

OPENNTF WEBINARS

March 16, 2023

**OpenNTF March, 2023 Webinar:
TOTP - This is the Way**



AGENDA

- Welcome
- Presentation
Keith Brooks
- Q and A



THANKS TO THE OPENNTF SPONSORS

- HCL made a contribution to help our organization
 - Funds these webinars!
 - Contests like Hackathons
 - Running the organization
- Prominic donates all IT related services
 - Cloud Hosting for OpenNTF
 - Infrastructure management for HCL Domino and Atlassian Servers
 - System Administration for day-to-day operation



THIS IS OUR COMMUNITY

- Join us and get involved!
- 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



UPCOMING EVENTS

- Engage User Group Meeting
The Future is NOW
April 24-26
Felix Meritis
Amsterdam, Netherlands
- MWLUG
 - In Person!
 - Save the Date, August 30 and 31



ADMIN REPAIR CAFES

- Bring your topic!
- Discuss ideas on how to tackle the issue
- Two Scheduled this month:
 - Wednesday, March 22 at 12:00PM Eastern US time (EDT)
 - (APAC) Thursday, March 23 at 9:00PM Eastern US time (EDT)



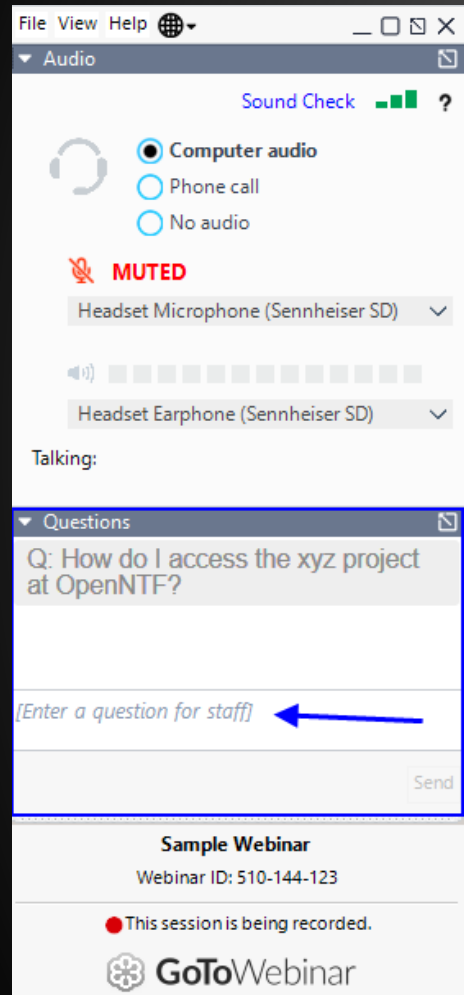
NEXT WEBINAR

April Webinar: Domino REST API by HCL

April 20th



ASKING QUESTIONS



- First Question – Will this be recorded?
 - Yes, view on YouTube!!!
 - <https://www.youtube.com/user/OpenNTF>
- Use the Questions Pane in GoToWebinar
- We will get to your questions at the end of the webinar
- The speakers will respond to your questions verbally
 - (not in the Questions pane)
- Please keep all questions related to the topics that our speakers are discussing!!!
- Unrelated Question => post at:
 - <https://openntf.org/discord>



PRESENTATION

OpenNTF March, 2023 Webinar: TOTP - This is the Way
Keith Brooks



OPENNTF WEBINARS

March Edition

Presented by Keith Brooks

@LotusEvangelist

HCL Ambassador

IBM Champion

OpenNTF Contributor





TOTP THIS IS THE WAY

Keith Brooks
CEO - B2B Whisperer
keith@b2bwhisperer.com

Keith Brooks



Blog: <https://blog.vanessabrooks.com>

keith@b2bwhisperer.com

@Lotusevangelist

Certificate Exams Writer 2012-2014, 2022



2013-2019

IBMCHAMPION 
noun /ˈtʃæmp-i-ən/ 
They're experts. They're leaders.

HCL Ambassador

2019 - 2023

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

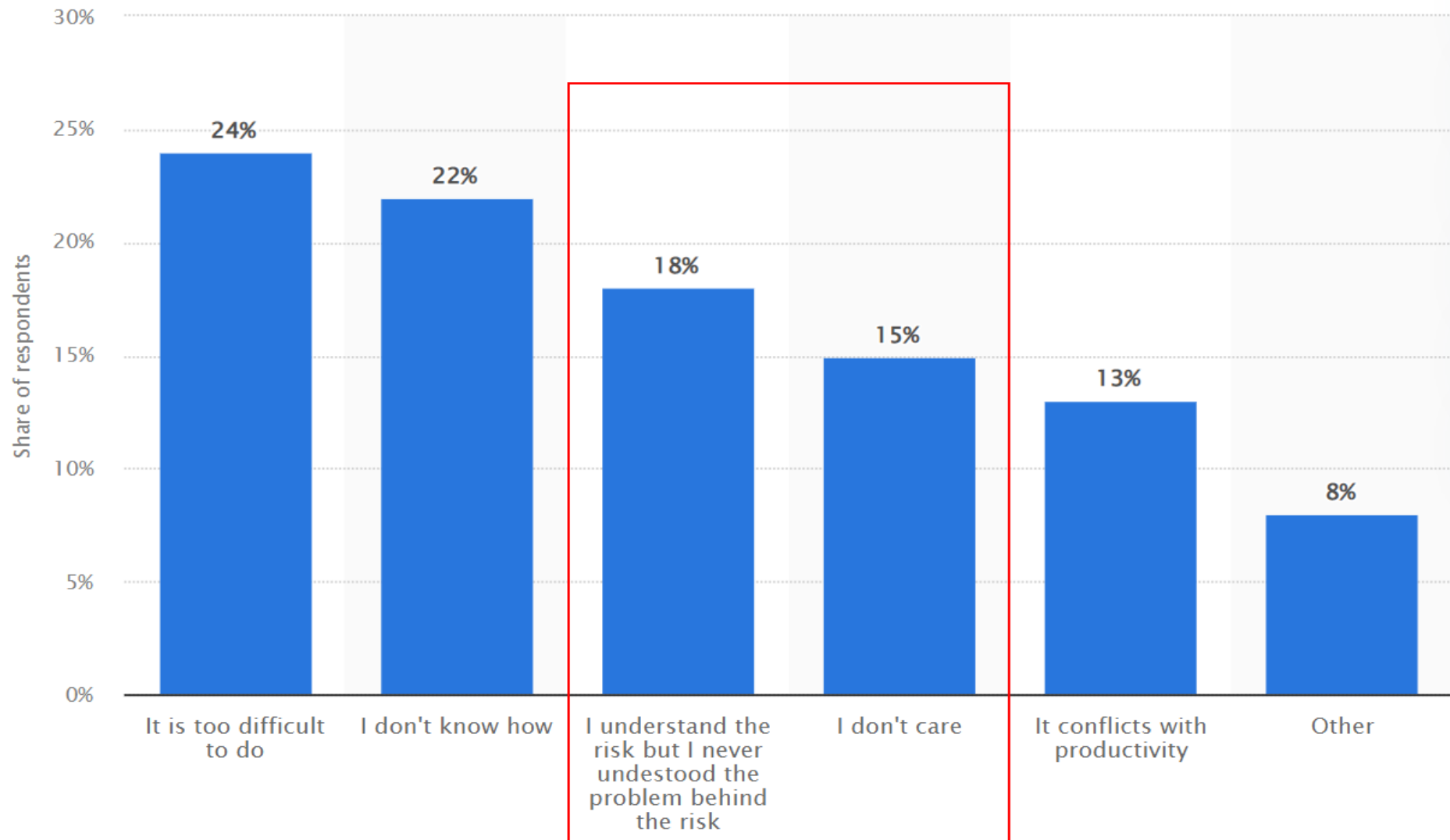
User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything



<https://www.statista.com/statistics/1305250/reasons-for-not-using-mfa-us-uk/>

What is this MFA Thing?

- MFA (Multi-Factor Authentication)
- OTP (One Time Password)
- HOTP/HMAC OTP (Hash-Based Message Authentication Code/Counter)
- TOTP (Time-Based One-Time Password)
- Are Notes ID files a form of MFA?
- Is SSO a form of MFA?
- Is SSO a secure idea?
- Why do you, or your customers, need TOTP?

Insurance/Compliance



Reasons for TOTP	Reasons Against TOTP
Insurance/Compliance/Security	What security does it add if the MFA is on the phone?
	Increase in Support Tickets due to lockouts
	Must login every time to check for mail, but this can be adjusted
	ID Vault may not be up to date for everyone to have their ID files there
	SAML is not supported for TOTP

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

This is the way

TOTP for Domino

Is URL defined,

NOT

Server or Application defined!

The setup and installation is **Server
defined,**

but how a user interacts with TOTP,
starts with a URL,

ALWAYS!

Planning is a MUST

- iNotes is the most common TOTP requirement
 - iNotes Redirector works with TOTP
- Web applications also are a top TOTP requirement
- What if you also have Traveler/Verse users?
 - https://help.hcltechsw.com/traveler/12.0.2/mobile_support_totp.html



- You may need some secondary domains(Internet Site Documents) because Traveler users will not want to log in every time to check their mail.

Applications vs Mail for TOTP

Application / Product	Internal / External	TOTP Required	Website URL Example (Need a web site document per URL)
Verse/iNotes	Internal	No	MAIL.ABC.COM
Verse/iNotes	External	Yes	WEBMAIL.ABC.COM
Application	Internal	No	APPN.ABC.COM
Application	External	Yes	APPT.ABC.COM
Traveler/Verse	External	Yes/No	TRAVELER.ABC.COM
NOMAD	External	Yes/No	NOMAD.ABC.COM DOESN'T WORK WITH DOMINO TOTP

Remember to update your outside and inside, DNS and Firewall

Who's ready for NOMAD?

Domino TOTP is **NOT supported** by
NOMAD

NOMAD
and
TOTP

NOMAD will work with some other
TOTP offerings, namely HCL's SafeLinx.

If you want DOMINO TOTP to work
with NOMAD,
go vote for it:

<https://domino-ideas.hcltechsw.com/ideas/DMA-I-179>

TOTP Prerequisites

- User's IDs need to be in the ID Vault that is set up and working correctly
- Server must be R12
 - Mail templates do not need to be on R12, but should be if possible
- Need a cert.id file accessible in the server Data directory
 - If putting it there now, you may need to restart the server to recognize it properly
- SSL should be enabled. Most companies have done this. If you have not, creating SSL certificates is included in R12 for free*

Mail Users, ID Vault ID Files, and TOTP

User	Type of User	ID File in Vault	Next Steps
Internal	Mail (Notes/iNotes/Verse)	Yes	Set up a URL, Set up TOTP
External	Mail (Notes/iNotes/Verse)	Yes	Set up a URL, Set up TOTP
Internal	Mail (Notes/iNotes/Verse)	No	Set up a URL, Create ID Vault, upload ID via .csv or wait for login [^] , Set up TOTP
External	Mail (Notes/iNotes/Verse)	No	Set up a URL, Create ID Vault, upload ID via .csv or wait for login [^] , Set up TOTP

[^]=To enable the use of ID vault for iNotes users, select Yes for **Allow Notes-based programs to use the Notes ID vault** on the ID Vault tab of the Security policy settings document.

App Users, ID Vault ID Files, and TOTP

User	Type of User	ID File in Vault	Next Steps
Internal	Applications Only	Yes	Set up a URL, Set up TOTP
External	Applications Only	Yes	Set up a URL, Set up TOTP
Internal	Applications Only	No	Set up a URL, Create ID Vault, upload ID via .csv*, Set up TOTP
External	Applications Only	No	Set up a URL, Create ID Vault, upload ID via .csv*, Set up TOTP

*= Must be registered as a Notes user with a mail file and home server

- The .csv file and details to correct everything is in a blog post I wrote:
- <https://blog.vanessabrooks.com/2021/10/sntt-totp-needs-id-file-in-id-vault-to.html>
- You will need to write some simple agents, as explained, and delete unwanted mail files in the mail folder.
- If you agree HCL could do better and fix this for us, go vote on the Aha request here: <https://domino-ideas.hcltechsw.com/ideas/ADMIN-I-99>

How to put ID Files in the ID Vault

Most common way is once the ID Vault is running, the IDs go there automatically when created or recertified

But what if you already have 1,000s of people registered and now created the ID Vault?

The process is a mix of Registering users via a .txt file coupled with some automatic settings

Due to time constraints, I have provided links to blog posts from myself and Ales Lichtenberg that explain how to do this and can be found at the end of this presentation

Mobile Client Support and Limits for TOTP Authentication

TOTP Support requirements

- HCL Verse for Android 12.0.0 and later clients. HCL Verse for iOS 12.0.2 and later clients.
- Traveler server endpoint configured for TOTP authentication (requires HCL Domino 12.0.0 and higher).
- 3rd party signed SSL certificates for the Traveler server endpoint.

Limitations

- TOTP authentication support is limited to the HCL Domino support. Authentication proxies that may provide multi-factor authentication are not supported.
- The HCL Companion or To Do applications for iOS do not support TOTP Authentication.
- TOTP authentication is not supported by clients that use the Microsoft Exchange ActiveSync protocol, including the Apple iOS Mail client.
- The HCL Traveler for Outlook clients does not support TOTP Authentication.
- TOTP authentication is not available when working with encrypted mail. The end user is prompted for their Notes ID password.
- For HCL Verse Android, application passwords are not supported when configured for TOTP authentication. A Traveler server setting or policy setting requiring application passwords will be ignored.

No
SAML
or
Basic
Authentication
Support

TOTP is **NOT** available for Basic Authentication or SAML Session Authentication configurations.

https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_enabling_for_server_through_internetsite.html



4. In the **Session authentication** field, select **Single Server** or **Multiple Server (SSO)**.



Note:

- TOTP is not supported with Basic authentication or with SAML.

SAML and TOTP

One customer wants to use SAML for users from Windows computers and TOTP for other devices (Mobile/tablets).

They will end up with multiple URLs since TOTP does not support SAML.

It is easier if you are talking about specific customers or applications.

Not simple if random people in your company or customers need it.

Your
Certifier
ID
and
Password
is
Required

The cert.id needs to be placed in the Domino\data directory to set up TOTP. It can be removed once TOTP is setup.

Let us presume you have no idea where your Certifier ID is, or maybe you lost the password to it.

What do you do now? TOTP Requires it for the setup

If you said, you need to create a new certifier, migrate everyone to it, or cross-certify everyone for the moment, you win this round.

OR

If you had the CA setup there is a way to reverse out your ID and passwords.

Windows Server Update And Domino R12 Update

If you follow Best Practices and maintain at least a Dev and Prod environment, great, but some of you live dangerously.

If you are replacing your old Windows server and upgrading to R12, you may find the TOTP process easier while testing with a clean environment.

You can copy the R9 files to the R12 server and configure everything as needed, just do not turn on replication with the old server until you are ready to cut over the data. **You have been warned!**

Once you build a new server to migrate the old data, how do you manage the ID Vault on 2 servers and versions?

Your ID
Vault Age
and
Password
are
Important

Remember When You Created Your ID Vault?

1. Guess what?

- **It expires after 10 years!** WTF? Right? Go renew it!

https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0037905

https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0076358

2. At the time you created an ID Vault ID file, you also created a password at the same time.

- Why do you need it now?
- You will need the password for your ID vault ID file in order to replicate your ID vault to your new R12 server.
- Why would I do that?

ID Vault Replication and Building a New Server

You may want to replicate the ID Vault from the old one:

- https://help.hcltechsw.com/domino/11.0.0/conf_addingorremovingidvaultservers_t.html

But you may run into a snag looking for a lost id vault ID and password

- https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0038943

The below won't help either. You need the original password

- https://help.hcltechsw.com/domino/10.0.1/conf_changingthepasswordonthevaultidfile_t.html

Update Your ID Vault Admins

Because the ID Vault is so integral to TOTP, you should review the policies, settings, and especially the Administrators assigned to the ID Vault.

Now is an excellent time to update your Admins listed.

Password Reset:

In the Admin client, open the names.nsf – Security-ID Vaults-Password Reset Authority

Add/Remove Vault Administrators:

In the Admin client, open the names.nsf – Security-ID Vaults- Manage- Add or Remove Vault Administrators

TOTP for Docker Requires

- Create or replicate an ID vault on the Domino on Docker server.
 - All TOTP-specific configuration is saved in users' ID vault documents.
- Make sure that the websites or virtual servers within the Docker container are accessible from outside the container.
- HCL recommends running the Domino HTTP server with a default Internet site, TLS enabled, and Server Name Indication (SNI) enabled to connect to a web site or host name.

Configuring cross- domain TOTP authentication

You can enable TOTP authentication for users in a secondary Domino domain.

When the configuration is complete, users registered in the secondary domain can set up and use TOTP authentication configured in the primary Domino domain.

NOTE:

Domino Web servers from both domains participating in TOTP authentication must run at least Domino 12.

At least one ID vault server in the primary or secondary domain must run at least Domino 12.

There are steps to run in both the primary and secondary domains.

Configuring the Primary Domain for cross- domain TOTP Authentica tion

1. Add the following notes.ini setting to all Web servers in Domain1 and to the ID vault server in Domain1: `ENABLE_IDV_CROSSDOMAIN_AUTHENTICATION=1`
2. Ensure the Domain1 Domino directory has a Notes cross-certificate at the /Org level for Domain2 that establishes trust.
3. Configure DA (directory assistance) to look up names in the Domain2 Domino directory.
 - Create a directory assistance database (if not created already) on a server in Domain1.
 - Add a Directory Assistance Document for Domain2. The following fields in the document are required
 - On the **Basics** tab: **Domain type** Select **Notes**.
 - **Domain name** Specify the Domino domain of the secondary directory
 - **Make this domain available to** Select **Notes Clients & Internet Authentication/Authorization**
 - **Enabled** Select **Yes**.
4. On the Naming Contexts (Rules) tab, select Enabled > Yes and Trusted for Credentials > Yes for at least one rule that applies to Domain2.
5. On the **Domino** tab, specify the replica of the Domain2 Domino directory on the Domain2 administration server.
6. Configure TOTP authentication for Domain1 like normal.
7. Replicate the Domain1 Domino directory and Directory Assistance database to all participating Web servers in Domain1.

Configuring the Secondary Domain for Cross- Domain TOTP Authentica tion

1. Add the following notes.ini setting to all Web servers in Domain2 and to the ID vault server in Domain2: `ENABLE_IDV_CROSSDOMAIN_AUTHENTICATION=1`
2. Ensure that the Domain2 Domino directory has a Notes cross-certificate at the /Org level for the Domain1 /Org that establishes trust.
3. Create a replica of the Domain1 Domino directory on the ID vault server for Domain2.
4. Configure directory assistance on the ID vault server for Domain2 to look up names in its local replica of the Domain1 Domino directory.
 1. Create a directory assistance database (if not created already) on the ID vault server for Domain2.
 2. Add a Directory Assistance Document for the Domain1 Domino directory. The following fields in the document are required
 - On the **Basics** tab: **Domain type** Select **Notes**.
 - **Domain name** Specify the Domino domain of the secondary directory.
 - **Make this domain available to** Select **Notes Clients & Internet Authentication/Authorization**
 - **Enabled** Select **Yes**.
 - On the Naming Contexts (Rules) tab, select Enabled > Yes and Trusted for Credentials > Yes for at least one rule that applies to Domain2.
 3. On the **Domino** tab, specify the replica of the Domain1 Domino directory that you created on the ID vault server in Domain2.

Configuring the Secondary Domain for Cross- Domain TOTP Authentica- tion Continued

4. Run the following commands from the server console of the ID vault server to create Multi-Factor Authentication Certificates for the Domain1 Org and the Domain2 Org using each one's respective certifier id.

```
mfamgmt create trustcert <Notes DN1 to allow>  
<certifier ID1 file> <certifier1 password>
```

```
Example: mfamgmt create trustcert */O=Org1 cert1.id P@ssword1
```

```
mfamgmt create trustcert <Notes DN2 to allow>  
<certifier ID2 file> <certifier2 password>
```

```
Example: mfamgmt create trustcert */O=Org2 cert2.id P@ssword2
```

These certificates are created in the Domain2 Domino directory.

Replicate the Domain2 Domino directory and Directory Assistance database to all participating ID vault servers in Domain2.

Common Question

TOTP requires the ID vault to have the V12 design and be running on a V12 server.

Will this cause problems for other servers with the ID vault not yet upgraded to V12?

Yes, and No.

HCL says it is fine.

- My customers have not been able to do this without issues.
- You can run an ID Vault from another server in conjunction with TOTP on a different server.
- As long as both servers are R12 AND their templates have been updated for **ID Vault, DOMCFG and the Directory**

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

Configuration Step 1

Go to the server console (easier from the Admin client) and after putting the cert.id on the server type:

- `mfamgmt create trustcert */O=domainname cert.id certidpassword`
- Replicate the Directory across your domain
- In the Directory, check the Certificates view for a Multi-Factor Authentication Certificate section
 - From a server console type: `show idvault`
 - Look for the following:
 - Administration Server: DOM1/Domain
 - /DOMAIN trusts this vault
 - /Domain trusts /Domain for MFA

```
COMMAND SENT: sh idvault
ID Vault /VBI_ID (IBM_ID_VAULT\VBI_ID.nsf)
Vault Name: /VBI_ID
Description: VBI ID Vault
Administrators: Keith Brooks/VBI
Servers: Music/Server/VBI
Administration Server: Music/Server/VBI
/VBI trusts this vault
/VBI trusts /VBI for MFA
Setting VBI_IDVaultSetting uses this vault
```


Configuration Step 2

1. From the Admin client, open the Configuration tab
2. Go to the Messaging section
3. Open the Default Configuration Settings document (or the server specific one that will handle the TOTP)
4. Open the Security tab
5. Configure the MFA options (See next screen for example)
6. Save the page and close it

of Devices:
pc, phone, ipad

Select the one
you require

Configuration Settings

- Basics
- Security
- Client Upgrade
- LDAP
- Router/SMTP
- MIME
- NOTES.INI Settings
- Help

Multi Factor Authentication

Time-based one-time passwords (TOTP) for web authentication: Enable

Allow emergency scratch codes: Yes

Email scratch codes to a user: Yes

Maximum number of secrets: 3

Algorithm: HMAC-SHA256

Issuer: Your Domain

Internet Password Verification

☒ Check internet password in directory
☐ Check internet password in vault
☐ Check vault first, then directory

Internet Lockout

Enforce Internet Password Lockout: Yes

☒ Also enforce lockout based on IP address
☐ Count user name failures also as IP address failures

Log Settings: ☒ Lockouts ☒ Failures

Default Maximum Tries Allowed: 5

Default Lockout Expiration: 10 Minutes

Default Maximum Tries Interval: 1 Days

Server ID Protection on Windows Servers (12.0 and later)

Server ID protection: Use OS credentials

This supports
Google, PingID.
Authy, Duo,
Microsoft use
HMAC-SHA1

Configuration - Step 3 (Web Site Document)

From the Directory go to the Configuration-Web-Internet Sites

Go to the Configuration tab

Go to the Security tab

Save your changes

In the web site document go to the Domino Web Engine tab

In the Domino Access Services section select TOTP from the drop down

Select the TOTP option in both Name and Password fields

Set Session Authentication to Single Server

In the Allowed Methods section, you must check Delete and Put

Name & password: ☐ Yes ☐ No ☒ Yes with TOTP
TOTP option available if Session authentication is Single or SSO.

Allowed Methods

Methods:

<input checked="" type="checkbox"/> GET	<input checked="" type="checkbox"/> POST	<input checked="" type="checkbox"/> TRACE	<input checked="" type="checkbox"/> DELETE
<input checked="" type="checkbox"/> HEAD	<input checked="" type="checkbox"/> OPTIONS	<input checked="" type="checkbox"/> PUT	<input type="checkbox"/> PATCH

WebDAV: ☐ Enable

Domino Access Services

The following setting is a place holder for services provided by an external plug-in.

Enabled services: ☒ TOTP, TravelerAdmin

Edit Web Site Web Site... TOTP Configuration Check

Web Site VerseTOTP

Basics | Configuration | Domino Web Engine | Security | Comments

HTTP Sessions

Session authentication: Single Server

Idle session timeout: 500 minutes

Configuration Step 4A (Secure Mail Operations)

Note: When you enable this feature, the ability for iNotes users to upload and download their IDs to and from the vault is disabled.

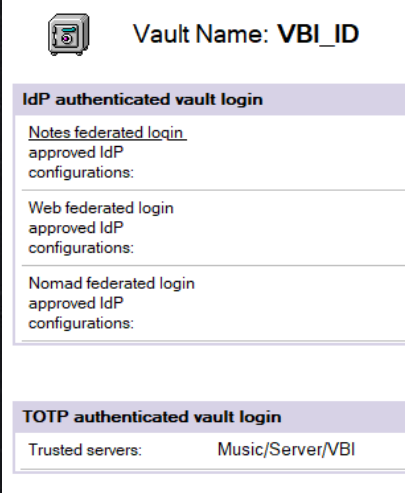
- Open the Security Settings Policy document and click the ID Vault tab.
- In the section TOTP-based ID Downloads, select Yes in the Allow TOTP authentication with the ID vault field.
- To allow web users who do not use TOTP to continue downloading their Notes IDs for secure mail operations, select Yes in the Allow password authentication with the ID vault.
- To require all web users to use TOTP to download their Notes IDs, select No.

TOTP-based ID Downloads:	
Allow TOTP authentication with the ID vault:	<input type="text" value="Yes"/>
Allow password authentication with the ID vault:	<input type="text" value="Yes"/>

Configuration Step 4B (Secure Mail Operations)

In the vault Configuration document of the idvault.nsf (IBM_ID_Vault folder), specify the servers that use the ID vault and are enabled for TOTP and secure mail operations.

- Open the vault database.
- Open the Configuration document.
- In the TOTP authenticated vault login section, specify all of the Domino web mail server names in the Trusted servers field.



The screenshot shows the configuration document for the vault named 'VBI_ID'. It features a vault icon and the title 'Vault Name: VBI_ID'. The document is divided into two main sections: 'IdP authenticated vault login' and 'TOTP authenticated vault login'. The 'IdP' section contains three subsections: 'Notes federated login', 'Web federated login', and 'Nomad federated login', each with a label 'approved IdP configurations:'. The 'TOTP' section contains a 'Trusted servers:' field with the value 'Music/Server/VBI'.

Vault Name: VBI_ID	
IdP authenticated vault login	
<u>Notes federated login</u> approved IdP configurations:	
<u>Web federated login</u> approved IdP configurations:	
<u>Nomad federated login</u> approved IdP configurations:	
TOTP authenticated vault login	
Trusted servers:	Music/Server/VBI

Configuration Step 5A (The TOTP Login Form)

NOTE: If you have a domcfg file, you can skip this and go to the next page

How to Create the Domino Web Server Configuration database (DOMCFG.NSF):

1. From the Domino Administrator, choose File > Application > New
2. Enter the name of the Web server in the Server field
3. Select Show Advanced Templates
4. Select the Domino Web Server Configuration template (DOMCFG5.NTF)
5. Enter a Title for the database
6. For the File name field, you **MUST** enter DOMCFG.NSF
7. Click OK

Configuration Step 5A (The TOTP Login Form)

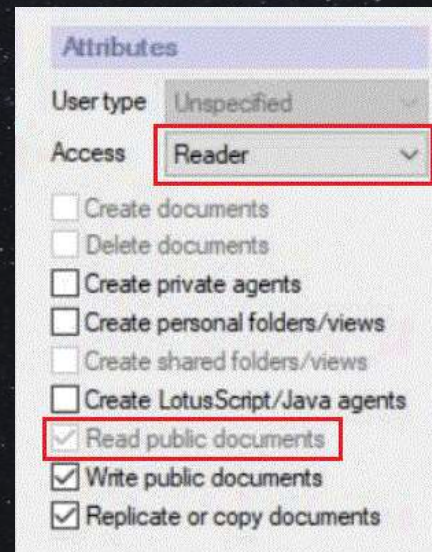
Need to Specify the \$\$LoginUserFormMFA as the log-in form:

- Open the DOMCFG.NSF and open the Sign In Form Mappings view.
 1. Click Add Mapping.
 2. Under Site Information, choose either: All Web Sites/Entire Server or Specific Web Sites/Virtual Servers
 - To use the custom log-in form for all Web Sites on the server, or for the entire Web server
 - Or to map the custom log-in form to specific Web Site documents or Virtual Servers.
 - Under Form Mapping, for Target Database specify DOMCFG.NSF
 - And for Target Form, specify \$\$LoginUserFormMFA.

Form Mapping	
Target Database:	domcfg.nsf
Target Form:	\$\$LoginUserFormMFA

Configuration
Step 5C
(ACL and
Restart)

Make sure you set the ACL properly
for the domcfg.nsf



And then restart your ID Vault
server

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

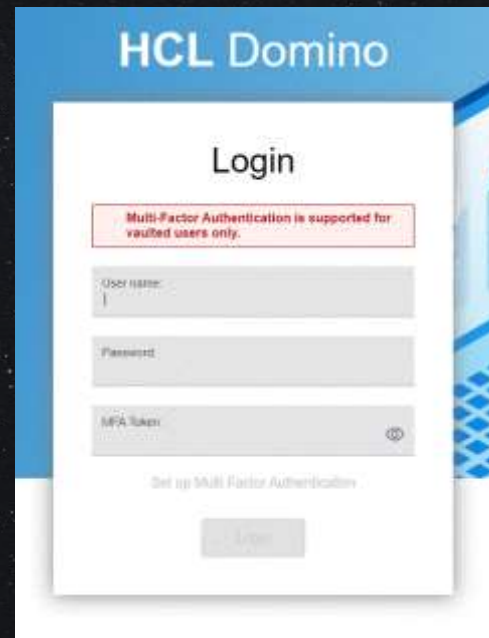
Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

What was New for TOTP in 12.0.1

- TOTP is supported for HCL Verse 2.2 users.
- When users who do not have Notes IDs in the ID vault try to log in when TOTP is enabled, they now see the message:
 - Multi-Factor Authentication is supported for vaulted users only.



Notes.ini Optional Settings

These
Require a
Server
Restart

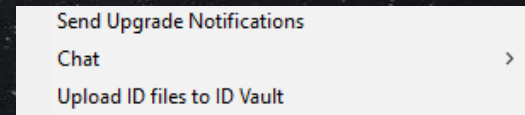
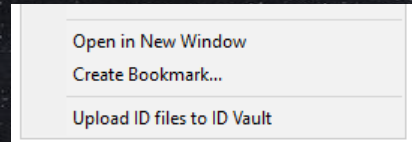
Setting	Description
TOTP_STEPSIZE= <i>seconds</i> If you feel your users require more time, this is where you change the default	How long, in seconds, a TOTP token is valid. Without the setting, tokens are valid for 30 seconds before they expire. NOTE: Not all TOTP applications honor this setting.
TOTP_TIMESKEW_STEPS= <i>TOTP_STEPSIZE factor</i>	Additional time allowed to accommodate time differences between the ID vault server and the user devices. Specify the TOTP_STEPSIZE factor to add before and after the TOTPStepSize. By default, the value is a factor of 1, meaning assuming default TOTP_STEPSIZE value of 30 seconds, by default an allowance of 30 seconds is added before and after.
ENABLE_IDV_CROSSDOMAIN_AUTHENTICATION=1 If you need DA Cross-Domain lookup support add this one	If directory assistance is configured for cross-domain directory lookups, add the notes.ini setting to your Domino servers. Then, when a user accesses a Domino server and the user is registered in a secondary domain, the server is able to access the ID vault in the secondary domain to manage TOTP authentication.
DEBUG_TOTP=2 DEBUG_IDV_TOTP_TRANS=1 DEBUG_IDV_TRUSTCERT=1 Very Detailed info to help you	To help troubleshoot TOTP problems, use these settings to enable debug logging in console.log.

Some IDVault Debug Parameters

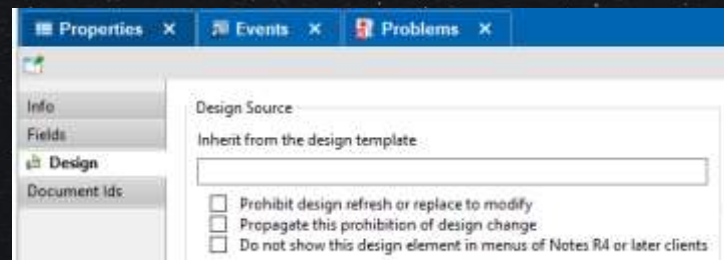
- `DEBUG_IDV_CONNECT=1` (Details each ID Vault Connection)
- `DEBUG_IDV_API=1` (checks ID Vault API access)
- `DEBUG_IDVAULT_SERVER_SELECTION=1` (Traces search for an ID Vault Server)
- `DEBUG_INETPWD_CHECK=1` (checks internet password)
- `WEBAUTH_VERBOSE_TRACE=1` (authentication, access, and LDAP verifications)
- `DEBUG_SAML=31` (full SAML debug)
- `DEBUG_IDV_QVAULT=3` (1 does not help, use 3)
- `DEBUG_IDV_TRACE=1` (ID Vault Client behavior)
- `DEBUG_IDV_TrustCert=1` (ID Vault trust certificate validation)
- `DEBUG_IDV_ViewUpdate=1` (force update the IDFile view in the Vault on each look up of the user in the Vault)
- `DEBUG_IDV_IDP_CONFIG=1`

Unable to Upload ID Files

If you do not see “Upload ID Files to ID Vault” when you right-click on a user in the Directory, or when selecting Actions from the menu bar, you may have a “no update People view” customization in your directory



One way to fix this, open your Directory in the Designer client and find the People View and, in the Properties, – Design box below, uncheck “Prohibit design refresh or replace to modify”

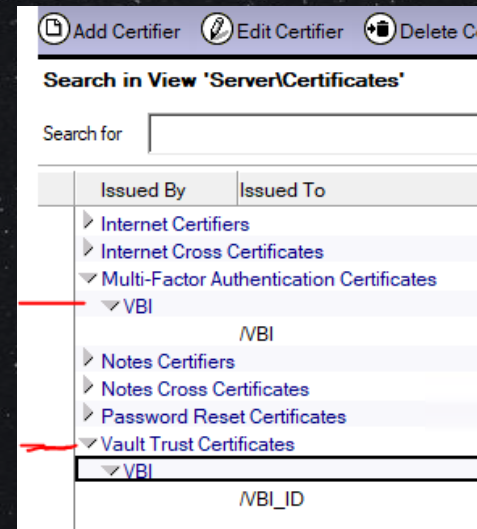


ID Vault Creation Error

If you see this message in your server console or logs, your ID Vault was not properly setup.

```
Administration Server: DOM1.
Invalid or nonexistent document: No certifiers found that trust vault.
Invalid or nonexistent document: No certifiers that trust vault. Vault trust any password reseters
```

1. Delete the Vault Trust and Multi-Factor certificates, Security-Certificates section of the Directory



2. Then recreate the ID Vault and run the mfamgmt command again

Another ID Vault Error Message



Server Error: Missing or invalid Password Reset Trust certificate. Check the log file for details.

OK

This points to ID Vault corruption

1. Delete the Vault Trust and Multi-Factor certificates, Security-Certificates section of the Directory
2. Then recreate the ID Vault and then run the mfamgmt command

Issued By	Issued To
Internet Certifiers	
Internet Cross Certificates	
Multi-Factor Authentication Certificates	
VBI	
	/VBI
Notes Certifiers	
Notes Cross Certificates	
Password Reset Certificates	
Vault Trust Certificates	

If
The MFA
Is
Not
Allowing
User Setup

- You may see the login page, that is preset in the domcfg.nsf
- But it may not take you to the setup after you try to login with your name and password
- Or if you try to click on MFA it will not do anything
- This means you may have to redo the console command: mfamgmt create trustcert
- And/or you may need to say **NO** in the Configuration document where it asks “Allow TOTP authentication with the ID vault field”

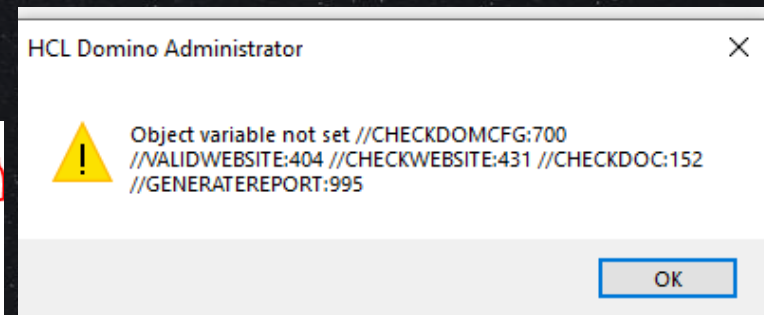
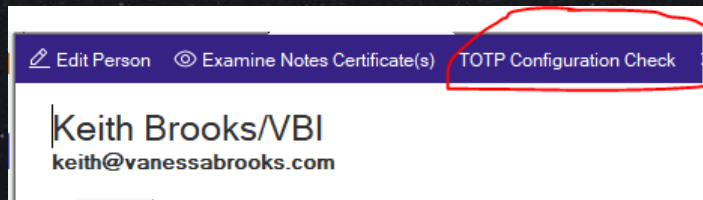
Odd Issue with Some Environm ents

If the server reports an error like one of these when you try to check the TOTP Configuration:

TOTP Configuration Checker Report

Checking Web Site MFA Site.

There is no 'Sign In' Form Mapping for Virtual Server MFA Site.



You Need the Public Directory Template for 12.0.2 and verify domcfg is also up to date

Token Field is Missing Error

Login

Configuration error: TOTP Token field is missing. Please contact your Domino administrator.

This came up in testing.

The token field issue was because of 3 things.

1. A second reference to the TOTP server showed up
2. The template(s) needed to get replaced
3. The domcfg, needed a new file created that ignored the existing one, we had replicated it over

Create Mfamgmt Issues

```
mfamgmt create trustcert */O=mfatest1 cert.id  
C0llab$ph3r3
```

Server Console says it worked but

- Server Console “Show IDVault” does not show it worked

```
[0B84:000B-0914] Vault Name: /VBI_ID  
[0B84:000B-0914] Description: VBI ID Vault  
[0B84:000B-0914] Administrators: Keith Brooks/VBI  
[0B84:000B-0914] Servers: Music/Server/VBI  
[0B84:000B-0914] Administration Server: Music/Server/VBI
```

- Certificate list in the Directory does not show any MFA Entry



```
[0B84:000B-0914] Vault Name: /VBI_ID  
[0B84:000B-0914] Description: VBI ID Vault  
[0B84:000B-0914] Administrators: Keith Brooks/VBI  
[0B84:000B-0914] Servers: Music/Server/VBI  
[0B84:000B-0914] Administration Server: Music/Server/VBI  
[0B84:000B-0914] /VBI trusts this vault  
[0B84:000B-0914] /VBI trusts /VBI for MFA
```

Verify the Directory template is R12, most likely, it is not.
Once you replace the template, it will appear in the Certificate view

```
> Notes Certifiers  
> Notes Cross Certificates  
> Password Reset Certificates  
> Vault Trust Certificates
```



```
Multi-Factor Authentication Certificates  
  VBI  
    /VBI  
  > Notes Certifiers  
  > Notes Cross Certificates  
  > Password Reset Certificates  
  > Vault Trust Certificates
```

Hot Fix
Alert
For DA
Issue in
12.0.1FP1

Bypassing the TOTP authentication

If you have enabled Directory Assistance (DA) there's an issue where TOTP is bypassed.

This is documented under **SPR # SPPPCDVFB2** and a hotfix is available to install on top of Domino server version 12.0.1FP1.

If you enabled DA and want TOTP to be active, feel free to open a case at HCL and receive the hotfix (should be in 12.0.2).

Verse iOS 12.0.14 and Traveler 12.0.1 with TOTP (1 week ago)

- HCL Verse for iOS already configured for TOTP Authentication
- HCL Traveler server running on Domino 12.0.1 (any fixpack level)
- After updating the HCL Verse for iOS application to 12.0.14, the user fails to login to the Traveler server via TOTP Authentication. After entering the user's credentials and MFA token on the TOTP login form, nothing happens after tapping "Login".

Workaround

- The customer can upgrade the Domino version of their Traveler server to 12.0.2 (or higher) to take advantage of the new TOTP features available. HCL Verse for iOS 12.0.14 has added support for the mobile setup of MFA on the HCL Verse mobile apps.
- Upgrading the Domino server to 12.0.2 will require that the Traveler server be updated to 12.0.2. If the Traveler server is already running 12.0.2 when Domino is upgraded to 12.0.2, the Traveler server will need to be re-installed.
- After upgrading the Domino server to 12.0.2 it is recommended to run a Refresh Design on the DOMCFG.nsf using the updated domcfg5.ntf template. This will ensure that the TOTP login form will use the new design and support the Mobile MFA Setup on Domino 12.0.2.
- Or go to Verse iOS 12.0.15
- https://support.hcltechsw.com/csm?id=kb_article&sys_id=cd7784581b652190574121f7ec4bcbc9

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

How Users Set up TOTP

- Users need to install on their device one of the common authenticator applications
 - Duo, Google, Microsoft, Authy, PingID, etc.
- Go to the Domino Login page with the TOTP and then log in as usual **FROM A COMPUTER**
- The system will bring them to the MFA setup
- User enters a name for the account and then scans the bar code shown on the screen or enters the code into their Authenticator
- Afterwards, they enter the code from the Authenticator
- They receive scratch codes for emergencies and then select Done
- They log in as usual but now include the authenticator code

Changing Authentication Configurations

Enabling or disabling TOTP for the Traveler server endpoint affects existing HCL Verse mobile clients.

Enabling TOTP for existing clients

- An existing HCL Verse for Android client (that supports TOTP) already configured for Traveler can detect and switch to the TOTP authentication mode without requiring a reconfiguration and re-synchronization.
- **An existing HCL Verse for iOS client (that supports TOTP) must be re-installed/re-configured to detect a TOTP-enabled endpoint.**

Disabling TOTP with existing clients

- If the TOTP configuration for HCL Traveler is disabled, existing HCL Verse mobile clients cannot switch back to another authentication method. In this scenario, all clients need to be reconfigured.

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

Managing TOTP

Your Admin tools, while testing and after:

1. The Internet Password Lockout database
 - Users lock themselves out, and you will need to clear them from the lockout database
2. The ID Vault database
 - The ID Vault database can tell you who has set up TOTP plus more details
3. The Person Document
 - TOTP Configuration Check
4. The Server Document
 - TOTP Configuration Check
5. The Web/Internet Side Document
 - TOTP Configuration Check

The Internet Password Lockout Database

Internet Lockouts




Locked Out Users/IP Addresses

Login Failures

Mark for Delete/Unlock

Delete Marked Items

Server Name ▾	User Name/IP Address ▾	Locked Out ▾	Failed Attempts ▾	First Failure Time ▾	Last Failure Time ▾
▼ Music/Server/VBI					
	102.165.41.29	Yes	5	20/01/2023 10:13:52	20/01/2023 10:14:02
	116.48.150.154	Yes	5	03/02/2023 05:36:15	25/02/2023 02:28:33
	141.98.10.180	Yes	5	14/01/2023 00:35:14	14/01/2023 00:45:23


Internet Lockouts		Mark for Delete/Unlock		Delete Marked Items	
		Server Name ▾		User Name/IP Address ▾	
 Locked Out Users/IP Addresses		 Music/Server/VBI			
 Login Failures					

TOTP ID Vault Database

Keith Brooks/VBI's ID File - HCL Domino Administrator

File View Create **Actions** Help

Reset TOTP Items
Close Document
Open selected document(s) in scanEZ...
Open selected document(s) in scanEZ...

 **Keith Brooks/VBI's ID File**

ID file information

Modification Date/Time: 30/12/1899 00:00

TOTP

Devices configured: 1
Unused scratch codes: 10

ID Vault Music

Open Document Mark ID Inactive Help

Owner	ID Modified Date/Time	PW Modified Date/Time	TOTP	TOTP Devices	Scratch Codes Remaining
Fran band/VBI	19/11/2022 23:22:00				
Keith Brooks/VBI	26/10/2022 18:47:47		✓	1	10

Vault Users
 Vault Users\By Last NFL Access
 Vault Servers
 Configuration
 Inactive User IDs

TOTP Person Document

[Edit Person](#) [Examine Notes Certificate\(s\)](#) [TOTP Configuration Check](#)

Keith Brooks/VBI
keith@vanessabrooks.com

Basics | Work/Home | Other | Miscellaneous | Certificates | Roaming |

Notes Certificates | Internet Certificates | Flat Name Key |

TOTP Configuration Checker Report

Checking user Keith Brooks/VBI.
According to policy, user should be in vault O=VBI_ID.
Checking ID vault for user Keith Brooks/VBI.
No problems found with user "Keith Brooks/VBI". Please run TOTP Troubleshooter on the server or site document that's failing.

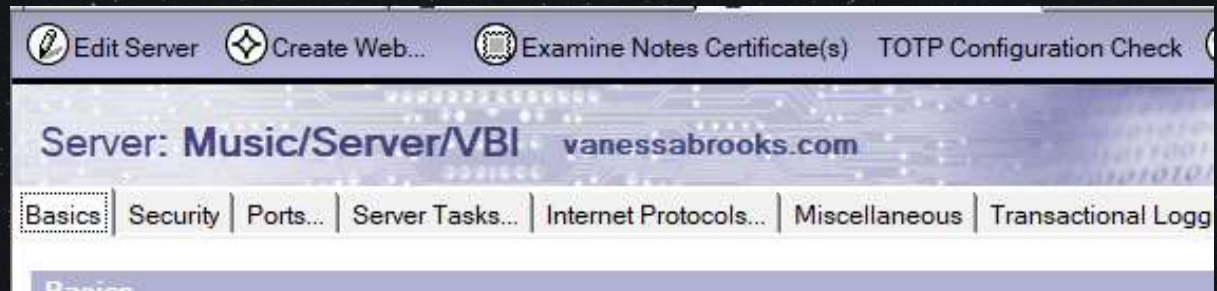
TOTP Configuration Checker Report

Checking user Vanessa Brooks/VBI.
According to policy, user should be in vault O=VBI_ID.
Checking ID vault for user Vanessa Brooks/VBI.
The ID was not found in the vault. Your problem may have to do with vault synchronization.

TOTP Configuration Checker Report

Checking user khbrooks.
This person is not a Domino user.

TOTP Server Document



TOTP Configuration Checker Report

Checking server Music/Server/VBI.

The server is set to use settings from Web Site or Virtual Server documents.

Checking Web Site Auto Generated Internet Site Document for Web Protocol.

There is no 'Sign In' Form Mapping for Virtual Server Auto Generated Internet Site Document for Web Protocol.

TOTP Configuration Checker Report

Checking server Quickr/Server/VBI.

Server {0} is not a high enough version to support TOTP (version 12.0 or higher required).

TOTP Web / Internet Site Document

Edit Web Site Web Site... TOTP Configuration Check Cancel

Web Site vanessabrooks.com

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

TCP Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☐ Yes ☐ No ☒ Yes with TOTP
TOTP option available if Session authentication is Single or SSO.

Redirect TCP to TLS: ☒ Yes ☐ No
TLS Name & Password is set to use TOTP, so TCP should be redirected unless your SSL certificates are hosted elsewhere.

TLS Authentication

Anonymous: ☒ Yes ☐ No

Name & password: ☐ Yes ☐ No ☒ Yes with TOTP

Client certificate: ☐ Yes ☒ No

TLS Options

TOTP Configuration Checker Report

Checking Web Site vanessabrooks.com.
TOTP appears to be configured correctly.
If particular users are having trouble signing in, try running TOTP Troubleshooter on the Person document.

TOTP Configuration Checker Report

Checking Web Site KeithBrooks.
There is no 'Sign In' Form Mapping for Virtual Server KeithBrooks.

New qvault Option Updates User Data 12.0.1

A new qvault command option, -p, allows you to update user data in the ID vault.

This option checks for new user certificates in the Domino directory to update in the ID file stored in the ID vault.

It also updates new ID file size and certificate expiration columns in the Vault Users view.

The syntax for the command is: `load qvault -x <vaultname> -u <username> -p.`

Omit -u to run against all user data.

Example for all users: `load qvault -x O=Renovations -p`

Example run for one user:

```
load qvault -x O=Renovations -u "CN=John  
Doe/O=Renovations" -p
```


New Query Vault Commands (12.0.1)

The Query Vault (qvault) command provides options to inactivate and reactivate a user's ID vault documents.

For example: if you have seasonal employees, you could inactivate their ID vault documents when they're not working to prevent them from authenticating and reactivate the ID vault documents when they return.

To inactivate: `load qvault -x <vaultname> -u <username> -i`

For example: `load qvault -x O=Renovations -u "CN=Samantha Daryn/O=Renovations" -i`

To reactivate: `load qvault -x <vaultname> -u <username> -v`

For example: `load qvault -x O=Renovations -u "CN=Samantha Daryn/O=Renovations" -v`

The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

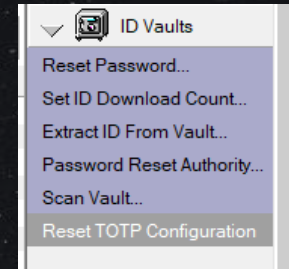
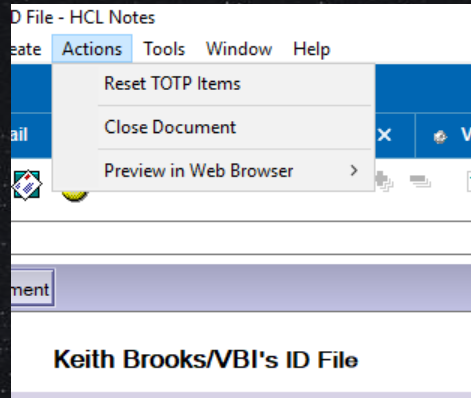
Links for Everything

Resetting the Users TOTP

You MUST log on as an ID Vault administrator and then use one of these two options to reset a user's TOTP details:

- From the ID Vault database
 - In the ID Vault Users view, select a user
 - Select from the Actions menu “Reset TOTP Items”
- From the Domino Administrator client, select the People & Groups tab then:
 - Select Tools, then ID Vaults
 - Select the person document in question
 - Select Reset TOTP Configuration

Checking and Resetting the User's ID Vault Document



The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

Customizing the Login Page Graphic

Open the
DOMCFG5.NTF
file in the
Designer client

Go to Resources-
Images

Export the
MFASetup1.png file
to your PC and
open in your
graphic editor

Add your company logo
or any text on the LEFT
side of the graphic,
about an inch or 2 away
from the border

Save the file to your
local desktop using
a different #
(MFASetup2.png)

Upload the file by
clicking "Import
Image Resource"
from the Designer
Client

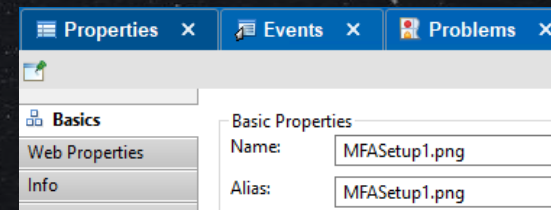
Rename the
original to #3

Change the
original Alias in
Basic properties
as well to #3

Rename the
uploaded file to
MFASetup1.png

Set the alias in the
Properties-Basics
box, to
MFASetup1.png
also

Save your changes,
replace domcfg.nsf
design and then
refresh your login
page



Customizing the Login Page TEXT

One client asked to remove the HCL Domino Name from being displayed.

A different client asked us to move it.

- To edit the login form, open the Designer client
- Open domcfg5.NTF
- Go to the Forms list and open \$\$LoginUserFormMFA
- Edit the HTML
- Replace the domcfg.NSF design
- Refresh your browser
- Remember to test it!
 - It may not appear where you think or how you expect it to be seen if you are adding text



Abandon All Hope

Ye Who Enter Here

User name:

|

Password:

MFA Token:



[Set up Multi Factor Authentication](#)

Login



The Plan For Today

What is this MFA thing? And why you might need it

TOTP Planning and Prerequisites

How do we configure TOTP

Troubleshooting when the TOTP configuration does not work

User instructions to setup TOTP on their end

Managing Your TOTP Environment

Resetting a User's TOTP Details

Customizing the TOTP Form Login Pages

Links for Everything

Links and References for TOTP Topics

- https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_overview.html
- https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_configuring.html
- https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_how_users_setup_totp.html
- https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_resetting_users_secret_keys.html
- https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_docker_requirements.html
- https://help.hcltechsw.com/domino/12.0.2/admin/conf_totp_configuring_cross_domain.html
- <https://blog.vanessabrooks.com/2021/10/sntt-changing-some-but-not-all-users.html>
- https://help.hcltechsw.com/domino/12.0.2/admin/conf_registeringusersfromatextfile_t.html?hl=registering%2Cusers%2Ctext%2Cfile
- https://help.hcltechsw.com/traveler/12.0.2/mobile_support_totp.html
- <https://blog.vanessabrooks.com/2021/10/sntt-totp-needs-id-file-in-id-vault-to.html>
- <https://blog.vanessabrooks.com/2010/06/id-registration-via-text-file.html>
- <https://alichtenberg.cz/how-to-register-notes-users-from-a-file/>
- **My Previous Decks about TOTP:**
- https://drive.google.com/viewerng/viewer?url=keithbrooks.com/download/SUTOL_2022_kbrooks_TOTP.pdf
- <https://e1.pcloud.link/publink/show?code=kZ3PjRZclvMCiF7euVOlBTWLd9rl0c4zlx7>
- <https://www.slideshare.net/kbmsg/yes-its-number-one-its-totp>
- **HAR File Details:** https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0091868

WHAT IN THE *OpenNTF*
BLUE BLAZES

TOTP

**THIS
IS
THE
WAY**

Happy St. Patrick's Day!

QUESTIONS?

Thank You!

Keith Brooks

@Lotusevangelist

keith@b2bwhisperer.com



QUESTIONS?

Use the GoToWebinar Questions Pane

Please keep all questions related to the topics that our speakers are discussing!!!

Unrelated Question => post at:

<https://openntf.org/discord>

