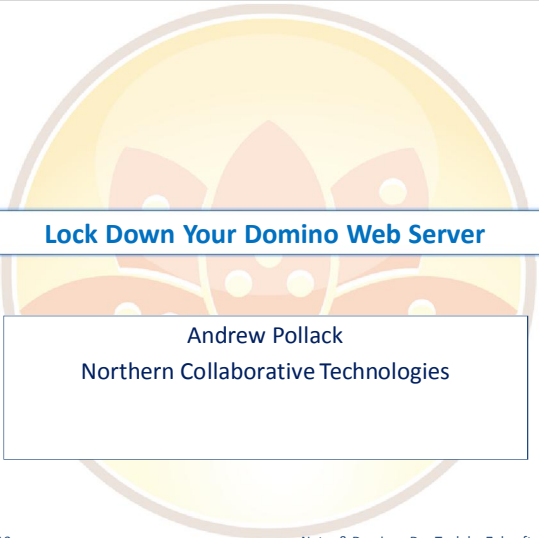




Lock Down Your Domino Web Server

Andrew Pollack
Northern Collaborative Technologies

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

What We'll Cover ...

- The First Two Rules of Internet Security
 - Understanding Threat Vectors
 - The Domino Security Model
 - Server Level Security
 - Configuring SSL
 - Field Level Encryption

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

The First Two Rules of Internet Security

If You Don't Want it Accessed
Keep It Off The Net

If It Is Not Encrypted
It Is Public

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren



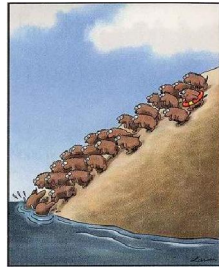
UNDERSTANDING THREAT VECTORS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Unskilled External Threats

- Extremely Common
 - General Spam
 - Malware via Email & Browser
 - Script Kiddies
- Easiest to Manage through application of best-practices
 - Anti-Virus / Anti-Spam
 - Operating System Updates
 - Software Patches



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Skilled External Threats

- Least Common
 - Domino Aware & Site Aware
 - Focused Goals
 - Reasonably Manageable
 - Never Totally Safe



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Unskilled Internal Threats

- May come from skilled administrators making mistakes
- Accidents & Unintended Consequences
- Users Bypassing the Rules & Processes
- Often results in data loss or exposure of private information
- Avoided by good security and administrative practices
- Managed through Backup & Restore, Disaster Recovery



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

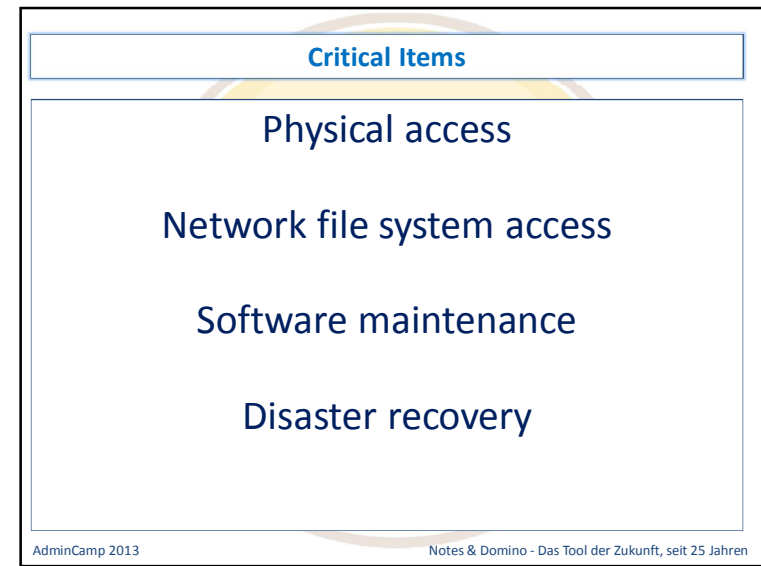
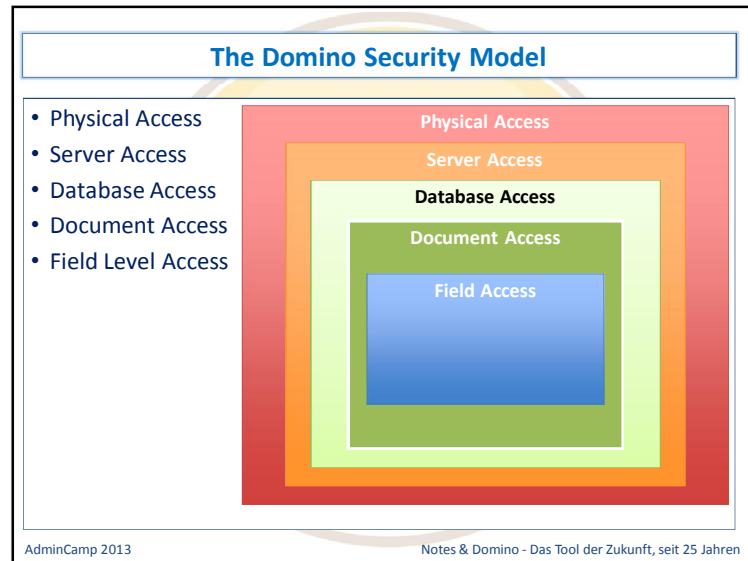
Skilled Internal Threats

- The Most Dangerous Kind
 - Network & Domino Administrators
- Common Goals of Skilled Internal Threats
 - Unauthorized Access to Management Email or HR Information
 - Employee Harassment or Stalking
 - Retribution – often related to promotion, termination, or redundancy
 - Theft of Information – often related to leaving the company



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren



User Management Processes

- Are these processes documented?
 - New User Process
 - Lost Password Process
 - User Terminations
 - Mail Retention
- Are the processes followed?
- Do they meet their requirements?
- Are Terminations tied in some way to the HR department?
 - Avoid delays in this process
 - Lag time in terminations is a key weakness

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Reliability is Security

- Denial of Service is the most common threat
 - It is also the easiest hostile action to take, in most cases
- Service Levels can be Mission Critical
 - Financial Institutions the week before taxes are due
 - Decision Support Systems
 - Sales People and their Email
- Does a response plan exist?
 - Has it been tested?
- If the whole system fails – what will the result be?

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Physical & Network Security

- Who accesses the hardware routinely?
- Who else can gain access to the hardware?
 - Including swapped RAID drives & Backup
- Support Facilities Security
 - Redundant Power
 - Redundant Cooling
 - Fire, Flood, Storm, and other Natural Events
 - Building Lock-Out Issues
 - Live Hot-Site Requirements

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Operating System Security

- Who manages the network level access?
- Are the database files stored with local encryption?
- Who manages the operating system?
 - Patches & Updates
 - Anti-Virus
 - Backup Software
 - Operating System network firewall
 - Domino Software Installation
- Is Remote Access software used?
 - VNC, Remote Desktop, Terminal Services, etc.
- What other OS level services are enabled?

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Backups & Data Security

- Is the backup & restore process documented?
 - Has it been recently tested?
- Is the backup software certified for use on a Domino Server?
 - Have you checked the version?
- Is the backup data encrypted?
 - Who has the decryption keys?
- Is the backup data kept off-site?
 - Who has access to it?
 - How long does it take to retrieve it?

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Enterprise Integration

- Key vector for credential spoofing or theft
- Common Integration Paths
 - End User Desktop Single Sign-on
 - Back end RDBMS, ERPS, & CRM
 - User Credential Pass-Through
 - Batch Data Transfer
- Each case is unique – look for exploitation paths
 - Access to stored credentials
 - Network intercept of tokens or credentials
 - Source Data poisoning
- SQL Injection Matters Here
 - While Domino itself tends to be fairly resistant to sql injection, it can be used to pass data to other systems which are more vulnerable

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

SERVER DOCUMENT SETTINGS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

The Internet Sites View

- Load Internet Configurations from Sever\Internet Sites View
- Many key security features configured Here
- Older servers may not have this value saved!



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Enforce Server Access Settings

- Very well hidden – but very important

The screenshot shows the Domino Server configuration console. The 'Web' tab is selected, and the 'Enforce server access settings' checkbox is checked. Other settings visible include TCP/IP port number (80), TCP/IP port status (Enabled), and various authentication options.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Internet Authentication

- Fewer Names with Higher Security

- With This setting

- Full Hierarchical Name
- Common Name
- User Name Field Aliases
- Internet Address
- LDAP UID (if LDAP is in use)

- With the lower security setting

- All of the above
- Last Name Only
- First Name Only
- Short Name
- Soundex Value!

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

WEBSITE CONFIGURATION DOCUMENT SETTINGS

Do not use a "Default Site" – Specify by name

- If you use a default site, it will get used accidentally in the case of a misconfiguration

The screenshot shows the Domino Web Site configuration console for 'n64test.thenorth.com'. The 'Site Information' tab is selected. A blue arrow points to the 'Use this web site to handle requests which cannot be mapped to any other web sites' checkbox, which is currently unchecked. The 'Host names or addresses mapped to this site' field is empty.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Do not use a "*" for servers that host – specify by name

- Same Reason --
- If you use a default site, it will get used accidentally in the case of a misconfiguration – possibly on servers you don't expect

Web Site n64test.thenorth.com

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

Site Information

Descriptive name for this site: n64test.thenorth.com

Organization: thenorth

Use this web site to handle requests which cannot be mapped to any other web sites: ☐ Yes ☒ No

Host names or addresses mapped to this site: *

Domino servers that host this site: *

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Use IP addresses wherever possible to identify the server

- To use SSL you must either use an IP address or make this the default and only internet site document
- If you use IP addresses, you can associate a different SSL keyring with each internet site on the same server

Web Site n64test.thenorth.com

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

Site Information

Descriptive name for this site: n64test.thenorth.com

Organization: thenorth

Use this web site to handle requests which cannot be mapped to any other web sites: ☐ Yes ☒ No

Host names or addresses mapped to this site: 192.168.201.10

Domino servers that host this site: NCT_W64_TESTthenorth

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Turn off Allowed Methods for "Options" and "Trace"

- These settings are not used by most web applications
- Unless you have a specific reason to use these, disable them
 - There is no point in giving hackers more information

Allowed Methods

Methods:

☐ GET ☒ HEAD ☒ POST ☒ OPTIONS ☒ TRACE ☐ DELETE ☐ PATCH

WebDAV: ☐ Enable

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Session Authentication

- You should pretty much always use Session Based Authentication
 - You can exclude certain addresses if need be
 - Traveler
 - Web Services
- Single Server
 - A token will automatically be created and used
- Multiple Servers
 - You must specify an LTPA Token
 - We'll walk through creating one in a few pages
- SAML
 - A giant Single Sign On standard now supported by Domino
 - Come see my presentation about this on Wednesday

HTTP Sessions

Session authentication: Multiple Servers (SSO)

Web SSO Configuration: LTPAToken2

Force login on SSL: No

Select Keywords

Keywords: SAML, Multiple Servers (SSO), Single Server, Disabled

OK Cancel

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Redirect TCP to SSL

- Even if you allow unencrypted access to your pages you should never allow credentials to be passed in the clear

Web Site n64test.thenorth.com

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

TCP Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☐ Yes ☒ No

Redirect TCP to SSL: ☒ Yes ☐ No

SSL Authentication

Anonymous: ☐ Yes ☒ No

Name & password: ☐ Yes ☒ No

Client certificate: ☐ Yes ☒ No

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Disable Old SSL Ciphers

- These are out of date and almost no browser still needs them
- Is this a huge security threat?
 - No.
- Will you get an entry on some security reviewer's checklist?
 - Yes.

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

☐ AES 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

NOTE: These only apply to SSLv3. (You cannot adjust the SSLv2 ciphers.)
A MAC is a Message Authentication Code which assures that a message has not been tampered with.

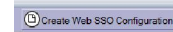
AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

SETTING UP AN LTPA TOKEN

Creating the LTPA Token

- In the Internet Sites View



- Make sure the DNS Domain matches your website
- Mapping names in the token will allow the token credentials to work even if the user has no person document on one of the servers
- Require SSL to prevent MiM attacks that steal tokens
 - E.g. "Firesheep"

Web SSO Configuration for :

Basics | Comments | Administration

Token Configuration

Configuration Name:

Organization:

DNS Domain:

Map names in LTPA tokens: ☒ Enabled

Require SSL protected communication (HTTPS): ☒ Enabled

Restrict use of the SSO token to HTTP/HTTPS: ☒ Disabled

Participating Servers

Domino Server Names:

Windows single sign-on integration (if available): ☒ Disabled

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

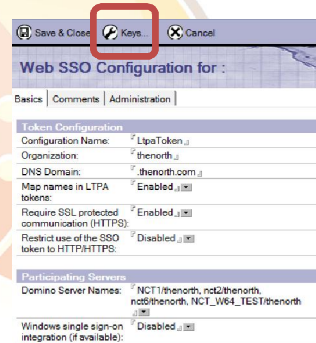
Before you save, click “keys” to generate the token

- The Domino Server Names you list must be in the Directory when you create or save this document

- Their Public Key is used to encrypt the LTPA Token Credentials.

- To share an LTPA token with servers in another Domino Domain:

- Copy that server's document into your directory and set it to your domain while you create and save the token
- Copy the created token to the other server's directory



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

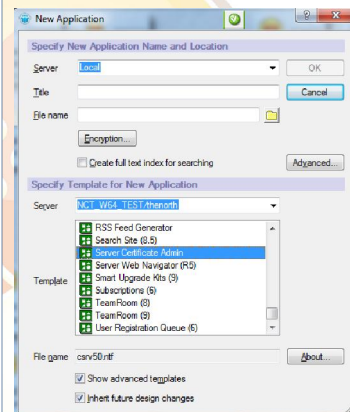
SETTING UP SSL KEYRINGS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Create A Cert Admin Database

- The template is on your server
- Click the advanced templates button



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Open the Database

- See the Nice Menu



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Create A Key Ring

- This file, and its sibling will be copied to your Domino server when you're done. Use a good password – you won't have to enter it when you restart Domino.
- The entries in these fields are picky. Make sure to read the help line as you're entering the information

Create Key Ring	
The first step is setting up SSL on a server is to create the key ring. When the key ring is created, a self-signed certificate is generated and stored in the key ring.	
Key Ring Information	Quick Help:
Key Ring File Name: NCTKeyfile.kyr	Specify the name and password for the key ring.
Key Ring Password: [password]	Note: You'll be returning to this screen in subsequent steps as you create and install certificates in the key ring.
Confirm Password: [password]	
Key Size	Key Size: 1024 (bits)
Key Size: 1024 (bits)	Key size is the size of the distinguished key pair in bits. The larger the key size, the greater the strength.
Distinguished Name	Note: This Edition of Domino provides the ability to generate PKA input with TCGA, JPA and D12 in accordance with request regulations worldwide.
Common Name: www.thenorth.com	The Distinguished Name is the information about your site that will appear in a certificate request.
Organization: Northern Collaborative Technologies	
Organizational Unit: Production (optional)	Note: Make sure the Distinguished Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.
City: Cumberland (optional)	
State or Province: Maryland (optional)	
Country: US (two character country code)	
[Create Key Ring]	

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Hooray! You have a keyring!

Key Ring Created	
Your key ring has been created.	
Key ring file name:	C:\notesdata\NCTKeyfile.kyr
The following Distinguished Name will be used for all certificates created for this key ring:	
Common name:	www.thenorth.com
Organization:	Northern Collaborative Technologies
Organizational unit:	Production
City:	Cumberland
State:	Maine
Country:	US
Next Step:	
You can now add certificates to your key ring. Choose "Create Certificate Request" from the main menu to generate a certificate request.	

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Back to the Menu

- Now Create A Certificate Request



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Creating A Certificate Request

- Make sure to log the request, so you can get back to it if you need a new copy of the request key.
- You almost always will be pasting this value into the CA's website

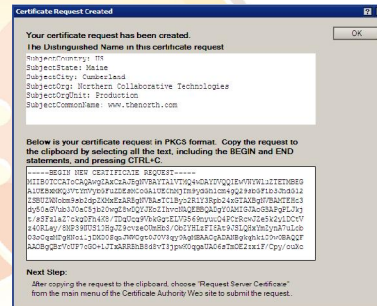
Create Server Certificate Request	
A certificate is required for the public key in the key ring you created. To obtain a certificate, you create a certificate request, and provide it to a Certificate Authority for signing. Use this form to create the certificate request.	
Note: Before proceeding you should read the documentation provided by the Certificate Authority you are using to see how they require the certificate request to be delivered.	
Key Ring Information	Quick Help:
Key Ring File Name: C:\notesdata\NCTKeyfile.kyr	Specify the key ring file.
	Note: The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information	
Log Certificate Request: ☒ Yes ☐ No	Log certificate requests for future reference.
	Note: Choose "View Certificate Request Log" in the main menu page to see a listing of all logged requests.
Method: ☒ Paste into form on CA's site ☐ Send to CA by e-mail	Choose how to submit the certificate request to the Certificate Authority.
	Note: The "Paste" method is recommended if it is supported by the Certificate Authority you are using.
[Create Certificate Request]	

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Copy Your Certificate Request

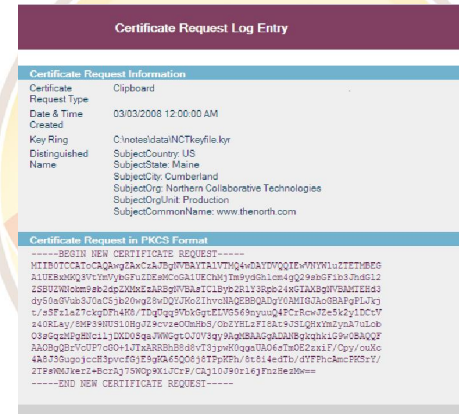
- You want the whole text from "Begin" to "End" including those lines
- If you click ok and need to get this back, its in the log document



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Here's the Log Entry

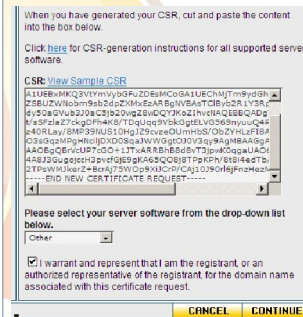


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Now Go to the Certificate Authority

- Each CA will have their own byzantine process by which you must submit the certificate request.
- Most will need to verify you are who say you are.
- This is a tricky step, and you have to deal with poorly designed CA web sites.
- GoDaddy, Verisign, and InstantSSL are three of many CA's to pick from.
 - I like to use "namecheap.com"

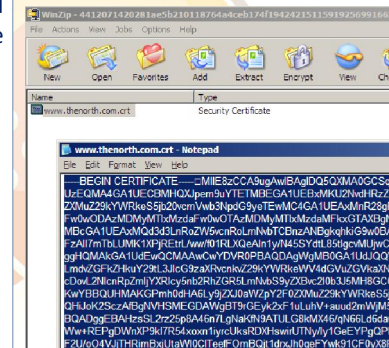


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Get the Certificate From The CA

- The CA will have a strange and painful process to give you the certificate.
- In this case, when I finally got it, it is in a certificate file.
- I just open that file in NOTEPAD and copy the text.
- Most CA's will let you just get the certificate as text.



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Back to the Database

- You may have to select “View & Edit Key Rings” to open yours before you can proceed

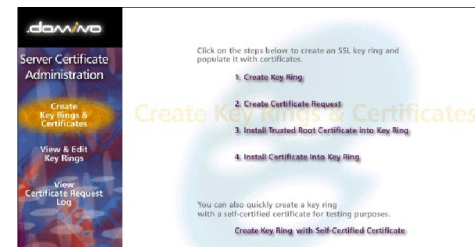


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Back To The Menu

- Install Certificate Into Key Ring



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Install the Certificate

Install Certificate into Key Ring

The Certificate Authority will notify when your signed certificate is ready. The specifics depend on the Certificate Authority. But typically you will receive an email specifying a URL where you can pick up the certificate. Once you have obtained the signed certificate, this form lets you install it into your key ring. **Note:** Before installing this certificate, it is recommended that you install the certificate of the signing Certificate Authority in your key ring as a Trusted Root. If you haven't already done so, choose "Accept This Authority in Your Server" from the main menu of the Certificate Authority Web site to obtain the CA certificate.

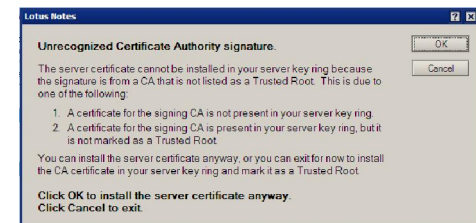
Key Ring Information	Quick Help
Key Ring File Name: C:\notes\data\NCTkeyfile.kyr	Specify the key ring file.
Certificate Information Certificate Source: ☐ File ☒ Clipboard	The source of the certificate can be from a file or from the clipboard.
Certificate from Clipboard: -----BEGIN CERTIFICATE----- d99yeS9n2F9pbR1om11291hd9Uy3JOM0GAL7ddYQWBSX/EDR5e4Y0gRv71ED Q81Jok23oeAfbgNVRMEGDWqB9T9G5y42kF1uLokVauud2mNjMS2eBqNVRREE 1jAgghb3dcou5b1zm9y4d9u129ggxk4CPub3J7Ac32b0wQ1W6o1Iwvob1QEF BQ40g95BA2e512ez29p44eT1g10M4F9ATULG9M0A6/qv6Ld6de9F0N02d1 Wp9SLA0Xa0c370dAX2+DyE3ve9G6EDz4ppkXZfheREP0p4HRTzrLpB6Bhd2FVW Ww=REFgD0W-XF9k17R54xom11y2cUkeRDXMlaw1zUTby/1y19eEY9gPRTh1IkX0 b7zC1q7P78dMk7P7vCB8g2a+RaB5Y112wzweb7RUL0EP9qCTs0t6oaS01+R8V2z F2U/so4V3j7R1m8y37a61C1TeeFomBQ31d8x7h3qFVw91G79yK8F3yD0K fndg4g288pnrve1Q9G3Q1Ky4Oenb8= -----END CERTIFICATE-----	Paste the clipboard

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

You May Need A “Trusted Root”

- You'll get this from your CA Provider
- The Trusted Root is proof to that the actual certificate you have was issued by someone trustworthy even though they're not the top level certifier.



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Install The Trusted Root Certificate

- Back to the CA who will give you a lengthy set of instructions to download their trusted root certificate.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

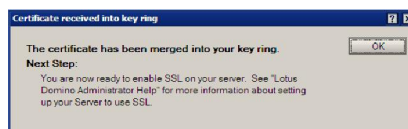
You Can Also Install From .CRT Files

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Finally – You're All Done

- If you had to install trusted root certificates, you may not see this OK screen unless you re-install your actual certificate at the end.
- It is ok to re-install your certificate if you want to be sure

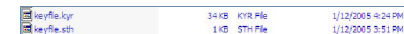


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

What Do You Do Now?

- Copy your .KYR file and another file with the same first name by the extension .STH which you'll find in the same directory – over to your Domino Data directory
- Remember, in Linux, to set its Owner and Group to 'notes' and its permissions to 644 so that the server can read it properly



```
rw-r--r-- 1 notes notes 34K Dec 8 13:19 keyfile.kyr
-rw-r--r-- 1 notes notes 1K Dec 8 13:19 keyfile.sth
```

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

And Finally...

- Reference the .KEY file (Key Ring) in your Internet Sites document for the HTTP site you're setting up!
- You have to restart the http task for this to take effect.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

WEB SITE RULES

These are RESPONSE documents to the website document.
Your best bet is to create them from the open website document using the action button.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

File Protection Rules

- These allow you to set ACLs on file folders in the Domino HTML directory

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Directory Rules

- You can serve content from elsewhere on the server

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Redirection/Substitution Rules

- Substitution rules are invisible to the user

- The user sees:
http://2sig.com/nws/alert1145.html

Web Site Rule	
Basic	Comments Administration
Basics Description: NWS ALERTS Type of rule: Substitution Incoming URL pattern: /nws/* Replacement pattern: /nws/alerts.net/alertsByUniqueKey*	

- Redirection Rules Refresh The Page

Web Site Rule	
Basic	Comments Administration
Basics Description: Type of rule: Redirection ☒ Incoming URL pattern: /Members Redirect to this URL: https://secure.secdigital.com/secdigital/ssi.nsf/welcome?readform&login Send 301 Redirect: ☐ Yes	

- The user sees the full, longer URL

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

HTTP Response Headers

- This is useful for controlling cache headers
 - I tend to set long cache timeouts on files that don't change
- For example, scripts that are "stable" and won't change go in a filetree.nsf database and are set to 30 days cache.

Web Site Rule	
Basic	Comments Administration
Basics Description: Cache JPG Type of rule: HTTP response headers Incoming URL pattern: /filetree.nsf* 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) ☒ Specify as number of days ☐ Specify as date Expires after 30 days Custom headers: Name: Value ☐ Override Name: Value ☐ Override Name: Value ☐ Override	

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Override Session Authentication

- For specific services like traveler or custom web services
 - Allows you to use Session Based Authentication on your site
 - Uses standard authentication on just these locations

Web Site Rule	
Basic	Comments Administration
Basics Description: Type of rule: Override Session Authentication Incoming URL pattern: /sscommms.nsf*	

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

SSO CONCERNS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

How much do you trust the credential provider?

- Users will still expect common services
 - You may no longer be managing a users credentials but your users will still expect some things to work well
- How can user access be revoked?
- If a "Problem" user is accessing your system but authenticating somewhere else, can you lock them out?
- Can you block certain user login ids from being passed from the provider?
- Are you hack resistant?
 - Can the authentication provider be spoofed
 - Can the credential data being passed to you be altered?
 - Does your site expose data from the credential provider that can be used to access other sites?
- Authentication is not Authorization

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

OTHER SERVER ADMINISTRATION SECURITY ISSUES

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

USE the IDVAULT and Keep Passwords in Sync

Just do it already.

IDVAULT will make your phone ring less.

It's easy.

Search for Gabriella Davis's Presentations
on How to set it up and get working on it.
This one is low risk, high reward.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Keep Your Sever Up To Date

- There are script kits available for download pretty easily that automate exploiting security holes.
- I have watched menu driven tools identify server versions, offer a choice of exploits and payloads, and give almost instant command prompt access to DOMINO servers only one revision behind.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Consider a Reverse Proxy

- IBM HTTP Server (IHS) can now run on the same computer as a Domino server and supports Transport Layer Security (TLS)
 - Domino has the option of running the IBM HTTP Server on the same computer as a Domino HTTP server; the purpose of this enhancement is to support the Transport Layer Security (TLS) protocol.
 - Note: This IHS server module is supported only on Windows™.
- A linux box running Apache can also be used as a reverse proxy

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

SOME INI PARAMETERS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Remove Server Header Details

- There is no value in advertising to hackers what you're running
 - INI Setting HTTPDisableServerHeader=1
- Before


```

Response Headers
Cache-control: private
Content-Length: 489
Content-Type: image/gif
Date: Thu, 19 Sep 2013 19:57:26 GMT
ETag: W/"HTAL00E-84NTT1W03PQAwHJ3Q8Y1LTg1HJ
8VbdhY2sV7z1Ba0Vub310Aa=="
Last-Modified: Thu, 19 Sep 2013 07:09:14 GMT
Server: Lotus-Domino
      
```
- After


```

Response Headers
Accept-Ranges: bytes
Content-Length: 45
Content-Type: image/gif
Date: Thu, 19 Sep 2013 20:01:03 GMT
Last-Modified: Wed, 18 Nov 1998 21:12:02 GMT
      
```
- There Are Script Toolkits Which Automate Attacks Using This

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Or....you can get jiggy with it....

- INI Setting HTTPDisableServerHeader=0
- + Site Rule

```

Response Headers
Cache-control: no-cache
Connection: close
Content-Length: 15998
Content-Type: text/html; charset=US-ASCII
Date: Tue, 24 Sep 2013 08:31:03 GMT
Example: Found
Expires: Wed, 25 Sep 2013 23:59:59 GMT
Last-Modified: Tue, 24 Sep 2013 08:31:01 GMT
Server: Andrews-Super-Server
      
```

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)
	☒ Specify as number of days ☐ Specify as date
Expires after:	1 days
Custom headers:	Name: Server Value: Andrews-Super-Server ☒ Override

- **WARNING:** This isn't as safe
- **At least make sure you include ALL of the response codes!**
- http://en.wikipedia.org/wiki/List_of_HTTP_status_codes

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

DominoNoBanner=1

- Default in newer versions is 1 but check
- When set: DominoNoBanner=0

```

Headers Preview Response Cookies Timing
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<!-- Lotus-Domino (Release 8.5.3FP3 - November 15, 2012 on Linux for Intel) -->
<head>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=US-ASCII">

```

- When set: DominoNoBanner=1

```

Headers Preview Response Cookies Timing
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=US-ASCII">
<meta name="viewport" content="width=device-width, height=device-height" />

```

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

A Couple of other new ones in Domino 9

- iNotes_WA_CalViewShowPrivateEntry
 - Fixes a problem where Private All Day events and Anniversaries which were marked Private, are visible to a delegated user. New notes.in: ...
- QUOTE_LTPA_COOKIE=1
 - Added a notes.ini, QUOTE_LTPA_COOKIE, which places quotes around the value of the cookie. This makes the LTPA cookie compliant with RFC 2109 and RFC...
- DominoValidateRedirectTo=1
 - Addresses an exploit related to hacking the "redirectto" parameter in the login process. This looks ugly.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Antivirus Software

- Non-Domino Aware
 - Can stop your server being corrupted if an exploit does get it
 - Products like Norton 360 no longer rely on virus definitions
 - They watch for any executable that tries to run that isn't already known
 - Make sure you EXCLUDE the Domino Data directory
 - Set Domino to use it's own "Temp" location
 - Exclude that "temp" location from the antivirus scan
- Domino Aware
 - Useful particularly if you accept files and attachments

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

APPLICATION LEVEL SECURITY

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

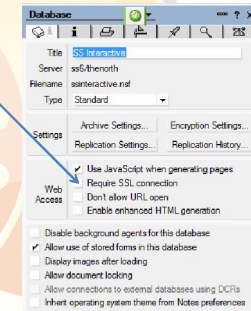
DATABASE PROPERTIES

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Require SSL Connection

- Will force browser access only with an HTTPS connection even if the website allows clear text access.

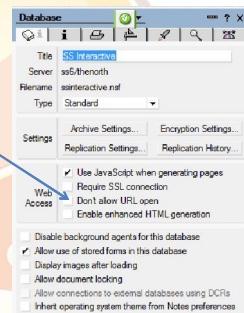


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Don't Allow URL Open

- Excludes the entire database from being accessed by the HTTP task.

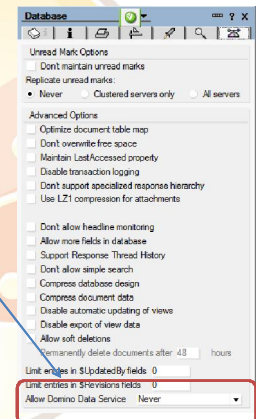


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Allow Domino Data Service

- NEW!**
- Enables a JSON API access to documents that can be used to expose fields and values on documents you may not want



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

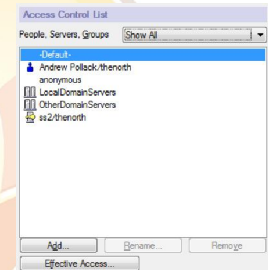
DATABASE ACL SECURITY SETTINGS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Anonymous vs. Default ACL

- If a user is authenticated but not specifically listed in the ACL or in a group in the ACL they get DEFAULT access
- If a user is NOT authenticated they get "anonymous" access
- If you do not have an entry for "anonymous" then unauthenticated users get DEFAULT access

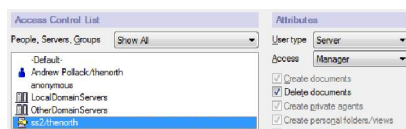


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Assign "User Type"

- The "User Type" prevents someone from spoofing a person document with the name of a server and getting too much access
- Other ways to exploit this include SSO solutions

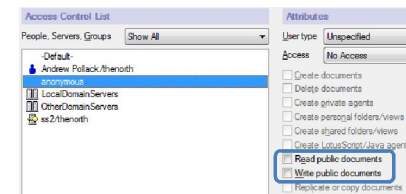


AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Read/Write Public Documents

- Forms and documents saved from those forms may be marked "public access" to allow use by users who otherwise do not have access to read or create in a database



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Maximum Internet Name and Password

- This is a great way to limit access with a browser even if you have access as the designer or manager of a database.

Maximum internet name and password Editor

- If you do your managing from your Notes client but sometimes access from the browser when on the road, this can save you a nightmare if someone gets your session at the coffee shop

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

USING ENCRYPTED FIELDS

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Use Case : Order Form on My Website

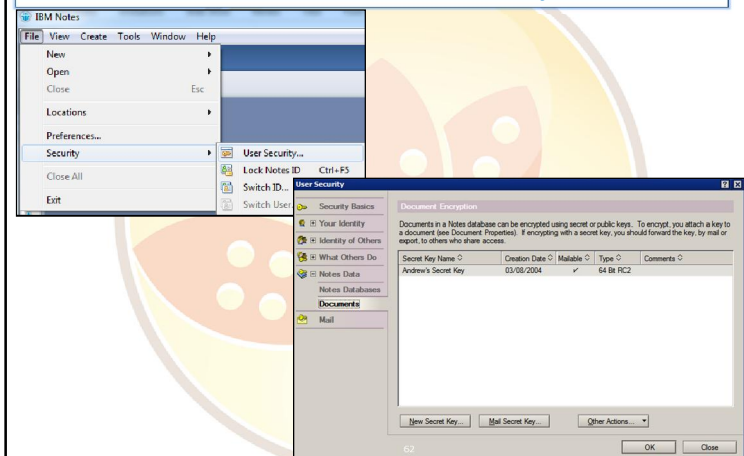
- The fields on this form are encrypted
- The PUBLIC key is stored on the form
- The PRIVATE key does not exist on the server
- Even if the server was stolen, the data could not accessed

Credit Card Information	
Credit Card Type	-- not selected --
Credit Card Number	
Expiration Date	Month: -- not selected -- Year: -- not selected --
3 or 4 digit safety number (if applicable)	

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Create a "Shared Private" Key



AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Store the PUBLIC Key On The Form or Document

The image shows two screenshots of the Domino security interface. The left screenshot is for a 'Form' and the right is for a 'Document'. Both show the 'Default read access for documents created with this form/document' set to 'All readers and above'. Under 'Who can create documents with this form/document', 'All authors and above' is selected. In the 'Default encryption keys' section, '128-bit AES Shared Secret Key' is checked. In the 'Encryption Keys' section, 'Secret Encryption keys' are set to 'None', and 'Public Encryption keys' are set to 'Andrew's Secret Key'.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Enable Encryption for this Field or Document

The image shows two screenshots of the Domino security interface. The left screenshot is for a 'Field' and the right is for a 'Document'. Both show the 'Who can read this document' set to 'All readers and above'. In the 'Security Options' section, 'None' is selected. In the 'Encryption Keys' section, 'Secret Encryption keys' are set to 'None', and 'Public Encryption keys' are set to 'Andrew's Secret Key'. A blue arrow points from the 'Field' screenshot to the 'Document' screenshot, indicating the same settings are applied to both.

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

A FINAL NOTE: MAKE SECURITY A PRIORITY

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Don't Make Security Choices On The Fly

- Requires all developers to understand all the options and implications
- Requires business content owners to pay for expense of implementation
- Results in a complete lack of standards for securing applications

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Create a Criteria for Evaluating Applications

- Based on content
 - o Employee Data
 - o Customer Data
 - o Competitive Secrets
- Based on purpose
 - o Decision Support Data
 - o Testing Results
 - o Regulatory Requirements

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Apply Security Standards Based on Ratings

- Rate application security requirements on your own scale
 - Green / Yellow / Red / Infrared / Ultraviolet
 - Public / Customer / Internal / Management / CEO / Burn Immediately
 - Pick your own scale
- Match Security Choices to Applications
 - Create a security requirements document for each level on your application security scale
 - Define which minimum security choices must be used for each level on the scale and which may not
 - Avoids conflicts at design time between developers and business units where the cost of security is played off against the risk

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren

Fill Out Your!
Evaluations

Now Go Forth and Be Secure

Ask Questions Now
Or Contact Me Later
andrewp@thenorth.com
<http://www.thenorth.com>
Twitter: @FirefighterGeek

AdminCamp 2013

Notes & Domino - Das Tool der Zukunft, seit 25 Jahren