/demo - IBM Domino Administrator
File Edit View Create Actions Administration People Help
DEMO Domain - iloghost/demo
People & Groups
Files
Server...
Messaging...
Replication
Configuration
Tools
Add Person
Edit Person
Delete Person
Copy to Personal Address Book
Send Upgrade Notifications
Open Mail F

Users 16 objects

Name	Type	Description
Administrator	User	Built-in account for administeri...
Andras Horvath	User	
Cert Publishers	Security Group ...	Members of this group are per...
Domain Admins	Security Group ...	Designated administrators of t...
Domain Computers	Security Group ...	All workstations and servers joi...
Domain Controllers	Security Group ...	All domain controllers in the do...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators of t...
Group Policy Creator Owners	Security Group ...	Members in this group can mod...
Guest	User	Built-in account for guest acce...
HelpServicesGroup	Security Group ...	Group for the Help and Suppor...
RAS and IAS Servers	Security Group ...	Servers in this group can acces...
Schema Admins	Security Group ...	Designated administrators of t...
SUPPORT_388945a0	User	This is a vendor's account for t...
TelnetClients	Security Group ...	Members of this group have ac...

Server: **iloghost/demo**
Release 8.5.2 on Windows/2003 5.2 Intel Pentium

Name	Telephone	Company	E-Mail
Administrator			Administrator/demo@demo
Horvath , Andras			Andras Horvath/demo@demo

1. Illustration: Andras Horvath registered in both directory

Lotus Shared login implementation

Notes shared login allows users to start Lotus Notes and use their Notes IDs without having to provide Notes passwords. Instead, they only need to log in to Microsoft Windows using their Windows passwords. This is not the same mechanism as Notes single login, a feature that was introduced in a previous version of Notes. Notes single login was a method of synchronizing the Windows and Notes passwords, Notes shared login removes the need for a Notes password altogether. Enabling an ID for Notes shared login alters it so the ID works only on the computer on which the feature is activated. This is because the feature relies on a Windows security infrastructure specific to that computer. With Notes shared login users only need to remember their Windows passwords and administrators are not required to manage Notes passwords or assist users who have forgotten their passwords because there are no longer Notes passwords to manage! **Notes shared login works without interruption when Windows passwords are changed either by users or by administrators on a Windows domain controller.**

Please study your production environment and consider all aspects before Shared login implementation (optionally discuss it with your Lotus Business Partner).

This guide is created in a demo environment, you have to use your own names and passwords.

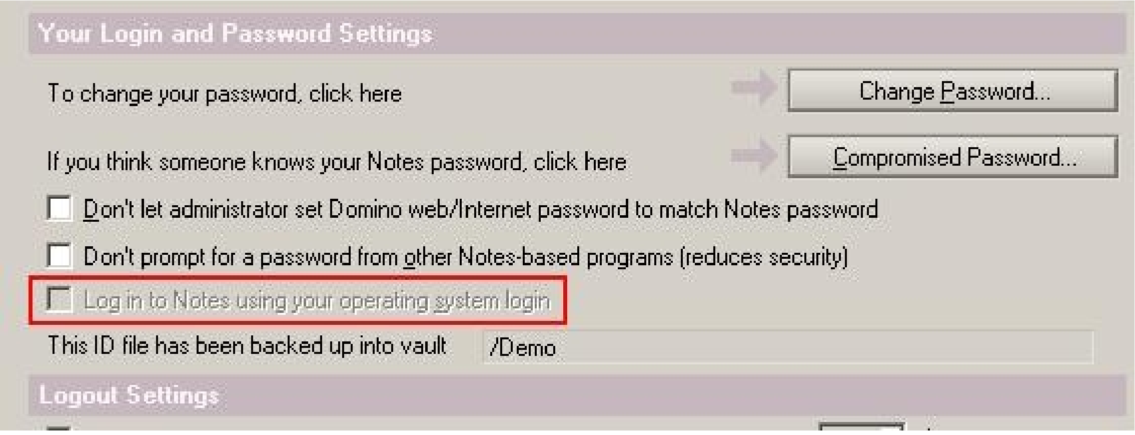
13. Start Lotus Notes (if not already started)

14. Select or switch to **Online - Admin** location

15. Enter password of “**passw0rd**”

16. Select **File > Security > User Security** from the menu

17. Enter password of “**passw0rd**” again.

18. 

Your Login and Password Settings

To change your password, click here

If you think someone knows your Notes password, click here

□ Don't let administrator set Domino web/Internet password to match Notes password

□ Don't prompt for a password from other Notes-based programs (reduces security)

□ Log in to Notes using your operating system login

This ID file has been backed up into vault /Demo

Logout Settings

19. Note the option to login to Notes using the operating system login is greyed out. This is because this feature is disabled by default.

20. Close the dialog and open the Domino Administrator client.

21. Switch to the **People & Groups** tab and select **Settings**

22. Open the **DemoVault** settings document. Since Notes ID vault and Notes Shared Login can work together we will configure them through the same policy.

23. Select the **Password Management** tab and then the **Notes Shared Login** tab.In this lab we are going to configure Notes Shared Login to be turned on by default and not allow the user to change this.

24. Select **Edit Settings** from the Action bar

25. Configure the tab as follows:

Enable Notes shared login with operating system	26. Yes
How to apply this setting	27. Set value whenever modified
Allow User Changes?	28. No
How to notify users when enabled	29. System dialog
How to notify users when disabled	30. System dialog

31. Click **Save & Close** in the action bar

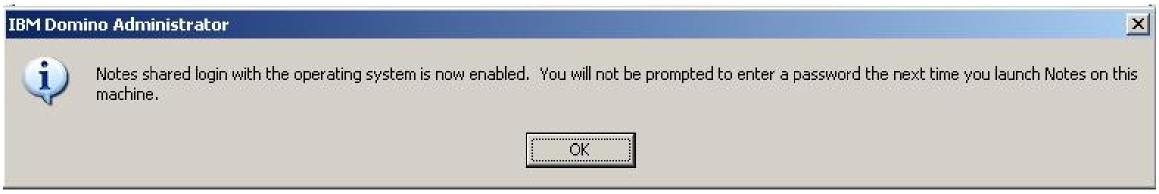
32. Close both the Notes and Domino Administrator clients

33. Start Lotus Notes client.

34. Select **Online – New User1** as the location document and enter "**newpassw0rd**" as password.

35. Within a minute you should get a message pop-up as follows.

36.

37. 

IBM Domino Administrator

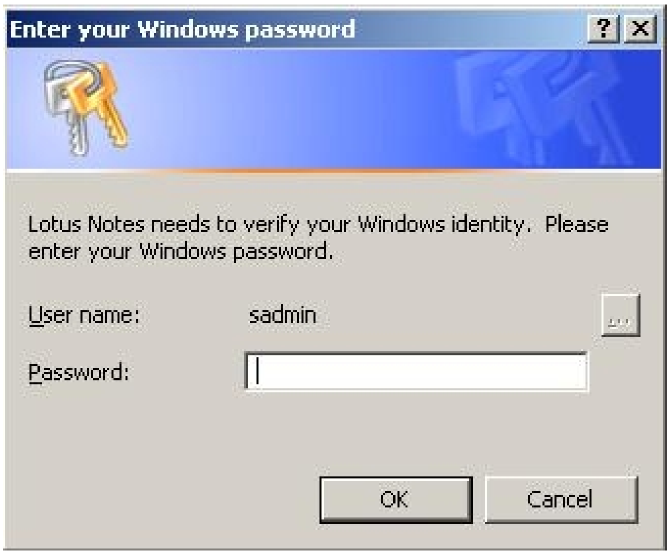
Notes shared login with the operating system is now enabled. You will not be prompted to enter a password the next time you launch Notes on this machine.

Troubleshooting

If the message does not appear after a short while – try starting up the Domino Admin client – this may kick it into action

38. Click **OK** to close the message.

39. **Select File > Security > User Security** from the menu

40. 

Enter your Windows password

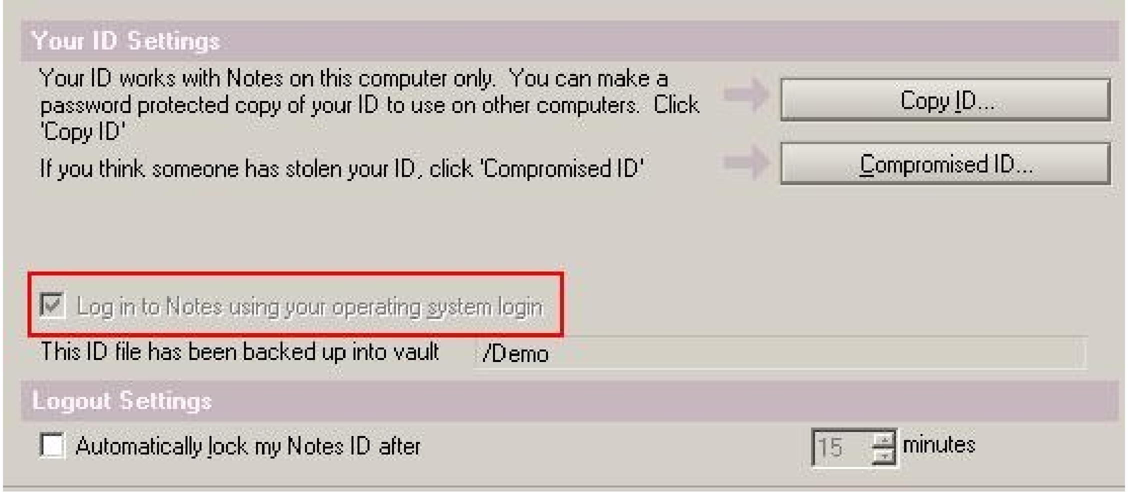
Lotus Notes needs to verify your Windows identity. Please enter your Windows password.

User name: sadmin

Password:

41. Notice that you are no longer prompted for your Notes password as you try to access a secured area of the client. Instead you are prompted for the operating system password of the Windows account with which you are logged in.

42. Enter the windows password for **sadmin** which is "**passw0rd**" and click **Login**

43. 

Your ID Settings

Your ID works with Notes on this computer only. You can make a password protected copy of your ID to use on other computers. Click 'Copy ID'

If you think someone has stolen your ID, click 'Compromised ID'

☑ Log in to Notes using your operating system login

This ID file has been backed up into vault /Demo

Logout Settings

□ Automatically lock my Notes ID after 15 minutes

44. Notice that the options under Your ID Settings have changed. The option to login to Notes using the

operating system login is now selected and not greyed out and the option for synchronizing your Notes password with your HTTP password and suppressing password prompts from other Notes-based programs are no longer displayed. Neither of these are compatible with Notes Shared Login as there is no longer a password associated with the Notes ID that you are now using with the Lotus Notes 8.5 client.

45. Restart the **Notes** client and notice that you are no longer prompted for a password.

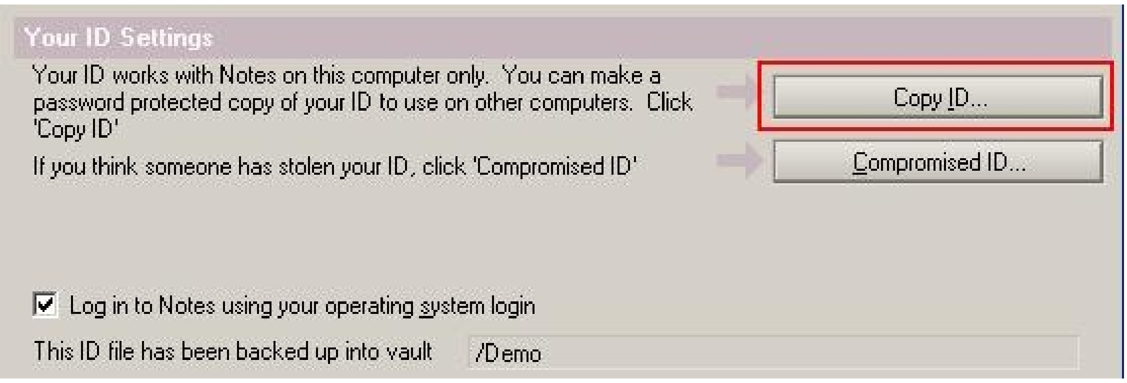
46. Creating password-**protected** copy of ID

47. Once Notes Shared Login has been enabled, the ID cannot be copied via operating system mechanisms and used on another client. Enabling an ID for Notes shared login alters the ID so that it only works on the computer on which the feature was activated. This is because the feature relies on a Windows security infrastructure specific to that computer. In this step we will show how a user can create a copy of their ID for use on another client.

48. Select **File > Security > User Security** from the menu and enter the windows password "**passw0rd**".

49. **Click** on the **Copy ID** button.

50.



Your ID Settings

Your ID works with Notes on this computer only. You can make a password protected copy of your ID to use on other computers. Click 'Copy ID'

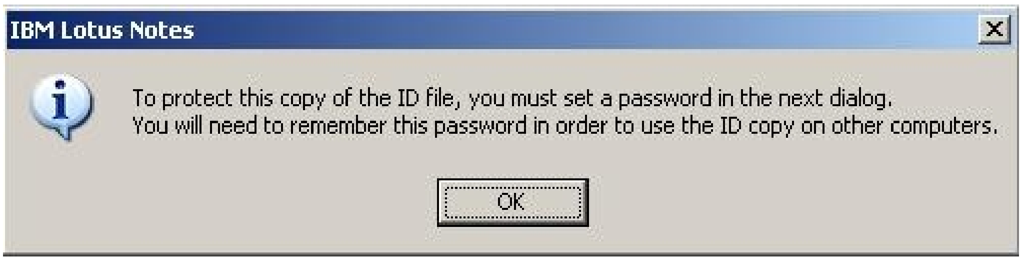
If you think someone has stolen your ID, click 'Compromised ID'

☑ Log in to Notes using your operating system login

This ID file has been backed up into vault /Demo

51. Save the new copy in the same directory as the original ID with the file name **user-newcopy.id**

52.



IBM Lotus Notes

To protect this copy of the ID file, you must set a password in the next dialog.
You will need to remember this password in order to use the ID copy on other computers.

53. Note that you are now prompted to set a password on this new copy to protect it during the transfer to another computer.

54. Click **OK** to close the message dialog

55. Set a password of "**copypassw0rd**" and click **OK**

56. Click **OK** again on the dialog confirming the creation of the password protected ID

57. Click **Close** to close the **User Security Settings** dialog.

58. Because we no longer have a Notes login prompt we don't have the opportunity to select a location on Notes client start-up. To re-instate a prompt we have to switch to a new location and then shut down the Notes client.

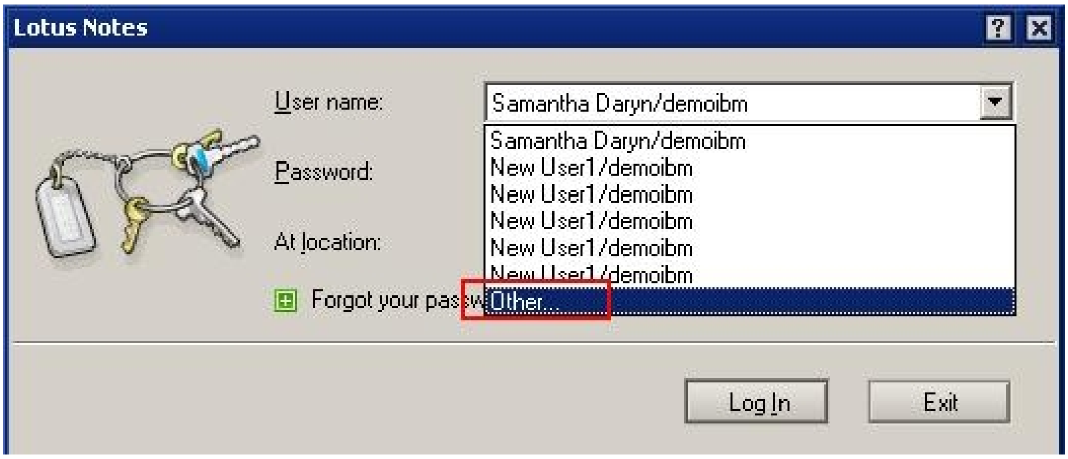
59. Switch to the location **Online – Samantha**

60. Enter "**passw0rd**" as the password and click **Login**.

61. Then close down the Notes client.

62. Restart Notes.

63. Leave the location selected as Online – Samantha but click on the arrow next to the user identity and select "Other"

64. 

65. Navigate to the **C:\Lotus\Notes\Data** directory and select **user-newcopy.id** and click **Open**

66. Enter the password "**copypassw0rd**" and click **Login.** Note that although New User1 won't be directed to the correct mail file when using this location, we won't be using mail in this step and this anomaly should not matter.

67. After a short while you should see the message telling you that Notes Shared Login has been implemented for this new ID copy.

68. Before exiting the Notes client make sure that you switch back to the Online – New User1 location.

Lotus ID Vault implementation

The Notes ID vault is an optional, server-based database that holds protected copies of Notes user IDs. An ID vault allows administrators and users to easily manage Notes user IDs. Users are assigned to a vault through policy configuration, and copies of user IDs are uploaded to a vault automatically once the policy has taken effect. The Notes ID vault has the potential to replace time-consuming, expensive ID file and password recovery systems. Instead of administrators having to send out physical copies of ID files to new users, the ID files can be automatically downloaded from the vault when the user first logs into their Notes client. Administrators can provide instructions in the Notes login window for users who have forgotten their passwords, with either contact details or a link to a self-service password reset application
If ID files are lost or damaged, users are not hindered because copies of the IDs can be immediately downloaded from the vault when users provide the correct passwords. In addition, tasks involving the ID file, such as ID file synchronization, ID renames, and ID key roll-overs, no longer require any user involvement and can automatically be handled by the ID vault, reducing complication and saving time. **The "Auditor" function can be used to extract ID files for legal discovery or access to encrypted data, potentially preventing the loss of valuable information.**

ID Vault creation

Please study your production environment and consider all aspects before Shared login implementation (optionally discuss it with your Lotus Business Partner).

This guide is created in a demo environment, you have to use your own names and passwords.

1. Check that Domino server is up and running.

2. Start the Domino Admin client from the desktop icon.

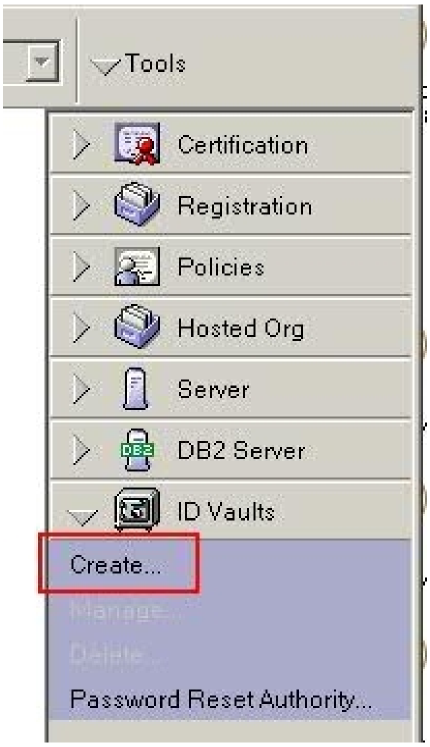
3. Login as sadmin with password passw0rd.

4. Press Cancel when prompted to log on to instant messaging

5. Close the Welcome Screen

6. Switch to the Configuration tab

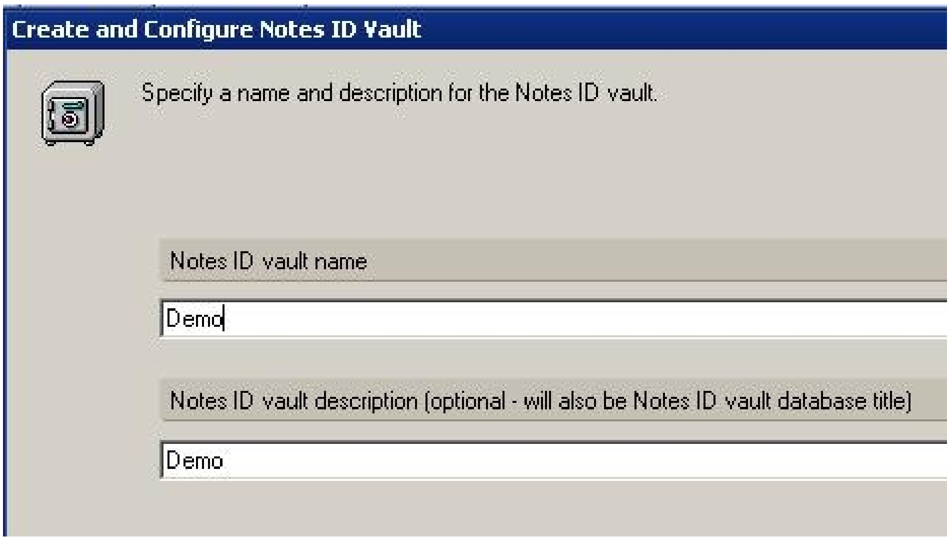
7. Select Create from the ID Vaults section in the Tools navigator



8.

9. Click Next on the Create and Configure Notes ID Vault page

10. Enter “Demo” for the Notes ID Vault name and description and click Next



Create and Configure Notes ID Vault

Specify a name and description for the Notes ID vault.

Notes ID vault name

Demo

Notes ID vault description (optional - will also be Notes ID vault database title)

Demo

11.

12. Enter “passw0rd” as the Vault ID password and click Next

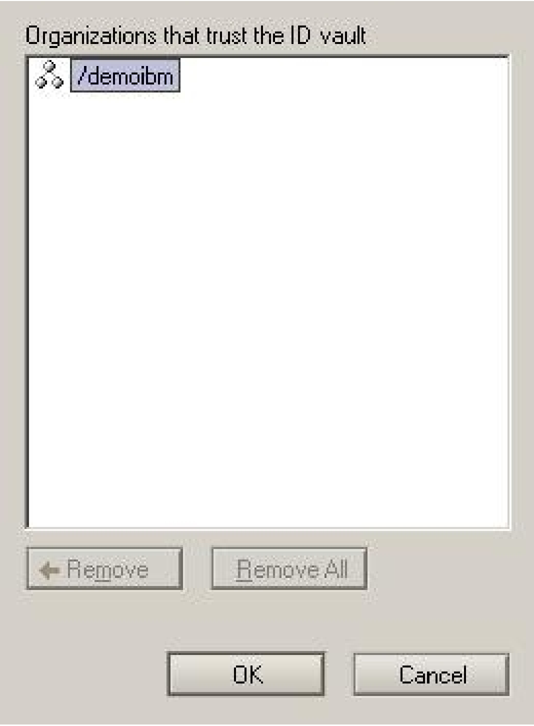
Note

A vault ID will be created in the Notes client data directory location as indicated. This ID will be required for certain vault operations such as creating and removing vault replicas and should be secured in the same way as a certifier ID.

13. Accept Domino85/demoibm as the vault server – this is the server on which the vault will be created - and click "Next"

14. Accept sadmin/demoibm as the vault administrator – this is the person who will have physical access to the vault, will be able to add or remove other vault administrators and delete IDs from the vault - and click Next

15. On the Organizations dialog, click Add or Remove, select /demoibm - only IDs certified with this certifier will be able to be uploaded to the vault - and click Add and then OK and Next

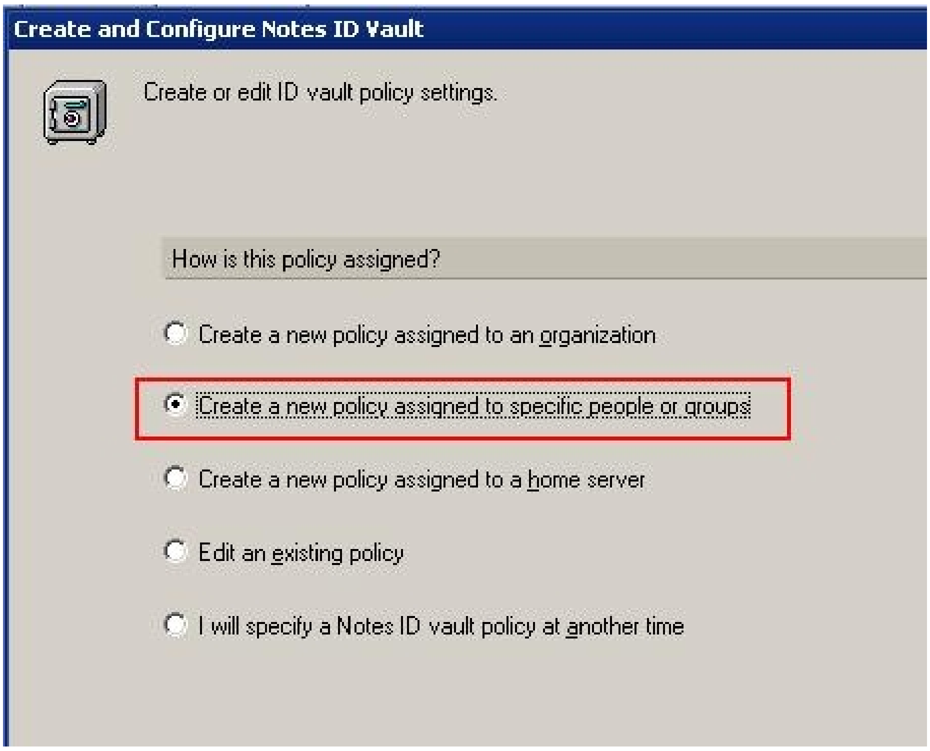
16. 

Organizations that trust the ID vault

/demoibm

17. For the names that are authorized to reset passwords select sadmin and Natalie Olmos and click Add and then Next

18. For the policy assignment, select Create a new policy assigned to specific people or groups and click Next



Create and Configure Notes ID Vault

Create or edit ID vault policy settings.

How is this policy assigned?

○ Create a new policy assigned to an organization

● Create a new policy assigned to specific people or groups

○ Create a new policy assigned to a home server

○ Edit an existing policy

○ I will specify a Notes ID vault policy at another time

19.

20.

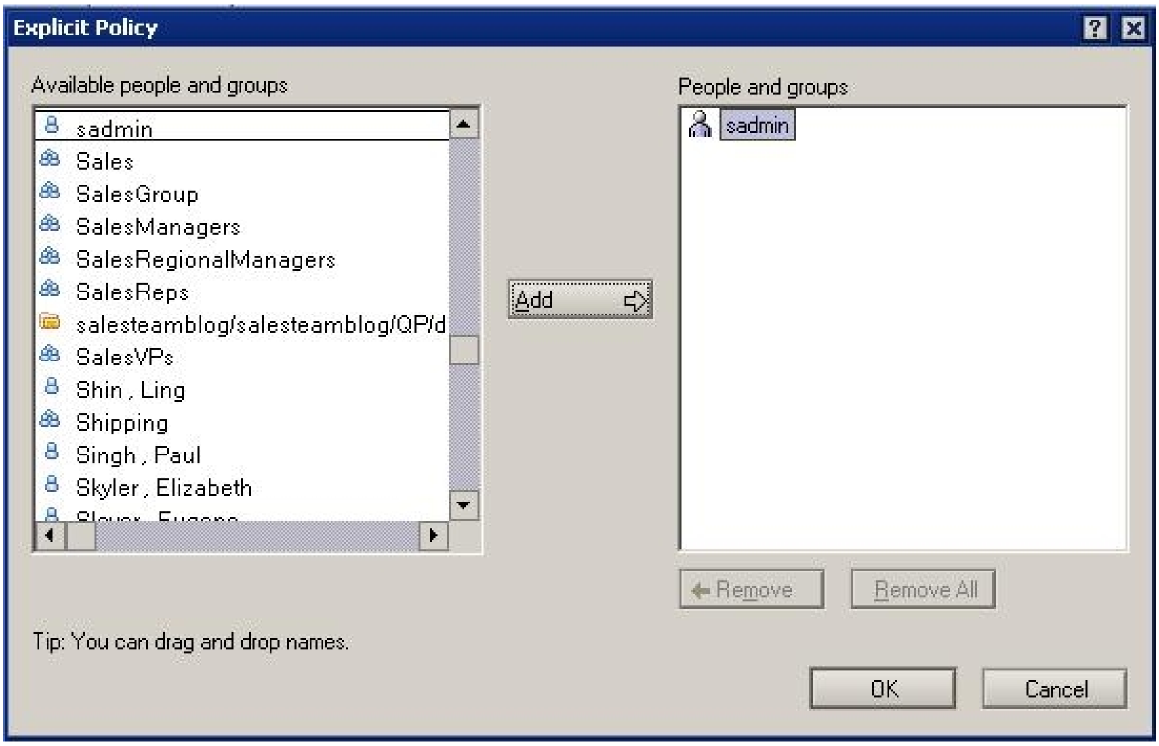
21.

22. Note

23. An efficient way to deploy the ID vault could be to create a new policy assigned to a home server. This will result in an auto-populated group being created which will keep its membership in sync with the set of users whose home server is selected. However, this involves waiting for server background processes to populate the group and to update certain hidden views in the Domino Directory. For the purposes of this lab it is easier if we work with individual users.

24.

25. On the “Select People” screen, click the Add or Remove button and select sadmin, click Add, OK and then Next

26. 

Explicit Policy

Available people and groups

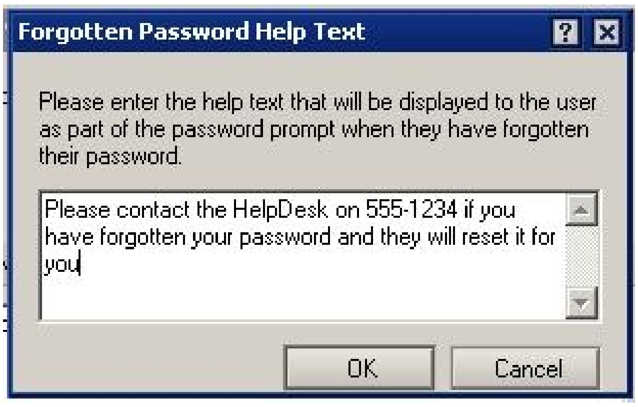
- sadmin
- Sales
- SalesGroup
- SalesManagers
- SalesRegionalManagers
- SalesReps
- salesteamblog/salesteamblog/QP/d
- SalesVPs
- Shin , Ling
- Shipping
- Singh , Paul
- Skyler , Elizabeth

People and groups

- sadmin

Tip: You can drag and drop names.

27. Add some text in the Forgotten Password Help Text dialog and click OK

28. 

Forgotten Password Help Text

Please enter the help text that will be displayed to the user as part of the password prompt when they have forgotten their password.

Please contact the HelpDesk on 555-1234 if you have forgotten your password and they will reset it for you

29. Verify your selections and select Create Vault

30. The vault creation process will begin and you will be prompted to enter the location of the certifier.

31. Click on the Certifier ID button and navigate to C:\Lotus\Notes\Data\IDs\cert\cert.id and click OK

32. When prompted enter “passw0rd” as the password

33. The vault should be created and a summary dialog displayed.

34. Click Done to close the dialogReview end result of ID Vault Creation

35. Switch to the Files tab in the Domino Administrator client

36. Select the IBM_ID_VAULT folder. This view shows the database that has been created to store and manage the Notes Ids

Troubleshooting

If the IBM_ID_VAULT folder is not in the folder list press F9 to refresh the view

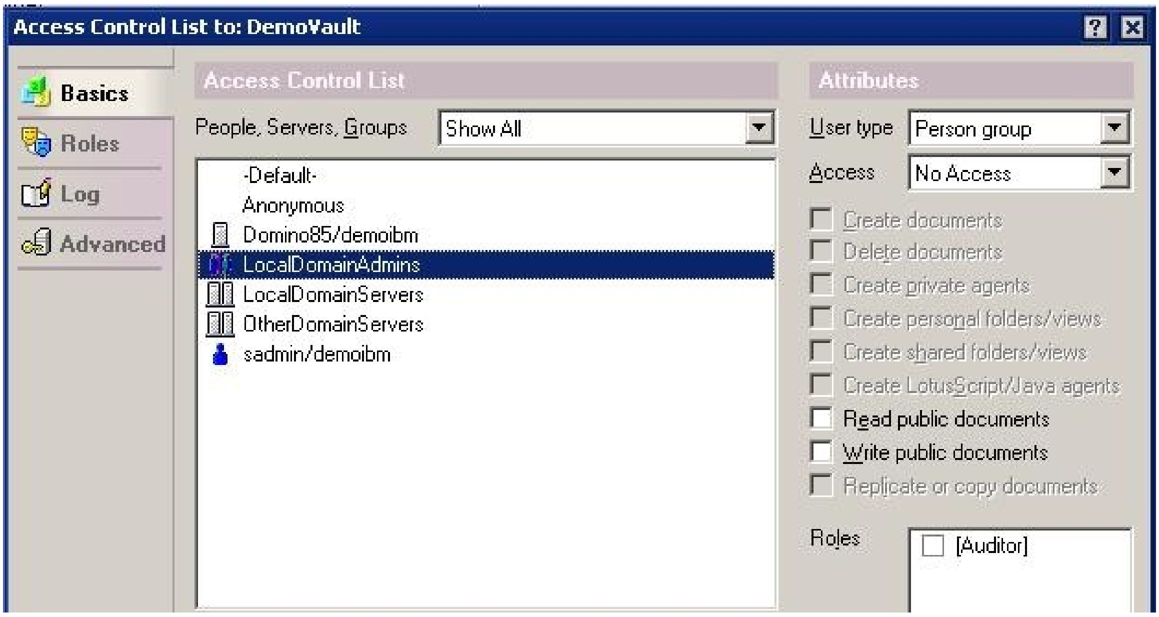
37. Open the Demo database and look at the three views

38. The Vault Users view should be empty – this is because no IDs have yet been uploaded to the vault.

39. The Vault Servers view shows us the single server on which we have deployed the vault. If we were to create replicas of the vault on other servers, those servers would then be listed here.

40. The Inactive User Ids view should also be empty – this view would show us any IDs that were stored in the vault but were no longer in use within our environment – for example those for users who have left the organization.

41. Open the ACL of the vault database. (File menu -> Application -> Access Control)



Access Control List to: DemoVault

Access Control List

People, Servers, Groups: Show All

-Default-
Anonymous
Domino85/demoibm
LocalDomainAdmins
LocalDomainServers
OtherDomainServers
sadmin/demoibm

Attributes

User type: Person group

Access: No Access

☐ 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: ☐ [Auditor]

42. Notice that the only IDs who have any access to the server are the vault administrator and the server on which the vault is deployed. All other entries in the ACL are set to have No Access. Notice also the Auditor role. This has not been assigned to any ID yet. We will be looking at this feature later in the lab so to save having to come back later, we will enable it now.

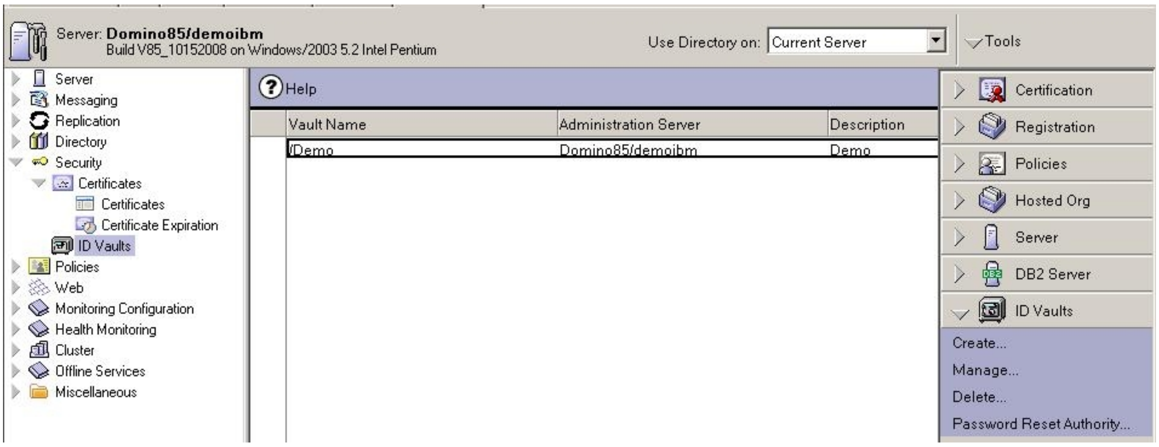
43. Highlight sadmin/demoibm in the ACL and click on the Auditor role.

44. Click on OK and then close the Demo vault database.

45. Switch to the Configuration tab.

46. Expand the Security section of the navigator to see a new section here for ID Vaults.

47. Click on ID Vaults to see the directory entry for the ID Vault that we just created.

48. 

Server: Domino85/demoibm
Build V85_10152008 on Windows/2003 5.2 Intel Pentium

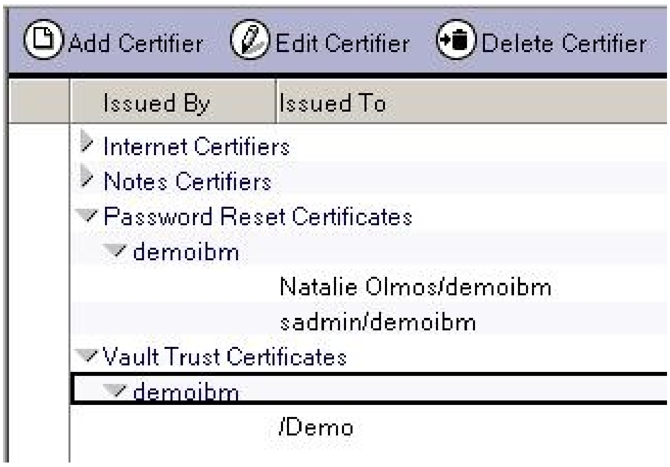
Use Directory on: Current Server

Vault Name	Administration Server	Description
/Demo	Domino85/demoibm	Demo

49. Notice that the ID Vaults Manage and Delete tools now become available in the Tools navigator. The vault administrator can use these tools to amend the configuration of the ID vault or remove it from the domain.

50. Expand the Certificates section and click on the Certificates view. Collapse everything, either with the menu selection, the toolbar button, or the “Shift-” keyboard shortcut.

51. Expand the Password Reset Certificates and Vault Trust Certificates sections.

52. 

Issued By	Issued To
Internet Certifiers	
Notes Certifiers	
Password Reset Certificates	
demoibm	
	Natalie Olmos/demoibm
	sadmin/demoibm
Vault Trust Certificates	
demoibm	
	/Demo

53.

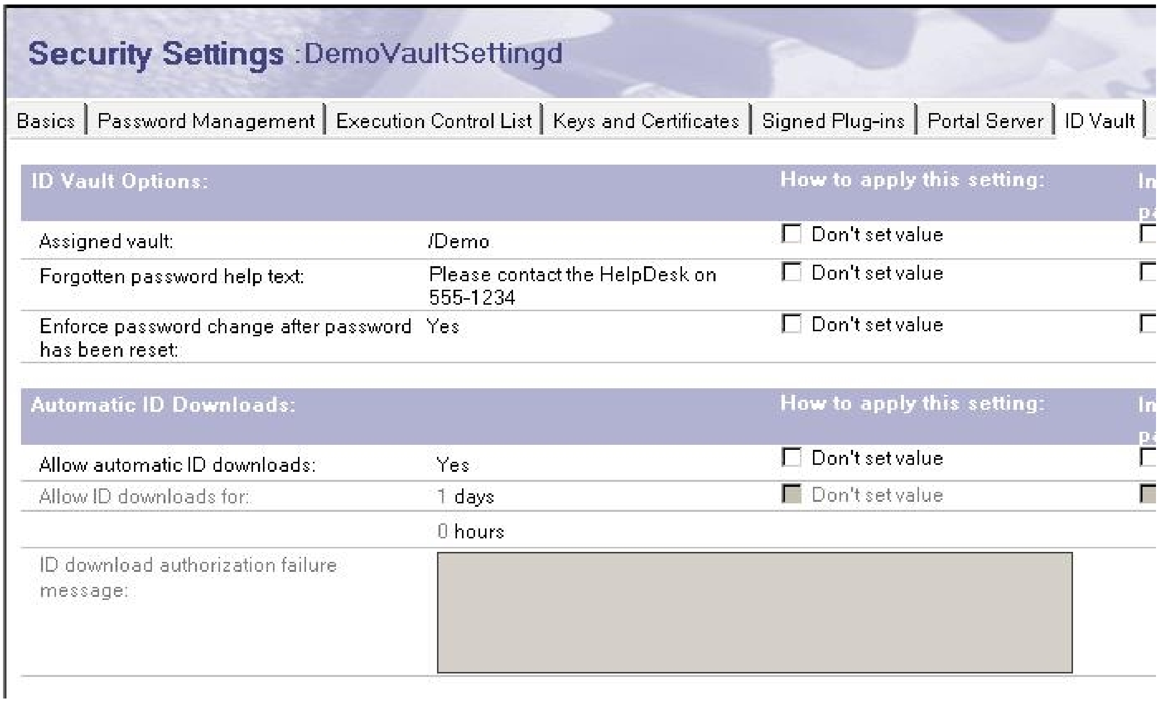
54. These are the certificates that were created during the vault deployment process

55. Notice that there are two password reset certificates – one for Natalie Olmos and one for sadmin. The Password Reset Certificates show that these two users are certified to reset passwords for IDs that have been certified by /demoibm

56. Notice that there is a single vault trust certificate between /demoibm and /Demo. This shows that the Demo vault is certified to store IDs that have been certified by /demoibm

57. Switch to the People & Groups tab, click on Settings in the navigator

58. Open the DemoVaultSetting Security Settings document and click on the ID Vault tab. This is the policy security setting that was created during the Vault deployment process.

59. 

Security Settings :DemoVaultSettingd

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | ID Vault

ID Vault Options:		How to apply this setting:	In p
Assigned vault:	/Demo	□ Don't set value	□
Forgotten password help text:	Please contact the HelpDesk on 555-1234	□ Don't set value	□
Enforce password change after password has been reset:	Yes	□ Don't set value	□

Automatic ID Downloads:		How to apply this setting:	In p
Allow automatic ID downloads:	Yes	□ Don't set value	□
Allow ID downloads for:	1 days	□ Don't set value	□
	0 hours		
ID download authorization failure message:			

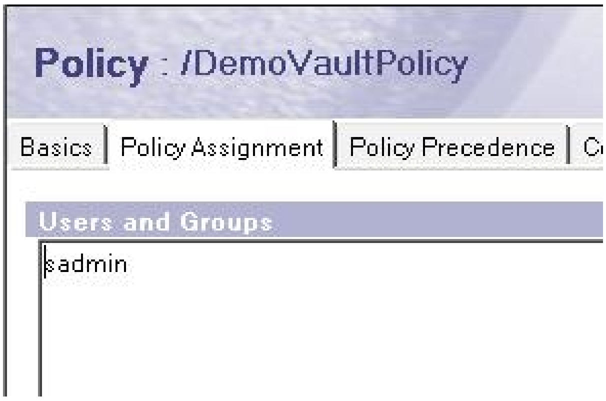
60. Notice that by default “Allow automatic ID downloads” is set to Yes. This means that a user can download the ID as many times as they need after initial registration, a password reset or an ID recovery action. If this field is set to “No”, administrators can restrict the number of times an ID can be downloaded and for how long the ID is available for download. Notice also that, by default, the user will be prompted to change their password after a password has been reset.

61. Close the Settings document.

62. Still in the People & Groups tab, click on Policies in the navigator.

63. Open the DemoVaultPolicy. This is the policy that was created during the Vault deployment - notice that this is set to use the DemoVaultSetting security setting. Notice also the new Policy Assignment tab. In Domino 8.5, users and groups can be assigned to explicit policies (instead of explicit policies being individually assigned to users through the person document).

64. Click on the Policy Assignment tab and you should see the entry for sadmin.

65. 

Policy : /DemoVaultPolicy

Users and Groups

sadmin

66.

67. Process for existing user

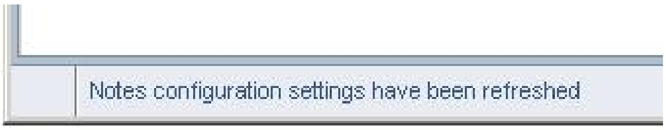
68. To break out the information into a third-level heading and subsection, use this format. This workshop template uses a Step List style with underscore to provide a checklist appearance.

69. Close down any Notes or Domino Administrator client that you currently have open.

70. Launch the Notes 8.5 client and select Online – Admin as the location.

71. Enter the password “passw0rd” and click Login

72. Watch the status bar and you should see the message indicating that the Notes configuration has been refreshed.

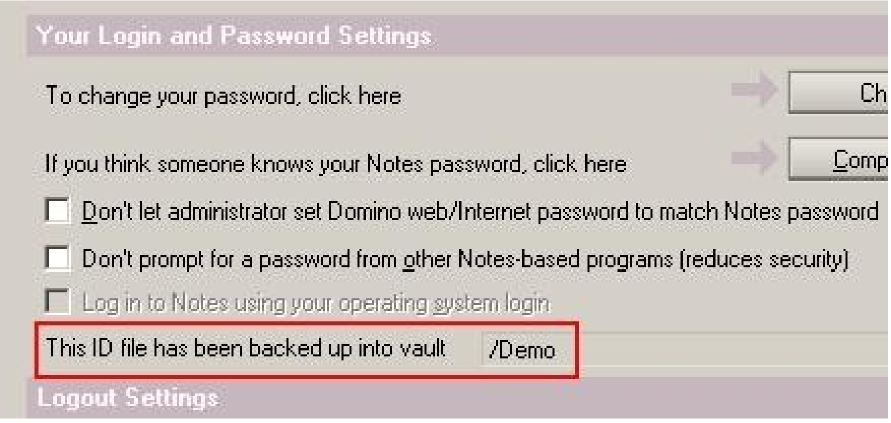
73. 

Notes configuration settings have been refreshed

74. Select File > Security > User Security from the menu

75. Enter the password “passw0rd” again

76. In the Your Login and Password Settings section you should see the message indicating that the ID has been backed up into the vault.

77. 

Your Login and Password Settings

To change your password, click here

If you think someone knows your Notes password, click here

☐ Don't let administrator set Domino web/Internet password to match Notes password

☐ Don't prompt for a password from other Notes-based programs (reduces security)

☐ Log in to Notes using your operating system login

This ID file has been backed up into vault /Demo

Logout Settings

Troubleshooting

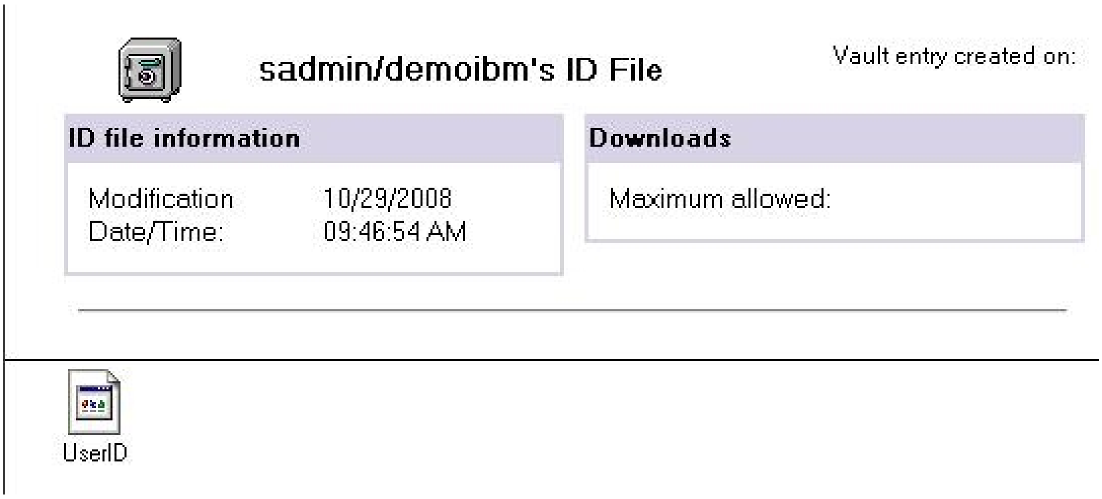
It may take some time for the policy to be invoked. During that time, the field highlighted above will be not appear. If this happens, try manually forcing the policy. To do so, open the Domino Directory on Domino85/demoibm then open the person document for “sadmin” and put it into edit mode. On the Administration tab, go to the “Assigned policy” field and enter /DemoVaultPolicy. Save and close the person document then restart the Notes client, and try the steps again. If that doesn't work, just wait a while. Proceed with the lab section “Process for new users”, and check back on this step later. Notes may not upload the ID file immediately.

78. Click OK to close the dialog and launch the Domino Administrator client from the Open menu

79. From the Files tab, select the IBM_ID_VAULT folder and open the Demo database.

80. You should see a single record in the Vault Users view indicating that sadmin's ID has been uploaded into the vault.

81. Open the record to see the entry along with the encrypted ID file.



sadmin/demoibm's ID File

Vault entry created on:

ID file information

Modification Date/Time: 10/29/2008 09:46:54 AM

Downloads

Maximum allowed:

UserID

Note

Although you could save a copy of the attached file in this document it could not be used as a Notes ID file. The only way to extract a working ID file from the vault is to use the Domino Administrator tools.

82. Process for new users

83. For supporting sections, use this format. Replace the heading above with your own title, and then add an introduction. If you need to add steps, copy and paste the step list below.

84. Make sure that you are logged into the Domino Administrator with the sadmin ID and switch to the Configuration tab

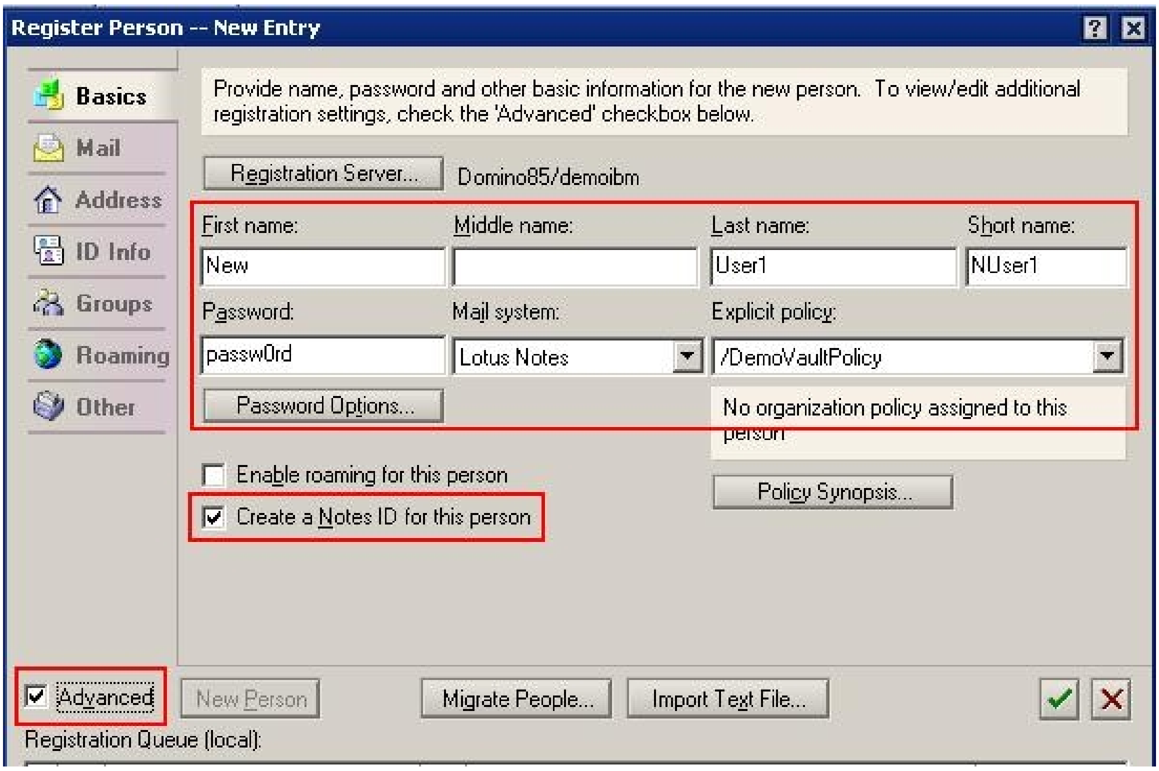
85. Select Registration > Person from the Tools menu

86. You should be prompted for the password for the /demoibm certifier. Enter “passw0rd” as the password and click OK

87. Enter the details for a new user as follows:

First Name	New
Last Name	User1
Password	passw0rd
Explicit Policy	/DemoVaultPolicy
Create Notes ID for this person	Checked

88. Check the Advanced checkbox so that the other options are displayed.

89. 

Register Person -- New Entry

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

Registration Server... Domino85/demoibm

First name: New

Middle name:

Last name: User1

Short name: NUser1

Password: passw0rd

Mail system: Lotus Notes

Explicit policy: /DemoVaultPolicy

No organization policy assigned to this person

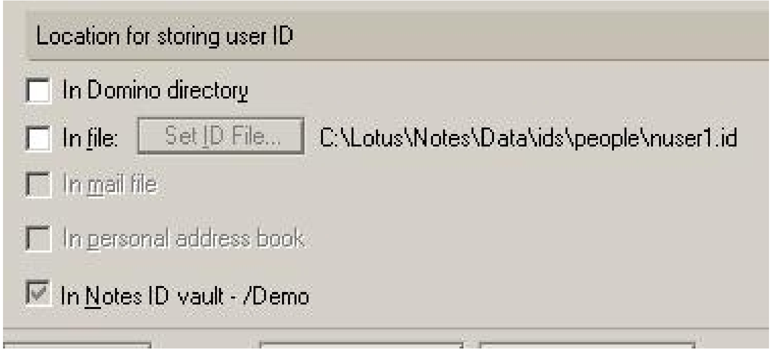
□ Enable roaming for this person

☑ Create a Notes ID for this person

☑ Advanced

Registration Queue (local):

90. Click on the ID Info tab and make sure that “In Domino Directory” and “In file” are not checked as locations for storing the user ID.

91. 

Location for storing user ID

□ In Domino directory

□ In file: Set ID File... C:\Lotus\Notes\Data\ids\people\nuser1.id

□ In mail file

□ In personal address book

☑ In Notes ID vault - /Demo

92. Notice that, as a result of selecting the DemoVault policy, the location “In Notes ID vault” has been automatically selected and cannot be deselected.

93. Click the green tick in the bottom right corner to add New User1 to the registration queue.

94. Return to the Basics tab and perform the same steps to create a second user “New User2”

95. Select Register All to register the users and create the mail files and Notes IDs

96. Click OK to the “People registered successfully prompt” and then Done to close the dialog box.

97. Switch to the Files tab and open the Demo Vault again (IBM_ID_VAULT\demo.nsf). You should see the new entries for New User1 and New User2 with their encrypted IDs attached. Your admin ID might be here by now. If it is, go back up and complete that step, then come back here.

98. In order to see what happens when a new client is configured, we will need to simulate a new client installation. Close down any Notes or Administrator client that you currently have open.

99. Double-click on the Domino85 Computer icon on the desktop and navigate to the C:\Lotus\Notes directory.

100. Locate the notes.ini file and open it with notepad.

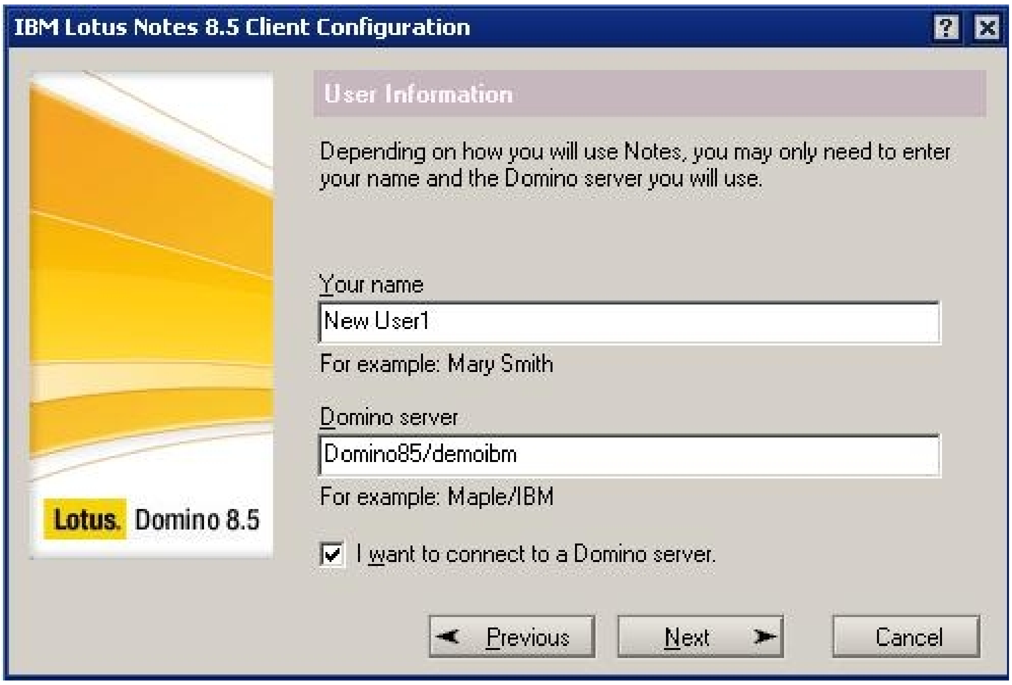
101. Delete all the lines below InstallType=2 but make sure that you leave the cursor on the line below the last line of text when you save the document.

102. Then navigate to the C:\Lotus\Notes\Data directory and rename the names.nsf file to names-old.nsf – Don't delete the original file as we will re-instate this later.

103. Start the Lotus Notes client and you will see the Lotus Notes 8.5 Client Configuration dialog you would expect if you were starting an unconfigured client for the first time.

104. Click Next on the first page

105. Enter “New User1” for Your name and “Domino85/demoibm” for the Domino server and click Next

106. 

IBM Lotus Notes 8.5 Client Configuration

User Information

Depending on how you will use Notes, you may only need to enter your name and the Domino server you will use.

Your name: New User1

For example: Mary Smith

Domino server: Domino85/demoibm

For example: Maple/IBM

☑ I want to connect to a Domino server.

107. You should then be prompted for the user's password. Since the ID file has not been saved anywhere except in the ID vault, the configuration process must be communicating with the ID vault.

108. Enter “passw0rd” for the password and click Login

109. Click Next on the Additional Services dialog and the client should start up.

110. Select File > Security > User Security from the menu and enter the password again and you should see the dialog indicating that you are using an ID that has been backed up into the vault.

111. Re-instate original NAMES.NSF

112. Before we go any further we will re-instate the original NAMES.NSF as this contains location documents for our users which match their user IDs with their mail files and ensure that, as we switch user identities, we pick up all the correct user settings.

113. Close down any Notes or Domino Administrator client that you currently have open.

114. Double-click on the Domino85 Computer icon on the desktop and navigate to the C:\Lotus\Notes\Data directory

115. Rename the names.nsf file to names-new.nsf

116. Rename names-old.nsf to names.nsf

117. Restart the Notes client

118. Select Online – Admin location document.

119. Enter password “passw0rd”

120. We will create a new location document for New User1 to make it easy to switch to the appropriate Notes settings.

121. Select File > Preferences from the menu

122. Click on Locations

123. Highlight the Online-Admin location and click Copy

124. Edit the copied location document

125. On the Basics tab, change the location name to “Online – New User1”

126. On the Basics tab, change the Internet mail address to “nuser1@demoibm.com”

127. On the Mail tab, change the mail file to “mail\nuser1.nsf”

128. On the Advanced tab, change the user ID to “C:\Lotus\Notes\Data\user.id”

129. Click OK to save the changes

130. Switch to the Online - New User1 location and log in to test it.

131. User forgets password

132. In this step we will review what happens when a user forgets their password. For the purposes of this exercise we will imagine that New User1 has forgotten their password and rings the HelpDesk to get the password reset. Remember that we gave Natalie Olmos the rights to reset passwords during the vault creation process. In this step Natalie, will reset the password for New User1

133. Close down any Notes and Domino administrator client that you currently have open.

134. Start Lotus Notes and select Online – New User as the location.

135. Click on the “Forgot your password” link.

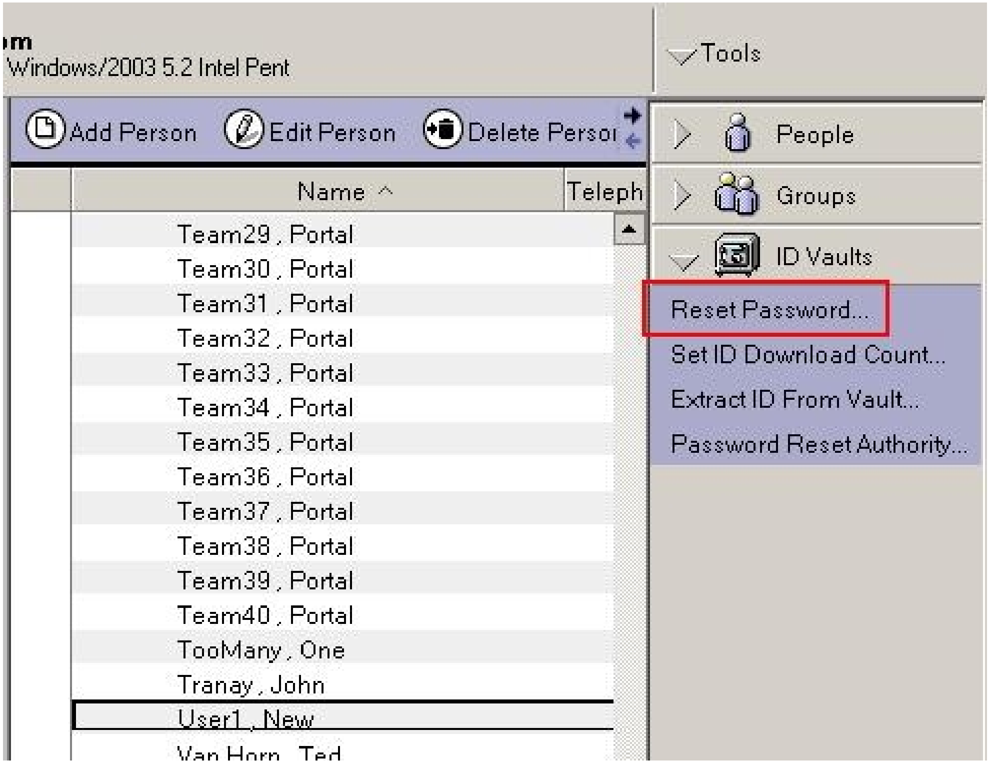
136. Notice that the text shown is the text we entered as the help text during the vault configuration process.

137. Switch to the Online – Natalie location and login with password “passw0rd”

138. Open the Domino Administrator client from the Open menu

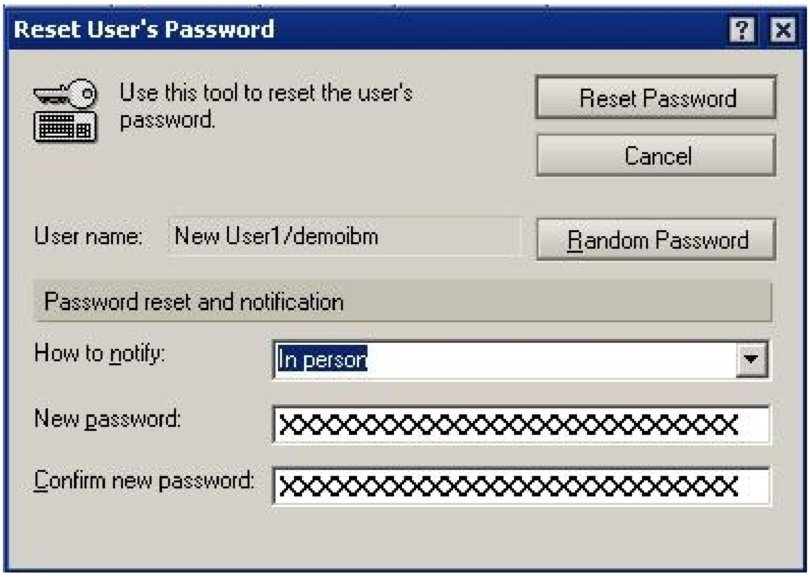
139. Close the Welcome page

140. Click on the People & Groups tab and then the People viewNavigate to New User1's person document and with the document highlighted in the view select ID Vaults > Reset Password from the Tools navigator on the right side of the screen.

141. 

Name
Team29 , Portal
Team30 , Portal
Team31 , Portal
Team32 , Portal
Team33 , Portal
Team34 , Portal
Team35 , Portal
Team36 , Portal
Team37 , Portal
Team38 , Portal
Team39 , Portal
Team40 , Portal
TooMany , One
Tranay , John
User1 , New
Van Horn , Ted

142. In the Reset User's Password dialog, enter a new password eg: “resetPassw0rd1” and click the Reset Password button.

143. 

Use this tool to reset the user's password.

User name: New User1/demoibm

Password reset and notification

How to notify: In person

New password: XXXXXXXXXXXXXXXXXXXXXXXXXXX

Confirm new password: XXXXXXXXXXXXXXXXXXXXXXXXXXX

144. When you receive a message indicating that the password has been successfully reset, click OK.

145. Close the Domino Administrator client and the Notes client.

146. Now let's login as New User1 again. Launch the Notes client and select the Online – New User1 location.

147. Enter the new password “resetPassw0rd1”. As specified in the policy, because the password has been reset, you are now prompted to change the password to one of your own choosing.

148. Change the password back to “passw0rd”

149. User changes password

150. In this step we will review what happens when a user changes their password on one copy of their ID. First we will create a separate copy of New User1's ID to simulate the use of the Notes client on a second computer. Then we will change the password on one copy of the ID and observe what happens when we switch to the other copy of the ID.

151. Close down any Notes or Domino Administrator client that you currently have open.

152. Double-click on the Domino85 Computer icon on the desktop and navigate to the C:\Lotus\Notes\Data directory

153. Locate the file user.id

154. Create a copy of the file and name it user1.id

155. Start the Lotus Notes 8.5 client

156. Select the Online – New User1 location

157. Enter the password “passw0rd” and click Login

158. Select File > Security > User Security from the menu and enter the password again.

159. Click on the Change Password button.

160. Enter the current password again (“passw0rd”) and click Login

161. Enter a new password – eg: “newpassw0rd” and click OK

162. Click OK on the “Your password change succeeded” dialog and click OK to close the User Security dialog. As part of the password change process, the changed password information has been synchronized with the ID vault record.

163. Select File > Security > Switch ID

164. Navigate to C:\Lotus\Notes\Data select user1.id and click Open

165. Enter “newpassw0rd” as the password and click Login. Notice that you are able to login with your

new password even though you did not change the password on this copy of the ID file.

166. Select File > Security > Switch ID again and switch back to the original user.id file.

167. ID becomes corrupted or lost

168. In this step we will review how recovery from a corrupted ID can be achieved. In the case of corruption, the affected user ID would need to be deleted from the data directory so that a new ID could be downloaded.

169. Shut down any Notes or Domino Administrator clients that are currently open.

170. Double-click on the Domino85 Computer icon on the desktop and navigate to the C:\Lotus\Notes\Data directory and delete any user ID files – user.id, user1.id, user-old.id, that are here. Do NOT delete any ID files that are in subdirectories of the Data directory.

171. Restart the Notes client

172. Select the Online – New User1 location and enter “newpassw0rd” as the password.

173. Even though there was no user ID present you were seamlessly logged into Notes because the correct password was entered allowing a new copy of the ID to be downloaded to your client from the vault.

174. Check the C:\Lotus\Notes\Data directory and you will see a new copy of the user ID has been created.

175. Auditor feature

176. In this step we will review how an auditor can be configured to get access to a user's ID without their co-operation or knowledge. In order to perform this, a user must both be a vault administrator and have the Auditor role configured in the ACL. When we were reviewing the ID Vault configuration, we assigned the Auditor role to sadmin. In this step we will use sadmin's ID to download a copy of New User1's ID and use it to login to Notes where sadmin would then be able to access any data encrypted by or for New User1. To show this we will first send some encrypted mail to New User1.

177. From the bottom right corner of the client, select the Online – Natalie location.

178. Enter “passw0rd” as the password and click Login

179. Open Natalie's mail file from the Open menu

180. Select New Mail and complete as follows

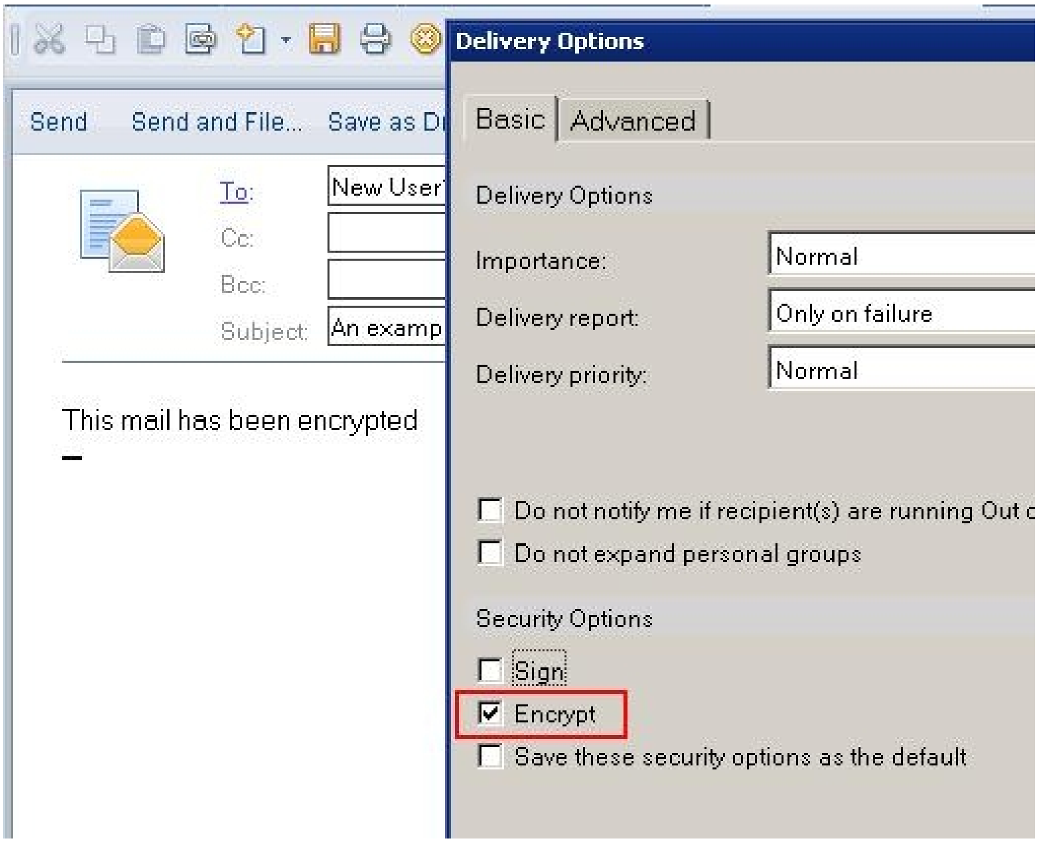
181. Enter “New User1” in the To: field

182. Enter “An example of encrypted mail” as the Subject

183. Enter “This mail has been encrypted”

184. Click on “Delivery Options” in the Action bar, check the Encrypt check box under Security Options and click OK.

185.



To: New User

Cc:

Bcc:

Subject: An examp

This mail has been encrypted

Delivery Options

Importance: Normal

Delivery report: Only on failure

Delivery priority: Normal

□ Do not notify me if recipient(s) are running Out o

□ Do not expand personal groups

Security Options

□ Sign

☑ Encrypt

□ Save these security options as the default

186. Send the email.

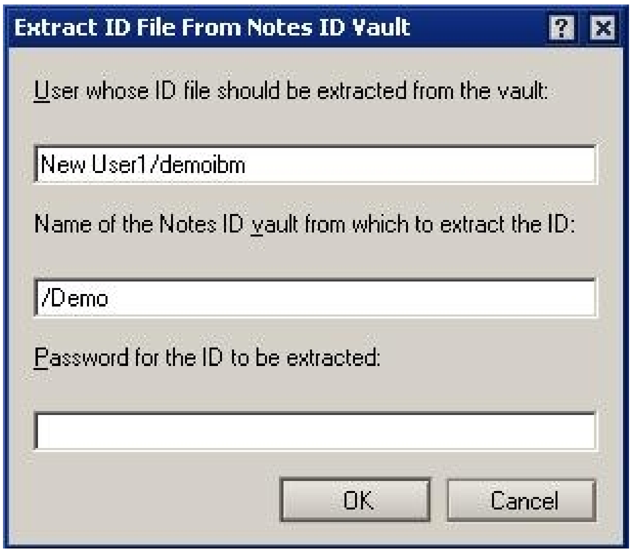
187. From the bottom right corner of the client, select the Online – Admin location and enter the password “passw0rd”

188. Open the Domino Administrator client from the Open menu.

189. Switch to the People & Groups tab and click on the People view.

190. Highlight the person entry for New User1

191. From the Tools navigator, select Extract ID from Vault from the ID Vaults section.

192. 

Extract ID File From Notes ID Vault

User whose ID file should be extracted from the vault:

New User1/demoibm

Name of the Notes ID vault from which to extract the ID:

/Demo

Password for the ID to be extracted:

193. If the ID was being extracted so that a physical copy can be given to the user, and the vault administrator performing the task did not have the Auditor role, the current password for the ID would have to be supplied here. This means that either the user would have to have given the administrator the current password or the administrator would have had to have reset the password to something that he/she would then know. In either of these cases, the user would be aware an activity had been performed against their ID.

194. As sadmin has the Auditor role, a password does not need to be supplied in this dialog.

195. Click OK without supplying a password.

196. Enter user-audit.id as the file name and click Save

197. The administrator is then prompted to supply a new password for the new ID copy.

198.

199. ℹ

200. Note

201. This password is for this copy of the ID only and does not affect the copy in the vault and therefore no copy in use by the user.

202.

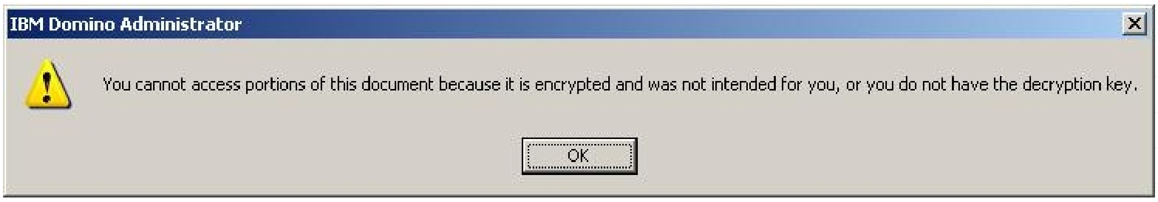
203. Enter a new password of “auditpassw0rd” and click OK

204. First let's prove that although the administrator has access to New User1's mail file (LocalDomainAdmins have Manager access to all mail files) the ID is not able to read the encrypted mail that was sent from Natalie.

205. Switch to the Files tab

206. Open the file mail\nuser1.nsf

207. Open the email sent from Natalie.

208. 

IBM Domino Administrator

You cannot access portions of this document because it is encrypted and was not intended for you, or you do not have the decryption key.

209. You should see the message indicating that the document is encrypted and not intended for you.

210. Click OK. Notice that the email opens but you are not able to read the contents.

211. Close New User1's mail file

212. Close the Domino Administrator client.

213. Select File > Security > Switch ID from the menu

214. Navigate to the C:\Lotus\Notes\Data directory and select user-audit.id

215. Enter the password “auditpassw0rd”

216. Select File > Open > Lotus Notes Application

217. Select Domino85/demoibm as the server

218. Navigate to the New User1 mail file in the mail directory.

219. Open the mail file and the encrypted document. Note that you can now see the contents of the mail message.

220. Select the Online – New User1 location.

221. Login with New User1's password “newpassw0rd” and notice that this is still valid and does not require changing.

222. If you open New User1's mail file you will notice that the encrypted mail message now shows as having been read. In a real audit scenario, it is more likely that a copy of the required application would be made so that any action by the auditor would not be visible to the users.

223. User leaves the organization

224. In this step we will show what can happen in the situation where a user leaves the organization but their ID needs to be securely retained for audit or information retrieval purposes. We need to use our New User1 identity in the next exercise so in this step we will remove the account of New User2.

225. Switch to the Online – Admin location.

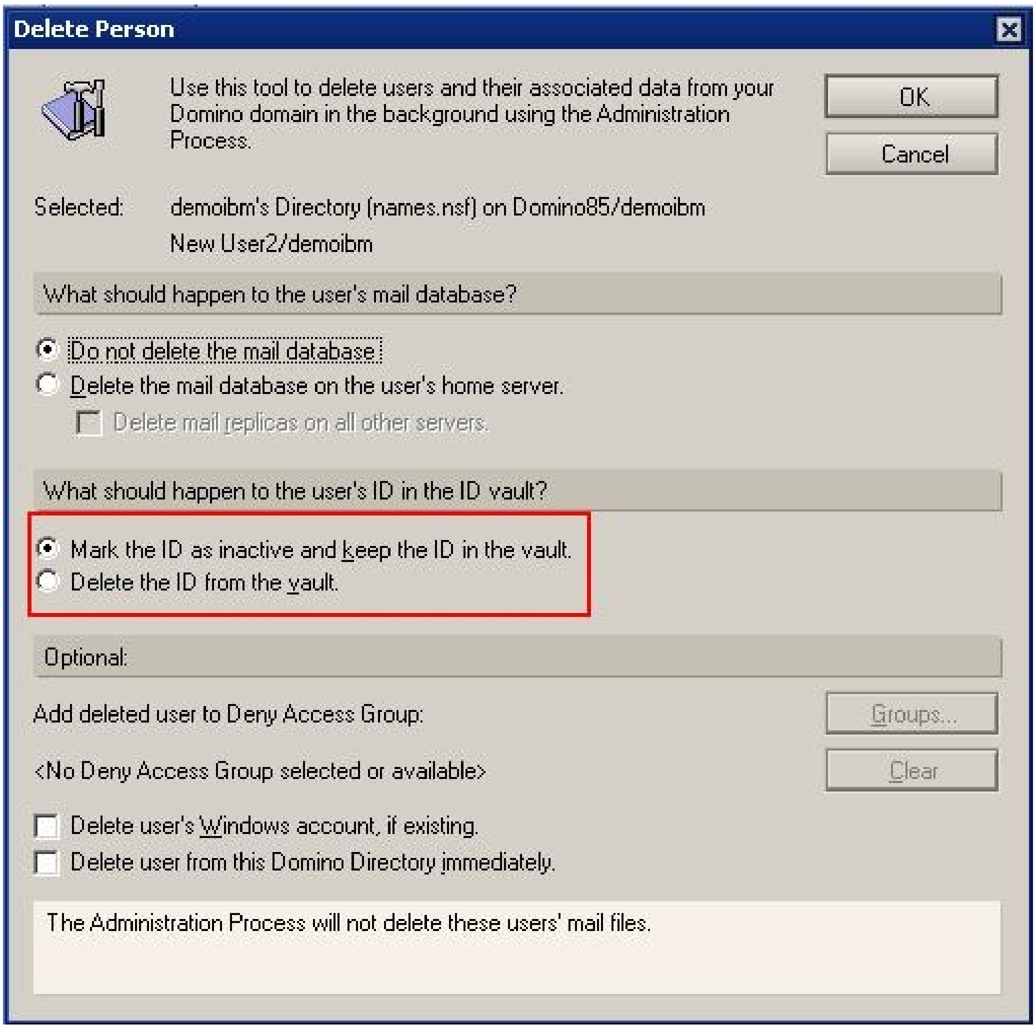
226. Open the Domino Administrator client.

227. Select the People & Groups tab and then the People view

228. Locate New User2's person record

229. From the Tools navigator, select Delete from the People section.

230.



Delete Person

Use this tool to delete users and their associated data from your Domino domain in the background using the Administration Process.

Selected: demoibm's Directory (names.nsf) on Domino85/demoibm
New User2/demoibm

What should happen to the user's mail database?

● Do not delete the mail database
○ Delete the mail database on the user's home server.
□ Delete mail replicas on all other servers.

What should happen to the user's ID in the ID vault?

● Mark the ID as inactive and keep the ID in the vault.
○ Delete the ID from the vault.

Optional:

Add deleted user to Deny Access Group:

<No Deny Access Group selected or available>

□ Delete user's Windows account, if existing.
□ Delete user from this Domino Directory immediately.

The Administration Process will not delete these users' mail files.

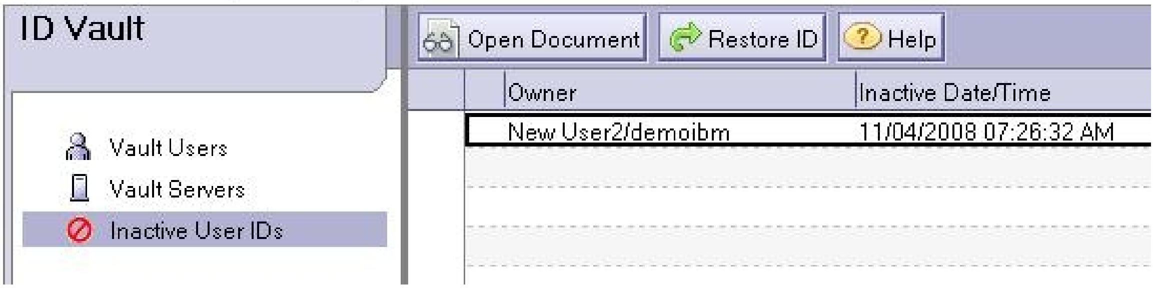
231.

232. Note the option to mark the ID as inactive but keep in the vault.

233. Leave all the settings as default and click OK.

234. Switch to the Files tab and open the Demo vault database. Notice that the New User2's record is no longer in the Vault Users view.

235. Click on the Inactive User IDs view and you should see the New User1's ID record.

236. 

Owner	Inactive Date/Time
New User2/demoibm	11/04/2008 07:26:32 AM

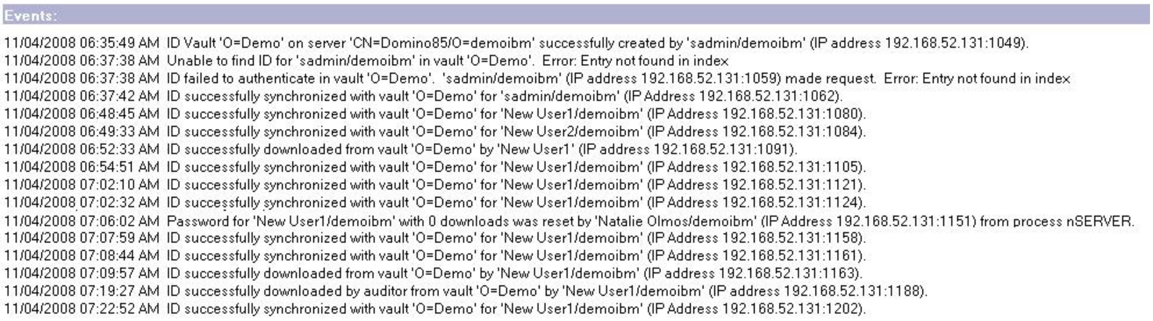
237. Audit trails and logs

238. In this step we look at how the various actions on the vault and the IDs within it are recorded.

239. Switch to the Files tab and open Domino85's log (log.nsf)

240. Click on the Security Events view

241. Open the document(s) in this view

242. 

```
Events:
11/04/2008 06:35:49 AM  ID Vault 'O=Demo' on server 'CN=Domino85/O=demoibm' successfully created by 'sadmin/demoibm' (IP address 192.168.52.131:1049).
11/04/2008 06:37:38 AM  Unable to find ID for 'sadmin/demoibm' in vault 'O=Demo'.  Error: Entry not found in index
11/04/2008 06:37:38 AM  ID failed to authenticate in vault 'O=Demo'.  'sadmin/demoibm' (IP address 192.168.52.131:1059) made request.  Error: Entry not found in index
11/04/2008 06:37:42 AM  ID successfully synchronized with vault 'O=Demo' for 'sadmin/demoibm' (IP Address 192.168.52.131:1062).
11/04/2008 06:48:45 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1080).
11/04/2008 06:49:33 AM  ID successfully synchronized with vault 'O=Demo' for 'New User2/demoibm' (IP Address 192.168.52.131:1084).
11/04/2008 06:52:33 AM  ID successfully downloaded from vault 'O=Demo' by 'New User1' (IP address 192.168.52.131:1091).
11/04/2008 06:54:51 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1105).
11/04/2008 07:02:10 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1121).
11/04/2008 07:02:32 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1124).
11/04/2008 07:06:02 AM  Password for 'New User1/demoibm' with 0 downloads was reset by 'Natalie Olmos/demoibm' (IP Address 192.168.52.131:1151) from process nSERVER.
11/04/2008 07:07:59 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1158).
11/04/2008 07:08:44 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1161).
11/04/2008 07:09:57 AM  ID successfully downloaded from vault 'O=Demo' by 'New User1/demoibm' (IP address 192.168.52.131:1163).
11/04/2008 07:19:27 AM  ID successfully downloaded by auditor from vault 'O=Demo' by 'New User1/demoibm' (IP address 192.168.52.131:1188).
11/04/2008 07:22:52 AM  ID successfully synchronized with vault 'O=Demo' for 'New User1/demoibm' (IP Address 192.168.52.131:1202).
```

243. You should be able to see all the key vault associated activities including

244. Vault Creation

245. Upload of ID to the vault (note that this activity is not well recorded yet – where you see an “Unable to find ID... Error: Entry not found in index” message directly before an “ID successfully synchronized with vault” message for the same user, this is an indication that the ID has been uploaded. Log entries for this activity will be improved in the next release.)

246. Download of ID from the vault

247. Password change (recorded as ID synchronization)

248. Password reset

249. Auditor download of ID from the vault