



BE Systems Ltd

www.besystems.eu

Client Security and Lockdown

Warren Elsmore
SNUG 2006

Agenda



BE Systems Ltd

www.besystems.eu

- Why secure your clients?
- How to secure your clients
 - Custom client builds
 - Security Settings
 - Desktop Settings
 - Mail Settings
- Testing and deploying these settings
- Q & A

Why secure your clients?



BE Systems Ltd

www.besystems.eu

- A little knowledge is a dangerous thing...
- Prevents attacks internally and externally
- Enforce preferential settings on all clients
- Reduce number of support calls
- Simplify support procedures
- Save time, and save money!.

How to Secure your clients



BE Systems Ltd

www.besystems.eu

- Custom client builds
- Security Settings
- Desktop Control.

Custom client builds



BE Systems Ltd

www.besystems.eu

- What is a custom client build?
- Remove unnecessary features (templates, modem files etc)
- Turn off unused features (eg IM)
- Simplify client build for non-Notes administrators.

Installshield Tuner



BE Systems Ltd

www.besystems.eu

- Part 1 of a custom client
 - Contained on the Lotus Notes CD
 - Available as a separate download from Passport Advantage
 - Is client version specific
 - Allows you to edit the installation files and data
 - Invoked by setup command line
 - `msiexec /i "Lotus Notes 6.5.4.msi" TRANSFORMS="transform.mst" /qb-`

InstallShield Tuner



BE Systems Ltd

www.besystems.eu

Property	Value	Comment
<input type="checkbox"/> DiskPrompt	[1]	
<input type="checkbox"/> Registration	No	
<input type="checkbox"/> UpgradeCode	{5BA7CD07-4D6C-4D16-B1A6-2B50DD5F17AD}	
<input type="checkbox"/> IBM_exeInitialize	Not Set	
<input type="checkbox"/> DATADIR	Q:\lotus\notes\data	
<input type="checkbox"/> PROGDIR	C:\program files\lotus\notes	
<input type="checkbox"/> LAUNCHPROGRAM	0	
<input type="checkbox"/> LAUNCHREADME	0	
<input type="checkbox"/> PARTITIONED_INSTALL	0	
<input type="checkbox"/> USENOTESFOREMAIL	1	
<input type="checkbox"/> ApplicationUsers	OnlyCurrentUser	
<input type="checkbox"/> FileInUseProcess	0	
<input type="checkbox"/> AgreeToLicense	No	
<input type="checkbox"/> LAPAgree	No	
<input type="checkbox"/> LAPEnAgree	No	
<input type="checkbox"/> _IsMaintenance	Change	
<input type="checkbox"/> SetupType	Typical	
<input type="checkbox"/> _IsSetupTypeMin	Typical	
<input type="checkbox"/> Display_IsBitmapDlg	1	
<input type="checkbox"/> ARPREADME	http://www.lotus.com/ldd/releasenotes	
<input type="checkbox"/> ProductCode	{5A7970BE-2F8A-4004-ABE9-4CDB55A216E6}	
<input type="checkbox"/> ProductName	Lotus Notes 7.0	
<input type="checkbox"/> ProductVersion	7.00.5244	
<input type="checkbox"/> ARPCONTACT	OurCo HelpDesk	
<input type="checkbox"/> ARPHHELPINK	www.ourco.com/helpdesk	
<input type="checkbox"/> ARPHELPTTELEPHONE	01234 567890	
<input type="checkbox"/> ARPPRODUCTICON	ARPPRODUCTICON.exe	
<input type="checkbox"/> ARPURLINFOABOUT	http://intranet.ourco.com/	
<input type="checkbox"/> ARPURLUPDATEINFO	http://intranet.ourco.com/software/updates	
<input type="checkbox"/> AdminProperties	ADMIN_IMAGE	
<input type="checkbox"/> DWUSINTERVAL	30	
<input type="checkbox"/> DefaultUIFont	Tahoma8	
<input type="checkbox"/> DialogCaption	Install for Windows Installer	
<input type="checkbox"/> DiskSerial	1234-5678	

Properties are variables that Windows Installer uses during the installation. Windows Installer uses three categories of variables during an installation.

Ready

Setup response file

- Part 2 of a custom client
 - Customises the installation at runtime (“Notes Setup is complete”)
 - Can be user specific OR standardised
 - Triggered by a line in the ‘stub’ notes.ini.



BE Systems Ltd

www.besystems.eu

Setup Response file

Setup.txt

KeyFileName=q:\lotus\notes\data\user.id

Domino.Name=server/ou/Company

Domino.port=tcp/ip

im.server=sametime.company.com

im.port=80

im.connectwhen=0

Domino.address=server.company.internal

AdditionalServices=0



BE Systems Ltd

www.besystems.eu

Custom Client Build



BE Systems Ltd

www.besystems.eu

- My recommendations:
- Combine the two
 - Use the install tuner to identify a response file
 - Use the response file to finish the configuration
- Transform file
 - Remove modem files (unless you need them)
 - Remove unnecessary templates
 - Set "About" information to your helpdesk
- Response file
 - Answer the IM questions and account questions
 - Setup standard connections

The screenshot shows a software installation wizard interface. On the left, a tree view displays the installation process steps: Package Validation, Prevalidation, Organization, Product Properties, Features, System Configuration, and Files and Folders. The main area shows the 'Destination Computer' file tree, highlighting the 'ProgramFilesFolder' and 'Lotus' folders, with 'notes' and 'Notes.ini' files visible under 'Lotus'. On the right, a 'Notes' table is displayed with the following data:

Key	Value	Action
ConfigFile	Q:\lotus\notes\data\setup.txt	Add Line

Policies and Settings



BE Systems Ltd

www.besystems.eu

Policies Refresher



BE Systems Ltd

www.besystems.eu

- New to Domino 6, *much* improved in Domino 7
- Allow administrators to create groups of settings to apply to users
- Can be applied either via OU (Organizational) or per person (Explicit)
- Organisational policies stress the importance of OU's
- Remember – the Notes 6 client will automatically accept a rename.

Policies Refresher



BE Systems Ltd

www.besystems.eu

- Policies are used to group settings documents together and apply them to users
- Policies can be applied by OU, and can also inherit settings from a parent OU
 - /Company – Some general restrictions
 - /IT/Company – No additional restrictions
 - /Call Center/Company – More restrictions
- You will need PolicyCreator and PolicyEditor roles to the directory to use policies
- Policy Synopsis Tool.

Settings refresher



BE Systems Ltd

www.besystems.eu

- Settings documents contain the preference or setting to be applied to each user
- Each setting has 3 options:
 - Allow user to change
 - Enforce in child policies
 - Inherit this setting from a parent policy
- 5 Settings types in Domino 6:
 - Registration
 - Setup
 - Security
 - Desktop
 - Archiving
- 1 new type in Domino 7:
 - Mail.

Security Settings



BE Systems Ltd

www.besystems.eu

The screenshot shows the IBM Domino Administrator interface for configuring security settings. The window title is "Security Settings: Default Security Settings - IBM Domino Administrator". The menu bar includes File, Edit, View, Create, Actions, Text, and Help. The toolbar contains various icons for file operations and editing. The main content area is titled "Security Settings : My Company Security Settings" and has tabs for Basics, Password Management, Execution Control List, Keys and Certificates, Comments, and Administration. The "Basics" tab is active, showing the following details:

- Name:** My Company Security Settings
- Description:** These are our default security settings.
- Change Log:**
 - 30/09/06 - Created standard settings. WE
 - 1/10/06 - Enabled Password checking. WE

At the bottom of the window, there is a status bar with a scroll bar and a description field containing the text "Description or purpose of the group." The status bar also shows a key icon, a disconnected status, and the name "Office".

Security settings



BE Systems Ltd

www.besystems.eu

- 3 Main tasks
 - Set Execution Control Lists
 - Set Password quality
 - Set Key update policy.

Security Settings



BE Systems Ltd

www.besystems.eu

- You should have a managed ECL
- You should sign all application code with a signing ID
- You should **ONLY** allow users in the ECL to run code
- Note that the user who edits this setting needs rights to amend ECL's.

Security Settings

- Password Policies



BE Systems Ltd

www.besystems.eu

Security Settings



BE Systems Ltd

www.besystems.eu

- My recommendations:
 - Edit this setting document with the signing ID
 - Set custom password policy to match corporate standard
 - Enforce a standard ECL
 - Default / Anonymous – NO ACCESS
 - Signing ID / Lotus IDs – full access

Mail Settings



BE Systems Ltd

www.besystems.eu

The screenshot shows the IBM Domino Administrator interface for configuring mail settings. The window title is "Mail Settings: Default Mail - IBM Domino Administrator". The menu bar includes File, Edit, View, Create, Actions, Text, and Help. The toolbar contains various icons for file operations and editing. The main content area is titled "Mail Settings : My Mail Settings" and has tabs for Basics, Mail File Preferences, Message Disclaimers, Comments, and Administration. The "Basics" tab is active, showing the following fields:

- Name:** My Mail Settings (with a dropdown arrow) and Our default mail settings.
- Description:** Main items: disclaimer added, user forced to share scheduling information, user not allowed to change mail file ownership.
- Change History:** 30/09/06 - Settings Created (with a dropdown arrow).

At the bottom of the window, there is a status bar with the text "Signed by Warren Elsmore/Demo7 on 01/09/2005 10:45:54, according to /Demo7". The taskbar at the very bottom shows several open applications, including "Disconnected" and "Office".

Mail Settings



BE Systems Ltd

www.besystems.eu

- Are the only settings configured per mail file, not per Notes client
- Can change nearly all items under Mail Preferences dialog.

Mail Settings



BE Systems Ltd

www.besystems.eu

- My recommendations:
 - Don't allow users to change ownership
 - Set sent view to remove, not delete
 - Enforce calendar sharing
 - Use to add departmental mail disclaimers
 - Set multilingual MIME set to UTF-8.

Desktop settings



BE Systems Ltd

www.besystems.eu

The screenshot shows the 'New Desktop Settings' window in the IBM Domino Administrator. The window title is 'New Desktop Settings - IBM Domino Administrator'. The menu bar includes 'File', 'Edit', 'View', 'Create', 'Actions', 'Text', and 'Help'. The toolbar contains various icons for file operations and navigation. The main content area is titled 'Desktop Settings' and has a tabbed interface with 'Basics' selected. The 'Basics' tab shows the following settings:

- Name: My Desktop settings (created 30/09/06)
- Description: Change History: 02/10/06 - added "do not allow private location docs"
- Homepage/Welcome Page Options:
 - Corporate Welcome Pages database: (empty)
 - Default Welcome Page: No default Welcome Page
 - Home page selection: Do not allow users to change their home page
- Location Options:
 - Do not allow private location docs
- Notes Application Plug-in:
 - Allow users to change the settings in this section
 - Instant messaging provider: IBM Workplace Collaboration Services
 - Primary instant messaging name resolution performed: IBM Workplace Managed Client

At the bottom of the window, there is a text field with the placeholder 'enter a description or purpose for this settings document.' The taskbar at the bottom shows the Start button, several open applications (Demo7/Demo7: Lotus Do..., Portal by BE Systems - M..., New Desktop Settings...), and the system tray with the time 10:56.

Desktop settings



BE Systems Ltd

www.besystems.eu

- Powerful, wide range of controls
- Changes Notes preferences and location settings
- Can also:
 - Upgrade client version (Smart Upgrade)
 - Upgrade mail file template version (Seamless Upgrade).

Desktop Settings



BE Systems Ltd

www.besystems.eu

- My recommendations:
 - Do not allow private location docs (desktop users only!)
 - Enforce a mail template version
 - Set correct browser and proxies
 - Enable autosave every 10 minutes
 - Enable TCP/IP compression for remote users
 - Enable Diagnostics reports
 - Check all the settings, and apply for your company.

Advanced desktop settings



BE Systems Ltd

www.besystems.eu

- Desktop policy settings can include *any* Notes.ini variable or location document setting!
- Correct fields need to be added to the desktop settings document
 - LocAllLocationfieldname
 - \$Prefpreferencename
- Example
 - Create a field called LocAllReplicationEnabled, set to “1”
 - Create a field called \$Pref\$DisplayWindowment, set to “1”.

Advanced policy control

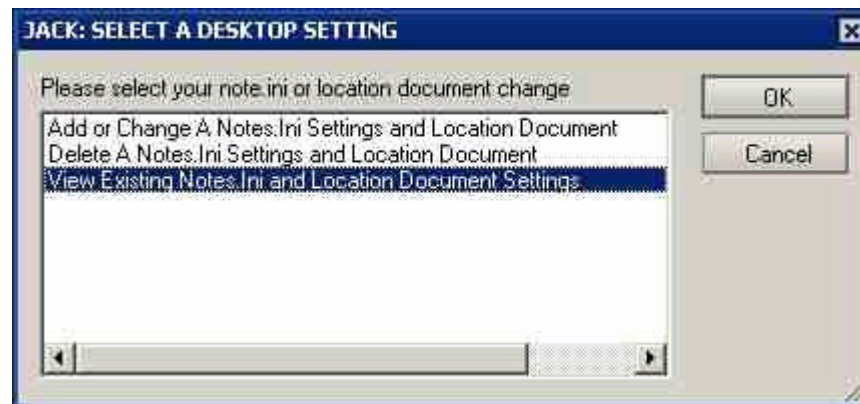


BE Systems Ltd

www.besystems.eu

- There is no UI for doing this 🤦‍♂️
- There is a tool available! 😊
- Written by Jack Dausman

<http://www.leadershipnumbers.com/MS.nsf/d6plinks/JDAN-6HCRKP>



Testing and deploying settings



BE Systems Ltd

www.besystems.eu

Testing policies



BE Systems Ltd

www.besystems.eu

- Never apply an untested organisational policy!
- Select a group of pilot users depending upon settings applied
- Apply the setting explicitly to these users
 - Remember that explicit policies are applied last, this may impact the applied policy.

Deploying settings



BE Systems Ltd

www.besystems.eu

- How are settings deployed?
- Mail settings
 - Deployed via Adminp on users' home mail server
 - Runs every 12 hours by default
 - Can force with "Tell AdminP process mailpolicy"
- All other settings
 - Deployed via the Dynamic client configurator (DCC).

Dynamic Client Configurator



BE Systems Ltd

www.besystems.eu

- Separate Notes executable (ndyncfg.exe) that populates user info, assist in settings, enables mail file moves etc
- DOES NOT RUN INTERACTIVLY!
- DCC is triggered when the user first authenticates with their home server
- AND
 - the users' person document has been altered since last authentication
 - OR their desktop policy has been altered since last authentication
- Runs a MAXIMUM of once per day.

Debugging DCC



BE Systems Ltd

www.besystems.eu

- Check the person document has client information
- Check the clients' log.nsf:

```
<date> 09:45:17 AM Dynamic Client Configuration started  
<date> 09:45:17 AM Initializing Dynamic Client Configuration  
<date> 09:45:17 AM Dynamic Client Configuration updating location information  
<date> 09:45:18 AM Dynamic Client Configuration shutdown
```

- DCC can be run manually, by Start\Run “ndyncfg.exe”
- Remember that certain settings only take effect after the client has been restarted.

Some common DCC Problems



BE Systems Ltd

www.besystems.eu

- If your administrator (admin group) is not in the administrator tab on the policy they cannot see the policy when trying to apply it via the admin client. They can if they try and apply it via the person doc
- The policy will not take effect on the client if there is a connection doc in their PNAB to their home server
- You may need to delete users cache.ndk before anything will happen
- DisableDynConfigClient=1 in users' notes.ini will disable DCC
- Check the users' location document for a field called "AcceptUpdates" – should be set to "1"
- Open the users' PAB, select Actions\Remove Address Book Preferences.

Conclusion



BE Systems Ltd

www.besystems.eu

- The Notes client is very flexible, but that can lead to support issues
- Use a standard build to baseline your client installs
- Policies provide a powerful way of managing a deployed infrastructure
- Always test before deployment!.

Resources



BE Systems Ltd

www.besystems.eu

- Lotus Domino Administrator help file
- “Creating Mail policies in Lotus Notes/Domino 7” (LDD technote)
- “Policy-Based system administration with Domino 6” (LDD technote)
- Frequently asked questions about the DCC (Support KB 1212699).

Any Questions?



BE Systems Ltd

www.besystems.eu

- My personal blog: www.elsmore.net
- Email me: warren.elsmore@besystems.eu
- Buy me a drink in the bar!