Lotusphere2011
IBM Software

Master Class:
Defense Against The Dark Arts

- Andrew Pollack
  President
  Northern Collaborative
  andrewp@thenorth.com

- Gabriella Davis
  Technical Director
  The Turtle Partnership
  gabriella@turtlepartnership.com

Smarter software for a Smarter Planet.

Are you in the right room?

- Approach of this presentation
  - There are an enormous number of security settings and features in Domino
  - We will take a look at the threats and risks you face, and the techniques used to combat those risks
- We assume you are a Domino Administrator
  - …Or a Developer that knows some admin stuff -- like what “servers” are
- Cast of characters
  - The Nosy Co-Worker
  - The “Loser”
  - The Rogue Developer & His Junior Sidekick
  - The Engineering Genius
  - Helpful Helpdesk Support
  - Script Kiddies & Spammers
  - The Bitter Ex-Admin
  - The Super Villain

Please Shut Off All Noisemaking Appliances

- We're not judging, just shut them off while we're talking
  - Unless they are medically necessary

Who are we to tell you anything?

- 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 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.

- We’re actually pretty good at this stuff.

We are required by a horde of lawyers to properly mark the first use of these terms in all presentations.

That's out of the way now. On with the show!

The Nosy Co-Worker

- Scooby doesn't mean any harm, he just wants to know what's going on
- He fancies himself as a bit of a techie
  - Or he just likes to know stuff others don't
- He won't do anything deliberately illegal
- He likes to know about the latest Lotus news and developments

Stepping Over Boundaries

- Using someone else's ID
- Opening applications he should have no access to
- Looking at Domino logs to track and fix his own "problems"
- Downloading and installing a new Notes client he read about online

Using Someone Else's ID

- He has been given someone else's id by IT
  - Usually because no-one knew how to get him access in a hurry to an application he needed
- He has been given someone else's id by that person
  - To work on that person's calendar
  - To access / work on an application he doesn't have direct access to on their behalf
- He found an id on a machine he was using and guessed the password

Using Someone Else's ID

- Use Notes Shared Logon to encrypt ids on shared machines with the Windows credentials of each user
  - Part of the Notes client install
  - Replaces Client Shared Login
  - Notes Shared Logon encrypts the Notes ID with the Windows credentials of the logged in user and the machine the user is logged into
    - Then removes the password from the Notes ID completely
  - Can be applied using a security policy

- If IDs are encrypted using the users Windows credentials then they can't be shared between users

Using Someone Else's ID

- Turn on public key and password checking for ids to prevent old passwords / ids being used
  - Turn on password checking on Notes IDs
  - No we have ID Vault we can reset passwords for Notes IDs easily so this becomes a more viable option

- Server Document - Security Page
  - Public Key Checking will verify if the public key in the user id matches the public key in their person document. If an ID is compromised, simply recertifying it will immediately invalidate the old id as the public key it has will no longer match
    - You can enable public key checking to simply log mismatches rather then block access, so you can monitor access with old ids
  - Password checking forces the server to retain a digest of the last known password used by the user's Notes ID. When a user attempts to log with an old ID to which they may have known the password, the login will fail as the server can tell it is not using the most up to date password for that ID.
    - You can invalidate old copies of an ID simply by setting a new password for it

Using Someone Else's ID

- Configure ID Vault to only download to one machine
- 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 all without needing any user involvement

Using Someone Else's ID

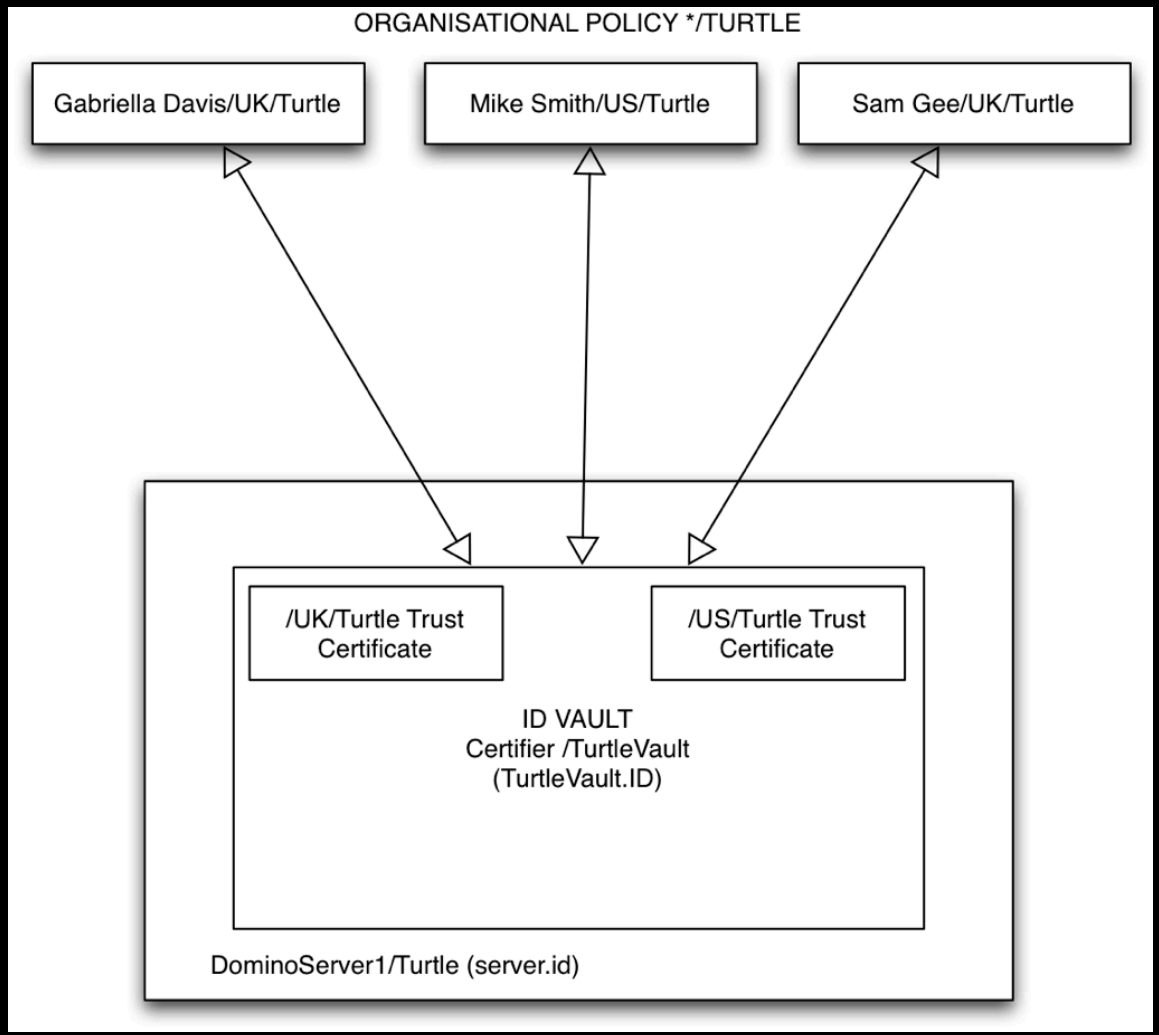
- How Does ID Vault Work
  - If no ID exists on the workstation the notes.ini fields keyfilename and keyfilename_owner are used to identify which ID should be downloaded
  - The ID can only be downloaded if the user knows the password for the ID stored in the Vault
  - So you can't hack a notes.ini file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

Using Someone Else's ID

- How Does It Work?
  - 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

Using Someone Else's ID

- How Secure Is It?



Opening Restricted Applications

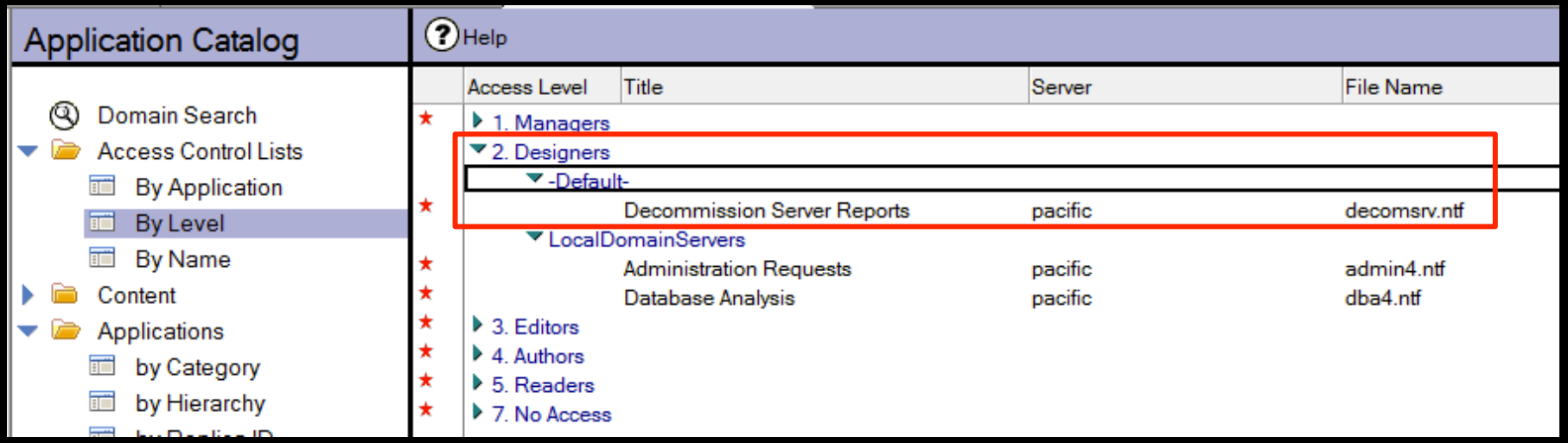
- Looks in DB Catalog for databases with -Default- access and tries to open them
- Sees databases in the “File Open” dialog and tries to open them

Opening Restricted Applications

- Use explicit ‘opt in’ ACL groups instead of using -Default-
- Enable DDM Database Security Review Probes to analyse database access levels
  - Or use the ‘by level’ view in the Catalog.nsf to see databases where -Default- is higher than “No Access”
- Monitor DDM.NSF for unauthorised access security alerts, showing someone trying to access a database they shouldn’t

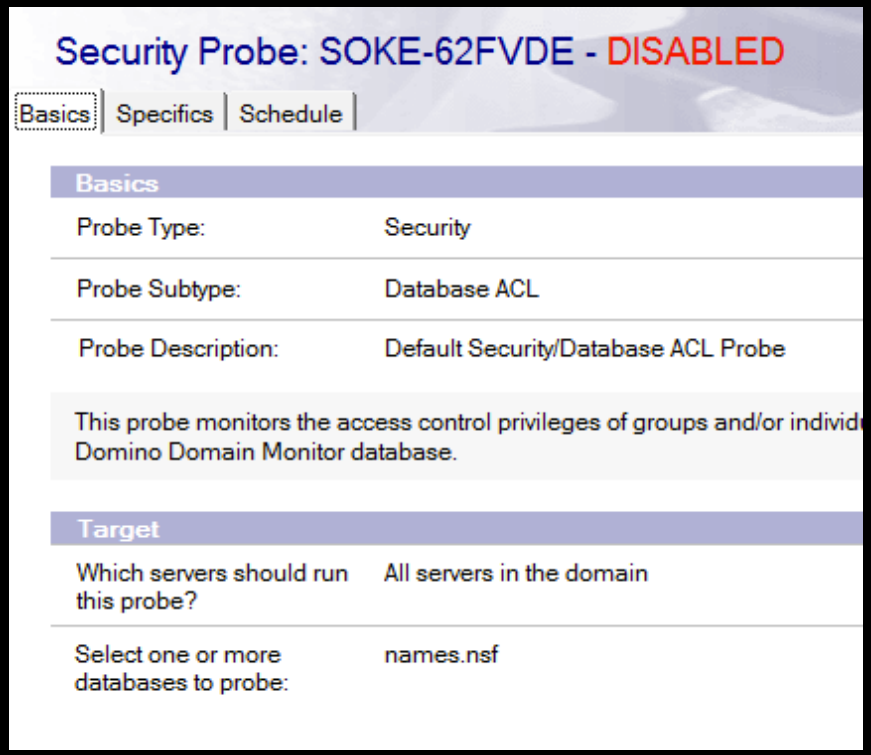
Opening Restricted Applications

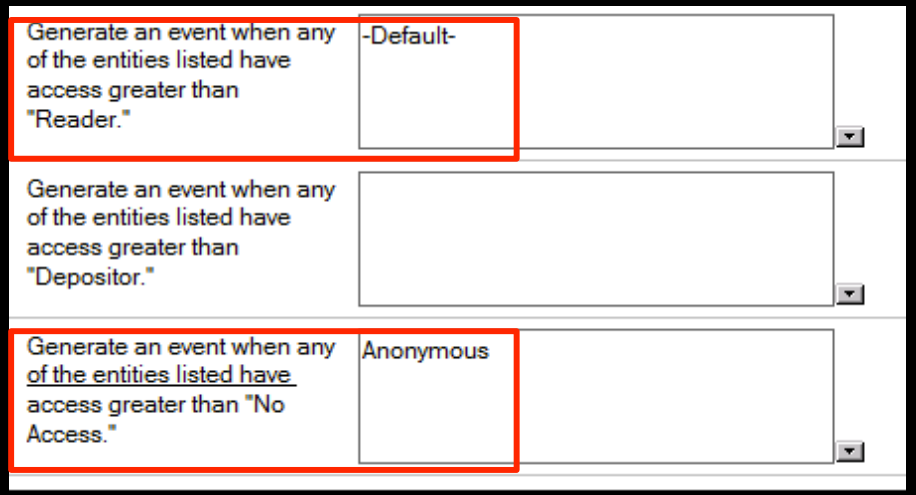
- Enable DDM Database Security Review Probes to analyse database access levels
  - Or use the 'by level' view in the Catalog.nsf to see databases where -Default- is higher than "No Access"



Opening Restricted Applications

- Enable DDM Database Security Review Probes to analyse database access levels
  - In events4.nsf
  - Pre-created on install, just configure and enable
  - Reports to ddm.nsf on each server



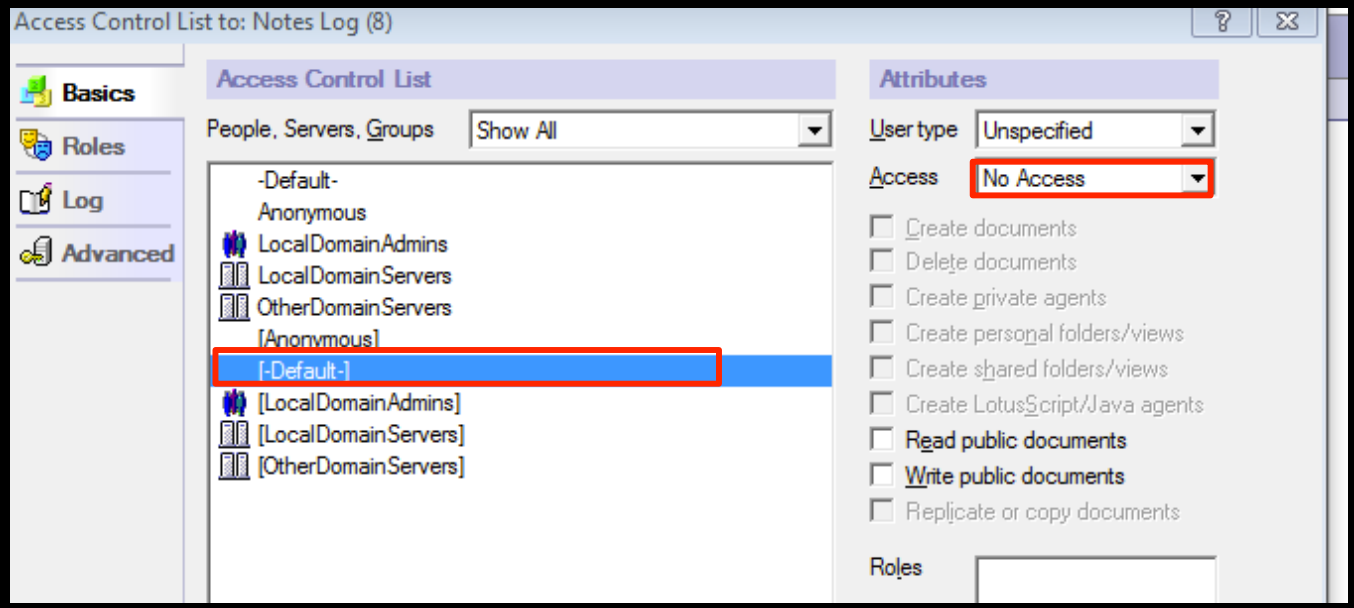


Looking In Server Logs

- Self - Diagnosing of problems of their's and other's!
  - not logged with Helpdesk
  - combined with ability to read notes.net results in a series of kludgy 'workarounds'

Looking In Server Logs

- Restrict ACL on log.nsf to -Default- = No Access
  - Users have no need to access server logs
  - Modify log.ntf template ACL to ensure all logs are created with the same access restriction
    - Modify the setting in square brackets to apply it to any db created from this template



Downloading & Installing Clients

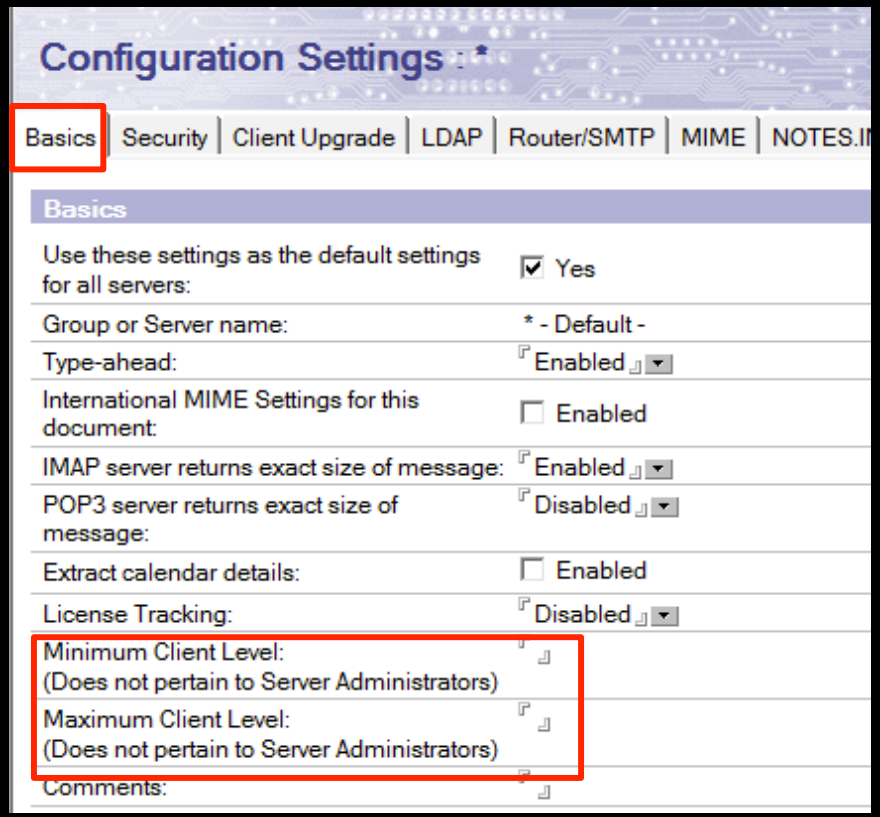
- Reads online communities, notes.net, technical blogs and hears about these new features he wants
- Finds trial versions of Notes clients online and downloads
- Installs the trial version on his machine and replaces his mail file design with the new template

Downloading & Installing Clients

- Restrict mail file ACL to Editor access
- With Editor access the user can't replace the design of their mail file
- Unfortuately can't mass change existing mail files
  - Either change manually or use an agent

Downloading & Installing Clients

- Use server configuration document to restrict server access to specific versions
  - Min and Max client versions allowed to access server
    - If the user updates their client, they will no longer be able to access the server

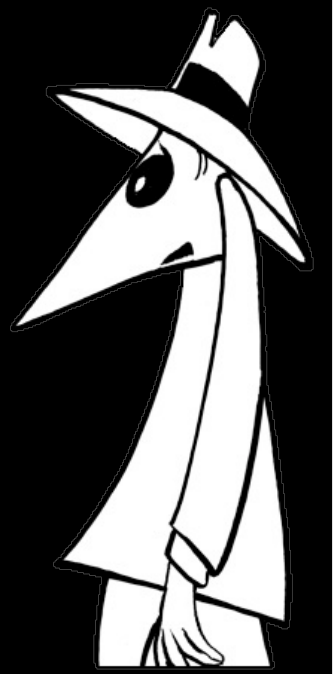


The Paranoid Coworker

- He is convinced that someone is reading his mail
- Sometimes, someone really is reading his mail
- What can you prove?

With Increased Access Comes Increased Risk

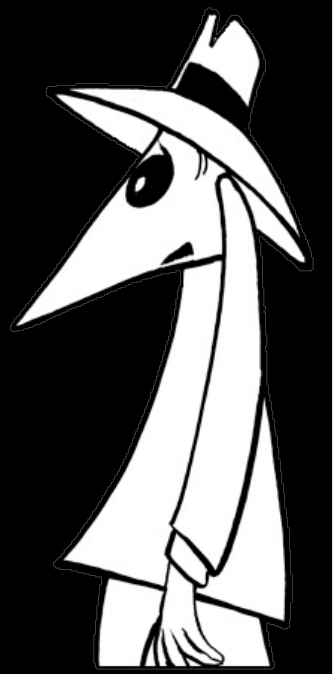
- Administrators require high levels of access to do their jobs
  - Fixing Access Control Rights
  - Repairing Damaged Databases
  - Creating & Moving Databases
  - Deploying Design Changes
- Information Technology workers are frequently accused of abusing their increased access to information
  - Accusations of reading other people's email
  - Accusations of harassment or stalking
  - Accusations of snooping payroll or other HR information
- In more and more jurisdictions criminal charges may result



Poor Authentication Control is a Serious Risk

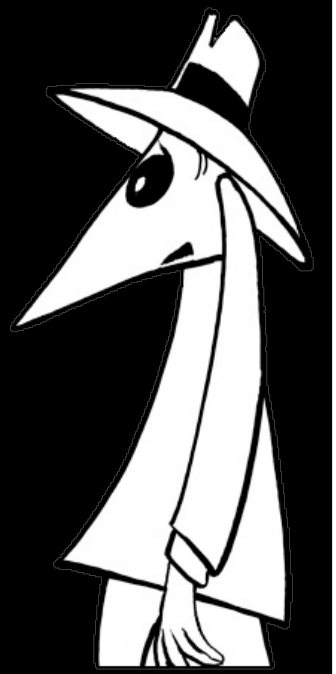
- Human Resources staff must frequently deal with a variety of complaints between coworkers that can end up in court
  - Harassment
  - Inappropriate Access to Data
  - Inappropriate Use of Resources

- To take action, a company must be able to prove that the specific person was responsible
  - A specific set of credentials were used
  - IT Staff and others did not have the ability to duplicate the credentials without leaving a trail
  - The log files generated could not be altered without leaving a trail



Protect Your Credentials

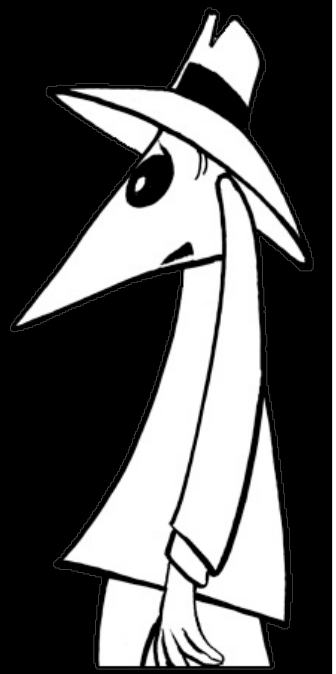
- Protect All ID Files & Certifiers
  - Certificate Authority Tools
  - Password Checking
  - Public Key Checking
  - ID File Password Recovery
  - NO MORE FOLDER OR DATABASE FULL OF BACKUP IDs
- Protect Network Access Passwords
  - Even if you don't think you use internet passwords!
  - Password Synchronization
  - Password Failure Lock-out
- Password Management Policies
  - Complexity
  - Frequency of Change



Protect Your Administrators

- Administrators' Personal Credentials
  - No Full Access Administration Rights
  - No Unrestricted Agent Rights
  - No "Special" Access to Mail Files, HR Databases, etc.

- When Full Access Administration is Required
  - Require Switching to a Special ID file
    - Specific to Each Administrator
    - Can use Web Administrator Instead
  - Use Event Logging to Track Full Access Admin Use
    - Immediately send a notification to a log file on another server
    - Involve third party oversight
    - Sometimes you have to ask forgiveness rather than permission



The “Loser”

- He’s not technical at all, in fact he’s barely interested in technology but he expects IT to have taken care of security
- He has to have a phone and a laptop and a blackberry to do his job
- He works remotely, often from new locations
- His “gadgets” regularly go missing.

Just Enough Knowledge To Be Dangerous

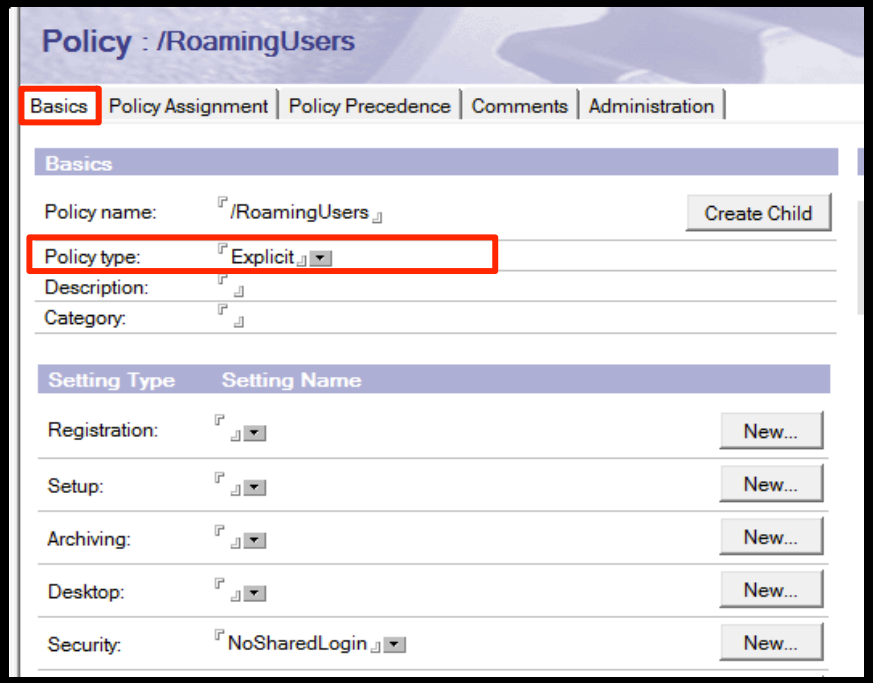
- Choosing ease of use over security
- Using public wireless networks
- Using other people's computers
- Installing other useful apps

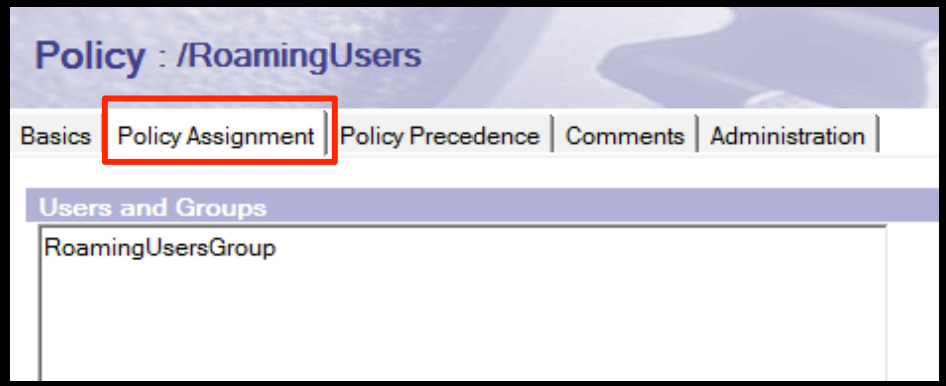
Choosing Ease Of Use Over Security

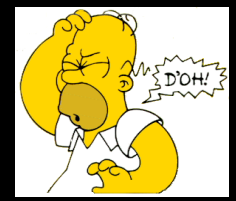
- When Homer gets a laptop or mobile device to use he still thinks the great and powerful IT guys have control over it
  - So he doesn't worry about securing it or the information on it
  - This is especially true with smartphones
  - After all you gave it to him, you must be happy for him to leave it unsecured
- Security != Convenience.
  - He won't set a PIN on his phone because that slows down how quickly he can get at it.
  - He won't log out of Notes or even lock it because that slows down how quickly he can get at it
- Homer didn't buy the device and won't pay for the replacement, he also wants it to be near at hand
  - Not put away somewhere secure

Choosing Ease Of Use Over Security

- Secure the applications you supply
  - For Notes be wary of using Notes Shared Login if giving to a roaming user
    - Homer probably doesn't log out of Windows, so the Notes data will be completely exposed
    - Use security settings on a dynamic policy assigned to a roaming users group to ensure Notes Shared Logon can't be enabled
  - A dynamic policy is an effective policy assigned to a group or group of users

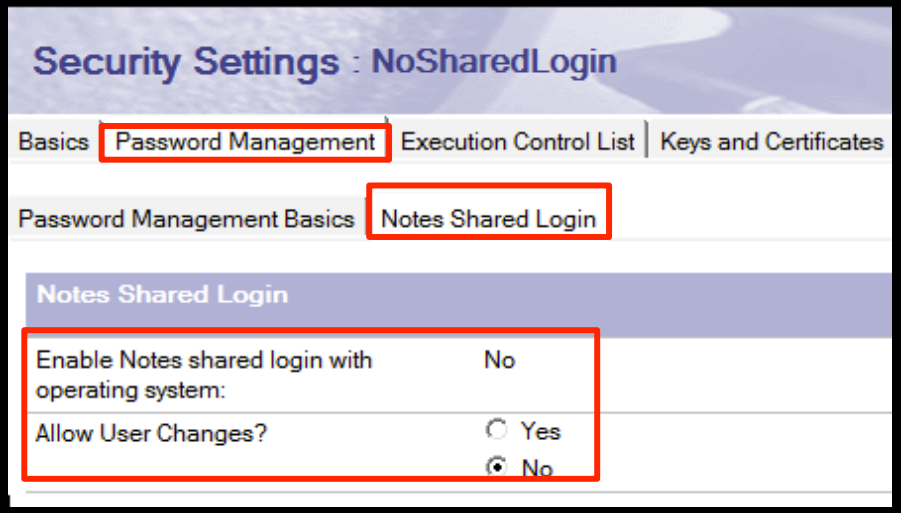






Choosing Ease Of Use Over Security

- Security Settings to disallow Notes Shared Login
  - prevents the user from enabling Notes Shared Login

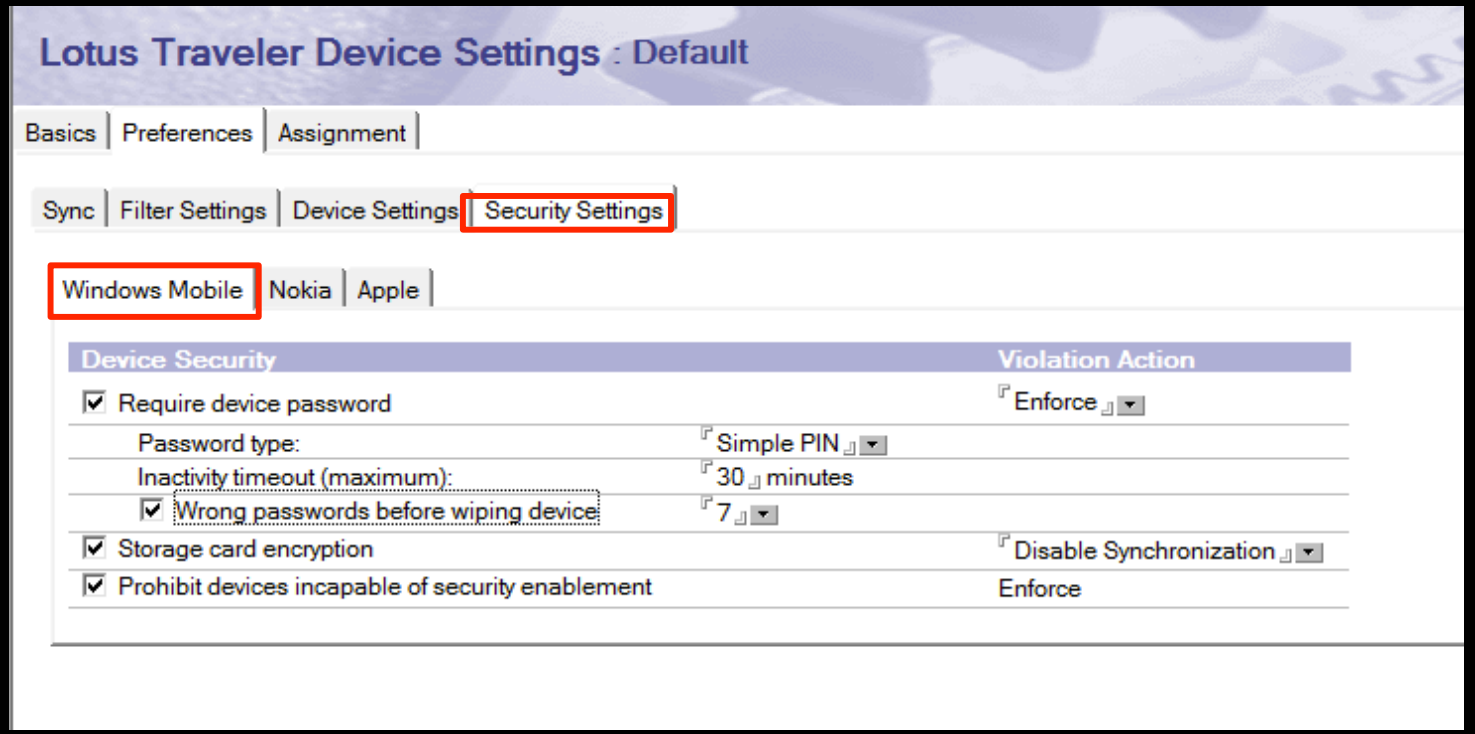


Choosing Ease Of Use Over Security

- If you're using Traveler use policies to
  - force a password on the device
  - encrypt the content
  - force a lock after x minutes
  - (same can be done with Blackberry devices on a BES)
- In lotustraveler.nsf - create device settings or edit default device settings
  - settings can be assigned by user

Choosing Ease Of Use Over Security

- Windows Mobile Security Settings



Choosing Ease Of Use Over Security

- Nokia Security Settings

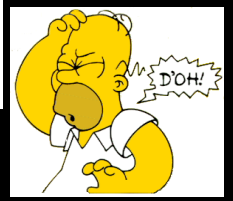
Lotus Traveler Device Settings : Default

Basics | Preferences | Assignment

Sync | Filter Settings | Device Settings | Security Settings

Windows Mobile | Nokia | Apple

Device Security		Violation Action
☑ Require device password		Enforce
Minimum password length:	4	
Maximum times character repeats:	0	
☑ No adjacent numbers		
☑ Require alphanumeric		
☐ Upper and lower case		
Inactivity timeout (maximum):	30 minutes	
Password expiration period:	30 days	
Password history count:	0	
☐ Wrong passwords before wiping device	7	
☑ Storage card encryption		Disable Synchronization
☑ Prohibit devices incapable of security enablement		Enforce



Choosing Ease Of Use Over Security

- Apple Security Settings

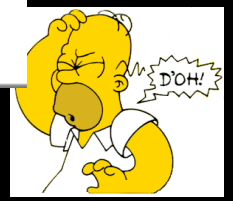
Lotus Traveler Device Settings : Default

Basics | Preferences | Assignment

Sync | Filter Settings | Device Settings | Security Settings

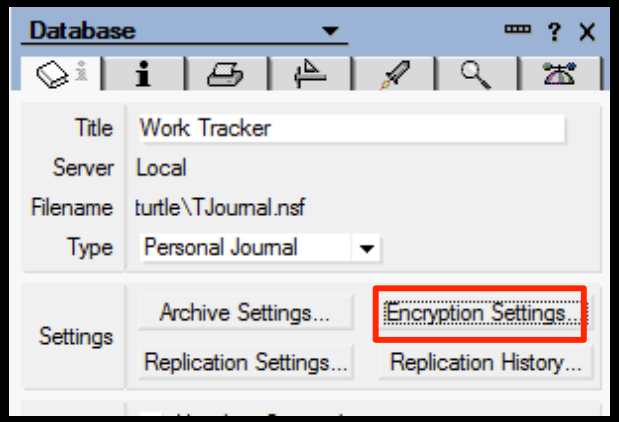
Windows Mobile | Nokia | Apple

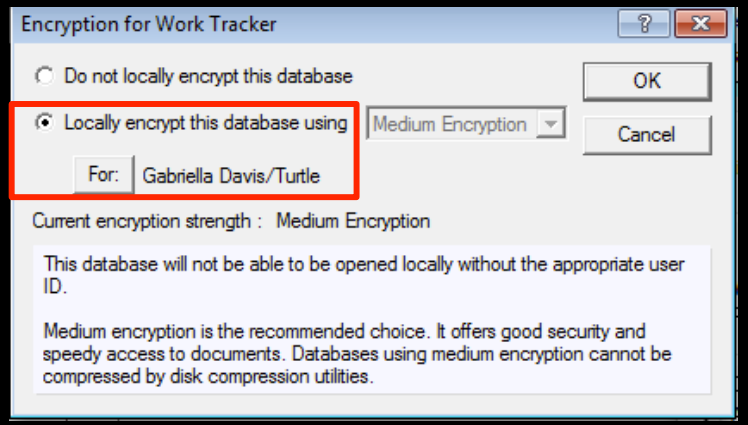
Device Security		Violation Action
☑ Require device password		Enforce
☑ Prohibit ascending, descending and repeating sequences		
☐ Require alphanumeric value		
Minimum password length:	4	
Minimum number of complex characters:	0	
Auto lock period (maximum):	30 minutes	
Password expiration period:	90 days	
Password history count:	0	
☑ Wrong passwords before wiping device	7	
☐ Prohibit unencrypted devices		
☑ Prohibit camera		Enforce
☑ Prohibit devices incapable of security enablement		Enforce



Choosing Ease Of Use Over Security

- Ensure all local replicas in Notes are encrypted
  - Encrypting local replicas means that the Notes ID has to be used to open them
  - As of Notes 8.x all new local replicas are encrypted by default

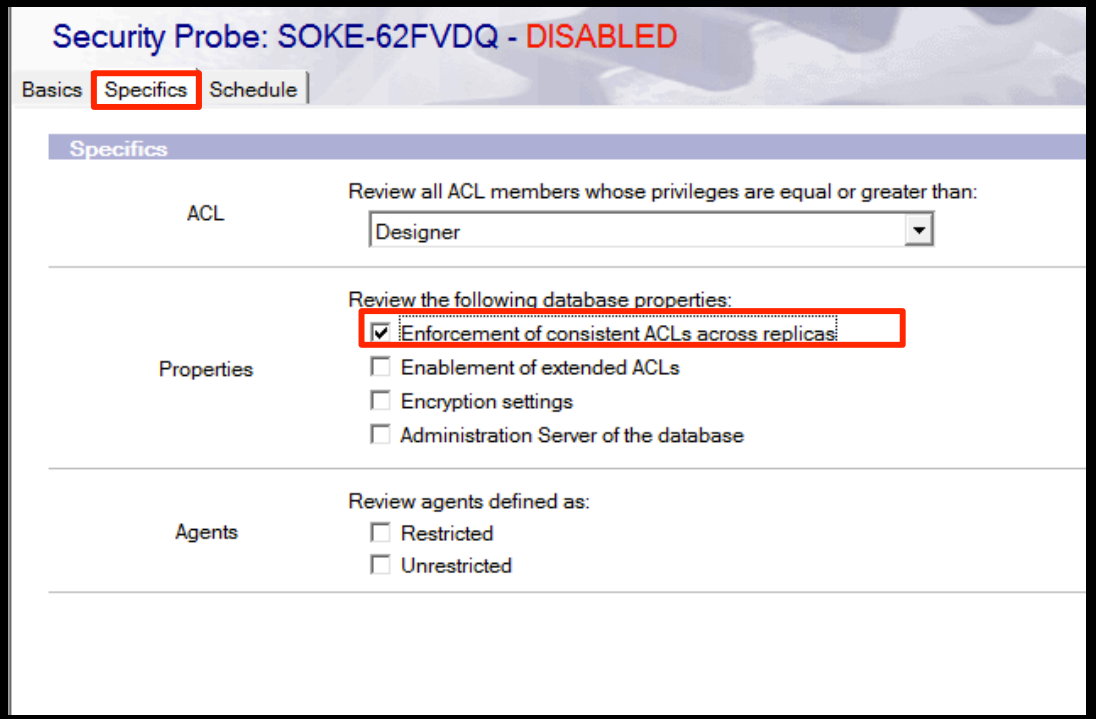




  - To encrypt an unencrypted local replica you must perform an OS level compact after changing the database property setting
    - pulling down a new encrypted replica is probably easier!

Choosing Ease Of Use Over Security

- Ensure “Enforce Consistent ACLs” is in place on every database that might be replicated
  - Advanced properties under database ACL
  - If it’s not enforced a local replica grants Manager access and no roles
- Use DDM Database Security Review probe in events4.nsf to check for databases on your servers without this setting in place



Choosing Ease Of Use Over Security

- Don't allow Homer to have author rights to the Domino Directory
  - You may be tempted to give him Author rights so he can keep his own person document up to date
  - If he has a local replica of names.nsf then he has to replicate with the server regularly
  - If he fails to replicate with the server for over 90 days - the deletion stubs that were in your replica copy will have disappeared
    - All the documents that were deleted prior to those 90 days will still be in his local replica and not on your server replica - so his replication will send them back to you !
    - Now you server names.nsf is full of old documents you deleted months ago
- Giving users access to the Domino Directory to treat it as an address book is a bad idea
  - There are plenty of tools that allow you to have the same functionality (changing http passwords, setting phone numbers, group management etc) without the risk of working directly in names.nsf
    - I have a free tool I use called Directory Updater but you could easily roll your own

Using Public Wireless Networks

- Public wireless are ubiquitous now
- Free wireless networks are unsecured
- Even hotel networks or networks that require logins are often unsecured
- Users aren't aware of the risks involved in using wireless networks

Using Public Wireless Networks

- You can't stop users from connecting to Wireless networks with their devices
- So you have to train them to understand the risk
  - Don't allow folder sharing
  - Make sure there is a local firewall if it's a laptop
  - Explain what SSL is and how using https:// etc encrypts traffic
- Discourage them from ever entering any passwords for software you don't manage whilst on public networks
- Notes passwords are not transmitted
- Domino HTTP passwords are hashed but not encrypted unless you are using SSL
- A corporate VPN provides additional security and protects Homer from local network snooping
- There are limited things you can do on smartphone devices to protect your users
  - Ensure they understand their level of exposure and that your corporate data is secured via SSL

Using Other People's Computers

- Everyone has a computer at home now
- Travelling on holiday or business there are business center's to use at hotels
- Borrowing a friend's computer to check your mail

- Browsers cache and remember leaving a trail of security clues behind

Using Other People's Computers

- Explain the risks involved in using someone else's browser
- Clear browser history
- Avoid storing passwords and usernames
- iNotes is designed to logout and clear cache

Installing Other Useful Apps

- Smartphones all come with their own “app stores” now
- They are designed to encourage users to install their own apps
- Many require location services and access to other application data to work

Installing Other Useful Apps

- It's all about understanding risk and exposure again
- It's also about protecting your corporate data from other applications
- Some platforms (like Blackberry) allow you to lock down devices to prevent other apps being installed

The Rogue Developer & His Junior Sidekick

- Hard to Fence In
  - His code can read (and write) to anything
- His agents steal I/O, Bandwidth, Performance, and Pic-a-nic Baskets
- He makes last minute “Fixes” on Friday Afternoon
- Junior Developers can be pressured into doing what they know is wrong
  - building applications with very poor security

Keep the Rogue Developer inside the Park

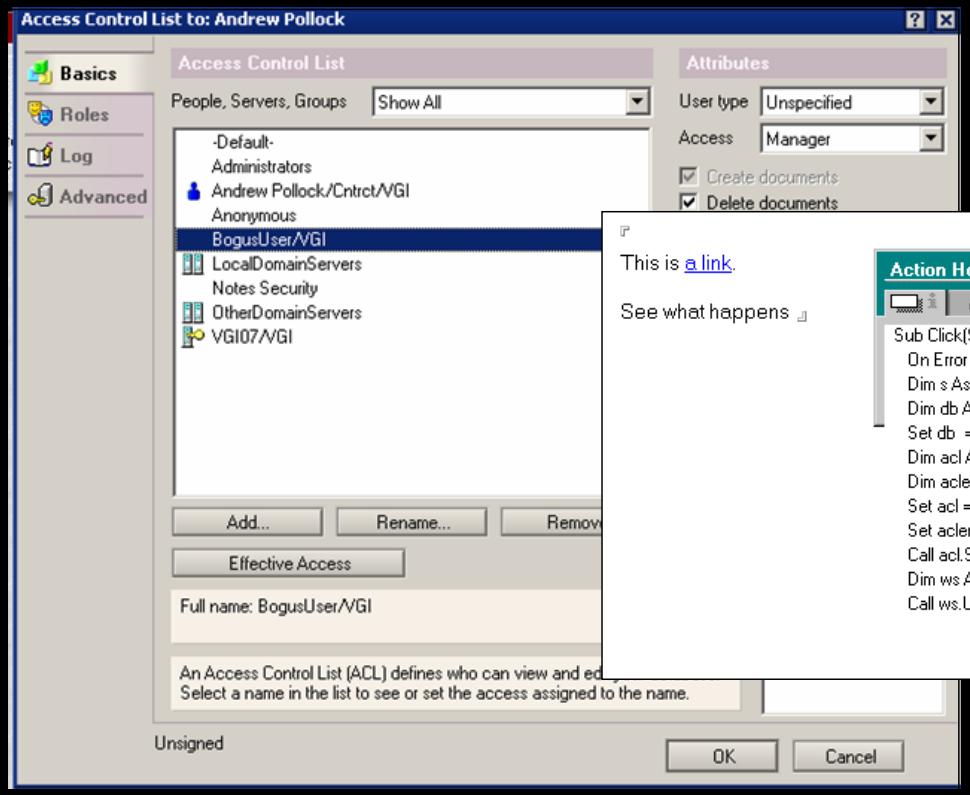
- Require Specific “Agent Signing” ID Credentials
  - Different (and more difficult to justify) credentials for unrestricted agents
  - No Full Access Administrator rights on Agents
    - If truly necessary, use a single unique credential for each use case
  - Consider a unique signing agent for truly confidential data sources
    - Use ACLs to block “normal” signing agents from accessing these
- Accommodate “Emergency” change control bypasses with special ID’s
  - Immediately log use of these credentials to log files on other servers
  - Consider automatic management notification when used
  - Sometimes you have to ask forgiveness rather than permission

Beware of Last Minute “Quick Solutions”

- Enforce Change Control
  - Do not allow developers to make changes on production servers
    - This includes deploying new templates
  - Some solutions must be tested in full scale environments
    - Particularly Java Agents
- Changes to production code without adequate testing
  - Rogue agents can consume a huge amount of resources
  - Changes made just before the weekend can destroy data
    - Leaving the helpdesk unable to satisfy user needs
- Beware the Law of Unintended Consequences

Protect Pic-a-nic Baskets from Rogue Developers

- Use ECLs (Execution Control Lists)
  - Prevent developers (and unofficial developers) from running unauthorized code on desktops



The Junior Developer Can Leave You Exposed

- Manage the process of deciding what security controls are appropriate when developing applications
  - 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

- 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

The Engineering Genius

- He loves technology and is an expert, just not on any Lotus product
- He regularly reads about new and exciting tools and wants to use them
- No problem is too small for him to divert his energy towards
- The geekier the solution the more he likes it

Even Genius Has Its Limits

- When you have a hammer everything looks like a nail
- “New” is always better than “Old”
- The Occam’s Razor rule of security - sometimes the simplest solution is the best

When You Have A Hammer .....

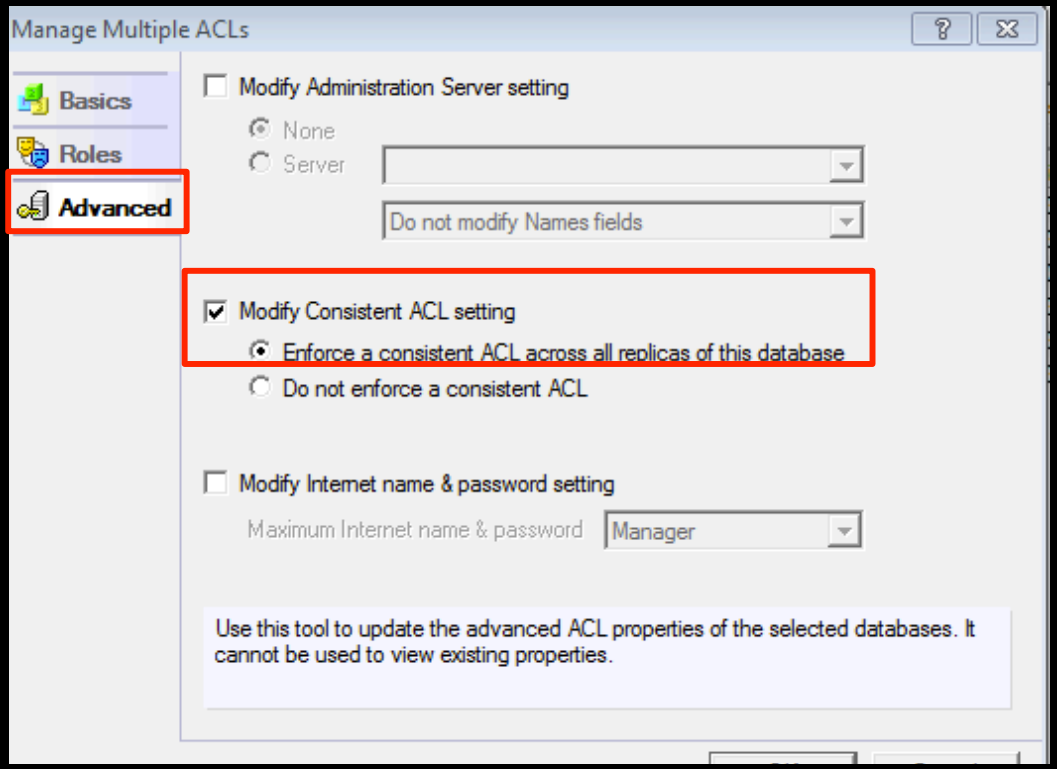
- OS guys and Network guys like doing OS and Network type stuff
  - Sharing folders and partitions so they are more accessible
  - Storing IDs on the network file share
  - Locking down the OS and accessible ports
  - Having a single “Administrator” ID that is shared
- SANs are expensive and the person with the most expensive technology gets to say how it works
  - Domino works fine with SANs but only if you configure it correctly
- Firewall guys who don’t know Domino opening the wrong ports

When You Have A Hammer .....

- There is no reason to want to browse to Domino data, you should always ensure that the file sharing for Domino data partitions is disabled
  - Don't share Domino data partitions with other programs
  - Databases stored directly on the Domino server aren't encrypted
- Enable "Enforce Consistent ACLs" on all databases to ensure access restrictions are maintained even if a database is copied somewhere else
  - Advanced properties under database ACL
  - If it's not enforced a local replica grants Manager access and no roles

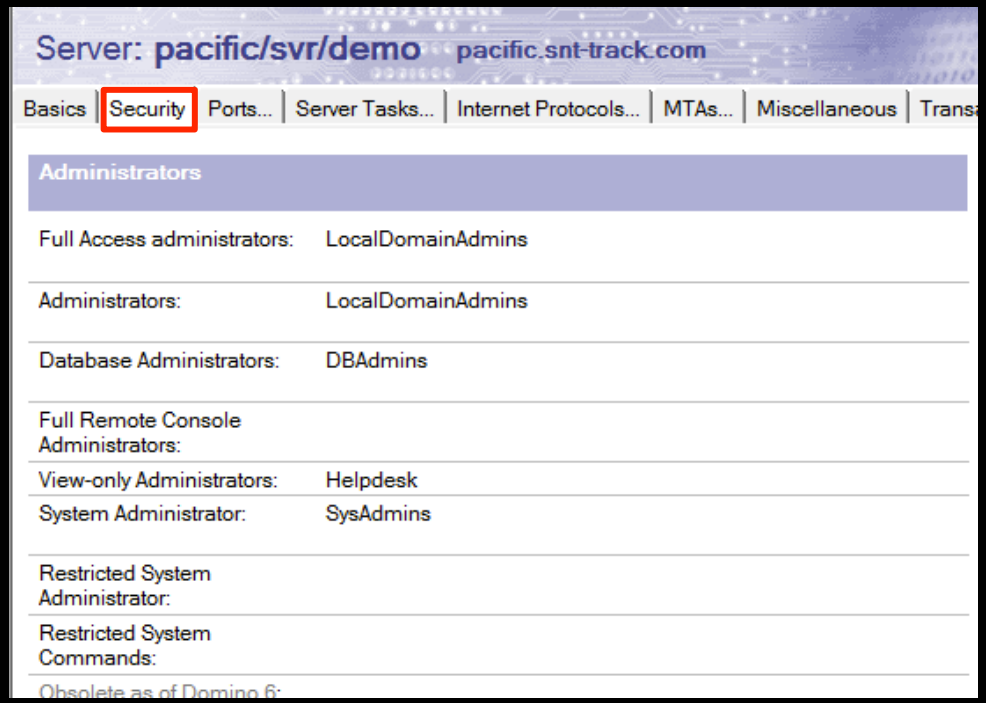
When You Have A Hammer .....

- To Mass Change “Enforce Consistent ACLs”
  - Actions - Full Admin Administrator from within the Administrator client
    - If you don’t do this you won’t have right to modify every database
  - Right click on the top level directory and choose “Access Control” then “Manage”
  - Click on Advanced and Modify Consistent ACL setting to “Enforce Consistent ACLs”



When You Have A Hammer .....

- IDs should never be copied around or shared
  - Complete the LocalDomainAdmins group with the names of all Administrators, or create your own group
  - In the server document - security page there are many options for granting administrative access to a server
    - Very few people need overall Administrative powers
    - Even fewer people need Full Access Administration
  - Use ID Vault to store ids in an encrypted secure environment



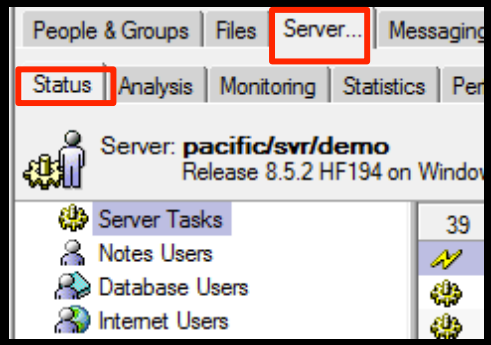
When You Have A Hammer .....

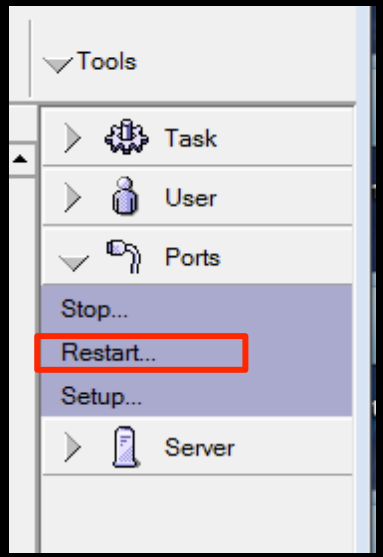
- If you're going to ask for firewall ports to be opened for your services, make sure you are only asking for secure ports
  - Enable SSL on any TCP port you use HTTP, POP, LDAP, IMAP, SMTP
  - Consider using TLS for outbound SMTP delivery if you use an outbound messaging service such as messagelabs or postini
    - SMTP transport on port 25 can be intercepted and isn't encrypted
    - Transport Security Layer - SSL for SMTP
    - Port 465 by default

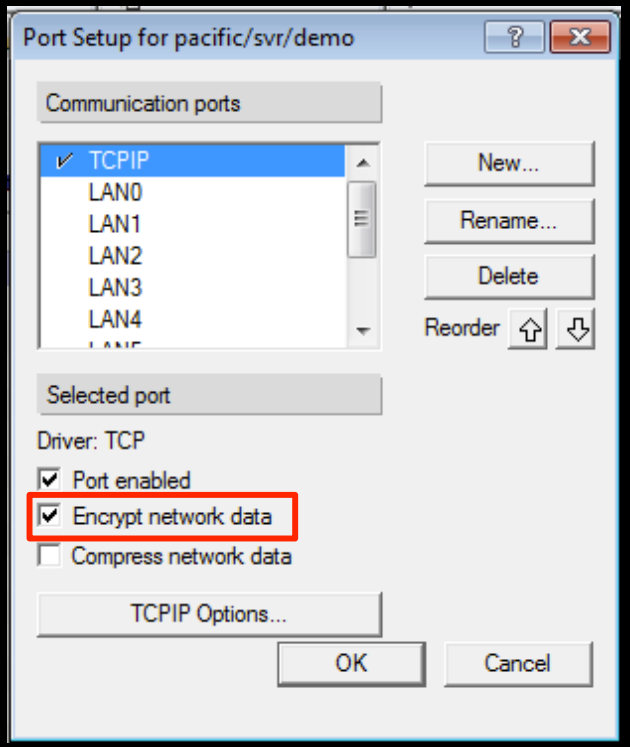
Mail	Mail (SMTP Outbound)
TCP/IP port number:	25
TCP/IP port status:	Enabled
Enforce server access settings:	N/A
Authentication options:	
Name & password:	N/A
Anonymous:	N/A
SSL port number:	465
SSL port status:	Disabled
Authentication options:	
Client certificate:	N/A
Name & password:	N/A
Anonymous:	N/A

When You Have A Hammer .....

- Set up a passthru server with an encrypted network port to handle roaming user replication requests
  - Set the server up in another domain so it has an empty names.nsf
  - Encrypt Network Data on its TCPIP port so that all traffic passing through Domino between a public client and your private network, is encrypted





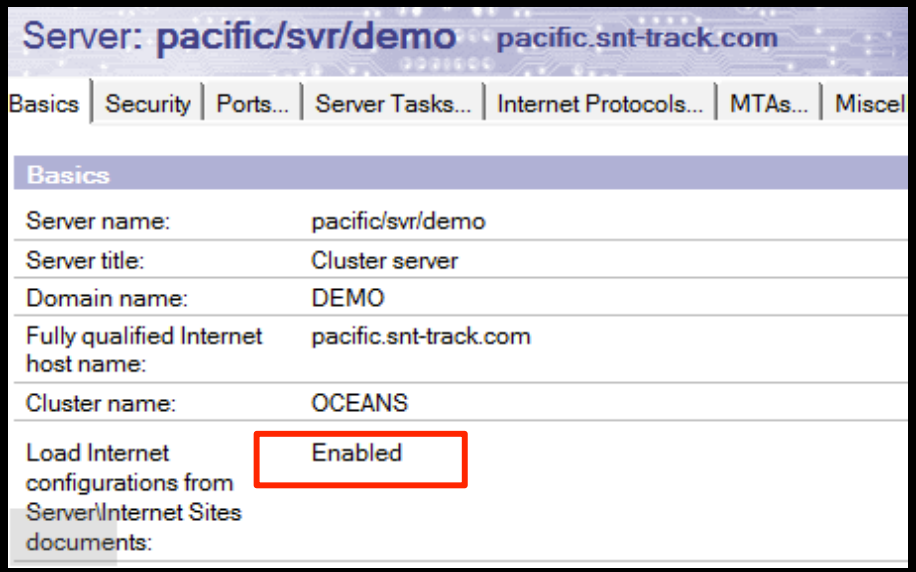


"New" Is Always Better Than "Old"

- The perception that a new piece of software has got to be better than an existing feature on software you already have
- The new software or technology is designed to standalone, getting it to work with Domino often involves compromising Domino's security
  - Desktop virus protection products that scan inside databases
  - Defragmentation tools
  - Disk Mirroring tools
  - Tools that require IMAP enabled or DIIOP

"New" Is Always Better Than "Old"

- Never enable a new access port for a single tool unless you have reviewed
  - what that tool is doing
  - what identity is being used to run the tool
    - who knows / uses that identity and how it is secured
- Always enable new ports using Internet Site Documents so you can restrict access to a specifically assigned hostname
  - Never allow anonymous access



"New" Is Always Better Than "Old"

- Don't disable a Domino security feature to allow another tool to work
  - Single sign on can be done via Notes Shared Login but the reason for not doing it would be policy based not technical so another tool offering single sign on would not necessarily be better
    - eg. if people don't logout of Windows when away from their desks
    - or if people share desks and Windows logins

"New" Is Always Better Than "Old"

- Use SPNEGO to enable single sign on for TCP activity such as HTTP or Sametime
- 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 if multi server single sign on is enabled

“New” Is Always Better Than “Old”

- Not enabling any ECL settings so that a 3rd party program can run effectively is a very bad idea
  - 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
- Enforce and lockdown ECLs via a policy with security settings so only the authority you need is granted rights

Occam's Razor Rule Of Security

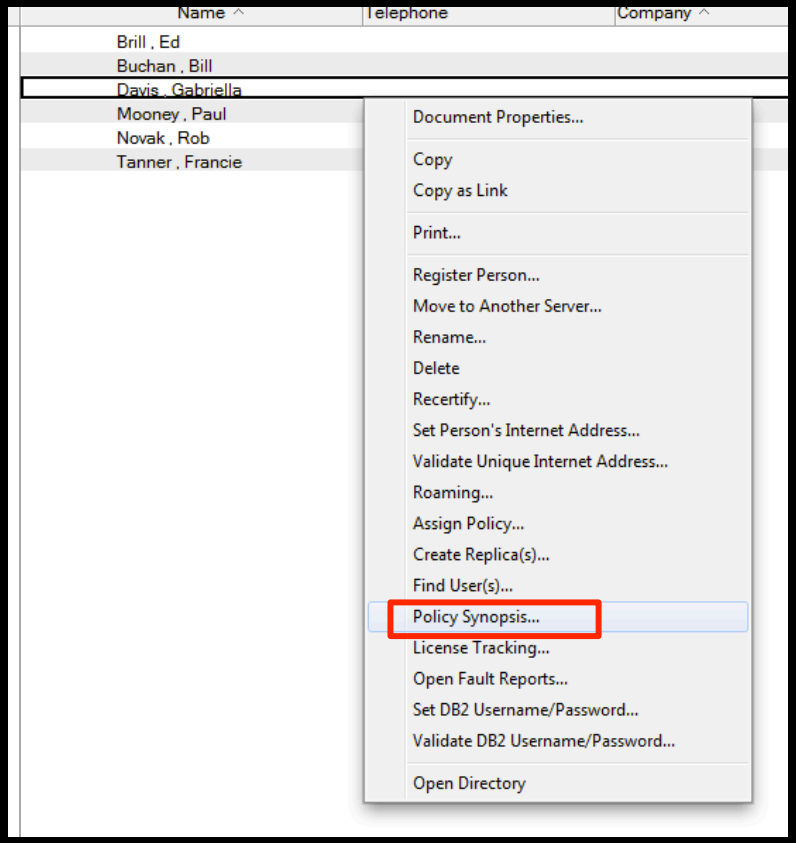
- More doesn't always mean better, too many security settings can make the system impossible to use
- Developers like to develop their way out of a problem

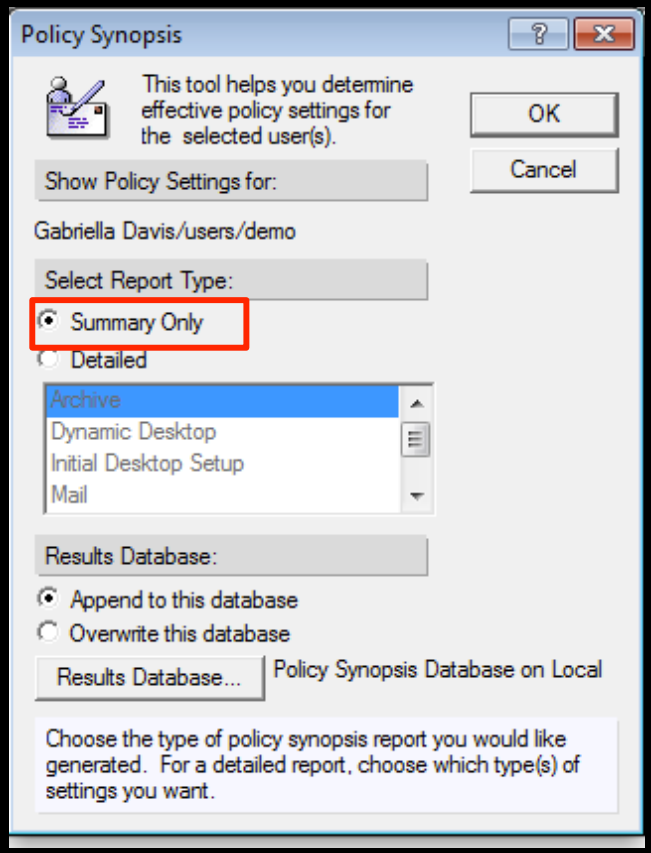
Occam's Razor Rule Of Security

- Multiple policies can be applied to a person and are resolved in the following order
  - Organisational ie /London/Turtle - everyone in the OU=London, O=Turtle hierarchy
  - Dynamically - an explicit policy that is assigned to a group
  - An explicit policy assigned manually
- Understanding what settings are going to be applied from the merging of multiple policies avoids unexpected results

Occam's Razor Rule Of Security

- A manually applied explicit policy overrides all other and there can only be one
  - dynamically applied explicit policy settings and organisational policy settings are merged as well and conflicting settings are resolved in the order
    - manual, explicit, organisational
- To review what policy settings will actually apply, right mouse click on the person document in Administrator and choose Policy Synopsis



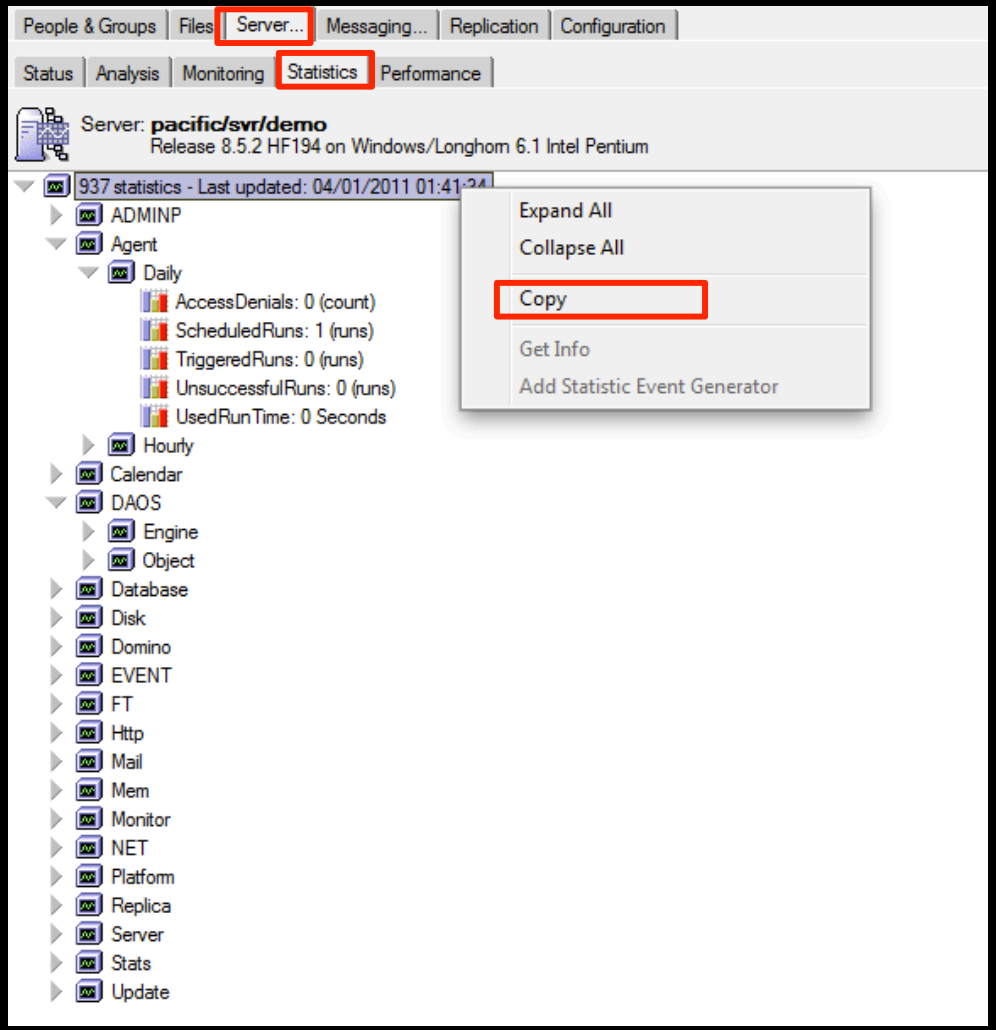


Develop Your Way Out Of A Problem

- There's a lot of information available via Domino reporting and statistics
- There are a lot of ways to apply mass changes to large groups of databases within Domino Administrator
- Code to retrieve the same kind of information or achieve the same effect would have to run at a very high security level on each server

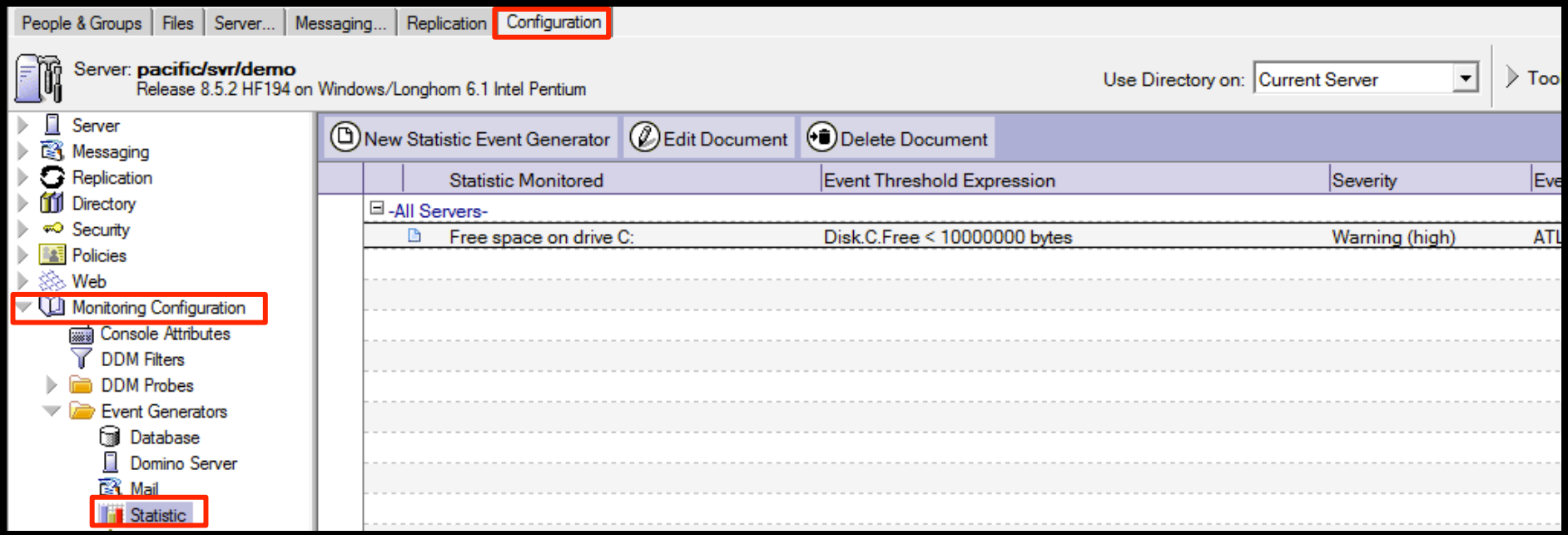
Develop Your Way Out Of A Problem

- Domino Statistics are readily available on each server and can be exported to a spreadsheet from Domino Administrator



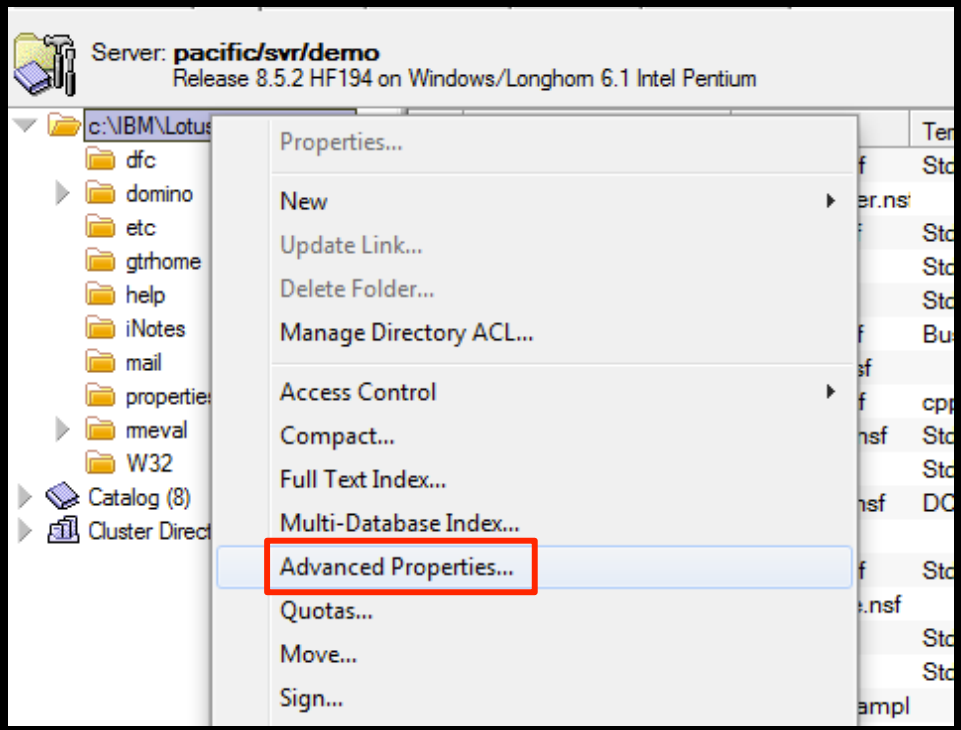
Develop Your Way Out Of A Problem

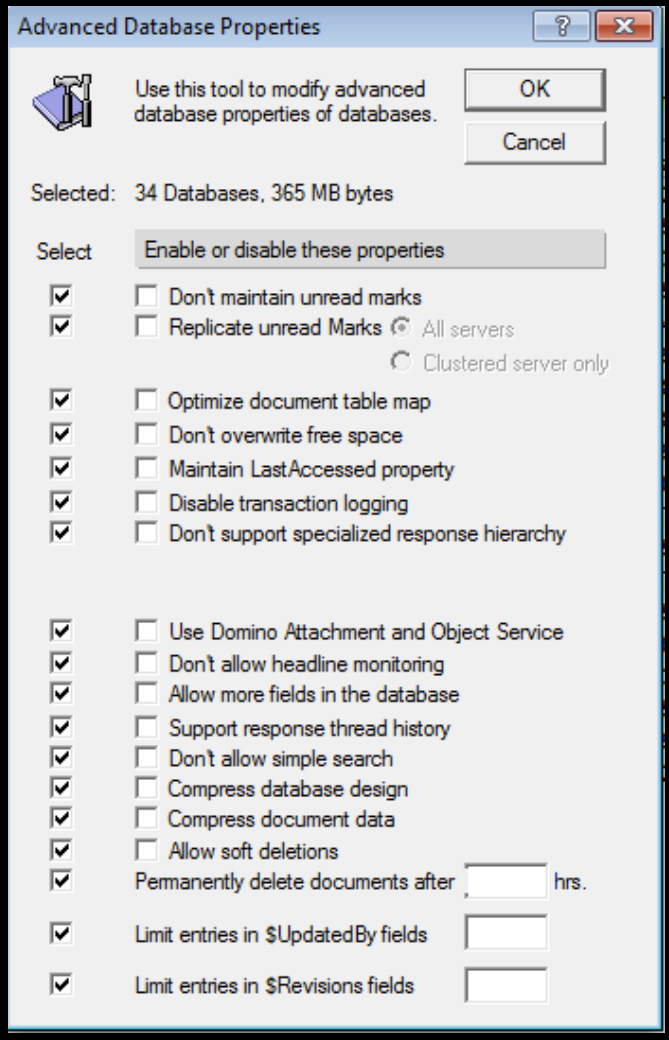
- Statistics Thresholds can be configured to generate alerts if they are hit, configure these in events4.nsf



Develop Your Way Out Of A Problem

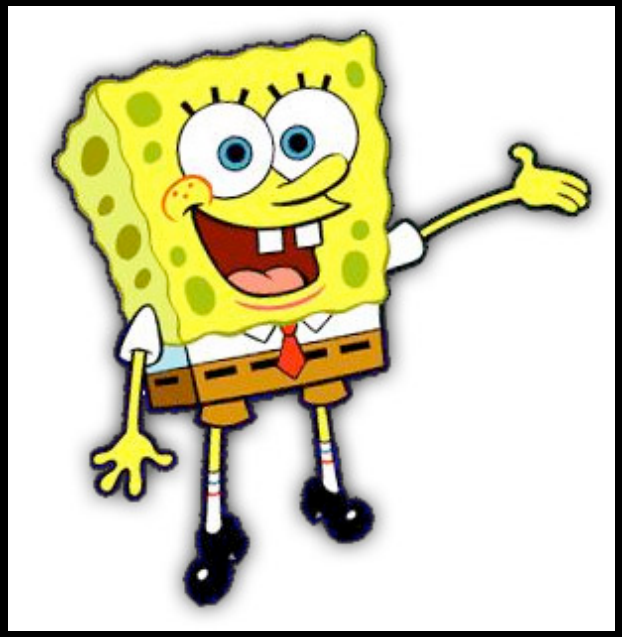
- Mass Changes to databases can be applied via the Advanced properties in the Files menu
  - Right mouse clicking at a directory level means “every db and sub directory under here”





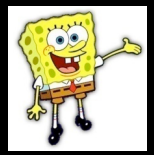
Helpful Helpdesk Support

- Spongebob usually works on 1st Line Support
- He enjoys his job and wants problems to go away quickly so his users are happy
- He knows you're busy and may not get to his problem immediately



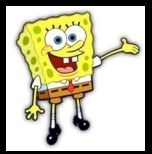
Helpful Is Good Up To A Point

- Often you will equip 1st line with simple tools to fix recurring helpdesk problems because you simply don't have time to fix everything yourself
  - recertify people
  - compact databases
  - refresh / replace design
  - forgetting ids / passwords



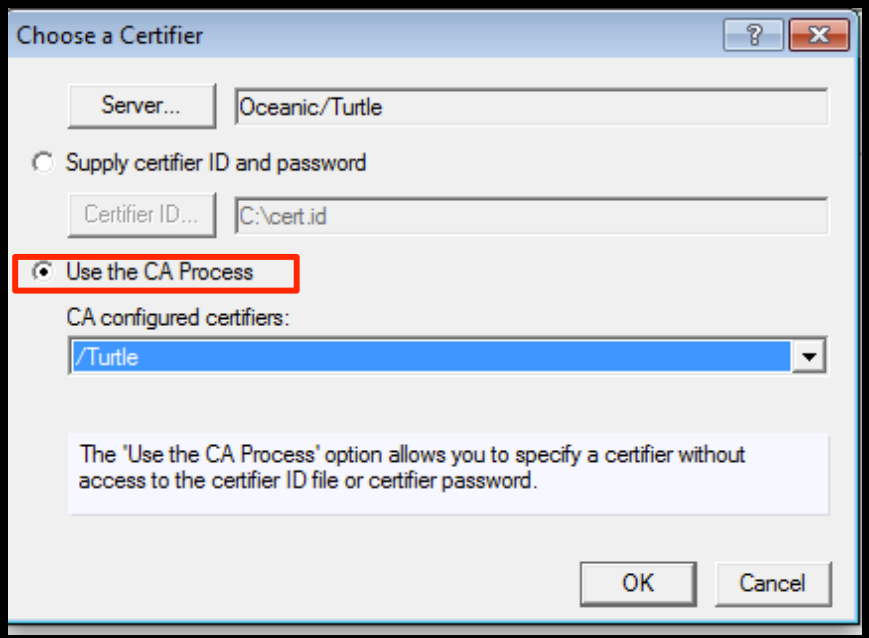
Recertify People

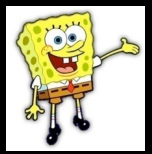
- Giving your helpdesk team certifier files and passwords is a risk
  - If someone leaves you've punched a great whole in your security
- If recertification isn't done properly the public keys aren't updated



Recertify People

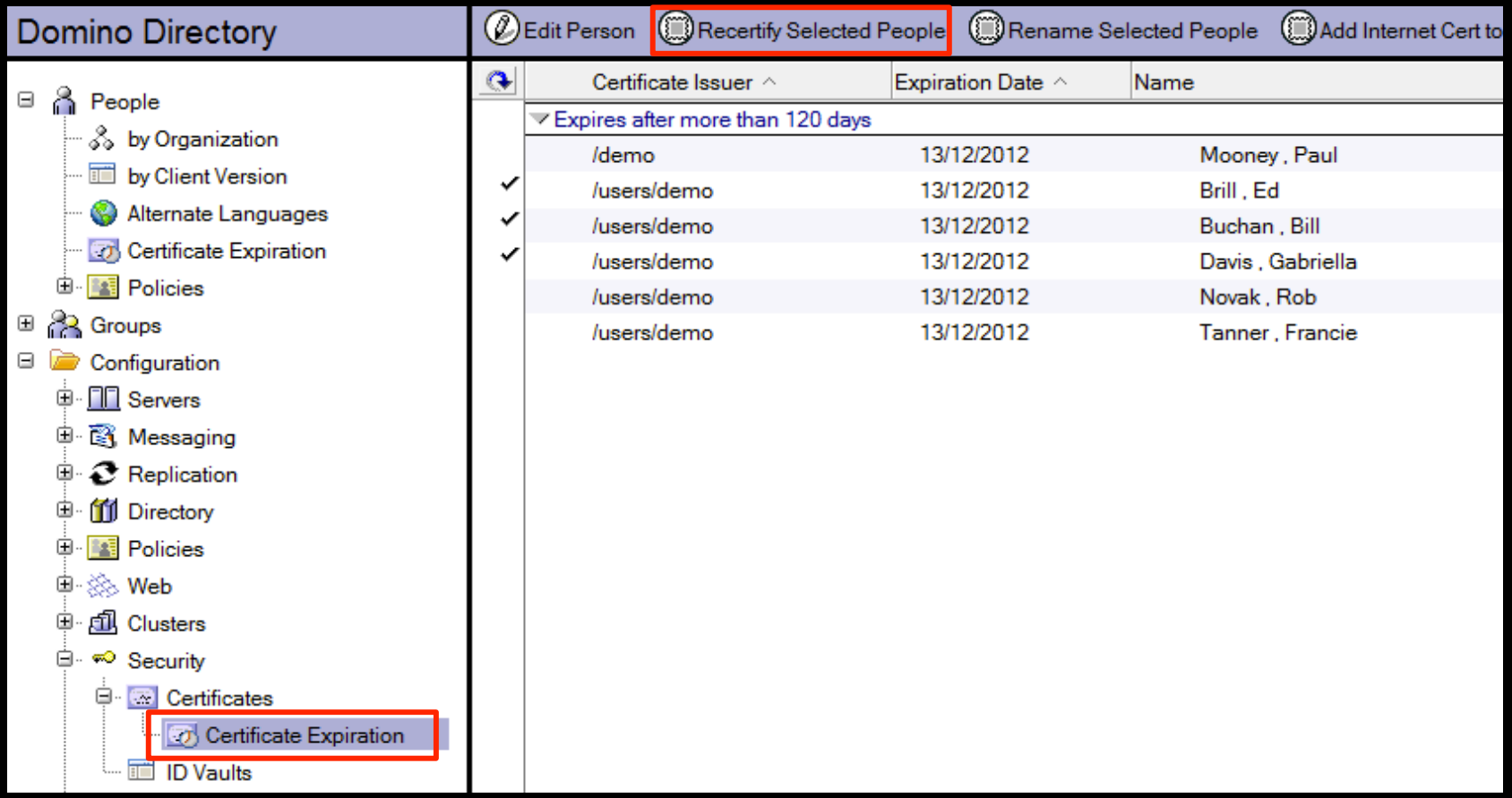
- Using the CA process is easy.
  - You don't need to give people access to certifiers or passwords
  - You grant encrypted rights to certifiers for named users, if they leave you can remove those rights
  - You can use Web Admin to register users





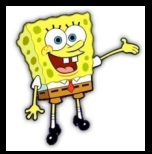
Recertify People

- Certify people in advance yourself, use the certificate expiration view in the Domino Directory
  - View can only be seen by opening the directory up as a database, not via Administrator client



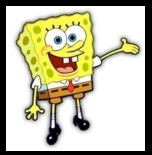
Recertify People

- Put the certlog only on the Admin server and train support to use that as the "Registration Server"
- Without a certlog the server can't create a certificate



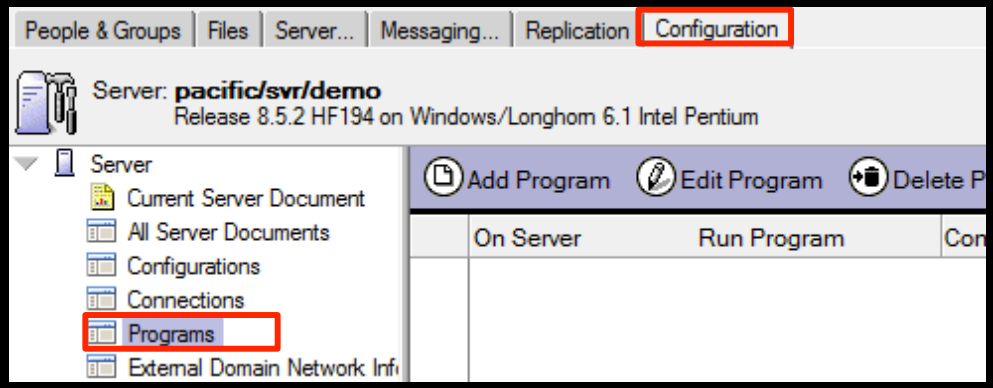
Compact Databases

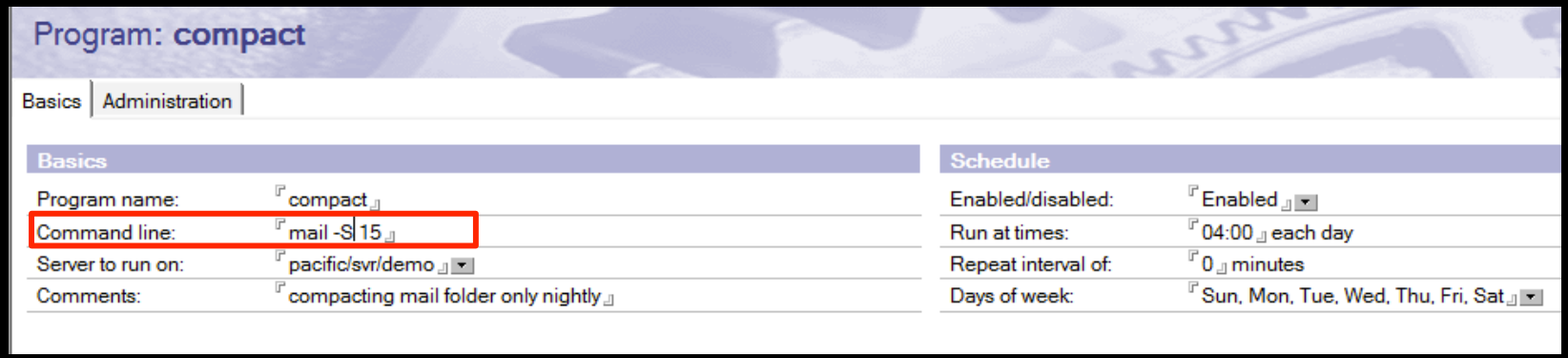
- Users log helpdesk calls asking for their databases to be compacted
  - They mostly do this if you use quotas
- Support are often told to use a copy style compact to fix low level corruptions
  - and once learnt they then re-use it for anything that sounds similar, locking the user out of their mail file and consuming server resources

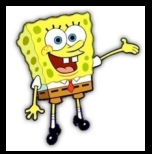


Compact Databases

- Program document that does an in place compact every night for databases with more than 10-15% space (-s 15)







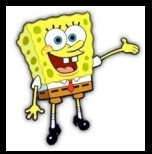
Compact Databases

- Program document weekly, copy style -c to fix low level corruption issues
- Or program document weekly, in place file reduction -B
  - This will create a new DBIID and will result in a full backup from your backup software if you use transaction logging

Program: **compact**

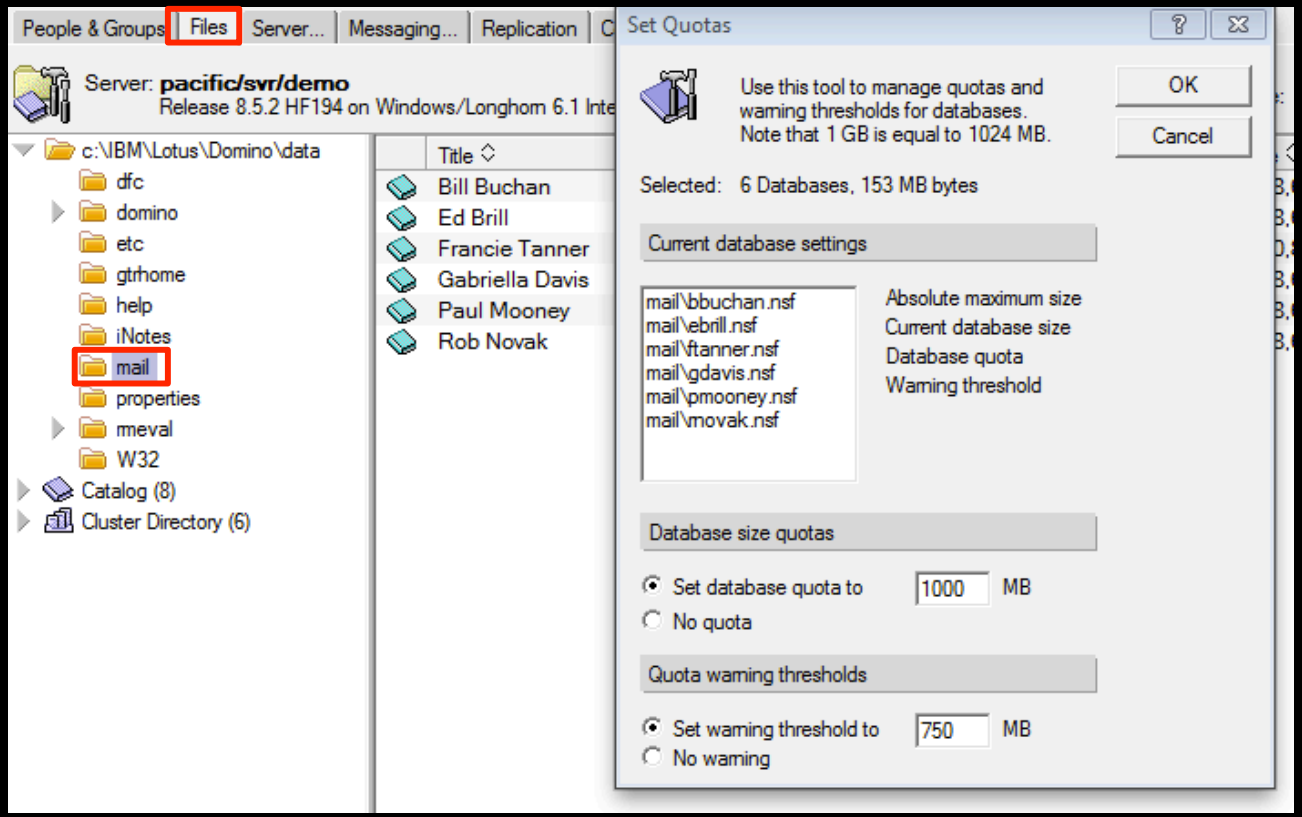
Basics | Administration

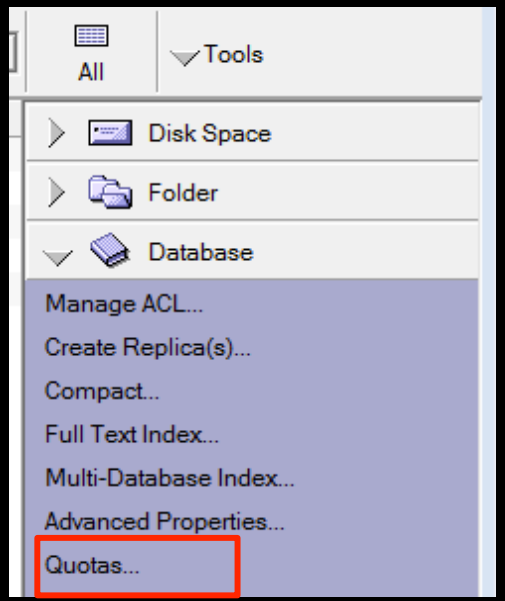
Basics		Schedule	
Program name:	compact	Enabled/disabled:	Enabled
Command line:	-c	Run at times:	11:00 each day
Server to run on:	pacific/svr/demo	Repeat interval of:	0 minutes
Comments:	compacting all databases	Days of week:	Sun

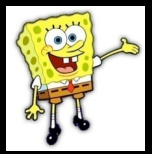


Compact Databases

- If you use quotas, also use warnings. Make sure the users have enough warning to fix their mail in time for a nightly compact
  - If quota is 1GB, warning should be 750MB
  - Allow for at least 2 day's mail traffic between warning and quota

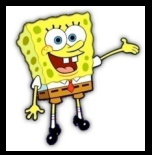






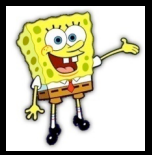
Compact Databases

- **Tip:** Use IND Files and mutiple program documents running at the same time
- IND files contain lists of database filenames
- A compact can be run using a IND filename eg
  - load compact -c -ag.ind
    - tells Domino to do a copy style compact on all files listed in the file ag.ind
- Multiple program documents running at the same time with different IND files will initiate multiple versions of compact simultaneously running against different files
  - Making maximum use of your server resources at off peak times and completing your compact maintenance faster



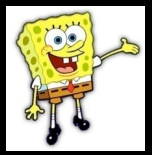
Refresh/Replace Design

- SpongeBob may not understand that the template version cannot be newer than the client version they are using
  - Just because your servers are upgraded to v8.5, doesn't mean your clients all are
    - Users often hotdesk between machines and different versions of Notes
    - Or the user makes a design change and overnight it's overwritten (it happens)
- Replacing designs whilst users are in the database can cause the view they are looking at to suddenly become populated with "replication or save conflicts"
- Replacing designs for remote users will send a lot of traffic during next replication
- Designs that continually 'revert' when replaced are a sign of a broken infrastructure which you need to know about
  - Fixing the same problem over and over frustrates users and makes them lose confidence in the product



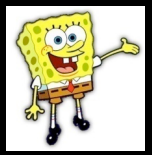
Refresh/Replace Design

- Disable the overnight design task that runs automatically
  - servertasksatx= line in notes.ini
  - Set config ServertasksAt1=Catalog
    - The default installation sets design to run at 1am alongside Catalog
- Remove all servertasksatx settings in notes.ini that the install puts there and replace them with program documents that can be clearly seen and managed across the domain
- If the design task doesn't run then the database design won't be updated unless it replicates in from another server



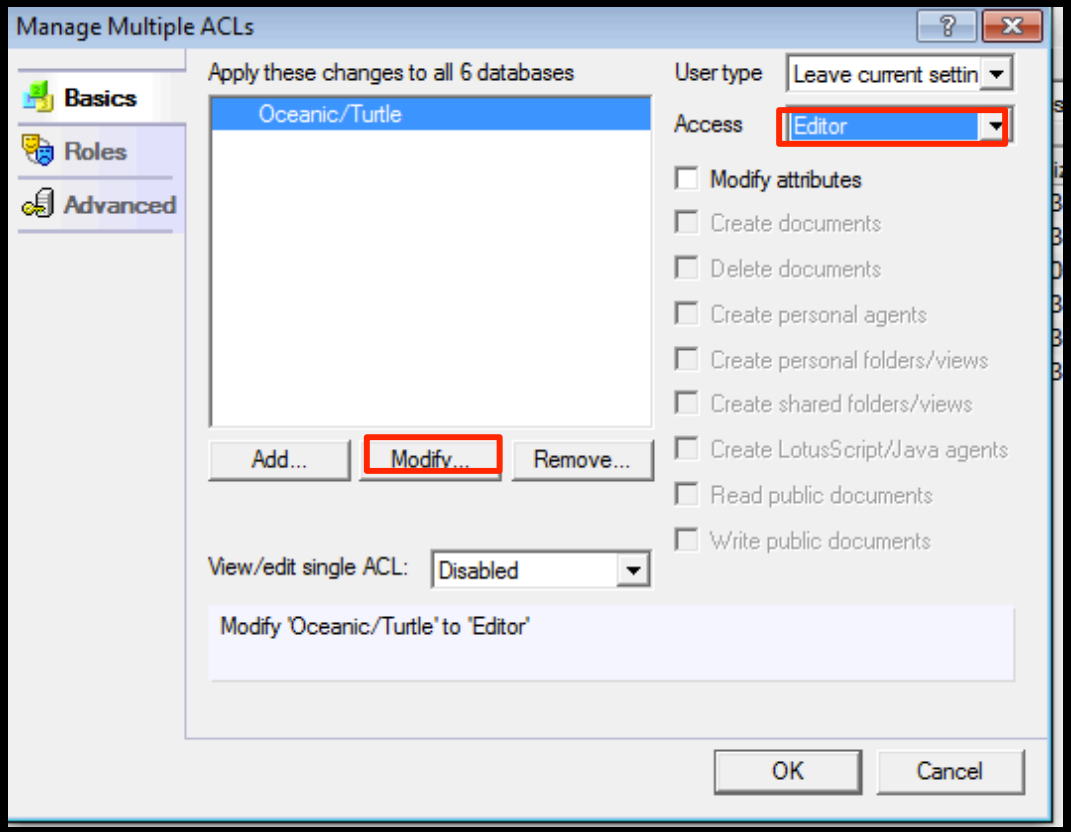
Refresh/Replace Design

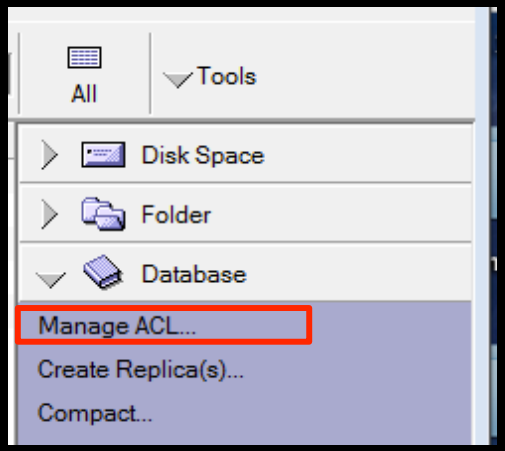
- Remove unnecessary templates from your servers
  - Most templates share replica ids between versions
  - If you install different versions on different servers you risk
    - Replicating templates between servers and updating a database with a template newer than the server can support
    - Not replicating templates between servers but updating the databases with different versions of the same template from different servers
      - This shouldn't happen but if you sign templates and update the design dates, it will

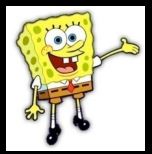


Refresh/Replace Design

- Reduce server access to Editor on all but your design update server
  - Use Global search / replace for ACLs to modify the server access level

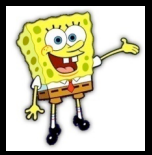






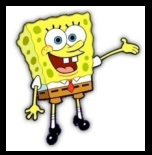
Refresh/Replace Design

- Track repeating calls / repeating problems
- One of any software's biggest problems is when a perceived problem moves to a perception of "that's how it works"
  - *"Notes is rubbish it can't do X"*
  - This often occurs because the user will keep calling with the same problem and SpongeBob, unable to fix it, will tell them "that's just how it works"
    - He doesn't want the user to think him unhelpful by saying "I don't know"
      - Result - user stops calling
      - Result - SpongeBob feels user is happy
      - Result - user never learns the right or better way to do a thing
      - Result - user internalises the concept that "Notes is Rubbish"
- Repeating calls are important, they point to a problem in either your systems or in user training
  - You need to have a plan for dealing with both



Starting Off On The Wrong Foot

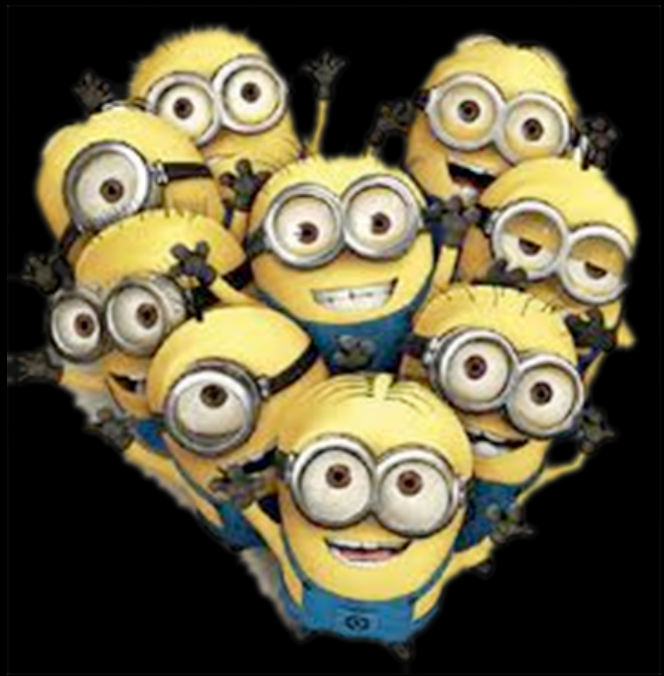
- Users often report, not the problem, but what they believe the problem is
- Fixing a problem is all about asking the right questions
- Give SpongeBob a workflow list of questions to ask users who log Notes related problems for example
  - Are you using Notes or a Browser?
  - What version are you using?
  - Does the same thing happen if you try another document?
  - Does the same thing happen if you try a new document?
  - What does the error message on screen say exactly ?
  - When did it last work correctly?



Script Kiddies & Spammers

- They can't be bargained with
- They can't be reasoned with.
- They don't feel pity, or remorse, or fear, and they absolutely will not stop, ever.

- Individually Harmless – But there are a lot of them
- They don’t know how they’re causing you problems
- They take advantage of common weaknesses
  - System Weaknesses
  - Human Weaknesses



Fighting Spam & General Malware

- Malformed spam and malware can cause major server problems
- Stop spam and malware before it gets to Domino
  - Offsite Third Party Mail Filtering
    - Best for micro, small, and medium businesses
    - Stops most virus, worms, and trojans embedded in email
    - Reduces the load on your internet connectivity
    - Privacy concerns for some companies
  - Onsite dedicated appliances & servers
    - Fewer privacy concerns
    - Does not reduce WAN connectivity load
    - Expensive to purchase, maintain, and scale up
  - Domino server based tools make a good secondary wall

Malware Sources Change

- In the first quarter of 2009, malicious PDF files made up 56% of all exploits tracked by ScanSafe. That figure climbed above 60% in the second quarter, over 70% in the third and finished at 80% in the fourth quarter.

"PDF exploits are usually the first ones attempted by attackers.

Attackers are choosing PDFs for a reason. It's not random. They're establishing a preference for Reader exploits."

  - Source: http://news.techworld.com/security/3212863/adobe-patches-pdf-vulnerabilities/

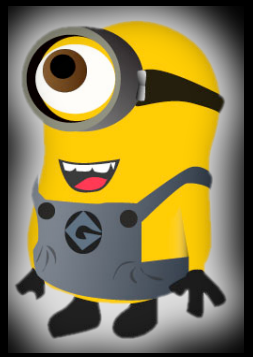
- Standard Anti-Virus/Anti-Malware software belongs on the desktop
  - Keep it up to date
  - Not necessary on the server
  - Never use non-Domino aware anti-malware on the Domino server

Script Kiddies & Spammers

- Scripted attacks look for weaknesses in your internet password management
  - Not just using the HTTP port
  - SMTP password guessing is a very common vector of attack
    - If a user's password is guessed, the spammer will use authenticated access to make your servers a spam source
  - Frequent name guessing targets are not just common names like "jsmith"
    - Common scripts attempt password guessing on names like this
      - test@domain.com
      - guest@domain.com
      - admin@domain.com
      - helpdesk@domain.com
      - support@domain.com
    - These named accounts frequently have common passwords

Scripts keep up with version changes. Do you?

- Scripted Attacks Know Your Software's Weaknesses
  - Many security fixes with version level patches are implemented through minor design changes in the standard templates
    - Avoid making changes that will prevent you from updating your standard template designs when patches come out
  - At least keep any public internet facing Domino servers patched with the latest security fixes
    - Even if you don't roll out a version change across the domian
- And of course – Follow industry standard security practices
  - Block all ports your don't need
  - Don't run services you don't use
  - Periodically review log data



The Bitter Ex-Admin

- He knows enough about Notes and Domino and how it's installed at your company to be dangerous
- He once had access to all your security; certifiers, passwords and sometimes even user ids or http passwords
- He will morph from happy to bitter in an instant if he loses his job or if he just leaves (or needs a nap!)
- He actively dislikes your company or at least someone at it so spite can be a motivator

Getting His Revenge

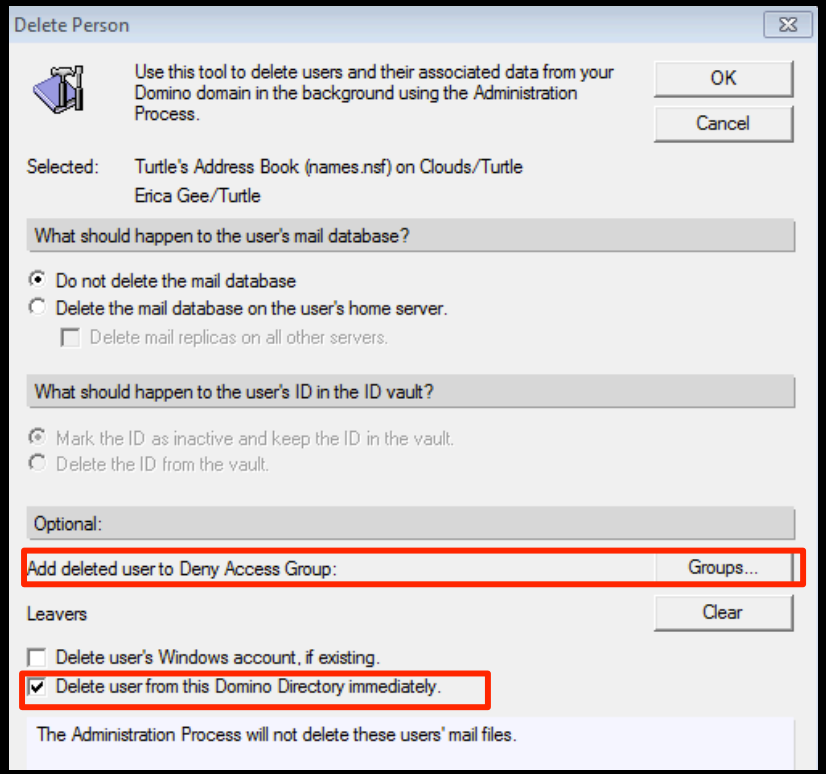
- Takes a copy of his Notes ID
- Takes copies of all your company ids
- Takes copies of all your certifiers
- Uses HTTP accounts he knows to continue to access information

Takes A Copy Of His Notes ID

- With his Notes ID and knowledge of your servers he can remotely access your environment
- Many companies are too scared to remove the Admin user from server rights, ACLs, agent signatures etc in case “things break”

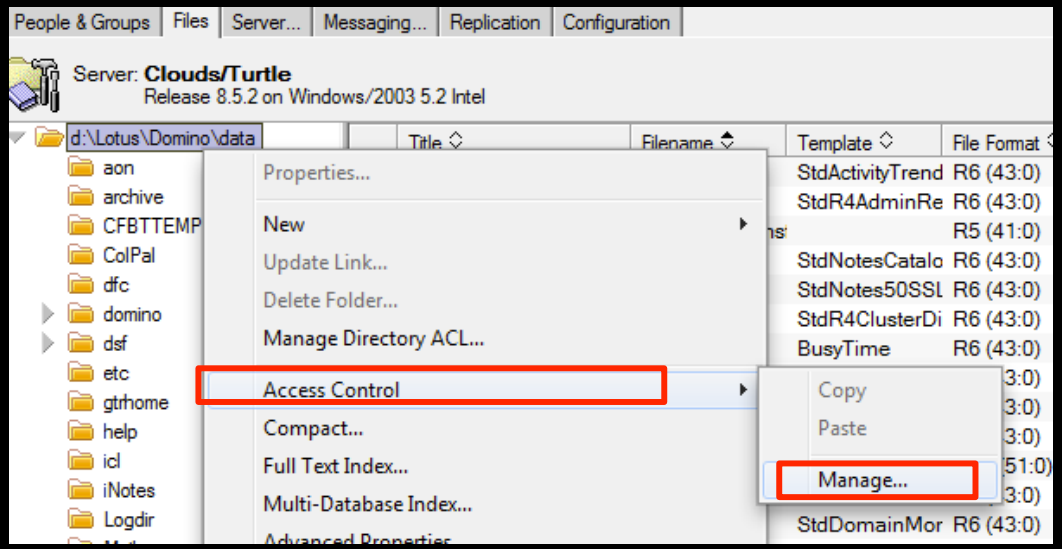
Takes A Copy Of His Notes ID

- Put him in the deny access group as soon as he leaves
  - Make sure that group is used by all servers
  - Make sure , if you have multiple Domino domains, that he is included in the Deny Access group for all of them
  - Delete him and let the adminp process remove him from everywhere

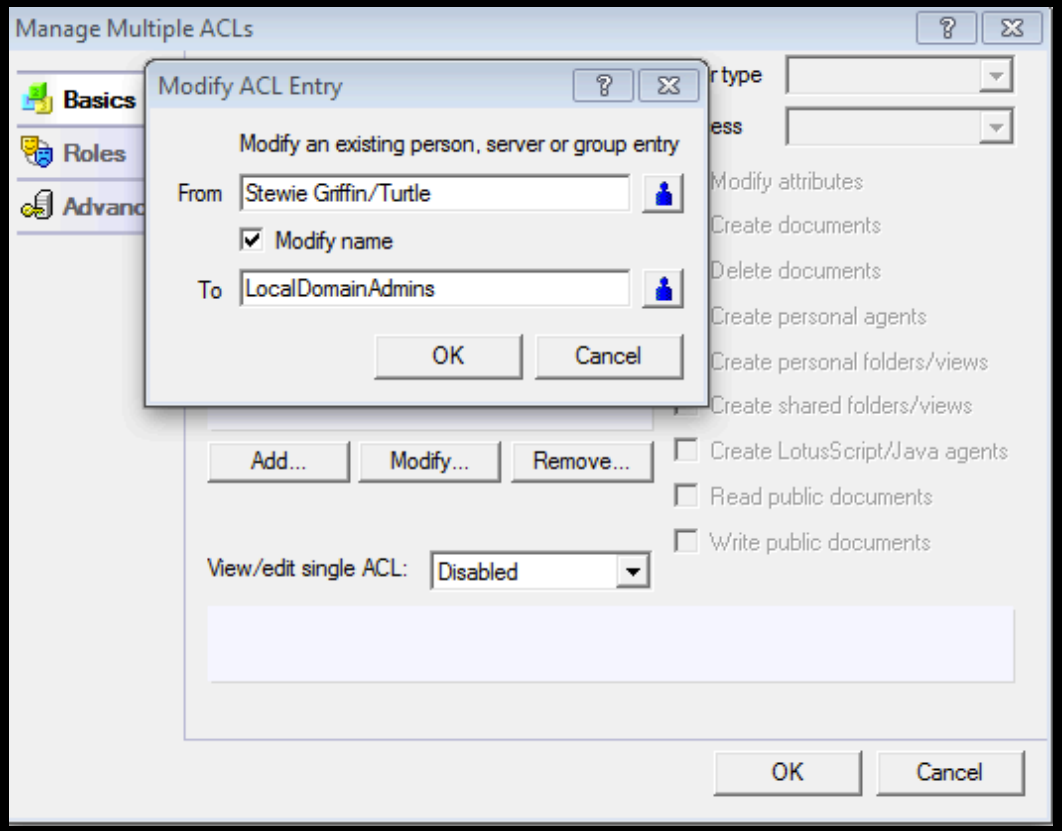


Takes A Copy Of His Notes ID

- Create an Administration group, if you don't have one already and use that for all ACL and server access settings
  - Use Global search / replace for ACLs to replace his name with the group name everywhere
  - Remove him from that group

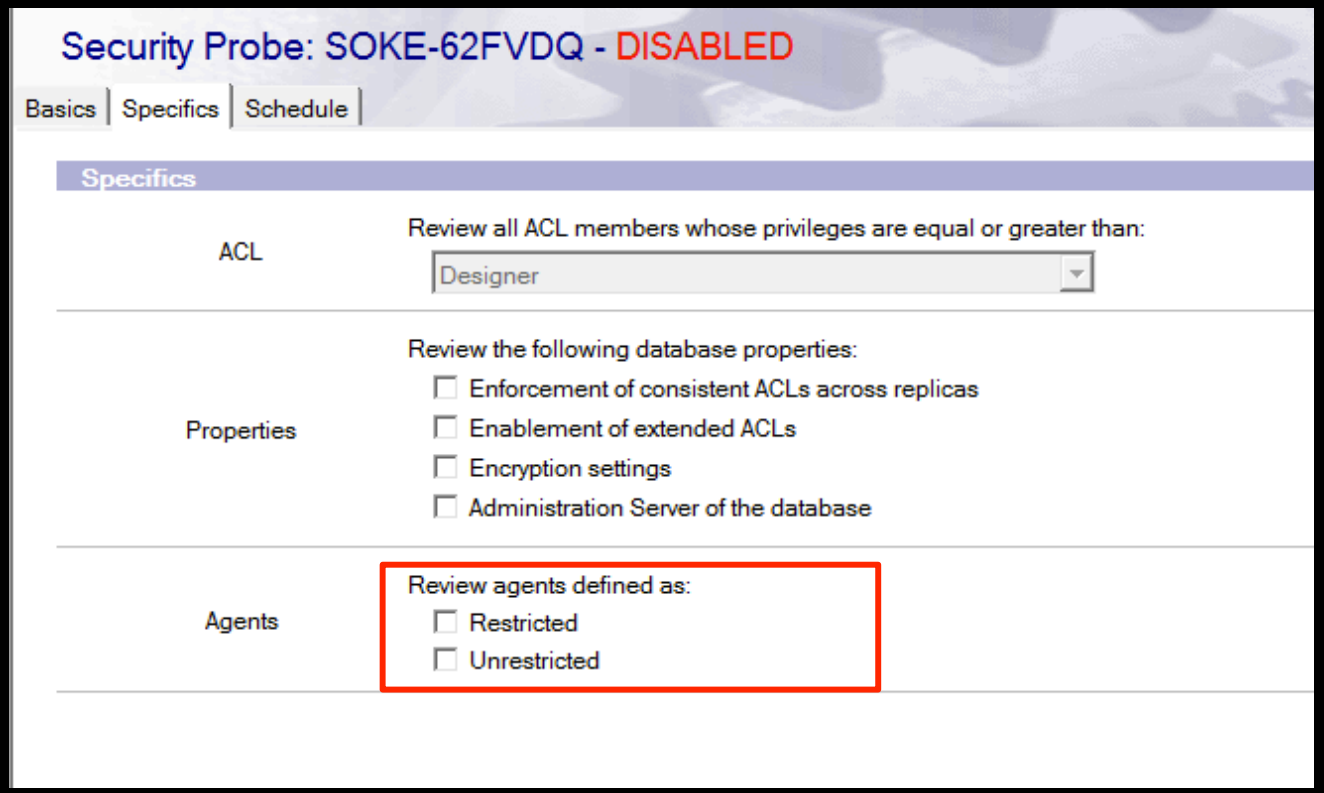


Takes A Copy Of His Notes ID



Takes A Copy Of His Notes ID

- Use DDM Security Database Review to report on all agents on a server and who signed them
- Use DDM Security Database ACL to report on any database ACLs still containing his name



Takes Copies Of ALL Your Company IDs

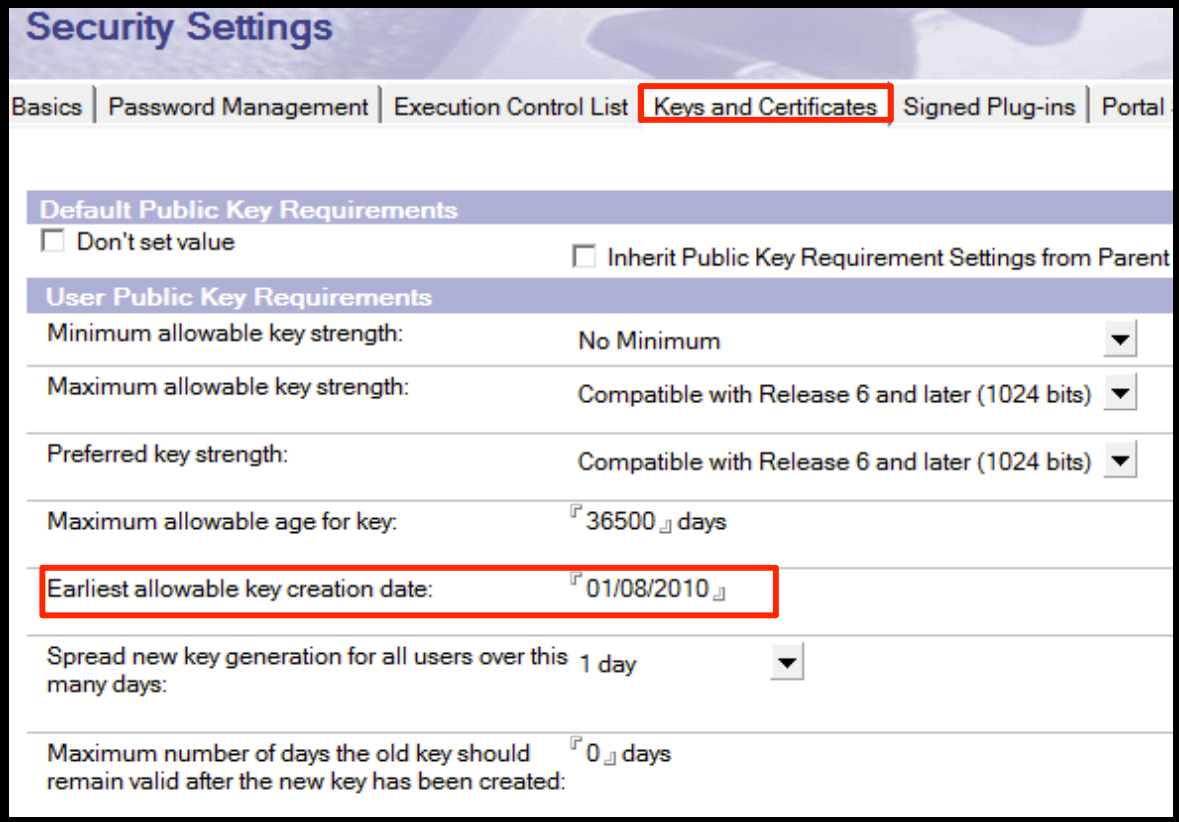
- You store your company IDs on a network share that is accessible by IT
  - these are ‘backup’ ids, copies of originals created with default passwords
  - since he has both the ids and the passwords, he can just use any id that is still valid (whose certifier hasn’t expired)
  - You can’t differentiate between his illegal use of the ID and a ID owner’s valid user

Takes Copies Of ALL Your Company IDs

- Don’t keep backups of IDs
  - You don’t need to with ID Vault now
  - They weren’t much good anyway since a recertification or name change would make them unusable
- Configure ID Vault and use that for storing IDs

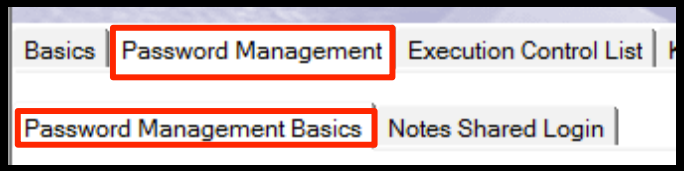
Takes Copies Of ALL Your Company IDs

- If your IDs are compromised, use a security policy to generate new keys for all users
  - Then turn on public key checking



Takes Copies Of ALL Your Company IDs

- If one or more IDs are compromised, turn on password expiry and password checking on each server
  - Password Expiry set in security settings under policies



Password Expiration Settings

Enforce Password Expiration	Notes & Internet
Required Change Interval	365 days
Allowed Grace Period	0 days
Password History (Notes only)	50 passwords
Warning Period	30 days
Custom Warning Message	

Takes Copies Of ALL Your Company IDs

- Password checking set in server document and in person documents
- Server Document - Security Page

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:	○ Yes ◉ No
Check passwords on Notes IDs:	◉ Enabled ○ Disabled

- Person document - Administration Page

Password Management	
Check password:	Don't check password
Required change interval:	0
Grace period:	0
Last change date:	
Password digest:	
Last change date: (Internet Password)	[redacted]22:24:28 GMT
Force user to change Internet Password on next login:	☐ Yes

Takes Copies Of ALL Your Certifiers

- Certifiers are the keys to your Domino kingdom
- Losing any certifier is bad, but losing a root certifier means he can create new OUs
  - Losing server ids which usually aren't password protected is also a high level risk
- Your entire infrastructure is potentially compromised

Takes Copies Of ALL Your Certifiers

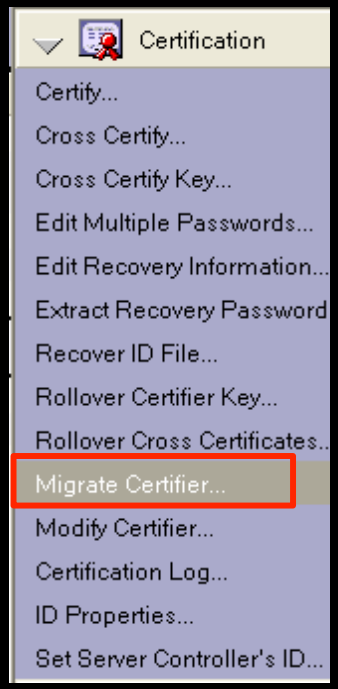
- Use the CA process to migrate the certifiers into encrypted databases and then lock the original files away
  - No-one, including the Admin should need access to, and passwords for, those certifiers so they can be secured away
  - The CA process means you don't need to grant anyone access to any of your certifiers, all certification is done by the server
  - Using the CA process doesn't preclude you from continuing to use certifiers if you want

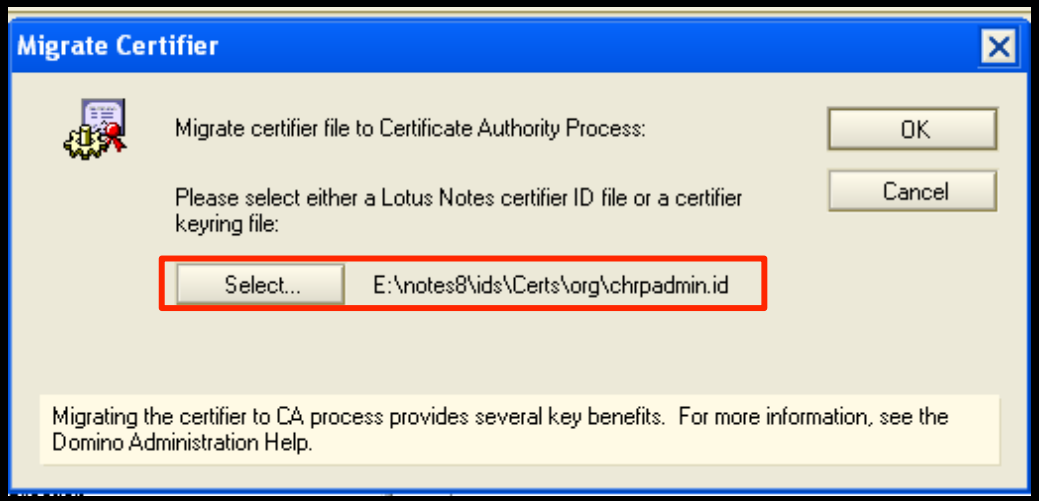
CA Process Steps

- 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 priviliges 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

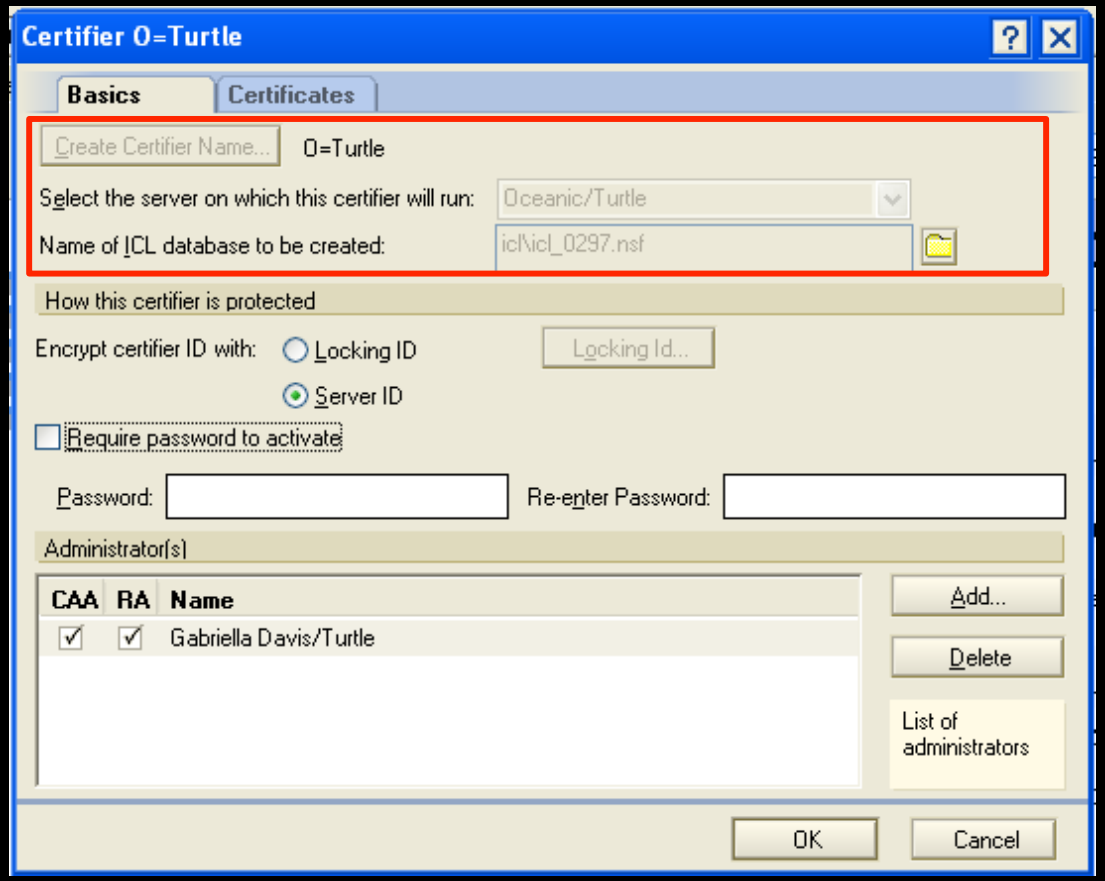
- Configuration tab in Domino Administration
- The properties of the physical certificate (e.g. password recovery) are migrated to the CA certificate when it is first set up but not kept in sync thereafter





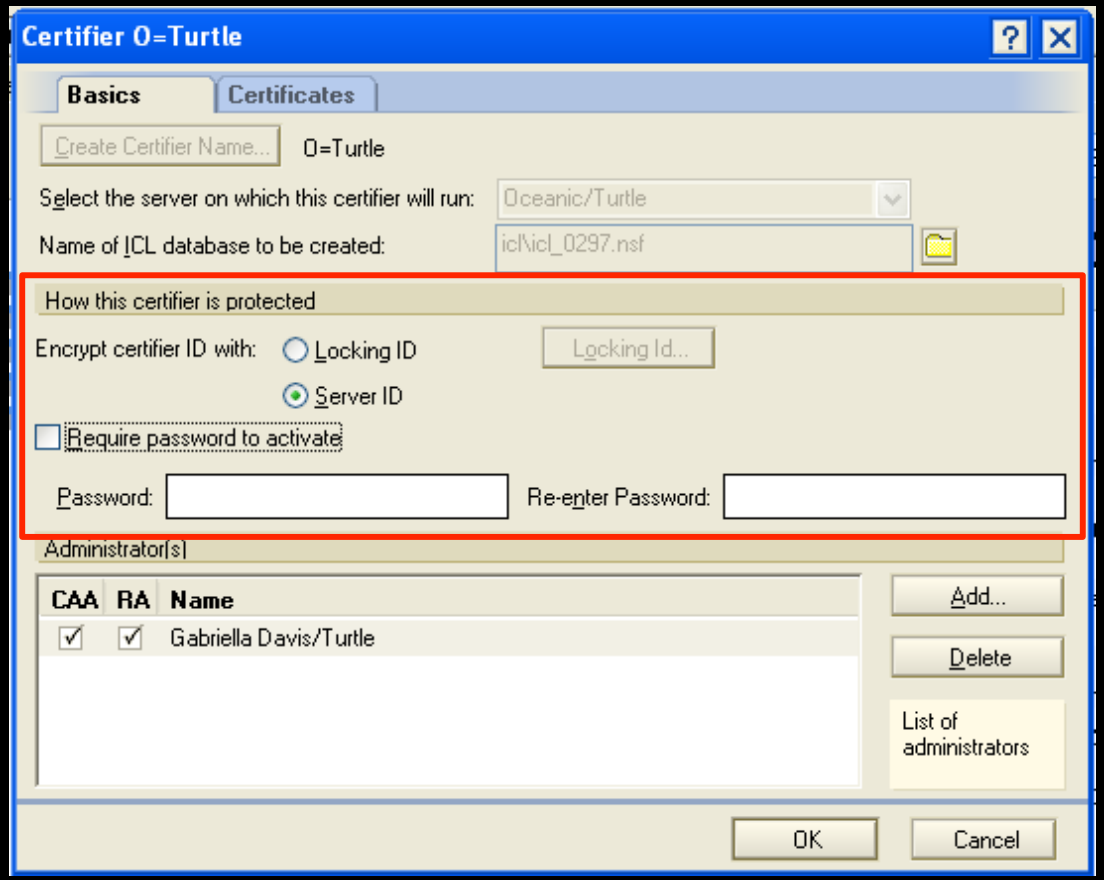
Working with IDs - Migrating to the CA Process

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



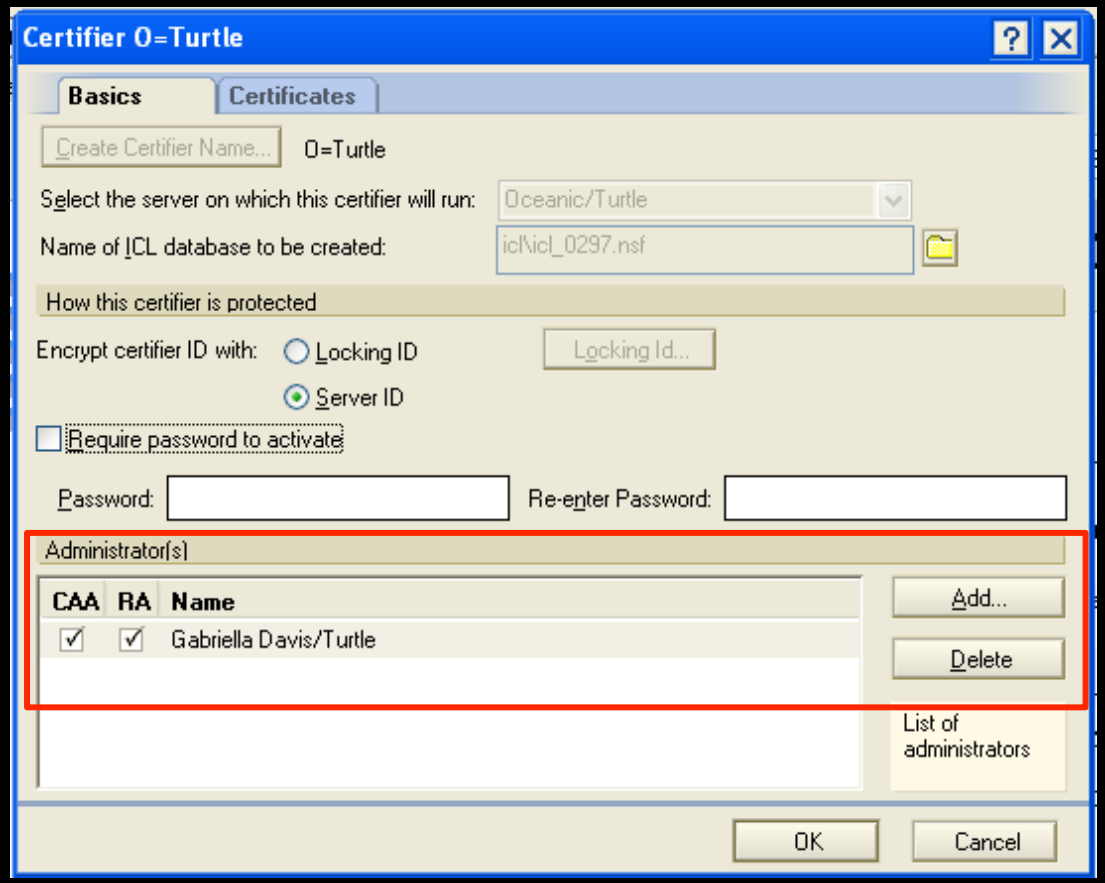
Working with IDs - Migrating to the CA Process

- 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



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 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

Rollover Keys

- If the certifiers are compromised then create new rollover keys and invalidate the stolen certifiers
  - Start with the certifiers
    - You can't use the security settings - rollover process for certifiers and servers you must use the Rollover Certifier option from the Configuration tab in Domino Administrator
  - Then the servers and users via a policy with security settings

Rollover Keys

Generate New Certifier Key

Specify the directory and certifier's ID file to be updated

Directory Server... Oceanic/Turtle

ID File... C:\cert.id

Name: /Labdon

Key and certificate information

Old (current) key

Force expiration in: 30 days

Creation Date: 22/03/1996 02:39:00

Identifier: 11Z4S UZYEE SYYG5 GPVQB AB21A 56451

Strength: Compatible with all releases (630 Bits)

New key

Strength: Compatible with 7.0 and later (2048 Bits)

Certificate expiration: 03/01/2111 17:17:00

The selected certifier ID file must be recertified as follows

The selected certifier is a top level certifier and will recertify itself

After the certifier ID file and directory entry have been updated, all people, servers, organizational units and cross certificates previously certified by this certifier should be recertified before the old key expiration period specified above.

Rollover | Previous Step | Cancel

Uses HTTP Accounts

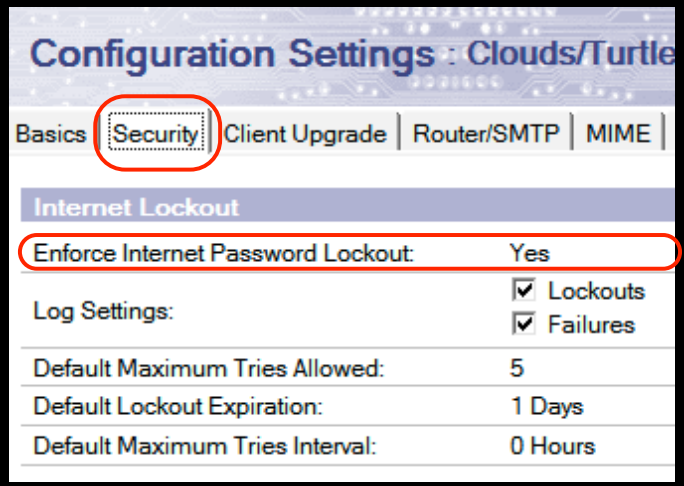
- If you set up Sametime for example within your company, did you give everyone a unique , secure password?
- If you gave them the same password then your Bitter Ex-Admin knows it
- He can use those account details and passwords to log in, not just to Domino HTTP sites but also to authenticate via SMTP and relay mail

Uses HTTP Accounts

- Treat the HTTP Password in the person document as a security field
  - Don’t be tempted to set a single simple password for all
- Monitor user activity on TCP ports for anything out of the ordinary
- If necessary, reset all user HTTP passwords to something unique

Uses HTTP Accounts

- Use the Internet Lockout feature
- 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 is configured in server configuration document



Stopping Stewie In His Tracks

- There is no foolproof way of protecting yourself from A Bitter Ex-Admin
  - Once they have access to your environment as part of their job they know enough to do some damage
  - What you can do is
    - be aware of the risks
    - don't take security shortcuts to make your day to day work easier
    - lock the stable door again once the horse has bolted

The Super Villain - Intentional Outside Attacker

- He knows about Domino
- He's a better programmer than you
- He's knows the internet better than you
- He's targeted you, specifically
- He is dedicated and Motivated

- Fortunately, he's pretty rare

- We spend way too much time worried about him

The Super Villain - Intentional Outside Attacker

- The Bad News
  - It is extremely difficult to stop a specifically targeted threat from a highly skilled and well resourced person or agency.
- See Also “STUXNET”
  - Likely created by a state intelligence agency
  - Specifically targeted a supposedly secret Iranian nuclear facility
  - Crossed an “Air Gap” security environment
    - No secure equipment any network with outside access
  - Targeted specific machine firmware
    - Rewrote firmware on specific models of equipment to cause seemingly random hardware failures
  - Believed to have delayed operation of the facility by more than a year before being discovered
  - http://en.wikipedia.org/wiki/Stuxnet

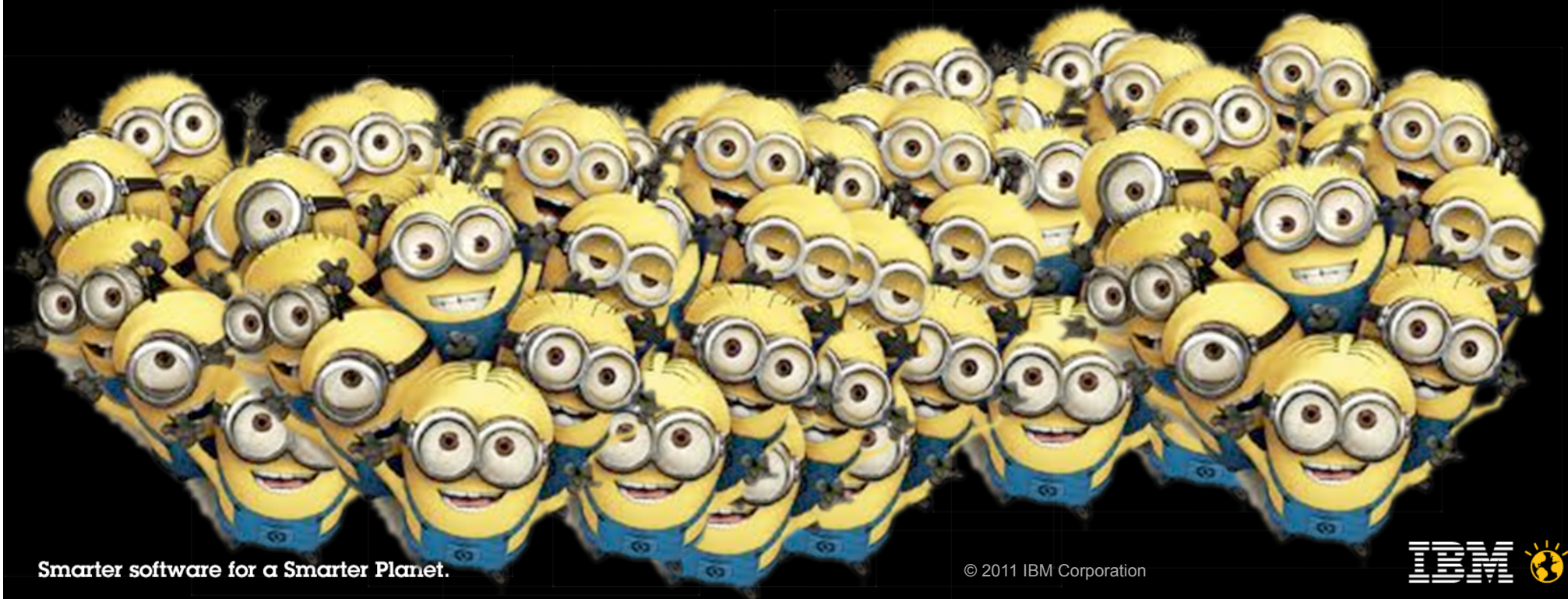
The Super Villain - Intentional Outside Attacker

- The Good News
  - This is not where we face the most risk
  - These threats are pretty rare.
  - Most of the security issues you need to be focused on involve the kinds of day to day issues we've been discussing.

- Protecting yourself from the Super Villain
  - Follow your security best practices, from network access to password management
  - Encrypt anything that is truly confidential in nature
  - Create a response plan to handle the unlikely event of a problem

Questions?

- Ask now, don't wait for the end and ask quietly at the podium
  - Gabriella Davis – The Turtle Partnership
    - http://www.TurtleWeb.com
  - Andrew Pollack – Northern Collaborative Technologies
    - http://www.TheNorth.com



Legal Disclaimer

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.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

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.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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.

Intel, Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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.

All references to any company refer to a fictitious company and are used for illustration purposes only.