Lotusphere® 2005

Best Practices Domino Security
BP112

Daniel Nashed - Nash!Com

About the speaker

- Daniel Nashed
  - Nash!Com - IBM/Lotus Business Partner from Germany
  - Member of The Penumbra group
    - an international consortium of selected Business Partners pooling their talent and resources
  - focused on Cross-Platform C-API, Domino Infrastructure, Security, Administration, Integration and Troubleshooting
    - Platforms: W32, Linux, AIX and Solaris, zLinux
  - Technical writer for German Groupware Magazine
  - CULT Shirt Sponsor (Certified Unofficial Lotusphere T-Shirt)

Agenda

- General Considerations
- Hardware/OS / Network Security
- Notes Client/Domino Server Security
- Tips & Best practices

- Q & A

Domino Security only a Notes team issue?

- No!
- This is a task for
  - People who take care about hardware, access to rooms, ...
  - Operation System Support Team
  - Networking Team
  - Domino Administrators
  - Domino Developers
  - People who install the Notes Clients / Configurations
  - End-Users, Specially Power Users

- Your security is as strong as your weakest link!

An holistic approach to Domino Security

- You need to take care about all levels
  - Physical access to building, data-center, machines, backup tapes, ...
  - Operating Systems
    - Parameters, Sub-Systems, ...
  - Network Security
  - Notes Infrastructure
    - Server, Server settings, ..
  - Databases & Database Settings
  - Applications
    - Use the right techniques for coding
    - Reader/Author names ...

Notes & Operating System Patches

- Known problems that are fixed in later versions are good instructions to hack not updated systems!
  - Keep systems on "current" patchlevels / Service packs
  - Also Client Notes Updates & OS Client patches are important!

- Be carefull when installing additional hardware and software
- Monitor security bulletins and release notes
  - Current versions provide better security, scalability and availability in general
  - Knowledge Base
  - http://www.microsoft.com/technet/security/bulletin
  - http://www.cert.org/
  - http://www.securityfocus.com

Report Security Concerns/Bugs

- Don't discuss security issues/ potential vulnerabilities you find in public forums

- It is always best to send those concerns directly to vendors
  - Normally thru support channels
  - But there are also special addresses for some vendors
    - security-alert@lotus.com
    - security-alert@ibm.com
    - security-alert@sun.com
  - That way normally security risks are reported in public after a software vendor already published a fix

User Accounts/System Restrictions

- Domino on Windows uses the system account
- Domino on UNIX/Linux does not use the root account
  - UNIX is designed as a Multi-Tasking and Multi-User Environment
    - You can and should use different users for each Domino partition! e.g. notes1 , notes2
  - Resources like allocated local & shared memory, files are protected on user level
  - Amount of resources used by a partition can be limited on OS level (e.g. security limits on AIX and Linux)

Network Security

- Network infrastructure
  - Make sure to eliminate or filter all traffic that you do not need!
    - Remove all network services/protocols you do not use
    - Disable NetBios if possible
  - Check connections between different parts of the network
  - Use switched networks and maybe a backbone for your servers
    - But a Firewally in front of your servers?
  - Use VPN for external traffic
    - There are free IP/Sec implementations for Linux :-)
- User Notes Port Encryption (Overhead < 12 %)
  - Tip: You can have different ports for internal and external traffic

Network Security W32 & Unix

- Take care about open ports
  - Windows Servers have a LOT of Services enabled by default
    - Bind services (like Workstation service) you cannot shutdown to loopback adapter
- Use netstat -an to check for ports in listen mode
  - Works for Win32 and on Unix/Linux
- Linux comes with a nice "stateful packet" firewall
  - IpTables implementation in 2.4 kernel
  - allows to lock down the access to the machine

Secure Shell (SSH)

- Linux
  - Normally installed by default with SuSE and Redhat
- Solaris
  - Part of Solaris 9
  - also downloadable from http://www.openssh.org
- AIX
  - Part of Bonus Pack for AIX 5.1 and 5.2
  - downloadable from http://www.openssh.org
  - http://www.ibm.com/developerworks/eserver/articles/openssh_updated.html
- Always keep SSH servers & clients updated!!!

The Human Factor

- Check for private agents - Some users are really creative
  - Forwarding messages to Internet accounts, ...
- Make sure users do not share passwords
- Have policies for changing passwords and password quality
- User screen saver with passwords/lock desktop
- Tell end-users to log-out from Notes (F5)

- Don't use NT Domino Single Sign-On unless you trust Microsoft security.
  - This means mixing PKI Security and User/Password Security

Notes.ID Password Security

- Sadly there are tools on the market for Notes.ID Password guessing
  - Not based on the Notes C-API and have not the delay restrictions you see in Notes
  - But they can only crack passwords by guessing them aka Buteforce Attack
- If you have a secure password you are still safe!

Password Tips

- User Numbers and Letters
- Use mixed casing
- Use special characters (&%$...)

- Don't use existing words
  - Maybe think about a sentence and take the first letter of each word?
  - Don't use names of pets, girl-friends, kids! ...

- Use at least 8 characters

Password Quality Checking

- Use password quality checking when registering a new user

- @PasswordQuality ("field-name")
  - Field has to be of type "password"
  - Also works in the web
  - Can be used to check passwords in your applications
  - Password-Fields provide hidden-type-in and is encryption enabled
  - Uses dictionaries to check password security

  - New in 6.0.5/6.5.4/7.0
    - Custom password policies
      - allow to push very specific/custom password policies to end-users

Overview Notes/Domino Security

- Client Security
  - ECL, Local Encryption, Logout time, ...
- Notes Server Access
  - Cross Certification, Security Settings in Server Document
- Database Access
  - Groups, Roles, ACL
- Document Access
  - Reader Fields, Roles, Encryption
- HTTP Server Access
  - with Username/ Password, Certificate, SSL, ...

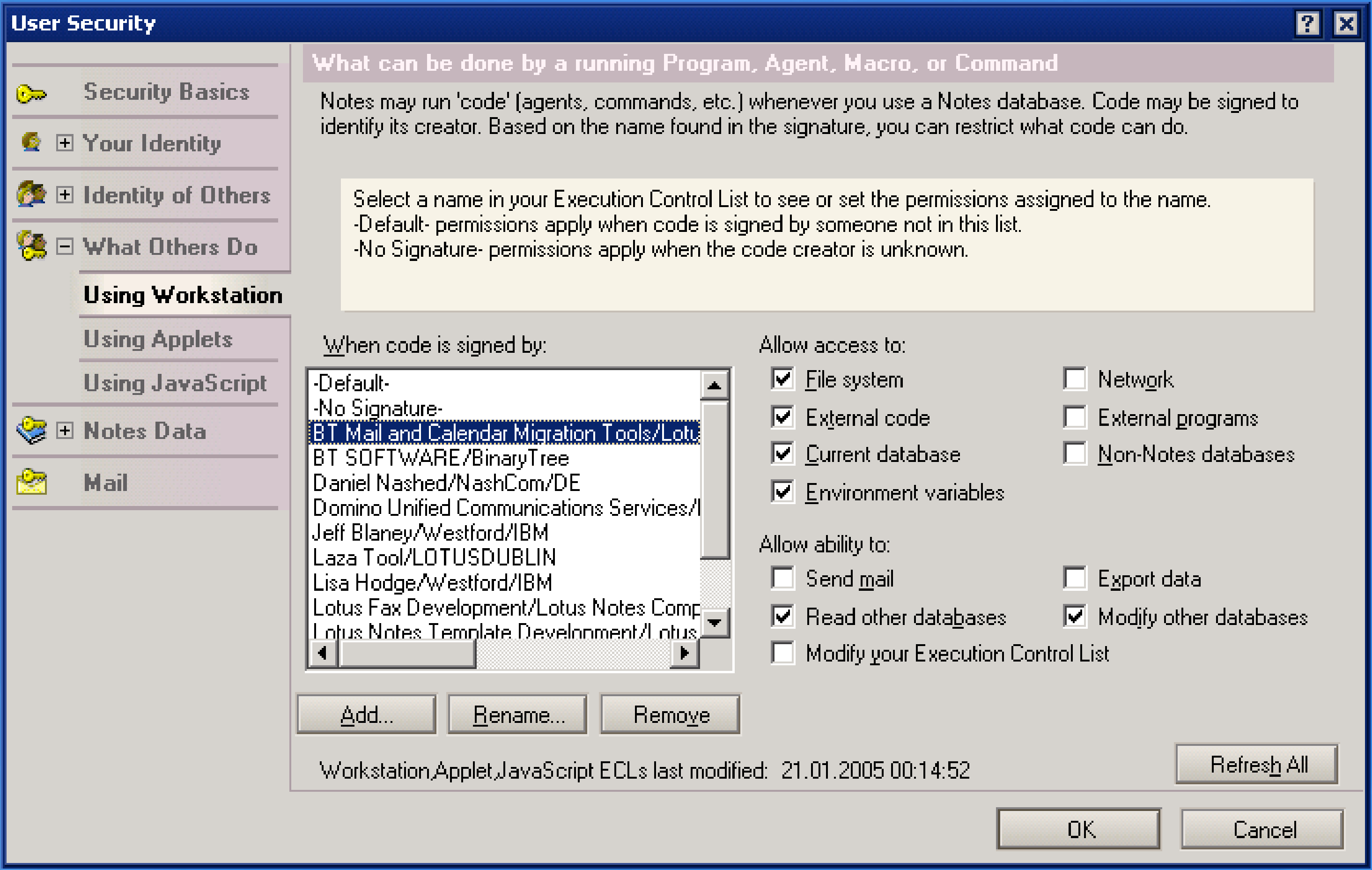
Security by Obscurity

- Hiding information is not a way to provide real security
  - Like Hidden Views, Hidden Documents, hide databases in the open dialog, ...
- Domino provides strong security available on different levels
  - Server, Database, Document, Field, ...
- Most secure way is to use encryption!
  - Domino provides a public/private key infrastructure
    - Available since Version 1.x!

Execution Control List (ECL)

- ECL defines which actions are allowed in your client for Notes and Java applications
- It is based on signatures of each design-element per user or organisation / organisational unit
- Many different actions can be allowed and denied
  - See details next slide
- Take care! New versions have stricter default settings!

Sample ECL Settings



User Security

What can be done by a running Program, Agent, Macro, or Command

Notes may run 'code' (agents, commands, etc.) whenever you use a Notes database. Code may be signed to identify its creator. Based on the name found in the signature, you can restrict what code can do.

Select a name in your Execution Control List to see or set the permissions assigned to the name.
-Default- permissions apply when code is signed by someone not in this list.
-No Signature- permissions apply when the code creator is unknown.

When code is signed by:

- -Default-
- -No Signature-
- BT Mail and Calendar Migration Tools/Lotu
- BT SOFTWARE/BinaryTree
- Daniel Nashed/NashCom/DE
- Domino Unified Communications Services/I
- Jeff Blaney/Westford/IBM
- Laza Tool/LOTUSDUBLIN
- Lisa Hodge/Westford/IBM
- Lotus Fax Development/Lotus Notes Comp
- Lotus Notes Template Development/Lotus

Allow access to:

- ☑ File system
- ☑ External code
- ☑ Current database
- ☑ Environment variables
- ☐ Network
- ☐ External programs
- ☐ Non-Notes databases

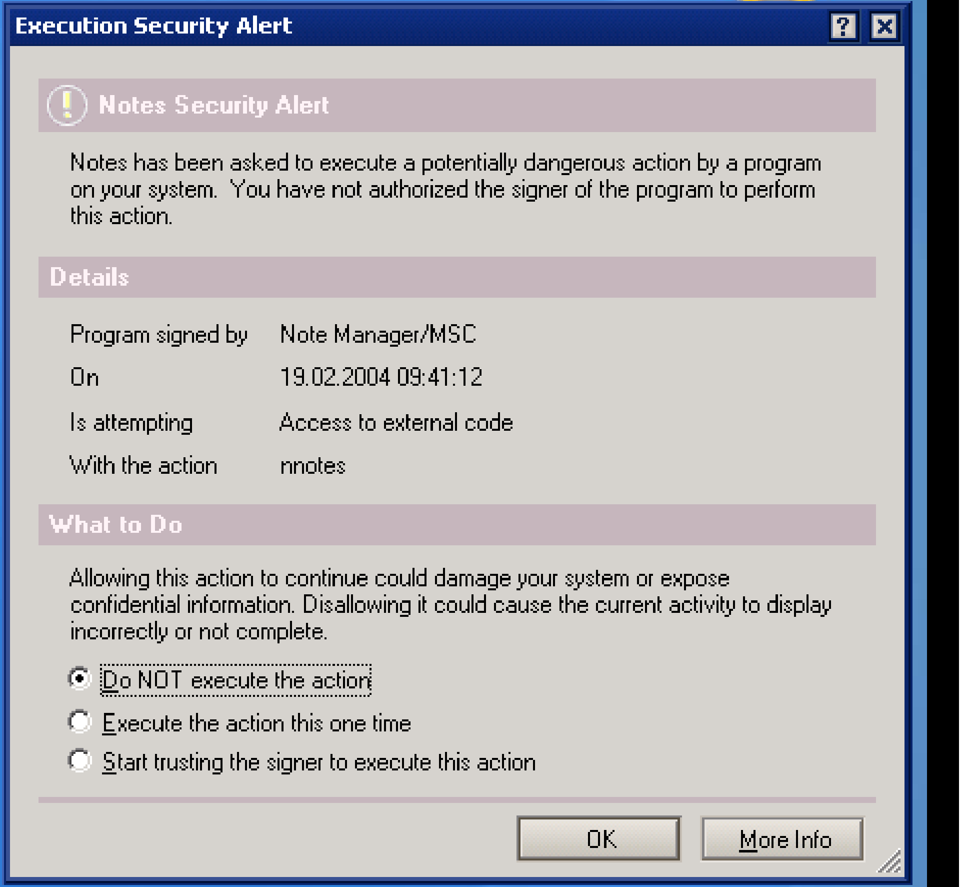
Allow ability to:

- ☐ Send mail
- ☑ Read other databases
- ☐ Modify your Execution Control List
- ☐ Export data
- ☑ Modify other databases

Workstation,Applet,JavaScript ECLs last modified: 21.01.2005 00:14:52

ECL Prompt for actions not yet allowed

- If action is not allowed user is prompted to approve the action
- You can block this behavior by using centralized, server based, ECL
  - details next slide



Execution Security Alert

Notes Security Alert

Notes has been asked to execute a potentially dangerous action by a program on your system. You have not authorized the signer of the program to perform this action.

Details

Program signed by	Note Manager/MSC
On	19.02.2004 09:41:12
Is attempting	Access to external code
With the action	nnotes

What to Do

Allowing this action to continue could damage your system or expose confidential information. Disallowing it could cause the current activity to display incorrectly or not complete.

● Do NOT execute the action

○ Execute the action this one time

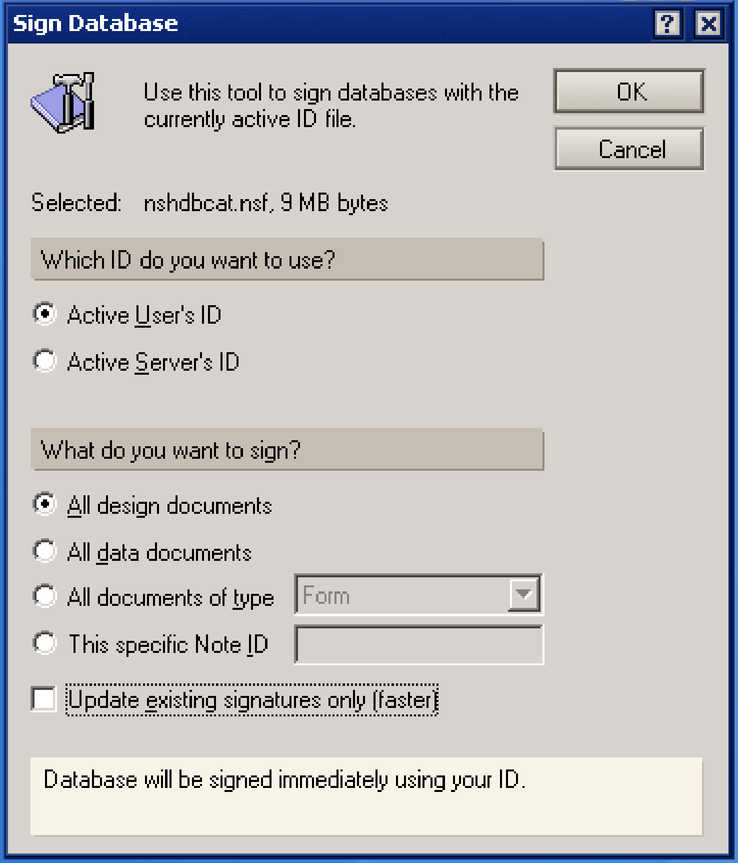
○ Start trusting the signer to execute this action

Centralized ECL in Domino Directory

- You can specify different ECLs in different directories
- Update Client ECL from Domino Directory via @RefreshECL(server : database ; name)
  - Works since 5.06
- In D6 you can push the ECL to clients (including overwrite, always, when changed, ...)
- Tip: Allow users to modify settings but push them back once per day

Signing Databases

- ECL can only work if databases have the right signature.
- You can sign databases with the Database Tools in R5 Admin Client
  - Sign with current user ID is performed immediately
  - Signing with Server.ID is performed via Adminp
- Best practice: Have a dedicated Siging-ID e.g. TemplateDevelopment/Acme



Sign Database

Use this tool to sign databases with the currently active ID file.

Selected: nshdbcat.nsf, 9 MB bytes

Which ID do you want to use?

● Active User's ID
○ Active Server's ID

What do you want to sign?

● All design documents
○ All data documents
○ All documents of type [Form]
○ This specific Note ID [ ]

□ Update existing signatures only (faster)

Database will be signed immediately using your ID.

ACL & Security

- Disable -Default- access to databases
  - Everyone who can access your server can access those databases if -Default- access is enabled!
  - Also true for Web servers if no "Anonymous" entry is present
  - Specially for servers where external users have access (e.g. Extranet)
- Add LocalDomainServers with full access to all databases to ensure correct replication
  - Manager with all roles enabled
- Also add e.g. LocalDomainAdmins with full rights and roles for support and troubleshooting

Domino Server Access

- Server Document defines general access to your server
- Take care that some settings allow access to everyone by default if you don't restrict access!
  - Server Access field should never be empty

- Passthru should be granted to external users
  - some people use firewalls with passthru servers to access Extranet servers
  - usual same right than access the server

- Have a group to deny access like "BlackList"
  - Terminated user IDs

- Review ACL via Catalog regularly!

Security for Paranoid Admins

- Only allow people to access servers listed in the Domino directory
  - Be carefull in a multi-domain environment
  - New settings in Server Access Section
    - allow all users listed in Directory + extra Groups (e.g. Guests)
- Compare public keys
- Use password change intervals and password checking
  - The first days after enabling this feature you might have a lot of hotline calls -> users with old public keys, settings, ...
- Restrict usage of single ports in the Notes.ini
  - Allow_Access_portname=names
  - Deny_Access_portname=names

Best Practices Reader Access

- Reader fields
  - If there is a non-empty reader field you have to be listed in one of those by name or group membership
    - This does also apply to servers and Admins!!!
    - But does not apply to the Full Access Administrator in D6 ;-)
- Each database should contain an "AdminReadAccess" role
  - This role should be given to all servers and admins to ensure replication & support
  - Tip: Add a computed Author Field containing this role to ensure Admin/Server full access to all documents
    - Author fields are "Read/Writers" fields and give document access also when reader fields a specfied.

Know Issue with Reader&Author/Fields

- SPR #MGAN5C7SD9 / TN #1088956
  - Error: "Authorization Failure" or "You Are Not Authorized" When Attempting to Open a Document
  - Not a bug -- Security Fix introduced Domino R5.0.10 / Domino 6.x
  - Documents containing reader or author fields without summary flag cannot be opened any more

  - In current Lotus Script calls flag is automatically set
  - The only way to fix this in existing documents is to fix the field flags in each document
  - Lotus Script Agents might not be the best choice to for fixing

How do ACL properties apply?

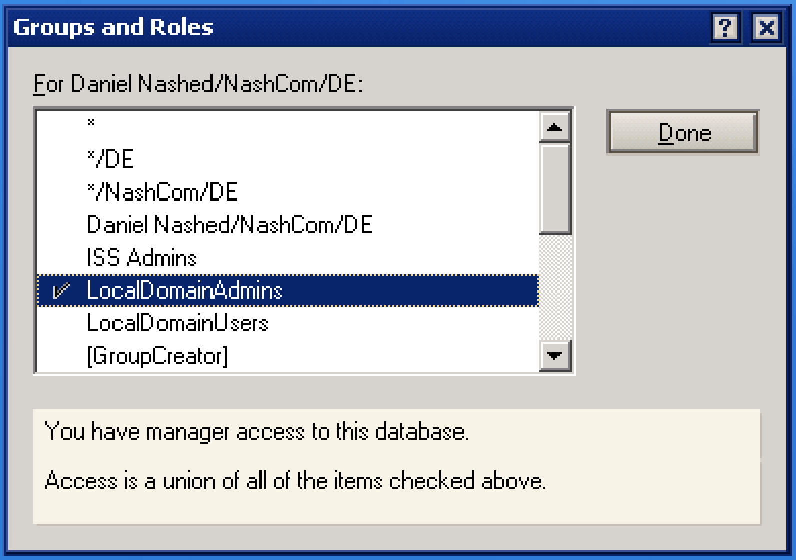
- Direct user entry takes precedence of group membership
- Always the highest access level right applies
- But all the roles and access flags are added for all matching entries
- Important: user is listed as author with delete option and listed as editor without delete he will be able to delete all documents!!!

UserNames List

- The user names list is build by server based on "($ServerAccess)"-View
  - It contains all groups a user is member of and all abbreviated forms
    - Example: Daniel Nashed, Daniel Nashed/NashCom/DE, */NashCom/DE, */DE)
  - You can see the list as user by clicking the icon next to the location name
- Be aware of the different user types!
  - Specially the Client installed on a Notes server even with server.id acts as a user!

Example UserNamesList

- Click on the Icon left of your Location name in the Notes status bar



Groups and Roles

For Daniel Nashed/NashCom/DE:

```
*
*/DE
*/NashCom/DE
Daniel Nashed/NashCom/DE
ISS Admins
✓ LocalDomainAdmins
LocalDomainUsers
[GroupCreator]
```

You have manager access to this database.

Access is a union of all of the items checked above.

Internal Views

- ($ServerAccess)
  - Is used to build the user names list
  - Essential for Server Access
  - Can cause problems
  - Design should never ever be modified!
- ($Users)
  - Is used to find users for mail addressing
  - Design should never ever be modified!

Inherit ACL from Templates

- You can use brackets around ACL entries to inherit ACL settings
  - ensures right out of the box security for every new database
  - Example: [-Default-] -> NoAcces
  - Add [LocalDomainAdmins] to all templates to ensure you have access to new created databases
- Domino 6 has nice out of the box ACL for all templates :-)
- Consider generating own replica IDs for standard Lotus templates in your organization and deploy them centralized and inherit design from standard templates

Encryption of Local Databases

- Encrypt local databases on notebooks
  - Make sure passwords are sufficient secure
  - Domino 6 allows to force local encryption for client databases via policy/local setting

- Don't encrypt server based databases.
  - Will not provide additional security unless you protect your server.id!
  - Could have impact on performance specially when using "strong" mode

How to protect real sensitive data?

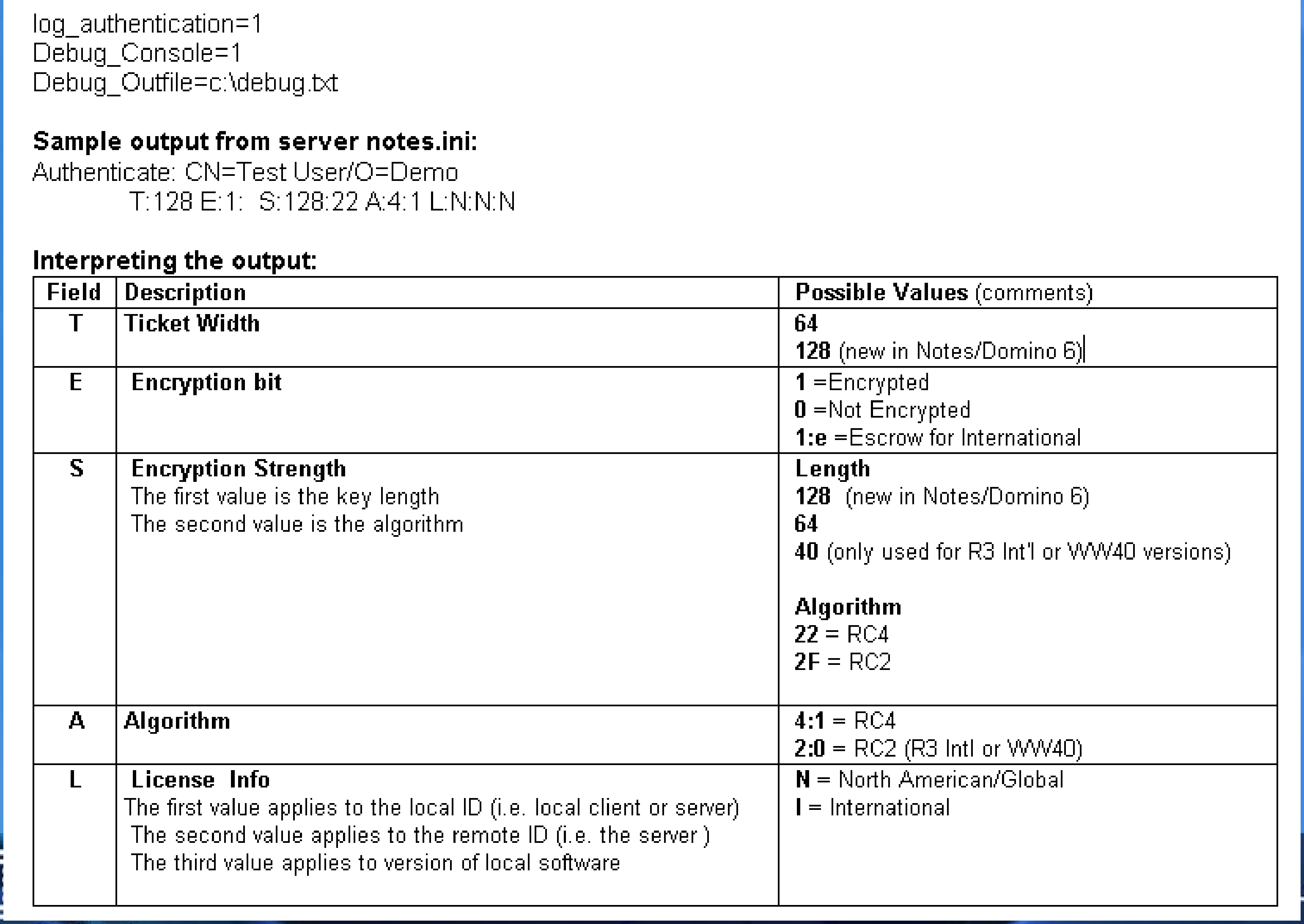
- Use named encryption keys shared between all users who should be able to access this information
  - Even administrators cannot read this information
  - but could see the encrypted items - and still support users in case of problems
  -
- This has to be enabled on application level
  - Developers & Administrators need to work together to get this implemented properly
- Organizational Policies needed for generating and distributing keys

Caveats for Encryption

- Encrypted fields cannot be used in views!
- Make sure someone has a backup copy of public encryption key
- Make sure user cannot redistribute encryption keys

- Don't import those key into the server.id until you really need it
  - users could read encrypted data too when they have access.
  - I case of external-archiving you might need an extra server without any user access or a separate ID accessing the databases

Debugging Authentication



```
log_authentication=1
Debug_Console=1
Debug_Outfile=c:\debug.txt
```

Sample output from server notes.ini:

```
Authenticate: CN=Test User/O=Demo
          T:128 E:1:  S:128:22 A:4:1 L:N:N:N
```

Interpreting the output:

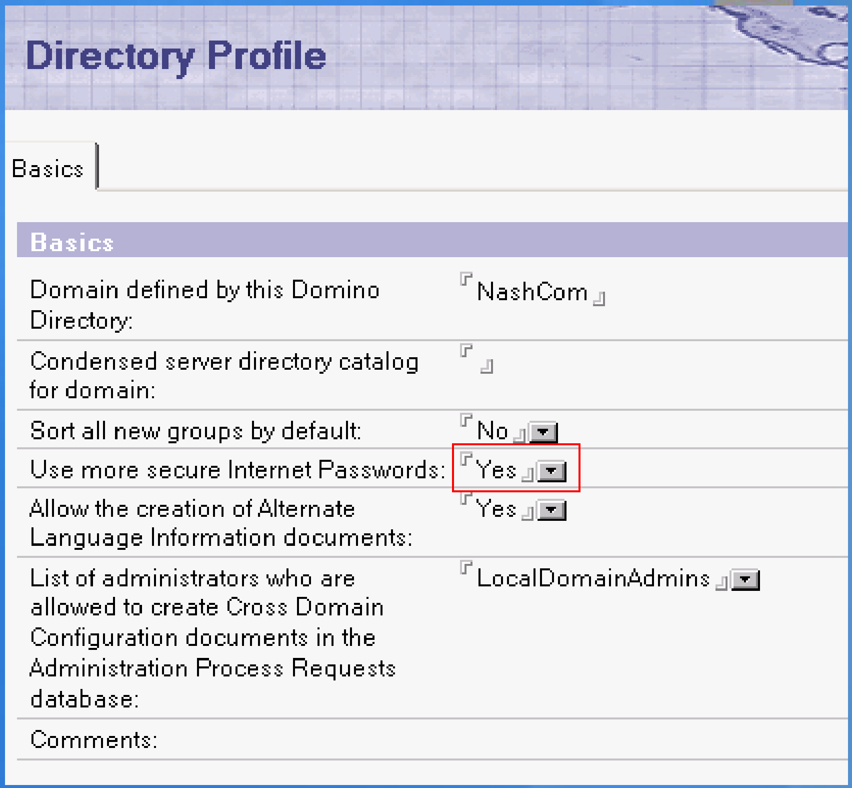
Field	Description	Possible Values (comments)
T	**Ticket Width**	**64** **128** (new in Notes/Domino 6)
E	**Encryption bit**	**1** =Encrypted **0** =Not Encrypted **1:e** =Escrow for International
S	**Encryption Strength** The first value is the key length The second value is the algorithm	**Length** **128** (new in Notes/Domino 6) **64** **40** (only used for R3 Int'l or WW40 versions) **Algorithm** **22** = RC4 **2F** = RC2
A	**Algorithm**	**4:1** = RC4 **2:0** = RC2 (R3 Intl or WW40)
L	**License Info** The first value applies to the local ID (i.e. local client or server) The second value applies to the remote ID (i.e. the server) The third value applies to version of local software	**N** = North American/Global **I** = International

Web-Security

- "Anonymous" matches before "-Default-"
- Maximum Internet Access limits access via Web regardless of ACL level
- Have file and directory protection config for webservers
- Insecure requests can be blocked via redirects
  - Example: /default.ida* , */system32/*
- Out of the box there is no way to limit the number of retries for HTTP password requests
  - Use tools like SecureDomino from TIMETOACT (http://www.securedomino.com)
- Re-create SSO document regularly

More Secure Internet Password

- $SecurePassword="1" in "Person" Document
  - via Agent "SetNewPasswordFormat"
- Generates passwords with more security ("Salted" Password)
- For new users change Domino Directory Profile "Use more secure Internet Passwords"



Directory Profile

Basics

Basics

Domain defined by this Domino Directory:	NashCom
Condensed server directory catalog for domain:	
Sort all new groups by default:	No
Use more secure Internet Passwords:	Yes
Allow the creation of Alternate Language Information documents:	Yes
List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process Requests database:	LocalDomainAdmins
Comments:	

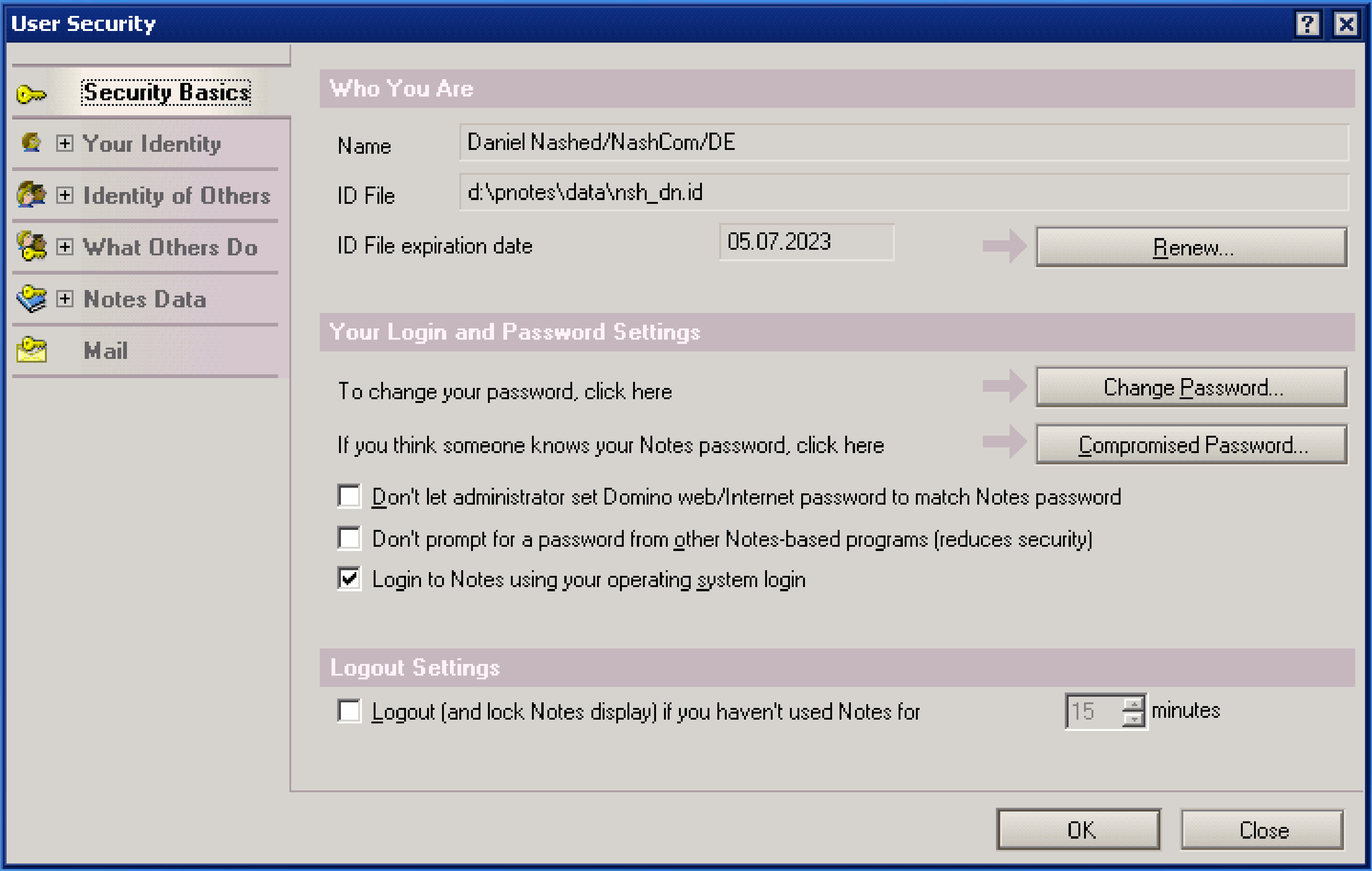
Stored Forms

- Stored Forms can be used to send own "code" to be executed when document is opened
  - TN #7003195 Q&A: BugTraq "Lotus Notes Stored Form Vulnerability"
  - This option can be a potential security problem
  - As long you have locked down ECL you are quite safe
- You can disable Stored Forms in most databases
  - Disable Stored Forms in Templates
  - Nash!Com provides a free command-line tool to disable "Stored Forms" property in existing databases

Monitoring & Logging

- Event Monitors for security options
  - ACL Monitors, Events for Security
- RTFL
  - Reading logs periodical makes a lot of sense - even you have implemented detailed event logging!
- Check the activities of databases
- Use Domlog.nsf
  - There are a lot of ways to filter the requests
  - A lot of partner tools will also help here

Client Security Settings



Who You Are

Name: Daniel Nashed/NashCom/DE

ID File: d:\pnotes\data\nsh_dn.id

ID File expiration date: 05.07.2023

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)

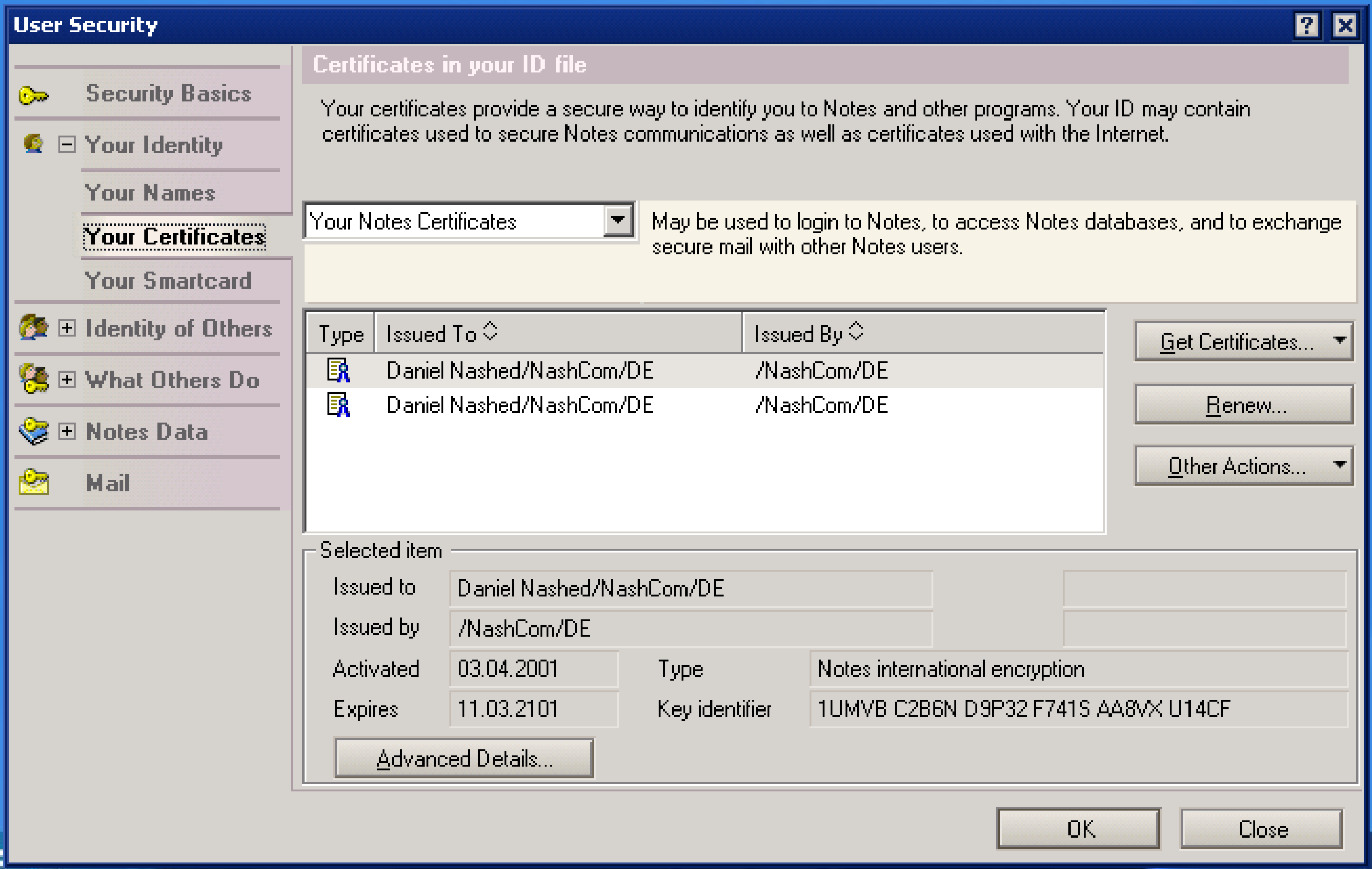
☑ Login to Notes using your operating system login

Logout Settings

□ Logout (and lock Notes display) if you haven't used Notes for 15 minutes

Better control of Security

- More detailed information available



Certificates in your ID file

Your certificates provide a secure way to identify you to Notes and other programs. Your ID may contain certificates used to secure Notes communications as well as certificates used with the Internet.

Your Notes Certificates — May be used to login to Notes, to access Notes databases, and to exchange secure mail with other Notes users.

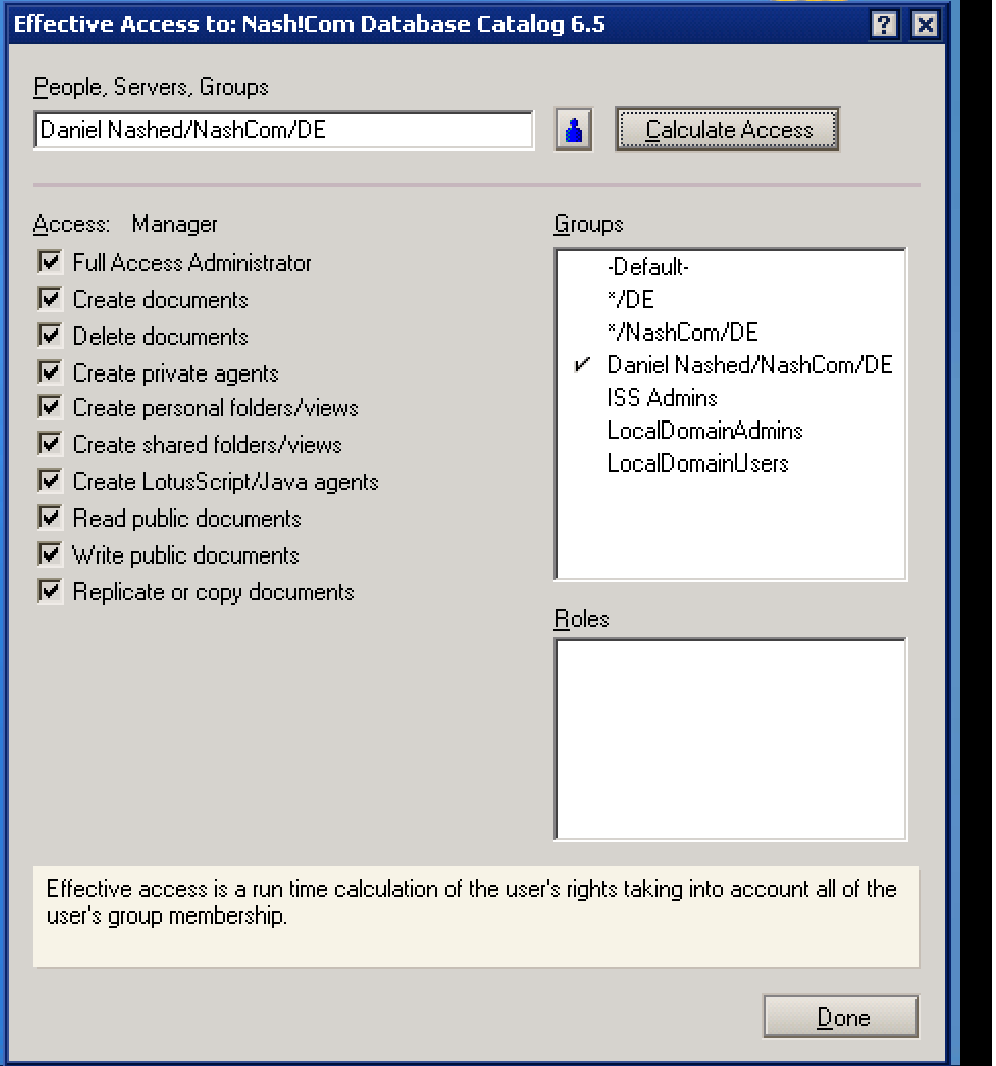
Type	Issued To	Issued By
	Daniel Nashed/NashCom/DE	/NashCom/DE
	Daniel Nashed/NashCom/DE	/NashCom/DE

Selected item

Issued to	Daniel Nashed/NashCom/DE		
Issued by	/NashCom/DE		
Activated	03.04.2001	Type	Notes international encryption
Expires	11.03.2101	Key identifier	1UMVB C2B6N D9P32 F741S AA8VX U14CF

Check Effective access

- Check access for specific user
- Already works with D6 client on R5 servers!



Effective Access to: Nash!Com Database Catalog 6.5

People, Servers, Groups

Daniel Nashed/NashCom/DE

Access: Manager

☑ Full Access Administrator
☑ 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

Groups

-Default-
*/DE
*/NashCom/DE
✓ Daniel Nashed/NashCom/DE
ISS Admins
LocalDomainAdmins
LocalDomainUsers

Roles

Effective access is a run time calculation of the user's rights taking into account all of the user's group membership.

Additional Notes 6 Security features

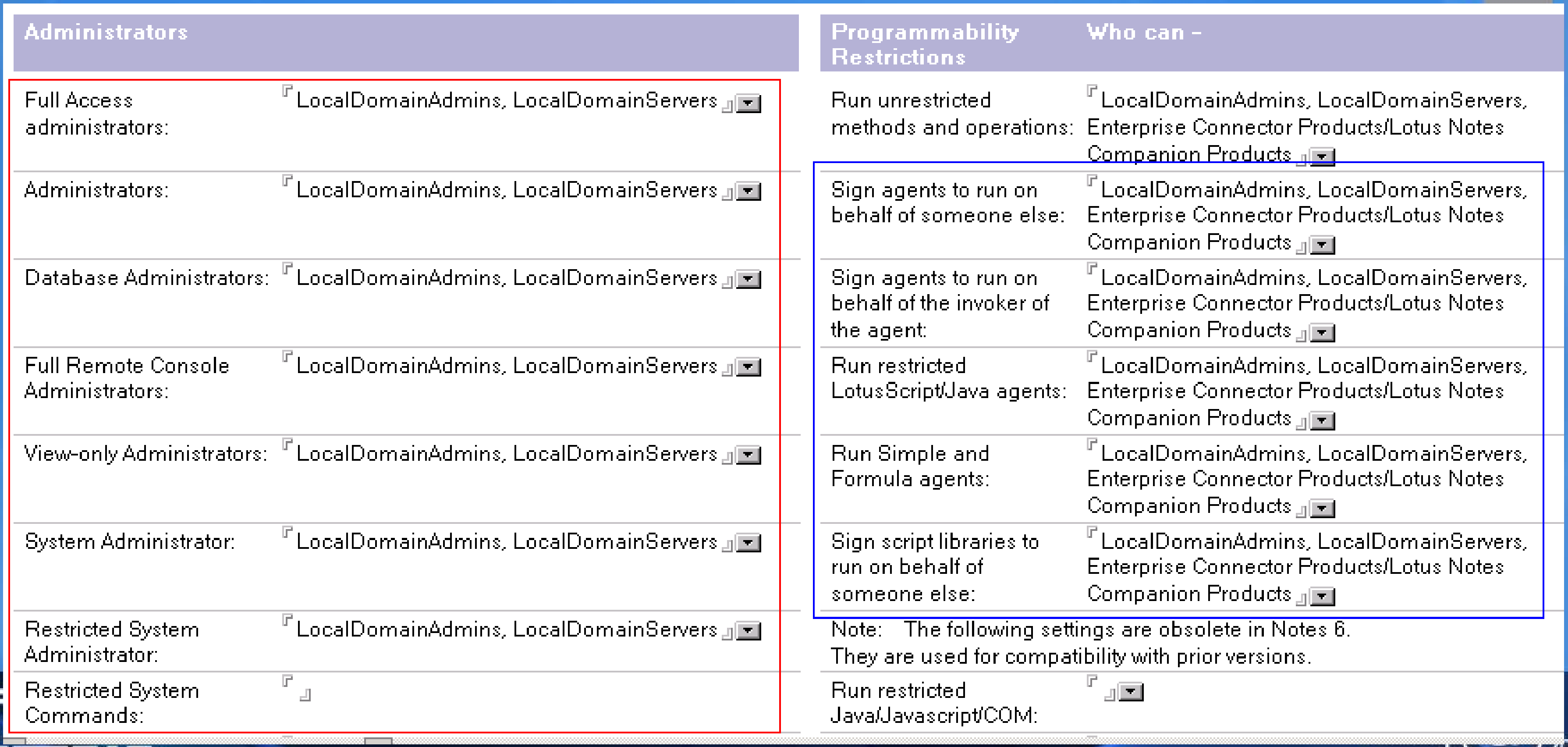
- Smartcard support (PKCS#11 standard)
  - Can be used to store the ID and Internet Certificates
- Synchronization of Notes & HTTP password
  - Needs to be enabled in person document
  - Uses AdminP to sync Notes password with HTTP password when connecting to home mail server
  - Admin can push ECL changes to users!

Domino 6 Directory Assistance

- Supports Groups in secondary Directory
  - Only one additional directory is supported
  - You can use an extended directory catalog to consolidate multiple directories
  - Users can come from both directories
  - Does work for Notes and Web

Server Security in Domino 6

- Multiple Administration Levels for Delegation
- New Security for Agents



Administrators	
Full Access administrators:	LocalDomainAdmins, LocalDomainServers
Administrators:	LocalDomainAdmins, LocalDomainServers
Database Administrators:	LocalDomainAdmins, LocalDomainServers
Full Remote Console Administrators:	LocalDomainAdmins, LocalDomainServers
View-only Administrators:	LocalDomainAdmins, LocalDomainServers
System Administrator:	LocalDomainAdmins, LocalDomainServers
Restricted System Administrator:	LocalDomainAdmins, LocalDomainServers
Restricted System Commands:	

Programmability Restrictions	Who can –
Run unrestricted methods and operations:	LocalDomainAdmins, LocalDomainServers, Enterprise Connector Products/Lotus Notes Companion Products
Sign agents to run on behalf of someone else:	LocalDomainAdmins, LocalDomainServers, Enterprise Connector Products/Lotus Notes Companion Products
Sign agents to run on behalf of the invoker of the agent:	LocalDomainAdmins, LocalDomainServers, Enterprise Connector Products/Lotus Notes Companion Products
Run restricted LotusScript/Java agents:	LocalDomainAdmins, LocalDomainServers, Enterprise Connector Products/Lotus Notes Companion Products
Run Simple and Formula agents:	LocalDomainAdmins, LocalDomainServers, Enterprise Connector Products/Lotus Notes Companion Products
Sign script libraries to run on behalf of someone else:	LocalDomainAdmins, LocalDomainServers, Enterprise Connector Products/Lotus Notes Companion Products

Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.

Run restricted Java/Javascript/COM:	

Full Access Administrators

- Additional Rights
  - FULL access to administer the server
  - Same rights as Administrators
  - plus Manager access to ALL databases , regardless of the ACL on the databases!!!
  - Does also override reader fields !
  - But does not override document encryption!
- You need to activate "Full Admin Mode" in Admin Client

Other Admin levels...

- R5 Administrator is still there

- Multile other levels to help decenralized administration
  - Database Administrators
  - Full Remote Console Administrators
  - View-only Administrators
  - System Administrator
  - Restricted System Administrator

Disable the Full Access Administrator

- Notes.ini: SECURE_DISABLE_FULLADMIN=1
  - This can only be changed editing the physical notes.ini on the server
    - No Set Config or Config Document applies!
  - Disables the Full Access Administrator independent of all settings in the Domino Directory

Domimo 6 Agent Manager Features

- Access databases on remote servers!
  - Server needs to trust the other (server doc)
- Programmatically Enable/Disable agents while running on server
  - Activate agents without signing!
- Run scheduled agents on behalf of users
- Allow persons without designer rights to enable agents
- Run Agents from Server Console!
- Assign a Reader List to an agent

New Agent-Restriction Settings

- **Unrestricted** - allows all agent operations

- **OnBehalf of anyone** - allows to create agents running on behalf of someone else
- **OnBehalf of invoker** - allows to create agents which can be invoked by someone else

- **Restricted** - allows LS/Java agents
- **Personal** - allows to run personal agents
- **Script Libraries** - allows to sign script libraries

- For more infos about agents check Lotus Developer Domain

More about Agent Manager

- All Personal Agents are visible to Managers

- Tell Amgr run "db name" 'agent'
- Tell Amgr cancel "db name" 'agent name'
- Show agents [-v] "database name"

- UI Classes in background agents now return errors which can be caught by "On Error"
  - Best practice is to catch any kind of error in applications with reasonable error messages

D6 Agent Manager Security Changes

- In R5 you cannot prevent users from running Simple and Formula agents
- D6 Changes in Server Document
  - R5: "Run personal agents"
  - D6: "Run Simple and Formula agents"
  - Private agents are now treated depending on their class (restricted/unrestricted)
  - Take care to check those details
  - Notes.ini: ENFORCE_PERSONAL_AGENTS=1 enforces the old mode for personal agents if really needed

D6 SMTP Enhancements

- More detailed Relay Control
  - Server Config Document: SMTP Inbound Control
    - Allow all authenticated users to relay
    - Only perform Anti-Relay check for external hosts
    - Host exclusion list for some hosts
  - D7 will introduce more flexible handling
    - White-Lists, ...
- SMTP C-API Extension Manager Calls
  - can be used to "hook" into inbound SMTP mail processing

Notes 6 User Client Access Security

- User does not need to be Manager in his mailfile
  - Delegation and Out of Office Agent still works
- You can restrict the minimum Notes Release of accessing Users (via server document)
  - Configuration Document "Basic" tab
  - Caution: This does also apply to connecting servers!
  - It is needed to fully ensure some security features like "disable replication"

Additional Resources

- Notes.Net Inside Notes Database
- Notes.Net articles
- Domino Security Zone
- Lotus & Microsoft Knowledge Base
- Readme of each Domino Release/Update

Interesting Articles

- http://www.ibm.com/developerworks/lotus/library/ls-user_security/
- http://www.ibm.com/developerworks/lotus/library/ls-security_overview/
- http://www.ibm.com/developerworks/lotus/library/ls-Using_the_ACL/index.html
- http://www.ibm.com/developerworks/lotus/library/ls-ECLs/index.html
- http://www.ibm.com/developerworks/lotus/library/ls-password_quality/index.html
- http://www.ibm.com/developerworks/lotus/library/ls-password_checking/index.html
- http://www.ibm.com/developerworks/lotus/library/ls-security_interview/index.html

Questions & Answers / Other Domino Security releated Sessions

- ID119 This Isn't Charlie's Security Session - But You Still Should Attend! (Katherine Spanbauer, David Kern)
  - Tuesday 3:00pm - 4:00pm Swan 10

- BP115 Best Practices for Internet Mail Security and S/MIME (Marc Luescher, Daniel Nashed)
  - Wednesday 4:15pm - 5:15pm Swan 1-2

- Q A: "The Speakers Room" Europe 8 after the session
- and Security BOF tonight + Fill out the EVALS

- http://www.nashcom.de, mailto: nsh@nashcom.de