

OPENNTF WEBINARS

September 21, 2023 OpenNTF Webinar

Domino SSL Implementation and Renewal, A Survivor's Guide



AGENDA

- Welcome
- Presentation
Avery Shaffer
- Q and A



THANKS TO THE OPENNTF SPONSORS

- HCL made a contribution to help our organization
 - Funds these webinars!
 - Events, Community interaction on Discord
 - Running the organization
- Prominic donates all IT related services
 - Cloud Hosting for OpenNTF
 - Infrastructure management for HCL Domino Servers
 - System Administration for day-to-day operation



COMMUNITY – WE ARE ALL OPENNTF

- Participate – we all learn from each other
- We are all volunteers
- No effort is too small
- If your idea is bigger than you can do on your own, we can connect you to a team to work on it
- Test or help or modify an existing project
- Write guides or documentation
- Add reviews on projects / stars on Snippets



AUTUMN 2023 COMMUNITY EVENT

- Blogathon!
 - Dust off your Blog, or create a new one, or a video, or a wiki
 - OpenNTF can host your post if you don't have a Blog
 - Share what you know with the Community
 - You never know what might happen
 - All blog posts will be featured on the OpenNTF Discord server (#blogathon) and in Collaboration Today
 - Get an OpenNTF Badge!
 - Helps with consideration as an HCL Ambassador



JOIN US ON DISCORD



UPCOMING EVENTS

- OpenNTF Repair Café
 - Admin topics
 - Next week! Thursday, Sep 28 @ 11:00AM EDT / 5:00PM CEST
- Dev and Admin topics each month



NEXT WEBINAR

October: HCL Domino Leap with Marty Lechleider

November: Sametime v12 with Erick Schwalb & Herwig Schauer

December: Annual Holiday Community Celebration



Domino SSL Implementation and renewal, A Survivor's Guide

Presentation by Avery Shaffer

- Senior Systems Administrator at Prominic.NET and primary certificate handler
- Domino Administrator since 2012
- Local fire performer of Champaign/Urbana



Why Are SSLs Such A Pain Now?



Why?

- Higher security with frequently changing certificates
- Newly released security features are updated faster (i.e SHA1 to SHA2)
- Exposed or compromised key chains removed quicker
- The “correct” theory that if we keep changing the certificates, the site can't be hacked

Who?

- In 2015 the CA/Browser Forum voted to reduce certificate validity from 5 years to 3 years.
- In 2019 they voted again to reduce certificate validity to 1 year but the vote failed.
- Apple decided independently to only allow 1 year SSL validation for Safari browsers, everyone following suite.

Future Change

- Google is pushing for maximum 90 day SSL key expiration by the end of 2024



- Uniformity is important as the entry is in several critical places
- Internet Site Documents, Internet Ports, SMTP, LDAP, IMAP ect
- Yearly .kyr name change can cause outages if an entry is missed

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

Notes Network Ports | Internet Ports... | Proxies

TLS settings

TLS key file name: keyfile.kyr

Accept TLS site certificates: ☐ Yes ☒ No

Accept expired TLS certificates: ☒ Yes ☐ No

SMTP Inbound Site Training

Basics | Security | Comments | Administration

TCP Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

TLS Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

TLS Options

Key file name: keyfile.kyr

Web Site

Basics | Configuration | Domino Web Engine | Security

TCP Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

Redirect TCP to TLS: ☐ Yes ☒ No

TLS Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☒ Yes ☐ No

Client certificate: ☐ Yes ☒ No

TLS Options

Key file name: keyfile.kyr

SSL Purchase and Renewal



Let's Encrypt

Pro

- Free!
- Updates Automatically
- Generates .key format. No need to convert (certmgr does not use .key!)
- Set Up and Go
- Wildcard supported (experience has varied)

Cons

- No warranty protection
- DV (domain validation) level certificate only
- Incomplete chain issues with certain Java applications
- Requires port 80 open

Paid Certificate

Pro

- § Higher Validation Levels offered (OV EV)
- Warranty
- Full Certificate Chain Provided
- Site Seal to reassure visitors
- No port validation needed

Cons

- Cost \$\$\$
- Must convert to .key or .pem manually
- Only valid one year and requires manual validation via email or DNS

Purchased SSL



- DNS Registrar
 - Can install keys for you if site is hosted by them
 - Generates the .csr and .key for you
- SSL Specialty Sites
 - Can purchase multi-year for cheaper (SSL still expires in one year)
 - Can pay extra for installation assistance
- Managed Hosting Providers
 - Handles the whole process for extra cost
 - Receive certificates in all formats needed
 - Can Install on Domino environment for you

Generating your .csr and .key

CollabSphere 2023

Chicago Botanic Garden | Growing Solutions for the World | August 29-31, 2023

Server Certificate Administration

- Does not support key size above 2048
- Keyfile.key buried in Domino server
- Template not available on modern Domino installations

OpenSSL

- Continuously updated
- Supports key size 4096
- Can generate .key as well as convert certs to .pfx .p12 ect
- Knowledgebase article:
 - https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0073175



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files\OpenSSL-Win64\bin

C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out server.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)

C:\Program Files\OpenSSL-Win64\bin>
```

- Stop the headache of single user validation
- People leave, emails change
- Streamline validation with a generic email and mail-in database

admin@trainingwheels.lol

Level 2 Generic Domain E-Mail Addresses

admin@trainingwheels.lol

administrator@trainingwheels.lol

hostmaster@trainingwheels.lol

postmaster@trainingwheels.lol

webmaster@trainingwheels.lol



SSL

dominolearn-2.trainingwheels.lol/trainingwheels

mail/SSL.nsf

admin@trainingwheels.lol

- Notes 9.0.1.3 to 11 can utilize the keyring/kyrtool
 - https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0073172
- Command line tool to view, create and import certificates to .kyr format
- Kyrtool installs with Notes 11 out of the box
- Notes/Domino 12 switch to Certificate Manager!

- Certificate Manager can import .pem, .p12 and .pfx formatted keys
- Simple as copy/pasting certificates in .pem format on a notepad and upload
- Replicated DOMAIN WIDE!
Huge deal for when 90 day keys are implemented for wildcard certificates

Format: ☒ PKCS12 - Binary encoded X.509 (P12/PFX)
☐ Base64 encoded X.509 (PEM, AES256 encrypted)
☐ KYR - Legacy keyring format

File name:

Current password:

Specify a strong password below!

New password:

Verify password:

```
-----BEGIN RSA PRIVATE KEY-----  
(Private Key: domain_name.key contents)  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
(Primary SSL certificate: domain_name.crt contents)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(Intermediate certificate: certChainCA.crt contents)  
-----END CERTIFICATE-----
```

Let's Encrypt



- Automated certificate management for Domino 10 and 11
- Two part streamlined installation on OS and Domino
 - Supports Linux and Windows OS
 - DSAPI filter entry required on Internet Site document
- Requires program document and http restart to update certificate chain
- Certificates stored in data directory as .kyr/.sth
- Server restart usually clears any renewal errors
- Test connection with staging setting before automating
 - Certificate requests are limited and you will get timed out!

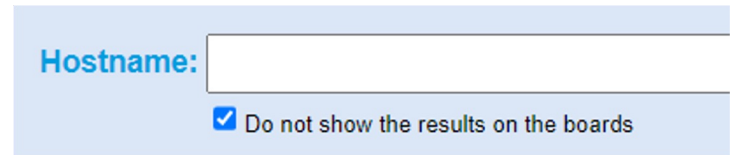
- Native automated certificate management for Domino 12
- One line Administrator command for installation
 - “load certmgr”
 - DSAPI filter entry required on Internet Site document (No longer when upgrading to 12.0.1!)
- Requires a server task entry to ensure the task runs on startup
 - Set config ServerTasks=Replica,Router,Update,Amgr,Adminp,Sched,CalConn,RnRMgr,HTTP,LDAP,Certmgr
- Replicated DOMAIN WIDE! Huge deal for if 90 day keys are implemented
 - Note: TLS credentials cannot be exported. The .key is encrypted
 - Workaround in Domino V12 Certificate Management slides linked at the end



Cipher Security by Domino Version



- Fantastic free tool for testing your site security
- Use it to check:
 - Certificate Chain
 - TLS Protocols Enabled
 - Ciphers
 - Handshake Simulation
 - Be sure to check “Do not show results on the boards”
- <https://www.ssllabs.com/ssltest>



Hostname:

☒ Do not show the results on the boards

- Domino 9.0.1 FP3 – Support for TLS 1.2 is implemented
- Domino 9.0.1 FP3 IF2 – Ability to disable TLS 1.0
 - SSL_DISABLE_TLS_10=1

SSL Cipher Settings

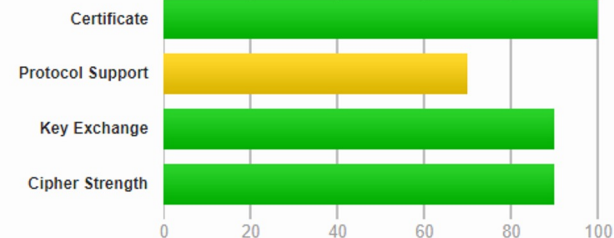
Choose the SSL Cipher Settings you wish to allow:

- ☒ AES encryption with 128-bit key and SHA-1 MAC
- ☒ AES encryption with 256-bit key and SHA-1 MAC
- ☐ RC4 encryption with 128-bit key and MD5 MAC
- ☐ RC4 encryption with 128-bit key and SHA-1 MAC
- ☐ Triple DES encryption with 168-bit key and SHA-1 MAC
- ☐ DES encryption with 56-bit key and SHA-1 MAC
- ☐ RC4 encryption with 40-bit key and MD5 MAC
- ☐ No encryption with MD5 MAC
- ☐ No encryption with SHA-1 MAC

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Overall Rating



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

This server supports TLS 1.0. Grade capped to B. [MORE INFO »](#)

- Updated cipher suite to include 256
- Weak ciphers are NOT removed automatically
 - Ciphers set in previous versions stay selected
 - New ciphers are not selected

SSL Cipher Settings

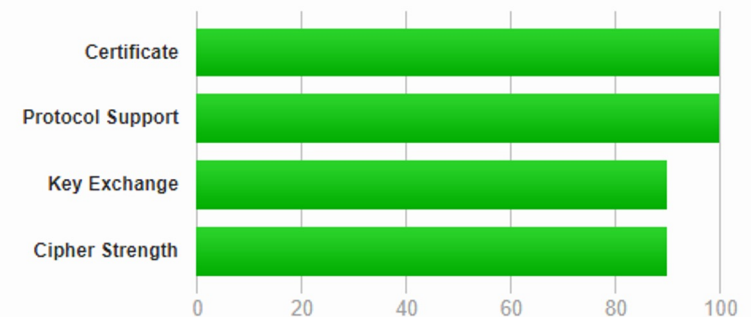
Select the SSL Cipher Settings to allow.

- ☒ ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ☒ DHE_RSA_WITH_AES_256_GCM_SHA384
- ☒ ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ☒ DHE_RSA_WITH_AES_128_GCM_SHA256
- ☐ ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ☐ DHE_RSA_WITH_AES_256_CBC_SHA256
- ☐ ECDHE_RSA_WITH_AES_256_CBC_SHA
- ☐ DHE_RSA_WITH_AES_256_CBC_SHA
- ☐ ECDHE_RSA_WITH_AES_128_CBC_SHA256
- ☐ DHE_RSA_WITH_AES_128_CBC_SHA256
- ☐ ECDHE_RSA_WITH_AES_128_CBC_SHA
- ☐ RSA_WITH_AES_256_GCM_SHA384
- ☐ RSA_WITH_AES_128_GCM_SHA256
- ☐ RSA_WITH_AES_256_CBC_SHA256
- ☐ RSA_WITH_AES_256_CBC_SHA
- ☐ RSA_WITH_AES_128_CBC_SHA256
- ☐ RSA_WITH_AES_128_CBC_SHA

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS	128

Overall Rating



- Domino 12.0.2 deprecated most weak/outdated ciphers
 - Domino 12 disables TLS 1.0 by default!
- Check your cipher lists!

TLS Security

TLS ciphers:

[Modify](#)

ECDHE_RSA_WITH_AES_256_GCM_SHA384 [C030]
DHE_RSA_WITH_AES_256_GCM_SHA384 [9F]
ECDHE_RSA_WITH_AES_128_GCM_SHA256 [C02F]
DHE_RSA_WITH_AES_128_GCM_SHA256 [9E]
ECDHE_RSA_WITH_AES_256_CBC_SHA384 [C028]
DHE_RSA_WITH_AES_256_CBC_SHA256 [6B]
ECDHE_RSA_WITH_AES_128_CBC_SHA256 [C027]
DHE_RSA_WITH_AES_128_CBC_SHA256 [67]
ECDHE_RSA_WITH_AES_256_CBC_SHA [C014] (deprecated)
DHE_RSA_WITH_AES_256_CBC_SHA [39] (deprecated)
ECDHE_RSA_WITH_AES_128_CBC_SHA [C013] (deprecated)
DHE_RSA_WITH_AES_128_CBC_SHA [33] (deprecated)
RSA_WITH_AES_256_GCM_SHA384 [9D] (deprecated)
RSA_WITH_AES_128_GCM_SHA256 [9C] (deprecated)
RSA_WITH_AES_256_CBC_SHA256 [3D] (deprecated)
RSA_WITH_AES_256_CBC_SHA [35] (deprecated)
RSA_WITH_AES_128_CBC_SHA256 [3C] (deprecated)
RSA_WITH_AES_128_CBC_SHA [2F] (deprecated)
RSA_WITH_3DES_EDE_CBC_SHA [0A] (deprecated)
RSA_WITH_RC4_128_SHA [05] (deprecated)

Note: Version 9.x Domino servers will ignore this selection. They use the server INI setting **SSLCipherSpec** instead.

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits	FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK 256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits	FS	WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA)	FS	WEAK 128
		FS	WEAK 128

SSL Report: awesomelaser.win (199.103.7.12)

Assessed on: Fri, 25 Aug 2023 20:18:17 UTC | [Hide](#) | [Clear cache](#)



- You have made all changes but still receiving an A in SSL Labs
- HSTS is the answer!
- This protocol is used to prevent man-in-the-middle attacks, downgrade attacks and cookie hijacking
- HTTP_ENABLE_HSTS=1
- HTTP_HSTS_INCLUDE_SUBDOMAINS=1
- Seeing a “Too Short” warning? Add the following notes.ini - HTTP_HSTS_MAX_AGE=63072000
- Too short can cause the browser to ignore the request for HTTPS connection and us HTTP
- <https://blog.darrenduke.net/darren/ddbz.nsf/dx/domino-adds-hsts-to-its-security-arsenal.htm>

SSL Report: awesomelaser.win (199.103.7.12)

Assessed on: Thu, 07 Sep 2023 18:07:44 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)

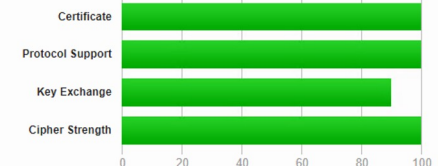
Strict Transport Security (HSTS)

Yes

max-age=63072000; includeSubdomains

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](#)

TLS 1.3?

- TLS 1.3 is currently not supported by any version of Domino
- HCL has stated it is on the roadmap, no current release date



Bonus Tips!



. Cipher errors present even after cleaning up Internet Site Documents

```
[650193:000152-00007FA959DBB700] 08/23/2023 07:48:59 PM Remote console command issued by Domino Admin [redacted]: tell http restart
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value C014
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value 39
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value C013
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value 35
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Invalid cipher(s) seen for server CN=[redacted]
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value C014
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Invalid cipher(s) seen for site Default site for monitoring
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value 39
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value C013
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value 35
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value C014
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Invalid cipher(s) seen for site iphora.io
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value 39
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value C013
[651065:000011-00007F0FAA7E3700] 08/23/2023 07:48:59 PM Ignoring invalid SSLCipherSpec value 35
[651065:000002-00007F0FF55BB540] 08/23/2023 07:48:59 PM XSP Command Manager terminated
[651065:000002-00007F0FF55BB540] 08/23/2023 07:49:00 PM iNotes Init: Credential Store Configuration not enabled, less secure mode.
[651065:000002-00007F0FF55BB540] 08/23/2023 07:49:00 PM XSP Command Manager initialized
[651065:000002-00007F0FF55BB540] 08/23/2023 07:49:00 PM HTTP Server: Restarted
```

Invalid Cipher Errors on HTTP Startup

CollabSphere 2023

Chicago Botanic Garden | Growing Solutions for the World | August 29-31, 2023

- Hidden views strike again!
- Configuration → Current Server Document to disable Internet Site Documents then save
- Ports → Internet Ports → TLS Ciphers
- To achieve an A+ in SSL Labs disable all but the top four

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

Basics

Server name: dominolearn2/trainingwheels

Server title:

Domain name: Trainingwheels

Fully qualified Internet host name: dominolear

Cluster name:

Load Internet configurations from Server/Internet Sites documents: Disabled

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | Miscellaneous | Transactional L

Notes Network Ports | Internet Ports... | Proxies |

TLS settings

TLS key file name: keyfile.kyr

Accept TLS site certificates: ☐ Yes ☒ No

Accept expired TLS certificates: ☒ Yes ☐ No

TLS ciphers:

Modify

TLS Cipher Settings

Select the TLS Cipher Settings to allow.

- ☒ ECDHE_RSA_WITH_AES_256_GCM_SHA384 [C030]
- ☒ DHE_RSA_WITH_AES_256_GCM_SHA384 [9F]
- ☒ ECDHE_RSA_WITH_AES_128_GCM_SHA256 [C02F]
- ☒ DHE_RSA_WITH_AES_128_GCM_SHA256 [9E]
- ☐ ECDHE_RSA_WITH_AES_256_CBC_SHA384 [C028]
- ☐ DHE_RSA_WITH_AES_256_CBC_SHA256 [6B]
- ☐ ECDHE_RSA_WITH_AES_128_CBC_SHA256 [C027]
- ☐ DHE_RSA_WITH_AES_128_CBC_SHA256 [67]
- ☐ RSA_WITH_AES_256_GCM_SHA384 [9D]
- ☐ RSA_WITH_AES_128_GCM_SHA256 [9C]
- ☐ RSA_WITH_AES_256_CBC_SHA256 [3D]
- ☐ RSA_WITH_AES_128_CBC_SHA256 [3C]
- ☐ RSA_WITH_AES_128_CBC_SHA [2F]

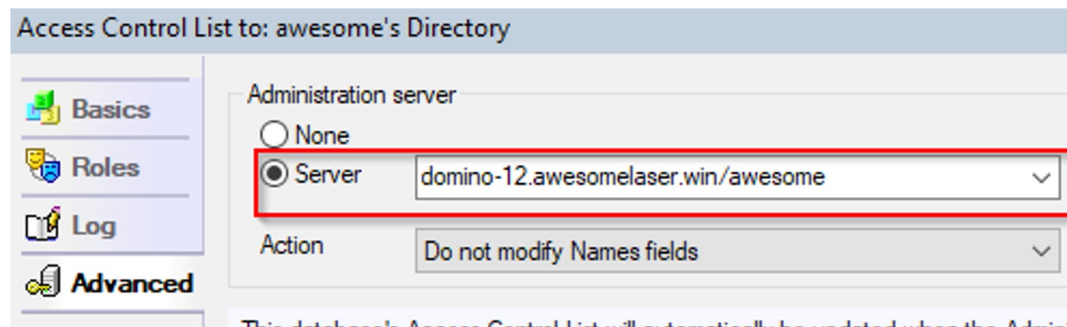
- Domino Version under Configuration → All Documents only updated by names.nsf admin server. Is it correct?

domino-12.awesomelaser.wi

domino-12.awesomelaser.win

Release 12.0.2

- No? Update the Administrator server on the names.nsf and restart server



- Be sure to refresh the design template of names.nsf as well

Certmgr – Port 80 Error

CollabSphere 2023

Chicago Botanic Garden | Growing Solutions for the World | August 29-31, 2023

Error Cannot verify challenge on server - Check HTTP port 80 inbound connection!
Failed to write one or more challenge(s)

- Certmgr auto renewal requires port 80 to be open
- Settings that redirect traffic to 443 will break this process
- Setting Anonymous access to no will also break auto renewal unless you update your notes.ini

HTTPPUBLICURLS=/iwaredir.nsf/*:/.well-known/acme-challenge/*

Outgoing TLS key file name: keyfile.kyr

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

Web
(HTTP/HTTPS)

TCP/IP port number:	80
TCP/IP port status:	Redirect to TLS
Enforce server access settings:	No
TLS port number:	443
TLS port status:	Enabled

TCP Authentication

Anonymous:	<input checked="" type="radio"/> Yes <input type="radio"/> No 1
Name & password:	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Yes with TOTP <i>TOTP option available if Session authentication is Single or SSO.</i>
Redirect TCP to TLS:	<input checked="" type="radio"/> Yes <input type="radio"/> No 2

TLS Authentication

Anonymous:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name & password:	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Yes with TOTP
Client certificate:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Bearer token (JWT):	<input type="radio"/> Yes <input checked="" type="radio"/> No

TLS Options

Key file name:	keyfile.kyr
----------------	-------------

- As of Domino 12.0.1FP1, HCL Nomad can be installed directly on the Domino server instance
- During the initial set up, Nomad will look for/install Certmgr and create a nomad.<yourdomain>.com entry
- To utilize your own purchased certificate, install Certmgr and set up nomad.<yourdomain>.com prior to installation.
 - This is not a requirement just a way to skip the extra step of having to modify/recreate the entry



- . If no matter what you change your Domino ciphers to does not reflect in SSL Labs, Check for proxy and passthru servers in the environment that may be handling Encrypting the traffic.

TLS Security

TLS ciphers:

Modify

ECDHE_RSA_WITH_AES_256_GCM_SHA384 [C030]
DHE_RSA_WITH_AES_256_GCM_SHA384 [9F]
ECDHE_RSA_WITH_AES_128_GCM_SHA256 [C02F]
DHE_RSA_WITH_AES_128_GCM_SHA256 [9E]

Note: Version 9.x Domino servers will ignore this selection. They use the server INI setting **SSLCipherSpec** instead.



Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits	FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA)	FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits	FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA)	FS WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 4096 bits	FS WEAK	128

- Redirect Rules can interfere with certmgr renewal, throwing a port 80 connection error
- Workaround – Temporarily disable Internet Site Documents → restart http → re-run the renewal
- Yes, this will break the auto-renew feature while the redirect is in place

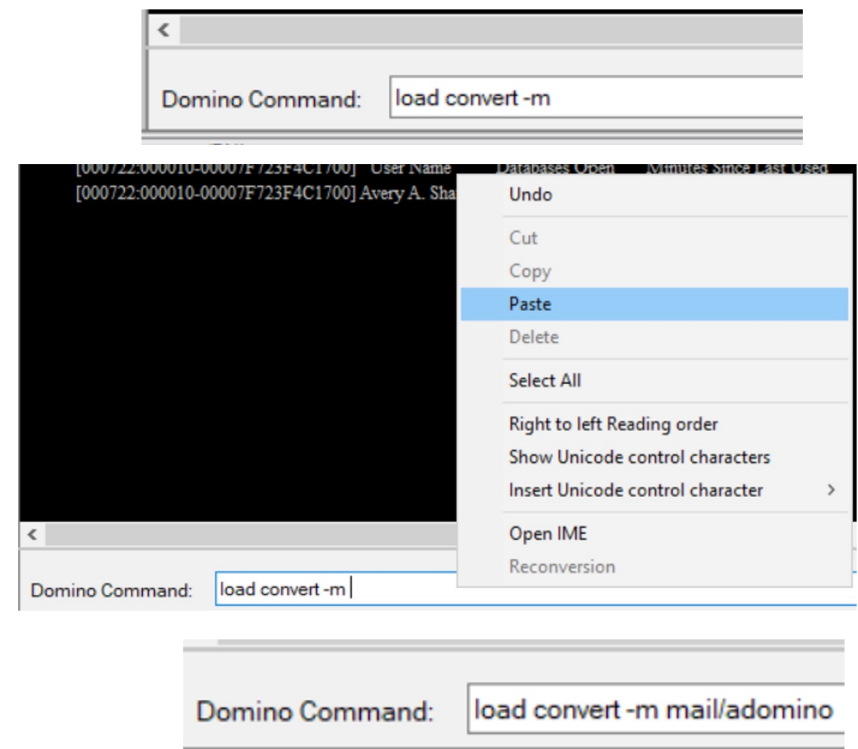
Main

Last updated: 1

Status:

Error Cannot verify challenge on server - Check HTTP port 80 inbound connection!
Failed to write one or more challenge(s)

- Type in a command and realize you want to copy in the email path?
- You still can! Though a CTRL + V will replace the line, a Right Click + Paste will insert your clipboard at the end of the line!



- Domino V12 Certificate Management
 - HCL Academy, by Daniel Nashed
 - https://blog.nashcom.de/presentations/openntf2021_domino_certmgr.pdf
- Let's Encrypt for Domino V10/11
 - <https://openntf.org/main.nsf/project.xsp?r=project/LetsEncrypt.org%20-%20Free%20SSL%20Certificates%20for%20Domino/summary>
 - <https://www.midpoints.de/de-solutions-LE4D>