

OPENNTF WEBINARS

Domino Security - not knowing is not an option

OpenNTF Webinar, March 2024

Darren Duke

Janitor Level 34

STS



Thanks to....

- **OpenNTF**

- Bruce and Nathan, all those years ago
- All the past and present board members, all the contributors, and the users, lurkers, posters
- Roberto and Kim for inviting me present

- **HCL**

- For giving Notes/Domino the development backing so sorely lacking in the latter years of IBM
- For the most part, I have nothing but great things to say about what HCL development has done since the acquisition

- **Lisa**

- She's now a published author (and didn't even force me to add this!)



About me

- AKA my favorite slide
- Started with “Lotus Notes” in R3
- Yes, really....R3
- That means 1996
- Yes, really....1996
- Yes, I do still think I look like this picture →
- No, I don't. But I still think I do
- Co-founder of STS in 2005
- Sometime blogger, ranting ex-Tweeter (or now ex-Xer?), ex-co-host of This Week In Lotus, Speaker
- <http://blog.darrenduke.net>
- Twitter/X [@darrenduke](https://twitter.com/darrenduke) (for utter silence these days)



10,000 feet view

- What we'll (hopefully) cover (in no particular order...sorry about that)
 - Server Security
 - User Security
 - Web



SERVER SECURITY



All security starts with Backup and Restore

- **Native VSS Support in Windows**

- Added in 12.0.2
- If your backup solution supports VSS, it now supports Domino on Windows
- See <https://blog.darrenduke.net/darren/ddbz.nsf/dx/domino-12.0.2-adds-vss-backup-support.htm>
- Also supports Veeam restores (a tad complicated though)

- **Native Backup and Restore in Domino!!!!**

- Supports to-file-system, Veeam and S3 repositories as is
- Added as server tasks, cross platform support
- Opensource
- See <https://opensource.hcltechsw.com/domino-backup/>
- Intended as “middleware”




Security is also patching and updating

- **9.0.x and 10.x go end of support, June 1st, 2024**
 - If you are running those versions, you will be insecure on June 2nd
 - Well, maybe not on June 2nd, but at some point you will be
 - Also Xwork EOS
 - Also LEI 9.0.x EOS
- 3 months from the date of this webinar
- 11.x and higher have no EOS date at time of writing
- See <https://www.hcl-software.com/resources/product-release/product-lifecycle-table?productFamily=domino>



Speaking of patching - Fix Packs



- **As a general rule, the higher the Domino version number, the more secure your server or client will be**
 - And Traveler, and Nomad, and Leap....and...and
- **Further to this rule, the higher the FP and the higher the IF, the more secure your server or client will be**
- **There is a new download site**
 - I mean, who knew we'd all think FixCentral was actually not that bad?
 - Well, FlexNet made us long for FixCentral.
 - FlexNet
 - Truly. Abysmally. Awful. Beyond words
 - If you have a favorite deity, give it thanks, because...
 - New download site is <https://my.hcltechsw.com/downloads>



Software Downloads

HCL Connections HCL Digital Experience HCL Domino HCL Link

Recently Released

Product	Release	Description
 Domino Leap	1.1.4	Release 1.1.4
 Traveler for Microsoft Outlook	3.0.9	Release 3.0.9

Server Security SSL/TLS/SHA2

- **SSLv3 is dead (SSLv2 has been dead for a long time)**

- Unless you need it for some ancient SMTP STARTTLS compatibility
- SSLv3 disabled by default since 9.0.1 FP9

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

- TLS 1.2 is now the default
 - TLS 1.0 disabled by default in 12.0+, Domino never had TLS 1.1 support
- Still no TLS 1.3 support in Domino
 - So sad, sad face goes here
 - <https://domino-ideas.hcltechsw.com/ideas/DOMINO-I-124>
- Here's to hoping HCL don't make the same mistake as IBM did with Poodle
 - They waited and waited on adding TLS support to Domino....then one day this happened:



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 supports FPS since 9.0.1 FP3 IF2/3

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



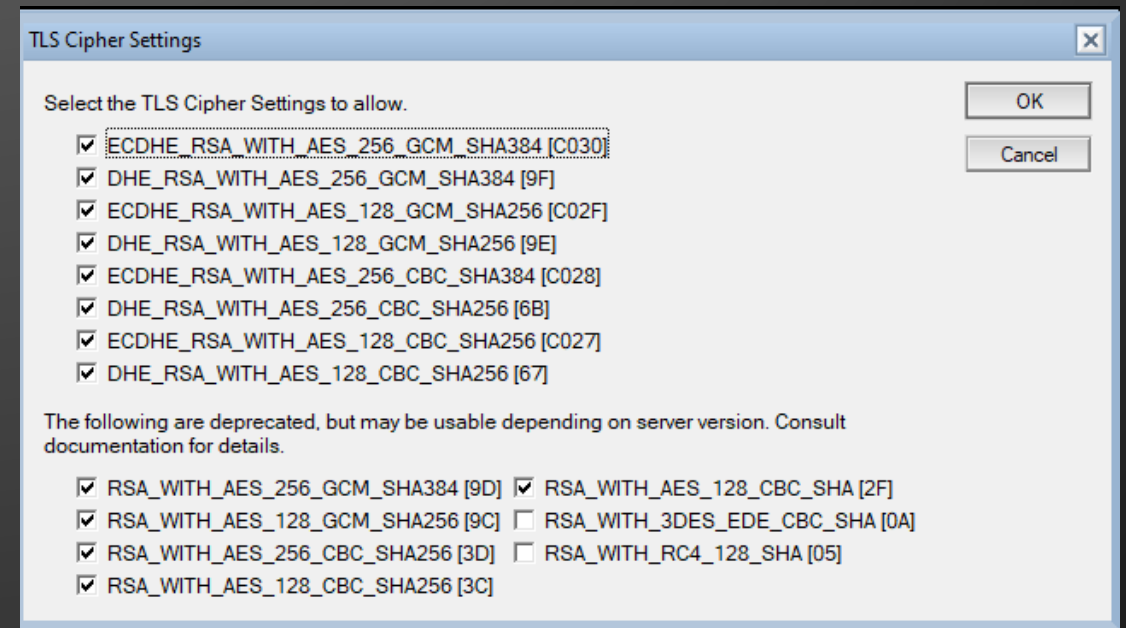
Server Security SSL/TLS/SHA2

•SMTP with STARTTLS

- Rarely needed these days, but some problems fixed with....
- Server notes.ini SSL_ENABLE_INSECURE_SSLV2_HELLO=1

•Ciphers

- Domino server now dictates the preferred cipher list
- No need to override with SSLCipherSpec notes.ini unless you really need to
- Updated frequently, but you still must manually disable deprecated ones
- Especially after server and/or NAB upgrade:



Speaking of STARTTLS and email....



- Your SMTP task should always be using STARTTLS
 - STARTTLS is encryption *only*
 - There is no in-built mechanism to verify the authenticity of the TLS certificate
 - Any TLS certificate is trusted when using STARTTLS
 - Even self signed
 - Inbound and outbound configured in different places!

Configuration Settings: hosted/STS

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Set

Basics | Restrictions and Controls... | Message Disclaimers | Message Tra

Journaling | Commands and Extensions | Controls

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

Controller

Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
110	25	25
Disabled	Enabled	Negotiated TLS
Yes	Yes	N/A
995	465	465
Disabled	Enabled	Disabled

Email continued....DKIM

- **DomainKeys Identified Mail (DKIM)**

- Tell the recipient server that the sender is cryptographically verified
 - Uses DNS and PKI
- Outbound support added in 12.0.1
- Inbound support added in 12.0.2
- DKIM, DMARC and SPF provide the basis of modern SMTP sender verification
 - Still not a perfect solution, but that's not Domino's fault
- Domino doesn't support DMARC (yet?), so it can't provide full protection for DKIM alignment rules.
 - Pile on to get it added:
<https://domino-ideas.hcltechsw.com/ideas/IDEAMLCT-I-6>



Let's Encrypt (LE) and CertMgr

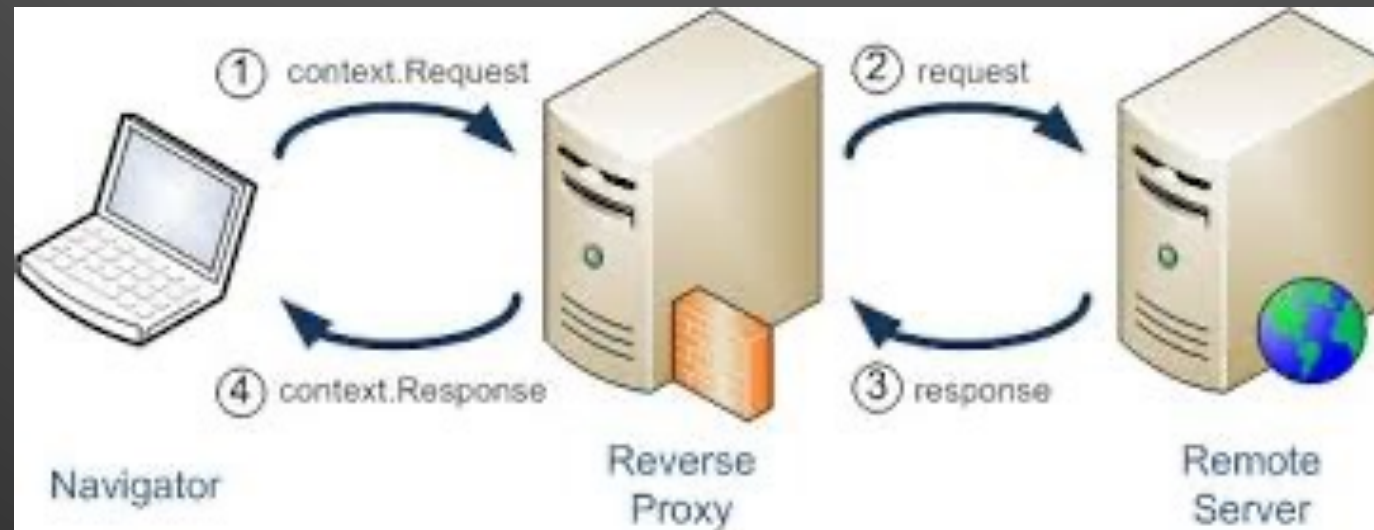


- **Added into Domino natively in 12.0**
- **LE does require port 80 open**
 - May fail security audits
- **New task and NSF added in 12, certmgr**
 - Certmgr stands for....never mind, you found this webinar, you're smarter than most
 - Automate requesting and renewing from certain trusted Internet CA's
 - Very good if you are using one of the supported vendors.
 - Even without a supported CA, it is easier than kyrtool.exe
 - But 20 years to life in prison is easier than kyrtool.exe
- **For versions prior to 12 there is LE4D from Midpoints**
 - <https://www.midpoints.de/de-solutions-LE4D>
- **You can still use kyrtool, and Gab Davis still has the most useful post for this**
 - <https://turtleblog.info/2015/06/22/creating-sha-2-4096-ssl-certificates-for-domino/>

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
- Can use self-signed/internal CA certs on inside

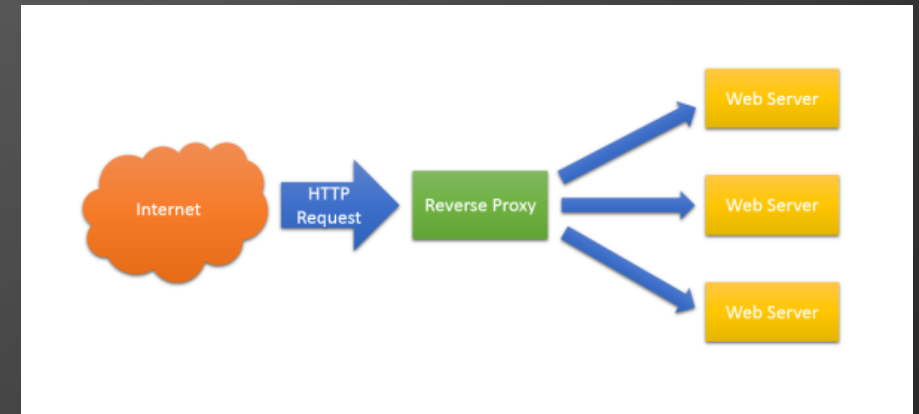
•Security

- Hide version/platform/application from the browser
- No direct access to backend servers
- Restrict URL access to Domino for only required URLs for

- iNotes/Verse/Nomad
- Traveler
- Domino web applications

•Load balancing

- Provide HA for iNotes, Traveler, etc



Reverse Proxies

- The Real Reason to use a Proxy

	Date Spec Released	Date Domino Added	Time taken by IBM/HCL
TLS 1.0	1999	2014	15
TLS 1.2	2008	2015	7
PFS	2011	2015	4
TLS 1.3	2018	Not - as of Mar 2024	6 and counting

- With a Proxy you may in the future avoid something like this:



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
- SafeLinx by HCL (nee LMC/IMC)
 - Used to be required for Nomad Web
 - Pretty complicated TBH



Reverse Proxies

•The Proxies

- Anything else really, but usually big dollar:
 - BigIP F5
 - Citrix NetScaler
- IBM HTTP Server
 - Keep away
 - No longer part of Domino install any more



BROWSER SECURITY



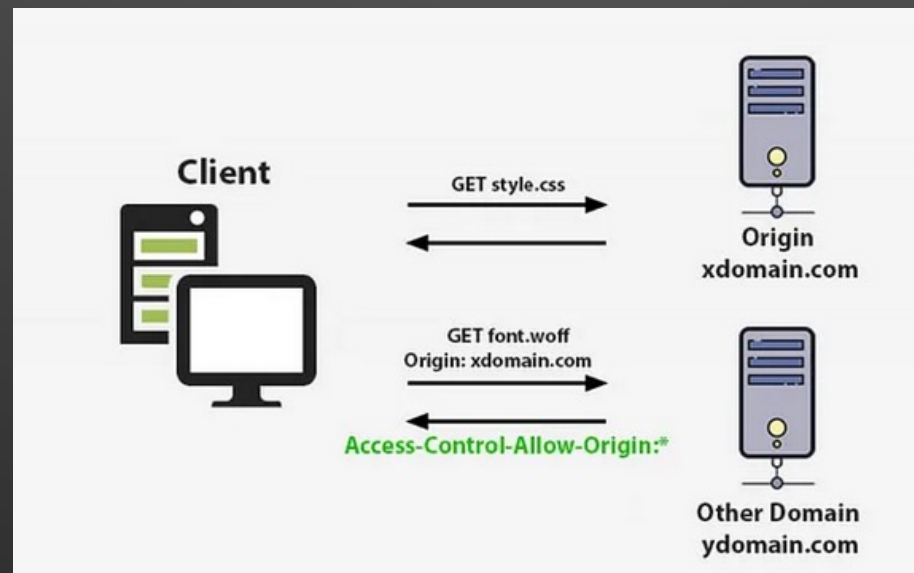
CORS – Cross Origin Resource Sharing

- **The web is a dangerous place**

- Browsers add security to protect the user
- Official CORS support in Domino added in 10.0.1 FP2
 - https://help.hcltechsw.com/domino/10.0.1/admin/conf_cors.html

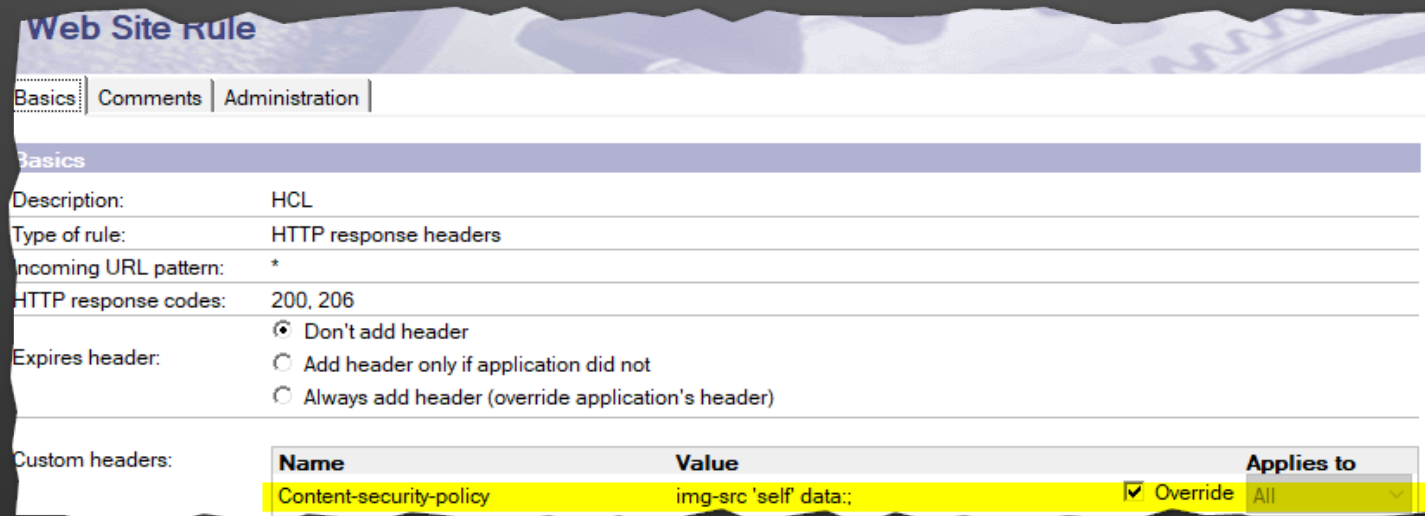
- One of the easiest-to-digest examples

- <https://medium.com/@manrvaldez.92/what-is-cors-2330158ef227>
- <https://lo-victoria.com/introduction-to-cross-origin-resource-sharing-cors>



CSP – Content Security Policies

- **Allows servers (via admins) to mitigate an array of attacks**
 - Mainly XSS, but also packet sniffing
- **Web Rules in Domino allow CSP headers to be added**
- **Browser side security, most have**
 - Can verify here: <https://content-security-policy.com/browser-test/>



The screenshot shows the 'Web Site Rule' configuration page in Domino. The 'Basics' tab is selected. The configuration includes:

- Description:** HCL
- Type of rule:** HTTP response headers
- Incoming URL pattern:** *
- HTTP response codes:** 200, 206
- Expires header:** ☒ Don't add header, ☐ Add header only if application did not, ☐ Always add header (override application's header)
- Custom headers:** A table with one entry: 'Content-security-policy' with value 'img-src 'self' data:;' and 'Applies to' set to 'All'.

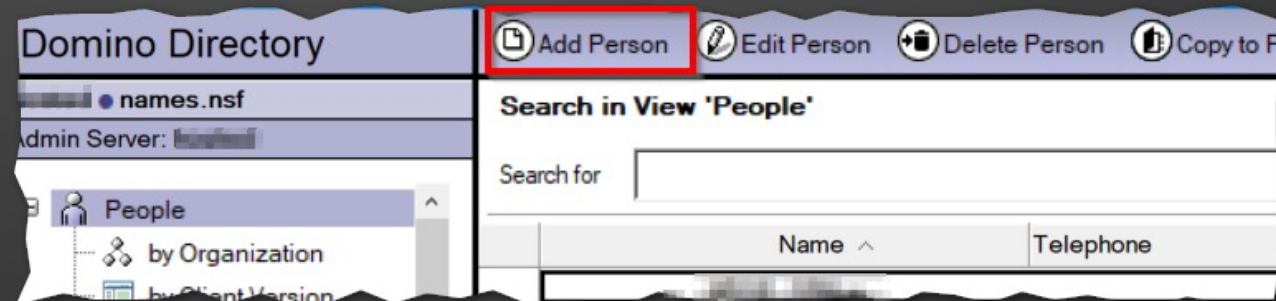
Name	Value	Applies to
Content-security-policy	img-src 'self' data:;	<input checked="" type="checkbox"/> Override All

USER SECURITY



User Security

- There is a current security bulletin with certain internet passwords < 14.0
 - Details here
https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107585
- CVSS v3.1 score of 5.2 (so “medium”)
- If you are using “Add Person” (as opposed to “registering a user”) for server versions earlier than 14.0
 - New NAB templates
 - Update existing person docs
 - Protect new person docs

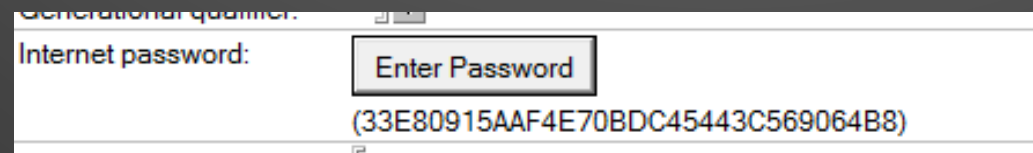


User Security

•Strong Internet Passwords

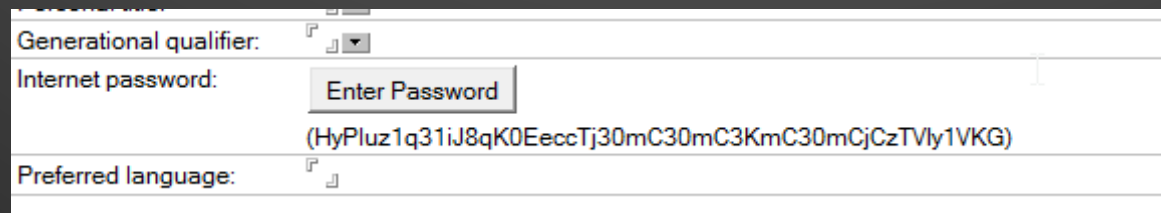
- Changes how passwords are stored in the Domino Directory
 - A salted hash is created for each user
 - @Password has starts a hex digit ('0' - '9', 'A'-'F'), with Domino 4.5
 - @Password2 hash starts with 'G', with Domino 4.6+
 - @Password3 hash starts with 'H', with Domino 8.5.1+
 - Obviously if you want 'G' or preferably 'H'

•Go from this



Generational qualifier: [dropdown]
Internet password: [Enter Password]
(33E80915AAF4E70BDC45443C569064B8)

•To this

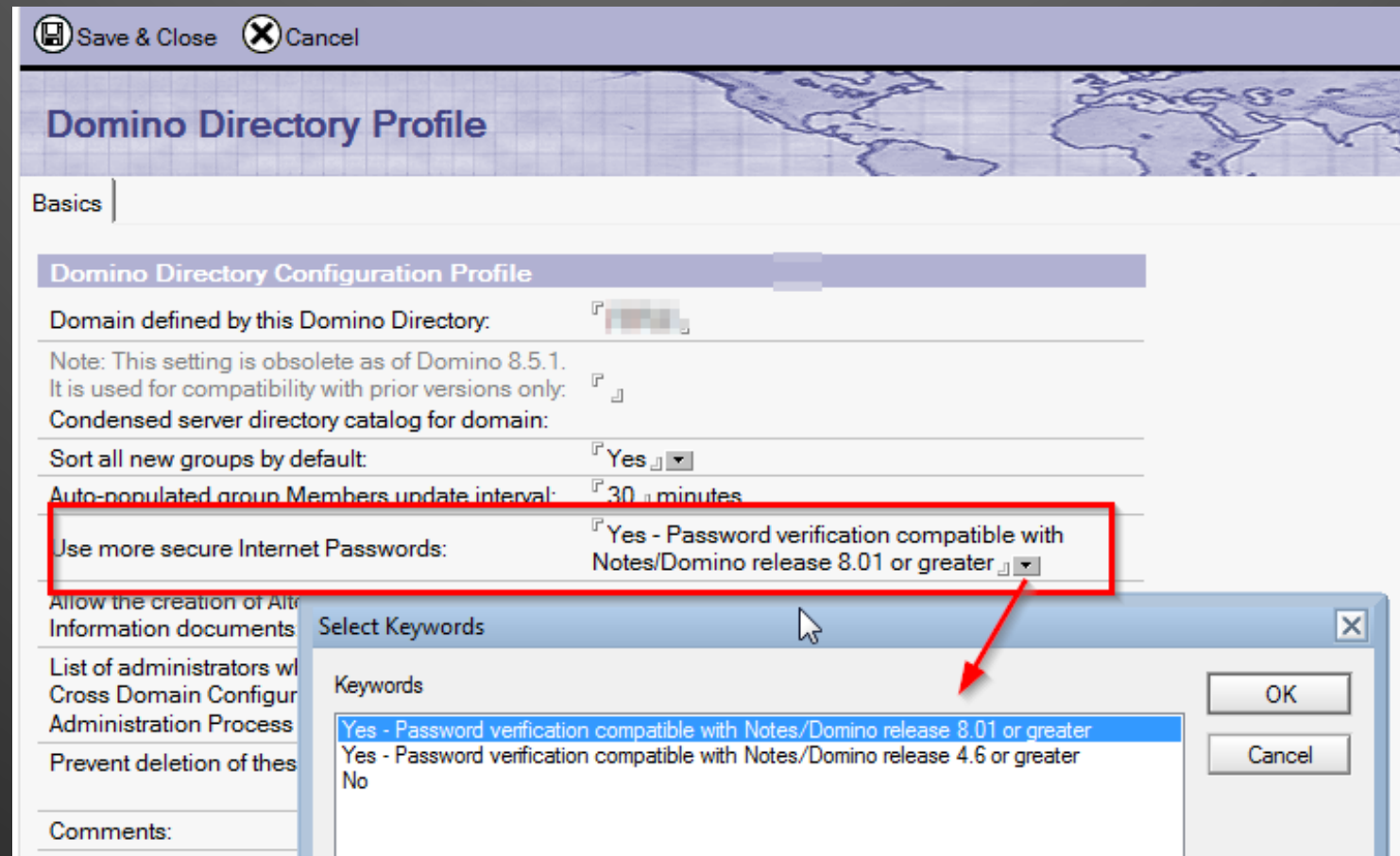


Generational qualifier: [dropdown]
Internet password: [Enter Password]
(HyPluz1q31iJ8qK0EeccTj30mC30mC3KmC30mCjCzTVly1VKG)
Preferred language: [dropdown]



User Security

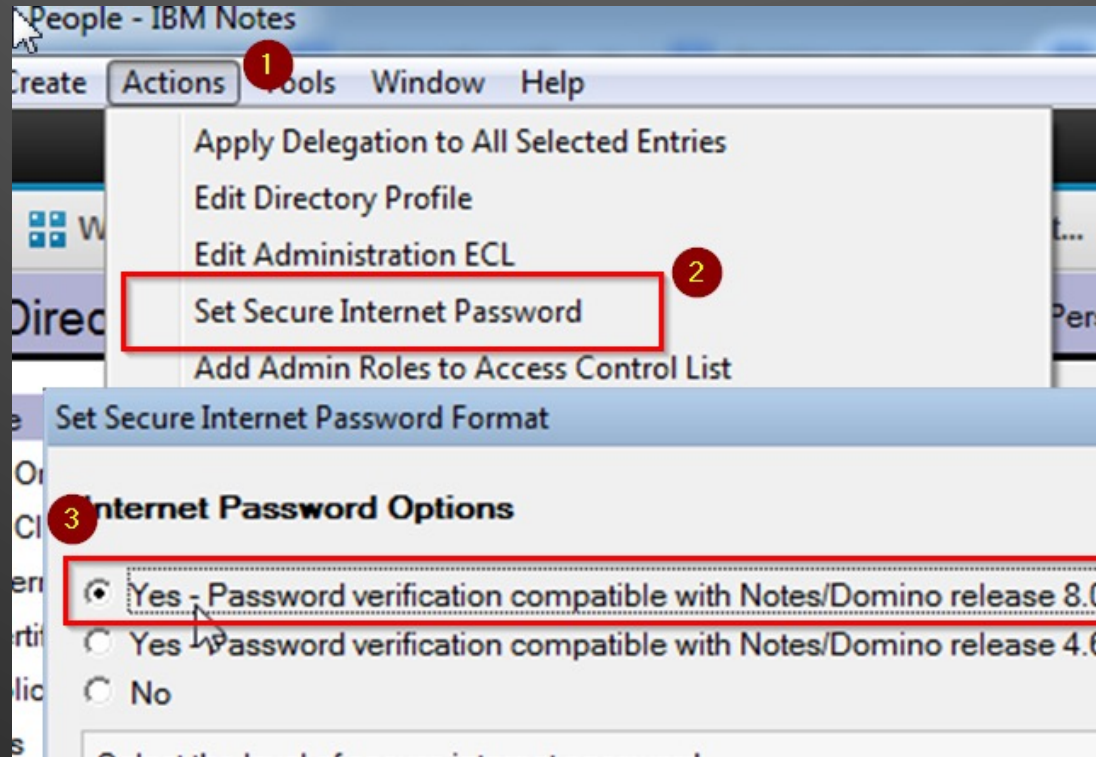
- Strong Internet Passwords for new users
- Edit Domino Directory Profile



User Security

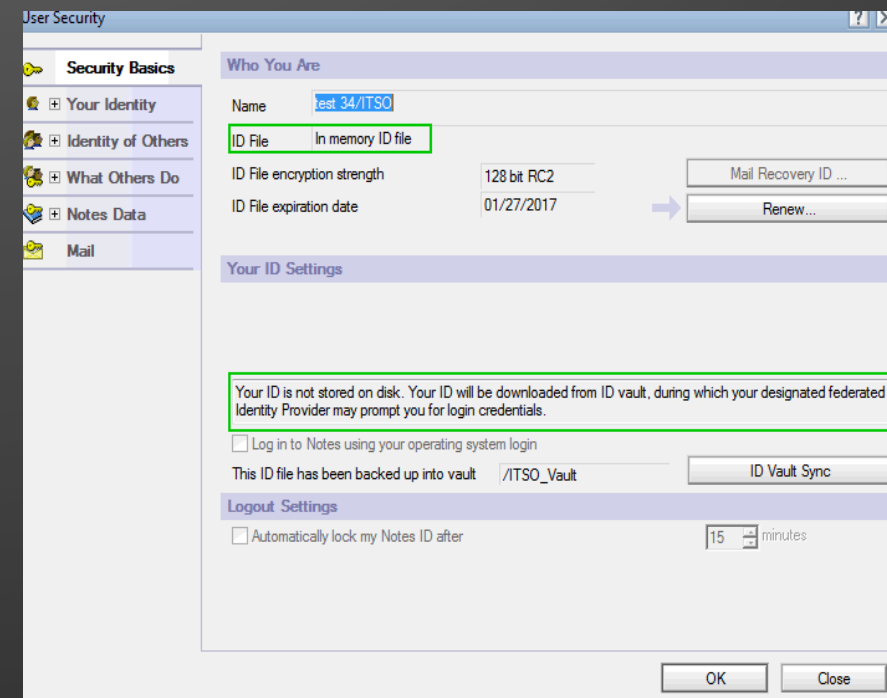
- **Strong Internet Passwords for existing users**

- Select the users in the Domino Directory then Actions\Set Secure Internet Password
- Then the top (8.0.1) option (but I think it started working in 8.5.1)



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
- **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!**



MFA for HTTP

•Two options:

•Native

- Added in 12.0
- TOTP, no push
- Per internet site setting
- Also works in Verse Mobile (and maybe Nomad too now...maybe?)
- Much easier than SAML
- There are some improvements HCL could add to make this much, much more useful
 - See the M365 implementation for ideas

•SAML

- You can control the MFA provider
- As stated previously, complicated



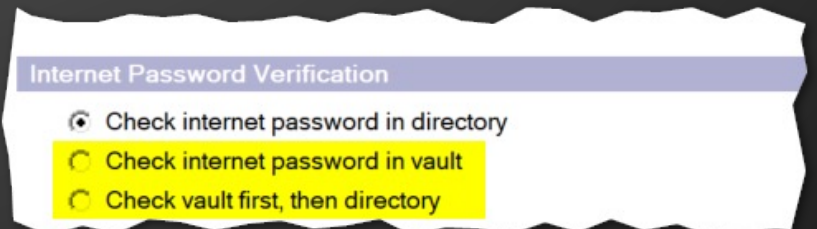
Internet Passwords – You have choices now

•Old way – two passwords:

- Notes ID password
- Internet Password stored in person document
- Two to manage
- Complicated
 - For admins, PITA
 - Users get aneurisms, two passwords manage
 - Lots of cludgy workarounds attempted to fix this

•New way – Shared Internet Password

- New in 11.0
- Allow Domino to use the Vaulted ID password
 - That's right, the password on the ID in ID Vault can now be the users' Internet Password
- One password to rule them all
- Much more simplified password management
 - Change in one, change in the other

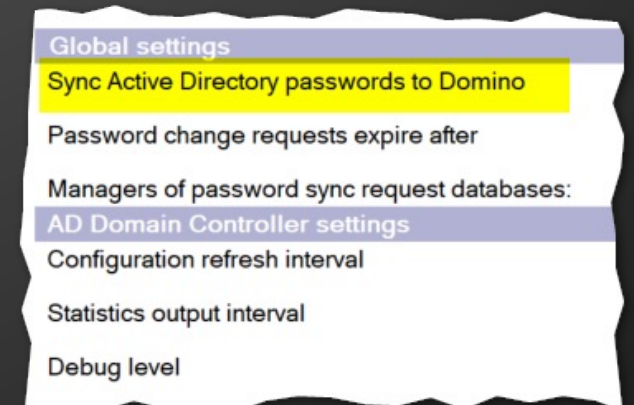


Internet Passwords – You have choices now

- But there's more.....

- ActiveDirectory Password Sync**

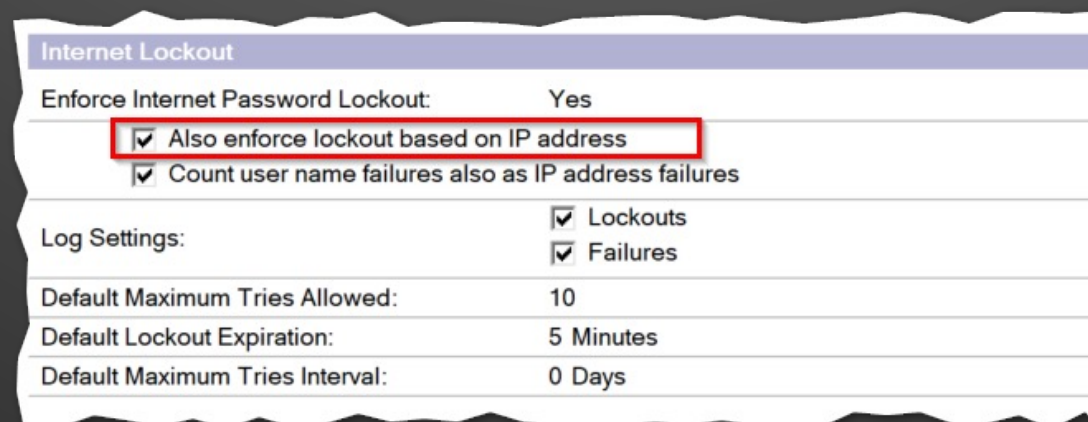
- Yes, I will repeat this.....ActiveDirectory Password Sync
- The pot of gold at the end of the rainbow actually exists now
- New in 12.0
- Will provide a 1-way-sync of AD User password changes into ID Vault
 - And with Shared Internet Password, that could also mean HTTP passwords are now your AD password
- Does required a Domino sever (non-running) to be installed on every writeable AD controller



Internet Passwords – Prevent the Brute Force Attacks

•Internet lockouts

- Extended in 12.0
- Now able to block based on IP address
 - This is how hackers really work
 - They sit on an IP and spray user name and password combos at your server
 - Pre 12.0 all you could block was the same user name being used
 - Now you can block the IP doing the attack
- Turn this on if you are \geq 12.0 servers!



The screenshot shows the 'Internet Lockout' configuration window. The 'Enforce Internet Password Lockout' option is set to 'Yes'. A red rectangular box highlights the checkbox for 'Also enforce lockout based on IP address', which is checked. Below it, the checkbox for 'Count user name failures also as IP address failures' is also checked. Under the 'Log Settings' section, both 'Lockouts' and 'Failures' are checked. The 'Default Maximum Tries Allowed' is set to 10, 'Default Lockout Expiration' is 5 Minutes, and 'Default Maximum Tries Interval' is 0 Days.

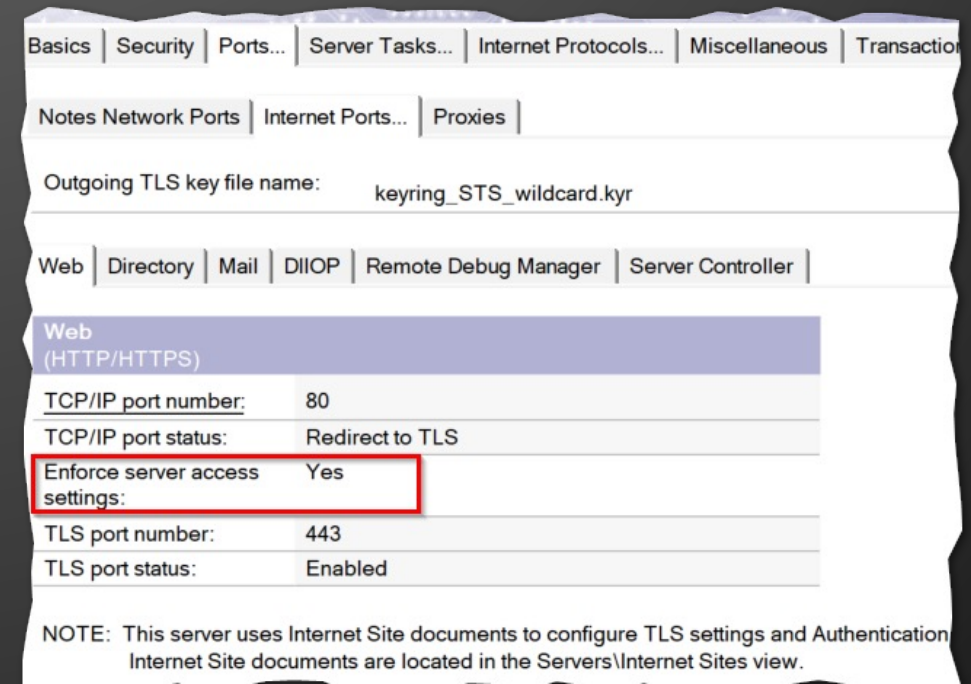
Internet Lockout	
Enforce Internet Password Lockout:	Yes
<input checked="" type="checkbox"/> Also enforce lockout based on IP address	
<input checked="" type="checkbox"/> Count user name failures also as IP address failures	
Log Settings:	<input checked="" type="checkbox"/> Lockouts <input checked="" type="checkbox"/> Failures
Default Maximum Tries Allowed:	10
Default Lockout Expiration:	5 Minutes
Default Maximum Tries Interval:	0 Days



Internet Passwords – NOT BLOCKED BY DENY ACCESS

- **By default, Deny Access ONLY works for Notes client traffic**

- Yeah, I know, weird right? Strange decision.
- You have to specifically choose to enforce deny access on other protocols (HTTP, LDAP, etc.)
 - Per server as well....grrrrr
- If not, you may deny a user access to Notes and email via a client, but that can still log into iNotes or Verse and send snoty emails about the management
- By default all protocols are set to “No”
- DLAU also highlights this now



Basics | Security | Ports... | Server Tasks... | Internet Protocols... | Miscellaneous | Transaction

Notes Network Ports | Internet Ports... | Proxies

Outgoing TLS key file name: keyring_STS_wildcard.kyr

Web | Directory | Mail | DIOP | Remote Debug Manager | Server Controller

Web (HTTP/HTTPS)

TCP/IP port number:	80
TCP/IP port status:	Redirect to TLS
Enforce server access settings:	Yes
TLS port number:	443
TLS port status:	Enabled

NOTE: This server uses Internet Site documents to configure TLS settings and Authentication. Internet Site documents are located in the Servers\Internet Sites view.

OTHER SECURITY



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 manually
 - 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

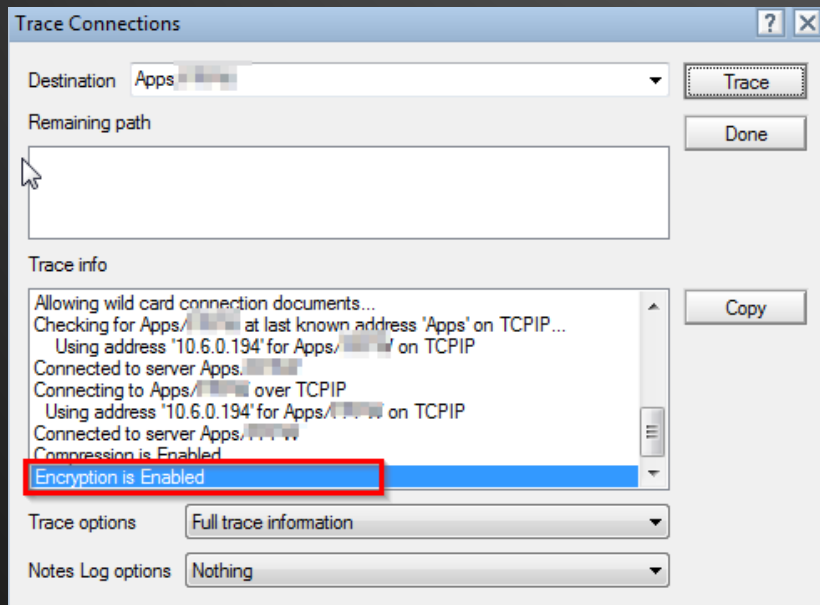
Enable SSL V2: ☐ Yes
(SSL V3 is always enabled)

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

	Mail (IMAP)	Mail (POP)
TCP/IP port number:	143	110
TCP/IP port status:	Disabled	Disabled
Enforce server access settings:	Yes	Yes
Authentication options:		
Name & password:	No	No
Anonymous:	N/A	N/A

Enable Things - Notes/Domino Port Encryption

- **For Domino server to server or Notes client to server communication**
 - Turn on at one end, works at both
 - AES and PFS are available, set in ini file on server or pushed do to client via policy
 - See https://help.hcltechsw.com/domino/11.0.1/admin/conf_port_encryption_t.html
 - WAN accelerators don't link this (or port compression)
 - Test via a trace in the Notes Client or the Server console (debug ini settings help)
 - See <https://blog.darrenduke.net/darren/ddbz.nsf/dx/9.0.1-fp7-and-how-to-enable-the-new-port-encryption-settings.htm>



```
ocation information using policy
[0C28:0002-0A18] 09/14/2016 04:34:02.96 AM DynConfig> Found $DPLocked field: $DP
Locked on policy note. Copying to location doc
[0C28:0002-0A18] 09/14/2016 04:34:02.97 AM DynConfig> Found $DPLocked field: $DP
LockedUnstripped on policy note. Copying to location doc
[0C28:0002-0A18] 09/14/2016 04:34:02 AM Dynamic Client Configuration shutdown
[253C:0006-2570:wrepl] Authenticate <1DB0002A>: CN=hosted/O=STS
[253C:0006-2570:wrepl] T: AES:128 E:1 P:c:e S: AES-GCM:256 A:2:1 L:N
:N:N FS: DHE-2048
[253C:0006-2570:wrepl] Authenticate <1DB0002B>: CN=hosted/O=STS
[253C:0006-2570:wrepl] T: AES:128 E:1 P:c:e S: AES-GCM:256 A:2:1 L:N
:N:N FS: DHE-2048
[20F0:0002-02FC] Authenticate <1DB0002D>: CN=hosted/O=STS
[20F0:0002-02FC] T: AES:128 E:1 P:c:e S: AES-GCM:256 A:2:1 L:N:N:N F
S: DHE-2048
[20F0:0002-02FC] Authenticate <1DB0002E>: CN=hosted/O=STS
[20F0:0002-02FC] T: AES:128 E:1 P:c:e S: AES-GCM:256 A:2:1 L:N:N:N F
S: DHE-2048
```


NOT SECURITY (?)



Antivirus Settings (OS)

•Domino Server Exclusions

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



•Notes Client Exclusions

- Notes\framework
- Notes\data\workspace\.config\org.eclipse.osgi
- JAR files

•See https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0093046



Antivirus Settings (OS)

- But Darren, what about when my users click on a virus infested email attachment?
- **HCL 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 covered
 - Remember, %TEMP% could be different per user



MISC. SECURITY



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)

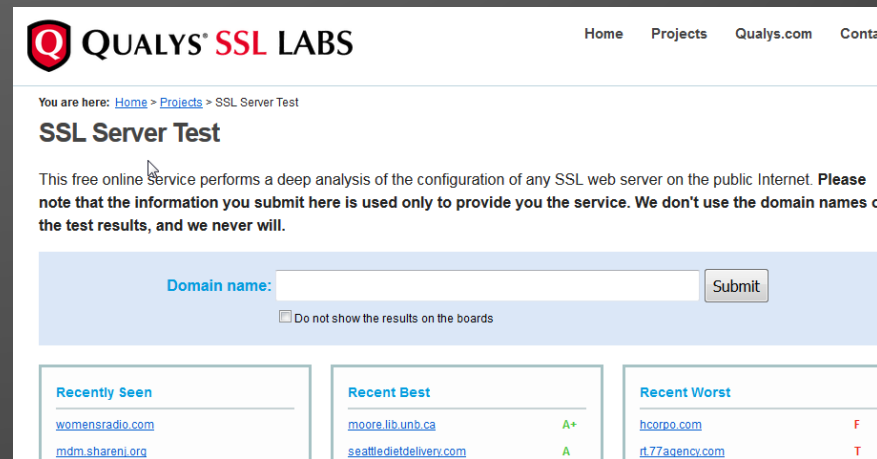
- See <https://www.us-cert.gov/> to sign up

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

Testing

- So you **think** you're secure? OK.....
- Testing is what elevates belief to evidence
- QualSYS 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.



The image shows the Qualys SSL Labs SSL Server Test interface. At the top, the Qualys SSL Labs logo is visible, along with navigation links for Home, Projects, Qualys.com, and Contact. Below the logo, the breadcrumb trail reads "You are here: Home > Projects > SSL Server Test". The main heading is "SSL Server Test". A paragraph of text explains that this is a free online service for analyzing SSL web server configurations on the public Internet, with a note that submitted information is used only for the service and not for domain names or test results. Below this text is a form with a "Domain name:" label, a text input field, and a "Submit" button. A checkbox labeled "Do not show the results on the boards" is also present. At the bottom, there are three columns of results: "Recently Seen", "Recent Best", and "Recent Worst".

Recently Seen	Recent Best	Recent Worst
womensradio.com	moore.lib.unb.ca A+	hcorpo.com F
mdm.sharenj.org	seattledietdelivery.com A	rt77agency.com T



Testing

- Here is my Domino Blog server behind an Apache Reverse Proxy

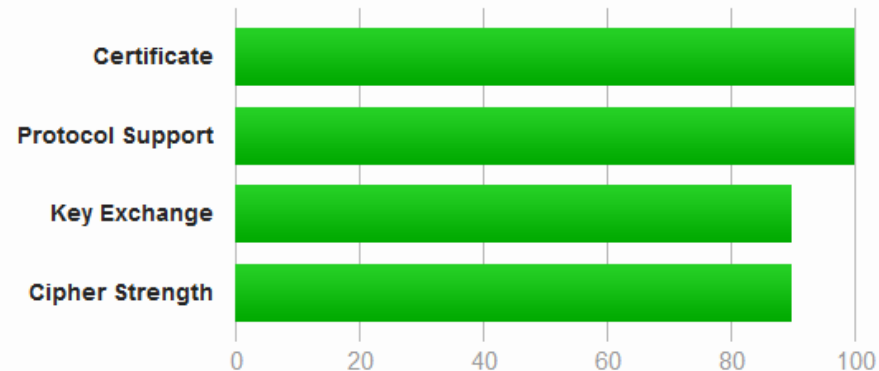
SSL Report: blog.darrenduke.net (199.103.7.9)

Assessed on: Thu, 21 Mar 2024 08:51:34 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

- Test SMTP STARTTLS at CheckTLS.com
 - <https://www.checktls.com/testreceiver.html>
 - Test both send and receive
- Receive example:

```
Trying TLS on simplified-tech-com.pl0.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
          250-8BITIME
          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.pl0.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 transaction

```
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., 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., pleased to meet you
<~~ 250-ENHANCEDSTATUSCODES
<~~ 250-8BITMIME
<~~ 250 HELP
```



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!!!!

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

Advanced Options

- 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)



Securing LDAP

- I see a shocking amount of Domino LDAP servers NOT using LDAPS
 - LDAPS is over port 636 by default
 - Provided Domino has been set up for SSL, enable LDAPS
 - If your LDAP clients supports LDAPS USE IT!

Web	Directory	Mail	DIIOIP	Remote Debug Manager	Server Controller
Directory (LDAP)					
TCP/IP port number:		389			
TCP/IP port status:		Enabled			
Enforce server access settings:		Yes			
Authentication options:					
Name & password:		Yes			
Anonymous:		No			
SSL port number:		636			
SSL port status:		Enabled			
Authentication options:					
Client certificate:		No			
Name & password:		Yes			
Anonymous:		No			



Securing LDAP

•Potential LDAPS issues

- Your LDAP client (copier, spam gateway, etc) may not support newer ciphers
 - DEBUG_SSL_ALL=3 is your friend when testing this
 - Usually, a firmware update will address this
 - Usually
 - Or a new copier ;)
 - Also enabling deprecated ciphers in Domino can help
 - Debug first to ensure you need too

