Domino V12 Security Preview

Online @ RNUG 9.12.2020

HCL SOFTWARE

Speakers

Daniel Nashed

- Nash!Com, Germany
- HCL Business Partner / ISV
- nsh@nashcom.de
- http://blog.nashcom.de

Thomas Hampel

- HCL Germany
- Director @ Product Management
- thomas.hampel@pnp-hcl.com
- https://blog.thomashampel.com

HCL Lifetime Ambassador

Please Note

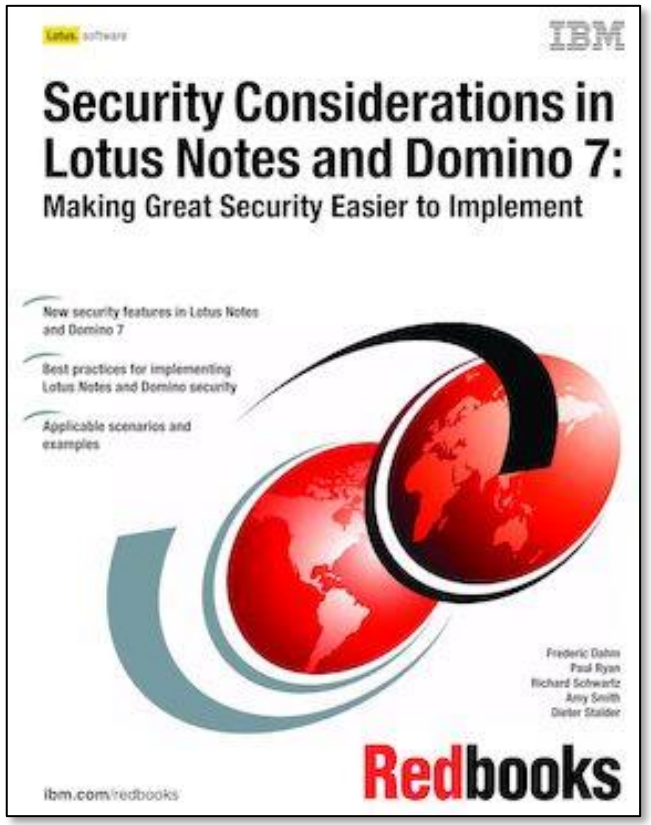
HCL's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at HCL's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard HCL benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.



Domino Early Access Program

- Available Free for all customers with a current entitlement

https://blog.hcltechsw.com/domino/introducing-hcl-domino-early-access-program

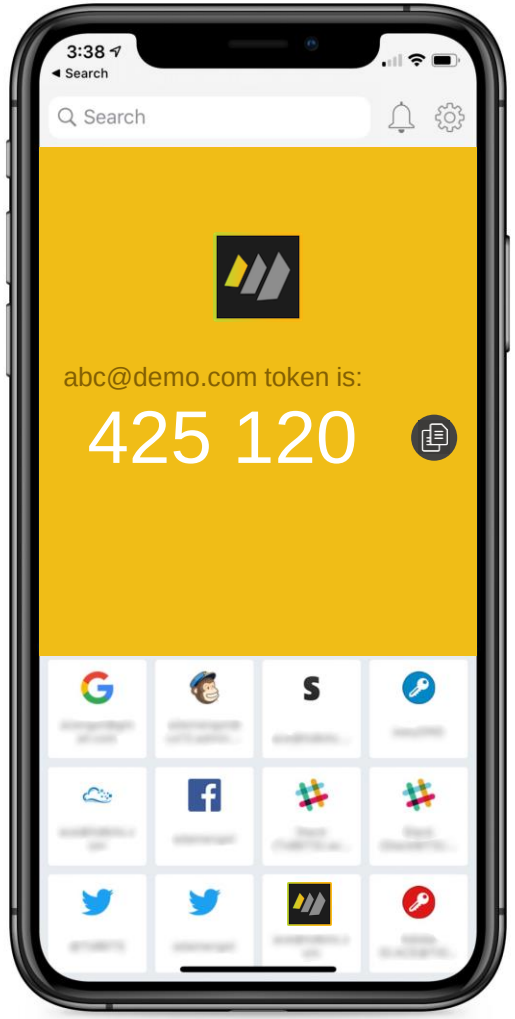
What is it

https://blog.hcltechsw.com/domino/introducing-hcl-domino-early-access-program

- Fast paced, technical preview to provide customers and partners the opportunity to provide feedback early in the development phase
  - Providing >specific< features in form of Code Drops
  - New code drops every couple of weeks
- Available for all existing customers with current subscription & support.
- This is **NOT** a traditional beta program!
  - There will be a separate Beta Program including Notes Clients & other server platforms at a later stage
- Public available documentation https://help.hcltechsw.com/domino/earlyaccess/early_access_welcome.html
- Discussion forum (same format we had before) https://registration.hclpartnerconnect.com/dominoearlyaccessforum.nsf?open
- **Docker only** with a short refresh cycle and new functionality in code drops
- Docker image download is provided via Flexnet

Time-based One-time Password (TOTP)

- Two-Factor Authentication built into Domino
- App-Based (e.g. Google Authenticator, Authy, etc.)



Home / DOMINO-I-29 / New idea

97
VOTE

2FA for web app and iNotes, Verse

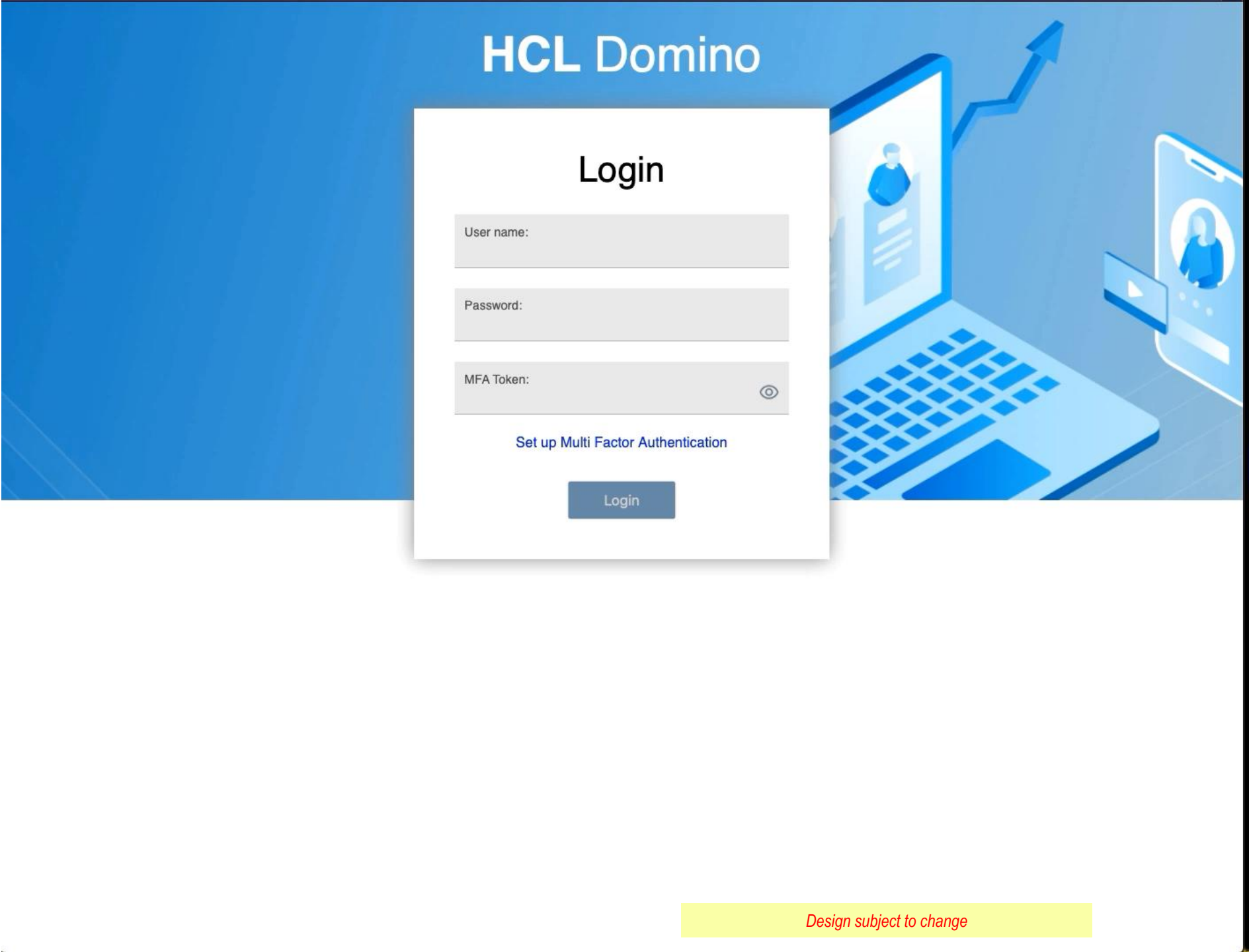
Domino is about security. 2FA is about security. Domino needs 2FA. Given the choice I'd pick SMS and Google Authenticator.

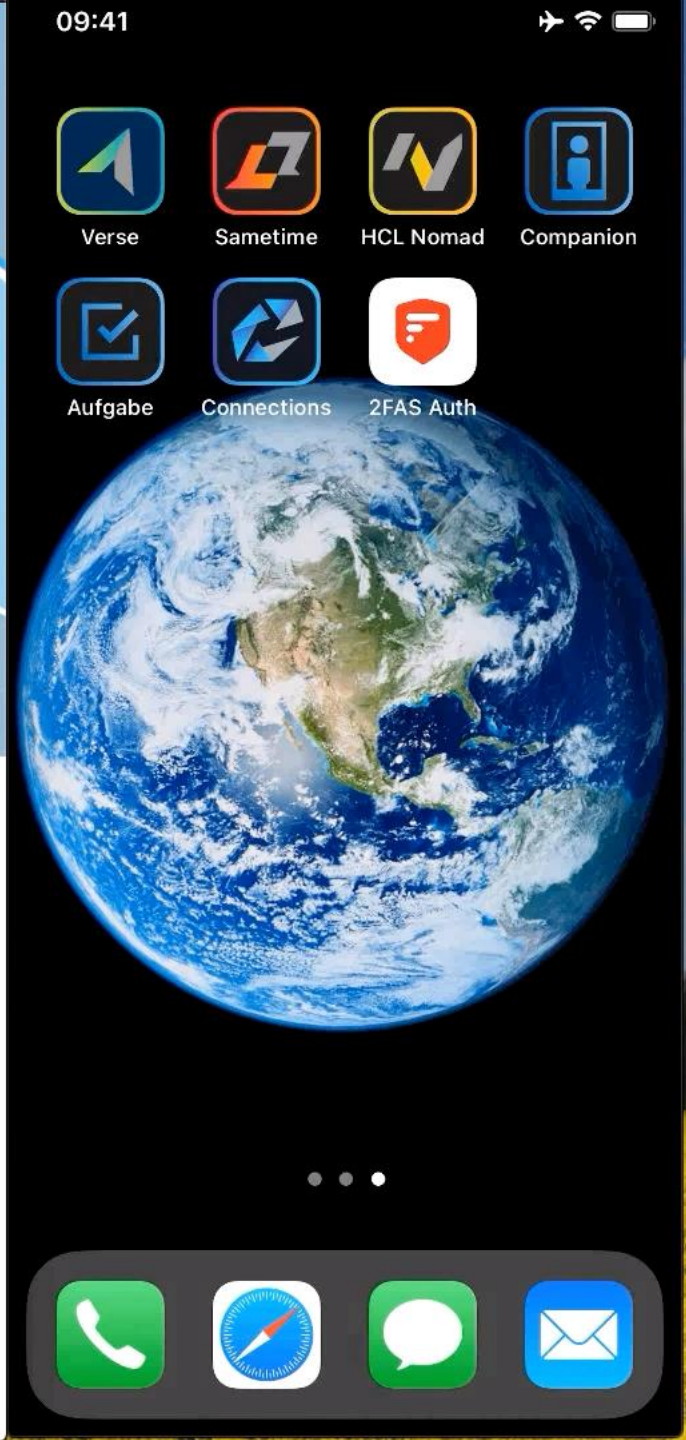
it would also be nice to have Traveler require some type of 2FA at device setup too.

Guest • Jul 16 2018 • Likely to implement

https://domino.ideas.aha.io/ideas/DOMINO-I-29

Design subject to change

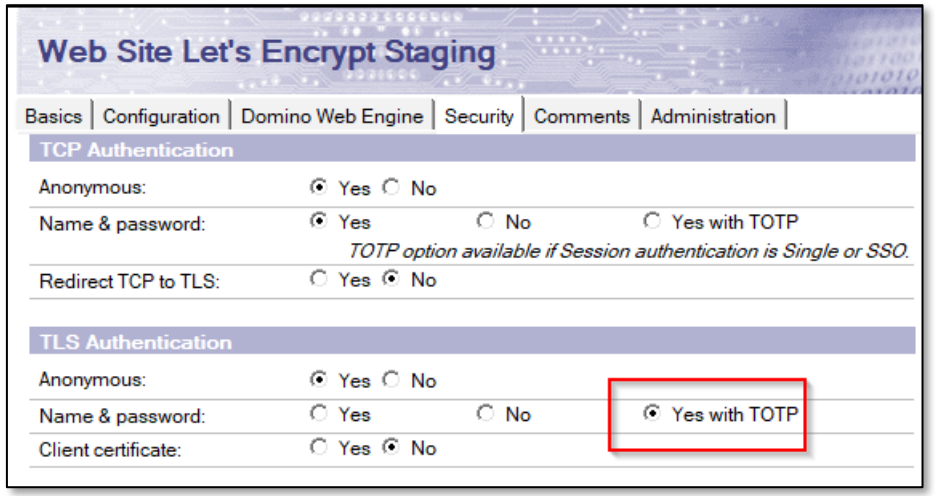


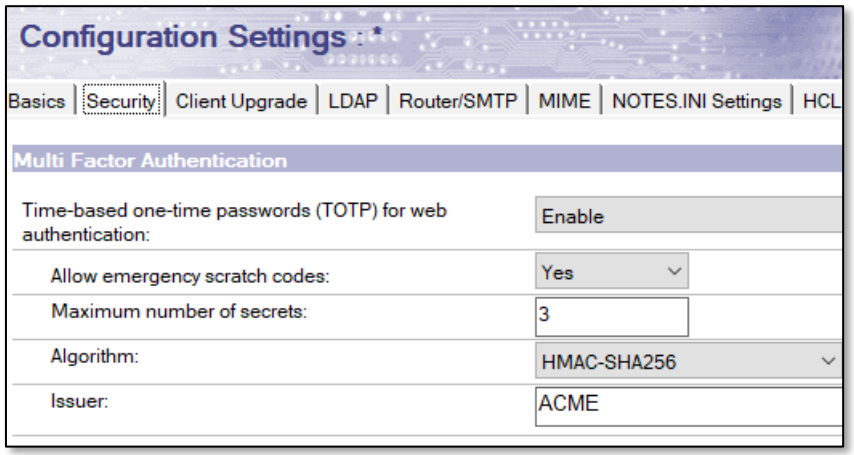


Design subject to change

TOTP Simple Config Steps

- 1. Generate Vault Trust Certificate
  - mfamgmt create trustcert "*/O=acme" cert.id super-secret
- 2. Edit security configuration tab
- 3. Enable TOTP in Server doc or Internet Site
- 4. Enable session based authentication (single or multi server)
- 5. Configure login form





Tips:

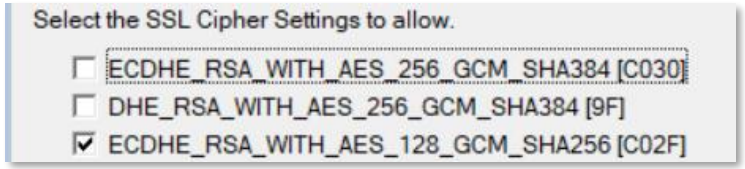
- Vault server needs to be restarted
- Public documentation contains troubleshooting section

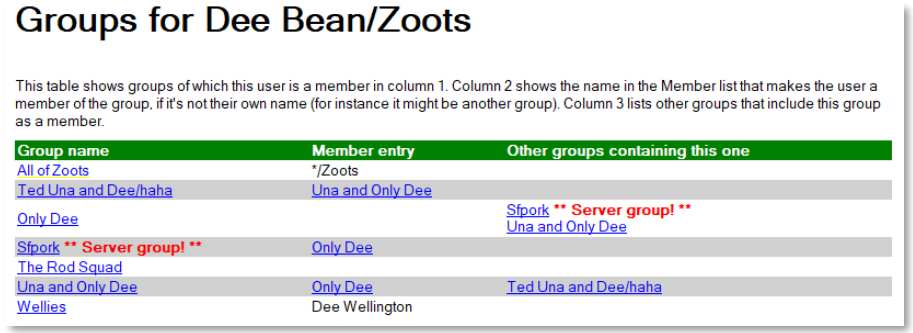
- See detailed steps:

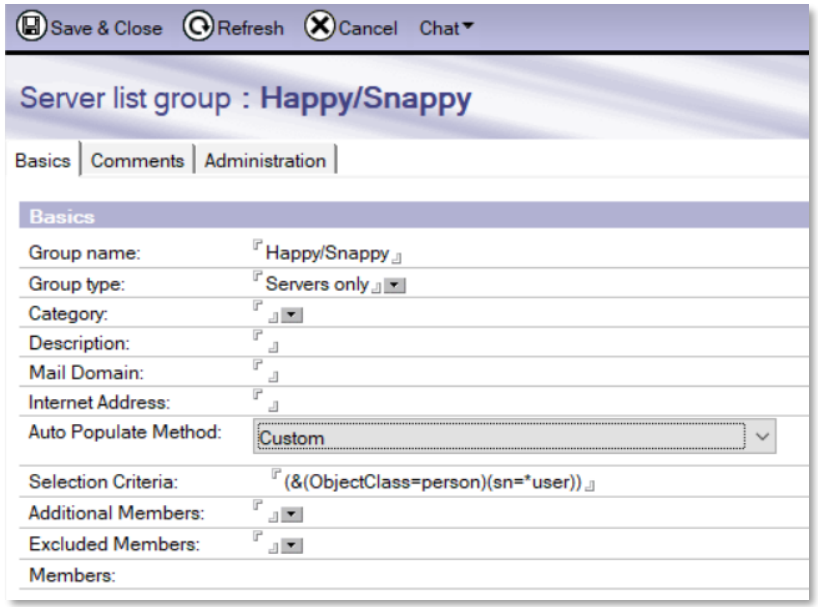
  https://help.hcltechsw.com/domino/earlyaccess/conf_totp_overview.html

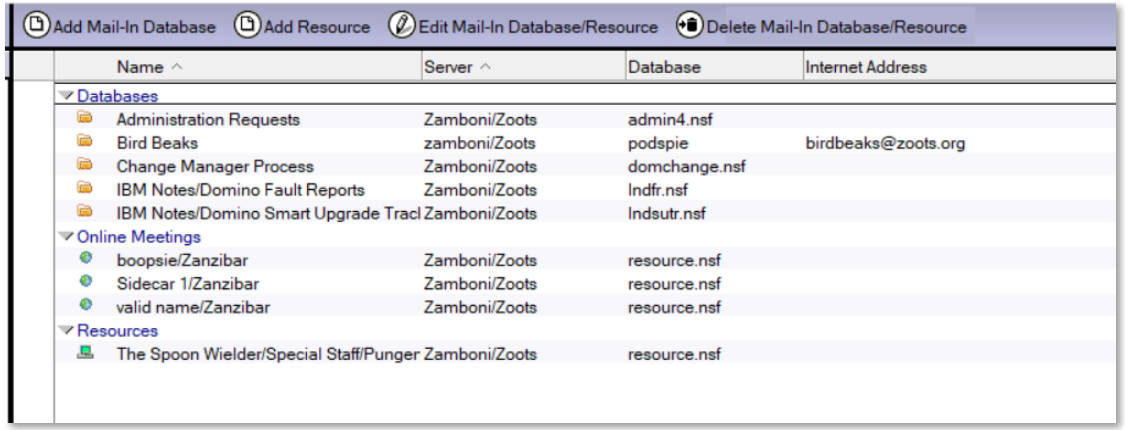
Improvements you were looking for

- Auto-Populate Groups with Custom criteria
- Display Internet Address in Mail-in DB view
- Display Hex code of SSL Cipher
- Find Groups that person is a member of
- And more !









Design subject to change

What Admins love to do…

- Hardware / Virtual machine / System Resources
- Operating System (License + Setup)

- Setting up Servers
  - Installing Domino
  - Configure Domino

- Setting up Business applications
  - Install Domino application(s)
  - Change server configuration to meet application needs

- Maintenance
  - Patching & Upgrading servers

What Admins love: One Touch Setup

- Automated setup experience
- One Touch scripted setup including ID Vault creation
- Have a certificate at first server start
- For example: Let’s Encrypt certificates with one load command working today
- Full demo in Docker presentation tomorrow

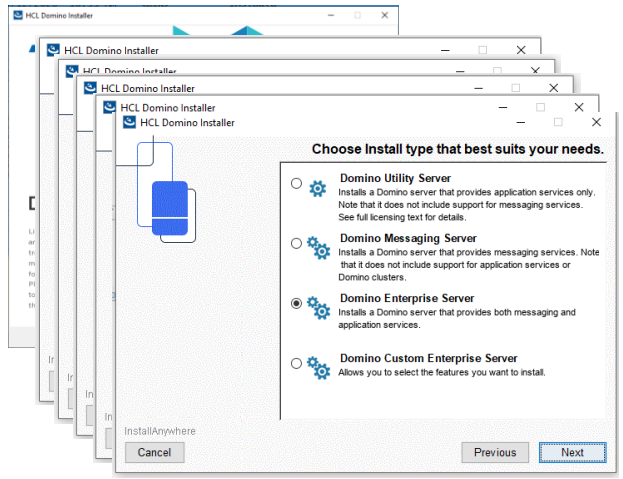
https://help.hcltechsw.com/domino/earlyaccess/inst_onetouch.html

Simple JSON Configuration

```
{
"serverSetup": {
"server": {
"type": "first",
"name": "adminserver",
"domainName": "ACME",
"title": "ACME Administration Server"
},
"network": {
"hostName": "adminserver.acme.com",
"enablePortEncryption": true,
"enablePortCompression": true
},
"org": {
"orgName": "sherlock",
"certifierPassword": "@Prompt:Enter
Certifier Password"
},
"admin": {
"firstName": "Sherlock",
"lastName": "Holmes",
"password":
"@Secret:c:\\run\\secrets\\adminpass.txt",
"IDFilePath": "admin.id"
},
"security": {
"ACL": {
"prohibitAnonymousAccess": true,
"addLocalDomainAdmins": true
}
}}
```

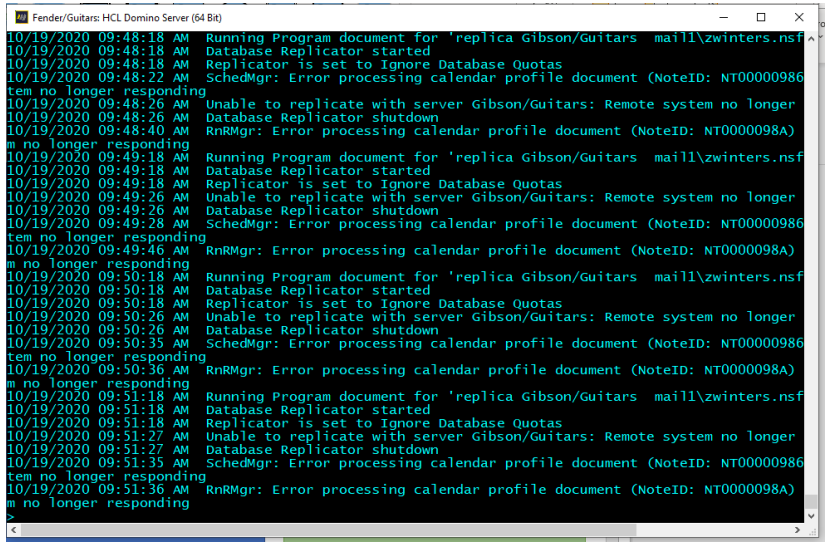
Server –autoconfig config.json

Install



On premises

Ready



HCL SOFTWARE

Automating Certificate Management

Let's Encrypt

- Request Let's Encrypt certificates from within Domino
- Free of charge SSL/TLS certificates
- No need to copy files to server
- No need to create or manage *.kyr files
  - Leveraging standard PEM format!
  - Domino can read directly from a domain wide new cerstore.nsf

Home / DOMINO-I-12 / New idea

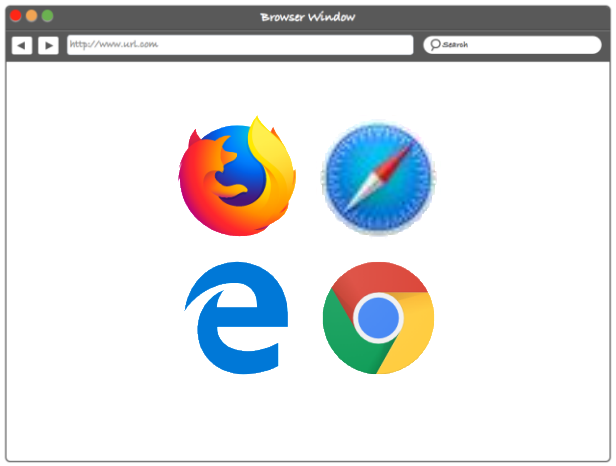
179 VOTE

Include Support for Let's Encrypt

see https://midpoints.de/de-solutions-LE4D

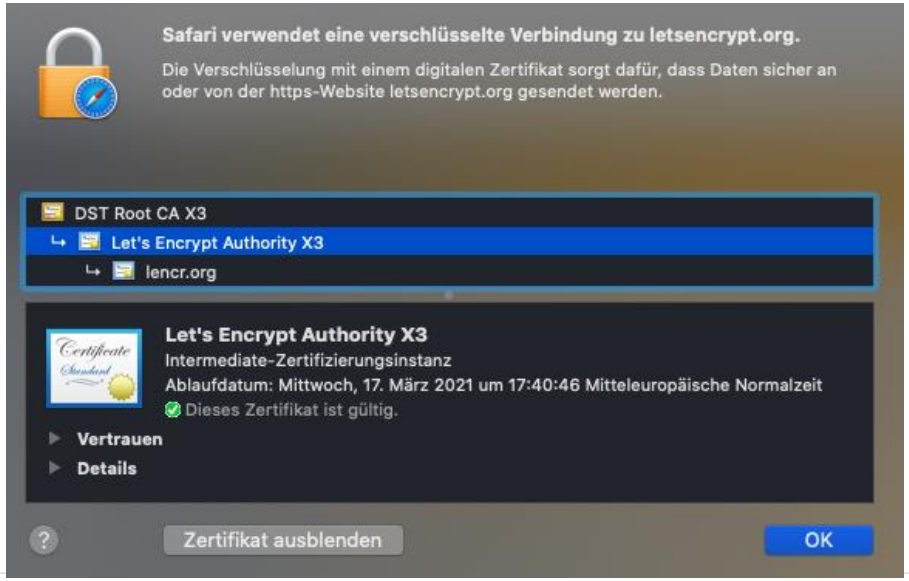
Guest • Jul 14 2018 • Planning to implement

Automating Certificate Management



Trusted Certificate

https://yourserver.com



HCL Domino V12

Technology

- Leverages existing and new Domino security APIs
- Implements Let's Encrypt uses ACME protocol V2 (RFC 8555)
  - **AMCE** = **A**utomatic **C**ertificate **M**anagement **E**nvironment
  - Own HCL implementation leveraging standards like
    - JSON, LibCurl, JWS, OpenSSL, Notes crypto including PEM, RSA and ECDSA keys ...
- Designed for automation
  - When server is available on HTTP (port 80) and HTTPS (port 443) **and** has an DNS entry, you can create your first certificate with one command today

Automatic Integrated Certificate Management

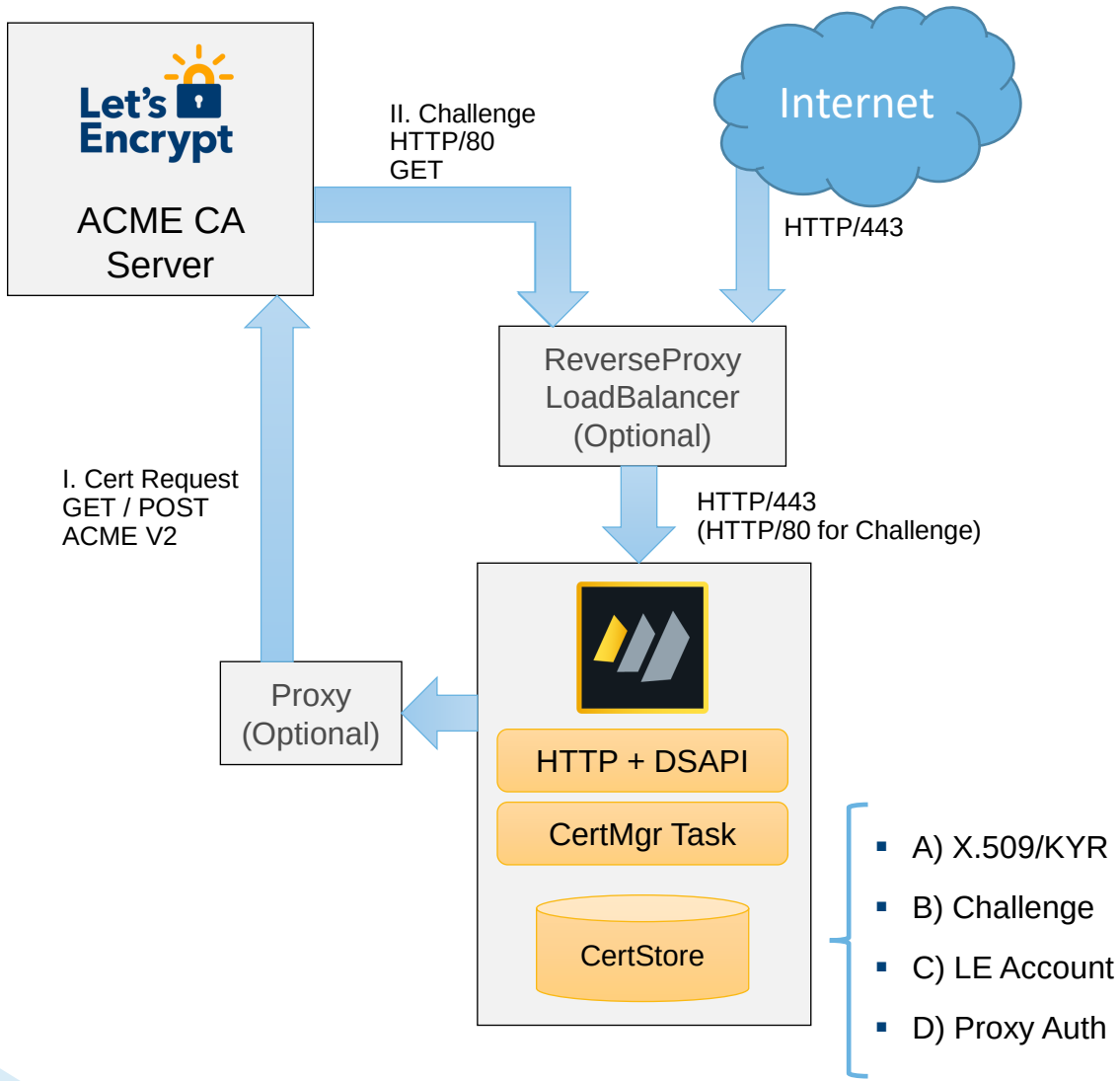
- First early code drop was to get feedback
- Each code drop shipped more functionality
- Agile approach to ship what is ready to test

- Currently implemented
  - Let's Encrypt® certificate requests leveraging “HTTP” challenges
  - New Domino Servertask “certmgr” and database “certstore.nsf”

- Certificates & keys are stored in PEM format
- New Term: **TLS Credentials** = { key pair + certificate + chain + root }
- Domino V12 will use the domain wide, secured certstore.nsf database!

- Note: Kyr-File format will remain as an option for older servers

Architecture Overview



Components

*) Connection between Domino, LE and CertStore could be local or NRPC

Domino HTTP and LE could be on separate server and just need a common CertStore.

(A) X.509 today in kyr file
(B) Challenge needed to verify request
(C) LE used to authenticate with ACME CA
(D) Proxy account needed for outgoing communication

Flow

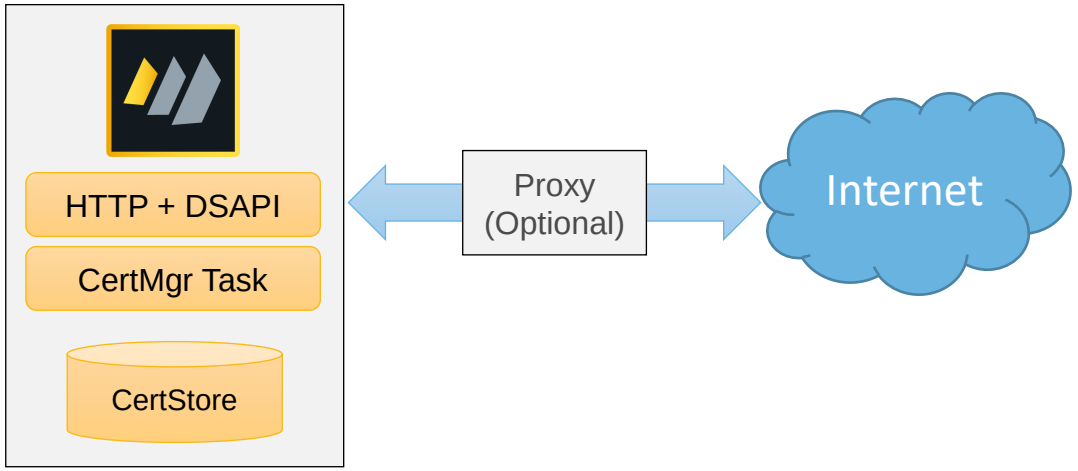
1. LE creates account (C) with ACME server
2. LE creates private key and writes it to CertStore (A)
3. LE creates CSR and sends it to ACME CA *)
4. LE puts received challenge (B) in CertStore
6. ACME server requests challenge on port 80 to verify
7. Domino HTTP replies with challenge (B) from CertStore
8. LE receives certificate including and writes it to CertStore (A)

HTTP (and INET tasks) read X.509 from CertStore (A)

*) Proxy communication uses Proxy user (D)

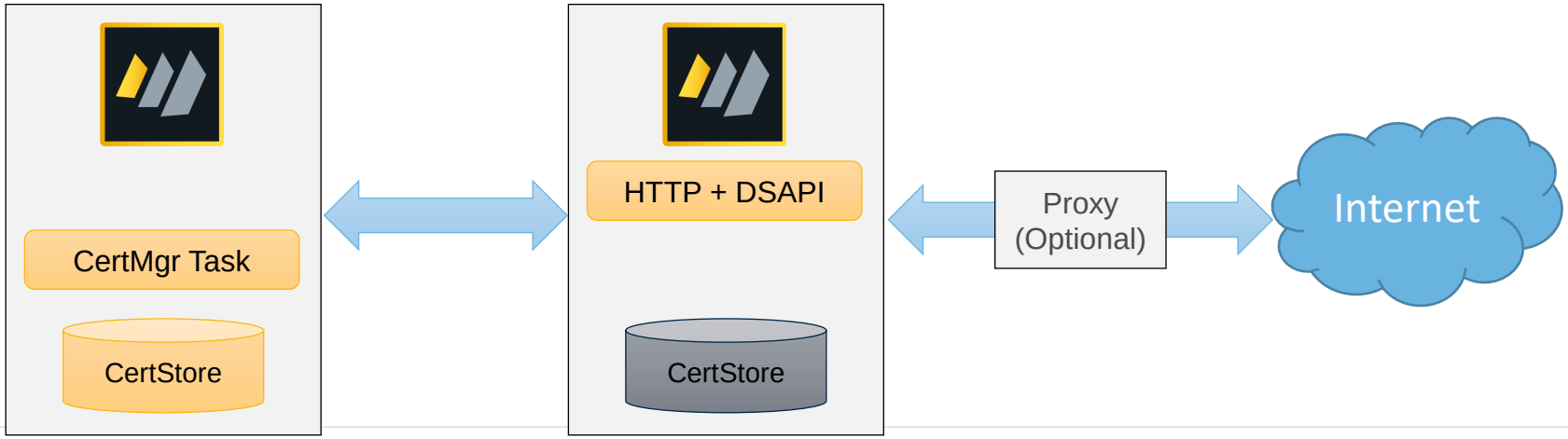
Standard Scenario - Domino V12 with inbound HTTP(S)

- Certmgr task and certstore.nsf on the same Domino V12 server
- DNS pointing to your server
  - Tip: DNS Domain entry like A record *.acme.com pointing to your server, allows you to test with any hostname ;-)
- Certmgr supports outbound proxy connections including authentication
- Inbound HTTP(S) connection can use an incoming proxy/load-balancer
- Allows automatic setup if DNS and hostname matches



Distributed Setup

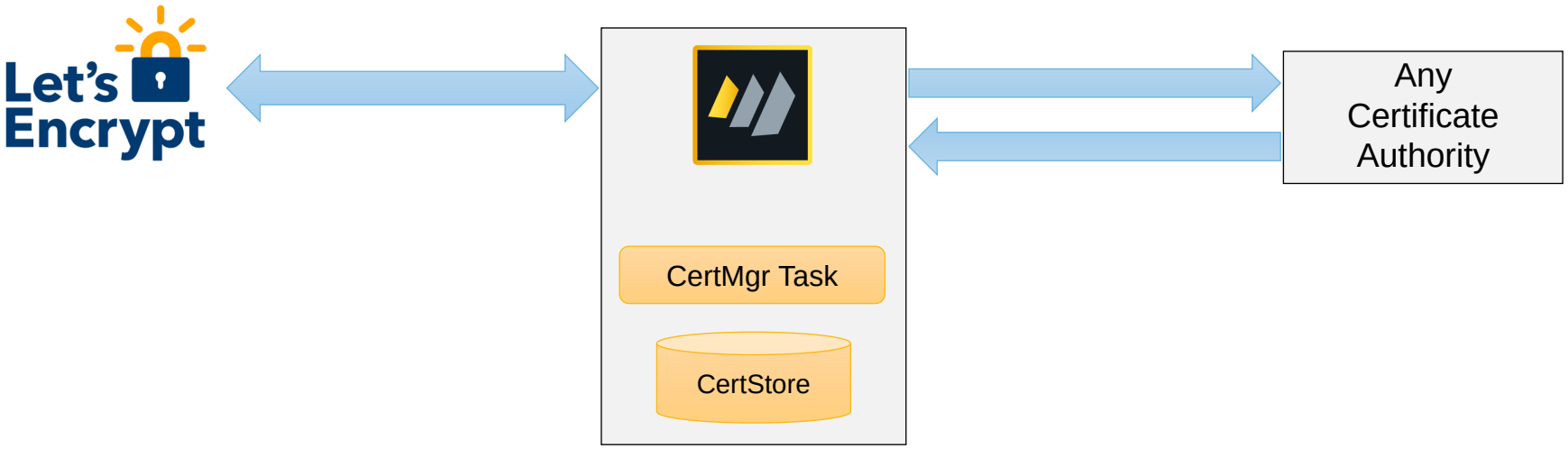
- Local Domino V12 server (e.g. on notebook)
  - Notes.ini **certmgr_server=domino-v11-server** pointing to an existing server with inbound HTTP(S)
- Domino V10/11 server running in corporate environment/at provider
  - DSAPI installed + certstore.nsf on Domino V11 server handling incoming Let's Encrypt Challenges
    - DSAPI is available for Linux64 and Win64 and works on Domino 10,11 & 12
- Certmgr running locally can request certificates for remote server
  - .kyr file has to be deployed manually on remote server
- You could also point your existing server to the Domino V12
  - If inbound NRPC is allowed
  - Notes.ini **certmgr_server=domino-v12-server** pointing to your internal server



3rd Party Certificate Authority

- What if you don’t want or can’t use Let’s Encrypt ?
- Creating Certificate Request Manually
  - Support for any Certificate Authority supporting a CSR flow or provides a PEM file with “key + certificates”

➔ DEMO: Request Certificate manually from a company Microsoft Certificate Authority



Subject Alternate Name support for Let's Encrypt

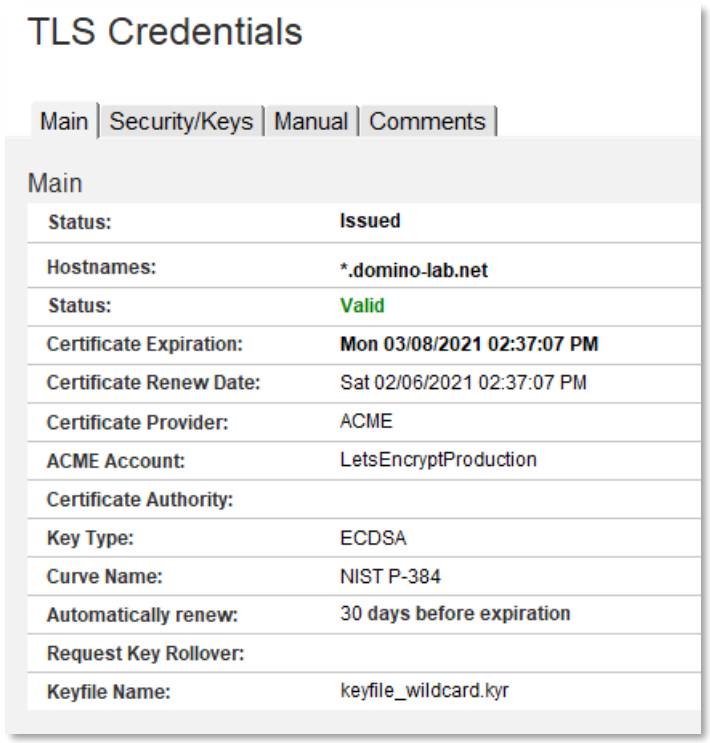
- **S**ubject **A**lternate **N**ame support is already available since 11.0.1
- CertMgr supports to request SANs
- Simply request multiple names in a single request
  - rnug.domino-lab.net
  - moscow.domino-lab.net
  - st-petersburg.domino-lab.net

Each SAN needs to reply to a separate ACME challenge

- Officially supported limit: 40 SANs
  - ACME supports maximum of 100 SANs

HCL Domino V12

Let’s Encrypt DNS Challenges & Wild Cards



- What if we want to support many websites?
- Maybe even on the fly without a new certificate?
- Or reuse the same “**TLS Credentials**” on many servers?
- Wildcard certificates are supported with Let’s Encrypt DNS-01 challenges
- Requires a DNS API to create DNS TXT records
  - Build in support to simply integrate 3rd party providers
  - A couple of providers are already implemented as examples
    Planned Interface: HTTP Request with @Formulas, Command Line, Notes Agent

ACME Standard – Already tested environments

- **Let's Encrypt Production**
  - https://letsencrypt.org
- **ZeroSSL**
  - https://zerossl.com
  - Requires external account binding (EAB)
- **BuyPass**
  - https://buypass.com
- **Internal deployment**
- **TIP: SmallStep ACME CA**
  - https://smallstep.com/docs/tutorials/acme-challenge
  - Full CA which can operate as a sub-CA with full ACME functionality
  - Setup on Docker in 10 minutes!

Test & Development

- Let's Encrypt Staging
  - https://letsencrypt.org/docs/staging-environment
- Let's Encrypt Boulder
  - https://github.com/letsencrypt/boulder
- Let's Encrypt Pebble
  - https://github.com/letsencrypt/pebble

Support for Elliptic Curves – “ECDSA Keys” vs RSA

- **ECDSA crypto provide higher encryption with less overhead**
  - 256 bit (NIST P-256) ECDSA key → 3072 bit RSA key or a 128 bit AES key.
  - 384 bit (NIST P-384) ECDSA key → 7680 bit RSA key or a 192 bit AES key.
  - 512+ bit ECDSA key (NIST P-521) → 15360 bit RSA key or a 256 bit AES key.
- Domino V12 supports ECDSA for all internet protocols
- CertMgr supports ECDSA for ACME account keys and internet certificates
- Support for key rollover from RSA keys to (new) ECDSA keys for ACME account keys and “TLS Credentials” (remember the new term)
- Two ciphers which are well supported for all current devices and browsers:
  - **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC02B)**
  - **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC02C)**
- We don’t want to bore you with details but if you care
  - https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet/
  - https://help.hcltechsw.com/domino/earlyaccess/wn_ECDSA%20cryptography.html

HCL Domino V12

Support for two important TLS 1.2 Curves – X25519 & X448

- **Strong security with improved performance**

- **The new order of curves**
  - **Curve X25519**
  - Curve NIST P-256
  - **Curve X448**
  - Curve NIST P-384
  - Curve NIST P-521

Details: https://en.wikipedia.org/wiki/Curve25519

HCL Domino V12

- **Ref: If needed curves can be disabled one by one via notes.ini**
  - **Best practice is to keep the out of the box configuration**

  - SSL_DISABLE_CURVE_X25519
  - SSL_DISABLE_CURVE_P256
  - SSL_DISABLE_CURVE_X448
  - SSL_DISABLE_CURVE_P384
  - SSL_DISABLE_CURVE_521

Reference: https://help.hcltechsw.com/domino/earlyaccess/wn_new_curves_ecdhe.html

NRPC port encryption supports forward secrecy using X25519

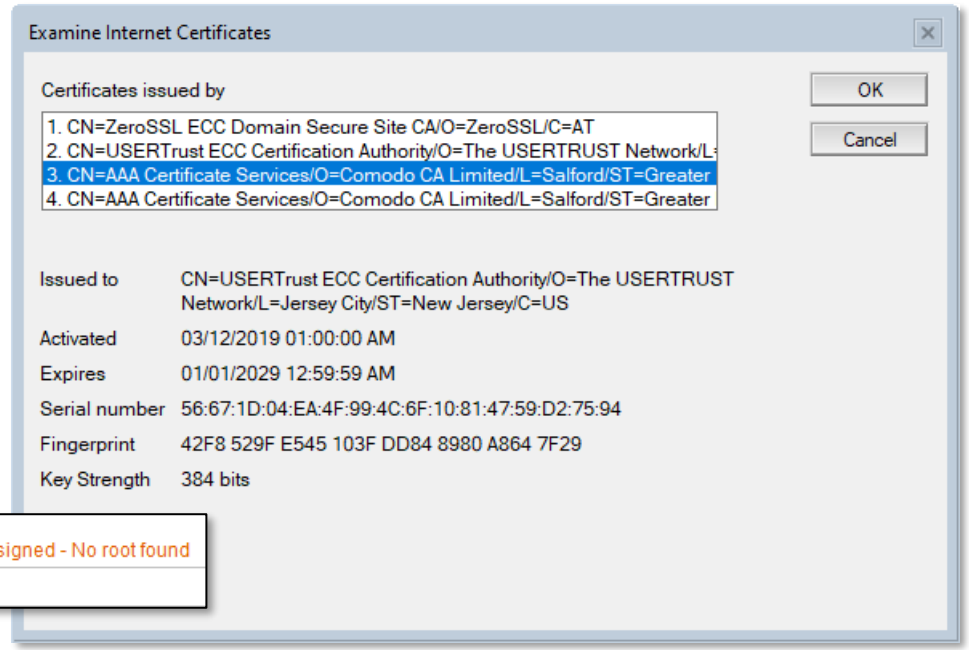
- Improved performance with higher security
- Enable:
  - Add 32 to your current value for the PORT_ENC_ADV notes.ini setting.
  - New recommendation: notes.ini **PORT_ENC_ADV=100**
  - Enables AES-128 GCM, AES tickets, and X25519 forward secrecy
- Investigating making the PORT_ENC_ADV=100 the default to provide high security with optimized performance. Performance testing is still on-going
- Tip: Check connections via **notes.ini LOG_AUTHENTICATION=1**
- Today you can only test between two Domino V12 servers until beta provides V12 clients as well

HCL Domino V12

Reference: https://help.hcltechsw.com/domino/earlyaccess/wn_new_curves_ecdhe.html

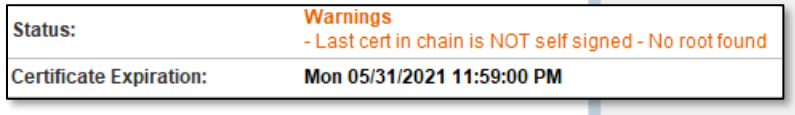
Manual Certificate operations to integrate with other CAs

Very simple copy & paste interface – No more openssl or kyrtool



- 1. Automatically create key pairs and CSRs
- 2. Copy the CSR directly via Action button to your favorite CA
- 3. Paste Certificate and chain back into the form

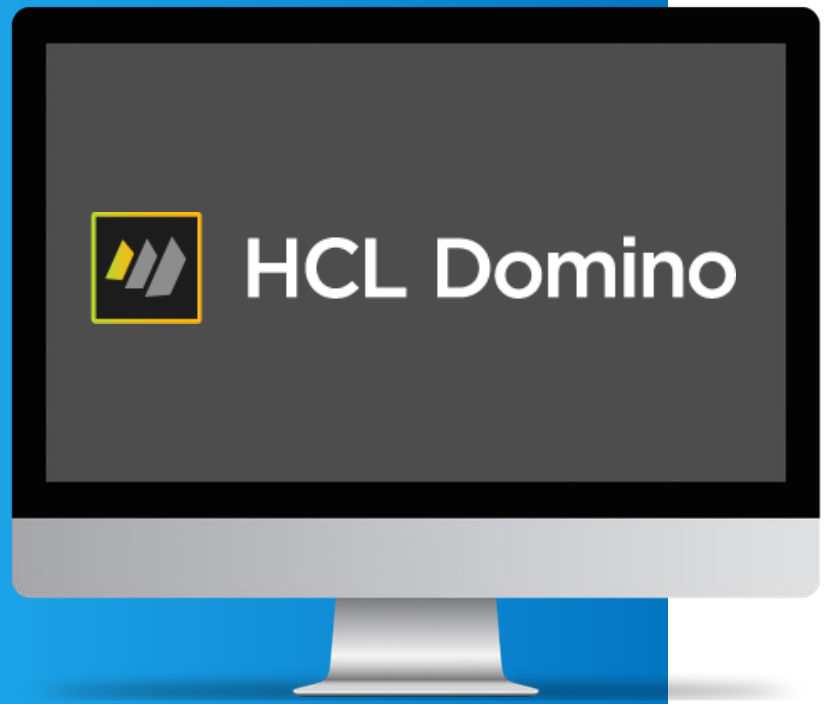
- Automatically creates a *.kyr file if needed



- "Certificate health check" with detailed information in the form
- Certificate Heath checks also checks for certificate expiration and generates statistics
- Example: CertMgr: Info: Health Check - Green: 12 Yellow: 1 Red: 2
- Existing certificate dialogs you already know, now also work for TLS Credentials.

- **Domino V12 will read certificates from the trusted Domino domain wide certstore.nsf …**

DEMO TIME



- Let’s Encrypt & CertMgr Live

What’s Next ?

HCL Digital Solutions Academy

https://blog.hcltechsw.com/domino/hcl-digital-solutions-academy/

Q & A

HCL SOFTWARE

Questions & Keep the Ideas Coming – Domino Ideas Portal

And, please follow these three steps:

- Where we gather and prioritize your ideas
- Where we want you to add, vote, comment on and share as many ideas as you like.

1

Search the forum to see if your idea already exists.

Vote for any ideas and add any additional comments that you may have related to that idea.

2

If your idea does not already exist, create a new idea and format your idea like:
"As a <insert role>, I would like to be able to <insert action> in order to <insert need>."

3

Create as many ideas as you'd like, but remember to keep each idea, separate.

Do not create idea that consist of more than one request for enhancement.

https://domino.ideas.aha.io/

HCL

Relationship™

BEYOND THE CONTRACT

$8.4 BILLION ENTERPRISE | 132,000 IDEAPRENEURS | 44 COUNTRIES

WATCH THE FILM