

# What's ID Vault & Why you can't live without it

Gabriella Davis  
The Turtle Partnership  
[gabriella@turtlepartnership.com](mailto:gabriella@turtlepartnership.com)



# Agenda

- ID Vault - What It Is
- Creating an ID Vault
- Managing ID Vault
- Resetting Passwords
- Setting up a security policy for ID Vault
- Auto processing requests
- A bit more about how it works and limitations

# First The Why

- ID Vault removes the pain from
  - Password Recovery
    - by allowing password resets without access to the id itself
  - Lost ids
    - by re-distributing the vault copy
  - Users with multiple id copies (we know you're out there)
    - by keeping multiple copies in sync
  - User renames
  - Re-issuing the keys
    - by doing both without needing any user involvement

# So...

- It makes you happy because you can keep your environment secure and not wait on users to complete your work
- It makes users happy because they have one sync'd id and can easily get a password reset
- It makes audit happy because you no longer have that backup directory of id files "just in case"



# How Does It Work - Downloading IDs

- If no ID exists on the workstation the notes.ini fields keyfilename and keyfilename\_owner are used to identify which ID should be downloaded
- The ID can only be downloaded if the user knows the password for the ID stored in the Vault
  - So you can't hack a notes.ini file to steal someone's ID unless you already know their password

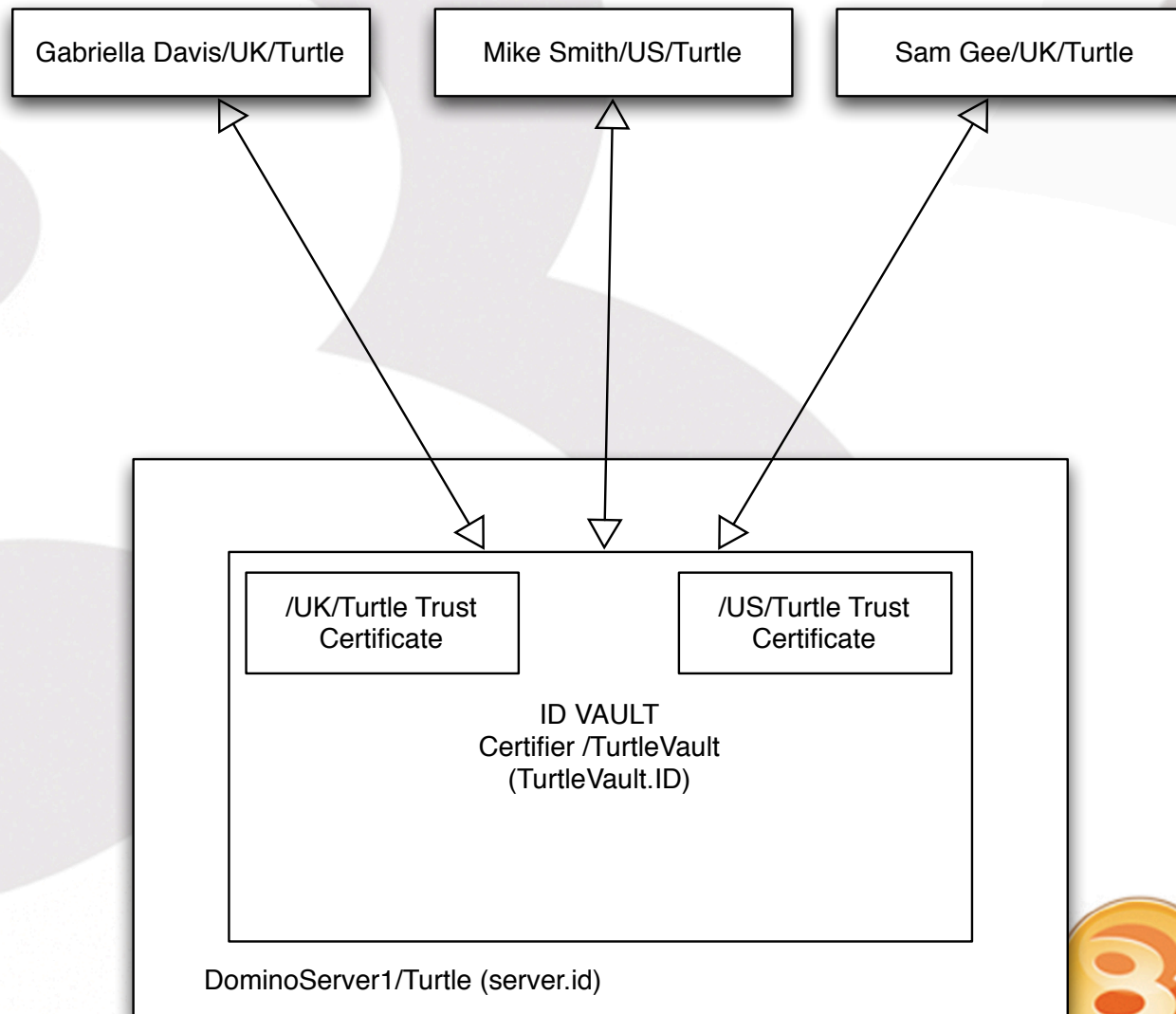


# How Does It Work - Updating IDs

- When a user connects to their home server the client asks for a list of servers containing a vault that matches their security policy
  - the server chosen from the list is random and is then cached for a few sessions so think about where you are placing your ID Vaults
- If a change is made in the vault (such as a password reset) that is downloaded to the client as they login
- If a change is made on the client version of the id then it is uploaded to the randomised ID Vault server

# How Secure Is It

ORGANISATIONAL POLICY \*/TURTLE



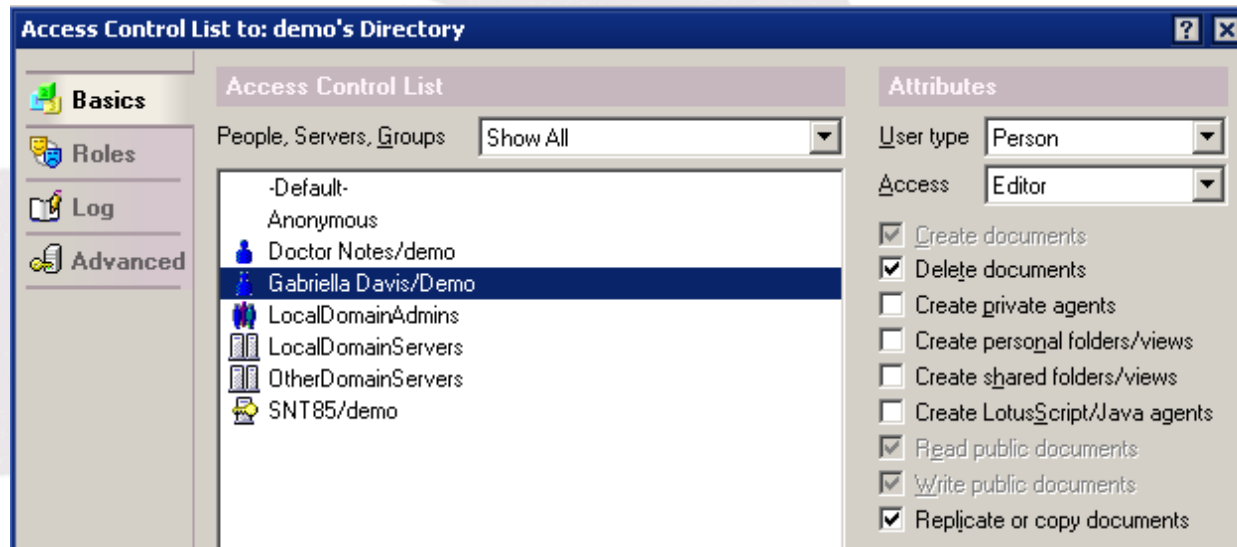
**BLUG**  
Belux Lotus User Group

# Let's jump right in & create an ID Vault

- Verify you have the access required to create the Vault on the server(s) you are using
- Create the Vault
- Check that everything created correctly

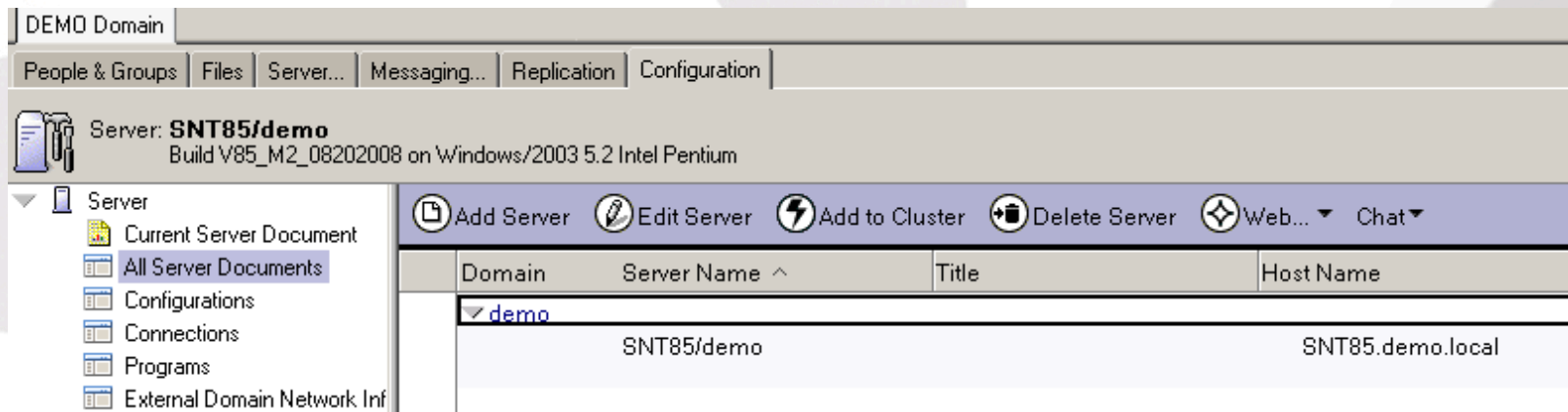


# Editor Access to the Domino Directory



- Go to 'People and Groups' tab
- File- Application - Access Control
- Ensure you or your group membership has Editor access (no specific roles)

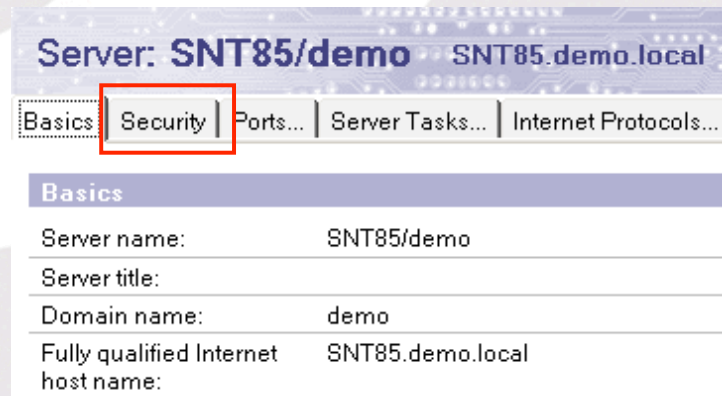
# What rights do you need to create an ID Vault?



- Rights to create databases and templates
  - Click on Configuration Tab
  - Select and Open Server Document

# Rights to create databases & templates

- Click on Server document 'Security Tab'



# Rights to create databases & templates

- Ensure your name or group is entered in the fields for
  - Create new databases and templates

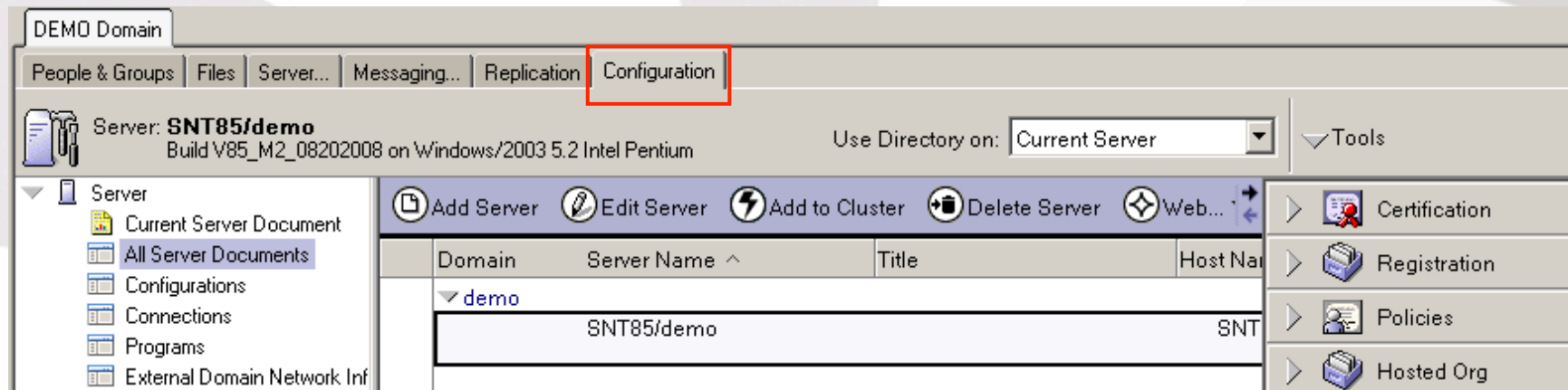
Server Access	Who can -
Access server:	All users can access this server
Not access server:	
Create databases & templates:	LocalDomainAdmins
Create new replicas:	
Create master templates:	
Allowed to use monitors:	*
Not allowed to use monitors:	
Trusted servers:	



# You may have to wait...

- If you modified the server document then it will cache
  - give it up to 30 mins or exit and start the server
    - don't do 'server restart'

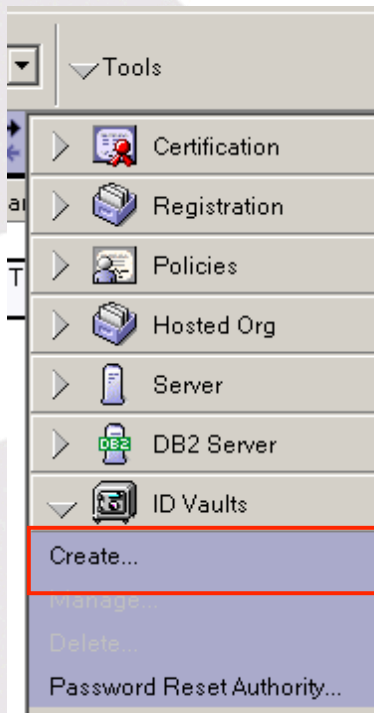
# Creating the ID Vault



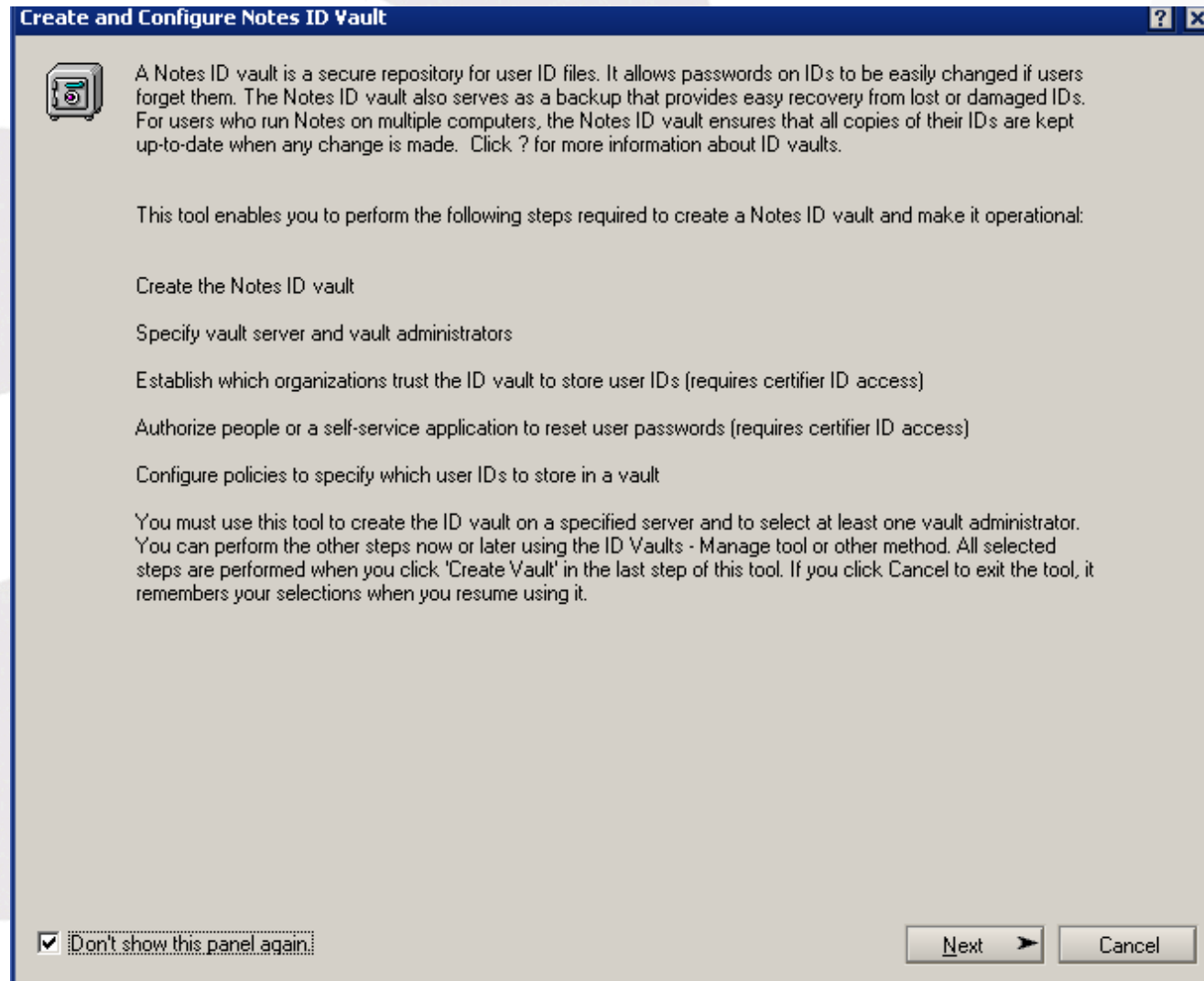
- Launch Domino Administrator
- Click the Configuration Tab

# Creating the ID Vault

- Select from right hand 'Tools' menu – or top "Configuration" menu
- Tools - ID Vaults - Create



# Creating the ID Vault





# Add a name & description for this vault instance

**Create and Configure Notes ID Vault**

Specify a name and description for the Notes ID vault.

Notes ID vault name  
DemoVault

Notes ID vault description (optional - will also be Notes ID vault database title)  
The primary vault for the demo certifier and related OUs

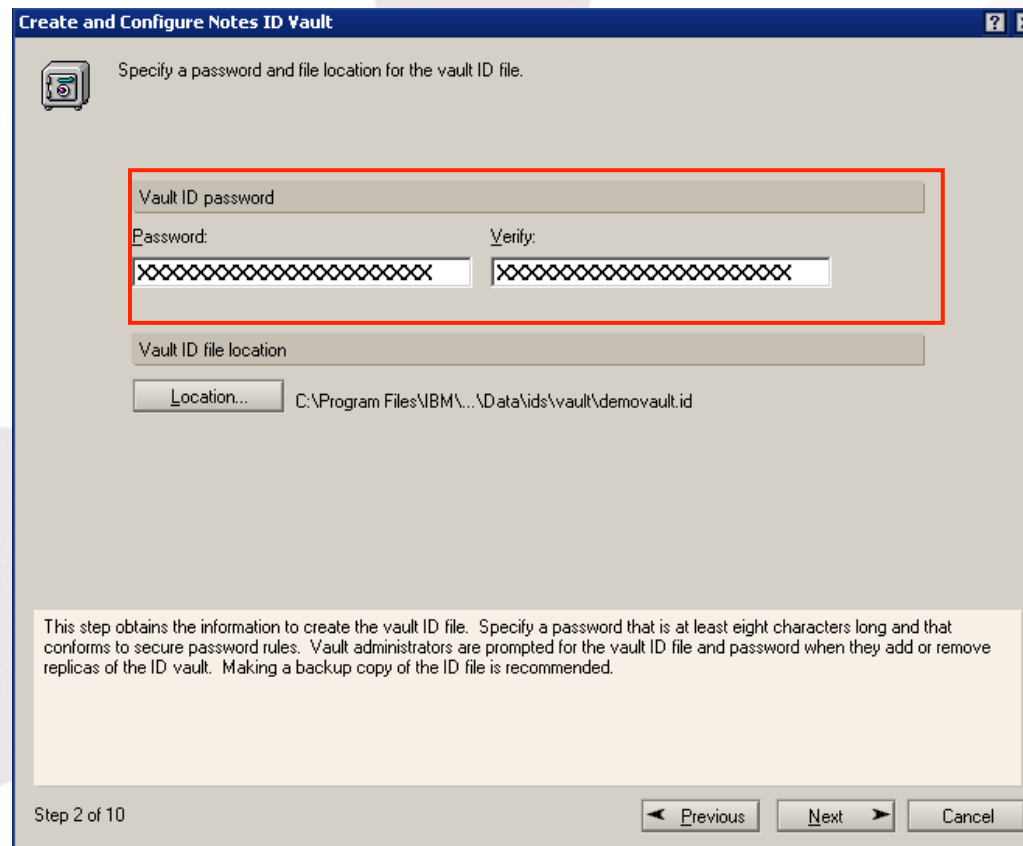
The name you specify is used to form the hierarchical name, the database file name and the ID file name for the Notes ID vault. The name can not be the same as any organization or organizational unit. Example: 'ACMEVault' results in the hierarchical vault name '/ACMEVault', the vault database file name 'acmevault.nsf' and the vault ID file 'acmevault.id'. Once the Notes ID vault is created in the last step of this tool, you cannot change its name.

Step 1 of 10

Next > Cancel

# Setting a password for the ID Vault

- An ID vault id is created automatically
  - the password you set must be used when Administrators attempt to create or delete replicas of the ID Vault itself



**Create and Configure Notes ID Vault**

Specify a password and file location for the vault ID file.

Vault ID password

Password:  Verify:

Vault ID file location

Location... C:\Program Files\IBM\...\Data\ids\vault\demovault.id

This step obtains the information to create the vault ID file. Specify a password that is at least eight characters long and that conforms to secure password rules. Vault administrators are prompted for the vault ID file and password when they add or remove replicas of the ID vault. Making a backup copy of the ID file is recommended.

Step 2 of 10

Previous Next Cancel

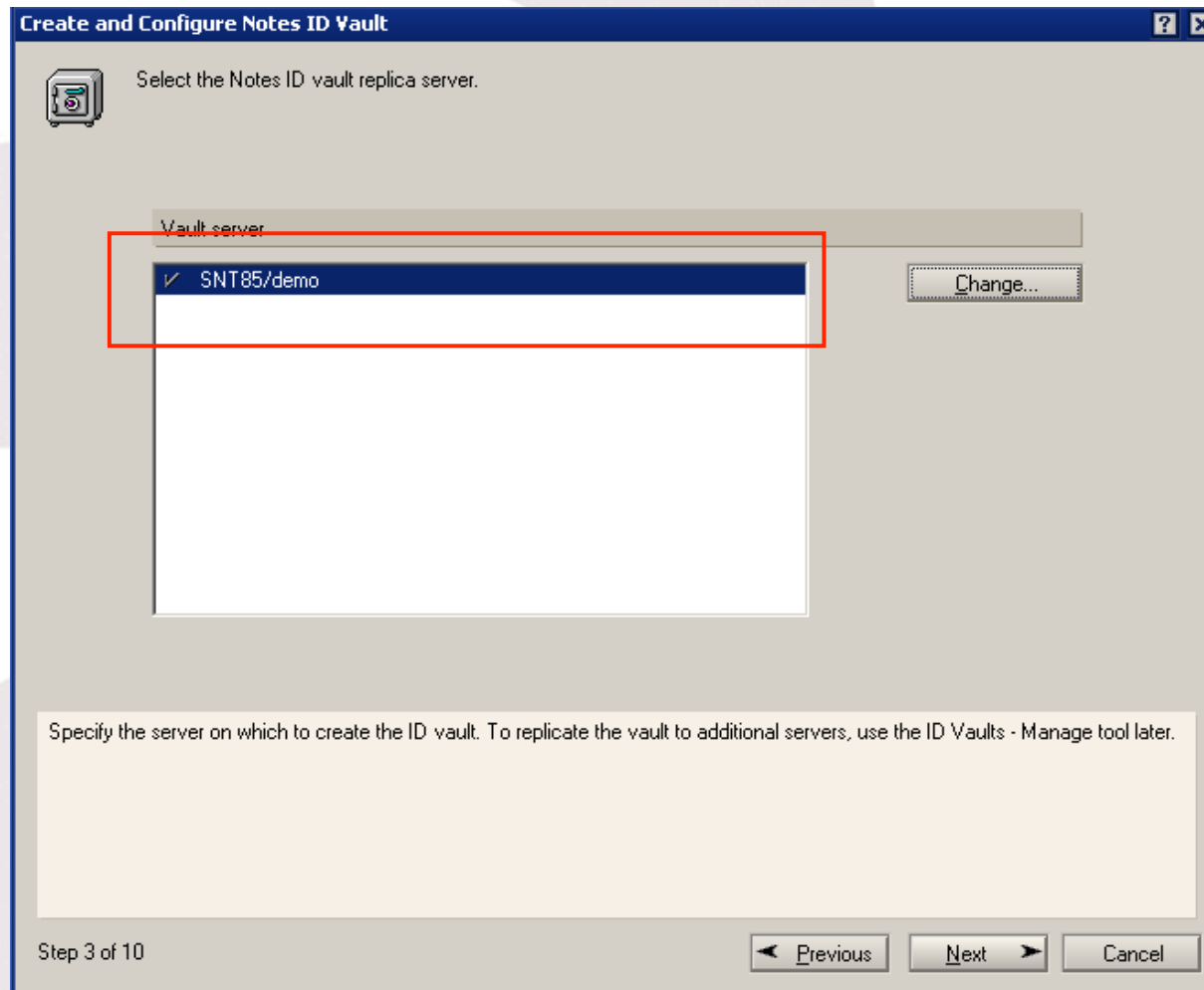
- Backup the vault id once it's created and any time you change its password

- The Vault ID and Server ID for the ID Vault server are the 2 keys to keeping your vault and the ids in it secure



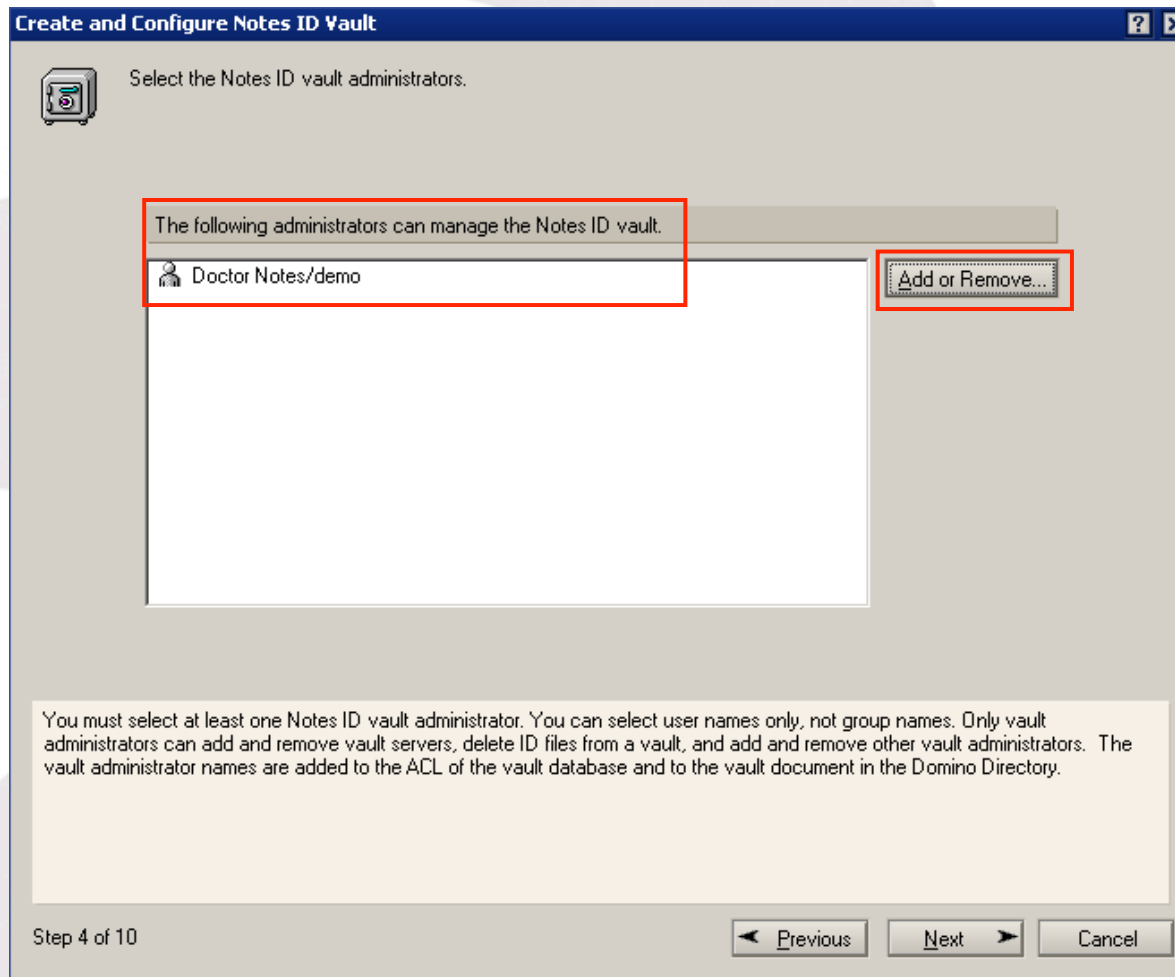
- Keep both your server and server id secure by password protecting the server id itself.

# Choosing the ID Vault Replica Server



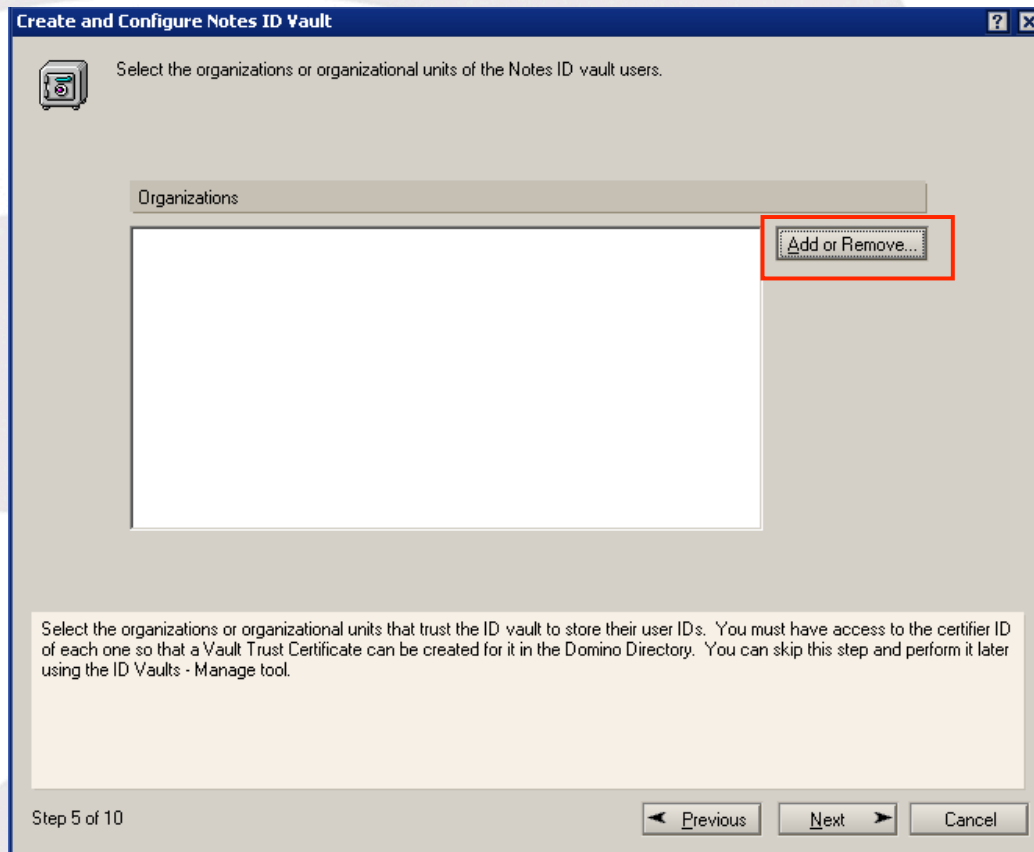
- You can specify only one server on initial creation but add others later<sup>22</sup>

# Setting up ID Vault Administrators



- Your name is automatically added as an administrator
- You can add other administrators and recovery authorities later

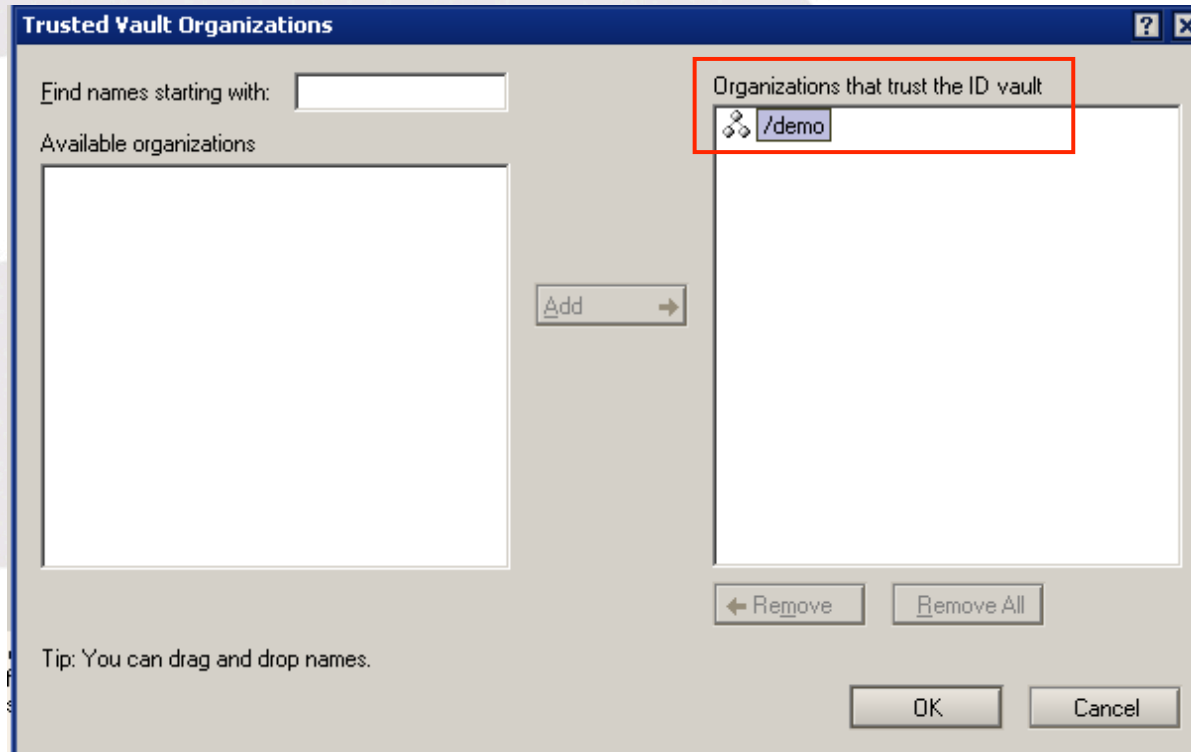
# Adding organisations to the ID Vault



- A trust certificate is created between the organisation and the ID vault
- You must use a physical certifier not the CA process to do this



# Selecting certifiers to add



- Later on in the process I will be prompted to point to the physical certifier
  - The list of certifiers authorised for this ID Vault can be modified later
  - You can only store IDs in the ID Vault if their parent certificate is also there

# Users Authorised to Reset Passwords

**Create and Configure Notes ID Vault**

Specify names that are authorized to reset passwords.

Directory: demo's Directory

Available users, groups and servers

- Lotus Notes/Domino Fault Rep
- Lotus Notes/Domino Smart Up
- Mooney, Paul
- Notes, Doctor
- OtherDomainServers
- SNT85/demo

Available organizational units

Password reset authority by organization

- /demo
  - Doctor Notes/demo
  - Gabriella Davis/demo
  - Paul Mooney/demo
  - SNT85/demo**
  - Warren Elsmore/demo

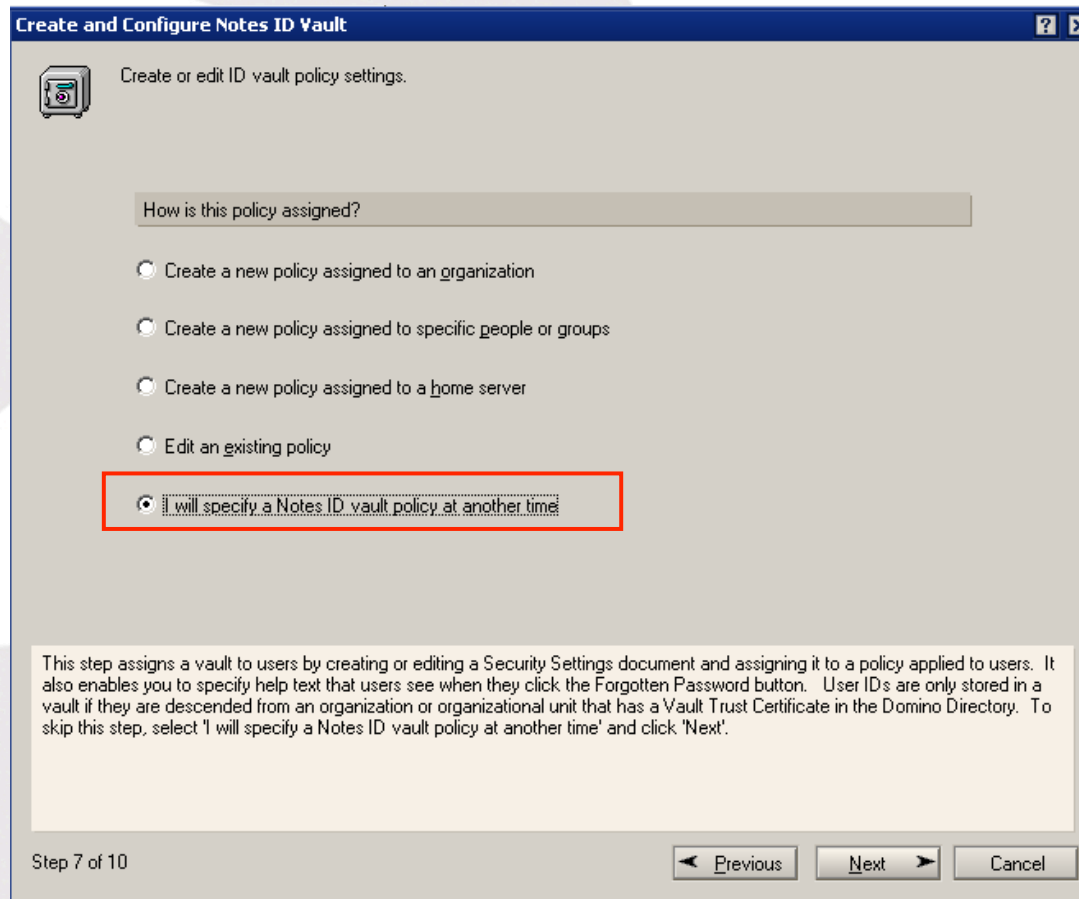
☐ Self-service password reset authority.

On the left, select the name of a user, group, server, or organizational unit to authorize to reset passwords. On the right, add the selected name to each user organization or organizational unit it will reset passwords for. Repeat to give password reset authority to additional names. A Password Reset Certificate will be created for each authorized user, group member, server, and organizational unit. To allow users to reset their own passwords using an agent, select 'Self-service password reset authority' for the user name that signs the agent and for each server on which the agent will run. For more information on password reset authority, including authorizing a non-agent self-service application, click ?

Step 6 of 10

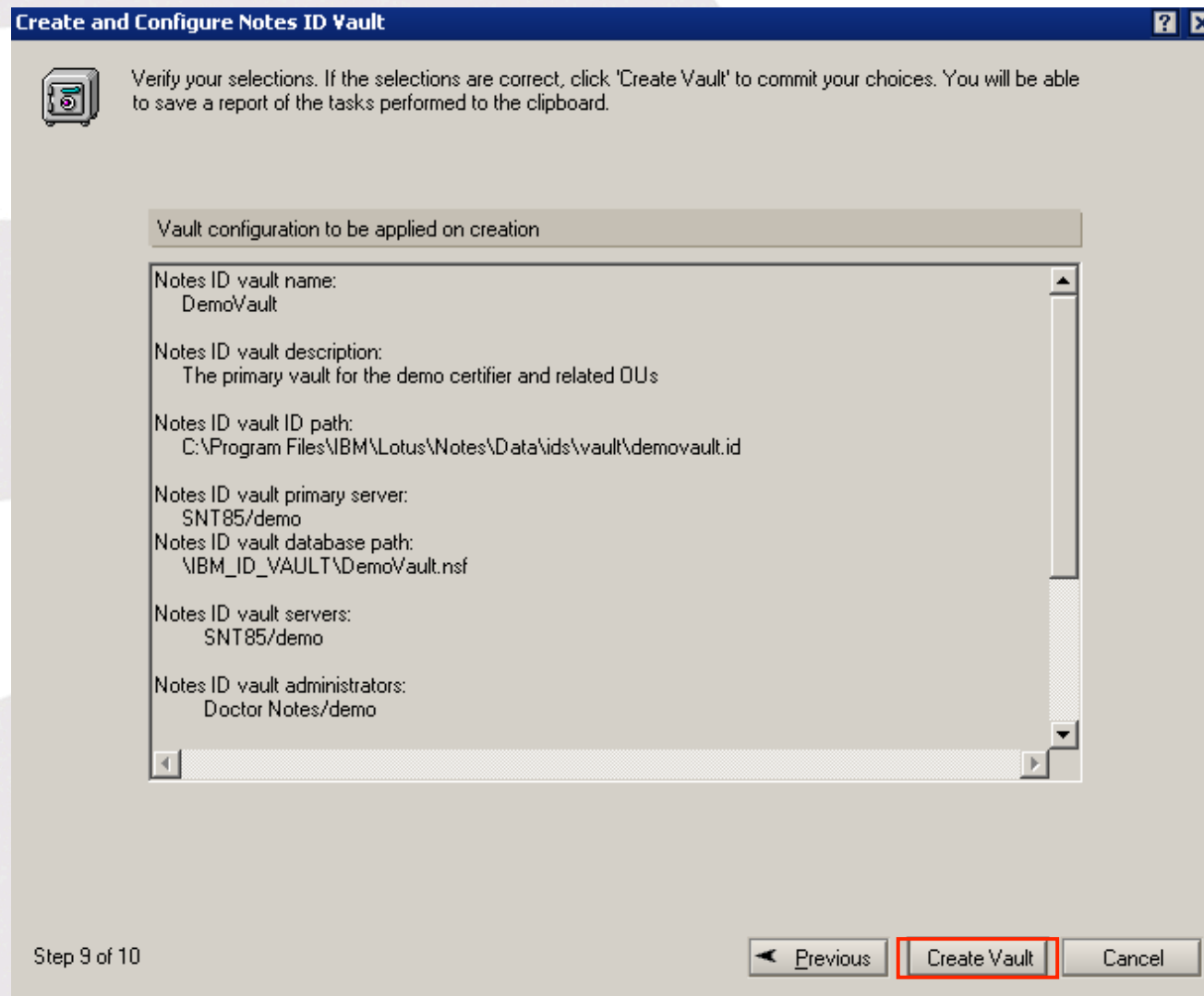
Previous Next Cancel

# Applying an ID Vault To A User



- ID Vault relationships are set up in user policies
  - You can configure or edit a security policy when you create the ID Vault. Or later.

# Summary of ID Vault Settings

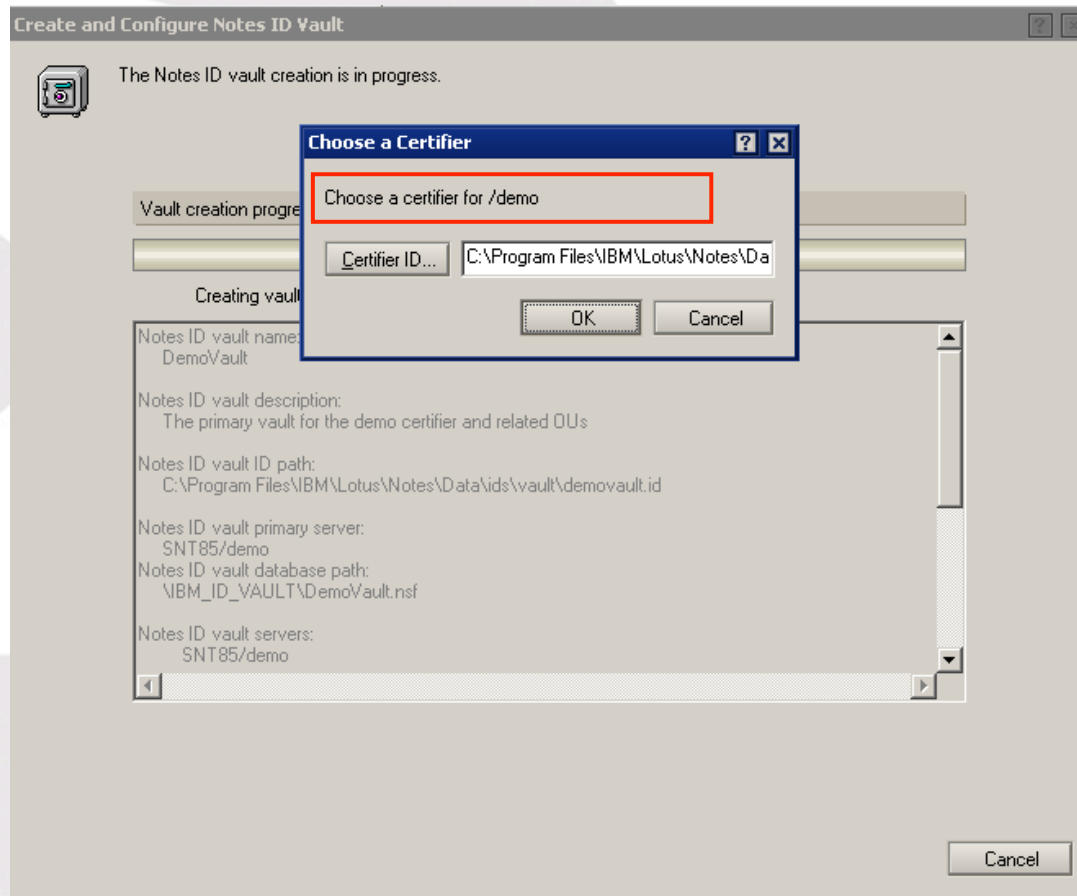


- Click 'Create Vault' on the summary screen to complete the<sup>28</sup> process



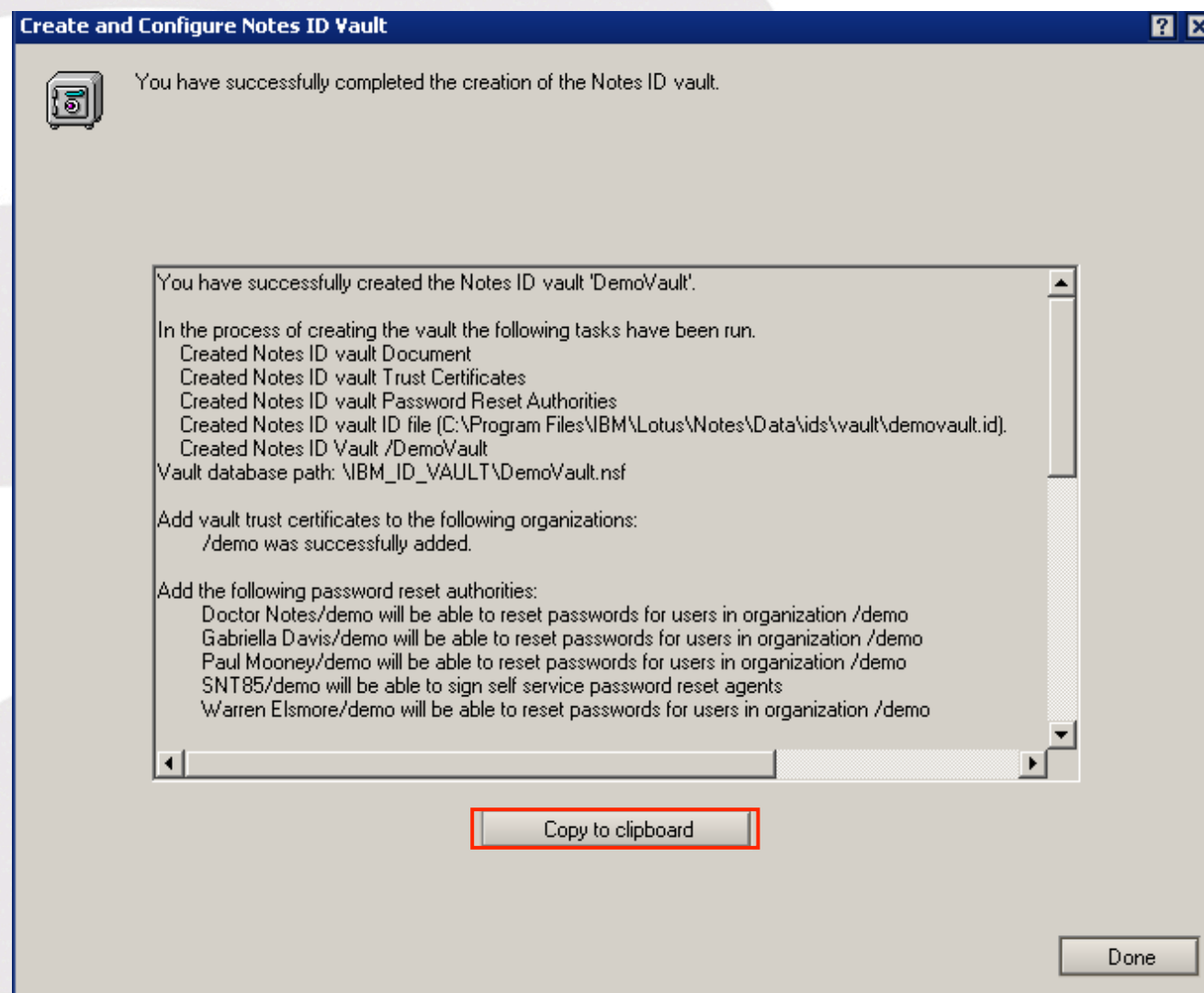


# Creating the ID Vault

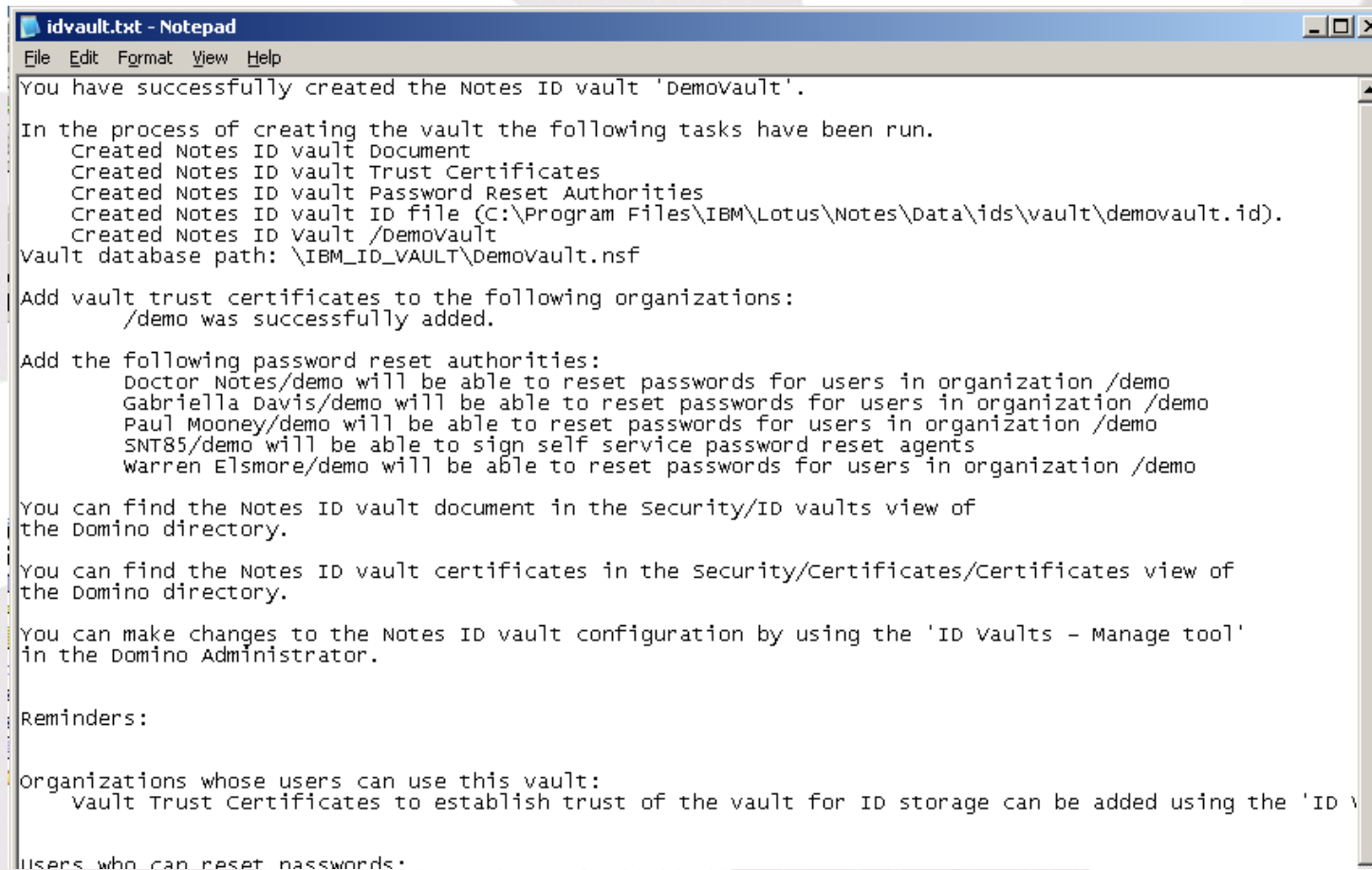


- As the ID Vault is created you will be prompted for the physical certifier and password for any organisations you specified be used

# Final Summary Screen



# Store a Record of the ID Vault Summary Clipboard



```
idvault.txt - Notepad
File Edit Format View Help

You have successfully created the Notes ID vault 'demovault'.

In the process of creating the vault the following tasks have been run.
  Created Notes ID vault Document
  Created Notes ID vault Trust Certificates
  Created Notes ID vault Password Reset Authorities
  Created Notes ID vault ID file (C:\Program Files\IBM\Lotus\Notes\Data\ids\vault\demovault.id).
  Created Notes ID vault /demovault
Vault database path: \IBM_ID_VAULT\demovault.nsf

Add vault trust certificates to the following organizations:
  /demo was successfully added.

Add the following password reset authorities:
  Doctor Notes/demo will be able to reset passwords for users in organization /demo
  Gabriella Davis/demo will be able to reset passwords for users in organization /demo
  Paul Mooney/demo will be able to reset passwords for users in organization /demo
  SNT85/demo will be able to sign self service password reset agents
  Warren Elsmore/demo will be able to reset passwords for users in organization /demo

You can find the Notes ID vault document in the Security/ID vaults view of
the Domino directory.

You can find the Notes ID vault certificates in the Security/Certificates/Certificates view of
the Domino directory.

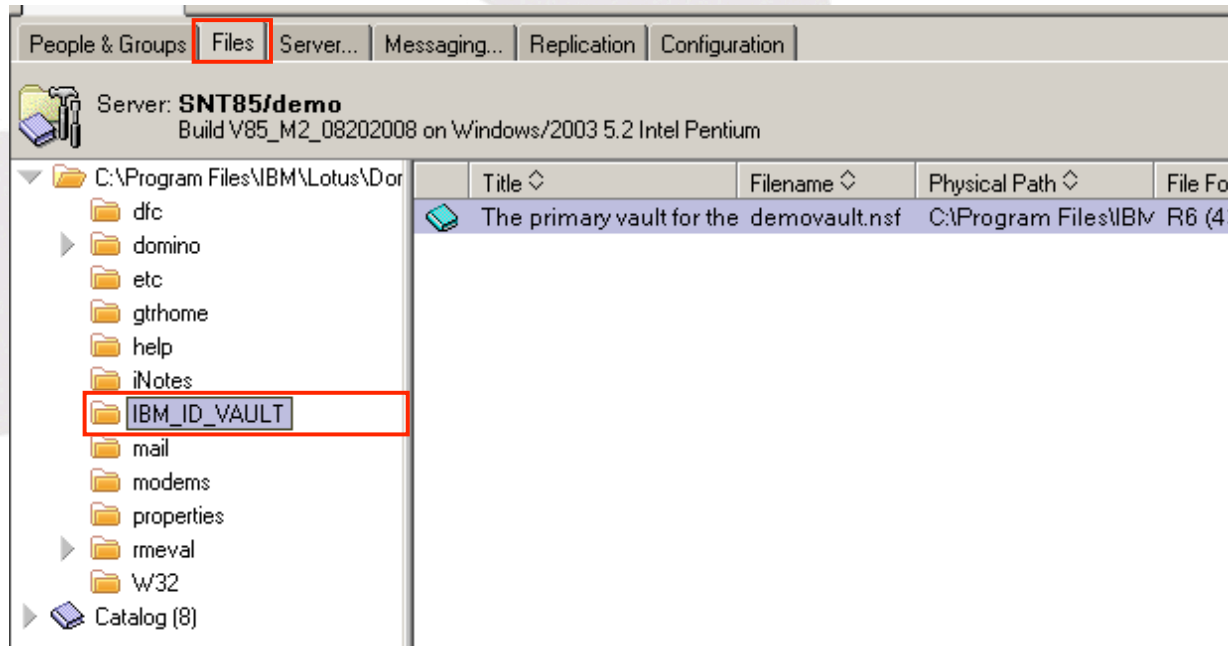
You can make changes to the Notes ID vault configuration by using the 'ID vaults - Manage tool'
in the Domino Administrator.

Reminders:

Organizations whose users can use this vault:
  Vault Trust Certificates to establish trust of the vault for ID storage can be added using the 'ID v
Users who can reset passwords:
```



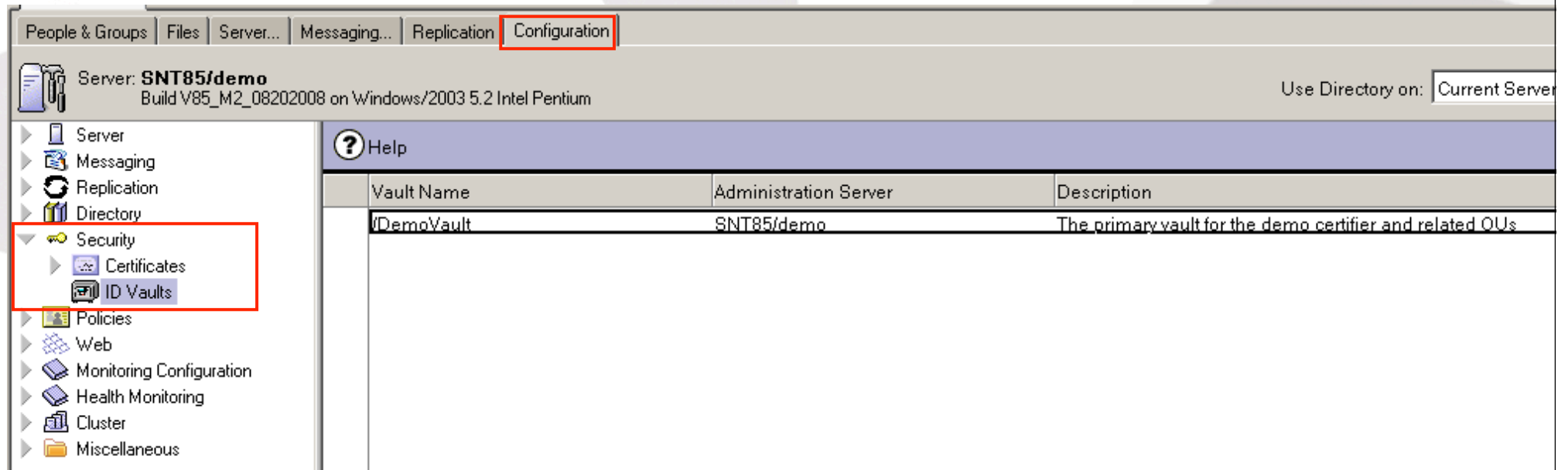
# Verifying the ID Vault Created Correctly



- ID Vault db with the title you specified will be in the IBM\_ID\_VAULT directory on the server you selected



# ID Vault Document Created Under Security



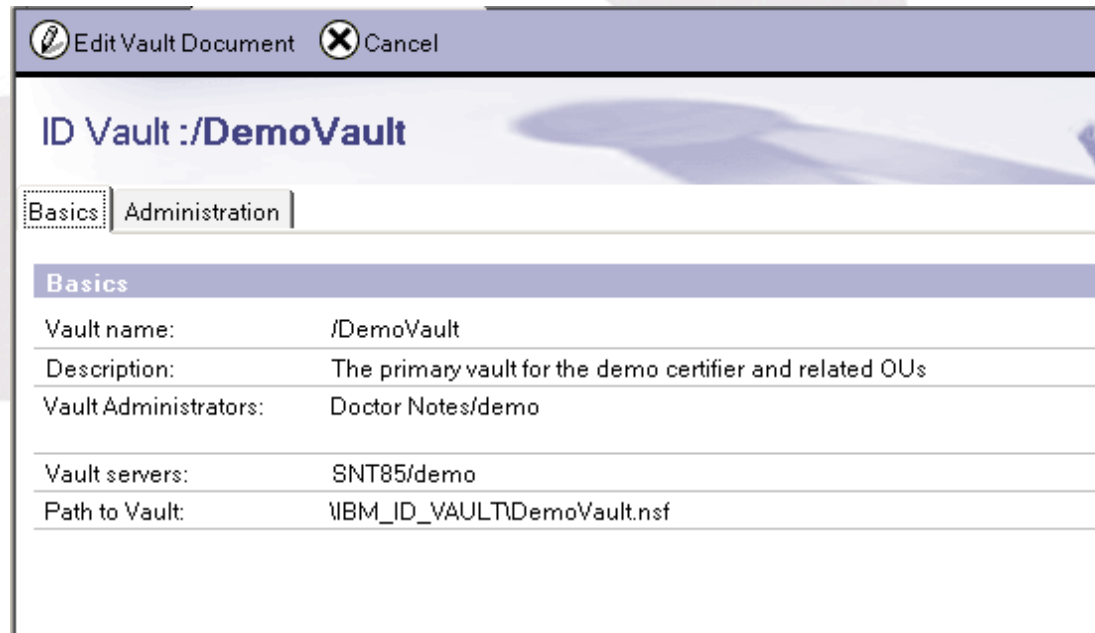
The screenshot shows the IBM Security Guardium Configuration console. The top navigation bar includes tabs for People & Groups, Files, Server..., Messaging..., Replication, and Configuration (which is highlighted with a red box). Below the navigation bar, the server information is displayed: Server: **SNT85/demo**, Build V85\_M2\_08202008 on Windows/2003 5.2 Intel Pentium. On the right, there is a dropdown menu for "Use Directory on:" with "Current Server" selected.

The left sidebar contains a tree view of the configuration options. The "Security" folder is expanded, and the "ID Vaults" option is highlighted with a red box. Other options in the sidebar include Server, Messaging, Replication, Directory, Certificates, Policies, Web, Monitoring Configuration, Health Monitoring, Cluster, and Miscellaneous.

The main content area displays a table with the following data:

Vault Name	Administration Server	Description
IDemoVault	SNT85/demo	The primary vault for the demo certifier and related OUs

# View of ID Vault Document



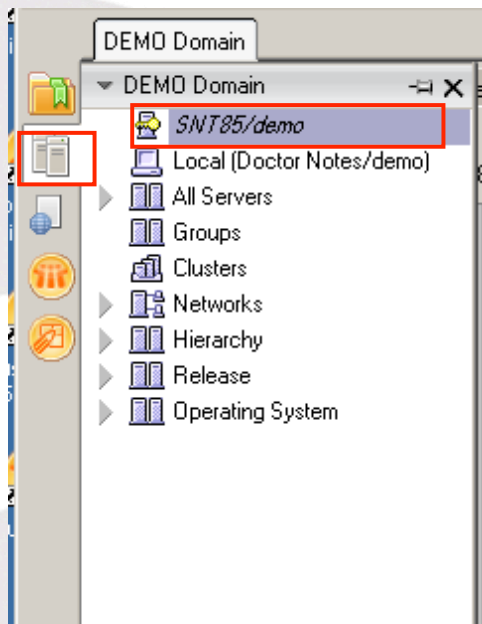
Dialog box titled "Edit Vault Document" with a "Cancel" button. The main title is "ID Vault :/DemoVault". There are two tabs: "Basics" (selected) and "Administration".

Basics	
Vault name:	/DemoVault
Description:	The primary vault for the demo certifier and related OUs
Vault Administrators:	Doctor Notes/demo
Vault servers:	SNT85/demo
Path to Vault:	IBM_ID_VAULT/DemoVault.nsf

- Always use the 'Manage Vault' process rather than edit this document manually to ensure all steps are completed

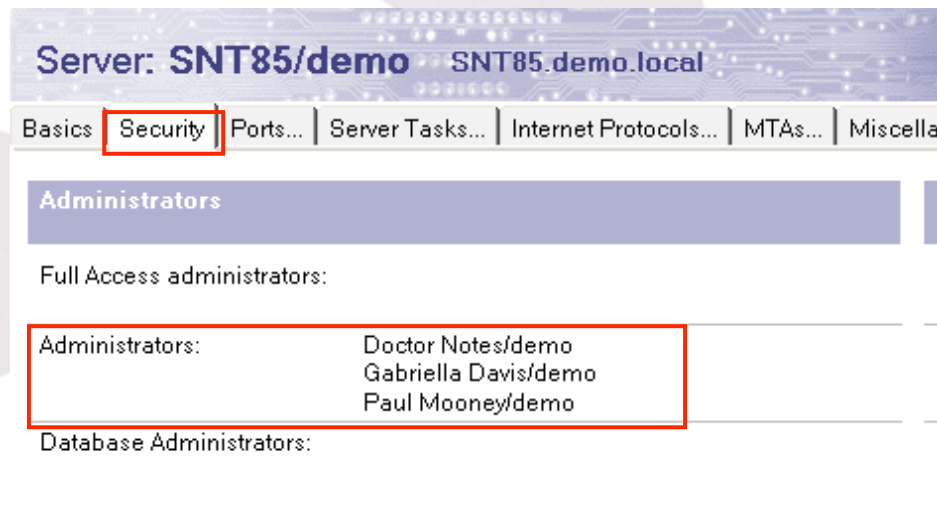


# Managing Vault Admins



- Make sure you have selected the server in the bookmark bar
  - don't use File - Open Server
  - if you find you have an empty list of 'Admins' to choose from
    - this could be why

# Managing Vault Admins



- To add someone as a Vault admin they must first have Administrator rights in the server document for the ID Vault server
- This setting caches on the server and without a restart will take a while to update



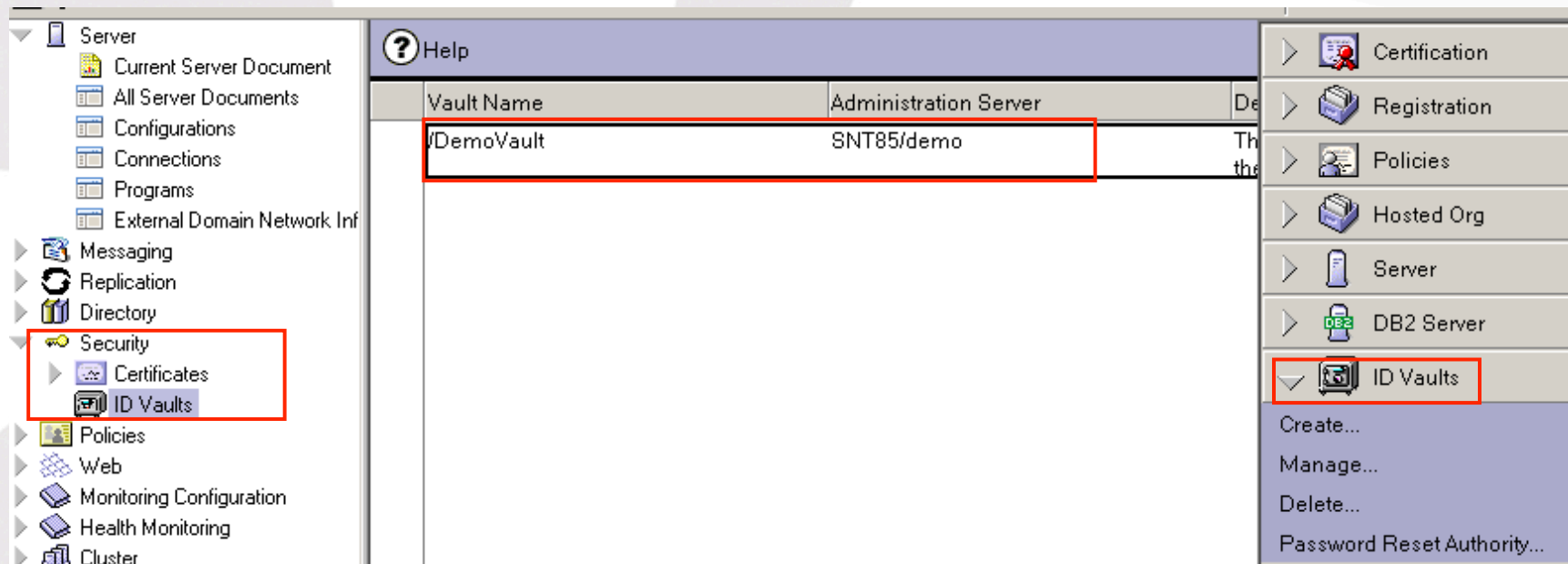
# Managing Vault Admins

- ID Vault Admins can make changes to the Vault itself including
  - adding or removing other admins
  - adding or removing certifiers
  - creating or deleting ID Vault replicas
- You do not have to give someone ‘Administrator’ rights if they are simply resetting passwords for users
  - They don’t even need access to the user ids or to know the original user passwords

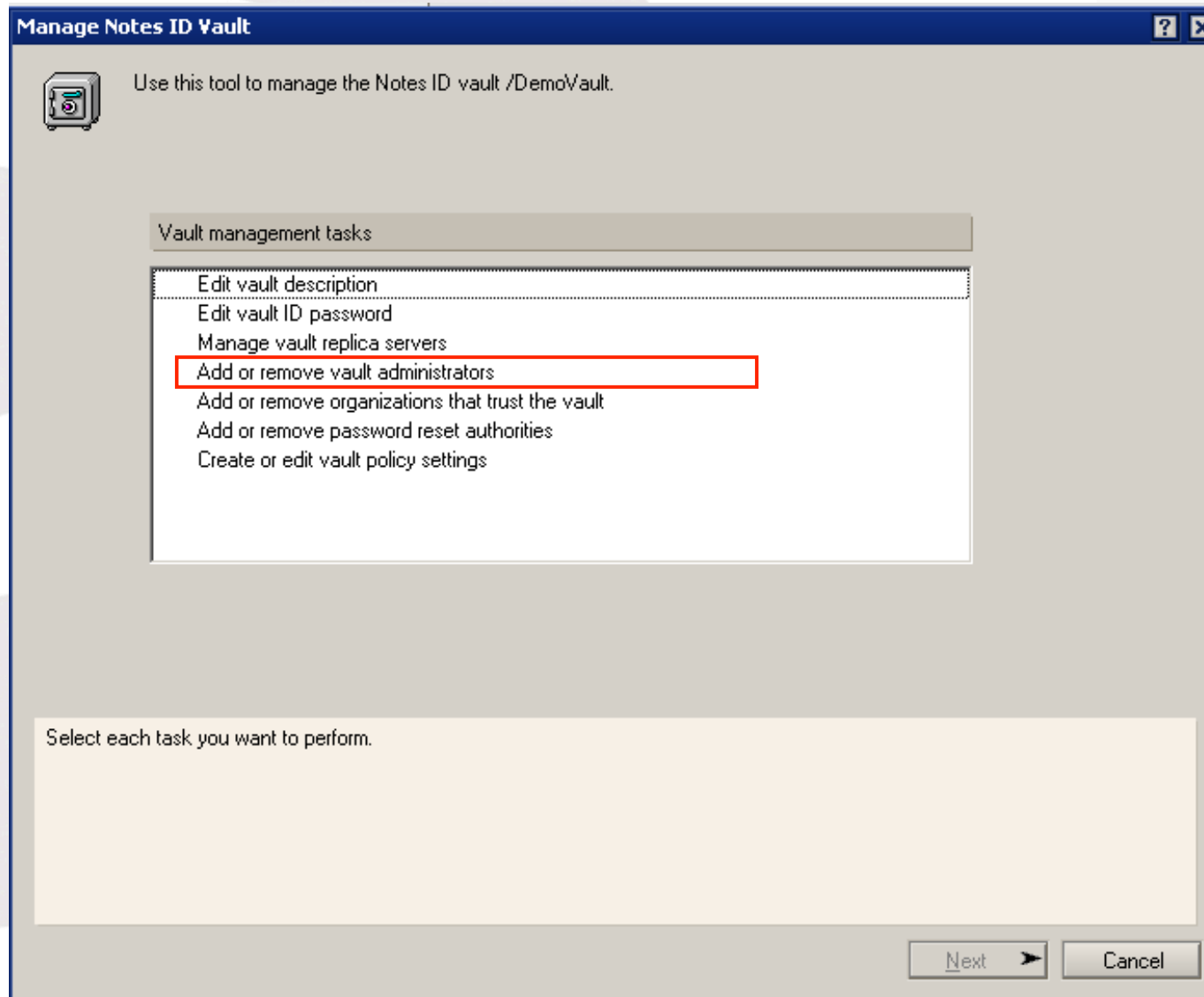


# Managing Vault Admins

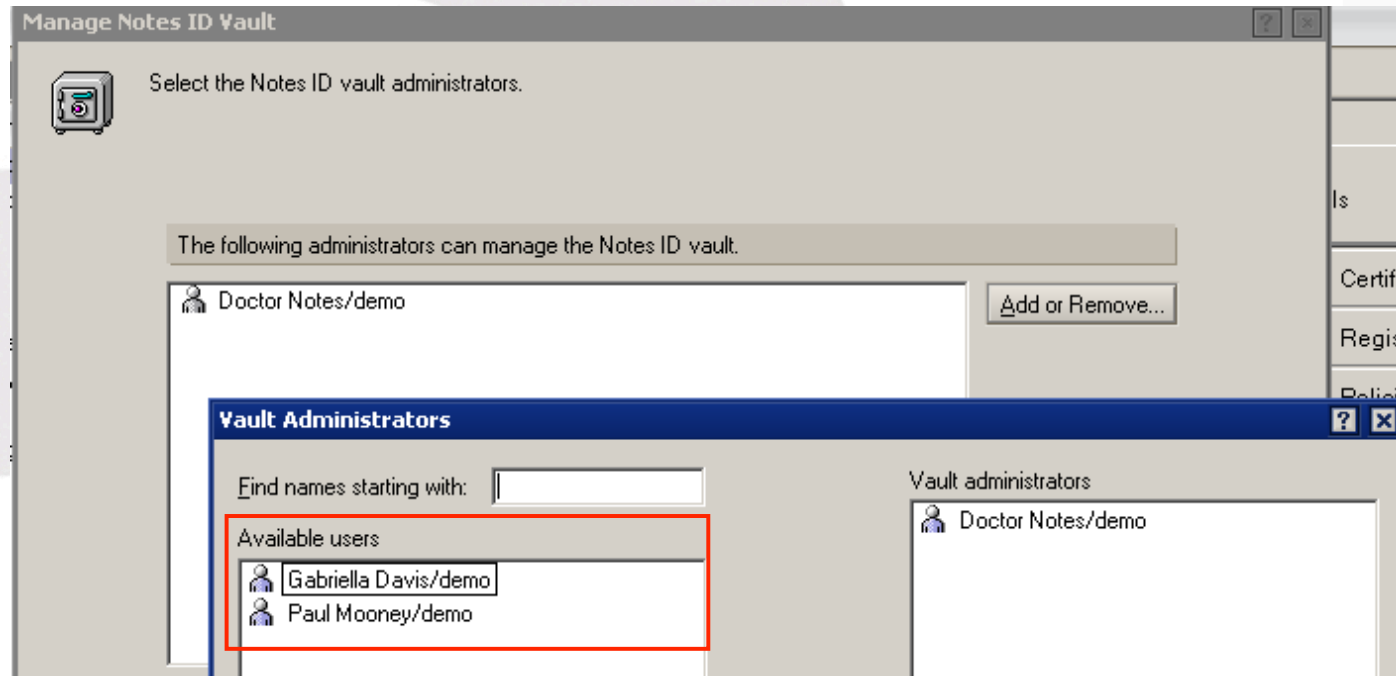
- ID Vault Security document must be selected
- Select Tools - ID Vault - Manage



# Managing Vault Admins



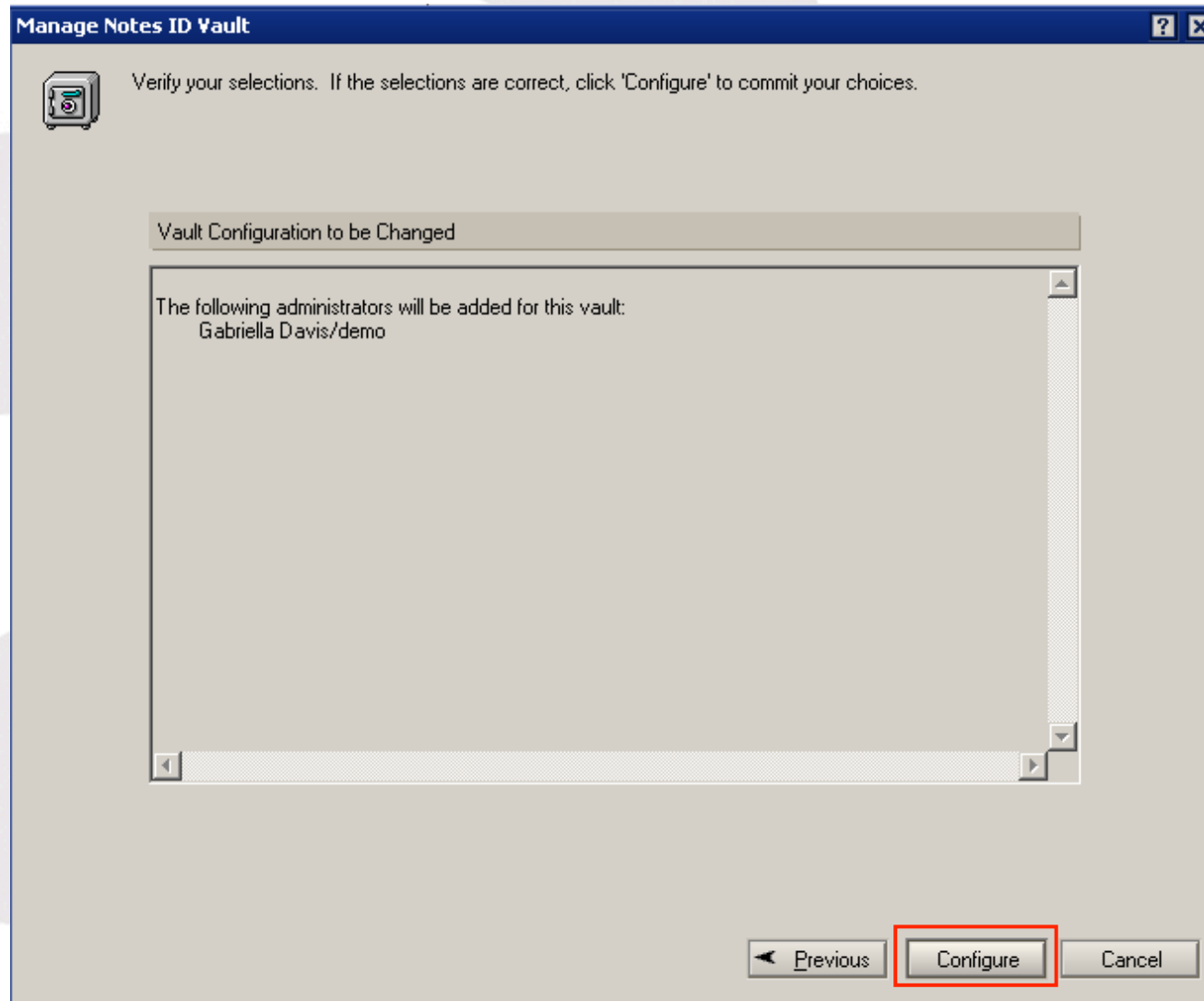
# Managing Vault Admins



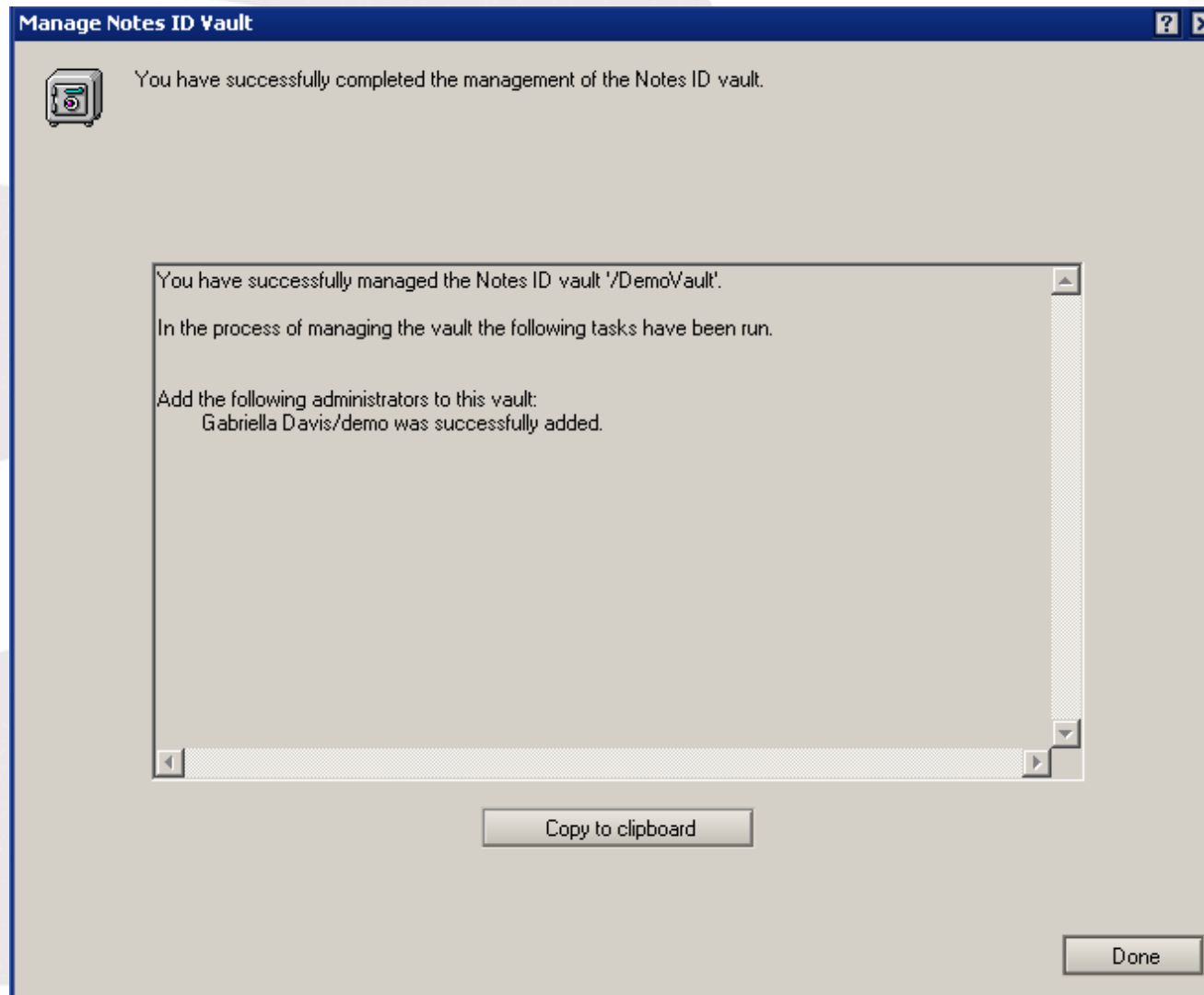
- Add or remove additional users as Administrators of this vault
  - Note you can only select from those listed in the 'Administrators' field of the server document



# Managing Vault Admins



# Managing Vault Admins - Summary Screen



# Verify Admin Change

- ID Vault Security Document

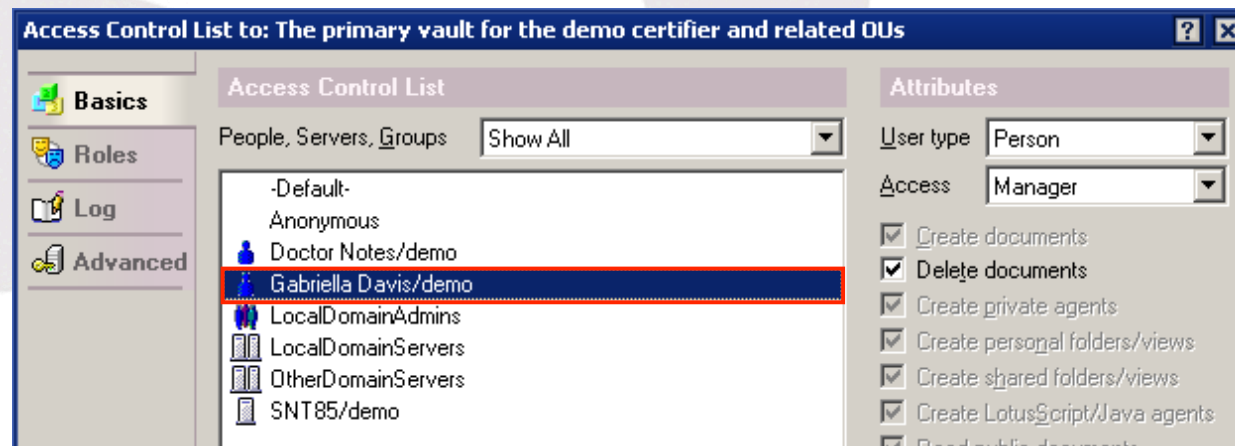
ID Vault :/DemoVault

Basics Administration

**Basics**

Vault name:	/DemoVault
Description:	The primary vault for the demo certifier and related OUs
Vault Administrators:	Doctor Notes/demo, Gabriella Davis/demo
Vault servers:	SNT85/demo
Path to Vault:	\\IBM_ID_VAULT\\DemoVault.nsf

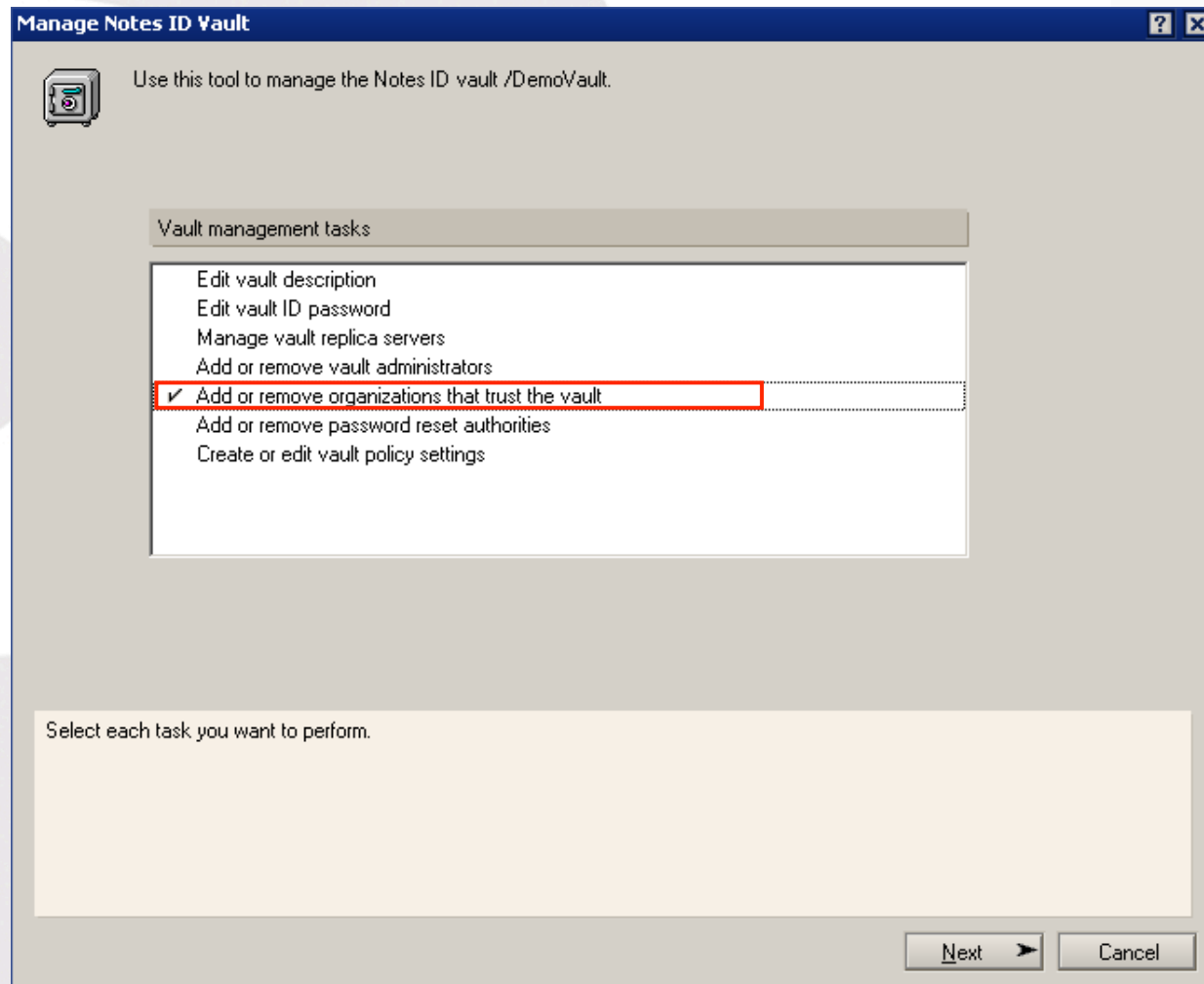
# Verify Admin Change



- ID Vault ACL
  - Default is Manager without the role 'Auditor'



# Adding other organisations that trust the vault

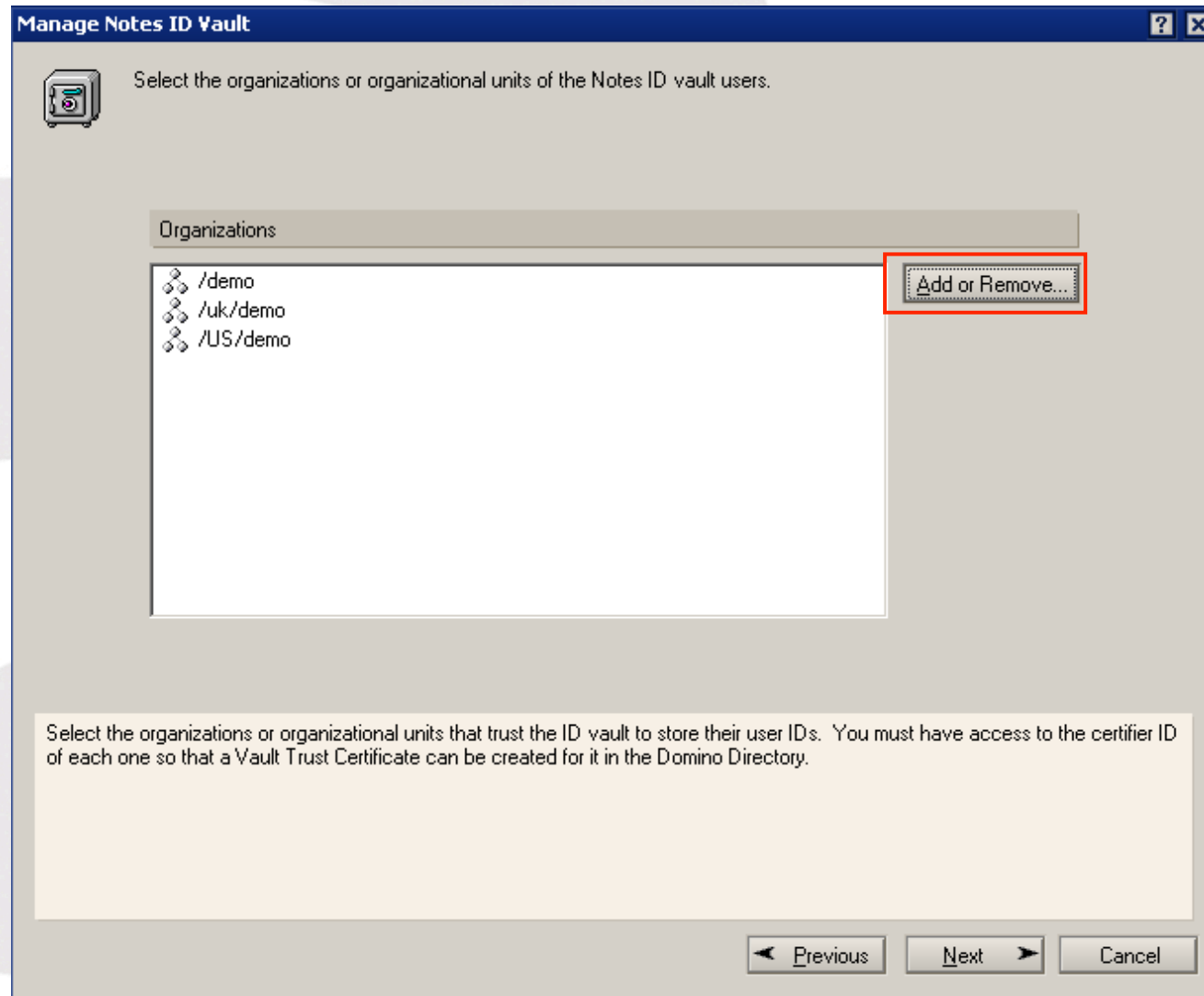


- A Vault can only store user ids if it holds a trust certificate for the parent certifier of that user

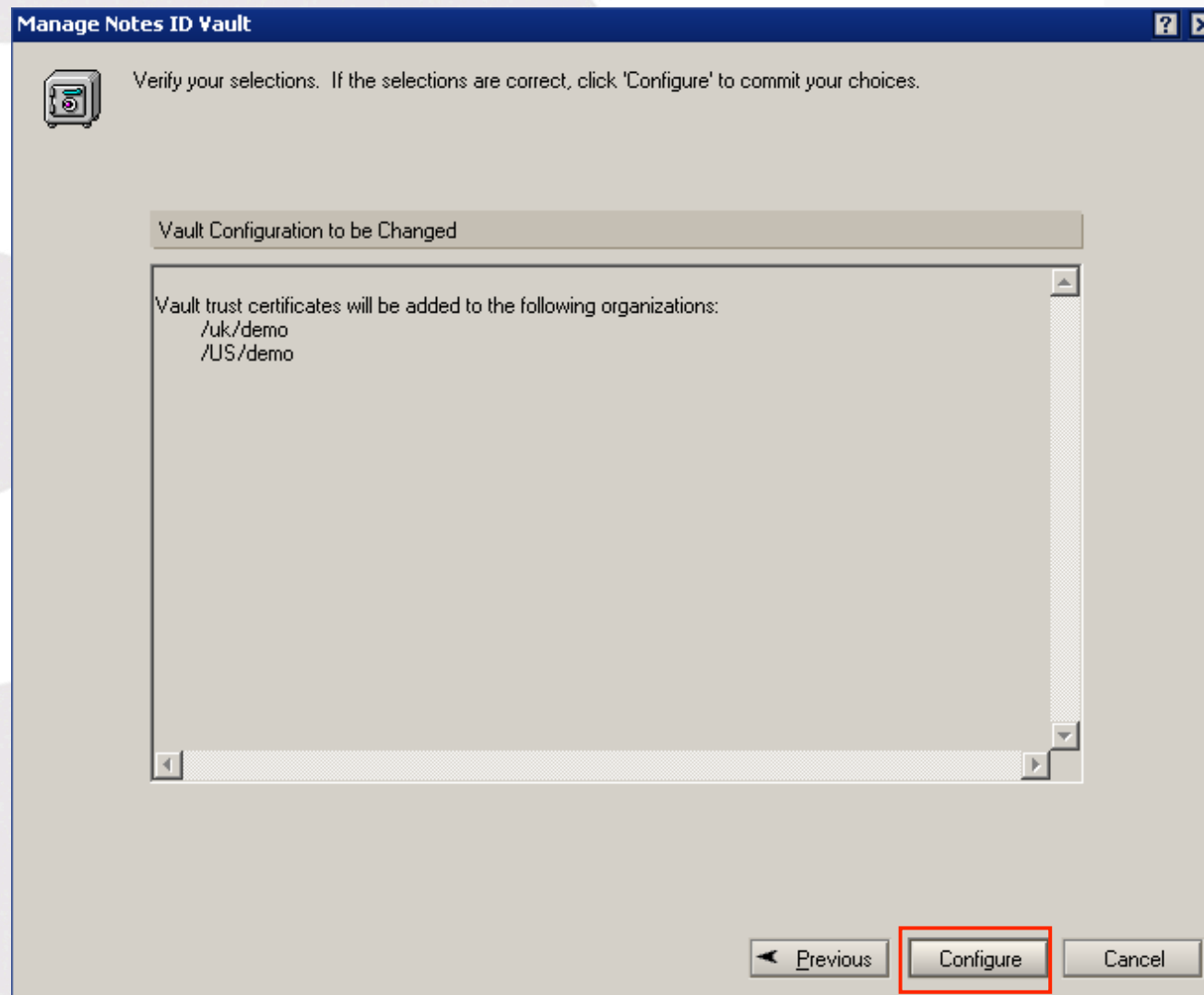


**BLUG**  
Belux Lotus User Group

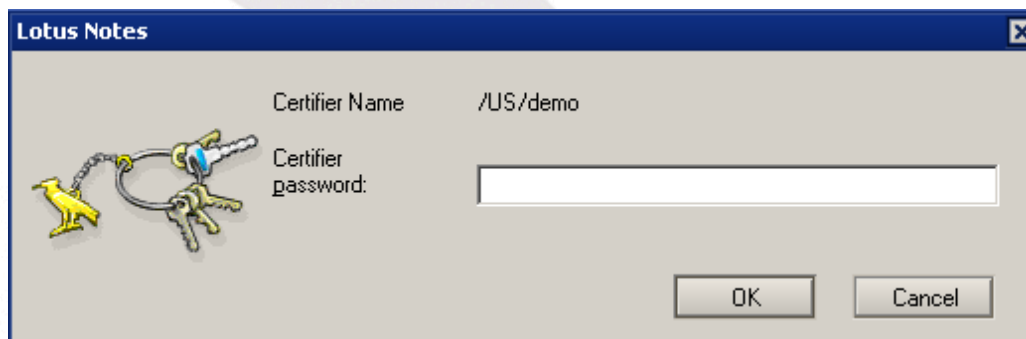
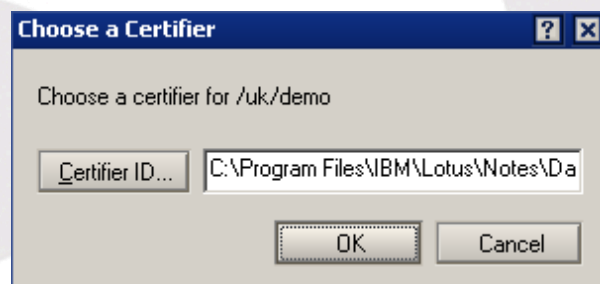
# Adding other organisations that trust the vault



# Adding other organisations that trust the vault

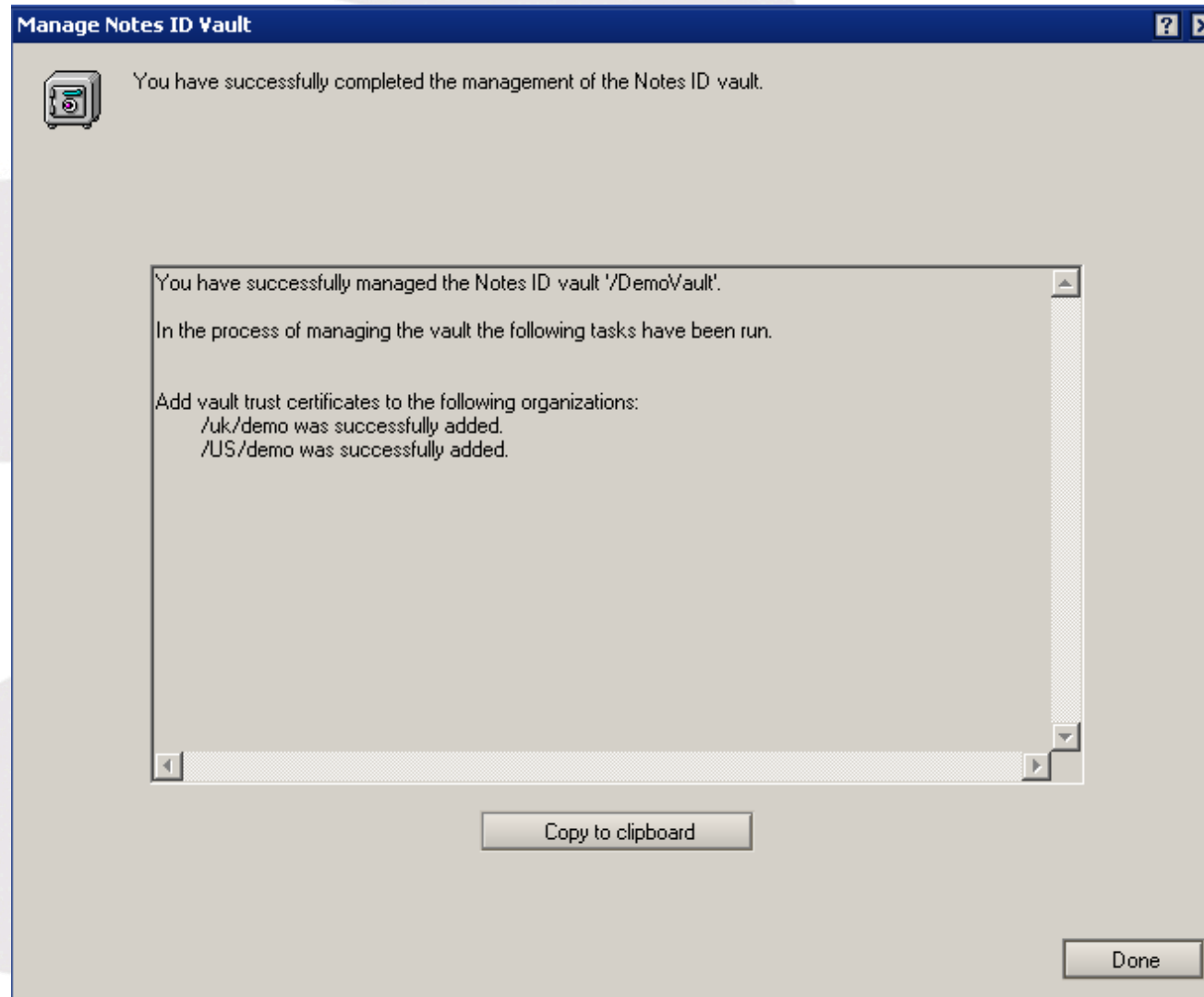


# Adding other organisations that trust the vault

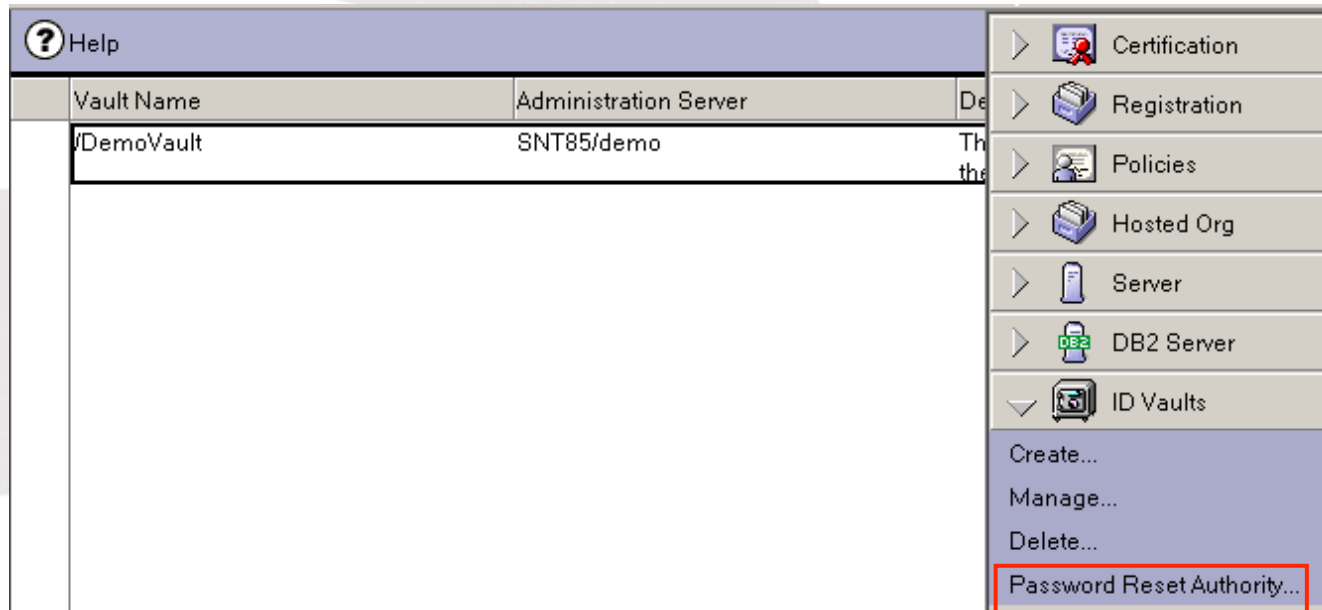




# Adding other organisations that trust the vault



# Configure Password Reset Authority



- Configuration Tab - Select ID Vault Document under Security
  - Tools - ID Vaults - Password Reset Authority

# Configure Password Reset Authority

**Authority To Reset Passwords**

Specify names that are authorized to reset passwords.

Directory: demo's Directory

Available users, groups and servers

- Administration Requests
- Davis , Gabriella
- Davis , Tim
- Elsmore , Warren
- LocalDomainAdmins
- LocalDomainServers

Available organizational units

- \*uk/demo
- \*US/demo

Password reset authority by organization

- /demo
  - Doctor Notes/demo
  - Gabriella Davis/demo
  - Paul Mooney/demo
  - SNT85/demo
  - Warren Elsmore/demo
- /uk/demo
- /US/demo

☐ Self-service password reset authority.

On the left, select the name of a user, group, server, or organizational unit to authorize to reset passwords. On the right, add the selected name to each user organization or organizational unit it will reset passwords for. Repeat to give password reset authority to additional names. A Password Reset Certificate will be created for each authorized user, group member, server, and organizational unit. To allow users to reset their own passwords using an agent, select 'Self-service password reset authority' for the user name that signs the agent and for each server on which the agent will run. For more information on password reset authority, including authorizing a non-agent self-service application, click ?

# Configuring for additional certifiers

**Authority To Reset Passwords**

Specify names that are authorized to reset passwords.

Directory: demo's Directory

Available users, groups and servers

- Lotus Notes/Domino Fault Rep
- Lotus Notes/Domino Smart Up
- Mooney, Paul**
- Notes, Doctor
- OtherDomainServers
- SNT85/demo

Available organizational units

- \*/uk/demo
- \*/US/demo

Add

Add To All

Remove

Remove From All

☐ Self-service password reset authority.

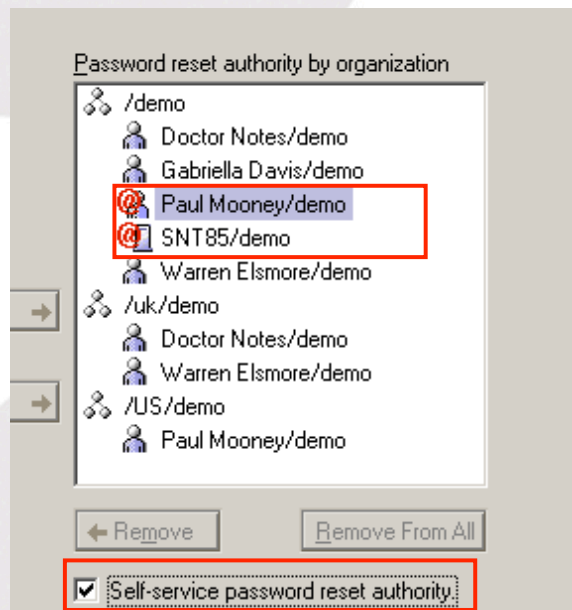
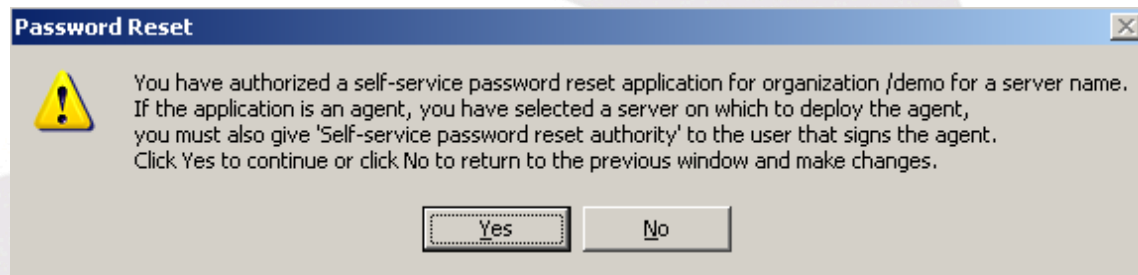
On the left, select the name of a user, group, server, or organizational unit to authorize to reset passwords.  
On the right, add the selected name to each user organization or organizational unit it will reset passwords for.  
Repeat to give password reset authority to additional names. A Password Reset Certificate will be created for each authorized user, group member, server, and organizational unit. To allow users to reset their own passwords using an agent, select 'Self-service password reset authority' for the user name that signs the agent and for each server on which the agent will run. For more information on password reset authority, including authorizing a non-agent self-service application, click ?

Next

Cancel

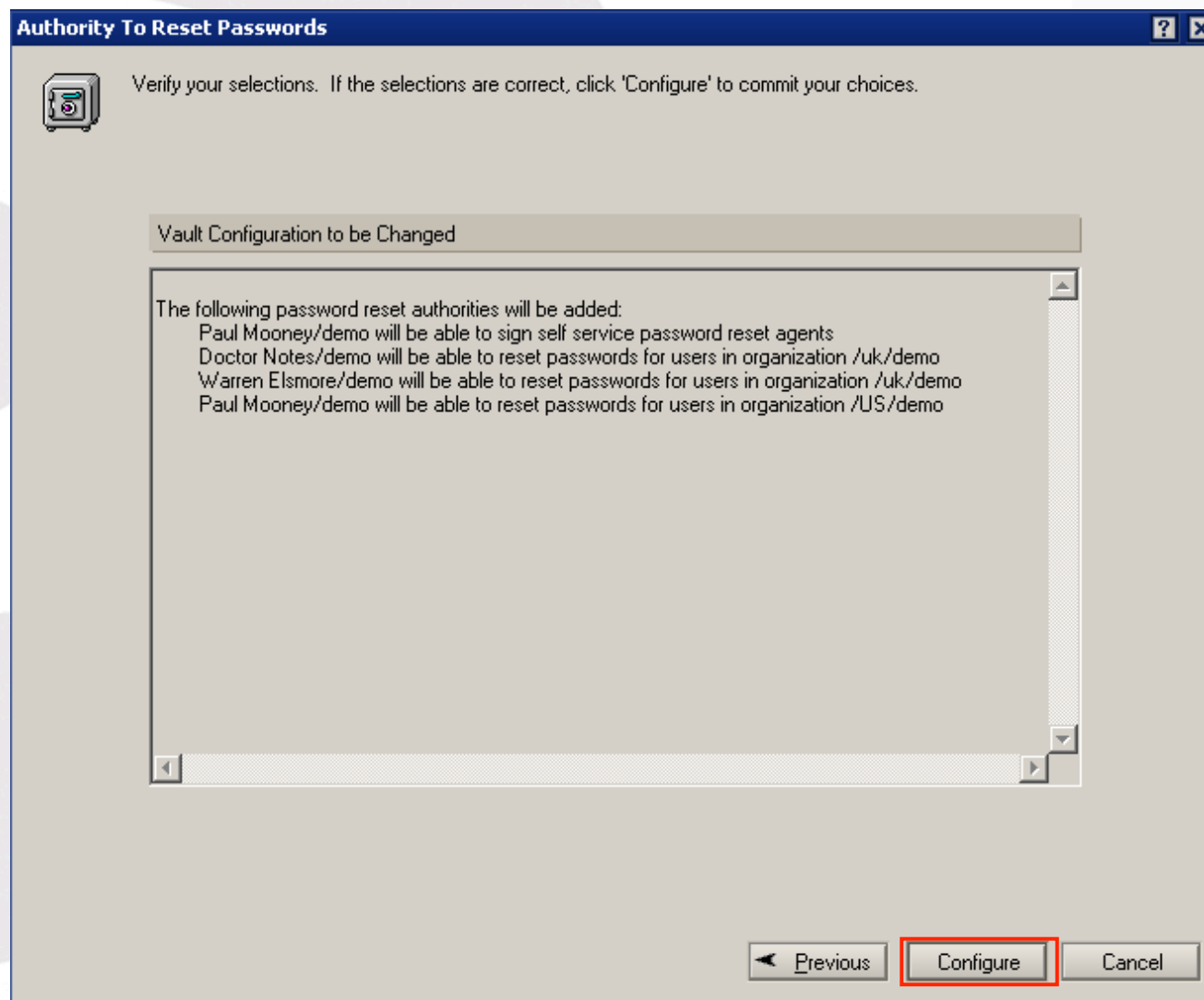


# Configuring for additional certifiers

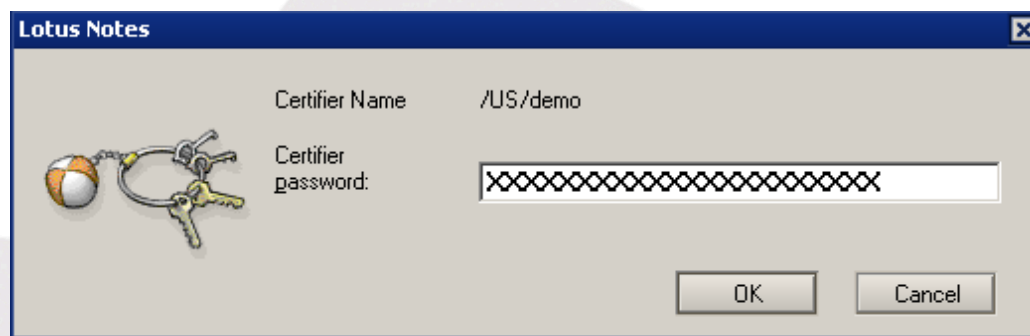
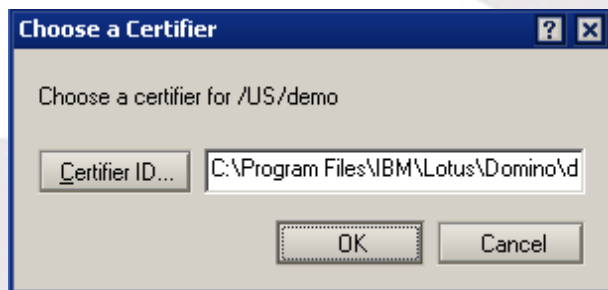


- If you are planning to use an application for auto processing password resets you will need a server authorised as 'Self Service Password Reset Authority' and also an agent signer
  - In this example an agent running on SNT85/ Demo and signed by Paul Mooney/demo can process requests

# Complete Configuring for Password Reset Authority



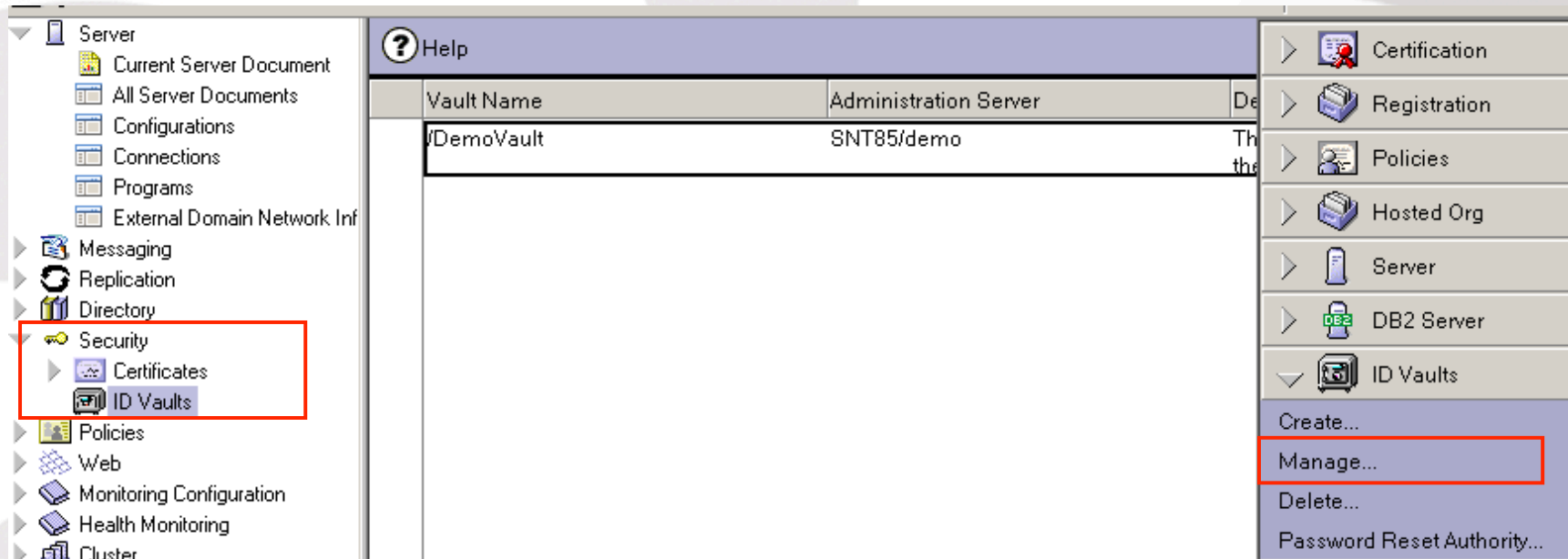
# Complete Configuring for Password Reset Authority



# Setting up a Policy to use the ID Vault

ID Vault Security document must be selected

Select Tools - ID Vault - Manage



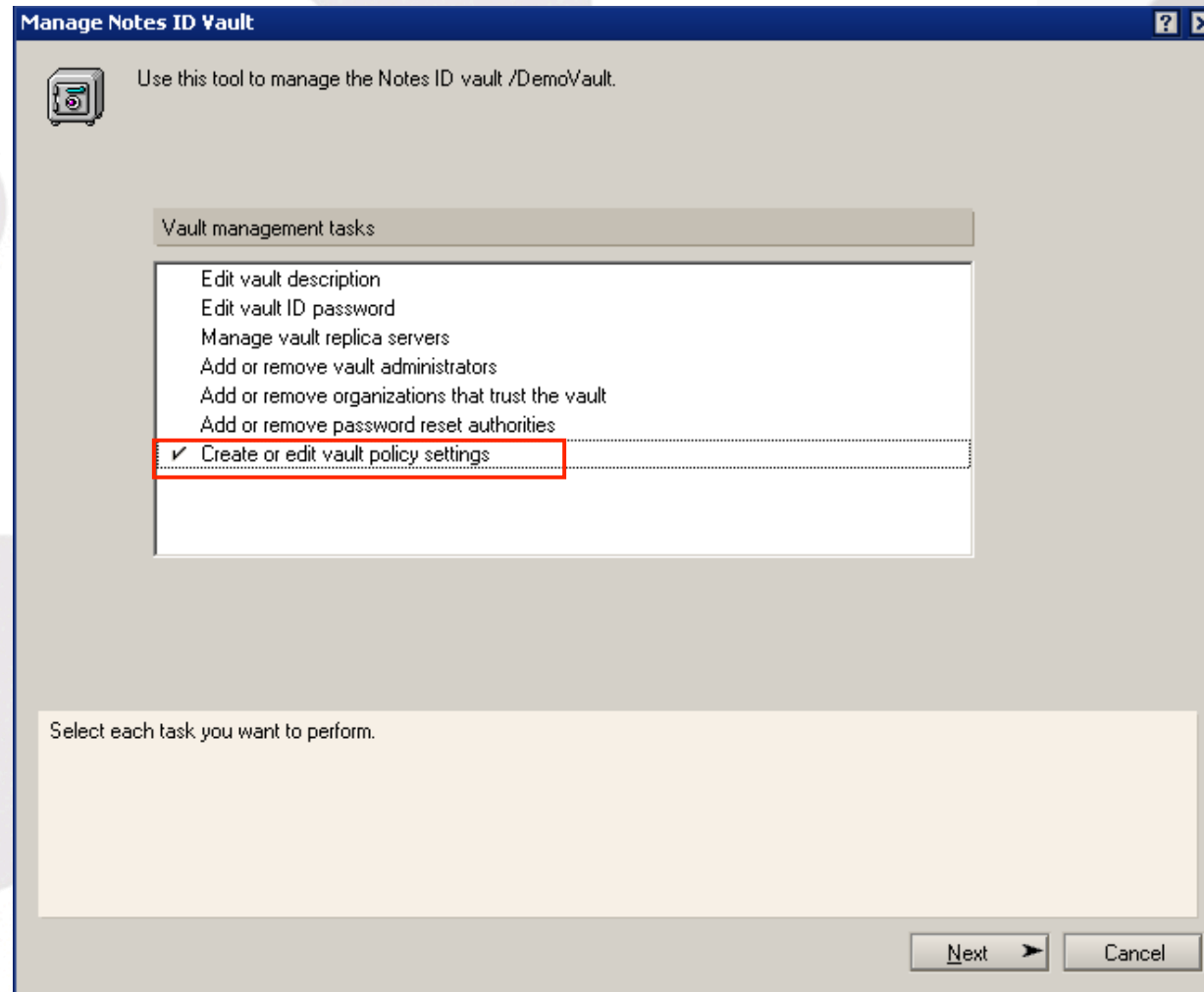
Configuration tab - Policies

–Tools - Policies - Create

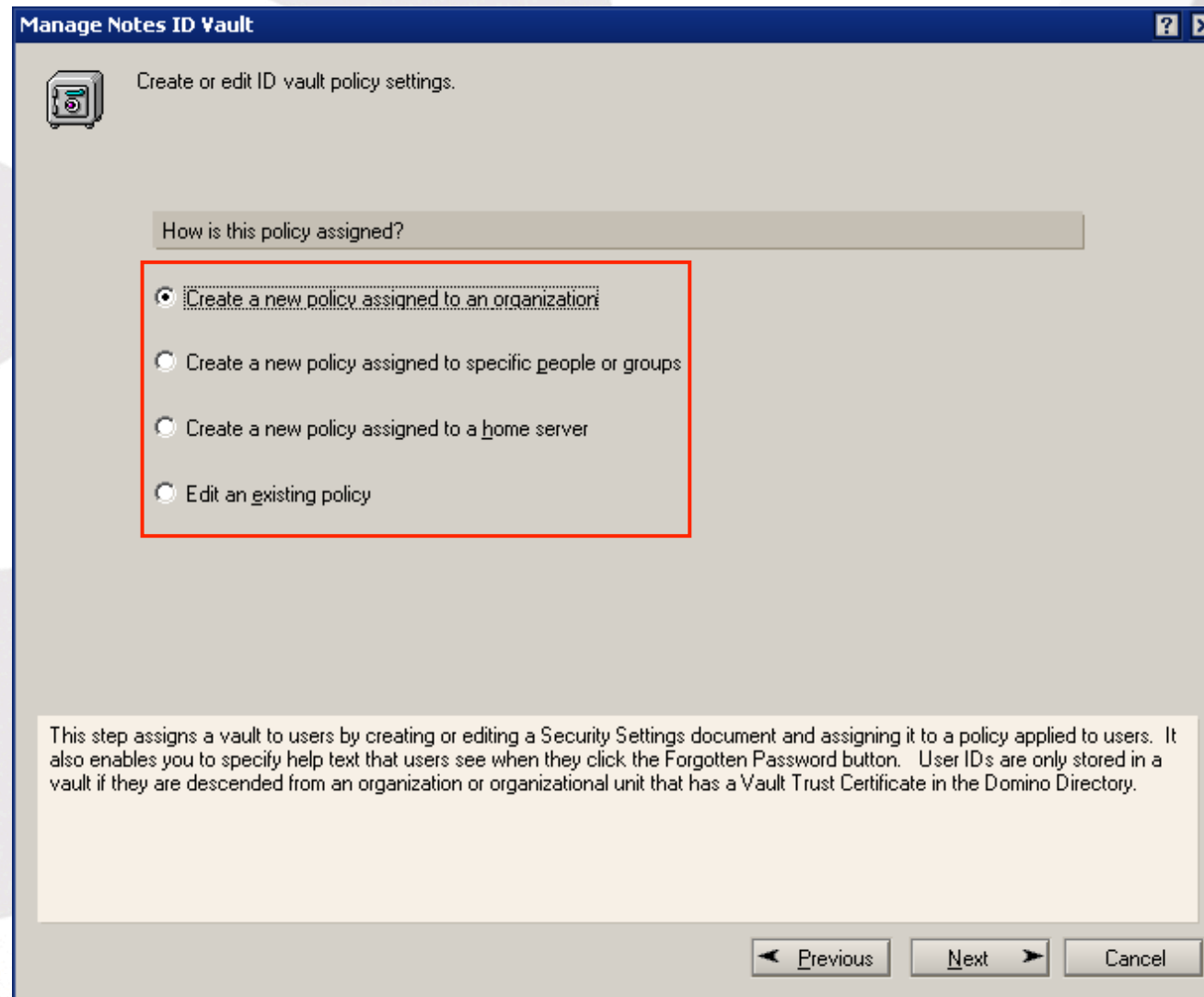


# Create or edit vault policy settings

- If you work with policies you can create the security policy outside of this process



# Select the type of policy to create or edit



Manage Notes ID Vault

Create or edit ID vault policy settings.

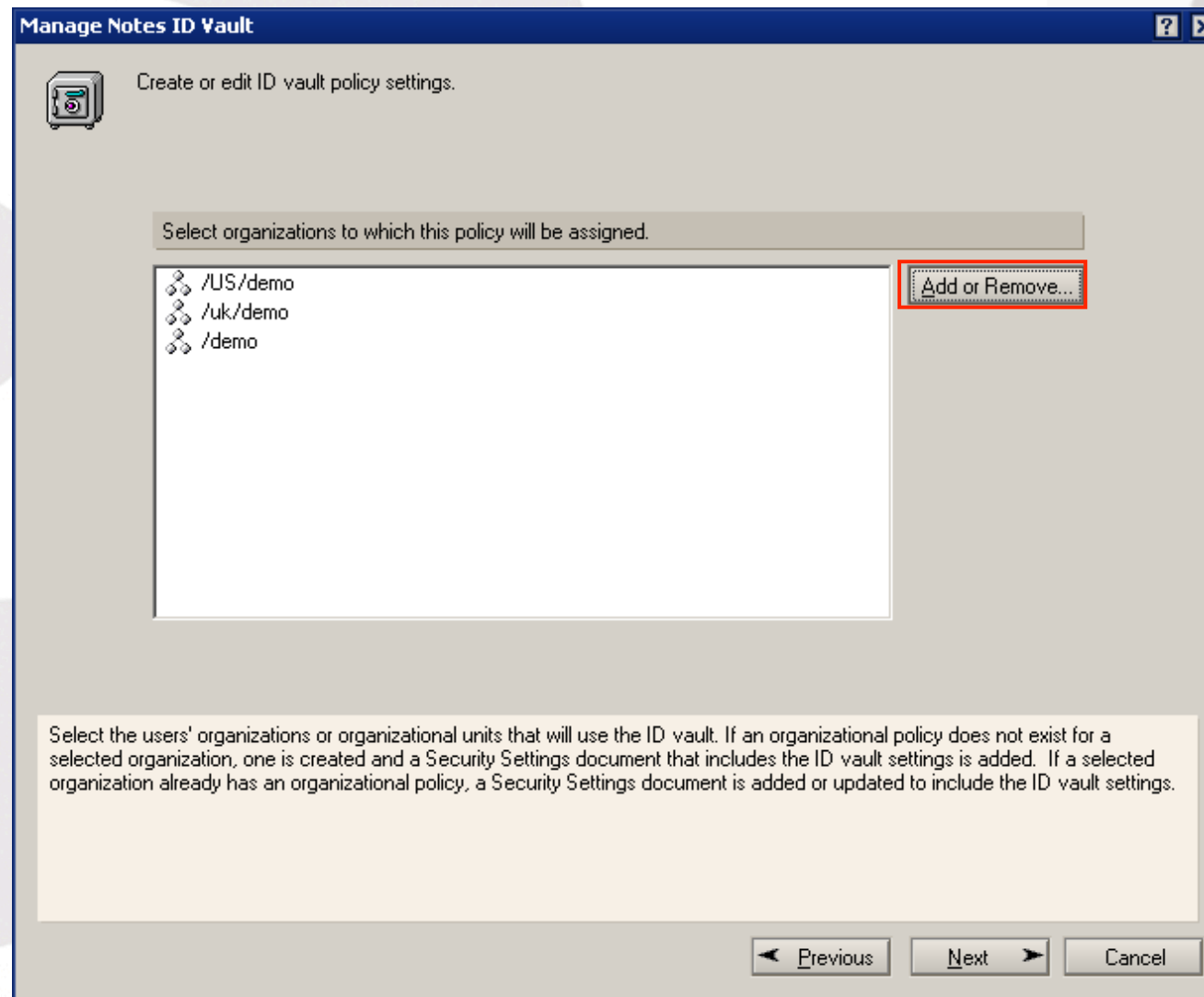
How is this policy assigned?

- ☒ 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

This step assigns a vault to users by creating or editing a Security Settings document and assigning it to a policy applied to users. It also enables you to specify help text that users see when they click the Forgotten Password button. User IDs are only stored in a vault if they are descended from an organization or organizational unit that has a Vault Trust Certificate in the Domino Directory.

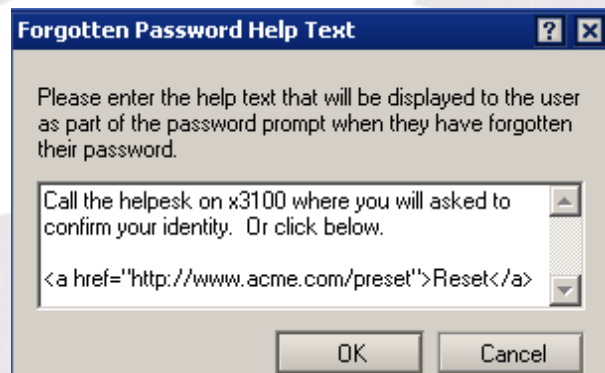
Previous Next Cancel

# Which certifiers are associated with this policy



# Setting up a user prompt

- This is what the user sees when they select 'Forgot Your Password'
  - You have 8 lines to write and can also use HTML to point to a link or button





# Verifying policies

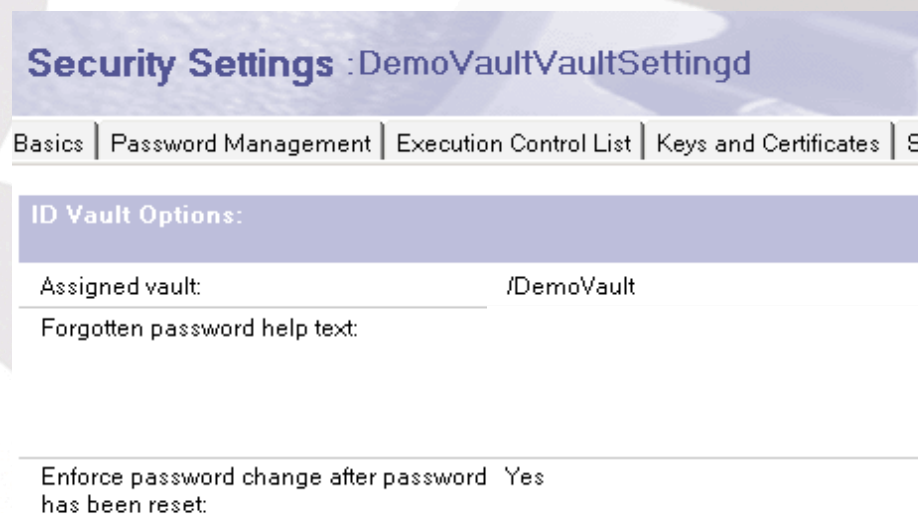
The screenshot displays the 'Policy : \*/demo' configuration page. On the left, a 'Policy Namespace' tree shows a hierarchy: 'Organizational Policies' > 'demo' > '\*/demo' > 'uk' > '\*/uk/demo' > 'US' > '\*/US/demo'. The right pane shows the 'Basics' tab for the selected policy. It includes fields for 'Policy name' (\*/demo), 'Policy type' (Organizational), 'Description' (Vault policy for DemoVault), and 'Category'. A 'Create Child' button is next to the policy name. Below these fields is a table for settings:

Setting Type	Setting Name
Registration:	
Setup:	
Archiving:	
Desktop:	
Security:	<a href="#">DemoVaultVaultSetting</a>
Mail:	

- These were created automatically by the Manage ID Vault process
  - You could create and manage them manually

# Adding an HTML link in the forgotten password help text

- 1. The link must be a full HTML link, including the tags
- 2. The tags are case sensitive, you must use upper case.
- 3. The target for the link must be enclosed in quote characters (").
- 4. The link must be the last part of the custom message. If you include the link in the middle of the message, any text after the link will be discarded.



**Security Settings : DemoVaultVaultSettingd**

Basics | Password Management | Execution Control List | Keys and Certificates | Si

**ID Vault Options:**

Assigned vault: /DemoVault

Forgotten password help text:

Enforce password change after password has been reset: Yes

# Editing an ID Vault Security Policy

**Security Settings : DemoVaultVaultSettingsd**

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

ID Vault Options:		How to apply this setting:	Inh
Assigned vault:	/DemoVault	<input type="checkbox"/> Don't set value	<input type="checkbox"/>
Forgotten password help text:	Call the helpesk on x3100 where you will asked to confirm your identity. Or click below.<a href="http://www.acme.com/preset">Reset</a>	<input type="checkbox"/> Don't set value	<input type="checkbox"/>
Enforce password change after password has been reset:	Yes	<input type="checkbox"/> Don't set value	<input type="checkbox"/>

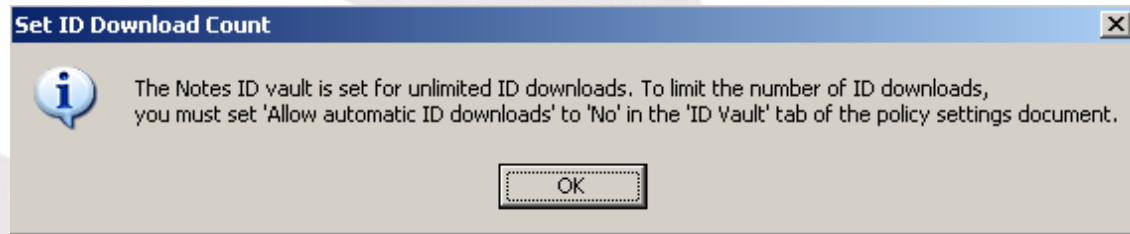
Automatic ID Downloads:		How to apply this setting:	Inh
Allow automatic ID downloads:	Yes	<input type="checkbox"/> Don't set value	<input type="checkbox"/>
Allow ID downloads for:	1 days	<input checked="" type="checkbox"/> Don't set value	<input checked="" type="checkbox"/>
	0 hours		
ID download authorization failure message:			

# Automatic ID Downloads

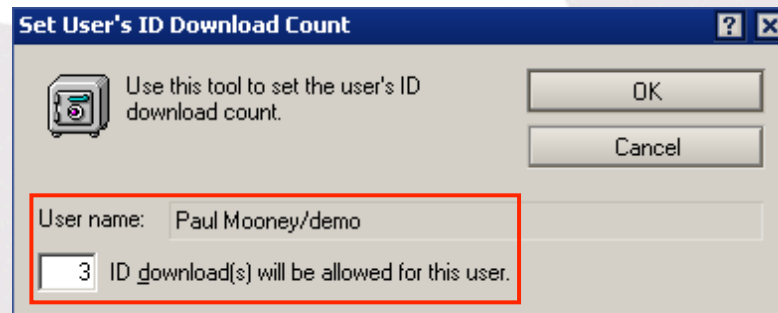
- Enabling 'Yes' for automatic ID downloads means an id is downloaded to whatever clients need it with no limit on the number of times they can be downloaded
  - If you know that a user has only 1 pc to work on then you can limit this by choosing 'no' and setting a number of downloads per user
- You can also control how long after an id change can that id still be downloaded
  - If you restrict it to 1 day then after than one day the id will no longer automatically download
- You can present a customised message to the user explaining that their updated id tried and failed to download and why



# Limiting the number of ID downloads

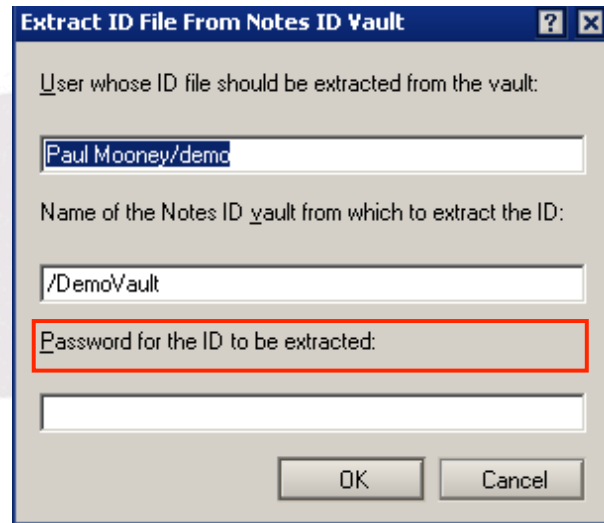


- Domino Administrator - People and Groups Tab
  - Select a Person
  - Tools - ID Vaults - Set ID download count



- If you haven't set the policy to allow unlimited downloads you might want to restrict how many times an updated id can be downloaded

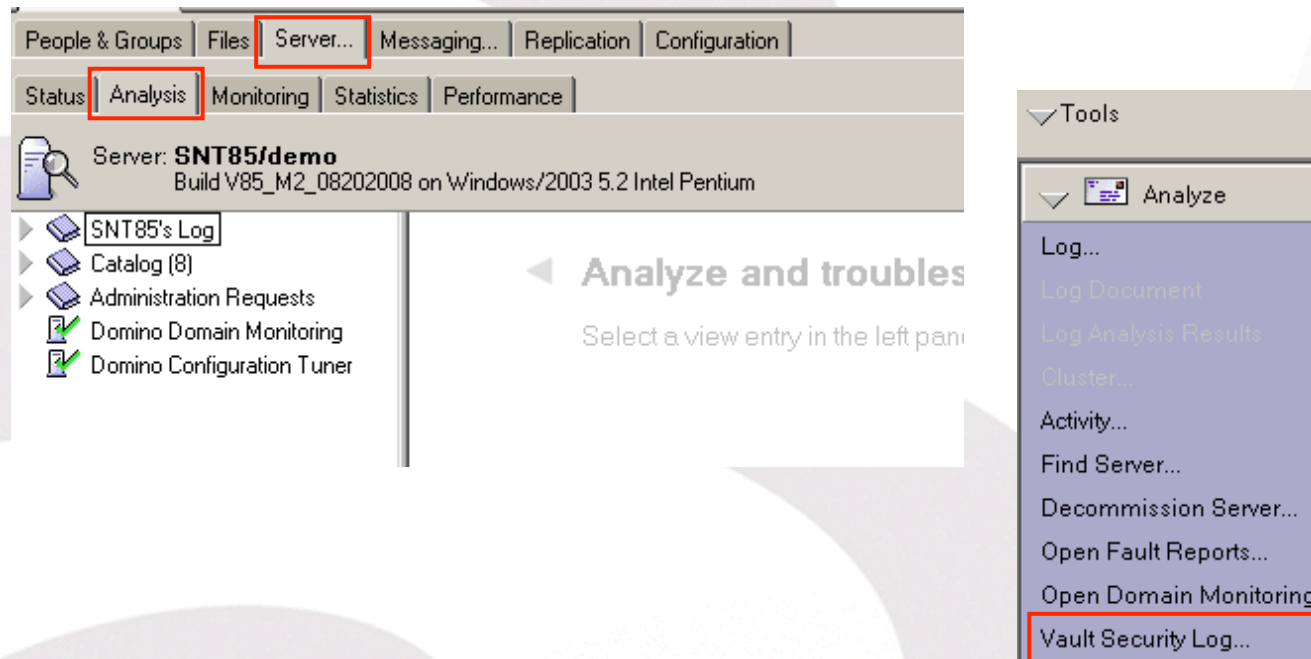
# Extracting an ID from the Vault



- Domino Administrator - People and Groups Tab

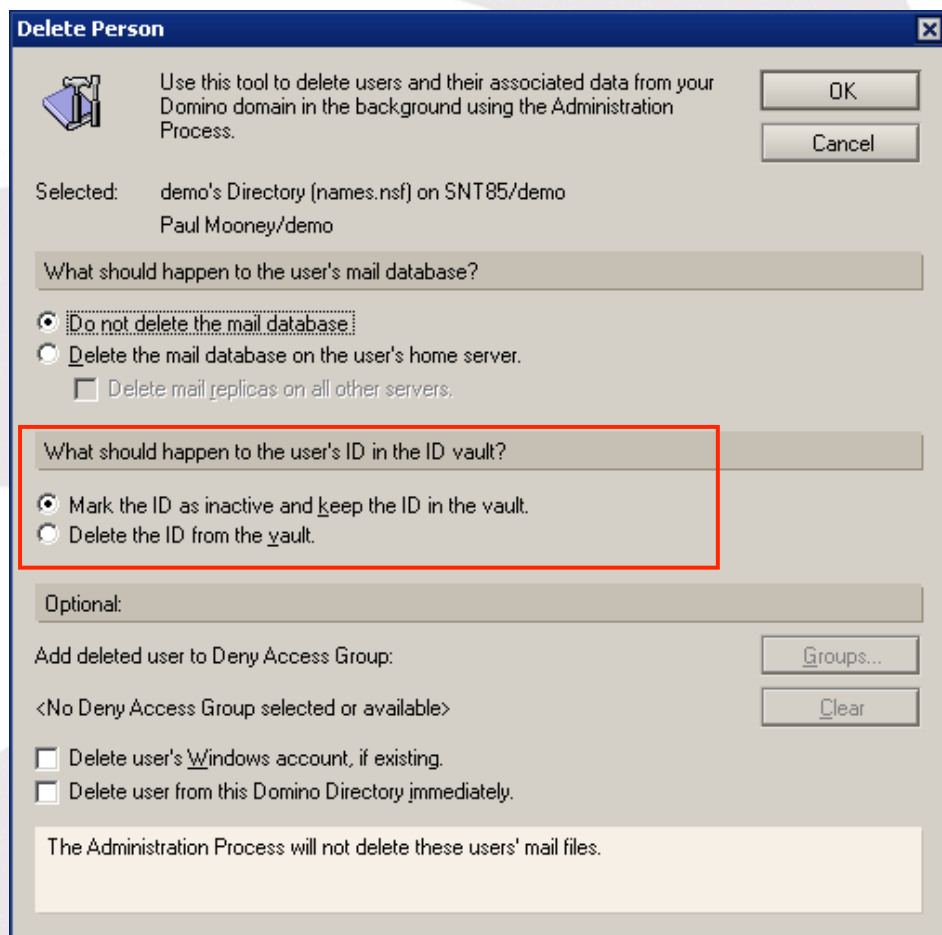
- Select a Person
- Tools - ID Vaults - Extract ID from Vault
- The password you will be asked for is the user id password not the vault password
- [Auditor] role in the ID Vault ACL allows the id to be extracted without requiring the user password
- SECURE\_DISABLE\_AUDITOR=1 disables the Auditor feature from that server

# ID Vault Logging and Events



- Review all Vault activity for a date range
- Domino Administrator - Server Tab - Analysis
  - Tools - Analyze - Vault Security Log

# Deleting IDs or Marking Them Inactive



**Delete Person**

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

Selected: demo's Directory (names.nsf) on SNT85/demo  
Paul Mooney/demo

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: Groups...  
<No Deny Access Group selected or available> Clear

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

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

- Deleting an ID stored in the Vault can now be part of the “Delete Person” process
- Deleting the id removes it from the vault
  - Marking it inactive leaves it in the vault but inaccessible



# Deleting an ID Vault

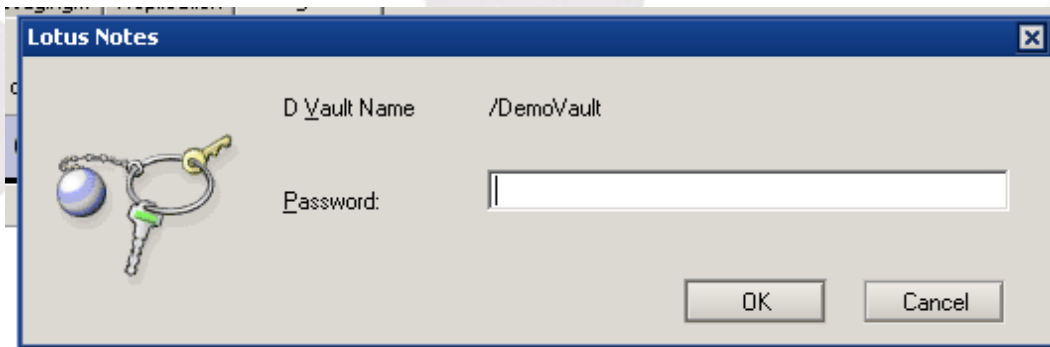
The screenshot shows the IBM Security Administrator console. On the left is a tree view with categories like Server, Messaging, Replication, Directory, Security, Certificates, ID Vaults (highlighted), Policies, Web, Monitoring Configuration, Health Monitoring, Cluster, and Miscellaneous. In the center is a table with three columns: Vault Name, Administration Server, and Description. The table contains one entry: DemoVault, SNT85/demo, and The primary vault for the demo certifier. On the right is a menu for ID Vaults with options: Create..., Manage..., Delete... (highlighted), and Password Reset Authority...

Vault Name	Administration Server	Description
DemoVault	SNT85/demo	The primary vault for the demo certifier

- Select the ID Vault document in Administrator
- If the vault is a replica choose 'Manage' and then "Manage Vault Replicas"
- If it's the primary ID Vault then choose 'Delete' from the ID Vaults menu
  - Make sure you have removed all other replicas via ID Vault - Manage - Manage Vault Replicas first

# Deleting an ID Vault

- Enter the password for the ID Vault when prompted



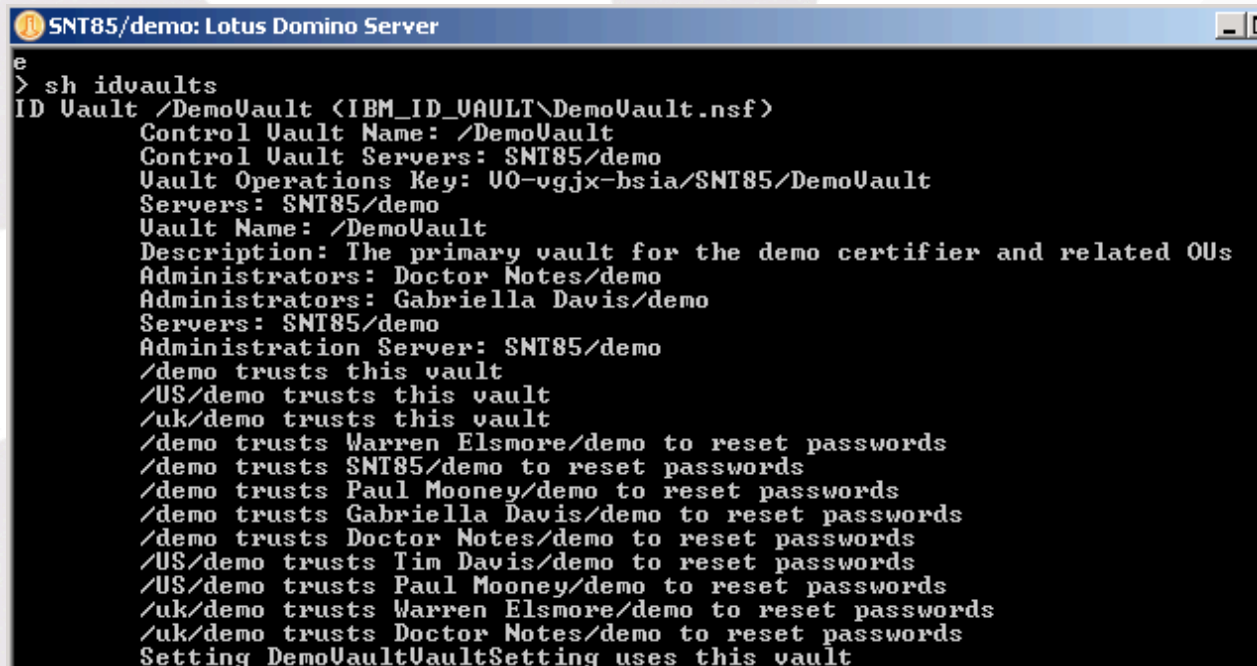
- The ID Vault is deleted by the server
  - If the database is open the ID Vault will try to delete it later
  - It will try once a day
  - “show idvaults” on the server console will also force a retry

# Deleting an ID Vault - What Happens

- The database in the IBM\_ID\_Vault directory is deleted
- Deletes all Vault Trust Certificates for the vault from the Security - Certificates view of the Domino Directory.
- Deletes the vault document from the Security - ID Vaults view of the Domino Directory.
- Removes the vault name from all Security Settings documents that specify it.

# ID Vault Problems or Status

- On server console type “sh idvaults”



```
SNT85/demo: Lotus Domino Server
e
> sh idvaults
ID Vault /DemoVault <IBM_ID_UAULT\DemoVault.nsf>
  Control Vault Name: /DemoVault
  Control Vault Servers: SNT85/demo
  Vault Operations Key: UO-vgjx-bsia/SNT85/DemoVault
  Servers: SNT85/demo
  Vault Name: /DemoVault
  Description: The primary vault for the demo certifier and related OUs
  Administrators: Doctor Notes/demo
  Administrators: Gabriella Davis/demo
  Servers: SNT85/demo
  Administration Server: SNT85/demo
  /demo trusts this vault
  /US/demo trusts this vault
  /uk/demo trusts this vault
  /demo trusts Warren Elsmore/demo to reset passwords
  /demo trusts SNT85/demo to reset passwords
  /demo trusts Paul Mooney/demo to reset passwords
  /demo trusts Gabriella Davis/demo to reset passwords
  /demo trusts Doctor Notes/demo to reset passwords
  /US/demo trusts Tim Davis/demo to reset passwords
  /US/demo trusts Paul Mooney/demo to reset passwords
  /uk/demo trusts Warren Elsmore/demo to reset passwords
  /uk/demo trusts Doctor Notes/demo to reset passwords
  Setting DemoVaultVaultSetting uses this vault
```



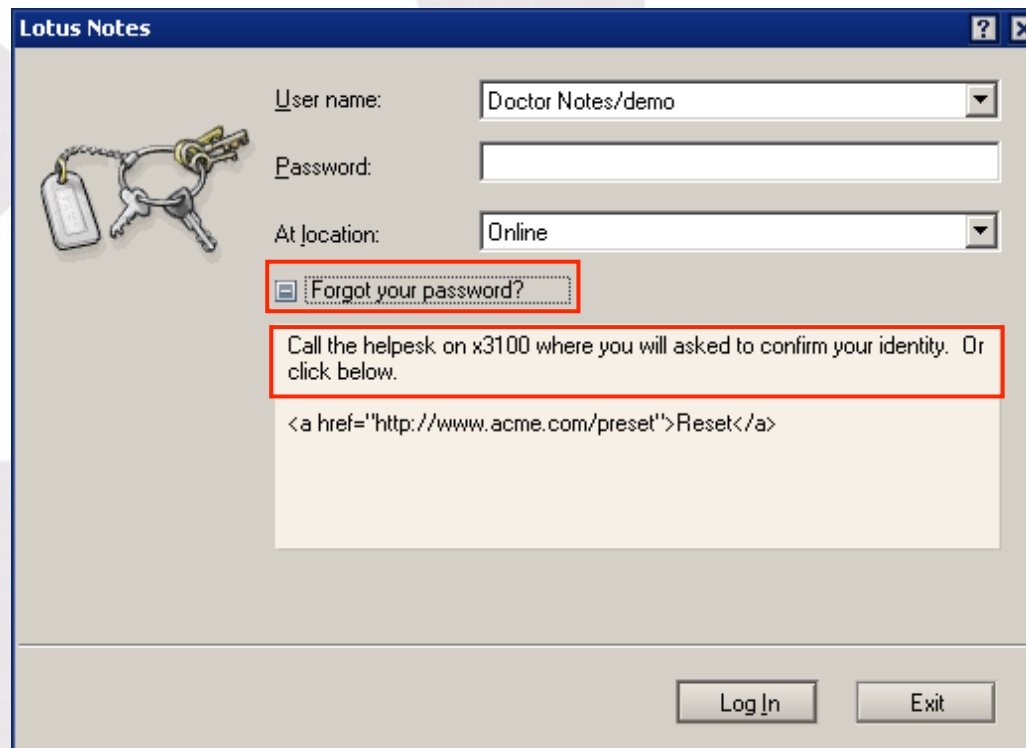
# Possible Reasons Why an ID Wouldn't Be Stored In The Vault

- Client isn't 8.5x
  - upgrade
- Local names.nsf isn't 8.5x
  - replace design
- No security policy exists for that user
  - check \$policies view in local names.nsf
- Notes.ini problems
  - verify keyfilename= matches the id being used
  - remove all ID Vault references already in notes.ini

# Resetting Passwords



# User Interface When Forgetting Their Password



The screenshot shows the Lotus Notes login window. On the left is an icon of a keychain. The login fields are: 'User name:' with a dropdown menu showing 'Doctor Notes/demo', 'Password:' with an empty text box, and 'At location:' with a dropdown menu showing 'Online'. Below these fields is a link labeled 'Forgot your password?' which is highlighted with a red rectangle. Below the link is a text box containing the instruction: 'Call the helpesk on x3100 where you will asked to confirm your identity. Or click below.' followed by a link: '<a href="http://www.acme.com/preset">Reset</a>'. At the bottom right are two buttons: 'Log In' and 'Exit'.

Lotus Notes

User name: Doctor Notes/demo

Password:

At location: Online

[Forgot your password?](#)

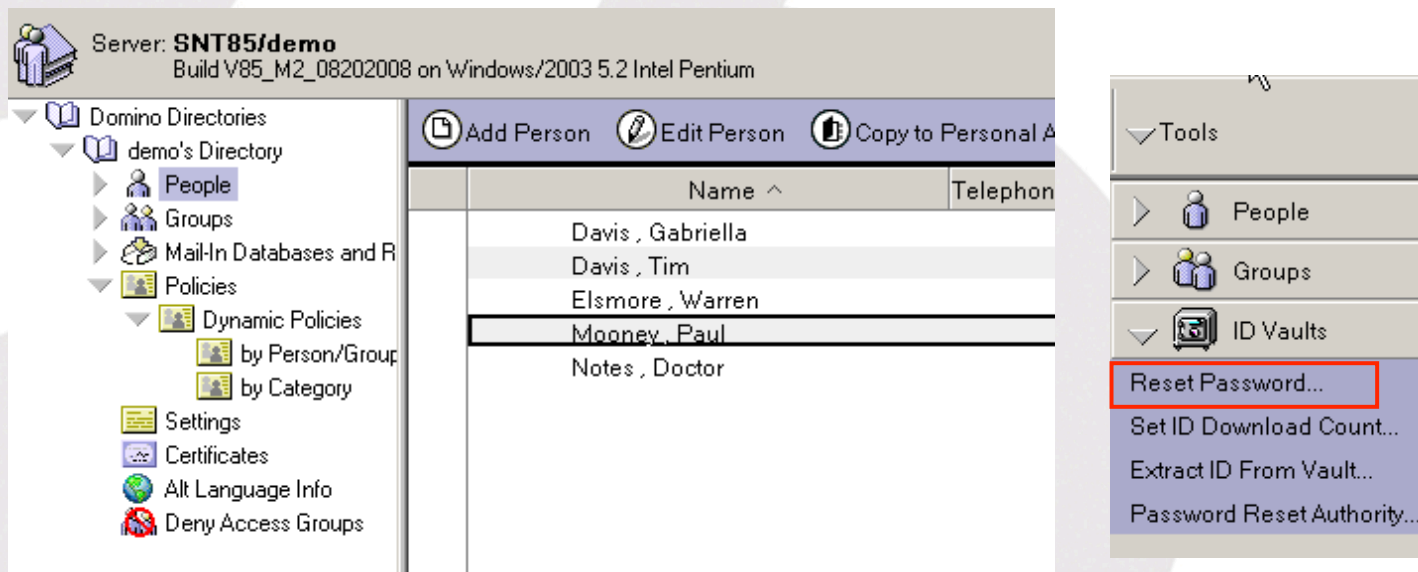
Call the helpesk on x3100 where you will asked to confirm your identity. Or click below.

[Reset](http://www.acme.com/preset)

Log In Exit

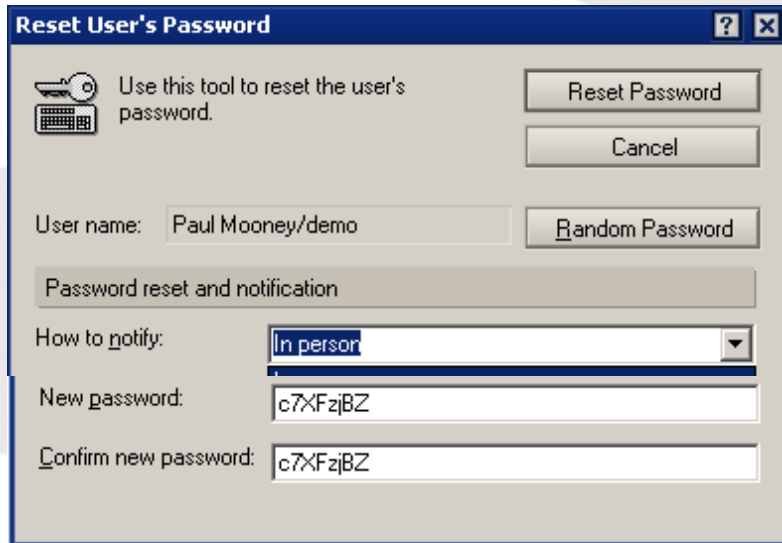
# To reset a user password as an authority

- Domino Administrator - People and Groups Tab
  - Select a Person
  - Tools - ID Vaults - Reset Password



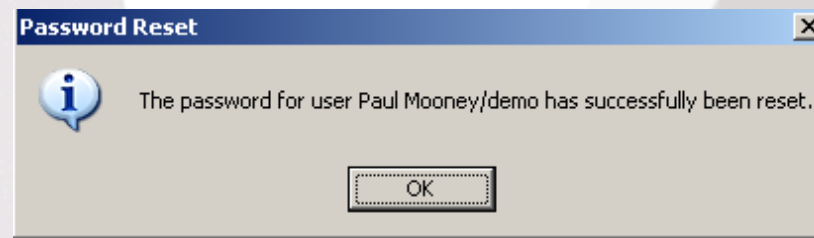


# To reset a user password as an authority



The 'Reset User's Password' dialog box contains the following elements:

- Icon of a key and keyboard.
- Text: "Use this tool to reset the user's password."
- Buttons: "Reset Password" and "Cancel".
- Text: "User name: Paul Mooney/demo"
- Button: "Random Password"
- Section: "Password reset and notification"
- Text: "How to notify:"
- Dropdown menu: "In person" (selected)
- Text: "New password: c7XFzjBZ"
- Text: "Confirm new password: c7XFzjBZ"



- When resetting a user password you have the option of
  - Notifying the user in person
  - Emailing an encrypted message to their Manager with the password enclosed
- Once you've reset the password the user can use this new one to login

# Autoprocessing Reset Password Requests

- A sample password reset application is available on the server
  - open `pwdresetsample.nsf`
  - set -Default- to Editor in the ACL
  - set whoever is to be the agent signer as 'Manager' in the ACL
  - sign the agent with the 'Manager's id
- Put a copy of the database on any server you want to enable password reset on
  - These needn't be ID Vault servers but they must run HTTP
- Ensure the agent signer has the right to run restricted lotuscript agents on those servers
  - That setting is in the server document - security tab

# Autoprocessing Reset Password Requests

- Each server id the database is installed on and the agent signer id must be configured as Password Reset Authorities in the ID Vault
  - They must also have the checkbox “Self Service Password Reset Authority selected”
- To request a password reset the user browses to
  - <http://servername/pwdresetsample.nsf>



The screenshot shows a web form titled "Reset User Password - Web Sample" with the IBM logo. It contains two input fields: "Enter new password:" and "Confirm new password:". Below these fields is a button labeled "Reset My Password".

- Obviously you need to know your HTTP password to reset your Notes ID password



# So a summary of the good stuff.....

- ID Vault means user ids are held securely and encrypted on Domino servers and not in the Domino Directory or on a file server somewhere
- Since ID Vault downloads the ID for each user as they log in you don't need to distribute ids to the desktops for new users
- You also don't need to worry about ids being kept in sync since ID Vault takes care of that too
  - if the user changes their password or their id it is uploaded to the ID Vault in the background and downloaded to their other machines when they go to use them
- User renames and certificate rollovers no longer require any user involvement
- Passwords can be reset by helpdesk people with no access to the ids themselves and no knowledge of existing passwords



# You know there has to be a BUT.....

- If the user ID is stored in a mail file, the ID Vault can only update that in v8.5.1 or later
- Smartcard enabled ids can't be stored in the ID Vault
- A Vault must be contained within a single Domino Domain
- All users of a Vault must be in that Domain
- If a client isn't connected to the network the ID from the vault can't download so if they change their password in the office and then work offline at home - their id will still have the old password until they sign online
- If you use the CA process the id that is stored in ID Vault on registering a user doesn't contain the hierarchical certificate and will not be usable when it downloads to the workstation on setup
  - You need to switch to that user's id and access the server so the certificates are updated and a new copy of the ID is sent to the vault

# Contact Details

- Gabriella Davis
- [gabriella@turtlepartnership.com](mailto:gabriella@turtlepartnership.com)
- <http://blog.turtleweb.com>
- Gabriella Davis on Skype, LotusLive etc
- Nerd Girl Community on LinkedIn