

# Demistifying Domino HTTP Server



**BLUG**  
Belux Lotus User Group

**Kris De Bisschop**  
**[k.debisschop@easi.net](mailto:k.debisschop@easi.net)**

# Agenda

- **Introduction**
- **Default Security**
- **Security First Aid**
- **Authentication/SSO**
- **Internet Password Lockout**
- **DomCfg**
- **Internet Sites**
- **SSL**
- **Load Balance iNotes**





**BLUG**  
Belux Lotus User Group

# Agenda

- **Introduction**
- **Default Security**
- **Security First Aid**
- **Authentication/SSO**
- **Internet Password Lockout**
- **DomCfg**
- **Internet Sites**
- **SSL**
- **Load Balance iNotes**





# Introduction



**Kris De Bisschop**



**12 years Lotus Notes/Domino experience**



**Project Manager @ EASI**



**Lotusphere fan**



**EASIsphere presentator**



**Lotus beta products tester**



**BLUG**  
Belux Lotus User Group

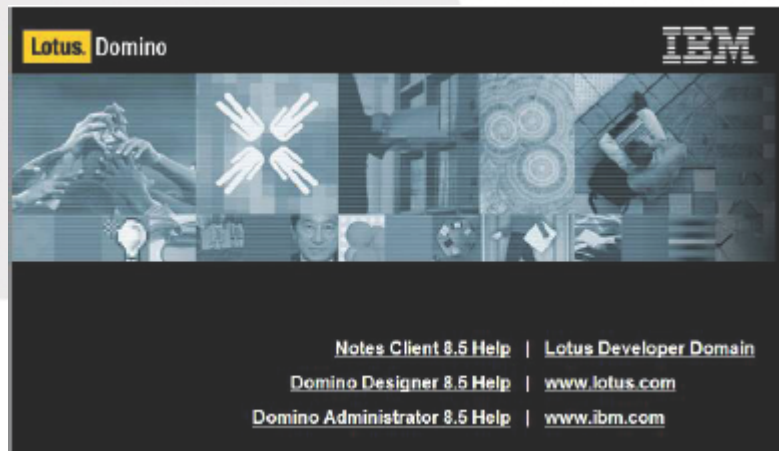
# Agenda

- Introduction
- **Default Security**
- Security First Aid
- Authentication/SSO
- Internet Password Lockout
- DomCfg
- Internet Sites
- SSL
- Load Balance iNotes



# HTTP – Default security

- Anonymous access is permitted
- Basic authentication is enabled with ugly grey log in prompt
- Server access lists are ignored for HTTP access
- No matter how (IP, hostname, FQDN) user opens the home page
- No password management
- No SSO activated out of the box



**BLUG**  
Belux Lotus User Group

# Agenda

- Introduction
- Default Security
- **Security First Aid**
- Authentication/SSO
- Internet Password Lockout
- DomCfg
- Internet Sites
- SSL
- Load Balance iNotes



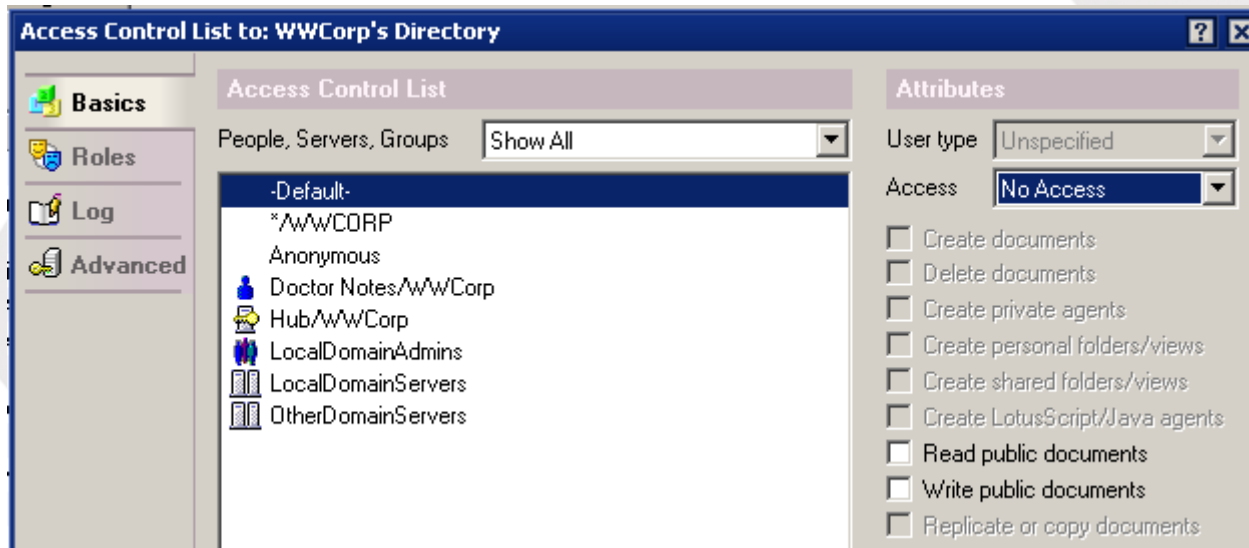


# HTTP – security first aid

- **Control anonymous access**
  - Review the ACL of all databases and set anonymous NO ACCESS
- **Maximum Internet Access**

Maximum Internet name and password

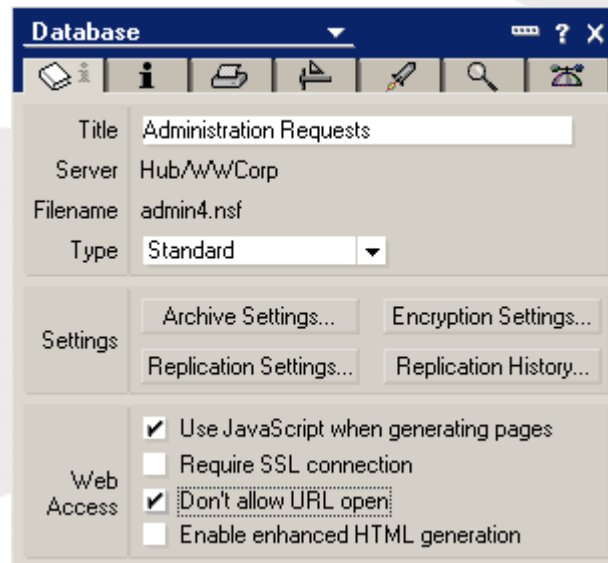
Editor



**BLUG**  
Belux Lotus User Group

# HTTP – security first aid

- Don't allow URL open
  - Database property to prevent web access



# HTTP – security first aid

- **Enforce server access rules on the web**
  - **Server document – Ports**
  - **“Enforce server access settings”**
  - **Applies deny access to server through HTTP**

Basics	Security	Ports...	Server Tasks...	Internet Protocols...	MTAs...	Mis...
Notes Network Ports						
Internet Ports...						
Proxies						
Web						
Directory						
Mail						
DIIOP						
Remote Debug Manager						
Server Controller						
Web						
(HTTP/HTTPS)						
TCP/IP port number: 80						
TCP/IP port status: Enabled						
Enforce server access settings: Yes						
SSL port number: 443						
SSL port status: Enabled						



# HTTP – Passwords

- Enable “Use more secure Internet password”
  - Set in directory profile of Domino Directory
  - Run the agent “Upgrade to more secure Internet password”

Basics

---

**Domino Directory Configuration Profile**

Domain defined by this Domino Directory:	<input type="text" value="EASISPHERE"/>
Condensed server directory catalog for domain:	<input type="text"/>
Sort all new groups by default:	<input type="text" value="Yes"/>
Auto-populated group Members update interval:	<input type="text" value="30"/> minutes
Use more secure Internet Passwords:	<input type="text" value="Yes - Password verification compatible with Notes/Domino release 4.6 or greater"/>
Allow the creation of Alternate Language Information documents:	<input type="text" value="Yes"/>
List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process Requests database:	<input type="text"/>
Comments:	

Actions	Tools	Window	Help
---------	-------	--------	------

---

Apply Delegation to All Selected Entries

Edit Directory Profile

Edit Administration ECL

populate DominoUNID

Rules Problem

Set Secure Internet Password

Test CrossCertify

---

Other...

---

Recertify Selected People

Add Internet Cert to Selected People

Rename Selected People

**Upgrade to More Secure Internet Password**

Edit Document

Forward

Move To Folder...

Remove From Folder

Send Upgrade Notifications

Chat





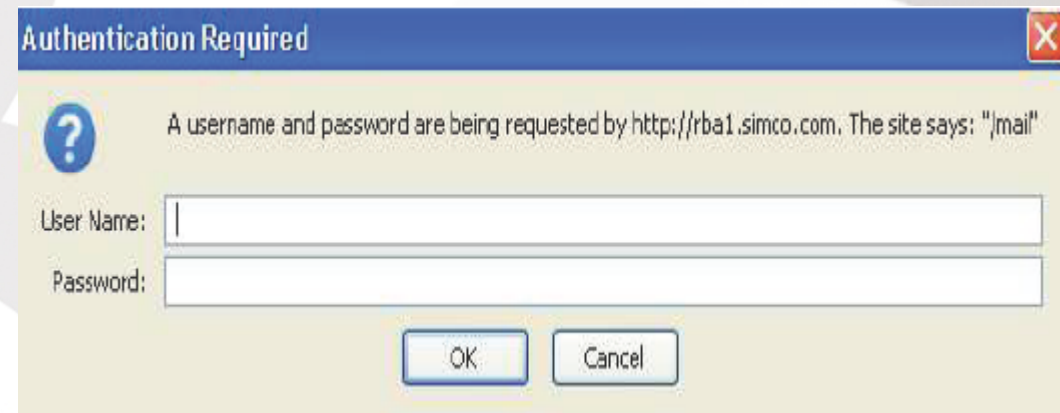
# Agenda

- Introduction
- Default Security
- Security First Aid
- **Authentication/SSO**
- Internet Password Lockout
- DomCfg
- Internet Sites
- SSL
- Load Balance iNotes



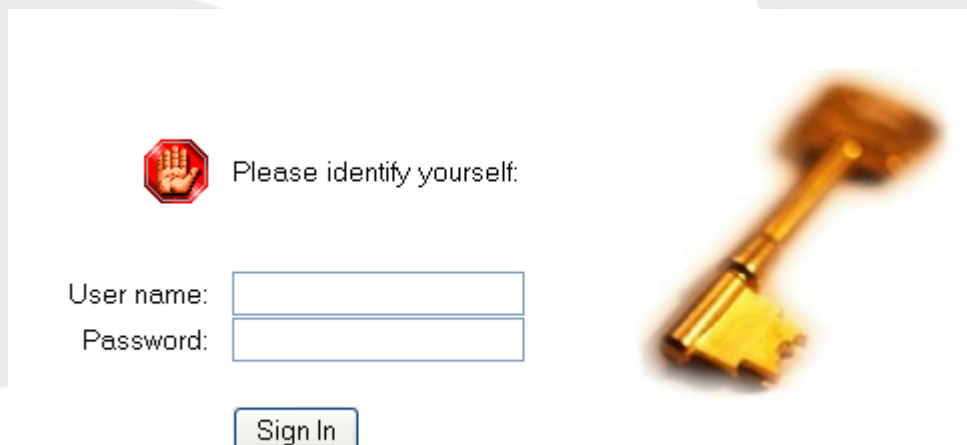
# HTTP – Authentication/SSO

- **Default method : Basic authentication**
- **Problems**
  - **It is ugly**
  - **Less secure**
  - **No password management**
    - **No utility for changing password**
    - **No forced password expiration**
    - **No management of user sessions**



# HTTP – Authentication/SSO

- SSO allows cookie based sessions across servers
- Customizable login and password change forms
- Ability to enforce password rules
- Possibility to enforce session expiration
- Allows single authentication between Domino and Websphere



# HTTP – Authentication/SSO

- **Default name is LtpaToken**
- **Multiple SSO configs are possible**
- **Each SSO config is tied to a DNS domain name**
- **Put FQDN for authentication to work**
- **Avoid using capitals in the DNS domain name**
- **SSO config can be shared between Internet Sites and regular web configuration (Sametime integration in iNotes)**





# Agenda

- Introduction
- Default Security
- Security First Aid
- Authentication/SSO
- Internet Password Lockout
- DomCfg
- Internet Sites
- SSL
- Load Balance iNotes



# HTTP – Internet Password Lockout

- Lock users out based on incorrect logon attempts
- Configured in two places
  - Server configuration document
  - Security policy settings
- Server configuration settings apply to all HTTP sessions on the server
- Policy settings per user can override server settings

## Server Configuration

Configuration Settings :

Basics | Security | Smart Upgrade | Router/SMTP | MIME | NOTES.INI Settings

### Internet Lockout

Enforce Internet Password Lockout:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Log Settings:	<input checked="" type="checkbox"/> Lockouts <input checked="" type="checkbox"/> Failures
Default Maximum Tries Allowed:	<input type="text" value="5"/>
Default Lockout Expiration:	<input type="text" value="15"/> Minutes
Default Maximum Tries Interval:	<input type="text" value="1"/> Hours


## Policy Settings

### Internet Password Lockout Settings

Override Server's Internet Lockout settings?	<input checked="" type="checkbox"/> Yes
Maximum Tries Allowed	<input type="text" value="10"/>
Lockout Expiration	<input type="text" value="5"/> Minutes
Maximum Tries Interval	<input type="text" value="5"/> Minutes

# HTTP – Internet Password Lockout


- Internet Password Lockout database (inetlockout.nsf)



Your account has been locked out

User name:

Password:



Mark for Delete/Unlock		Delete Marked Items	
Server Name	User Name	Locked Out	Failed Attempts
▼ Hub/WWCorp	Doctor Notes/WWCorp	Yes	5



# Agenda

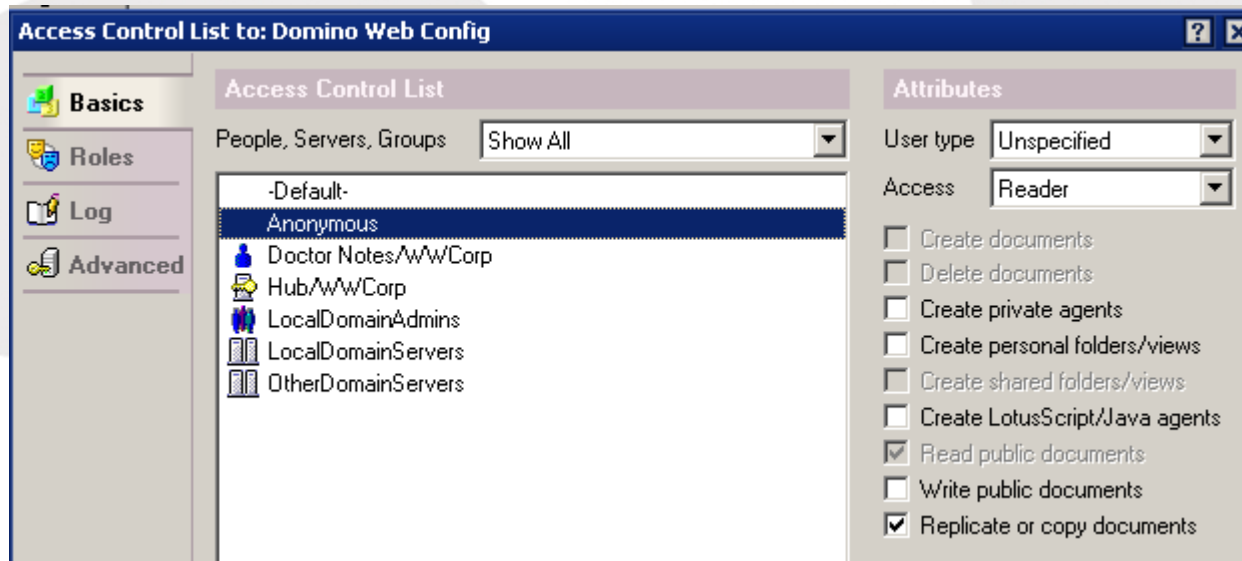
- Introduction
- Default Security
- Security First Aid
- Authentication/SSO
- Internet Password Lockout
- DomCfg
- Internet Sites
- SSL
- Load Balance iNotes





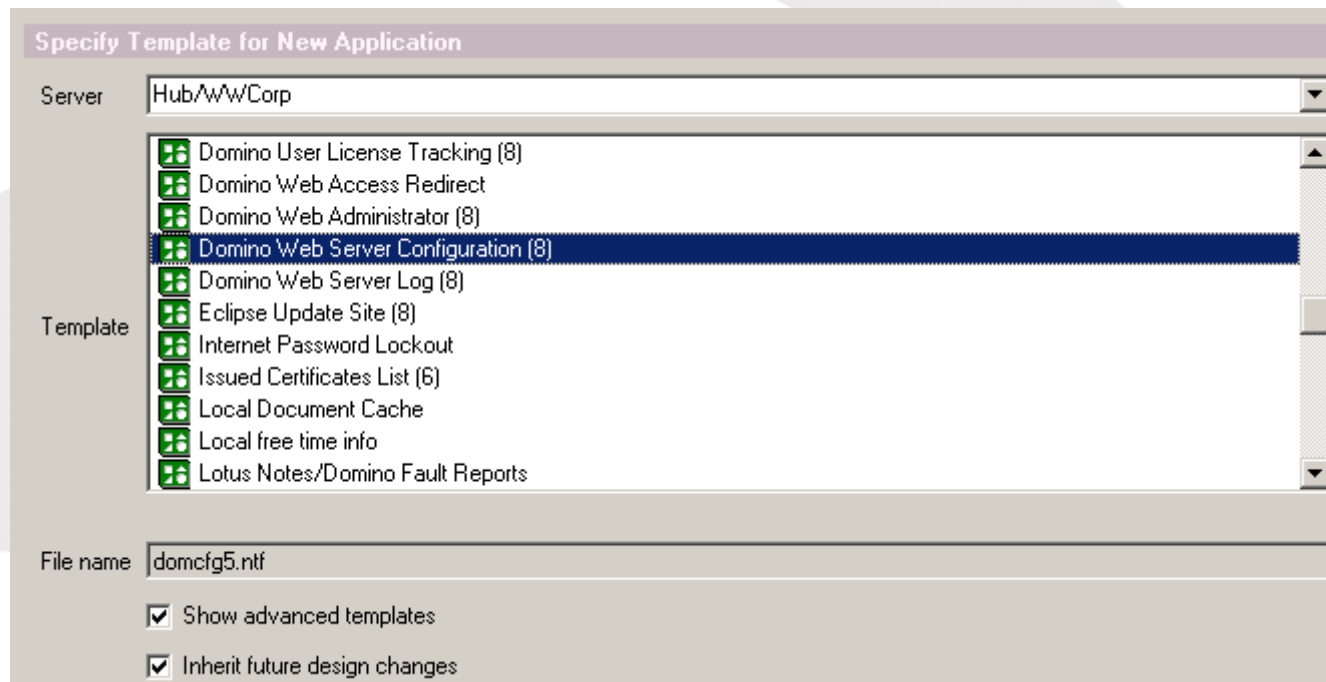
# DomCfg Database

- Used as of the moment SSO is enabled on the server
- Can configure custom
  - Login forms
  - Password reset forms
  - Error and Response forms
- Configurable per site
- Be careful about anonymous access => deselect write public documents



# DomCfg Database

- Created manually
- Name must be domcfg.nsf
- Is derived from the domcfg5.ntf template



# DomCfg Database

- Forms can be customized
- Other forms can be referenced
  - Inotes redirect login



Username :

Password :

Log In



Please identify yourself:

User name:

Password:

Sign In

Lotus. iNotes.

IBM.

Enter your user name and password and then click Log In.

User name:

Password:

Log In

Options

Select the mode



Full mode



Lite mode



Ultra-light mode



Shared or public computer

Licensed Materials - Property of IBM. L-GHUS-7XUT7L © Copyright IBM Corporation and its licensors 1985, 2010. All Rights Reserved. IBM, the IBM logo, Lotus and Notes are trademarks of IBM Corporation in the United States, other countries, or both. Other company, product or service names may be trademarks or service marks of others.



**BLUG**  
Belux Lotus User Group

# Agenda

- Introduction
- Default Security
- Security First Aid
- Authentication/SSO
- Internet Password Lockout
- DomCfg
- Internet Sites
- SSL
- Load Balance iNotes





# Internet Sites – What ?

- Introduced in Domino 6
- By default not enabled
- Most Admins leave current config => it works.....why changing ?
- Once enabled, create them for each service used
  - SMTP Inbound
  - HTTP
  - POP3
  - IMAP
  - LDAP



# Internet Sites – key determinants

- **Use of multiple hostnames on any internet protocol**
- **Multiple LTPA Tokens on a single server**
- **Multiple SSL Certificates for different hostnames on single server**
- **Requirement for different authentication schemes on the same server**
- **Requirement to span website or service on multiple servers**



# Internet Sites - Basics

- **“Host names mapped to this server”**
  - Can be IP Addresses or hostnames
  - Hostname must match what user types in the browser
  - In case of SSL, an IP Address must be set
- **“Domino Servers that host this site”**
  - Default value : \* => any server responding IP address or hostname
  - Helps in load balancing of websites



# Share LTPA token document

- **Useful in case of Sametime/iNotes integration**
  - **Sametime uses Web Configuration <=> Inotes uses Internet Sites**
- **Adapt the automatic created SSO document**
  - **Include the Domino Servers that will share the config**
- **Copy the adapted document to include the key**
  - **Set the Organization name for use with Internet Sites**





# Agenda

- **Introduction**
- **Default Security**
- **Security First Aid**
- **Authentication/SSO**
- **Internet Password Lockout**
- **DomCfg**
- **Internet Sites**
- **SSL**
- **Load Balance iNotes**



# SSL – Self-certified certificate

- Same type of protection
- Default expiration of 1 year
- Certificate needs to be trusted manually in the browser



## This Connection is Untrusted

You have asked Firefox to connect securely to **mail.** .be, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

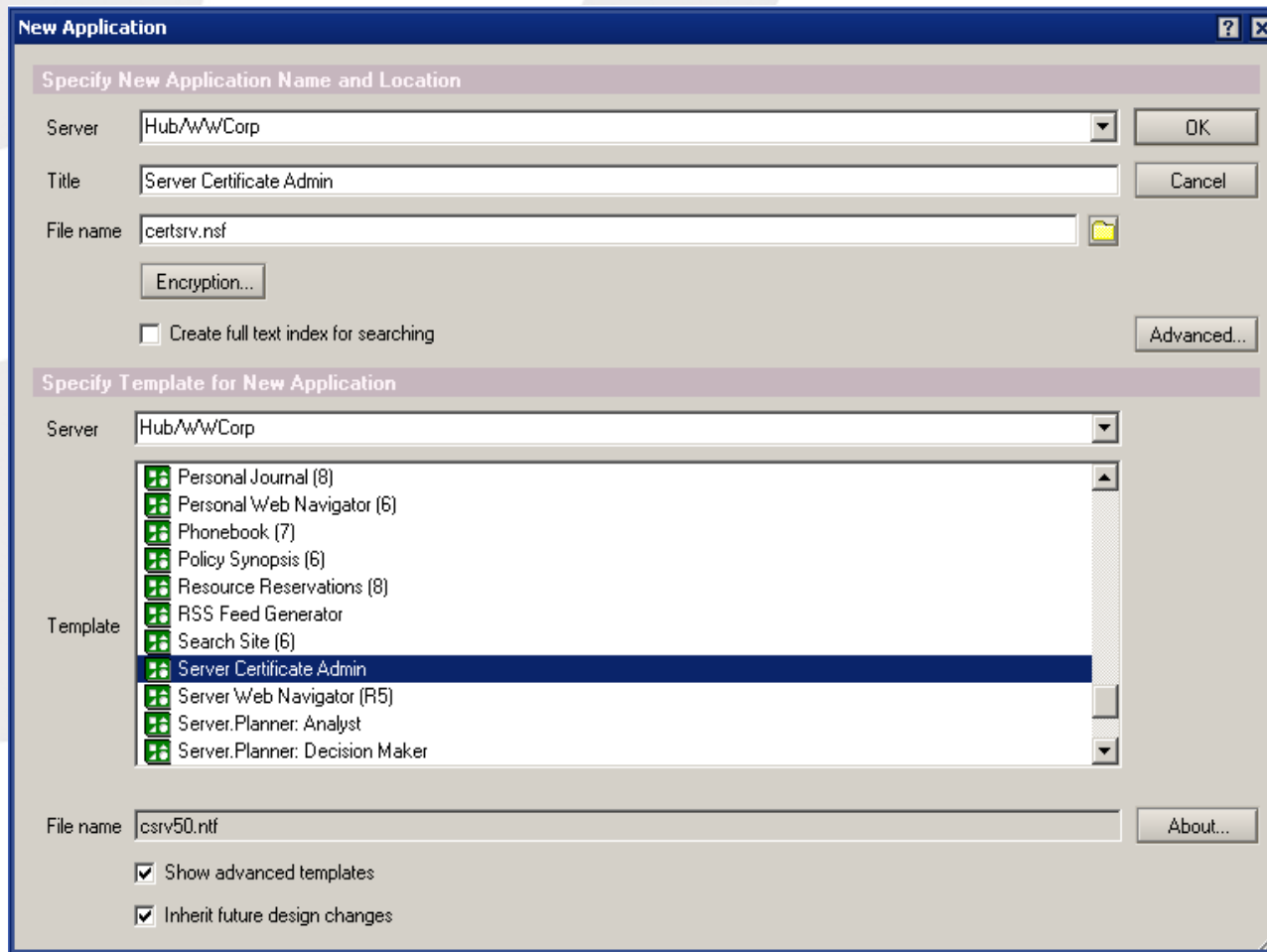
- ▶ Technical Details
- ▶ I Understand the Risks



**BLUG**  
Belux Lotus User Group

# SSL – Self-certified certificate

- Create a local folder on your machine to store the certificate
- Create Server Certificate Admin database



# SSL – Self-certified certificate

- Create Key Ring with Self-Certified Certificate



Click on the steps below to create an SSL key ring and populate it with certificates.

1. [Create Key Ring](#)
2. [Create Certificate Request](#)
3. [Install Trusted Root Certificate into Key Ring](#)
4. [Install Certificate Into Key Ring](#)

## Create Key Rings & Certificates

You can also quickly create a key ring with a self-certified certificate for testing purposes.

[Create Key Ring with Self-Certified Certificate](#)



**BLUG**  
Belux Lotus User Group



# SSL – Self-certified certificate

- Fill in the necessary info
  - Specify filename
  - Refer correct hostname

**Key ring created with self signed certificate**

Your key ring has been created with a self-certified certificate.

**Key ring file name:**  
c:\wwwcorplnotes.kyr

**Distinguished Name:**

Common name:	webmail.wwcorp.com
Organization:	WWCORP
Organizational unit:	
City:	
State:	Brussels
Country:	BE

This certificate is valid from:  
27/03/2011 to 27/03/2012

**Next Step:**  
You are now ready to enable SSL on your server. See the Domino User's Guide for instructions on how to configure the Server Record in the Domino Directory to enable SSL.

**Key Ring Information**

Key Ring File Name	c:\wwwcorplnotes.kyr
Key Ring Password	*****
Password Verify:	*****

**Distinguished Name**

Common Name	webmail.wwcorp.com
Organization	WWCORP
Organizational Unit	(optional)
City or Locality	(optional)
State or Province	Brussels (no abbreviations)
Country	BE (two character country code)



# SSL – Activate on Server

- Copy the created keyring files to the server's data directory (.kyr and .sth)
- Different steps to follow depending of you config
  - In case you don't use internet sites
    - Refer keyring file in the internet ports section
    - Adapt the Web part

Web	Directory	Mail	DIIOIP	Remote Debug Manager	Server Controller
<b>Web</b> (HTTP/HTTPS)					
TCP/IP port number:	80				
TCP/IP port status:	Redirect to SSL				
Enforce server access settings:	Yes				
Authentication options:					
Name & password:	Yes				
Anonymous:	Yes				
SSL port number:	443				
SSL port status:	Enabled				
Authentication options:					
Client certificate:	No				
Name & password:	Yes				
Anonymous:	Yes				

Basics	Security	Ports...	Server Tasks...	Internet Protocols...
Notes Network Ports	Internet Ports...	Proxies		
<b>SSL settings</b>				
SSL key file name:	inotes.kyr			
SSL protocol version (for use with all protocols except HTTP):	Negotiated			
Accept SSL site certificates:	<input type="radio"/> Yes <input checked="" type="radio"/> No			
Accept expired SSL certificates:	<input checked="" type="radio"/> Yes <input type="radio"/> No			



# SSL – Activate on Server

- In case you use internet sites
  - Create web site document
  - Adapt the security part

Basics	Configuration	Domino Web Engine	Security	Comments	Administration
--------	---------------	-------------------	----------	----------	----------------

---

TCP Authentication	
Anonymous:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name & password:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Redirect TCP to SSL:	<input checked="" type="radio"/> Yes <input type="radio"/> No

---

SSL Authentication	
Anonymous:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name & password:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Client certificate:	<input type="radio"/> Yes <input checked="" type="radio"/> No

---

SSL Options	
Key file name:	<input type="text" value="notes\keyr"/>
Protocol version:	<input type="text" value="Negotiated"/>
Accept SSL site certificates:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Accept expired SSL certificates:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Check for CRLs:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Trust expired CRLs:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow CRL search to fail:	<input checked="" type="radio"/> Yes <input type="radio"/> No



# Agenda

- **Introduction**
- **Default Security**
- **Security First Aid**
- **Authentication/SSO**
- **Internet Password Lockout**
- **DomCfg**
- **Internet Sites**
- **SSL**
- **Load Balance iNotes**



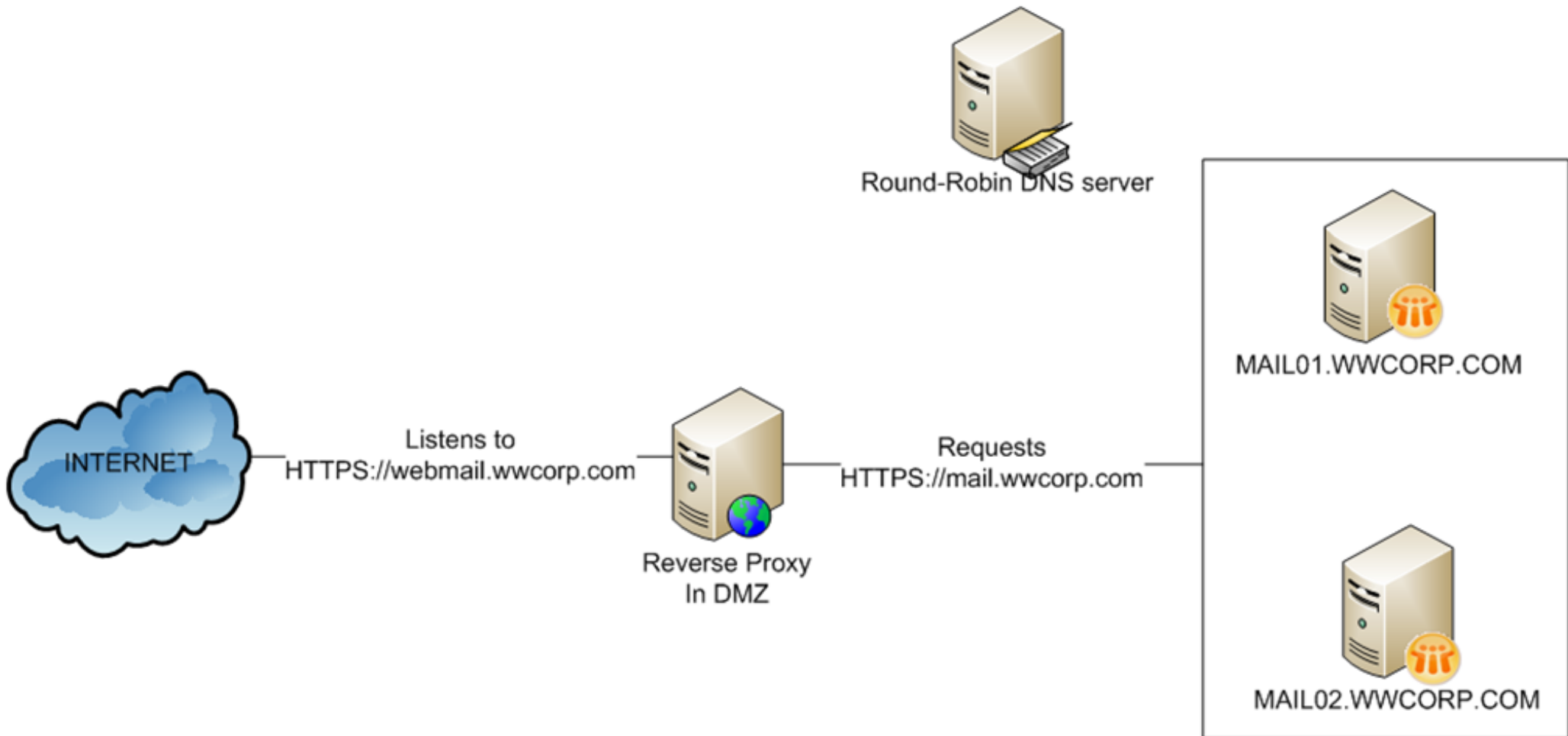


# Load balance iNotes

- **Configuration I set up in small and medium business**
- **Cluster the mail servers**
  - **Details about clustering will not be handled in this session**
- **Round-Robin is used on the internal DNS Server**
- **Apache or Squid reverse proxy Server in the DMZ**
- **Reverse proxy configured with 3<sup>rd</sup> party SSL certificate**
- **Domino Servers configured with each self-certified SSL certificate**



# Load balance iNotes



# Load balance iNotes

## Enable round robin in the DNS Server properties

The screenshot shows the 'Properties' dialog box for a DNS server, with the 'Advanced' tab selected. The 'Server options' section contains several checkboxes. The checkbox 'Enable round robin' is checked and highlighted with a red rectangle. Other options include 'Disable recursion (also disables forwarders)', 'BIND secondaries', 'Fail on load if bad zone data', 'Enable netmask ordering', and 'Secure cache against pollution'. The 'Name checking' dropdown is set to 'Multibyte (UTF8)', and the 'Load zone data on startup' dropdown is set to 'From Active Directory and registry'. The 'Scavenging period' is set to 0 days. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Properties

Debug Logging | Event Logging | Monitoring  
Interfaces | Forwarders | Advanced | Root Hints

Server version number:  
5.2 3790 (0xece)

Server options:

- ☐ Disable recursion (also disables forwarders)
- ☒ BIND secondaries
- ☐ Fail on load if bad zone data
- ☒ Enable round robin
- ☒ Enable netmask ordering
- ☒ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

Reset to Default

OK Cancel Apply

## Adapt TTL in the zone properties

The screenshot shows the 'wwwcorp.com Properties' dialog box, with the 'Start of Authority (SOA)' tab selected. The 'Minimum (default) TTL' is set to 1 hour. At the bottom, the 'TTL for this record' is set to 0 :0 :1, which is highlighted with a red rectangle. Other fields include 'Serial number' (1), 'Primary server' (master.wwwcorp.com), and 'Responsible person' (hostmaster.wwwcorp.com). The 'Refresh interval' is 15 minutes, 'Retry interval' is 10 minutes, and 'Expires after' is 1 day. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

wwwcorp.com Properties

Name Servers | WINS | Zone Transfers  
General | Start of Authority (SOA)

Serial number: 1 Increment

Primary server: master.wwwcorp.com Browse...

Responsible person: hostmaster.wwwcorp.com Browse...

Refresh interval: 15 minutes

Retry interval: 10 minutes

Expires after: 1 days

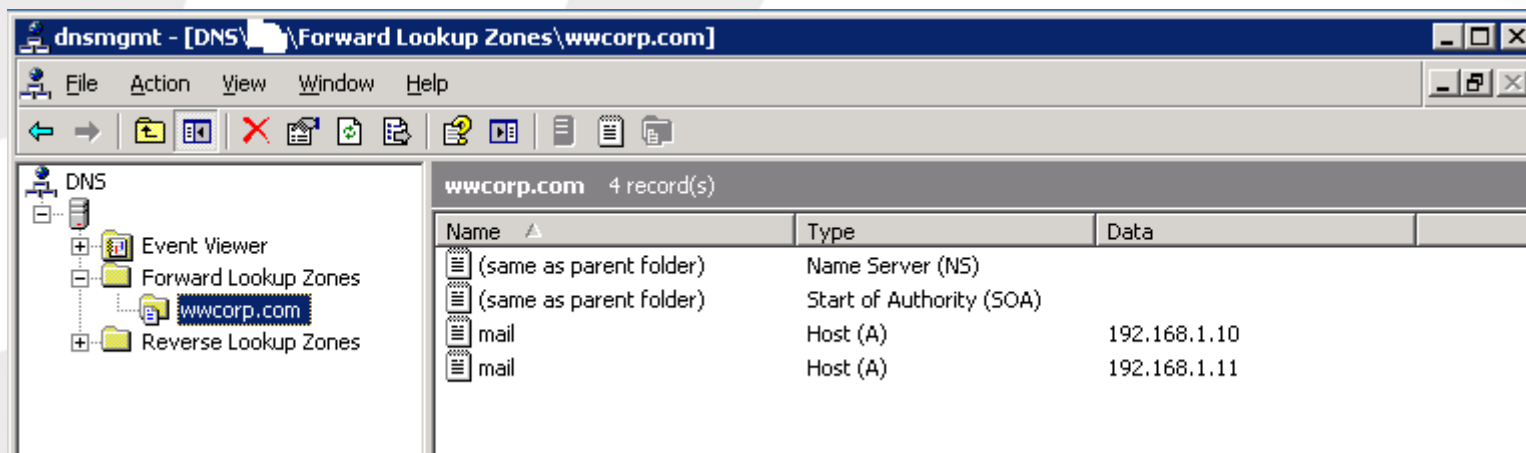
Minimum (default) TTL: 1 hours

TTL for this record: 0 :0 :1 (DDDD:HH.MM.SS)

OK Cancel Apply

# Load balance iNotes

**Create two A-Records with the name mail.wwcorp.com,  
Reference per record the IP address of the mailserver**





# Load balance iNotes

- Set up SSO for the domain .wwcorp.com

**Web SSO Configuration for :**

Basics | Comments | Administration

Token Configuration		Token Expiration	
Configuration Name:	LtpaToken	Expiration (minutes):	180
Organization:	WWCORP	Idle Session Timeout:	<input type="checkbox"/> Enabled
DNS Domain:	.wwcorp.com		
Map names in LTPA tokens:	Disabled		

Participating Servers	
Domino Server Names:	DOMINO01/WWCORP DOMINO02/WWCORP



# Load balance iNotes

- There is only 1 internet site configured for both servers

**Web Site WWCORP Webmail**

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

**Site Information**

Descriptive name for this site:	WWCORP Webmail
Organization:	WWCORP
Use this web site to handle requests which cannot be mapped to any other web sites:	<input type="radio"/> Yes <input checked="" type="radio"/> No Note: only one web site should have this option set to Yes
Host names or addresses mapped to this site:	mail.wwcorp.com mail01.wwcorp.com mail02.wwcorp.com 192.168.1.10 192.168.1.11
Domino servers that host this site:	DOMINO01/WWCORP; DOMINO02/WWCORP

**Web Site WWCORP Webmail**

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

**Default Mapping Rules**

Home URL:	/inotesredir.nsf?Open
HTML directory:	domino\html
Icon directory:	domino\icons
Icon URL path:	/icons
CGI directory:	domino\cgi-bin
CGI URL path:	/cgi-bin
Java applet directory:	domino\java
Java URL path:	/domjava
Default home page:	



# Load balance iNotes

**Web Site WWCORP Webmail**

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

**HTTP Sessions**

Session authentication:

Web SSO Configuration:

Force login on SSL:

When overriding session authentication, generate session cookie:

**Web Site WWCORP Webmail**

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

**TCP Authentication**

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

Redirect TCP to SSL: ☒ Yes ☐ No

**SSL Authentication**

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

Client certificate: ☐ Yes ☒ No

**SSL Options**

Key file name:

Protocol version:

Accept SSL site certificates: ☐ Yes ☒ No

Accept expired SSL certificates: ☒ Yes ☐ No

Check for CRLs: ☐ Yes ☒ No

Trust expired CRLs: ☒ Yes ☐ No

Allow CRL search to fail: ☒ Yes ☐ No



# Load balance iNotes

- A domcfg database needs to be created to reference login form
- The database needs to be present on both servers

Web Server Configuration		Add Mapping	Edit Mapping	Delete Document
		Web Site/Virtual Server	Database Path	Form Name
Sign In Form Mappings		mai02.wwwcorp.com	inotesredir.nsf	DWALoginForm
Change Password Form Mappings		mail01.wwwcorp.com	inotesredir.nsf	DWALoginForm
Error & Response Form Mappings		mail.wwwcorp.com	inotesredir.nsf	DWALoginForm





# Load balance iNotes

- Create the iNotes Redirect database on both servers

Save & Exit

Server Settings   UI Setup   Ultra-light/Mobile Settings   Application Setup

Please select the Redirection type

Help   Fixed   **Dynamic**   MailServer

---

If you wish to force the PATH, please enter it here  
(Leave blank to disable)

Help  

---

Do you wish to force SSL for the entire session ?

Help   **Yes**   No

---

Do you wish to force SSL only on authentication ?

Help   **Yes**   No

---

Please enter the SSL port number

Help  

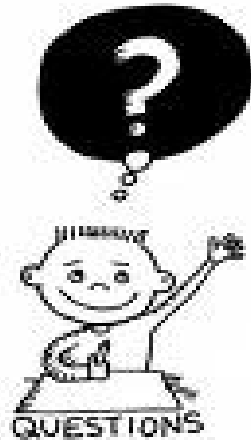
---

Enable Debug ?

Help   Yes   **No**



# Thank You



**BLUG**  
Belux Lotus User Group