

Domino Security - not knowing is not an option

Updated and all new
(well, some new)



Darren Duke

Janitor Level 57 56

Simplified Technology Solutions, Inc

10,000 feet view

- **What we'll (hopefully) cover**

- **Server Security**

- SSL/TLS/SHA2
- Reverse Proxies
- Testing
- Antivirus settings on the client and server

1 Slide Review

- **Get a SHA2 certificate**
- **Remove any SSLCipherSpec settings from notes.ini**
- **Upgrade to 9.0.1 FP6 IFx**
- **Restart HTTP**
- **Get a “B” on SSL Labs**
- **Ignore the rest of this presentation**
- **But you’ll miss a lot of snark.....And how to get an “A+”**

About Me

- **I'm just a poor boy**
- **From a poor family**
- **He's just a poor boy from a poor family**
- **Spare him his life from this monstrosity**
- **Easy come, easy go, will you let me go**



About Me

- **AKA my favorite slide**
- **Started with “Lotus Notes” in R3**
- **Yes, really....R3**
- **That means 1996**
- **Yes, really....1996**
- **Founder of STS (2005) based in Atlanta**
- **Sometime blogger, ranting Tweeter, ex-co-host of This Week In Lotus, Speaker (?), soon to be born-again podcaster**
- **<http://blog.darrenduke.net>**
- **Twitter [@darrenduke](https://twitter.com/darrenduke)**



Disclaimer

- **Everything in MY presentations are REAL**
 - Except maybe the 9.0.1 FP7 parts
 - No real need to have lawyers interject a crappy slide here
 - But asnot having unreadable garbage on this slide may diminish my professional reputation, here you go
- **Lorem ipsum dolor sit amet**, consectetur adipiscing elit. Sed rhoncus interdum leo, in aliquet velit mattis porttitor. Mauris vestibulum suscipit aliquam. Suspendisse sed euismod eros. Vestibulum pharetra vestibulum fermentum. Phasellus malesuada maximus libero, sit amet egestas justo vestibulum non. Vivamus at nisl id est consectetur sodales vitae nec quam. Nunc et consectetur nibh.
- Cras nec ultricies risus. Maecenas condimentum, tortor at venenatis elementum, lectus turpis mattis enim, et egestas nisl sem et turpis. Vivamus blandit tristique tortor, eu cursus augue. Donec lacinia mi id malesuada lobortis. Vivamus tristique, tellus id tincidunt feugiat, justo nulla commodo risus, in commodo enim augue non metus. Proin varius rutrum velit, ac pretium lorem efficitur a. Nulla non sem arcu. Suspendisse eleifend dui at lacus scelerisque, et scelerisque elit accumsan. Nullam eu iaculis nibh. Etiam ac diam quis mauris tincidunt bibendum. Pellentesque eleifend laoreet ultricies. Cras sollicitudin, quam vel fermentum ullamcorper, nisl metus volutpat odio, et lobortis eros eros id leo. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur sollicitudin ac massa efficitur eleifend.
- Cras orci lorem, tempus quis maximus ut, fermentum sit amet odio. Integer dolor diam, ullamcorper sit amet dignissim eu, facilisis rhoncus erat. In condimentum viverra accumsan. Maecenas metus mi, porta non augue nec, finibus finibus arcu. Integer quis augue quis massa fringilla ullamcorper feugiat et massa. Aenean et neque ante. Nam tristique elementum ipsum, ac tempus lorem euismod vitae. Ut ornare enim a nibh tincidunt cursus. Suspendisse at enim sodales, ullamcorper justo vitae, semper lectus. Nullam ex felis, sollicitudin vel lacinia quis, ultricies cursus turpis. Nullam elementum blandit risus vel porta. Nullam tempus eget augue a fringilla. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.
- Integer a ipsum a nisl eleifend dapibus. Nunc porttitor mi quis urna euismod consectetur. Donec placerat nisl gravida odio lacinia, non scelerisque urna aliquam. Sed dolor justo, varius id fermentum ut, fermentum ac mi. Curabitur eu sollicitudin nunc. Proin sodales, metus non dictum mollis, justo lectus sagittis quam, elementum fringilla est erat nec felis. Sed non euismod lorem, in hendrerit arcu. Donec eu euismod metus. Cras justo est, faucibus ut posuere quis, viverra a dolor.
- Sed gravida velit lacus, sed volutpat metus venenatis quis. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec iaculis accumsan ante eget porta. Duis sit amet commodo velit. Integer est tortor, euismod congue sem quis, lobortis convallis erat. Aliquam erat volutpat. Mauris pretium rutrum interdum. Nullam non magna nunc.
- Generated 5 paragraphs, 408 words, 2794 bytes of [Lorem Ipsum](#)

SHA2

- **SHA = Security Hashing Algorithm**

- Each SSL certificate is either SHA1 or SHA2
- SHA2 far more secure than SHA1
- SHA1 is dead. Browsers now have issues with SHA1.

- **SHA2 Support in Domino**

- If you are on 8.5.3, upgrade to 9.0.1 or put a proxy in front of it
- For 9.0.1 FP3+ you can now create SHA2 CSR's and import SHA2 certificates in Domino. Go to at least 9.0.1 FP5
- This is a very different process than what you are used to
 - See Gab's excellent step-by-step on how to do this:
 - <http://turtleblog.info/2015/06/22/creating-sha-2-4096-ssl-certificates-for-domino/>
 - <http://www-01.ibm.com/support/docview.wss?uid=swg21418982>

Server Security SSL/TLS/SHA2

- **SSLv3 is dead (SSLv2 has been dead for a long time)**
 - Unless you need it for SMTP STARTTLS compatibility
 - Disable it if you can (you can....no really, you can)
 - Server notes.ini `DISABLE_SSLV3=1`



Server Security SSL/TLS/SHA2

- **TLS is King, long live the King**

- TLS 1.0 via IF for the following releases

- With 8.5.3 FP6
 - 9.0
 - 9.0.1 FP2+

- TLS 1.2 for

- 9.0.1 FP3 (plus IF)
 - 9.0.1 FP4+
 - Perfect Forward Secrecy/HSTS
 - Additional (more secure) ciphers
 - SHA2



Server Security SSL/TLS/SHA2

- **Don't forget Perfect Forward Secrecy**

- In cryptography, **forward secrecy** (FS; also known as **perfect forward secrecy**, or PFS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. (via wikipedia)

- Domino now supports it as of 9.0.1 FP3 IF2/3 and higher

- The data is secure even if the server private key is compromised in the future
 - This is a good thing. Use it.

Server Security SSL/TLS/SHA2

- **Don't forget HSTS**

- **HTTPS Strict Transport Security**

- It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol (via wikipedia)

- **Domino now supports HSTS as of 9.0.1 FP4+**

- Add these to the server notes.ini

- **HTTP_HSTS_INCLUDE_SUBDOMAINS=1**

- **HTTP_HSTS_MAX_AGE=63072000**

- Will get you an A+ on SSL Labs with Domino native HTTP stack

- Also see <https://blog.darrenduke.net/Darren/DDBZ.nsf/dx/domino-adds-hsts-to-its-security-arsenal.htm>

Server Security SSL/TLS/SHA2

- **Don't forget OSCP Stapling**

- What is it?

- **OCSP stapling**, formally known as the **TLS Certificate Status Request** extension, is an alternative approach to the [Online Certificate Status Protocol](#) (OCSP) for checking the revocation status of [X.509 digital certificates](#).^[1] It allows the presenter of a certificate to bear the resource cost involved in providing OCSP responses by appending ("stapling") a [time-stamped](#) OCSP response [signed](#) by the CA to the initial [TLS Handshake](#), eliminating the need for clients to contact the CA

- Go faster strips for HTTPS connections

- Domino now supports OSCP Stapling as of 9.0.1 FP4+

- To configure see

- <https://blog.darrenduke.net/Darren/DDBZ.nsf/dx/supercharge-your-domino-servers-with-ocsp-stapling-real-go-faster-stripes.htm>

Server Security SSL/TLS/SHA2

•SMTP with STARTTLS

- You fix a lot of problems with

- Server notes.ini SSL_ENABLE_INSECURE_SSLV2_HELLO=1

•Ciphers

–No longer controlled in the Server/Internet doc (9.0.1). Now a notes.ini, but you don't really need to anymore

–Domino server now dictates the preferred cipher list

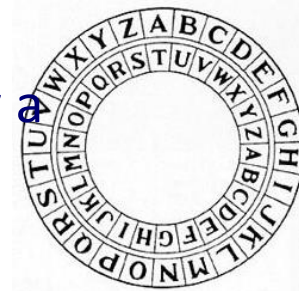
- For < 9.0.1 FP3 Server notes.ini SSLCipherSpec=AABBCCDDEE..ZZ
- Just upgrade to FP4+ and remove the SSLCipherSpec setting

•For all TLS 1.2 options see

–http://www-10.lotus.com/ldd/dominowiki.nsf/dx/TLS_1.2

–http://www-10.lotus.com/ldd/dominowiki.nsf/dx/TLS_Cipher_Configuration

read this one!!



Server Security SSL/TLS/SHA2

- **If you org only wants to allow TLS 1.2**

- You can disable TLS 1.0 (and obviously SSLv3)

- Server notes.ini SSL_DISABLE_TLS_10

- This could cause SMTP STARTTLS issues so beware

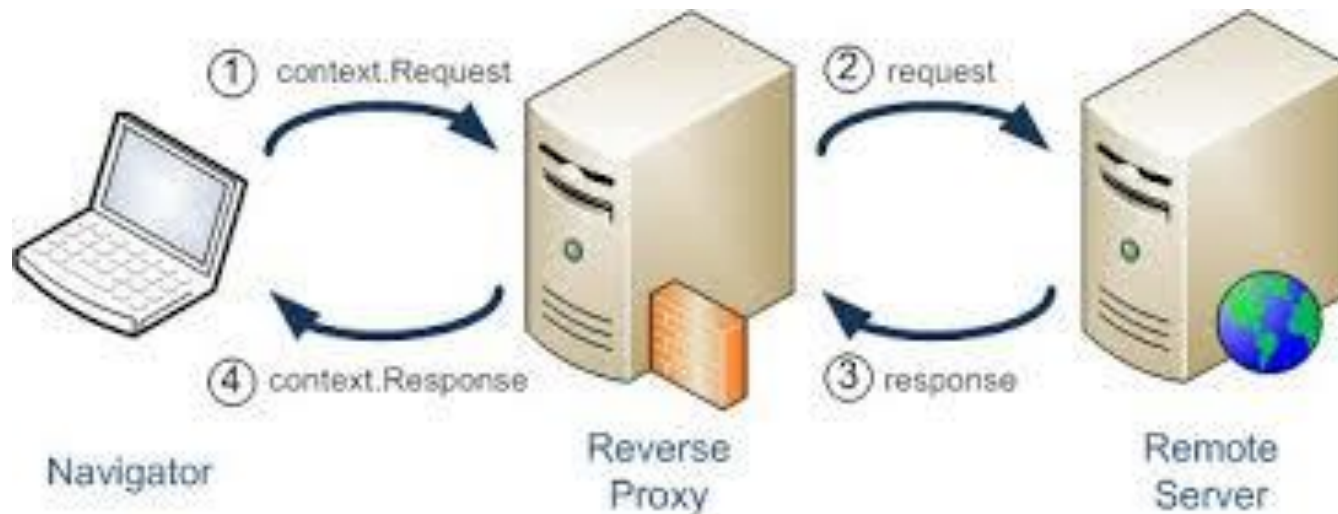
- All recent browsers have TLS 1.2 enabled by default now

- Older browsers (IE on XP) may not

Reverse Proxies

•What is a Reverse Proxy?

- In computer networks, a **reverse proxy** is a type of **proxy** server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as though they originated from the **proxy** server itself - Wikipedia



Reverse Proxies

•Benefits

- You can handle more than one web server per proxy

- Reduce (potential attack) surface area

SSL offloading

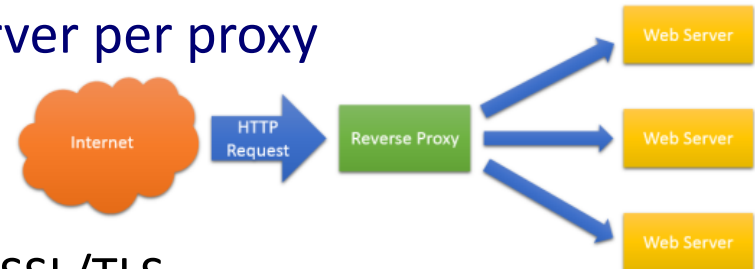
- Have the reverse proxy handle all your SSL/TLS
- When security issue detected, one place to fix

–Security

- Hide version/platform/application from the browser
- No direct access to backend servers
- Restrict URL access to Domino for only required URLs for
 - iNotes
 - Traveler
 - Domino web applications (allow Quickr to work with “modern browsers”)

–Load balancing

- Provide HA for iNotes, Traveler, etc



Reverse Proxies

•The Proxies

•NGINX (pronounced Engine X)

- Most popular today, used by Netflix, Zappos, et al
- Open source
- Can do mail and other TCP connections, not just HTTP(S)
 - IMAP
 - SMTP (including STARTTLS)

–Apache

- Most famous
- Open source
- I have a free Apache VM using Ubuntu you can use as starting point:
 - <http://blog.darrenduke.net/darren/ddbz.nsf/dx/here-is-a-freely-available-vm-to-reverse-proxy-domino-shoot-the-poodle.htm>

–I would normally use HAProxy in addition to the above to provide HA functions (on the same Linux Ubuntu server)

Reverse Proxies

•The Proxies

•IBM HTTP Server (IHS)

- No longer recommended by IBM as a front end to Windows Domino Servers

- Was in 9.0

- But only on Windows

- Never extended to other platforms

- Shocker, I know

–This was IBM's original fix in Domino 9 to add TLS1.0

- Don't do this anymore

–Websphere Edge Proxy

- It has the word "Websphere" in the title so won't touch it unless someone connects a car battery to my genitals

Reverse Proxies

- **The Real Reason to use a Proxy**

	Date Spec Released	Date IBM Added to Domino	Time Taken by IBM (in years)
TLS 1.0	1999	2014*	15
TLS 1.2	2008	2015	7
PFS	2011*	2015	4

- **With a Proxy you may have avoided SSLv3 and this:**



Testing

- So you **think** you're secure? OK.....
- Testing is what elevates belief to evidence
- Qualys SSL Labs test site for web sites
 - <https://www.ssllabs.com/ssltest/>
 - Scan a server, get a grade
 - Will take a few minutes
 - Also lists potential remediation
 - Tons of useful information
 - If you get a "A" or higher you're good
 - Scan every quarter or so. Things change!
 - Use on sites other than your own
 - Be scared. Be real scared.

[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Domain name: Do not show the results on the boards

Recently Seen

[womensradio.com](#)[mdm.shareni.org](#)

Recent Best

[moore.lib.unb.ca](#) A+[seattledietdelivery.com](#) A

Recent Worst

[hcorpo.com](#) F[rl77agency.com](#) T

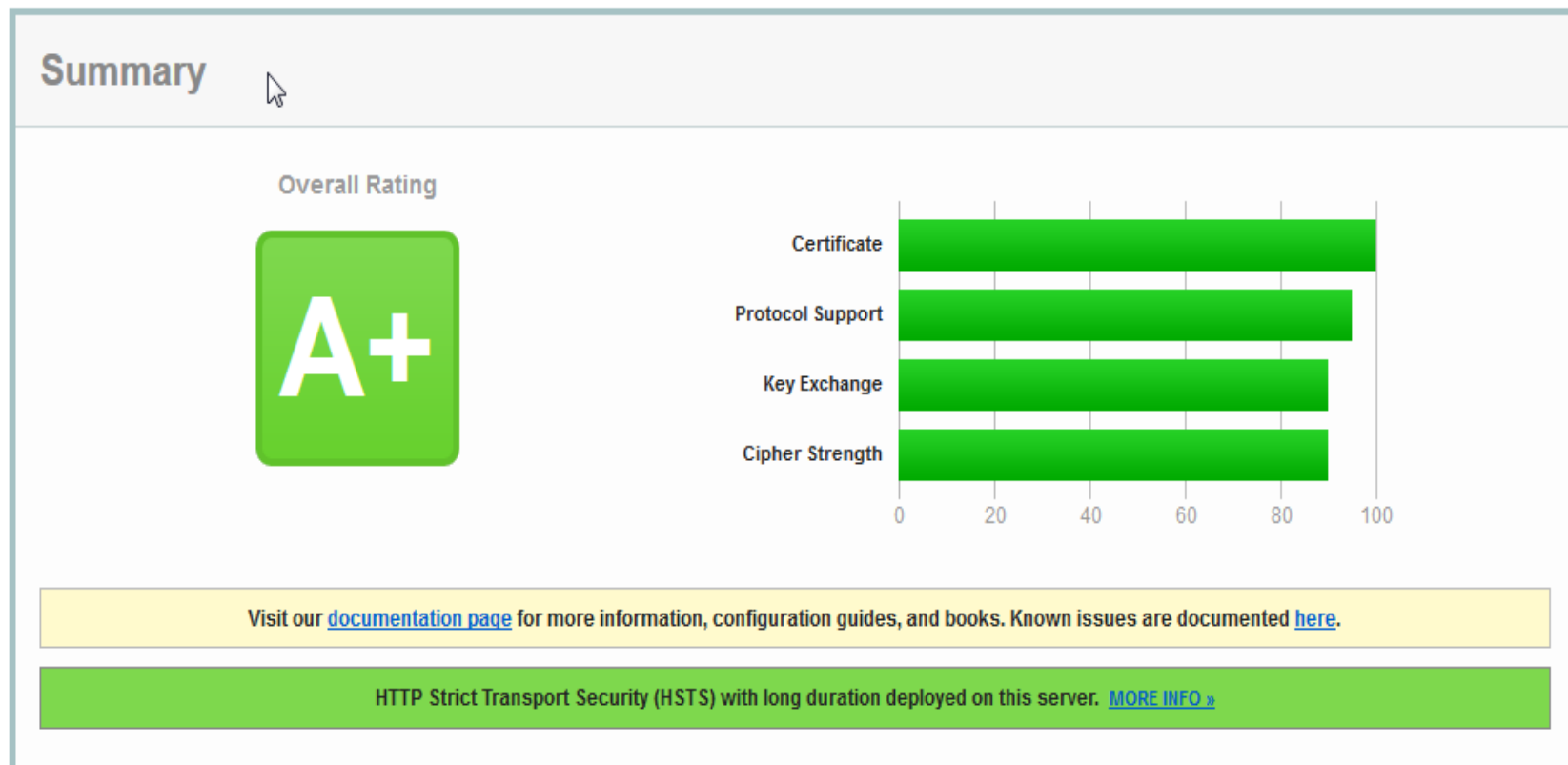
Testing

- Here is my iNotes server behind an Apache Reverse Proxy

SSL Report: [webmail.simplified-tech.com](https://www.ssllabs.com/ssltest/analyze.html?d=webmail.simplified-tech.com) (96.38.252.232)

Assessed on: Wed, 18 May 2016 20:31:24 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)



Testing

- Here is an iNotes server via SSL on Domino native (no proxy)

SSL Report: [REDACTED]

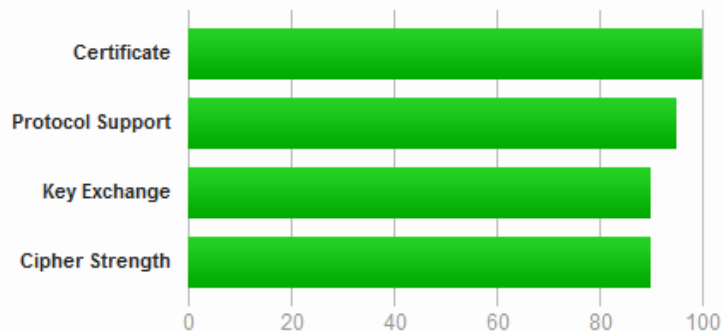
Assessed on: Wed, 18 May 2016 20:39:14 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another »](#)

Summary



Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Testing

- **A Note about Windows XP/2003 with IE Support and ciphers**
 - I know, you have a plan to get off XP and 2003
 - No, really, we believe you
 - Yes, I know you need to sunset your Windows 98 SE workstations first....

 - Most people think you need RC4 to support XP with IE

 - **YOU DON'T!!!**
 - 3DES will provide support for XP/2003 with IE
 - Domino now enables RC4 ONLY if TLS 1.2 is disabled
 - Chrome and FF on XP can do better than 3DES
 - The issue with embedding a browser into an OS.....

Testing

- Test SMTP STARTTLS at CheckTLS.com
 - <https://www.checktls.com/testreceiver.html>
 - Test bot
- Receive

```
Trying TLS on simplified-tech-com.p10.spamhero.com[209.105.224.168] (10):
seconds  test stage and result
[000.047]  Connected to server
[000.106]<--220 bolt10a.mxthunder.net ESMTP Postfix
[000.106]  We are allowed to connect
[000.107]-->EHLO checktls.com
[000.155]<--250-bolt10a.mxthunder.net
          250-PIPELINING
          250-SIZE 524288000
          250-ETRN
          250-STARTTLS
          250-ENHANCEDSTATUSCODES
          250-8BITMIME
          250 DSN
[000.155]  We can use this server
[000.155]  TLS is an option on this server
[000.156]-->STARTTLS
[000.205]<--220 2.0.0 Ready to start TLS
[000.205]  STARTTLS command works on this server
[000.356]  Cipher in use: DHE-RSA-AES256-SHA
[000.356]  Connection converted to SSL
[000.371]  Certificate 1 of 4 in chain:
          subject= /OU=Domain Control Validated/OU=PositiveSSL Wildcard/CN=*.mxthunder.com
          issuer= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA
[000.385]  Certificate 2 of 4 in chain:
          subject= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA
          issuer= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
[000.399]  Certificate 3 of 4 in chain:
          subject= /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Certification Authority
          issuer= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
[000.413]  Certificate 4 of 4 in chain:
          subject= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
          issuer= /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
[000.413]  Cert VALIDATED: ok
[000.413]  Cert Hostname DOES NOT VERIFY (simplified-tech-com.p10.spamhero.com != *.mxthunder.com)
[000.413]  (see RFC-2818 section 3.1 paragraph 4 for info on wildcard ("*") matching)
[000.414]  So email is encrypted but the host is not verified
```

Testing

- Send

- You send email with a code in it, CheckTLS then replies to you with the

```
Your email was successfully sent securely using TLS.
```

A transcript of the eMail SMTP session is below:

```
--> this would be a line from your email system to our test
<-- and this would be a line to your email system from our test
```

If TLS was negotiated, a line is added:

```
====tls negotiation successful (cypher: cyphername, client cert: certinfo)
```

Everything after that line is secure (encrypted), as indicated by:

```
~~> commands from your system then have wiggly lines
<~~ and responses from our system do too
```

Any errors that the test noticed are noted in the log by asterisk boxes:

```
*****
*** ***** Error Note ***** ***
***                               ***
*** The error message would be here ***
***                               ***
*****
*****
```

```
____TRANSCRIPT BEGINS ON THE NEXT LINE____
<-- 220 ts3.checktls.com CheckTLS TestSender Mon, 17 Aug 2015 14:14:03 -0400
--> EHLO smtp2.
<-- 250-ts3.checktls.com Hello smtp2. [redacted], pleased to meet you
<-- 250-ENHANCEDSTATUSCODES
<-- 250-8BITMIME
<-- 250-STARTTLS
<-- 250 HELP
--> STARTTLS
<-- 220 Ready to start TLS
====tls negotiation successful (cypher: AES256-SHA, client cert: Subject Name: undefined;Issuer Name: undefined;)
~~> EHLO smtp2.
<~~ 250-ts3.checktls.com Hello smtp2. [redacted], pleased to meet you
<~~ 250-ENHANCEDSTATUSCODES
<~~ 250-8BITMIME
<~~ 250 HELP
```

Antivirus Settings (OS)

•Domino Server Exclusions

- Transaction Logs
- Domino Data
- DAOS repository
- View Rebuild Dir folder

–See <https://www-304.ibm.com/support/docview.wss?uid=swg21417504>



•Notes Client Exclusions

- Notes\framework
 - Notes\data\workspace\.config\org.eclipse.osgi
 - JAR files
- See <http://www-01.ibm.com/support/docview.wss?uid=swg21407945>

Antivirus Settings (OS)

- **But Darren, what about when my users click on a virus infested email attachment?**

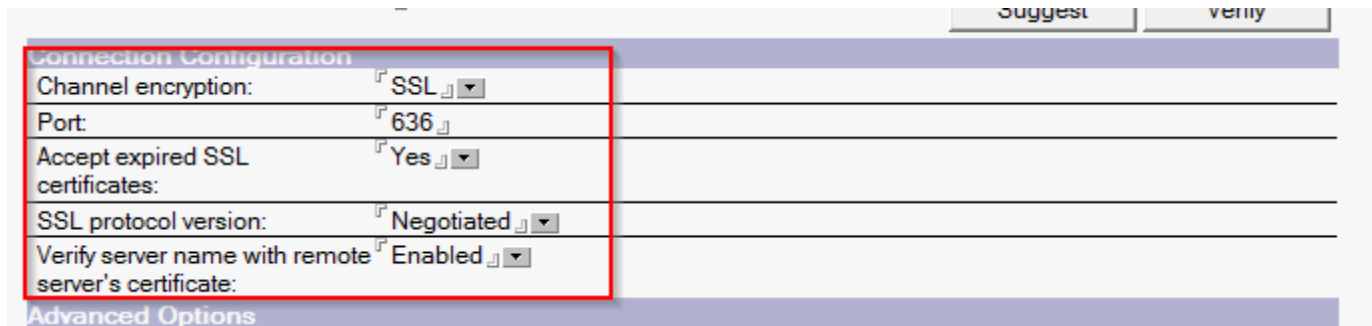
- **IBM Notes and Attachments**
 - All Notes attachments are saved to %TEMP% on Windows
 - So long as the OS AV has real time scanning of %TEMP% you are safe
 - Remember, %TEMP% could be different per user

Securing LDAP

- Using DA to AD for internet passwords?

–Also secure this otherwise your users AD passwords are going from Domino to AD in **plain text**

–Just checking the box in DA.NSF **is not** sufficient!!!!



The screenshot shows the 'Connection Configuration' dialog box in Domino. A red box highlights the following settings:

Channel encryption:	SSL
Port:	636
Accept expired SSL certificates:	Yes
SSL protocol version:	Negotiated
Verify server name with remote server's certificate:	Enabled

Below the highlighted section, the 'Advanced Options' section is partially visible.

–You also need to import your AD server SSL certificate in your server.id file

- See <http://blog.darrenduke.net/Darren/DDBZ.nsf/dx/solution-domino-directory-assistance-to-active-directory-when-using-ssl-does-not-break-with-9.0.1-fp4.htm> for details on how to do this (it's really not obvious)

Arriving in 9.0.1 FP7

- **Java**

- Java 8 support
- First to the server, then a few “weeks” later to the client



Arriving in 9.0.1 FP7

- **Notes NRPC Port Security**

- **AES support**

- It's currently 128 bit RC4

- Which you could find out in technote 1097816

- **BUT IBM DELETED IT**

- I would expect 128 bit AES, with maybe an option to enable 256 bit AES

Speaking of Fix Packs

- **As a general rule, the newer the FP and the newer the IF, the more secure your server or client will be**

- Fix Packs are cumulative. FP6 contains FP5 *and* some new stuff

- IBM are most likely changing the nomenclature around fix packs in the next few months

- I doubt this includes making them easier to find on PPA or FC though

- **Strongly consider going to 9.0.1 FP5/6**

- SHA2

- TLS 1.2/PFS/much higher quality ciphers

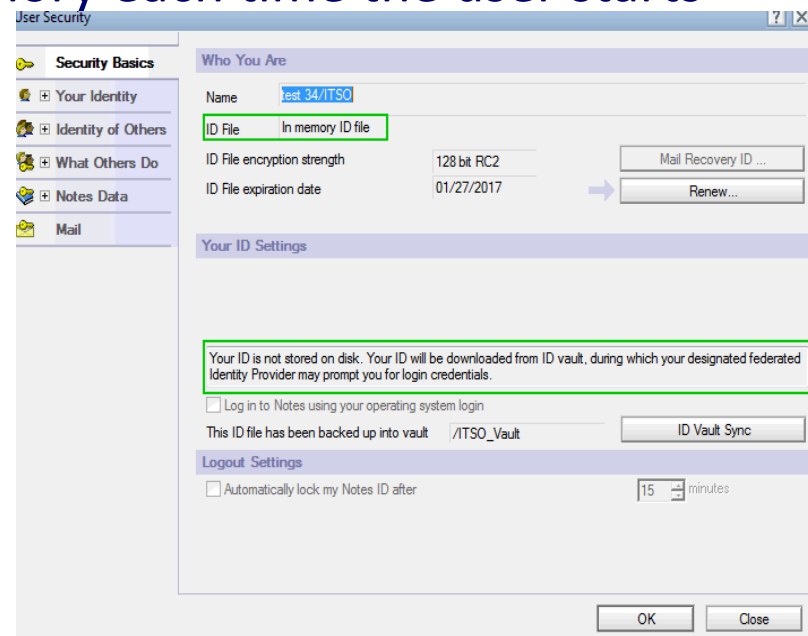
- You are most likely paying for it anyway

- News Flash!!!! No new security features are coming to 9.0 or 8.5.x

- **Fixpacks, IFs and Java updates are on IBM Fix Central**

SAML

- **Security Assertion Markup Language**
- **Allows Notes users to go password-less**
 - This can be a huge selling point
- **Can also be set up so that the Notes ID is never stored on the user's PC**
 - It gets downloaded and stored in memory each time the user starts Notes (well.....)
- **User NEVER has to enter password**
- **You need 9.0.1, ID Vault, patience**
- **No password = no post-it note with password written on it!**



Knowledge is Power

•Forewarned is forearmed and there are resources that allow you to be pro-active

•IBM My Notifications

- Sign up to receive emails from IBM on new product releases, fix packs, etc

- See <http://blog.darrenduke.net/Darren/DDBZ.nsf/dx/do-you-subscribe-to-the-ibm-daily-product-update-newsletter-you-should.htm> for details on setting

Dear Subscriber (),

Here are your bulletin e-mail notifications for your subscriptions at IBM My notifications.

Lotus Domino: Flashes

- [Domino data can be deleted during server shutdown if the temp directory points to the Domino data directory](#)

On a Domino 8.5.1 or later server, the contents of the Domino data directory can be deleted during shutdown if the following two conditions are true: 1) The temp directory points to the Domino data directory 2) The ~notetmp.reg file contains a null string This does not happen frequently or on all Domino servers. However, if this does happen, a backup restore of the data will be necessary. This is known to happen on UNIX (AIX, Linux, Solaris) and IBM i (i5/OS) platforms. It is suspected this co...

Manage your My notifications subscriptions, or send questions and comments.

Knowledge is Power

•Forewarned is forearmed and there are resources that allow you to be pro-active

–US CERT weekly email

- Be afraid, be very afraid (especially of Flash, Acrobat, AIR and Java)
- See <https://www.us-cert.gov/> to sign up

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.	2015-08-13	10.0	CVE-2015-5125 CONFIRM
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5130, CVE-2015-5134. CVE-2015-5539. CVE-2015-5540. CVE-	2015-08-13	10.0	CVE-2015-5127 CONFIRM

Disable Things

- Anything you don't use, disable. Anything you don't need, disable
- Need POP3 or IMAP? No?
 - Not having it in the Notes.ini will not start those tasks....BUT...
 - They can still be started
 - load pop3
- This is not sufficient, disable it in the Domino Directory
 - Now load pop3 won't actually load anything

SSL ciphers: RC4 encryption with 128-bit key and MD5 MAC
RC4 encryption with 128-bit key and SHA-1 MAC

Enable SSL V2: Yes
(SSL V3 is always enabled)

Web | Directory | **Mail** | DIIOP | Remote Debug Manager | Server Controller

	Mail (IMAP)	Mail (POP)
TCP/IP port number:	<input type="text" value="143"/>	<input type="text" value="110"/>
TCP/IP port status:	<input type="text" value="Disabled"/>	<input type="text" value="Disabled"/>
Enforce server access settings:	<input type="text" value="Yes"/>	<input type="text" value="Yes"/>
Authentication options:		
Name & password:	No	No
Anonymous:	N/A	N/A

Notes/Domino Port Encryption

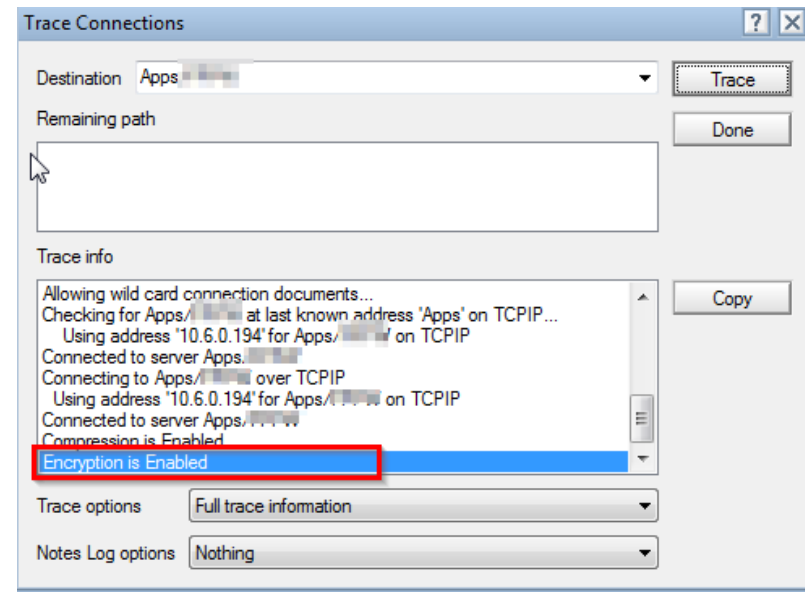
- **For Domino server to server or Notes client to server communication**

- Turn on at one end, works at both
- 128 bit RC4 encryption
 - 128 bit AES will ~~may~~ surface in 9.0.2 9.0.1 FP7

– WAN accelerators don't link this

– Still, provides more than adequate channel encryption for almost organization

– Test via a trace in the Notes Client or the Server console



The END

- It's security so there are no stupid questions, just compromised servers
- Q&A time

- @DarrenDuke on Twitter
- <https://blog.darrenduke.net>
- info@simplified-tech.com to hire me. Which you should. I'm hillerious