Practical IBM Notes and Domino Internet Security

engage Conference – G(h)ent 31.03.2015

Daniel Nashed, Nash!Com

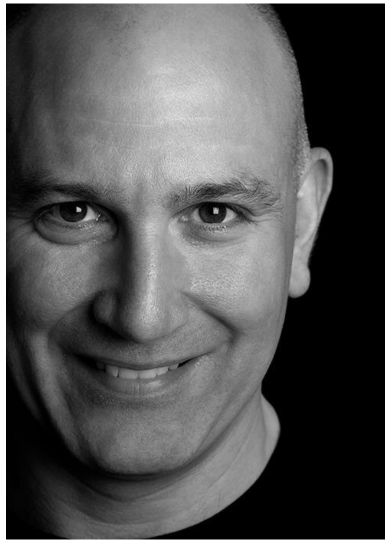
Updated Presentation,

originally presented with David Kern, IBM at ConnectED 2015

engage
by blug

About Daniel Nashed

- Nash!Com – German IBM® Business Partner/ISV
- Member of The Penumbra group -- an international consortium of selected Business Partners pooling their talent and resources
- focused on Cross-Platform C-API, IBM® Domino® Infrastructure, Administration, Integration, Troubleshooting and IBM® Traveler
- Platform Focus: Microsoft® Windows® 32/64, Linux® and IBM AIX®
- Author of the Domino on Linux®/UNIX® Start Script
  - Note: Working on RHEL7 + SLES 12 “systemd” support



IBM CHAMPION

Agenda

- General Internet Security

- Current Security Discussion
  - The POODLE and other Attacks

- Notes/Domino TLS Support
- Notes/Domino SHA-2 Support

- Notes S/MIME Support
  - Just as a reference. Too much details to cover in the SSL/TLS area and just 60 minutes of time

- Q&A

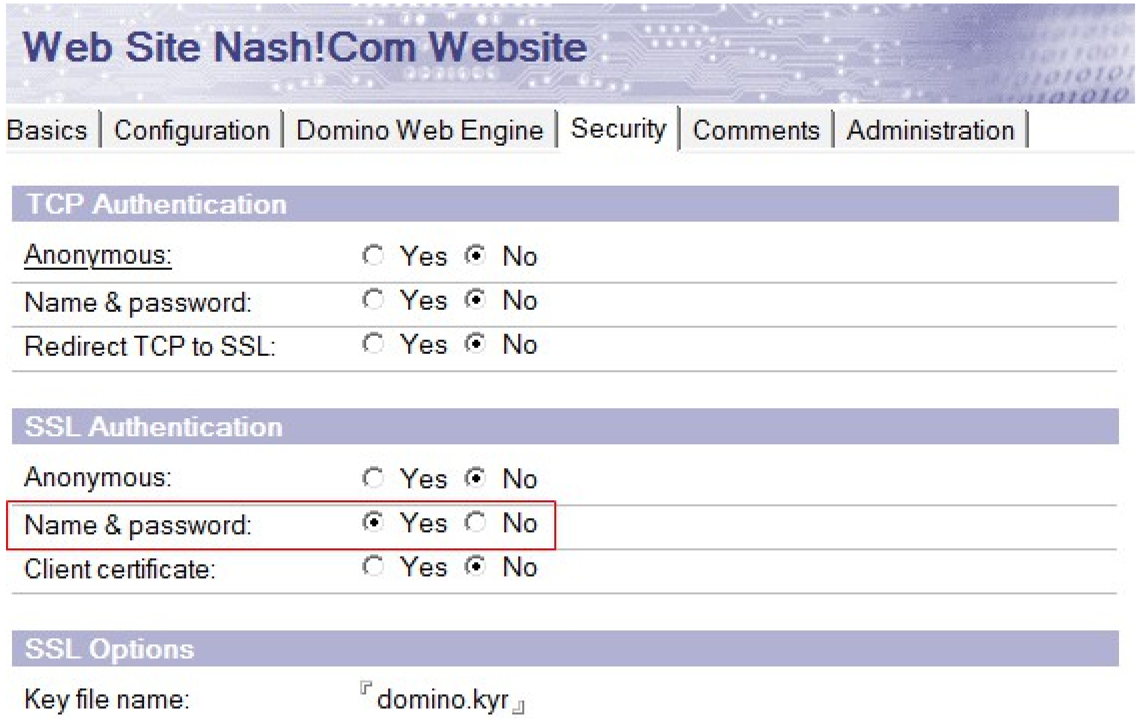
General Internet Security

Basic Security Principles

- All information that is not public available should only be accessible via authenticated connection
- All authentication information (user/password/**session cookies**, certificate exchange) should to be encrypted
- All information that needs authentication/authorization should only be accessible via encrypted channel
- Very sensitive data should use **end to end encryption** and should be **always stored encrypted**
- This is true for internet connections as well as for **internal communication**
- This is true for all protocols
  - Also think about Directory information via LDAP and specially authenticated LDAP connections

Internet Authentication

- For servers with no public information turn of **all anonymous connections**
  - Also allow only SSL connections
    - Works similar for all protocols
    - Disable the unencrypted port and enable the SSL Port
    - You will need a Server certificate stored in a "Domino Key Ring file"
  - For Internet Site configurations check <u>all</u> matching Internet Site configurations!
- Note: This does not fee you from ensuring all database ACL is properly set to not allow Anonymous connections
  - Tip: Use separate view in catalog.nsf to ensure ACL is right
  - **Caution:** If no Anonymous entry is set Default entry is used!!


Web Site Nash!Com Website
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:	domino.kyr

iNotes Redirect database with authenticated access only

- When your server only allows authenticated connections the login form in the redirect database cannot be rendered correctly
  - Because the user is not authenticated when the login form needs to be displayed

- Workaround: Define URLs that can be requested anonymously

  notes.ini **HTTPPublicUrls=/redir.nsf/***

  - Or more granular (more paranoid)

    8.5.3 → HTTPPublicUrls=/redir.nsf/iNotes-LoginBanner65short.gif:/redir.nsf/StylesheetLogin:/redir.nsf/Login.js

    - 9.0.x → HTTPPublicUrls=/redir.nsf/IBMLogo.gif:/redir.nsf/StylesheetLogin:/redir.nsf/Login.js

  - Requires HTTP task restart

- Detailed iNotes Redirect Database Slides available in the “Additional Material Appendix”

Internet Password Security

- **Enable Internet Password Lockout**
  - Strong requirement!
  - Without this feature everyone can try to brute force passwords
  - Configure Internet Password Lockout in Server Configuration Document

- Enable “more secure internet password” for internet password stored person doc
  - a.) Enable in Domino Directory profile
    b.) And use agent “**Set secure internet password**” to change all existing person docs
  - Set: “**Yes - Password verification compatible with Notes/Domino release 8.01 or greater**”

  - Tip / “Plan B”: Don't store internet password in person doc and instead use authentication data from a LDAP directory e.g. Active Directory via Directory Assistance
    - Works as long you have no internet password in person doc
      Domino will skip those documents and continue to search in Directory Assistance for user/password
    - Take care : In that scenario brute force attacks might block your AD user account!

SSO and Session Based Authentication

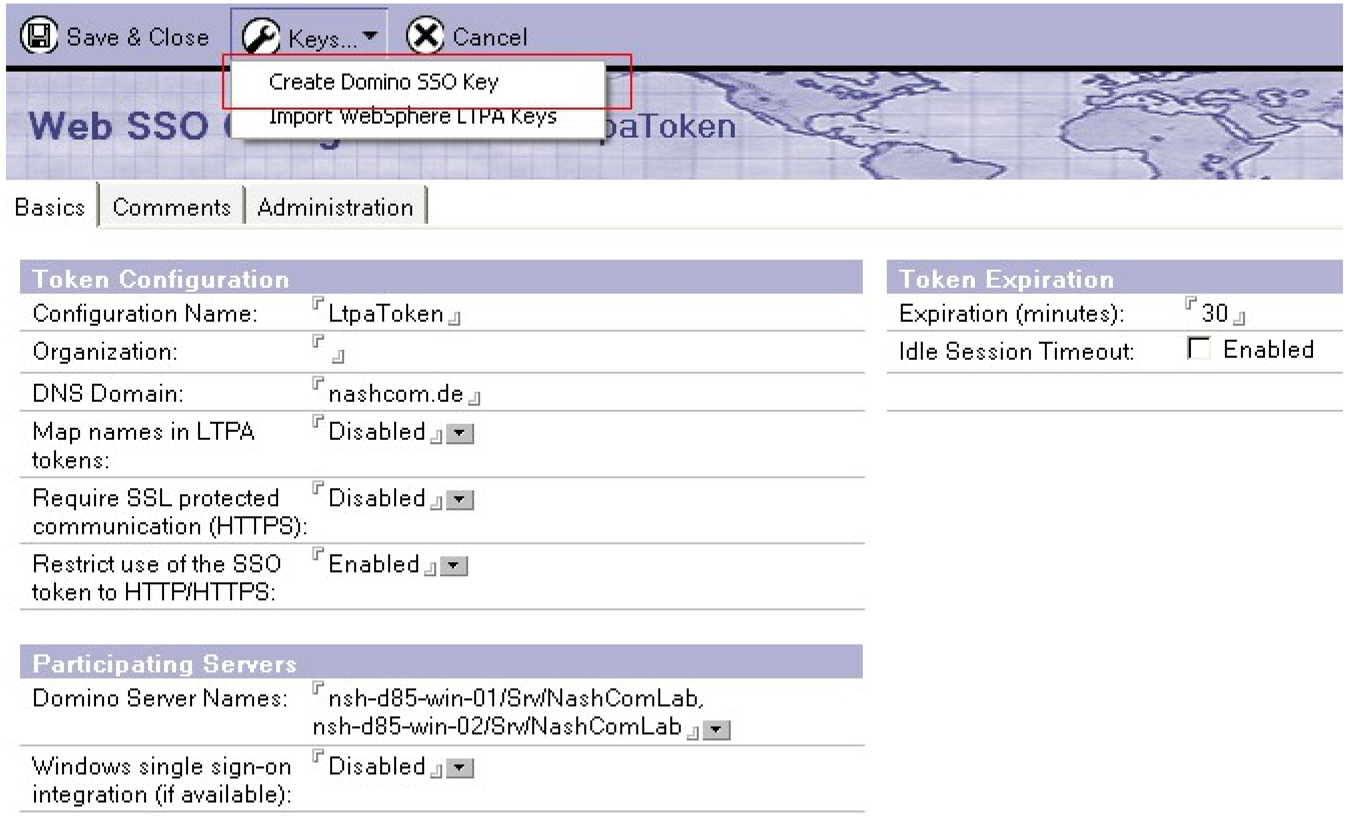
- Basic Authentication sends username and password with every request

- Recommendation: **Multi-Server-Session Authentication**
  - Best performance, security and flexibility
  - Cross Application integration with Websphere and Sametime
  - Also works when failing over to another server

- Two different modes
  - Plain Domino → “secret key” is created in Domino
  - Websphere enabled → “secret key” is imported from Websphere

Single Sign On (SSO) for HTTP

- SSO Configuration Document
- Settings in Server.Doc or Internet Site Document
  - Internet Site Document needs **Organization Name** set in SSO Config Doc



Token Configuration

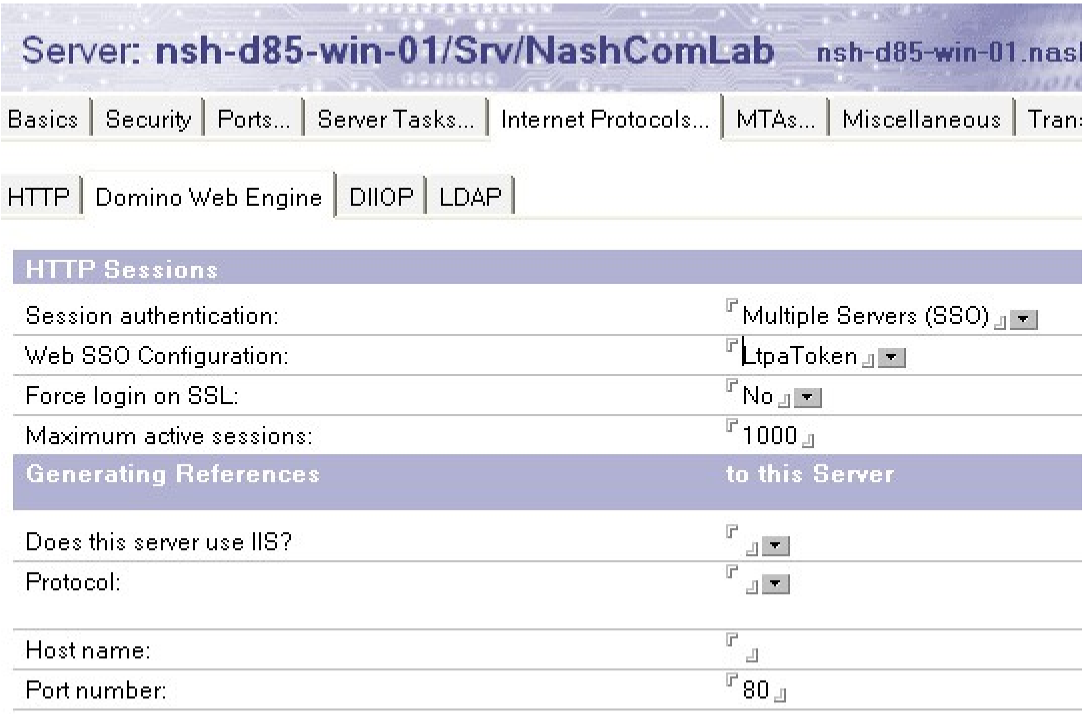
Configuration Name:	LtpaToken
Organization:	
DNS Domain:	nashcom.de
Map names in LTPA tokens:	Disabled
Require SSL protected communication (HTTPS):	Disabled
Restrict use of the SSO token to HTTP/HTTPS:	Enabled

Token Expiration

Expiration (minutes):	30
Idle Session Timeout:	☐ Enabled

Participating Servers

Domino Server Names:	nsh-d85-win-01/Srv/NashComLab, nsh-d85-win-02/Srv/NashComLab
Windows single sign-on integration (if available):	Disabled



HTTP Sessions

Session authentication:	Multiple Servers (SSO)
Web SSO Configuration:	LtpaToken
Force login on SSL:	No
Maximum active sessions:	1000

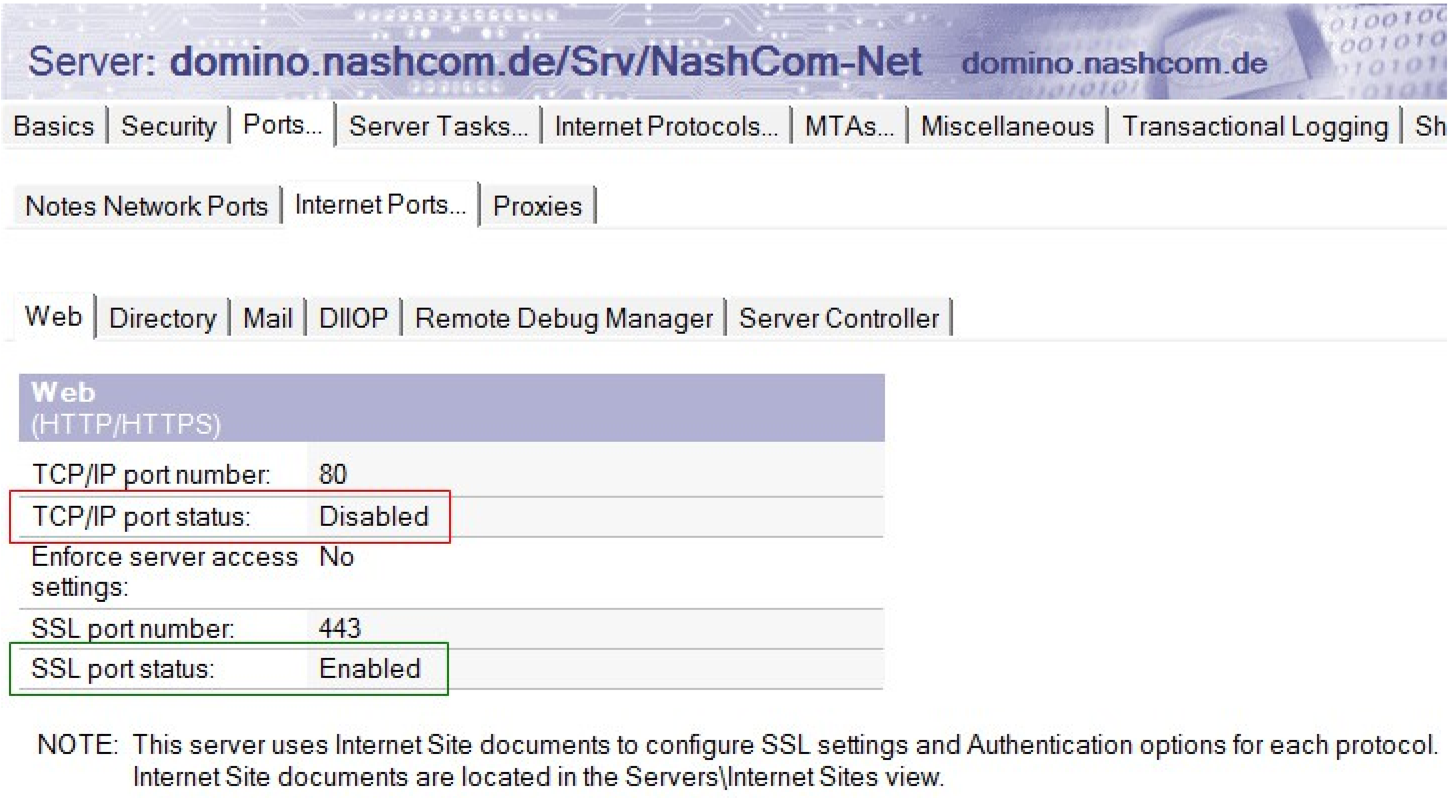
Generating References to this Server

Does this server use IIS?	
Protocol:	
Host name:	
Port number:	80

Channel (Port) Encryption

- Domino Supports SSL for all Internet Protocols
  - HTTP, IMAP, POP3, SMTP, LDAP
  - Requires a Server Certificate stored in a Domino Keyring file

- Until 9.0.1 FP2 Notes and Domino only support SSL up to SSL Version 3.0


Server: domino.nashcom.de/Srv/NashCom-Net
domino.nashcom.de
Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Sh
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:	Disabled
Enforce server access settings:	No
SSL port number:	443
SSL port status:	Enabled

NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options for each protocol. Internet Site documents are located in the Servers\Internet Sites view.

Current Security Discussion

The POODLE Attack

- The POODLE Attack changed the world of SSL
  - **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption

- Attack against SSL 3.0 and new since end of last year also TLS!
  - SSL 3.0 is vulnerable
  - TLS in some implementations (for example Domino and F5) are vulnerable

- The final solution is to disable SSL 3.0 and apply the current TLS Interims Fix
  - A workaround was to disable “CBC” ciphers until the new IF was released

- If you keep SSL 3.0 enabled for now ensuring that a downgrade attack cannot happen is important
  - The **TLS_FALLBACK_SCSV** protocol functionality ensures that only clients that don't support/request TLS will use a lower version like SSL 3.0
    - Needs to be supported on server and client side!

References for the “POODLE Attack”

- The Register has a good overview article
  - http://www.theregister.co.uk/2014/10/14/google_drops_ssl_30_poodle_vulnerability/

- Official Google Information
  - https://www.openssl.org/~bodo/ssl-poodle.pdf

- Very technical article “How POODLE happened”
  - https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html

Disabling SSL 3.0

- Disabling SSL 3.0 completely now might not be a good idea
  - The right first step is to support at least TLS 1.0 and implement **TLS_FALLBACK_SCSV**
    - **But the client also needs to support SCSV**
  - Some servers already disabled support for SSL 3.0 completely
    - This means you need a browser / an application with TLS 1.0 support now!
  - Take Care: In case of unpatched Notes Clients all internet protocols will not work any more!
    - The unpatched Notes Client does only support SSL 3.0
  - Most Java applications should support TLS 1.0 at least – Also Notes
    - As long developer did not explicitly use “SSLv3” when requesting a secure connection!
  - Disabling SSLv3 prevents DIIOP and iSpy from connecting
    - Both use the "ssllight" Java library for SSL
    - There will be a technote for iSpy soon

Reference for Firefox Changes

- https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/
- “SSLv3 will be disabled by default in Firefox 34, which was released on Nov 25”
  - This means auto updated clients will not be able to open any SSL 3.0 enabled website by default
- “As an additional precaution, Firefox 35 will support a generic TLS downgrade protection mechanism known as SCSV. If this is supported by the server, it prevents attacks that rely on insecure fallback.”

Notes/Domino TLS Support

Domino Interims Fix introduced TLS 1.0

- Available since 4. November 2014
- For all Platforms and supported Versions
  - 9.0.1 FP2, 9.0, 8.5.3 FP6, 8.5.2 FP4, 8.5.1 FP5
- First Version is a Server Fix
  - Only Standard Client has shipped simultaneously because of Cert Request SHA2 changes
- TLS 1.0 support for all Internet Protocols inbound and outbound
  - HTTP, SMTP, LDAP, POP3, IMAP
  - Support for **TLS_FALLBACK_SCSV**
  - First version does not allow to disable SSL 3.0 completely
  - Cipher suite list for outbound connections re-ordered to place AES ciphers first

Details about the first Interims Fix

- Removed support
  - SSLv2
  - SSL renegotiation has been disabled
  - All weak (<128 bits) cipher suites have been disabled

- No UI Changes in HTTP Configuration
  - The fix will override existing configuration with support for TLS 1.0

- Notes.ini DEBUG_SSL_HANDSHAKE=2
  - Will show the protocol version used

- Reference
  - http://www.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0

New “POODLE on TLS” Vulnerability

- There is a new exploit published 8.12.2014 that affects TLS!
  - Not all implementations of TLS are affected.
  - But Domino and also some other solutions like the F5 load-balancer are on the list

- For more details read and referenced articles on that page
  - https://community.qualys.com/blogs/securitylabs/2014/12/08/poodle-bites-tls

- First response was to disable all “CBC” ciphers
  - but this left us with only quite old RC4 ciphers

FREAK and other Attacks

- FREAK ("Factoring RSA Export Keys")
  - https://freakattack.com/
  - https://www.us-cert.gov/ncas/current-activity/2015/03/06/FREAK-SSLTLS-Vulnerability

- Domino is not vulnerable to the FREAK attack
  - it required an implementation bug

- RC4 Bar Mitzvah attack
  - IBM removed RC4-SHA from the default list for TLS 1.2 where backwards compatibility is less of an issue which mostly covers the RC4 Bar Mitzvah attack
  - http://en.wikipedia.org/wiki/Bar_mitzvah_attack

First Updated Domino Interims fix

- Interims Fixes for this issue are available since 20.12.2014
- SPR #KLYH9RMJGL: CVE-2014-8730 TLS 1.x Padding Vulnerability
  - Fixes the vulnerability for CBC ciphers
- SPR #KLYH9QXMQE: Disable SSL ini: **DISABLE_SSLV3=1**
- Security Bulletin: TLS Padding Vulnerability affects IBM Domino (CVE-2014-8730)
  - http://www.ibm.com/support/docview.wss?uid=swg21693142
- Detailed IF release numbers
  - **Domino** 9.0.1 FP2 IF 3, 9.0 IF7,8.5.3 FP6 IF6, 8.5.2 FP4 IF3, 8.5.1 FP5 IF3
  - **Notes** 9.0.1 FP2 IF4 and 8.5.3 FP6 IF4 added TLS 1.0 support
    - Windows, Linux and Mac OSX

What happens to other applications?

- Current Mobile devices support TLS
  - We did not ran into any issues yet – Also Traveler connections work fine even when disabling SSL 3.0 completely

- You need to test all your applications using SSL connections
  - Including Secure LDAP Connections for example in Directory Assistance

- Java
  - Java 1.6 supports TLS 1.0 (Notes/Domino currently ships with IBM Java 1.6)
    - New Java Patch on top of 9.0.1 FP3 SR 16 FP3 supported TLS 1.2 as well
  - Java 1.7 supports TLS 1.0, 1.1, 1.2
    - Most applications should work unchanged – take care that your are not hard-coding the SSL/TLS version!

- Applications based on OpenSSL
  - Newer versions work without any change
    - It is strongly recommend to keep security libs like OpenSSL updated anyway!

SSL V2 Client Hello - Known “Incompatibility”

- Sending the first SSL message (ClientHello) in SSLv2 format provided backwards compatibility with servers that only supported SSLv2
  - This is only needed if you want to connect to servers that only support SSLv2
  - Extremely useful in 1996!
  - Using an SSLv2 ClientHello circumvents many important security characteristics of SSL/TLS

- Domino completely disabled SSLv2 including SSLv2 “ClientHello”
  - Some other servers may still accept it even if SSLv2 itself is disabled

- SSLv2 ClientHello might be still used by some applications
  - For example older OpenSSL Libraries or out-of-date clients
  - Workaround is to force a specify protocol version “TLS 1.0”
    - Example: **wget.exe --secure-protocol=TLSv1** ..
  - Potential issue with external SMTP Clients that might not be able to connect any more

Domino 9.0.1 FP3 and IF1

- Domino 9.0.1 FP3 – released 21. Jan 2015
  - No changes in the SSL/TLS area on top of the previous IF
  - Updated JVM (1.6 SR16 FP2) which disables “SSL V3” completely
    - In contrast Oracle JVM only disables it by default
    - Interoperability issues with Java Server Controller/Console
    - FP3 Clients and Servers cannot communicate with earlier releases via Java Console
  - **You should update to 9.0.1 FP3 further updates (IF) with more TLS functionality planned**
- Domino 9.0.1 FP3 IF1 – released 13. Feb 2015
  - New Option to re-enable SSL V2 HELO
    - Notes.ini **SSL_ENABLE_INSECURE_SSLV2_HELLO=1**
    - Will log on protocol debug level: “Received an insecure SSLv2 record; processing by administrator request “

Current Notes.ini Settings

- **DISABLE_SSLV3=1**
  - Prevent incoming SSLv3 connections
  - Fallback to SSLv3 already prevented with some clients via TLS_FALLBACK_SCSV
- **DEBUG_SSL_ALL=2**
  - Or just DEBUG_SSL_HANDSHAKE=2 and DEBUG_SSL_CIPHERS=2 for less noise
- **USE_WEAK_SSL_CIPHERS=1**
  - Not recommended – but if you absolutely must allow frighteningly weak cipher specs
- **SSL_ENABLE_INSECURE_RENEGOTIATE=1**
  - Not recommended – but if you absolutely need “classic” SSL renegotiation
- **SSL_DISABLE_FALLBACK_SCSV=1**
  - Disables TLS_FALLBACK_SCSV functionality
  - Not recommended – Only use if a badly misconfigured client absolutely needs to connect to your server

Updated JVM 1.6 - SR16 FP3

- On top of 9.0.1 FP3
- Fixes vulnerabilities and adds TLS 1.2 support for IBM Java 1.6
  - http://www.ibm.com/support/docview.wss?uid=swg1IV66111
- Separate JVM Patch installer
  - Requires 9.0.1 FP3 to be installed properly because JVM is “patched”
- Next FP4 will include the latest IBM JVM version available at that time
- Separate JVM Patch utility allows more flexibility and quicker response but is an additional install step
  - TIP: There is a silent install option “-s” to install it without user interaction
    - But you still have to check if the JVM has been properly updated!
    - To test invoke for example: java -version

Domino 9.0.1 FP3 IF2/3

- Released 27.3.2015
- Different IF Numbers for servers and clients / Confusing Fixlist entries
    - for Clients you need IF3
    - for Servers you need IF2
- **Introduces TLS 1.2!**
- New Ciphers
    - **A**dvanced **E**ncrption **S**tandard (AES) **G**alois/**C**ounter **M**ode (GCM)
    - **P**erfect **F**orward **S**ecrecy (PFS) via Ephemeral Diffie-Hellman (DHE)
- Support for “secure renegotiation”
- HSTS (Http Strict Transport Security)
    - header informs supported browsers that the site should only be accessed over HTTPS

Secure Renegotiation

- Old-style renegotiation is vulnerable to session splicing attacks
  - Renegotiation disabled by TLS 1.0 Interim Fix

- Security scanners frequently confuse “**doesn't support secure renegotiation**” with “**supports insecure renegotiation**”

- RFC 5746 requires servers that do not support renegotiation to claim support for secure renegotiation

- Changed in 9.0.1 FP3 IF2
  - Now the security scanners are pleased

Why TLS 1.2?

- Uses SHA-256 internally instead of MD5 and SHA-1

- Adds support for ciphers with SHA-256 integrity checking

- Adds support for AEAD (AES-GCM) ciphers

- Other security-related improvements too numerous to mention

Caveats

- TLS 1.2 requires SHA-256 which requires Notes/Domino 9.0.x
  - Significant cryptographic changes between 8.5.x and 9.0.x
  - No plans to back port any enhanced TLS functionality to 8.5.x
- Any template, UI, and string changes require a Maintenance Release
  - Not just a Fix Pack, Interim Fix, or Hot Fix.
  - This is why a separate new keyring tool “kyrtool.exe” was released instead of a new database
- Therefore, until the next MR, configuration of TLS functionality will be limited to
  - notes.ini variables
  - server console commands
  - command line applications

Specifying Ciphers Explicitly - “SSLCipherSpec”

- Server Doc /Internet Site doc are still used to specify the currently supported ciphers
  - They have been re-ordered internally to use the “best ciphers” first
  - Server Doc/Internet Site UI-based Cipher settings are only used by the HTTP task
  - There are new ciphers under development which are not listed in the current dialog
    - Design changes in Domino Directory will have to wait for a maintenance release (9.0.2) , not a FP or IF

- Notes.ini “**SSLCipherSpec**”
  - Used to specify ciphers across all protocols
  - Concatenate the two hex digit numbers for the desired ciphers
  - Example: **SSLCipherSpec=0405**
    - Was used to disable the “CBC” ciphers for all protocols until the second (TLS) POODLE fix was released

      04 = SSL_RSA_WITH_RC4_128_MD5
      05 = SSL_RSA_WITH_RC4_128_SHA

Recommended Cipher List before IF2

- **SSLCipherSpec=2F35050A**
  - **2F** = SSL_RSA_WITH_AES_128_CBC_SHA
  - **35** = SSL_RSA_WITH_AES_256_CBC_SHA
  - **0A** = SSL_RSA_WITH_3DES_EDE_CBC_SHA
  - **05** = SSL_RSA_WITH_RC4_128_SHA
  - ~~**04** = SSL_RSA_WITH_RC4_128_MD5~~

- There is a complete cipher list for each new FP/IF
  - Which ciphers are enabled by default
  - Which additional ciphers can be enabled

- Check the Notes/Domino wiki for updates and details
  - http://www.lotus.com/ldd/dominowiki.nsf/xpViewTags.xsp?categoryFilter=TLS

New Cipher List Default in 9.0.1 FP3 IF2

- **TLS 1.2**
  - **9D** = RSA_WITH_AES_256_GCM_SHA384
  - **9C** = RSA_WITH_AES_128_GCM_SHA256
  - **3D** = RSA_WITH_AES_256_CBC_SHA256
  - **3C** = RSA_WITH_AES_128_CBC_SHA256
  - **35** = RSA_WITH_AES_256_CBC_SHA
  - **2F** = RSA_WITH_AES_128_CBC_SHA
  - **0A** = RSA_WITH_3DES_EDE_CBC_SHA
- That would be
  - SSLCipherSpec=9D9C3D3C352F0A

- **SSL3 / TLS 1.0**
  - **35** = RSA_WITH_AES_256_CBC_SHA
  - **2F** = RSA_WITH_AES_128_CBC_SHA
  - **0A** = RSA_WITH_3DES_EDE_CBC_SHA
  - **05** = RSA_WITH_RC4_128_SHA
    - Rated as weak and disabled for TLS 1.2 by default but is needed for clients which don't support the CBC ciphers

Problem: The All-Seeing Eye

- How do you protect against an attacker who can spy on all of your network traffic?
- In most SSL/TLS cipher specs the client transmits a “**PreMasterSecret**” to the server encrypted with the server's public key
- A passive attacker could record network traffic for years and then acquire the server's private key and decrypt all of that traffic
  - Sound like anybody you know?

Solution: Perfect Forward Secrecy

- No long-term keys are used to generate or transmit the keys used to encrypt your network traffic

- Incurs a significant performance penalty, so test in your environment before enabling
  - For larger websites you should really think twice if you really need it

- PFS shipped with 9.0.1 FP3 IF2
  - DHE_RSA_WITH_AES_128_CBC_SHA
  - DHE_RSA_WITH_AES_256_CBC_SHA
  - DHE_RSA_WITH_AES_128_CBC_SHA256
  - DHE_RSA_WITH_AES_256_CBC_SHA256
  - DHE_RSA_WITH_AES_128_GCM_SHA256
  - DHE_RSA_WITH_AES_256_GCM_SHA384

Additional Ciphers that can be enabled

- SSLCipherSpec=9D9C3D3C352F0A**3339676B9E9F**
  - **33** - DHE_RSA_WITH_AES_128_CBC_SHA
  - **39** - DHE_RSA_WITH_AES_256_CBC_SHA
  - **67** - DHE_RSA_WITH_AES_128_CBC_SHA256
  - **6B** - DHE_RSA_WITH_AES_256_CBC_SHA256
  - **9E** - DHE_RSA_WITH_AES_128_GCM_SHA256
  - **9F** – DHE_RSA_WITH_AES_256_GCM_SHA384
- So you really have to think about which ciphers make sense in your environment
  - Balance performance vs. security

SSL Test Tools

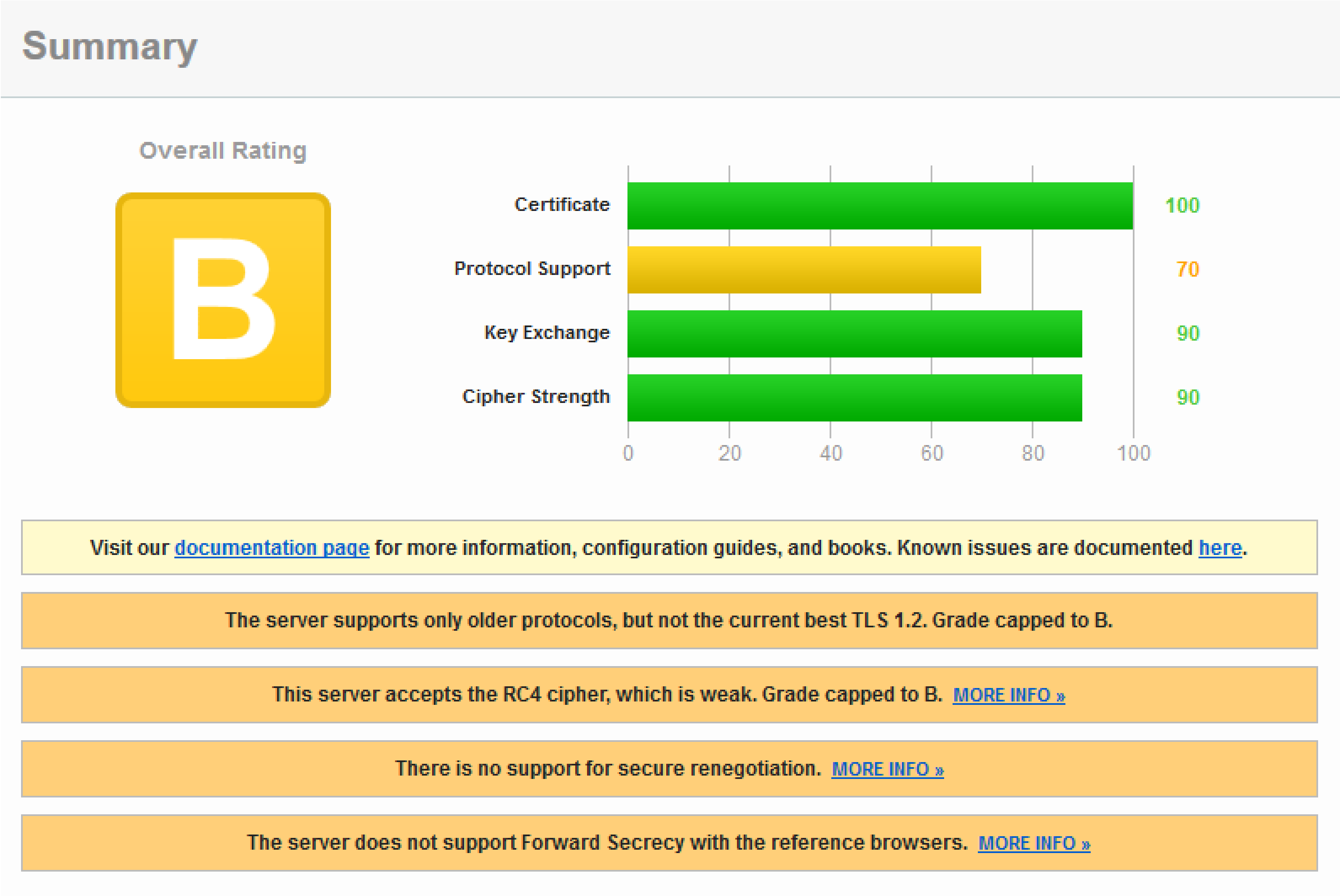
- Probably one of the most busy SSL Test Sites those days
  - Can be used to get an idea about your server security status
  - Will provide a a “rating” for your server from “A” to “F”
  - Also includes details about supported **SSL protocol version** and **ciphers**
    - Also contains a very useful “simulation” what ciphers certain applications might use
  - There is also a test to check which SSL protocol version and ciphers are supported

- Server Test
  - https://www.ssllabs.com/ssltest/

- Client Test
  - https://www.ssllabs.com/ssltest/viewMyClient.html

DEMO

SSL Lab Rating with first TLS Fixes



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

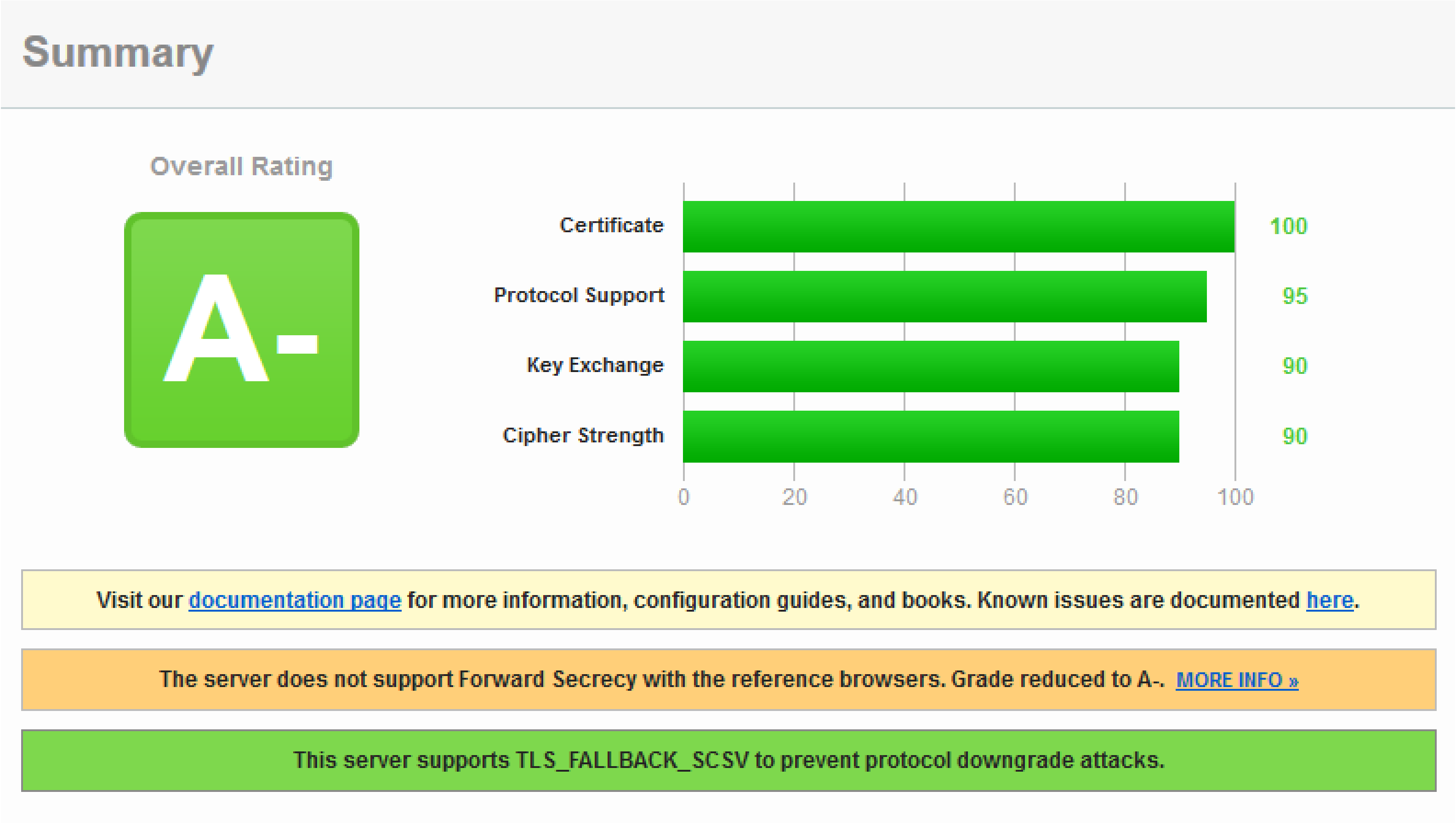
The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

There is no support for secure renegotiation. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

SSL Lab Rating with the new Fixes :-)



Summary

Overall Rating

A-

Certificate	100
Protocol Support	95
Key Exchange	90
Cipher Strength	90

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

DHE Cipher Issue with Java

- By default DHE Cipher use the Key-Length of your Private/Public key (Domino Keyring File)
  - The maximum value is currently 3072 and all values in between are rounded to multiples of 1024
- Java 1.6 and 1.7 does only support 1024 Key-Length
  - So it will pick the DHE Cipher if enabled and will not be able to connect for a key-length > 1024
- Solution
  - Use 1024 Bit key-length for DHE ciphers
  - Down side: SSL Labs already rates 1024 DHE key-size as soft of “weak”
  - Notes.ini **SSL_DH_KEYSIZE=1024** allows you to set the DHE-Key-Size

Cipher Order by default is server based

- In most cases you want the server to determine the ordering of the ciphers
  - In some cases you might want to configure servers to let the client choose the cipher order
  - See default Server Cipher order next slide

- New Notes.ini Parameter
  - SSL_USE_CLIENT_CIPHER_ORDER=1

Reference Slide - Server Cipher Order

- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-CBC-SHA256
- DHE-RSA-AES256-CBC-SHA
- DHE-RSA-AES128-CBC-SHA256
- DHE-RSA-AES128-CBC-SHA
- AES256-GCM-SHA384
- AES128-GCM-SHA256
- AES256-CBC-SHA256
- AES256-CBC-SHA
- AES128-CBC-SHA256
- AES128-CBC-SHA
- DES-CBC3-SHA

Not all Browsers and Applications support “DHE” Ciphers

- "Elliptic Curves ciphers" (ECDHE..) are the supported PFS ciphers in older IE versions and by Windows mobile
  - But they are currently not implemented on the Domino side
  - IBM implemented DHE based on priorities and demand
- ECDHE are needed by those platforms to be fully PFS compliant
  - SSL Labs Test does rate Domino as still not fully PFS compliant because of missing Elliptic Curves ciphers
  - It would also provide better performance compared to “DHE” ciphers
- No official statement -- it might be considered for a future update

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

TLS 1.3

- Cleans up and greatly simplifies the TLS protocol
  - TLS 1.3 overhauls SSL/TLS in the way that TLS 1.0 should have

- Currently just an Internet Draft, but we're following it closely
  - Currently only allows cipher suites with Perfect Forward Secrecy and Authenticated Encryption

- “Under consideration for inclusion in a future release of Notes/Domino”

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Additional New notes.ini Parameters

- DEBUG_SSL_CIPHERS=1/2
  - Debugging for Ciphers

- DEBUG_SSL_DHE=1/2
  - Debugging for the new DHE Ciphers

- SSL_DISABLE_TLS_10=1
  - New option to disable TLS 1.0
  - You should be very careful using this parameter because it might block many applications that don't support TLS 1.2
  - Makes only sense in a very controlled environment
    - Intranet, Between a Secure Proxy and Domino etc
  - Don't forget DISABLE_SSLV3=1

Logging SSL/TLS Errors

- Most of the logging has been “debug” only
  - Messages are only shown on console/console.log

- It is important to see some incompatibility issues and connections that cannot be established in log.nsf

- New logging available and enabled by default
  - You can disable additional logging via notes.ini **SSL_LOGGING_DISABLE=1**

- Examples of what is getting logged
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(1263) failed with server certificate chain requiring support for SHA384
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(3829) failed with no supported ciphers
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(3416) failed with rejecting incoming SSLv3 connection
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(1263) failed with server certificate chain signature alogrithms NOT supported by client

Reminder about Secure Proxies

- Many customers use Reverse Proxies and other SSL enabled proxies

- You need to review those servers as well and check their SSL/TLS support
  - This is not only true for inbound connections to the Proxy but also backend connections to internal severs
  - Most Secure Proxies do support TLS already
  - Many servers (for example Apache based servers) have still SSL 3.0 and older SSL enabled
    - Check SSL level supported and also cipher types!

- Example what to change in Apache and other OpenSource Solutions
  - Ensure Open SSL is up to date and pass the right parameters to OpenSSL
    - SSLProtocol All -SSLv2 -SSLv3
    - SSLCipherSuite AES+EECDH:AES+EDH:AES+RSA:!ECDSA:!DSS

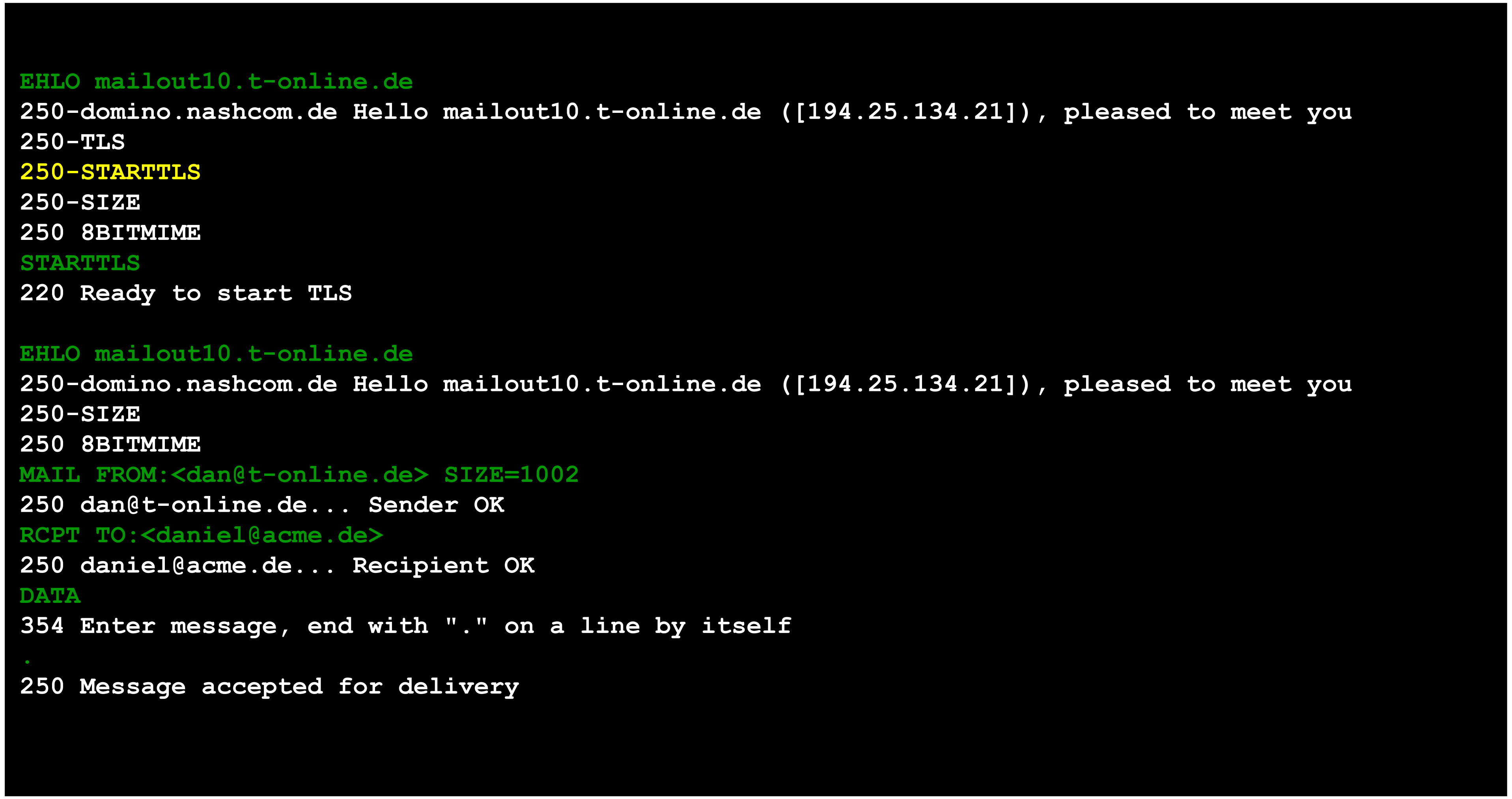
Reference for Useful OpenSSL Commands

- Connect test HTTPS
  - **openssl s_client -connect www.acme.com:443**
- Connect test SMTP TLS
  - **openssl s_client -connect mail.acme.com:25 -starttls smtp**
- Both print detailed information about certificate, protocol an cipher
- Options to force certain SSL versions
  - **-tls1, -no_tls1, -no_ssl3**
- “wget” - another test tool
  - Uses openssl libs and can be used for HTTPS requests
  - **wget.exe [--secure-protocol=TLSv1] --no-check-certificate https://www.acme.com**

Domino SMTP TLS Extension “STARTTLS”

- SSL/TLS for SMTP
  - Often confused with the TLS v1.x protocol
- STARTTLS is an **extension** to the SMTP protocol to allow channel encryption for SMTP on port 25
  - SSL/TLS version, ciphers, and Domino keyring are the same as for other protocols
- How does it work in general
  - Client connects with a “**EHLO**”, Server sends “**250-STARTTLS**” as one of the extensions
  - Client sends “**STARTTLS**”
  - Client and Server negotiate SSL/TLS protocol version and cipher
  - Server replies with “**220 Ready to start TLS**”
  - Client uses another “**EHLO**” to continue the session (now encrypted)
- Reference: “ SMTP Service Extension for Secure SMTP over Transport Layer Security”
  - ” https://www.ietf.org/rfc/rfc3207.txt

Reference Slide - STARTTLS Example



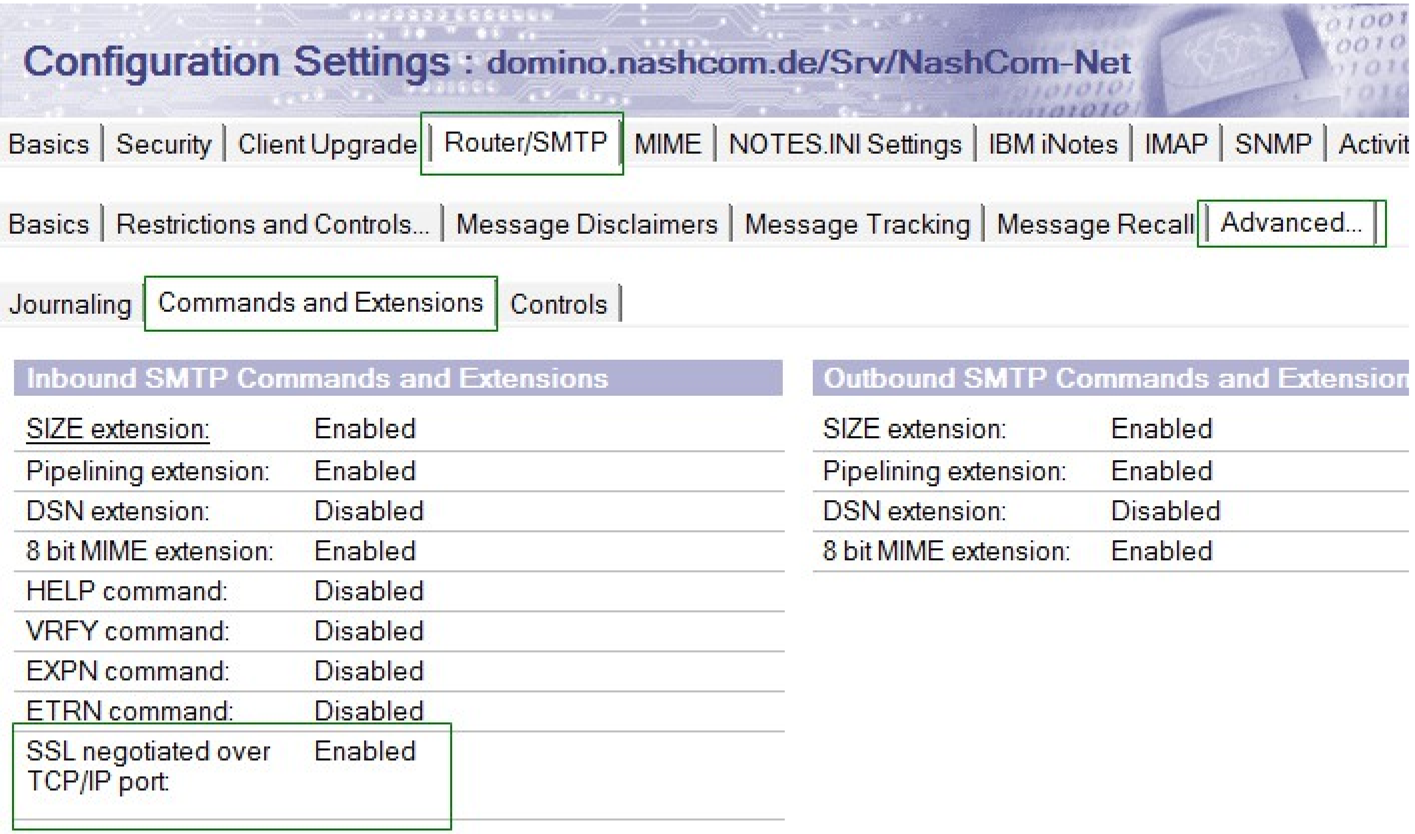
```
EHLO mailout10.t-online.de
250-domino.nashcom.de Hello mailout10.t-online.de ([194.25.134.21]), pleased to meet you
250-TLS
250-STARTTLS
250-SIZE
250 8BITMIME
STARTTLS
220 Ready to start TLS

EHLO mailout10.t-online.de
250-domino.nashcom.de Hello mailout10.t-online.de ([194.25.134.21]), pleased to meet you
250-SIZE
250 8BITMIME
MAIL FROM:<dan@t-online.de> SIZE=1002
250 dan@t-online.de... Sender OK
RCPT TO:<daniel@acme.de>
250 daniel@acme.de... Recipient OK
DATA
354 Enter message, end with "." on a line by itself
.
250 Message accepted for delivery
```

Configure the SMTP TLS Extension – Inbound

- Config Doc: Router/SMTP/Advanced

  Commands and Extensions SSL negotiated over TCP/IP port: Enabled



Configuration Settings : domino.nashcom.de/Srv/NashCom-Net

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | IBM iNotes | IMAP | SNMP | Activit
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced...
Journaling | Commands and Extensions | Controls

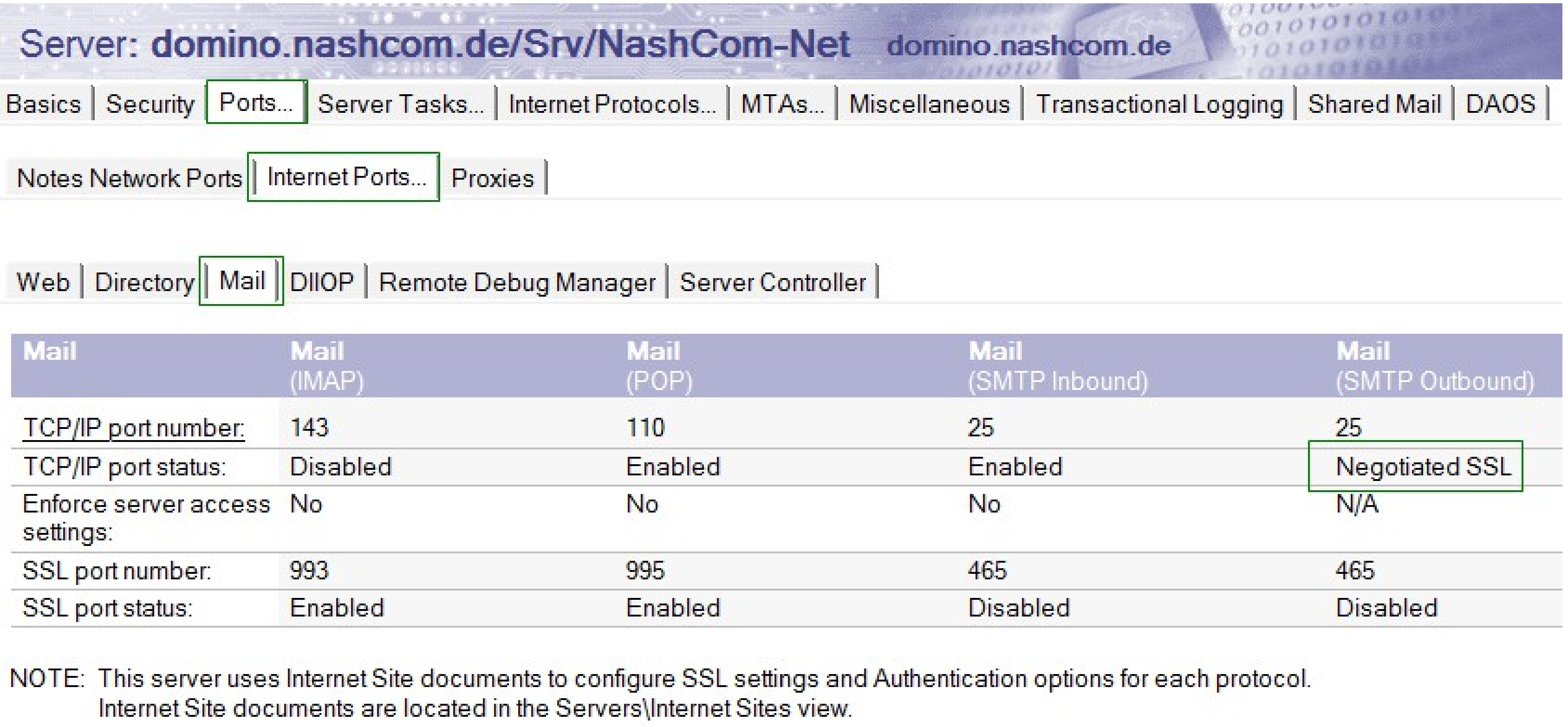
Inbound SMTP Commands and Extensions	
SIZE extension:	Enabled
Pipelining extension:	Enabled
DSN extension:	Disabled
8 bit MIME extension:	Enabled
HELP command:	Disabled
VRFY command:	Disabled
EXPN command:	Disabled
ETRN command:	Disabled
SSL negotiated over TCP/IP port:	Enabled

Outbound SMTP Commands and Extension	
SIZE extension:	Enabled
Pipelining extension:	Enabled
DSN extension:	Disabled
8 bit MIME extension:	Enabled

Configure Outbound TLS

- Server Doc: Ports/Internet Ports/Mail:

  SMTP Outbound: Negotiated SSL


Server: domino.nashcom.de/Srv/NashCom-Net domino.nashcom.de
Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail | DAOS
Notes Network Ports | Internet Ports... | Proxies
Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	25
TCP/IP port status:	Disabled	Enabled	Enabled	Negotiated SSL
Enforce server access settings:	No	No	No	N/A
SSL port number:	993	995	465	465
SSL port status:	Enabled	Enabled	Disabled	Disabled

NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options for each protocol. Internet Site documents are located in the Servers\Internet Sites view.

SMTP TLS Details

- Domino does not check if certificates of connecting clients are “valid”
  - But the X.509 certificate in your Domino Keyring file might be checked by other servers with more paranoid configuration
- Incoming connections might fail completely when no common SSL/TLS version or cipher can be negotiated
  - Less likely now with TLS 1.0 support
  - Tip: If you don't have it enabled it today wait for TLS 1.2 and additional cipher support
  - The “SSLv2 ClientHello” Issue could hit you if a server is for example using an older OpenSSL lib
- For outbound connections you can configure fall-back to non TLS
  - Notes.ini **RouterFallbackNonTLS=1**
- Once “STARTTLS” is configured clients and servers decide if they want to use it

Notes/Domino SHA-2 Support

SHA-1 is rated as “insecure”

- **SHA-1 is not recommended any more**
  - There are at least theoretical attacks against SHA-1
  - Customers are encouraged to move away from SHA-1 to avoid situations we had before with MD5
  - **SHA-256** is recommended and required for secure encryption
  - Governments recommend to move to SHA-256
  - SHA-256 is approved by Federal Information Processing Standard (FIPS) 140-2
  - German BSI also recommends to move to SHA-256

- **Browser vendors decided start to warn when using SHA-1 certificates**
  - For example: Google starts first to warn for certificates expiring end of this year
    - Reducing step by step the expiration time for the certs (1.1.2017, .. 1.1.2016)
  - Affected certificates are all Server and intermediate CAs signed with SHA-1
  - Root Certifiers are not affected because they are verified in a different way

Browser Vendors start to sunset SHA-1

- This means that you have to replace your certificates ASAP
  - Best practice is also to create a new public/private key
    - Key could have been compromised and you don't know about it yet
  - Ensure that the CA you are using already supports SHA-2
    - Most CAs only support SHA-2 today because for exact those reasons
  - If you server certificate expires later than **31.12.2015** and your server does not support SHA-2 yet, consider requesting a cert with a shorter valid period
    - Just a work-around. Better would be to update your server or put a secure reverse proxy in front of it
- References
  - https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/
  - http://googleonlinesecurity.blogspot.de/2014/09/gradually-sunsetting-sha-1.html

SHA-256 (SHA-2) Support

- Domino 9.0.x without the current IFs did already support SHA-256 in some areas
  - X.509 certificate signature verification and S/MIME signed mail
  - Some areas of Notes/Domino where a password such as the Internet (HTTP) password was previously "hashed."
  - Internet CA supports SHA-256

- Domino 9.0.1 FP2 IF1 supports SHA-2 Certificates for all Internet Protocols and for Keyring Files
  - SHA-2 support covers SHA-256, SHA-384, and SHA-512
  - **No Support for SHA-2 is planned for Domino 8.5.x**
    - Domino 8.5.x does not contain SHA-2 support
  - You should consider updating to the current 9.0.1 fixpack and IF if possible

  - New Keyring files Management Tool “**kyrtool**”

New Keyring Tool - “kyrtool”

- Separate Download
  - Available for Win32/64, Linux 32/64 on Client or Server → just needs to be copied to the N/D program directory

- Can be used to import, show, export certificates
  - But not to create a private/public key and a certificate request
- You can use OpenSSL to create the key and the request
  - Or you can use any other tool to create the key and the request
  - Or use an existing key and cert in PEM format

- Importing Trusted Roots
  - Either add all to a single PEM file from leave to note (key, cert, intermediates, root)
  - Or import roots separately
    - Needs Notes/Domino 9.0.1 FP2 IF1 code → Backend API change is needed

Create a Certificate using OpenSSL

- OpenSSL
  - native installed on Linux/Unix
  - On Windows you can use a cygwin environment

- 1. Create a Private/Public Key
  - **openssl genrsa -out server.key 2048**

- 2. Generate a Certificate Signing Request (CSR)
  - **openssl req -new -sha256 -key server.key -out server.csr**

- 3. Send CSR to CA for signing
  - Or create a "self signed" certificate for testing
    - **openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.pem**
  - **Result is a file in "PEM" format**

Verify Import File

- Before importing a PEM file, you should verify the content with the “verify” command
  - Ensure that the certificate chain is complete and ordered correctly (**key, cert, intermediate certs, root cert**)
  - **Special tip:** you can show the certs in an input via to figure out which cert is missing
    - Example: **kyrtool.exe show certs -i c:\domino\all.crt**

- **kyrtool.exe verify c:\domino\all.crt**
  - Successfully read 2048 bit RSA private key
  - INFO: Successfully read 4 certificates
  - INFO: Private key matches leaf certificate
  - INFO: IssuerName of cert 0 matches the SubjectName of cert 1
  - INFO: IssuerName of cert 1 matches the SubjectName of cert 2
  - INFO: IssuerName of cert 2 matches the SubjectName of cert 3
  - INFO: Final certificate in chain is self-signed

Create Keyring File

- Create a new Keyring File
  - **kyrtool create -k keyring.kyr -p password**
  - When creating a keyring file you need to specify a password
    - All other commands will read the password from the **".sth" file**
- Importing Key, Certificate, Intermediates and Trusted root
  - Copy key, cert, intermediates and root certificate into one PEM file
  - **kyrtool import all -k keyring.kyr -i server.pem**
- You can also import the different parts separately
  - **Kyrtool import all|keys|certs|roots -k keyring.kyr -i server.pem**
  - But that makes the import a lot more complicated

Keyring “show” command

- Can be used to show information from a keyring file
- **Kyrtool show certs -k keyfile.kyr**
  - Shows the entire cert chain including the root matching the cert
  - Tip: You can use the show command to dump all certs and use the “**verify**” command on the resulting file
- **Kyrtool show keys -k keyfile.kyr**
  - Shows all keys in the keyfile
- **Kyrtool show roots -k keyfile.kyr**
  - Shows all trusted roots in the keyfile
- Verbose option “-v” can be used to dump more detailed information
  - More “-v”s on the command line results in more information

Reference - Converting file formats

- Kyrtool requires “PEM” format (text based - BASE64 encoded DER format)
  - In many cases your CA might use different formats (e.g. Microsoft CA)

- OpenSSL is your friend when converting different formats
  - But syntax is not always easy to figure out
  - Convert a PKCS#12 file (.pfx .p12) containing a private key and certificates to PEM

    -
      ```
      openssl pkcs12 -in cert.pfx -out cert.pem -nodes
      ```
  - Convert Binary DER formatted certificate to text based (BASE64) PEM format

    -
      ```
      openssl x509 -inform der -in server.cer -outform pem -out server.pem
      ```
  - Convert Binary DER formatted certificate chain to text based (BASE64) PEM format

    -
      ```
      openssl pkcs7 -print_certs -inform der -in certificate_chain.p7b -outform pem -out chain.pem
      ```

Notes S/MIME Support

SHA-2 for S/MIME

- For SHA-2 with S/MIME the “FIPS 140-2” algorithms are required
- Enable Option in Person Doc on Admin Tab
  - **“Can decrypt documents using FIPS 140-2 approved algorithms: YES”**
- FIPS 140-2 algorithms need at least 1024 bit RSA keys
- Many Domino environments still use 512/630 RSA keys
  - This usually leads to increasing Cert.ID,/OU-Cert.ID, Server.ID, User.ID Cert Len in combination with a key-rollover
- This is not a simple click & ready project
  - You have to plan this migration!

ID Cert & Key Rollover – Step by Step

- 1. First recertify Certs.ID, OU-Cert.ID

- 2. Than recertify servers and users with the higher key len

- Finish re-certification before starting key-rollover for server and later users
  - 1. Key-Rollover is triggered in Server doc for servers and Security Policy for users
  - 2. Server/Client creates new Private/Public Key and sends a public key signing request
  - 3. Admin uses Certifier or Domino CA zu recertify server/user

  - Potential conflict with “Public Key checking”!
  - Certificate is always pushed to the user via changed certificate in person/server doc
  - Client/Server pickup certificate
  - User Workstation will push modified ID changes to ID-Vault

Known Issue for ID-Vault with Recert/Keyrollover

- User.ID is overwritten with the ID in ID-Vault
  - Recertification and Key-Rollover fails

- Defect SPR # YDEN9KYL23
  - Local Id Is Being Overwritten By The Copy In The Id Vault During Rollover/Recertification Even Though Local Id Is Up

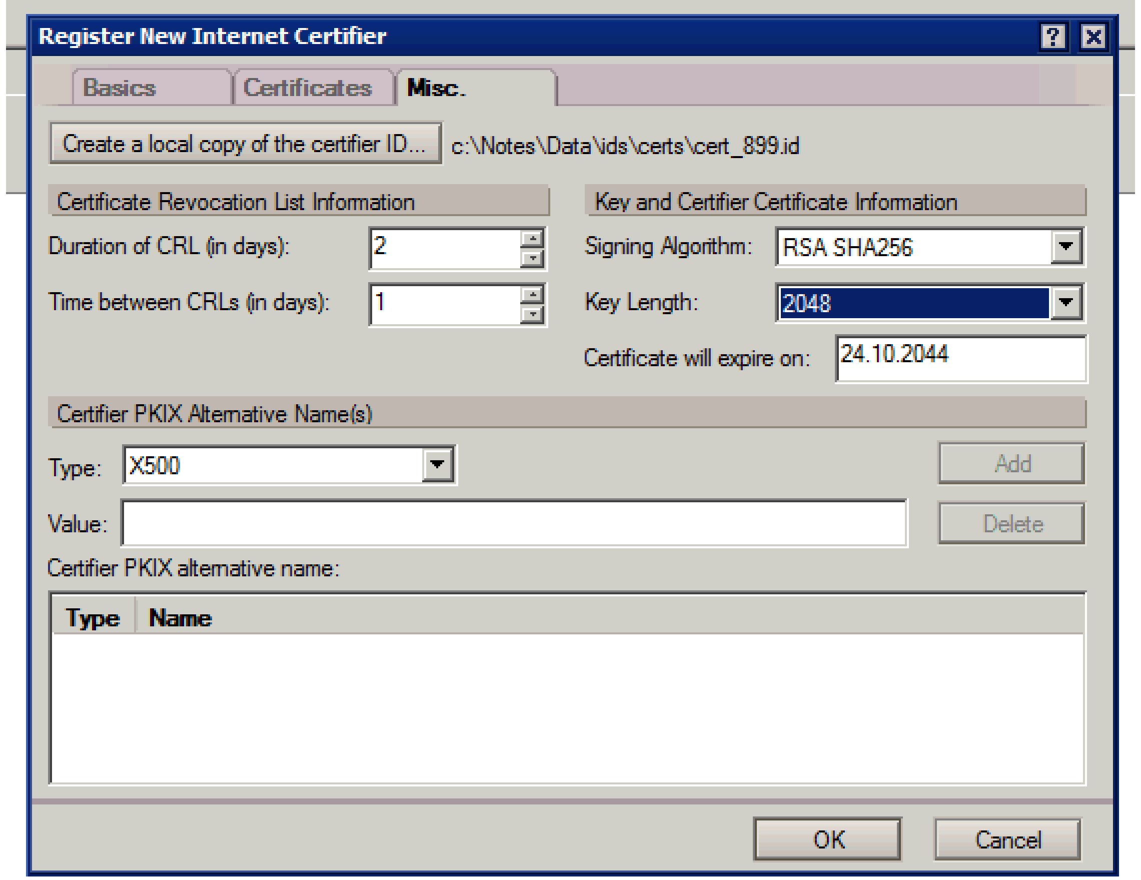
    The issue reported on SPR #YDEN9KYL23 was possible to be worked around by Deleting the affected user.id from the id vault and running updall -r on the id vault database

- First customer feedback as shown that the fix solves the re-certification and key-rollover issues we faced

- SPR is included in the current TLS interims fixes and 9.0.1 FP3

Increasing Internet Certificate Key Size

- Domino 9 Internet CA Supports SHA-2
  - You can remove an re-create the Internet Certifier with SHA256 and higher key length
  - Or create multiple Internet Certifiers



Register New Internet Certifier

c:\Notes\Data\ids\certs\cert_899.id

Certificate Revocation List Information

Duration of CRL (in days): 2

Time between CRLs (in days): 1

Key and Certifier Certificate Information

Signing Algorithm: RSA SHA256

Key Length: 2048

Certificate will expire on: 24.10.2044

Certifier PKIX Alternative Name(s)

Type: X500

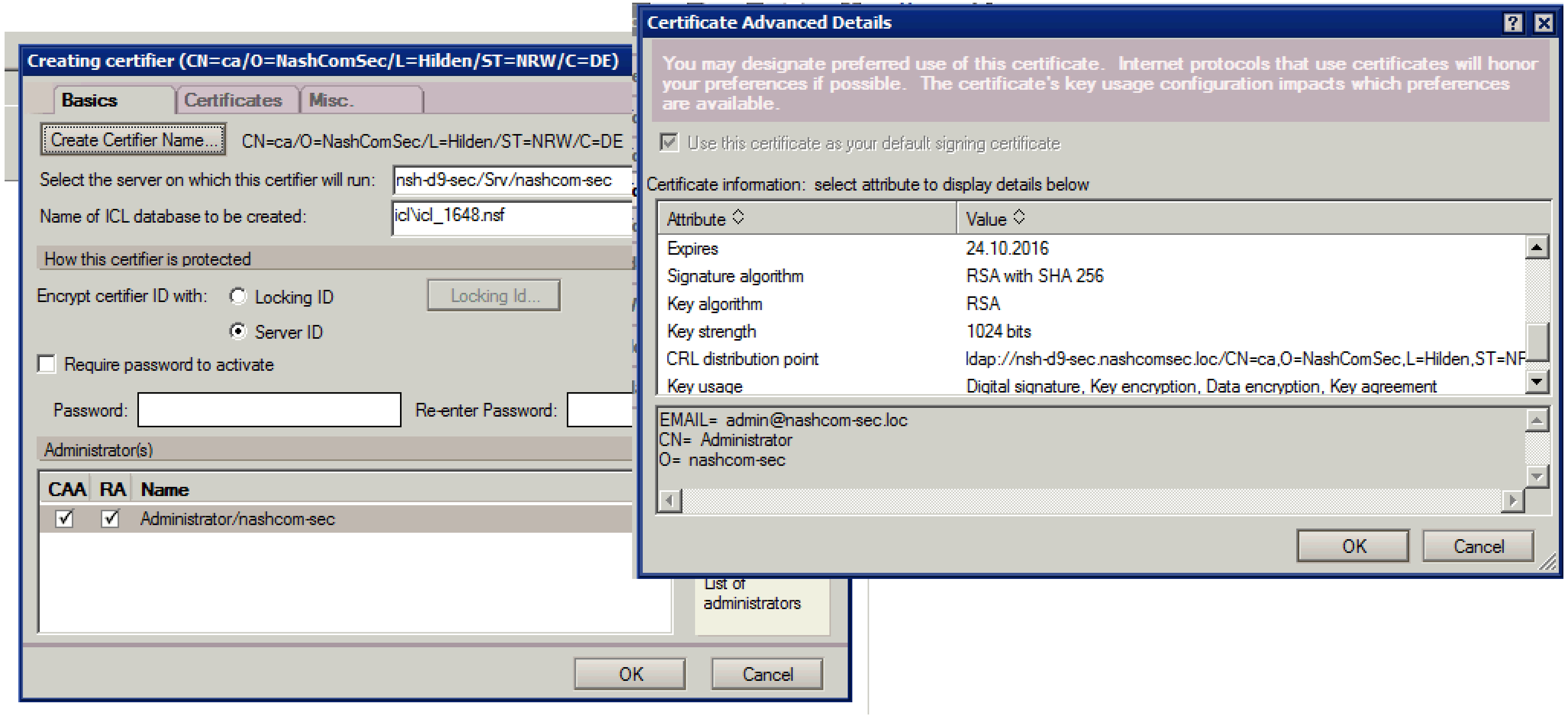
Value:

Certifier PKIX alternative name:

Type	Name

Internet CA Result

- Resulting CA can be used to assign new certificates to users via Person Doc



Creating certifier (CN=ca/O=NashComSec/L=Hilden/ST=NRW/C=DE)

CN=ca/O=NashComSec/L=Hilden/ST=NRW/C=DE

Select the server on which this certifier will run: nsh-d9-sec/Srv/nashcom-sec

Name of ICL database to be created: icl\icl_1648.nsf

How this certifier is protected

Encrypt certifier ID with: ○ Locking ID ● Server ID

□ Require password to activate

Password: Re-enter Password:

Administrator(s)

CAA	RA	Name
☑	☑	Administrator/nashcom-sec

List of administrators

Certificate Advanced Details

You may designate preferred use of this certificate. Internet protocols that use certificates will honor your preferences if possible. The certificate's key usage configuration impacts which preferences are available.

☑ Use this certificate as your default signing certificate

Certificate information: select attribute to display details below

Attribute	Value
Expires	24.10.2016
Signature algorithm	RSA with SHA 256
Key algorithm	RSA
Key strength	1024 bits
CRL distribution point	ldap://nsh-d9-sec.nashcomsec.loc/CN=ca,O=NashComSec,L=Hilden,ST=NF
Key usage	Digital signature, Key encryption, Data encryption, Key agreement

EMAIL= admin@nashcom-sec.loc
CN= Administrator
O= nashcom-sec

External Internet Certificates

- There is still no simple way to import external certificates
  - User has to manually import the cert

- Possible solution: Supported C-API Call to import the X.509 Certificate
  - Send the complete X.509 Certificate in a password protected P12
    - Send the password in the same email
    - Encrypt the email with the Notes.ID
    - Create Lotus Script button that descripts the mail and uses **PKCS12_ImportFileToIDFile** to import the key via C-API

C-API Call to Import X.509 Certificate

- Import Internet Certificate

  -
    ```
    STATUS LNPUBLIC PKCS12_ImportFileToIDFile(
    char *pPKCS12Filename,
    char *pPKCS12Filepassword,
    char *pIdFilename,
    char *pIdFilepassword,
    DWORD  ImportFlags,
    DWORD  ReservedFlags,
    void *pReserved);
    ```

Import External Certificate into Person Doc

User has usually no access to update protected fields in person doc

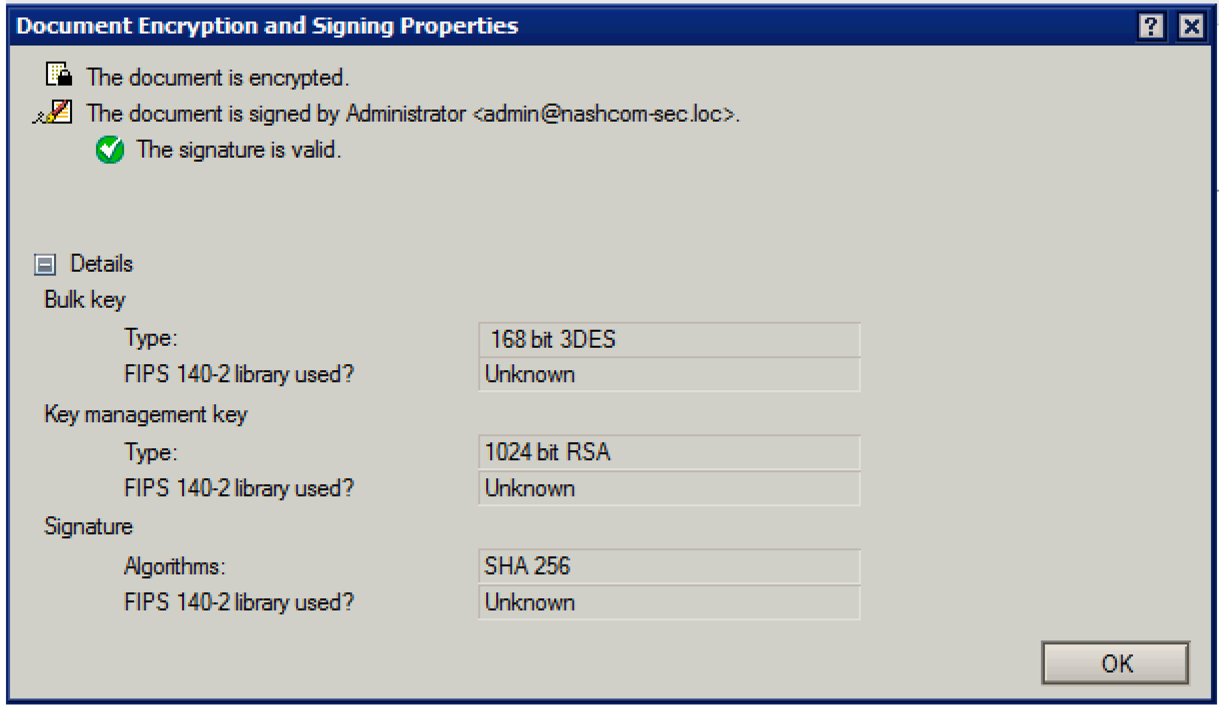
- Administrator might not have access to the user's certificate
  - User could send a signed mail after importing X.509 cert

- There is a C-API call to import the X.509 public key into the person document

  -
    ```
    STATUS LNPUBLIC SECNABAddCertificate(
        NOTEHANDLE  hNote,
        void *pCertificate,
        DWORD  CertificateSize,
        DWORD  ReservedFlags,
        void *pReserved);
    ```

Enabling stronger ciphers and SHA-2

- Client Notes.ini (deployed via desktop policy) needs the following settings
  - SMIME_CAPABILITIES_SEND=AES_128:SHA_256
  - SMIME_FIRST_CHOICE_CONTENT_ENC_ALG=AES_256



Document Encryption and Signing Properties

The document is encrypted.

The document is signed by Administrator <admin@nashcom-sec.loc>.

The signature is valid.

Details

Bulk key

Type:	168 bit 3DES
FIPS 140-2 library used?	Unknown

Key management key

Type:	1024 bit RSA
FIPS 140-2 library used?	Unknown

Signature

Algorithms:	SHA 256
FIPS 140-2 library used?	Unknown

New BSI Whitepaper – 11.2.2015

- **BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen"**
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf
- Use of block ciphers:
  - AES-128, AES-192, AES-256 with
    - Galois-Counter-Mode (GCM)
    - Cipher-Block Chaining (CBC)
    - Counter Mode (CTR)
- Asymmetric encryption:
  - ECIES 224 (after 2015 at least 250), DLIES and RSA >= 2048 Bits (after 2016 at least >= 3072 bits)
- Hashing: SHA-224, SHA-256, SHA-512/256, SHA-384, SHA-512, SHA-512/224
  - **SHA1 should not used for any new certificate** → After 2015 only: SHA-256, SHA-384, SHA-512, SHA-512/256
- Key exchange:Diffe-Hellma (DHE_RSA)/ EC Diffe-Hellman (ECDHE_RSA)

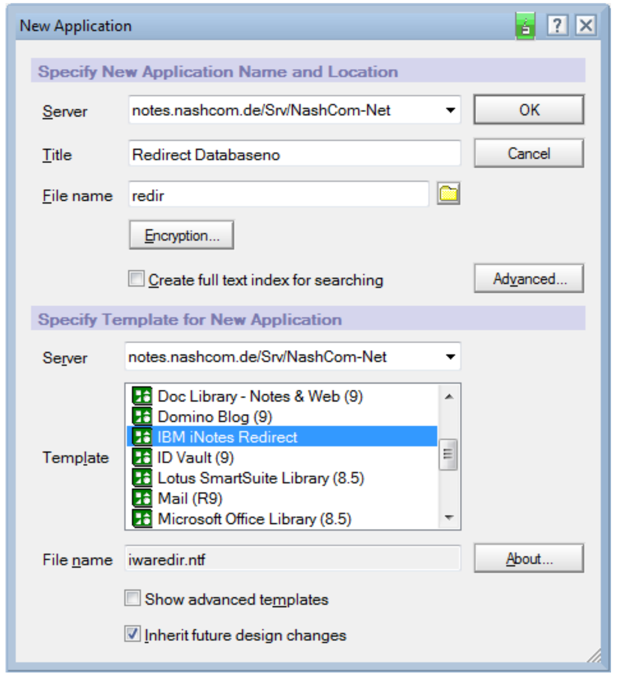
Q & A

- Thanks for your attention!
- Questions?
  - Now? or find me during the conference
- Stay tuned for new information
  - http://www.lotus.com/ldd/dominowiki.nsf/xpViewCategories.xsp?lookupName=Domino%20security
  - http://blog.nashcom.de / email: nsh@nashcom.de

Additional Material

iNotes Redirect Database

- The IBM iNotes Redirector
- Acts as an entry point and authentication prompt for IBM iNotes
- Database contains configurable settings for redirection, SSL, customization and mode selection/availability.



New Application

Specify New Application Name and Location

Server: notes.nashcom.de/Srv/NashCom-Net

Title: Redirect Databaseno

File name: redir

□ Create full text index for searching

Specify Template for New Application

Server: notes.nashcom.de/Srv/NashCom-Net

Template:
- Doc Library - Notes & Web (9)
- Domino Blog (9)
- IBM iNotes Redirect
- ID Vault (9)
- Lotus SmartSuite Library (8.5)
- Mail (R9)
- Microsoft Office Library (8.5)

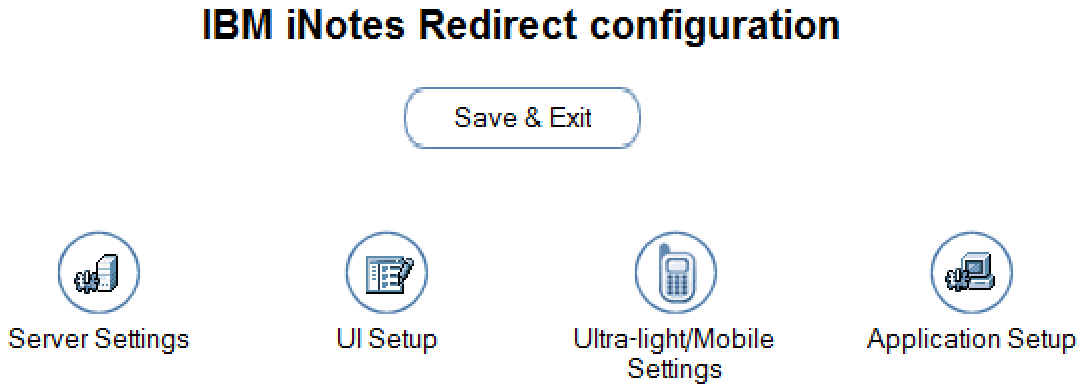
File name: iwaredir.ntf

□ Show advanced templates

☑ Inherit future design changes

iNotes Redirect Database

- Create database and start configuration
- Ensure database has “**No Access**” for **Anonymous** user
  - This will trigger authentication before redirect
- Redirect will lookup the user and redirect user based on configuration
- Multiple configuration types and options available


IBM iNotes Redirect configuration
Save & Exit
Server Settings
UI Setup
Ultra-light/Mobile Settings
Application Setup

iNotes Redirect Database ACL

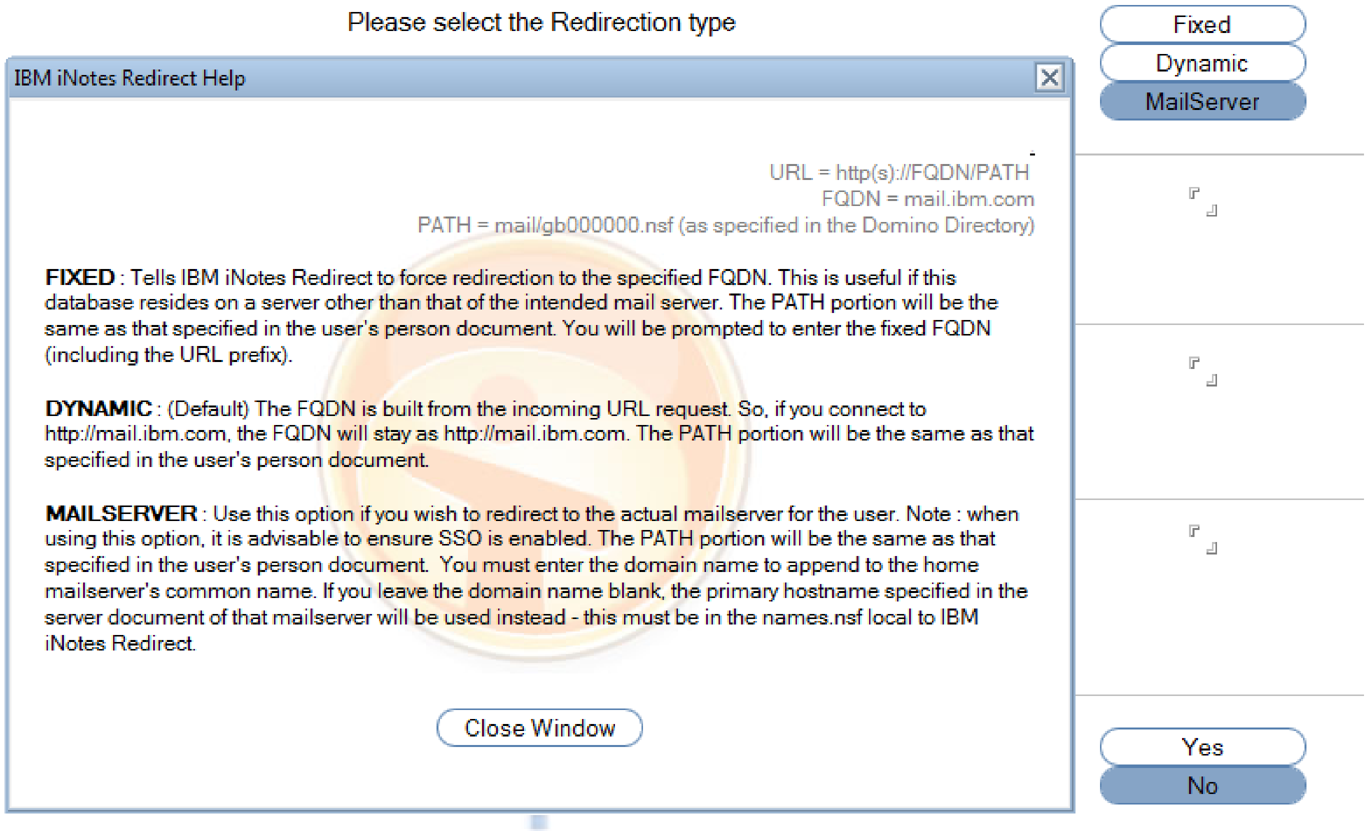
- It is important to have the right ACL configured

- Anonymous (for not authenticated users)
  - “No Access”
  - “Read Public Documents”

- Default (for authenticated users that are redirected
  - “Reader”

Redirection Types

- 3 Redirection Types
  - Fixed
  - Dynamic
  - MailServer



Please select the Redirection type

IBM iNotes Redirect Help

URL = http(s)://FQDN/PATH
FQDN = mail.ibm.com
PATH = mail/gb000000.nsf (as specified in the Domino Directory)

FIXED : Tells IBM iNotes Redirect to force redirection to the specified FQDN. This is useful if this database resides on a server other than that of the intended mail server. The PATH portion will be the same as that specified in the user's person document. You will be prompted to enter the fixed FQDN (including the URL prefix).

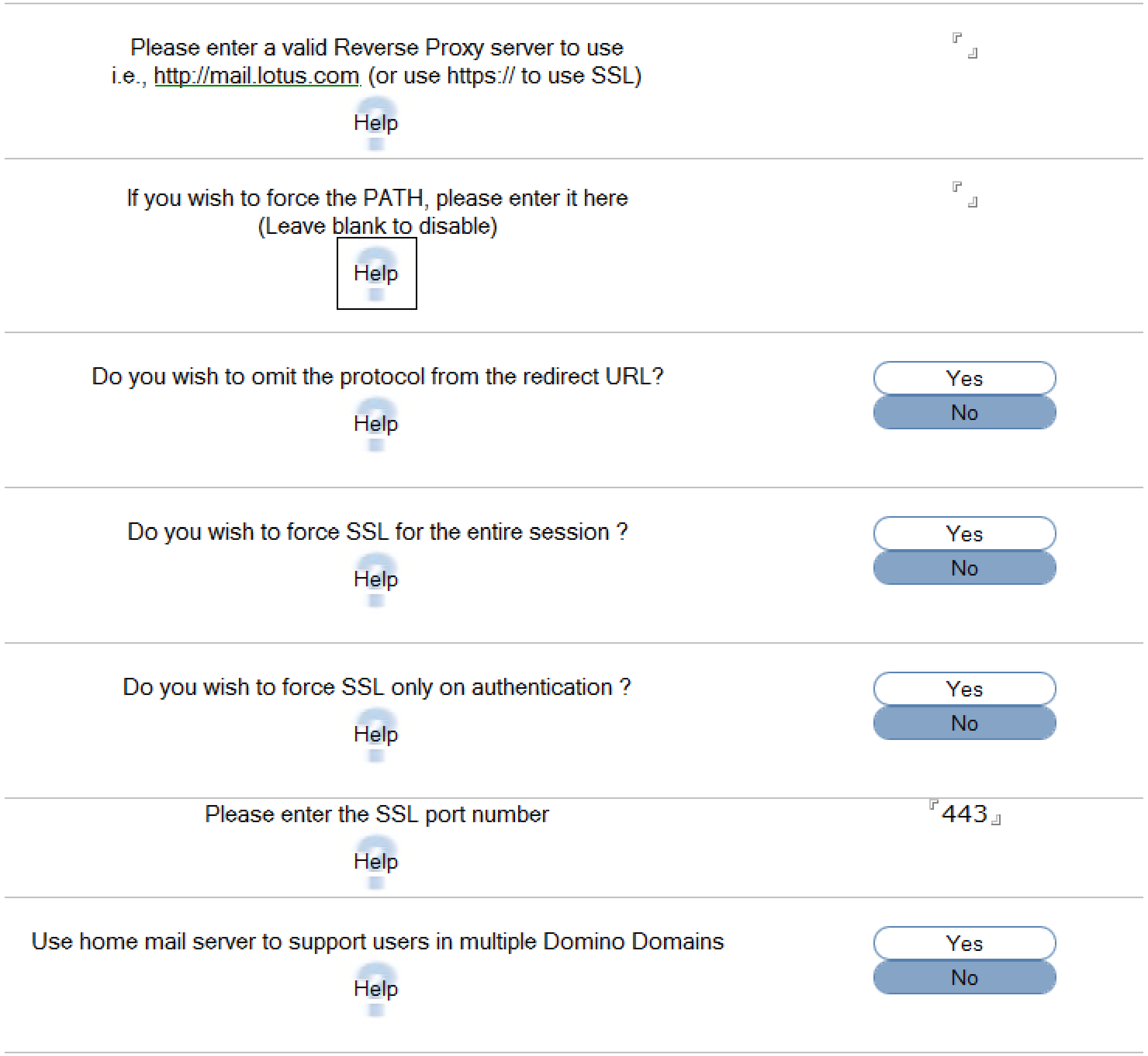
DYNAMIC : (Default) The FQDN is built from the incoming URL request. So, if you connect to http://mail.ibm.com, the FQDN will stay as http://mail.ibm.com. The PATH portion will be the same as that specified in the user's person document.

MAILSERVER : Use this option if you wish to redirect to the actual mailserver for the user. Note : when using this option, it is advisable to ensure SSO is enabled. The PATH portion will be the same as that specified in the user's person document. You must enter the domain name to append to the home mailserver's common name. If you leave the domain name blank, the primary hostname specified in the server document of that mailserver will be used instead - this must be in the names.nsf local to IBM iNotes Redirect.

How does this work with multiple Clusters?

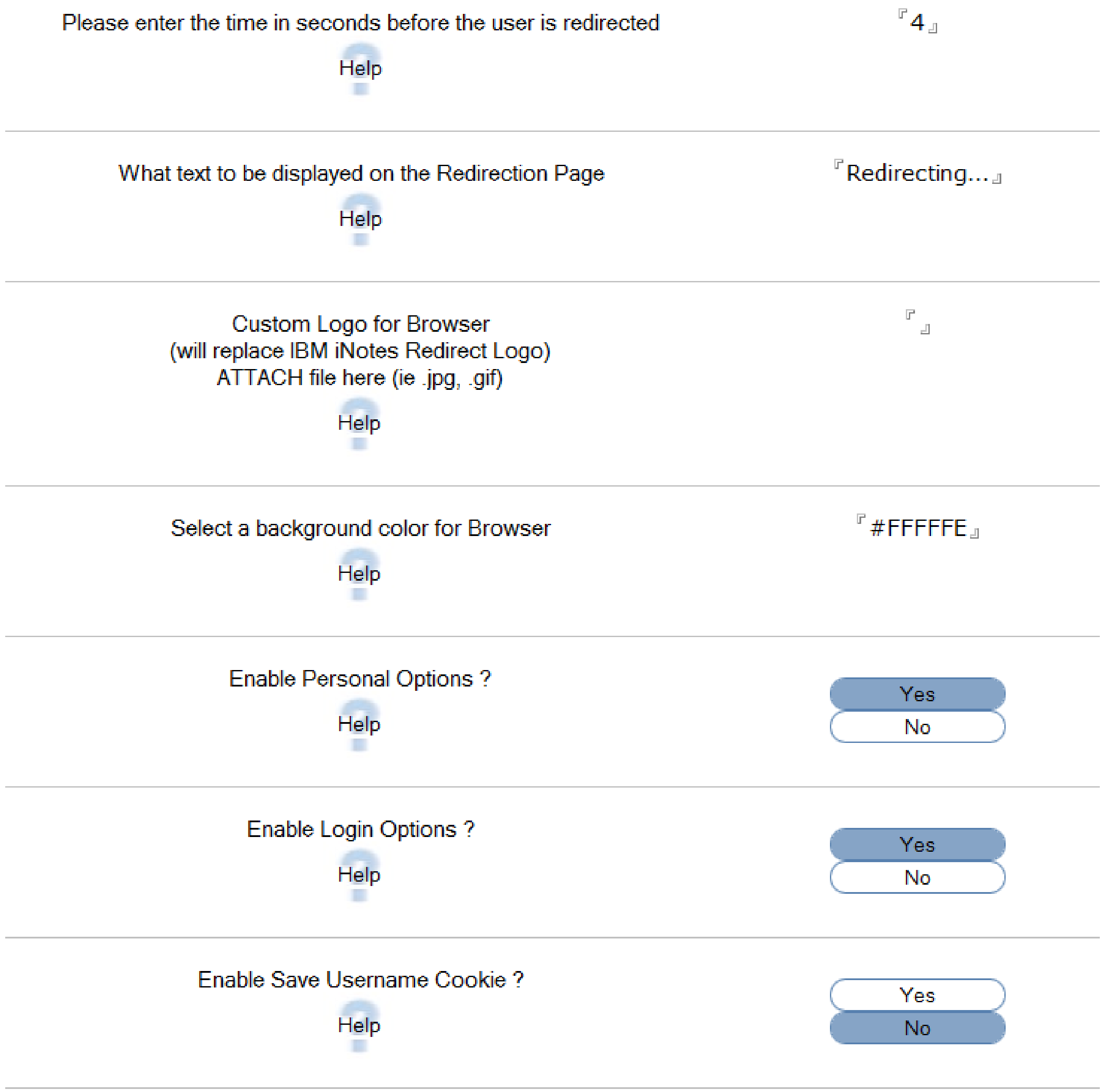
- One set of servers as entry point for your iNotes Redirect DB
- Choose “Mail-Server” redirection option
- One approach
  - Use a different “Full Qualified Server Name” than Domino Server Name because name need to point to the proxy instead of the server itself via DNS
  - Ensure the name points to your proxy
  - Have the primary back-end server in the proxy for that entry point to the primary server
  - Have the cluster partner as a fall-back server
  - Do the same for all your mail-servers
  - That way iNotes Redirect will always send users to their home-mail-server
    - Failover occurs only when home-mail-server is not reachable

REF: Many very detailed Options



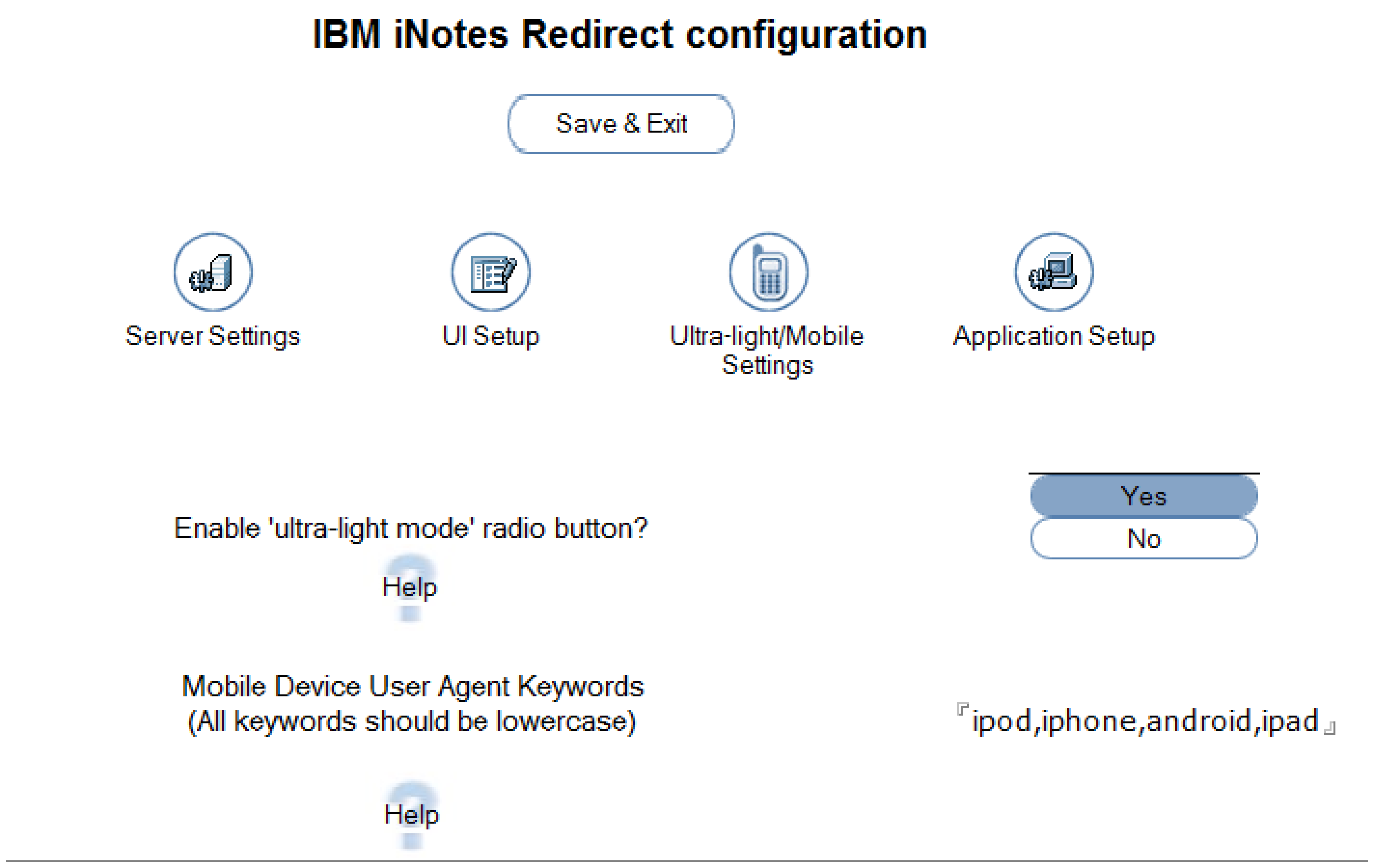
Please enter a valid Reverse Proxy server to use i.e., http://mail.lotus.com (or use https:// to use SSL) Help	⸢ ⸥
If you wish to force the PATH, please enter it here (Leave blank to disable) Help	⸢ ⸥
Do you wish to omit the protocol from the redirect URL? Help	Yes [✓ No]
Do you wish to force SSL for 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	⸢443⸥
Use home mail server to support users in multiple Domino Domains Help	Yes [✓ No]

REF: UI Options



Please enter the time in seconds before the user is redirected Help	4
What text to be displayed on the Redirection Page Help	Redirecting...
Custom Logo for Browser (will replace IBM iNotes Redirect Logo) ATTACH file here (ie .jpg, .gif) Help	
Select a background color for Browser Help	#FFFFFE
Enable Personal Options ? Help	● Yes ○ No
Enable Login Options ? Help	● Yes ○ No
Enable Save Username Cookie ? Help	○ Yes ● No

REF: Mobile Device Options



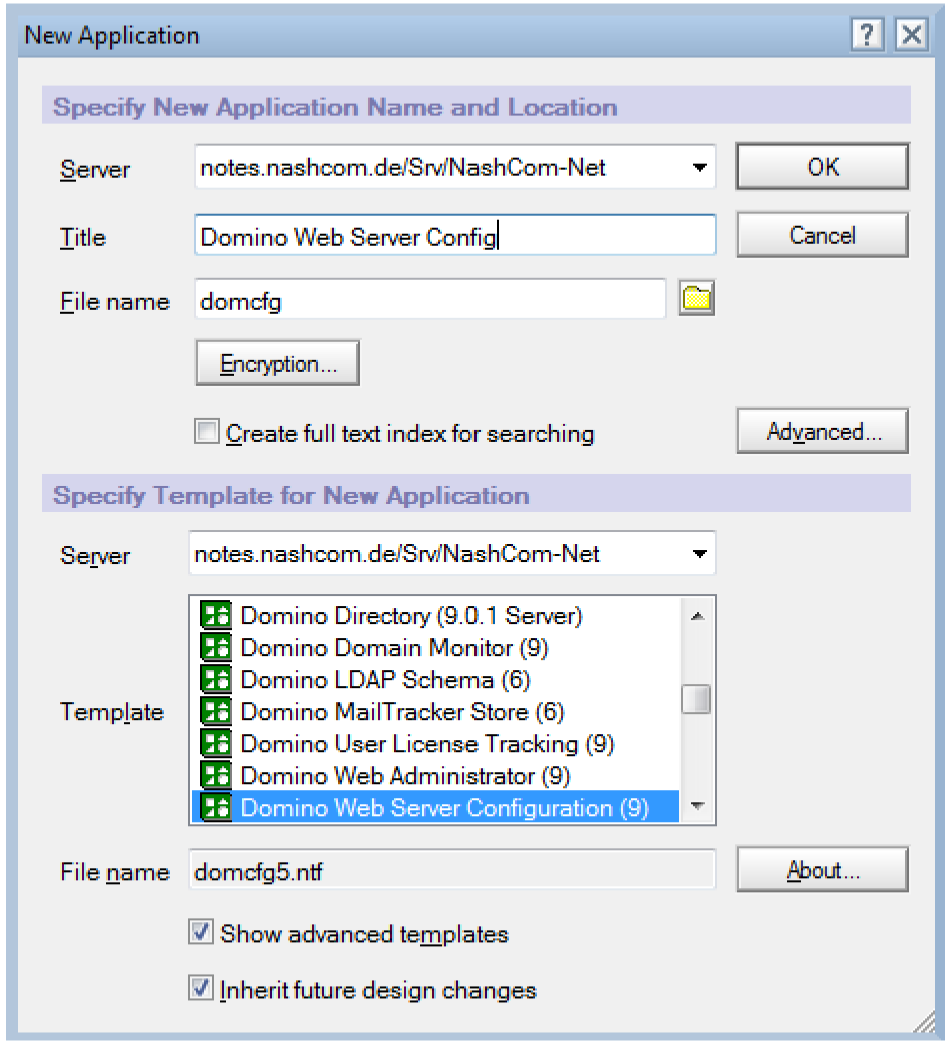
IBM iNotes Redirect configuration

Enable 'ultra-light mode' radio button? [✓ Yes] No

Mobile Device User Agent Keywords (All keywords should be lowercase) ipod,iphone,android,ipad

Domino Web Server Configuration DB

- DomCfg.nsf is required for using the custom login form from redirect database



New Application

Specify New Application Name and Location

Server: notes.nashcom.de/Srv/NashCom-Net

Title: Domino Web Server Config

File name: domcfg

☐ Create full text index for searching

Specify Template for New Application

Server: notes.nashcom.de/Srv/NashCom-Net

Template:
- Domino Directory (9.0.1 Server)
- Domino Domain Monitor (9)
- Domino LDAP Schema (6)
- Domino MailTracker Store (6)
- Domino User License Tracking (9)
- Domino Web Administrator (9)
- Domino Web Server Configuration (9)

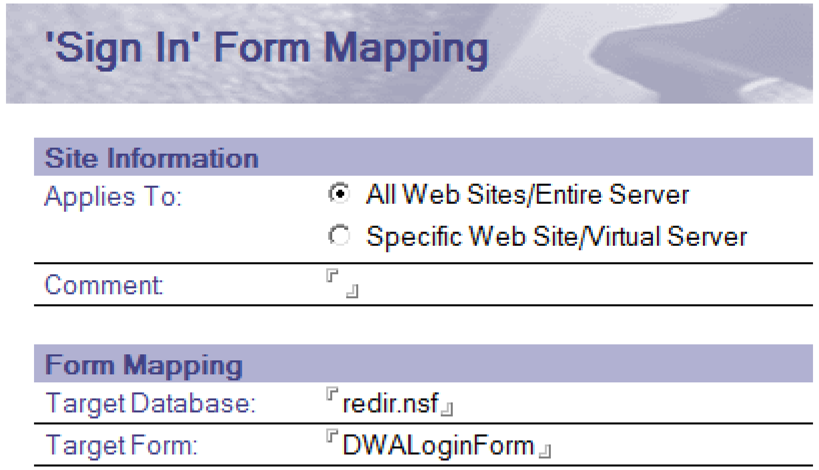
File name: domcfg5.ntf

☑ Show advanced templates

☑ Inherit future design changes

Map Redirect Form

- Create a “Sign In” Form Mapping
  - Point to DWALoginForm in your redirect database



'Sign In' Form Mapping

Site Information

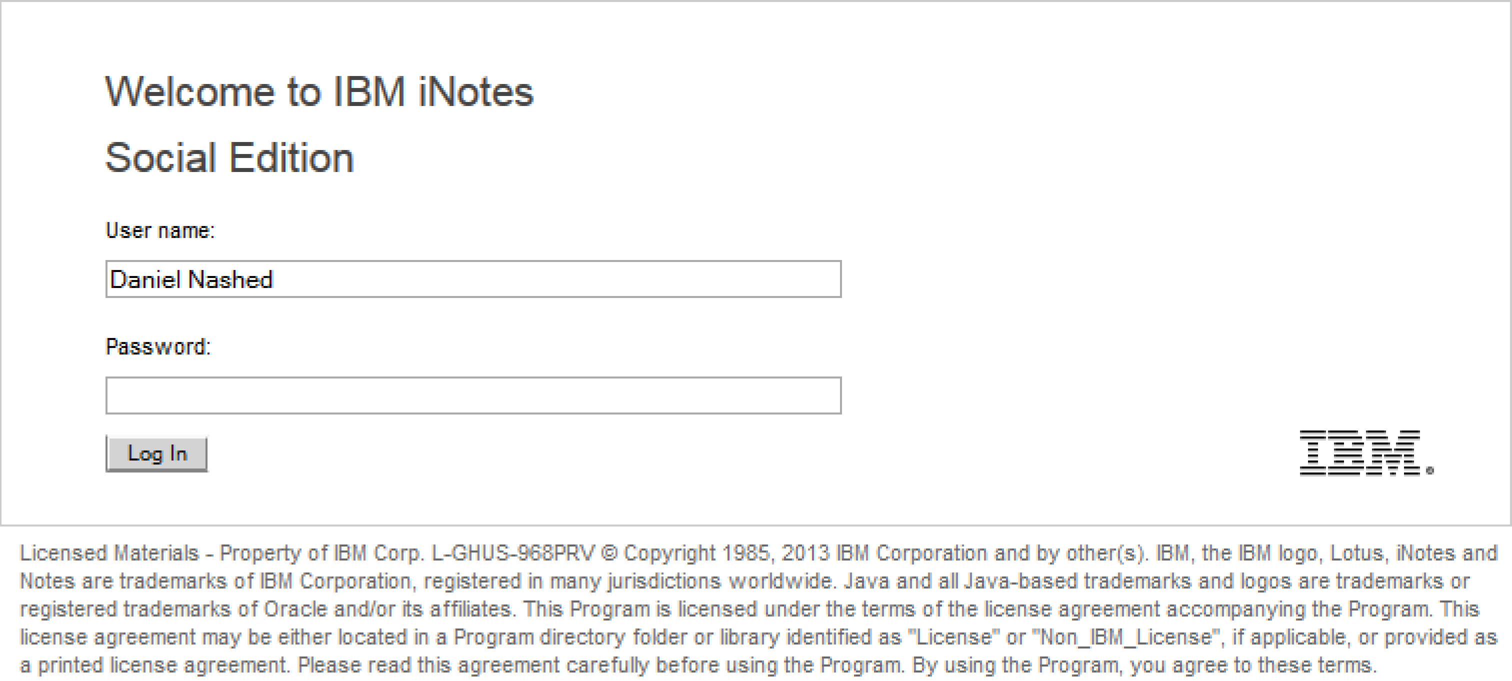
Applies To:	● All Web Sites/Entire Server ○ Specific Web Site/Virtual Server
Comment:	

Form Mapping

Target Database:	redir.nsf
Target Form:	DWALoginForm

Redirect Login Form UI

- This is the default UI
- You can customize the UI
  - Only the Look & Feel but not the fields!
  - Most of the internal logic is hardcoded in the HTTP Task



Welcome to IBM iNotes

Social Edition

User name:

Daniel Nashed

Password:

Licensed Materials - Property of IBM Corp. L-GHUS-968PRV © Copyright 1985, 2013 IBM Corporation and by other(s). IBM, the IBM logo, Lotus, iNotes and Notes are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. This Program is licensed under the terms of the license agreement accompanying the Program. This license agreement may be either located in a Program directory folder or library identified as "License" or "Non_IBM_License", if applicable, or provided as a printed license agreement. Please read this agreement carefully before using the Program. By using the Program, you agree to these terms.