Notes Domino 8.5

Notes ID Vault and Notes Shared Login

Tony Wehrstein
Certified Senior IT Specialist
SWG IBM Switzerland

Top Sheet

- This module describes the Notes ID Vault and Notes Shared Login features on Notes/Domino 8.5
  - The **Notes ID Vault** is an optional, server-based database that holds protected copies of Notes user IDs allowing administrators and users to easily manage Notes user IDs.
  - **Notes Shared Login** allows users to start their Notes client without having to provide Notes passwords.
- Benefits
  - These features offer a potential reduction in total cost of ownership (TCO) by simplifying Notes identity management
- Opportunities
  - This feature would be useful for any organization that has a large number of Notes user IDs to manage.
- Comparison with competition
  - Notes ID files have been a key consideration in managing end-user costs and administrator workload. However they have also been the key to Notes/Domino's highly secure reputation which distinguish us from the authentication systems of competitors' products.

Agenda – Notes ID Vault

- What is a Notes ID Vault
- Why deploy a Notes ID Vault
- Notes ID Vault Creation, Configuration and Clustering
- Operations on the Notes ID Vault
- Understanding Vault Security
- Password Reset Deployment Recommendations
- Requirements and Limitations
- Compatible Features and Processes
- Audit Tracking and Monitoring

What is a Notes ID Vault

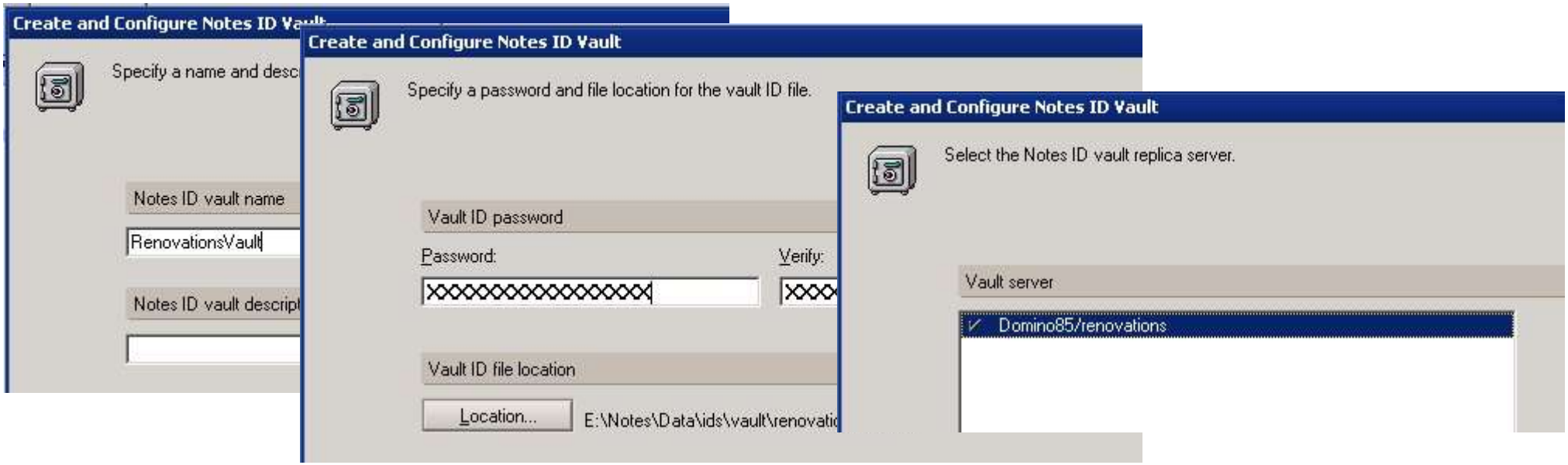
- The Notes ID Vault is an optional, server-based database that holds protected copies of Notes user IDs
  - Uploading copies of ID files for existing users
  - Adding ID files to vault during registration of new users
  - Resetting of passwords when forgotten
    - Help desk
    - Self service applications
  - Synchronization of ID files across multiple computers
    - Future integration with iNotes/Blackberry planned post 8.5
    - Recommended for use with new File Server Roaming
  - Auditor function to gain access to encrypted data
    - Requires administrator access to server, vault administration rights (manager in vault db ACL), auditor role
    - Can be disabled using SECURE_DISABLE_AUDITOR=1 in notes.ini
  - Marking of ID files as “Inactive”
    - via adminp when deleting users
    - directly in vault

Why Deploy Notes ID Vault?

- Can replace time-consuming, expensive ID file and password recovery systems, giving potential for significant reduction in user downtime and help desk costs
  - Simplifies provisioning of Lotus Notes ID credentials
  - Streamlines process for resetting forgotten passwords
    - Help desk options
    - Programmatic interfaces for self-service password applications
  - Automates ID file maintenance
    - ID file synchronization
    - ID renames
    - ID key rollovers
    - ID file replacement due to loss or corruption
- Supports processes for legal discovery/access to encrypted data, potentially preventing the loss of valuable information

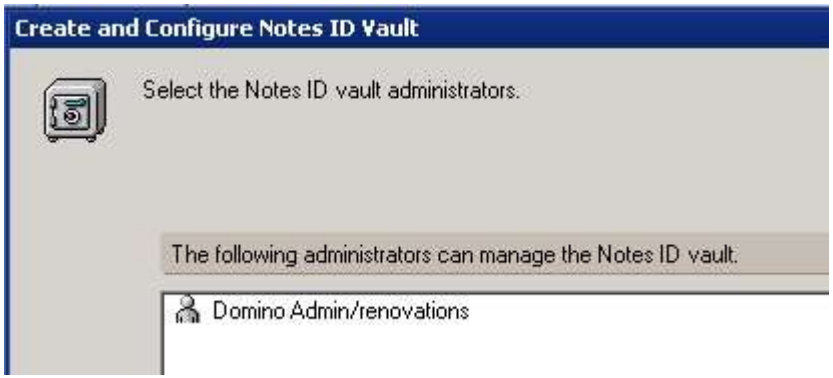
Notes ID Vault Creation

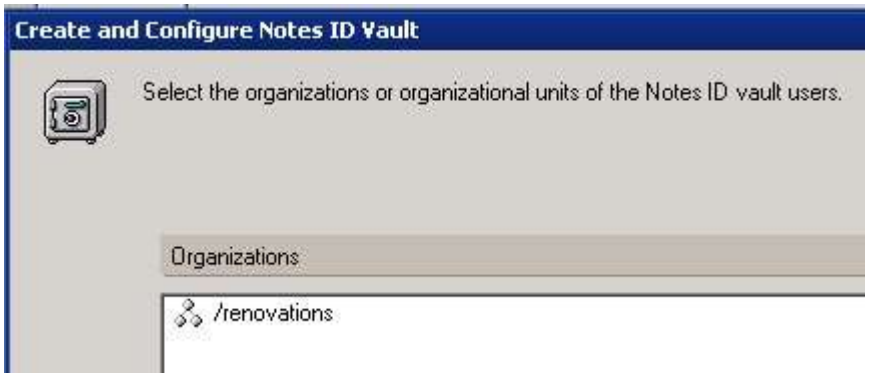
- "Tools > ID Vaults > Create" from Configuration tab
- Specify a name for the vault – used for
  - Hierarchical name of vault
  - Database file name
  - Vault ID file (used when adding or removing vault replicas)
- Specify password for vault ID
- Select server on which to deploy vault

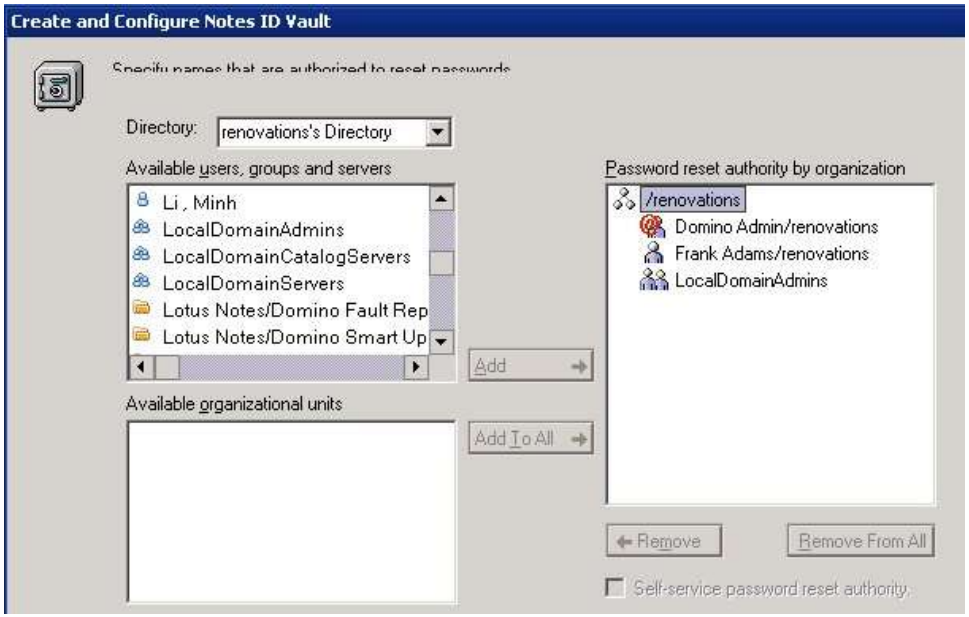


Notes ID Vault Creation continued

- Select at least one vault administrator
  - Add / remove vault servers
  - Delete ID files from the vault
  - Add / remove other administrators
- Select organizations or organizational units whose IDs will be stored
  - Need access to certifier IDs
  - Vault Trust certificates are created for each certifier and stored in Domino Directory
  - Only IDs registered with these certifiers can be uploaded to the vault
- Select user names that are authorized to reset passwords
  - Password Reset certificate is created for each user
  - Include IDs associated with any self-service password reset application

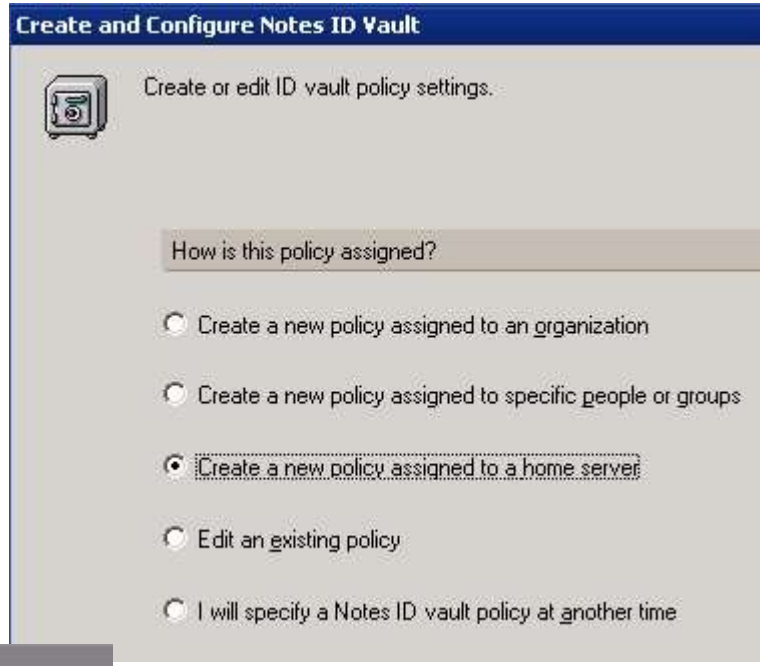


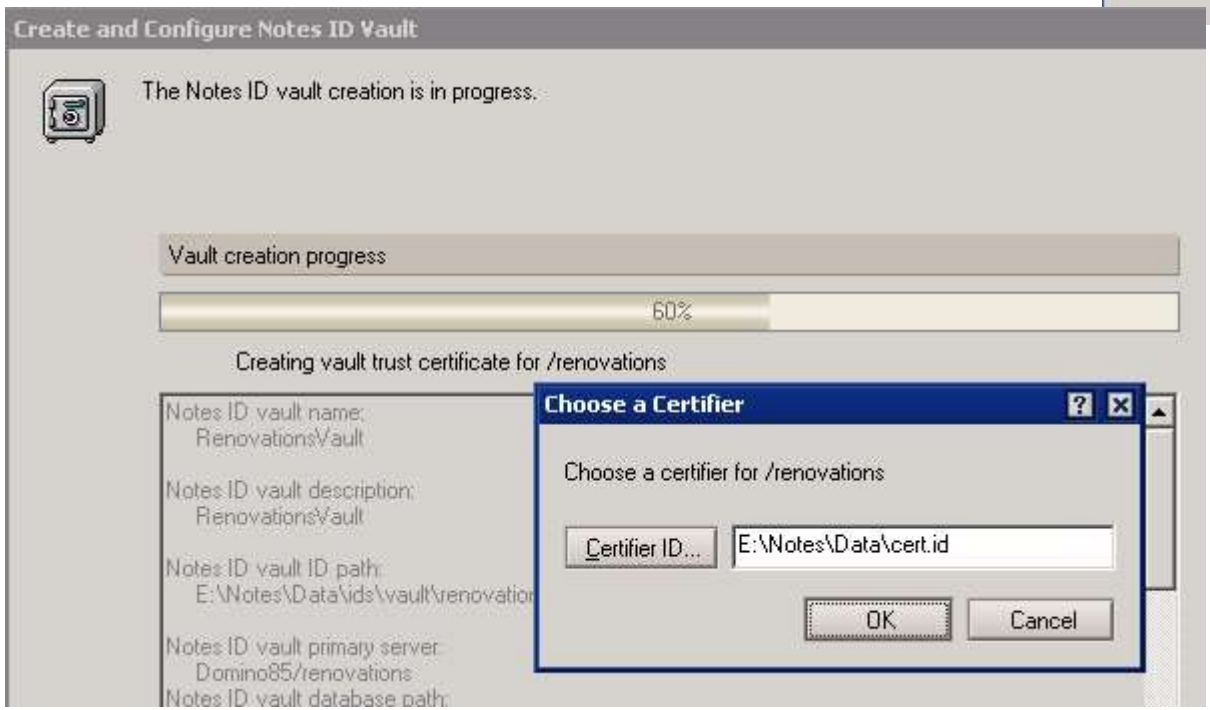




Notes ID Vault Creation continued

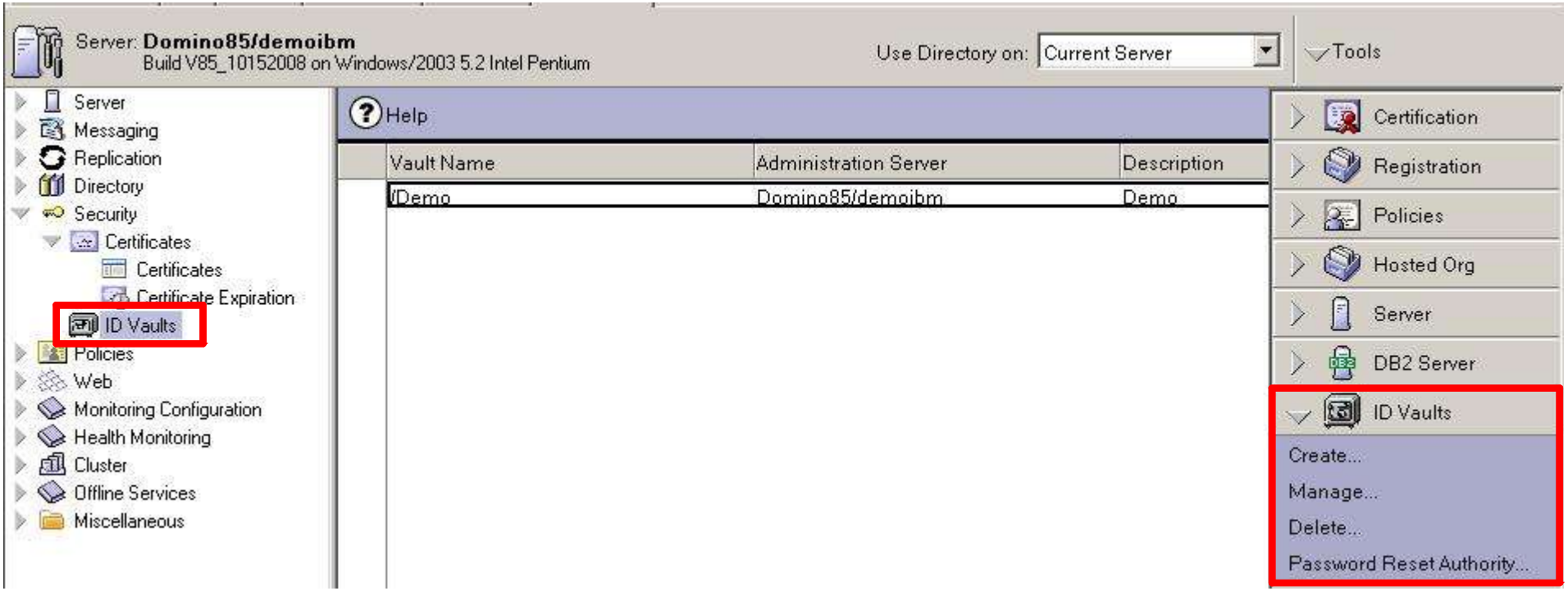
- Create ID vault policy
  - Create new
  - Edit existing
  - Skip and create later
- Create Vault
  - Locate certifier IDs





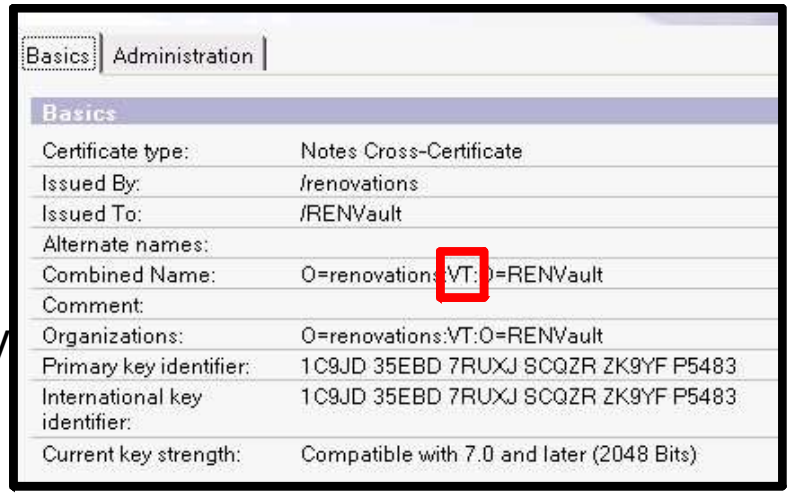
Notes ID Vault Creation Complete

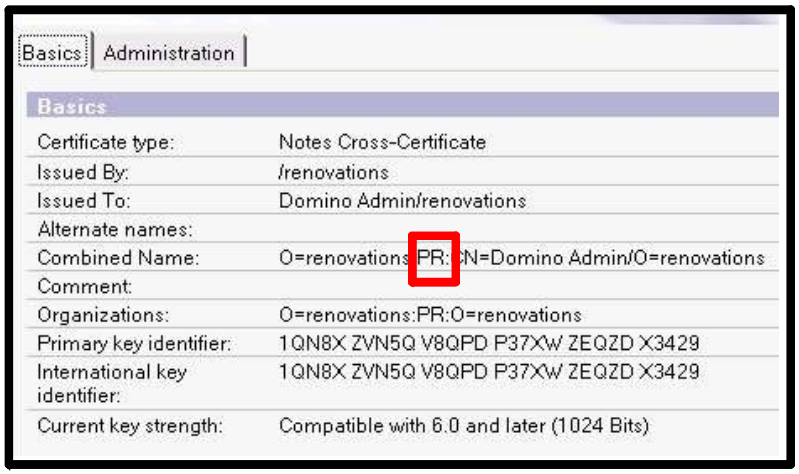
- Vault ID
  - On vault creators desktop
  - Should be secured like a certifier ID
  - Needed to create vault replicas
- ID Vault Directory Entry
  - From where ID vault can be managed



Notes ID Vault Creation Complete continued

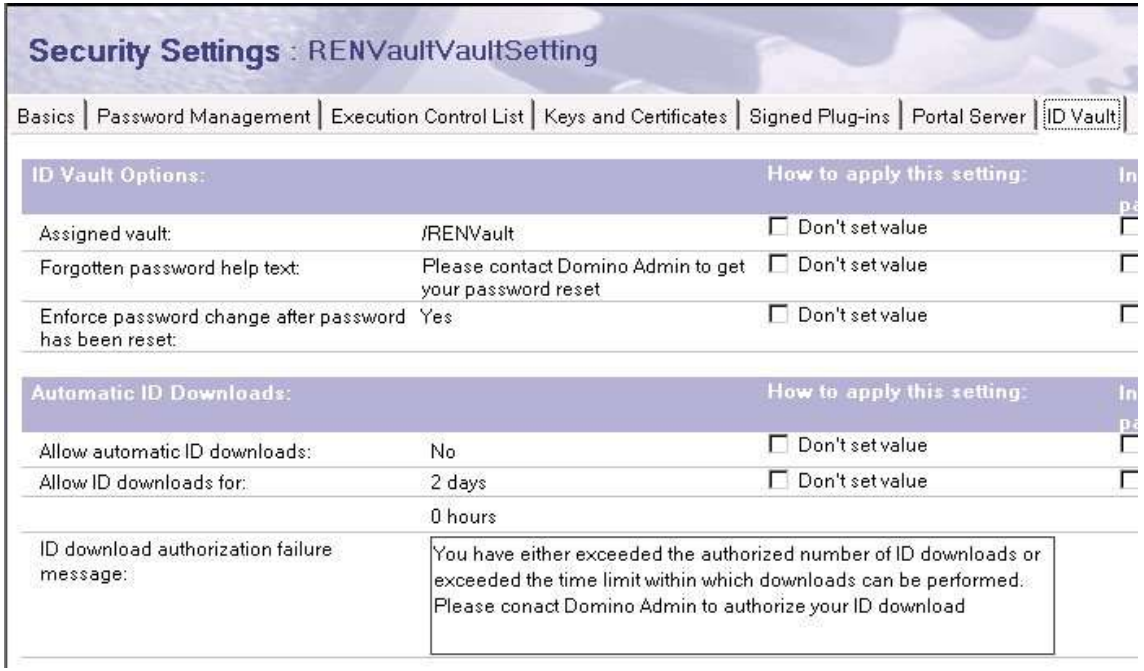
- ID Vault application
  - Stored on hosting Domino server
  - Encrypted with hosting Domino server ID
- Vault Trust Certificate
  - Notes Cross-Certificates stored in Domino Directory
  - One for each registered certifier
- Password Reset Certificates
  - Notes Cross-Certificates stored in Domino directory
  - One for each user or application authorized to reset passwords
- Policy Settings
  - If selected during Vault install
  - In new or existing policy document





Notes ID Vault Configuration

- Security Settings > ID Vault tab
  - Hierarchical name of vault
  - Forgotten password help text
  - Enforce password change
  - Automatic ID downloads
    - Time limit
    - Failure message
- Person document > ID Vaults
  - Number of downloads

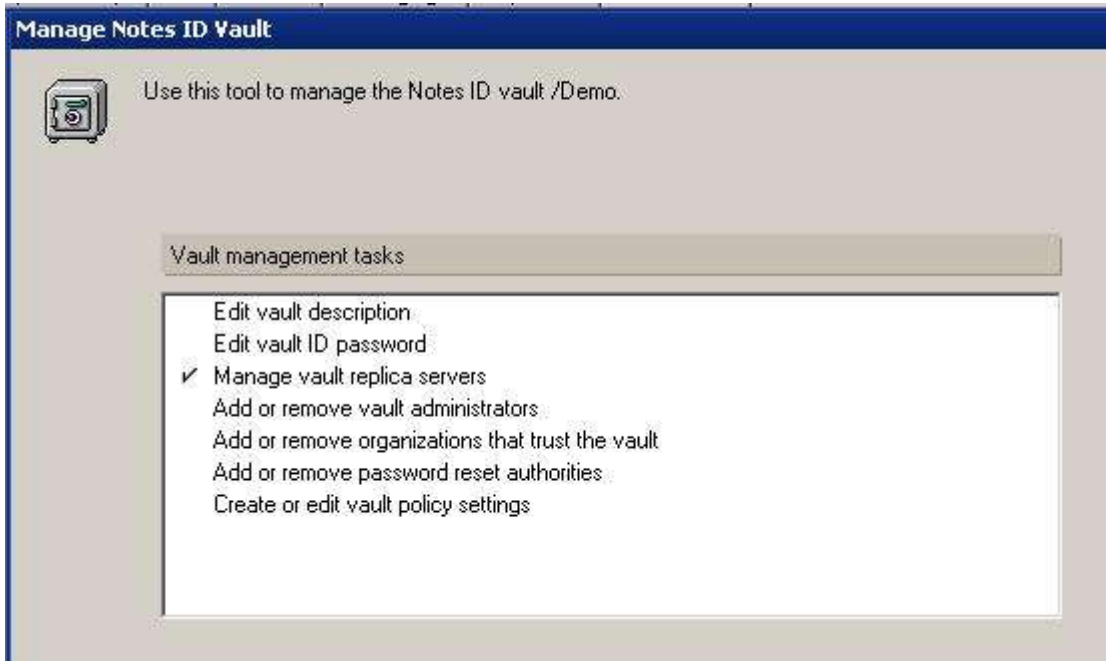


Notes ID Vault Application

- Application is encrypted with the host server's ID
- ACL
  - Vault Administrators - Manager
  - Vault server - Manager
  - No access required for anyone else
- Record per ID
  - Modification time
  - Download limit
  - User ID (encrypted)

Vault Replicas

- First vault
  - ID Vaults > Create
  - Primary Vault Server
  - Carries out key vault operations
    - Name changes
    - Key rollover
  - Last replica to be deleted
  - Checkmark in ID Vaults > Manage

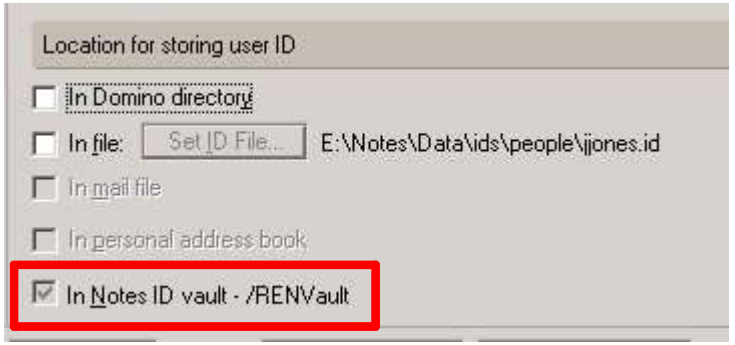


- Additional vault replicas
  - ID Vaults > Manage
  - Do not use Create Replica tool

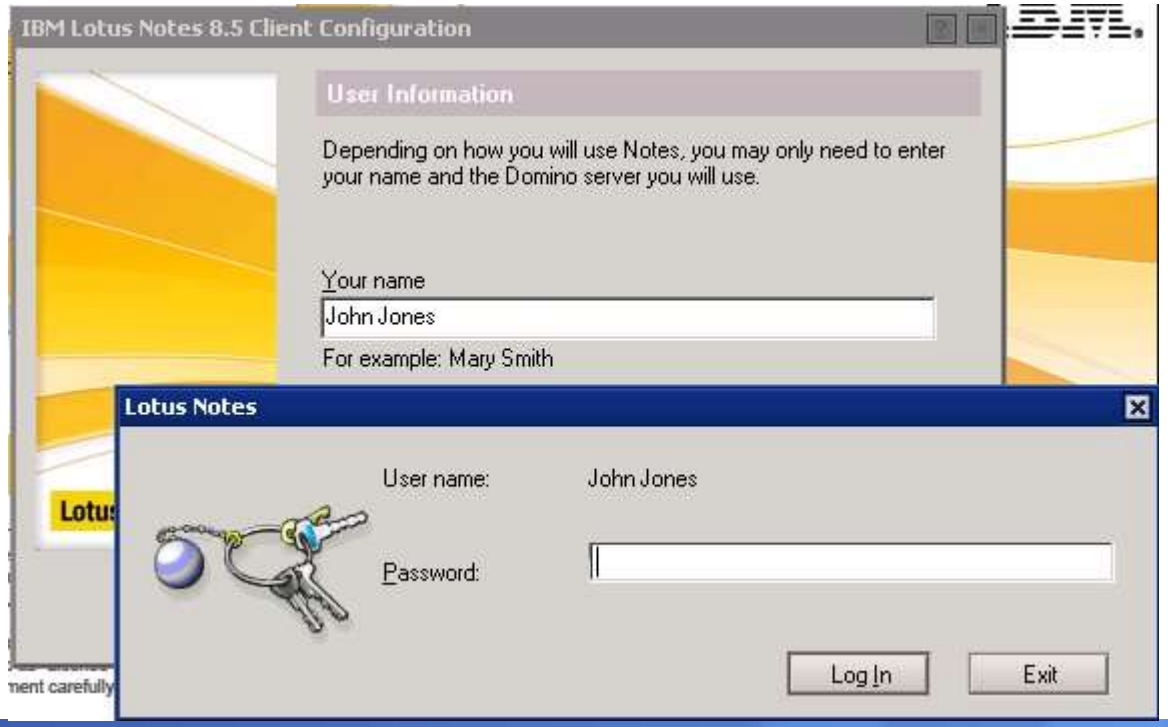
- Console command – show idvaults

Operation – Adding New Users to Vault

- Register new user
  - Select Vault policy in Basics tab
  - Vault will be automatically selected in ID Info tab



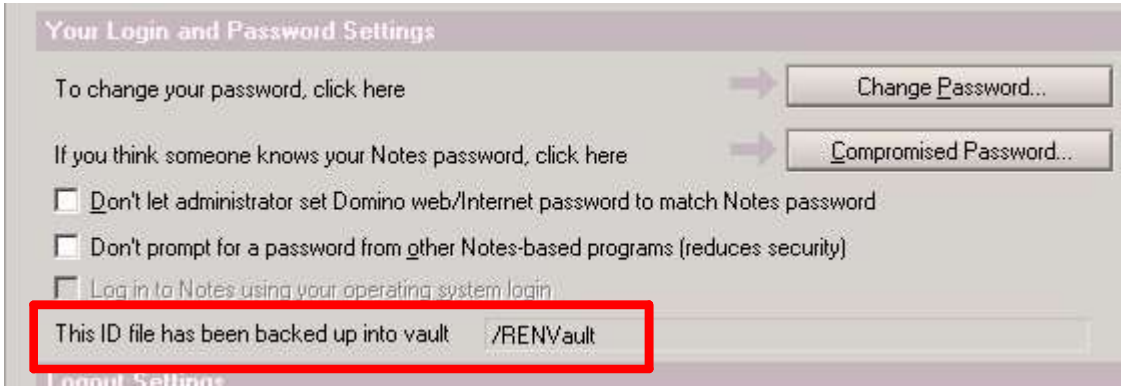
- During new user setup
  - User enters their name
  - Server identifies user as having ID in vault and prompts for password
  - Correct password results in ID being downloaded to desktop



Operation – Adding Existing Users to Vault

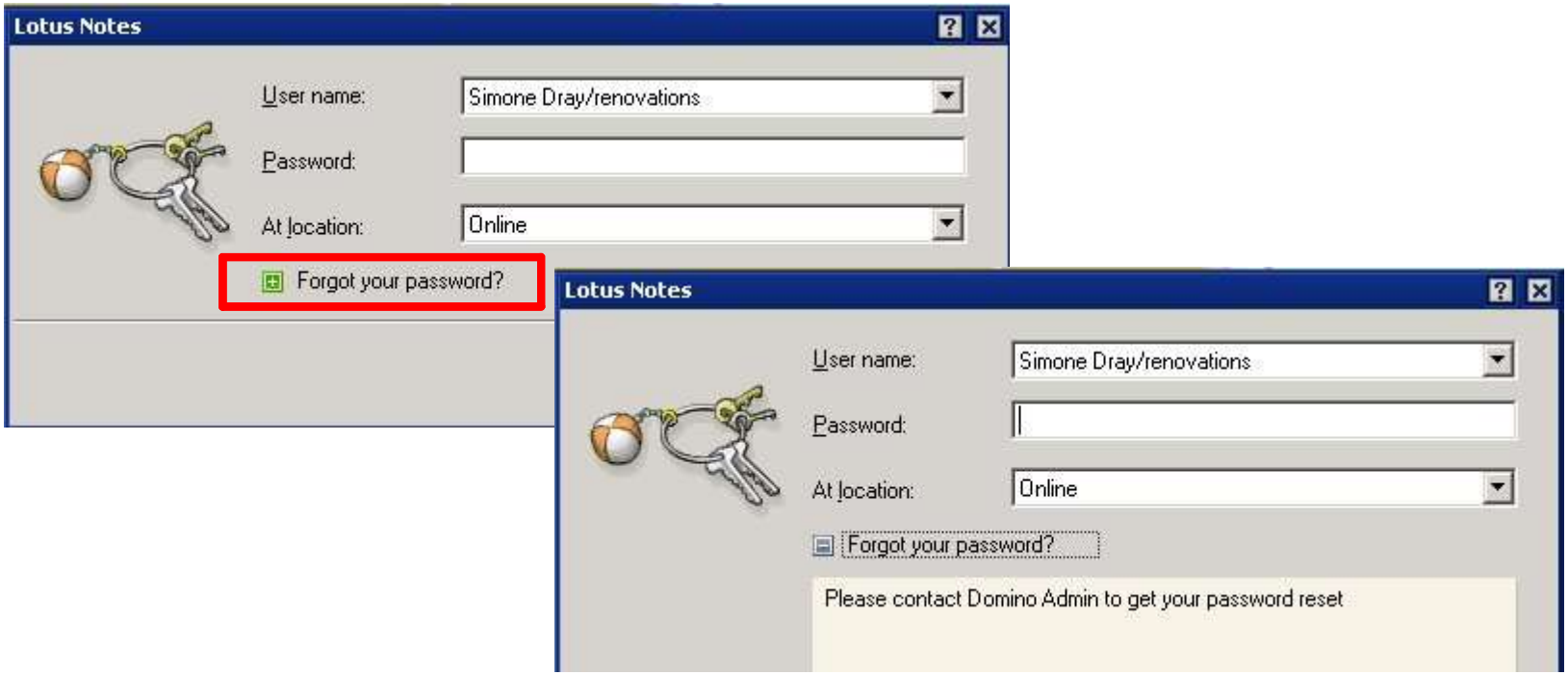
- Add user to policy
  - In person document
  - Or via policy assignment tab

- User logs into Notes
  - ID is uploaded in background
  - User Security Settings indicate ID has been uploaded to vault



Operation – Forgotten Password

- User clicks on link on login dialog



- User receives instructions to get password reset
  - Contact an administrator
  - Or use a custom-built self-service application

Operation – Resetting Password - manual

- Operator
  - Needs to verify user's identity
  - Requires Password Reset Certificate
  - Resets password from Person Document
  - Does not need access to Vault
  - Does not need access to ID file

- User
  - Enters new password
  - Can be prompted to change password immediately

Operation – Resetting Password - automated

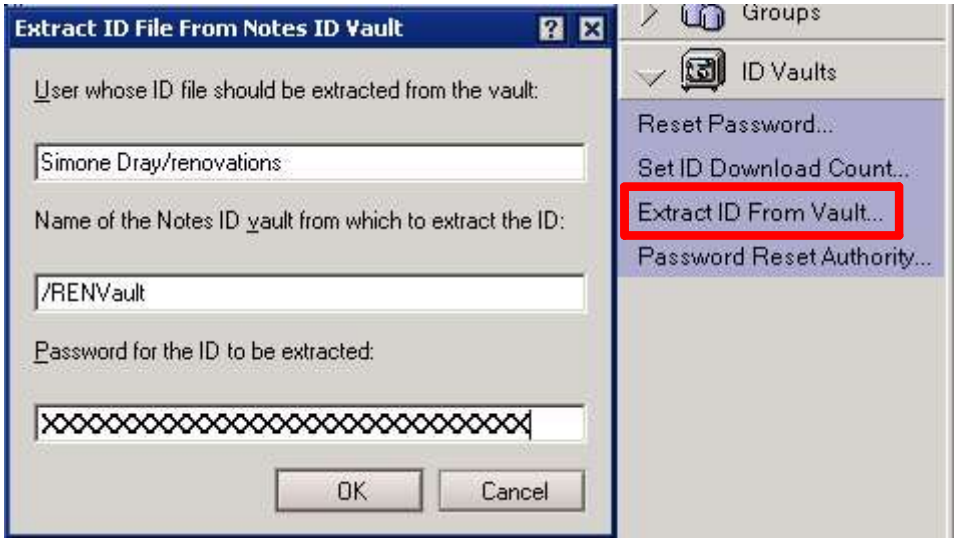
- Custom Application
  - Help Desk Application
  - Self-service application
- ResetUserPassword method
  - available in C, Java, JavaScript or LotusScript
  - only API call currently exposed
    - i.e: you cannot develop custom program to extract IDs
- Sample self-service application
  - code snippet supplied with Domino 8.5
  - uses the ResetUserPassword method in a LotusScript agent
  - can be used as basis for own application

Operation - Synchronizing IDs

- Synchronization Scenarios
  - Name change
  - Key Rollover
  - Password Change
  - Encryption Keys
- Vault treats synchronization and download differently
  - Synchronization: Client has the ID and password
  - Download: Client only has the password
- Synchronization occurs
  - At login
  - Immediately (if local ID change is made when user is online)
  - Polling interval (if local ID change is made when user is offline

Operation – Extracting ID from the vault

- Provide user with physical copy of ID
  - Extract ID from Person view
  - Supply current password for ID
  - Extract ID from Person document



- Supply copy of ID for Auditor
  - User should be unaware of access
  - Operator requires Auditor role
  - Extract ID from Person view
  - Don't supply current password (presumably not known)
  - Supply new password to be used by Auditor

Operation - Recovering ID

- ID deleted or corrupted
  - Remove corrupted ID
  - Ensure user can download a new ID
    - Automatic downloads set to Yes or
    - Number of downloads allowed set to greater > 0
  - User logs in and new copy of ID is downloaded

- ID lost or stolen
  - Reset password on the ID in the vault
  - Roll over the keys on the ID
  - Ensure that server key checking is enabled
  - Ensure user can download a new ID
  - User logs in and new copy of ID is downloaded

Understanding Vault Security

- Protection against the use of an unauthorized vault
  - Creation of vault trust certificate requires access to certifier ID(s)
- Protection against unauthorized:
  - Upload of IDs
    - Only IDs registered by authorized certifiers can be uploaded
    - Only IDs specified via policy will be uploaded
  - Downloads of IDs
    - Failed password attempts restricted to 10 per day (configurable)
    - Option to require authorization for all downloads
  - Password resets
    - Requires password reset certificate
    - Creation of password reset certificate requires access to certifier ID
  - Access to vault contents
    - Attached IDs are encrypted in vault
    - All encryption/decryption done in memory – no storage of IDs on disk
  - Access to data transmitted over network
    - ID vault transactions are encrypted

Password Reset Deployment Recommendations

- Issue password reset certificates to a small number of highly trusted individuals
- Issue a password reset certificate to an entire “helpdesk OU”
  - Renaming people into and out of that OU will grant/deny access
- Issue special IDs for resetting passwords
  - Administrators switch to these IDs to perform password reset tasks
- Issue a single password reset certificate to an application and give the help desk access to that application
  - Easy to add and remove people from that ACL
  - Can add supplemental logging and auditing

Requirements

- All replicas of a vault must be located within a single Domino domain
  - All vault users must have home servers in that domain too
  - Multiple organizational certifiers within a single domain can be supported though
- All servers participating in the ID Vault processes must be Domino 8.5
  - Administration server
  - Vault server
  - User home servers
    - if clustered, at least one server in the cluster must be Domino 8.5
- Only users of Notes 8.5 clients will have their IDs uploaded to an ID vault

Limitations

- Both ID Vault and ID Recovery can be used within the same domain
  - but individual Notes IDs can only be associated with one of the processes
- No ability for iNotes users to synchronize vault IDs with IDs stored in mail files
  - Planned for future release
- Notes Single Logon is not supported with ID files using the vault
  - Consider using Notes Shared login instead
- The following cannot be stored in a Vault
  - ID files with multiple passwords
  - Certifier and Server IDs cannot be stored in Vault
  - Smartcard-enabled IDs cannot be stored in a vault

Compatible Features and Processes

- CA Process can be used for upload of IDs during user registration
  - but initial creation of Vault requires access to physical copies of certifiers
- Roaming Users
  - Automatic downloads should not be restricted
- Notes Shared Login
- Password Checking
- HTTP password synchronization
- Public Key Checking
  - Select the "Enforce key checking for Notes users and Domino servers listed in trusted directories only" setting in the Server document
- User Renames
  - Performed on IDs in the vault and synchronized to the user's local ID file.
- User Key Rollover
  - Performed on IDs in the vault and synchronized to the user's local ID file.
  - Option for users to create new public keys from a Notes client is disabled

Audit Tracking and Monitoring

- ID vault events are reported to
  - Security Events view of the client and server log file (LOG.NSF)
  - Domino Domain Monitor database (DDM.NSF)

Security Events

Time: 17/10 15:36
Elapsed Time: (Unknown) minutes

Events:

17/10/2008 15:36:43 ID successfully downloaded by auditor from vault 'O=RENVault' by 'Simone Dray/renovations' (IP address 9.180.24.227:1057).
17/10/2008 17:55:18 ID for 'Ron Espinosa' (IP Address 9.180.24.227:1106) in vault 'O=RENVault' was not downloaded because the wrong password was supplied. Error: Wrong Password. (Passwords are case sensitive - be sure to use correct upper and lower case.)
17/10/2008 17:55:29 ID successfully downloaded from vault 'O=RENVault' by 'Ron Espinosa' (IP address 9.180.24.227:1106).
17/10/2008 17:56:15 ID successfully synchronized with vault 'O=RENVault' for 'Ron Espinosa/renovations' (IP Address 9.180.24.227:1114).
17/10/2008 17:57:07 ID for 'Ron Espinosa/renovations' (IP Address 9.180.24.227:1120) in vault 'O=RENVault' was not downloaded because the wrong password was supplied. Error: Wrong Password. (Passwords are case sensitive - be sure to use correct upper and lower case.)
17/10/2008 17:59:45 Password for 'Ron Espinosa/renovations' with 0 downloads was reset by 'Domino Admin/renovations' (IP Address 9.180.24.227:1136) from process nSERVER.
17/10/2008 18:01:12 ID for 'Ron Espinosa/renovations' (IP Address 9.180.24.227:1142) in vault 'O=RENVault' was not downloaded because the wrong password was supplied. Error: Wrong Password. (Passwords are case sensitive - be sure to use correct upper and lower case.)
17/10/2008 18:02:50 Password for 'Ron Espinosa/renovations' with 0 downloads was reset by 'Domino Admin/renovations' (IP Address 9.180.24.227:1160) from process nSERVER.
17/10/2008 18:03:46 ID successfully synchronized with vault 'O=RENVault' for 'Ron Espinosa/renovations' (IP Address 9.180.24.227:1165).
17/10/2008 18:04:14 ID successfully synchronized with vault 'O=RENVault' for 'Ron Espinosa/renovations' (IP Address 9.180.24.227:1168).

- Server Console Command
  - SHOW IDVAULTS

```
>
>
> sh idvaults
ID Vault /RENVault (IBM_ID_VAULT\RENVault.nsf)
        Control Vault Name: /RENVault
        Control Vault Servers: Domino85/renovations
        Vault Operations Key: VO-usca-sovd/Domino85/RENVault
        Servers: Domino85/renovations
        Vault Name: /RENVault
        Description: Vault for Renovations IDs
        Administrators: Domino Admin/renovations
        Servers: Domino85/renovations
        Administration Server: Domino85/renovations
        /renovations trusts this vault
        /renovations trusts Lukas Geiger/renovations to reset passwords
        /renovations trusts Domino Admin/renovations to reset passwords
        Setting RENVaultVaultSetting uses this vault
```

Notes ID Vault Summary

- In this section of the presentation we covered
  - What is a Notes ID Vault
  - Why deploy a Notes ID Vault
  - Notes ID Vault Creation and Configuration and Clustering
  - Operations on the Notes ID Vault
  - Understanding Vault Security
  - Password Reset Deployment Recommendations
  - Requirements and Limitations
  - Compatible Features and Processes
  - Audit Tracking and Monitoring

Agenda – Notes Shared Login

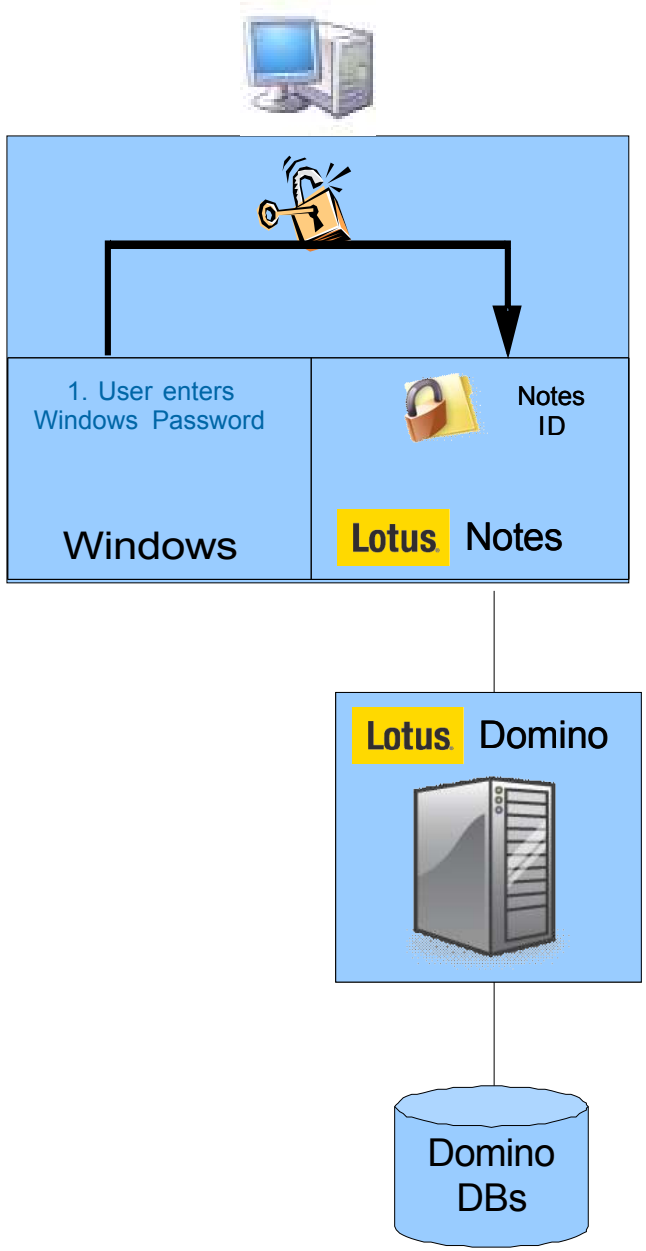
- What is Notes Shared Login.
- How does Notes Shared Login work.
- Enabling & Disabling Notes Shared Login.
- Notifying users when Notes Shared Login is activated or deactivated.
- Limitations when using Notes Shared Login
- When Notes Shared Login cannot be used
- Using Notes Shared Login and Notes ID Vault together
- Troubleshooting

What is Notes Shared Login

- Notes Shared Login allows users to start IBM Lotus Notes without having to provide Notes passwords. Instead, they only need to log in to Microsoft Windows using their Windows passwords.
- Added value to the End Users:-
  - Users need to remember only their Windows passwords.
  - Notes Shared Login works without interruption when Windows passwords are changed either by users or by administrators on a Windows domain controller.
  - Administrators use policies to control who uses the feature and whether its use is required or optional.

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

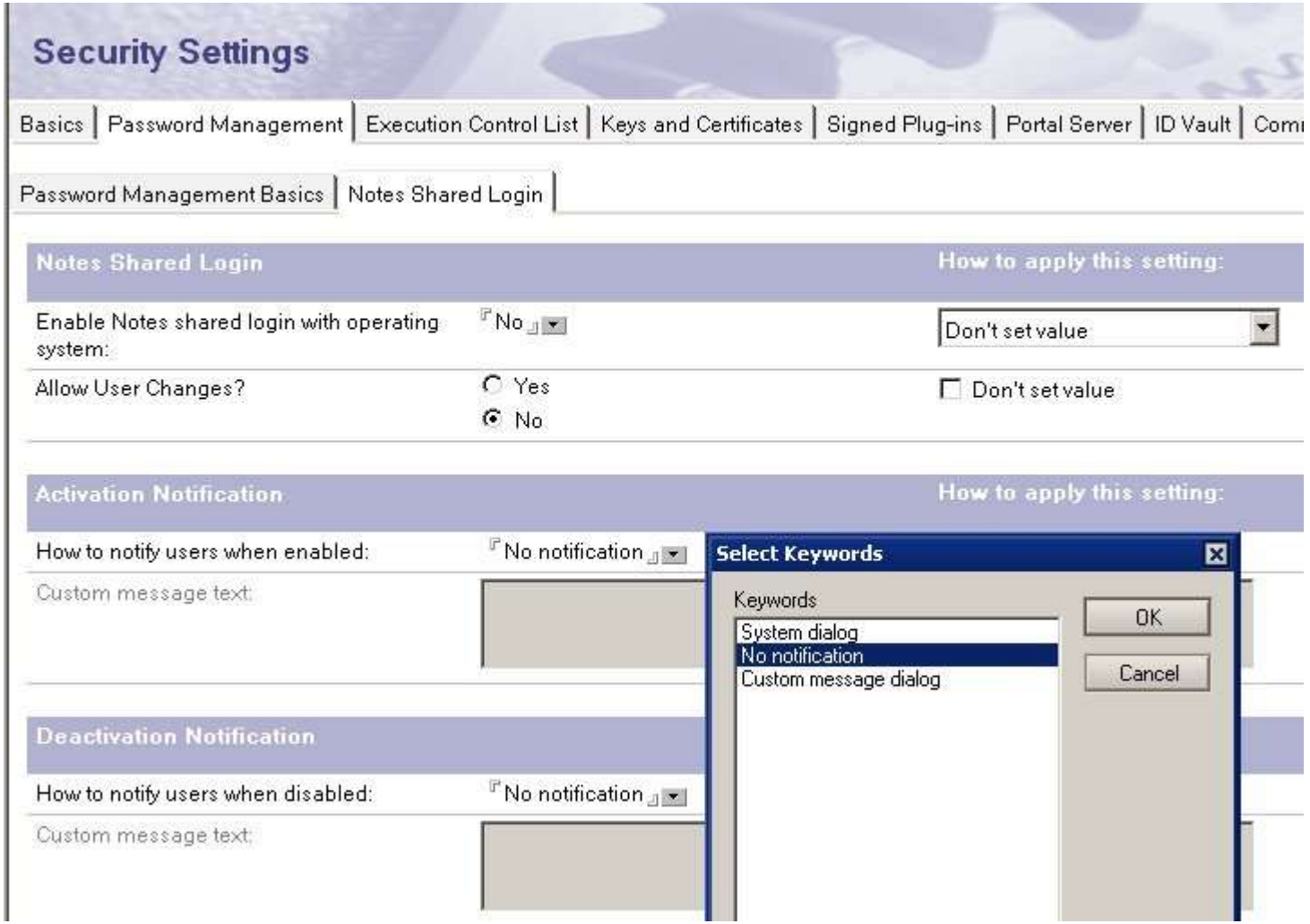


Using Microsoft Data Protection API (DPAPI)

- Windows DPAPI is used to protect ID files that are NSL-enabled
- Steps in process:
  - Generate new secret
  - Encrypt secret with DPAPI (using additional application specific entropy)
  - Save encrypted secret in user's profile directory
  - Encrypt ID file with bulk key derived from secret
  - Save updated ID file

Enabling & Disabling Notes Shared Login.

- The feature is disabled by default.

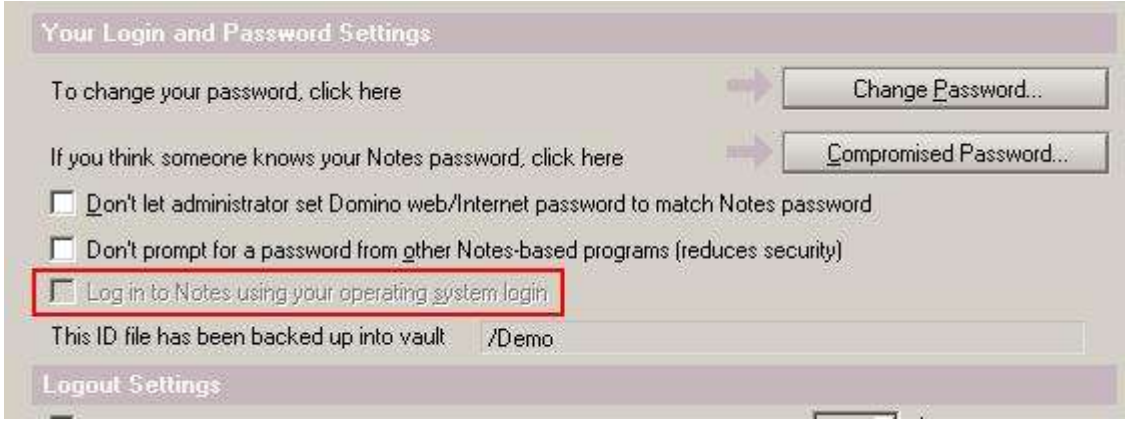


Notes Shared Login Configuration Options

NSL Configuration	Policy Setting Values
NSL is disabled: Users cannot change NSL state.	Enable NSL = No How to Apply = Set value whenever modified Allow user changes = No
NSL is enabled: Users cannot change NSL state.	Enable NSL = Yes How to Apply = Set value whenever modified Allow user changes = No
NSL is initially disabled: Users can change NSL state via User Security dialog.	Enable NSL = No How to Apply = Set initial value Allow user changes = Yes
NSL is initially enabled: Users can change NSL state via User Security dialog.	Enable NSL = Yes How to Apply = Set initial value Allow user changes = Yes

What the user sees...

- Before Notes Shared Login is enabled
  - Password options available
  - Login option unchecked



- After Notes Shared Login is enabled
  - Password options removed
  - Login option checked
  - New option to Copy ID

Limitations when using Notes Shared Login

- The following are not supported
  - Security Settings for policies that relate to Notes passwords
  - The "Check password on Notes ID file" security setting
  - Synchronization of Internet passwords with Notes passwords
- If Notes IDs are stored on a network share, the IDs can be used only from the computers on which shared login is activated.
- To open a Notes Shared Login-enabled ID through the Domino Administrator you must always use the computer and the Windows login name that were used when the ID was Notes Shared Login-enabled.

When Notes Shared Login cannot be used

- Notes Shared Login cannot be used with Notes Single Login
- Notes Shared Login cannot be used on IDs that are:
  - Used on Mac or Linux clients
  - Protected by Smartcards
  - Protected by multiple passwords
  - Used by roaming users
  - Used with Notes on a USB drive
  - Used in a Citrix environment
  - Used on computers with Windows mandatory profiles
  - Enabled for password checking/expiration (unless all servers are 8.5+)
  - Used with Notes to Internet password synchronization
- Notes Shared Login enabled ID cannot be imported into mail file for iNotes/Blackberry access
  - create password protected copy to import

Using Notes Shared Login with Notes ID Vault

- Notes Shared Login and Notes ID Vault are complementary features
  - Management of multiple copies of Notes Shared Login enabled IDs
    - IDs downloaded from vault
    - Notes Shared Login enabled
  - Can be configured in same policy settings document
- IDs participating in Notes Shared Login are stored without a password
  - Require a password reset in order to allow download
  - Different process for ID recovery

ID Recovery when using Notes Shared Login with ID Vault

- ID Recovery (deleted or corrupted ID)
  - Administrator resets password on copy of ID in the vault.
  - User is prompted for the new password when next starting Notes.
  - Copy of the ID file is downloaded to the client from the vault.
  - Notes Shared Login is re-enabled
- ID Recovery (lost or stolen ID)
  - Disable Notes Shared Login in the user policy
  - Force the policy to replicate to all vault servers
  - Process as per an ID that is not Notes Shared Login enabled
    - reset the password on the ID
    - roll over the keys on the ID
    - ensure that server key checking is enabled
  - Re-enable Notes Shared Login

Troubleshooting

- Notes Shared Login writes error/log messages to the "Miscellaneous Events" view of the local LOG.NSF database
  - Errors returned by DPAPI
  - Errors returned by Windows when reading or writing the NSL secrets file
  - Errors returned by core Notes security routines when working with NSL-enabled ID files
- DebugNSL=1 in NOTES.INI
  - Verifying a user's Windows password
  - Reading an Notes Shared Login-enabled ID
  - Checking for configurations which aren't compatible with Notes Shared Login (e.g. a smartcard-protected ID file)
  - Reading or writing the Notes Shared Login secrets file
- Things to keep in mind
  - If the "Lotus Notes Single Logon" service is installed, Notes Shared Login will be disabled.
  - The field "Log in to Notes using your operating system login" in the User Security dialog can be used to determine if the current ID file is Notes Shared Login enabled.

Notes Shared Login Summary

- In this section of the presentation we covered
  - What is Notes Shared Login
  - How does Notes Shared Login work
  - Enabling & Disabling Notes Shared Login
  - Notifying users when Notes Shared Login is activated or deactivated
  - Limitations when using Notes Shared Login
  - When Notes Shared Login cannot be used
  - Using Notes Shared Login and Notes ID Vault together
  - Troubleshooting