

KDA Tech Solutions – How to use Passportal

What is Passportal?

Passportal is a password management tool that enables you to create **long, complex, unique** passwords for every online account you possess. These passwords are stored inside your encrypted “vault” within your Passportal account and are automatically and efficiently filled into websites as you log into your accounts online. In the case that an online account experiences a security breach where your password is leaked onto the internet, none of your other online account passwords will be affected due to each website having a unique password.

There is a lot of features within Passportal to accomplish this and more.

Table of Contents

Activate account

- Installing Passportal extension in Your browser.
- Prepping browser
- Import Passwords

Web Extension Tour

- Saving new passwords
- Logging into a website – Autofill, not autofill
- Updating passwords
- Disabling passwords
- TOTP

Web Interface Tour

- Saving new passwords
- Updating passwords
- Disabling Passwords
- TOTP

To Begin:

Account Activation

1. A KDA representative or the administrator for your organization will send you an activation email. Open this email and select “Activate Account” and fill in your personal information per the prompts.
2. **You will be asked to choose your password for your account. Use a completely unique, complex password that you’ve never used online before. This is your “password of all passwords”. This will be the only password you’ll need to remember moving forward to sign into any online account.**
3. Select desired security questions for your account and fill in the blanks.
4. **Enter the organization key provided to you by your account admin or create an organization key now for your organization. If you are creating a key for your organization, this should also be completely unique and complicated.**

5. **Highly Recommended:** To enable MFA (Multi-Factor Authentication, aka using a code from your cell phone to verify your login to your account), make sure you're logged into your Passportal account on us-clover.passportalmisp.com, and navigate to:

Settings > General > Multi-Factor Authentication > Select "Enable MFA" > Select "TOTP Authentication" as MFA Communication Method > Select "Force All Users On MFA" > Select "Save"

The screenshot shows the Passportal web interface. On the left is a dark sidebar with a menu: 'User Management', 'Access Control', 'Reports', 'Settings' (highlighted in purple), 'Credential Types', 'Downloads', 'General' (highlighted in yellow), and 'Import / Export'. The main content area has three tabs: 'Advanced Options', 'Multi-Factor Authentication' (highlighted in yellow), and 'Trusted Locations'. Under the 'Multi-Factor Authentication' tab, there are several settings: 'Enable MFA' with a blue toggle switch turned on; 'MFA Communication Method' with a dropdown menu set to 'TOTP Authentication'; 'Allow Users to Change Method of MFA Communication' with a grey toggle switch turned off; and 'Force All Users On MFA' with a blue toggle switch turned on. At the bottom right of the settings area is a green 'Save' button.

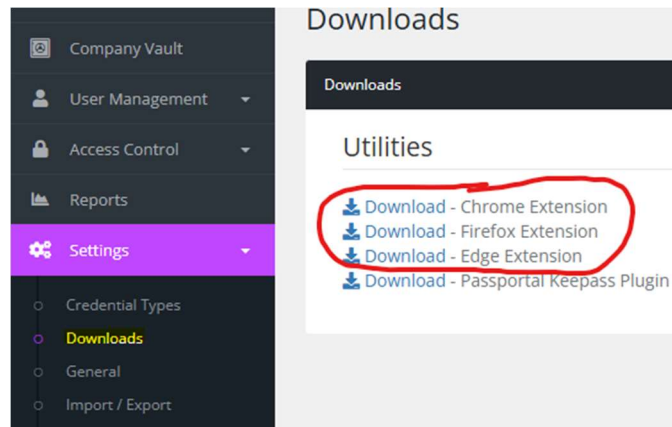
6. After MFA is enabled, log out and back into Passportal on us-clover.passportalmisp.com, and Passportal will ask you to configure MFA.
7. Use Google Authenticator, Authy, or Microsoft Authenticator on your cell phone to finish the MFA Configuration.
- Google Authenticator: Install on your [Android](#) device or [IOS \(Apple\)](#) device. Once installed, open the application and follow the prompts. You will be asked to sign into your google account to Backup your authentication codes, however you may choose not to if that is your preference. Once on the main screen of Google Authenticator, there is a colorful "+" icon that you select to add your Passportal account to Google Authenticator, Select "Scan a QR code" to scan the code on your computer screen.
 - Authy: Install on your [Android](#) device or [IOS \(Apple\)](#) device. Once installed, open the application and follow the prompts. You'll be asked to enter your cell phone number to register an account with Authy. You will also be asked to submit your email address to also be associated with your Authy Account. Verify your email address and phone through the codes Authy sends you. Add your Passportal account by selecting the "+" icon and selecting "Scan QR Code" to scan the code on your computer screen.
 - Microsoft Authenticator: Install on your [Android](#) device or [IOS \(Apple\)](#) device. Once installed, open the application and follow the prompts. Accept the privacy agreement. Choose if you'd like to share data with Microsoft. Sign into the app with your Microsoft account. **If Microsoft Authenticator offers to "autofill"**, deny them and say "Skip". Once your on the home screen of Microsoft Authenticator, select the "+" icon in the top right corner. Then select "Other Account" to scan the QR Code for Passportal on your computer screen.

After your Passportal account is configured, you can access your account from any device using this link: us-clover.passportalmsp.com

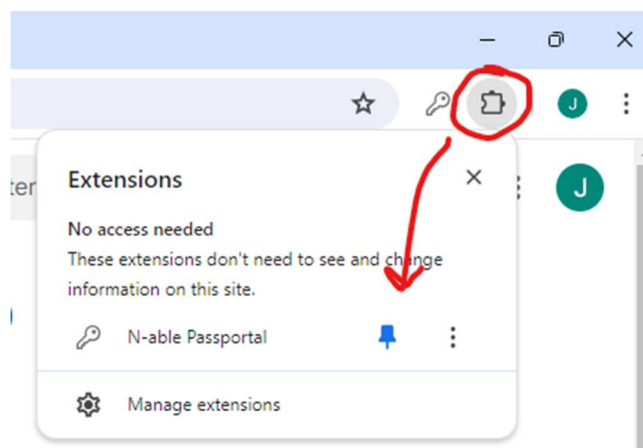
You can now also log into your Passportal browser extension, or your mobile app.

Installing Passportal Extension in a web browser

1. Open your browser of Choice.
2. Log into us-clover.passportalmsp.com with the account you've just activated.
3. Navigate to: Settings > Downloads
4. In the "Downloads" Page, select the appropriate "Download" button next to the browser you are using. If using a Chrome based browser (Like Brave Browser), select the "Download" button next to "Chrome Extension".



5. After selecting the appropriate "Download" button, you'll re-directed to that browser's web store to install the Passportal extension to your browser. Follow the prompts on this page to install the Passportal extension to your browser.
6. After the extension is downloaded to your browser, you may Pin it to your tool bar at the top of your browser by selecting the "Extensions" button and selecting the "Pin" icon next to the Passportal extension. See picture below.



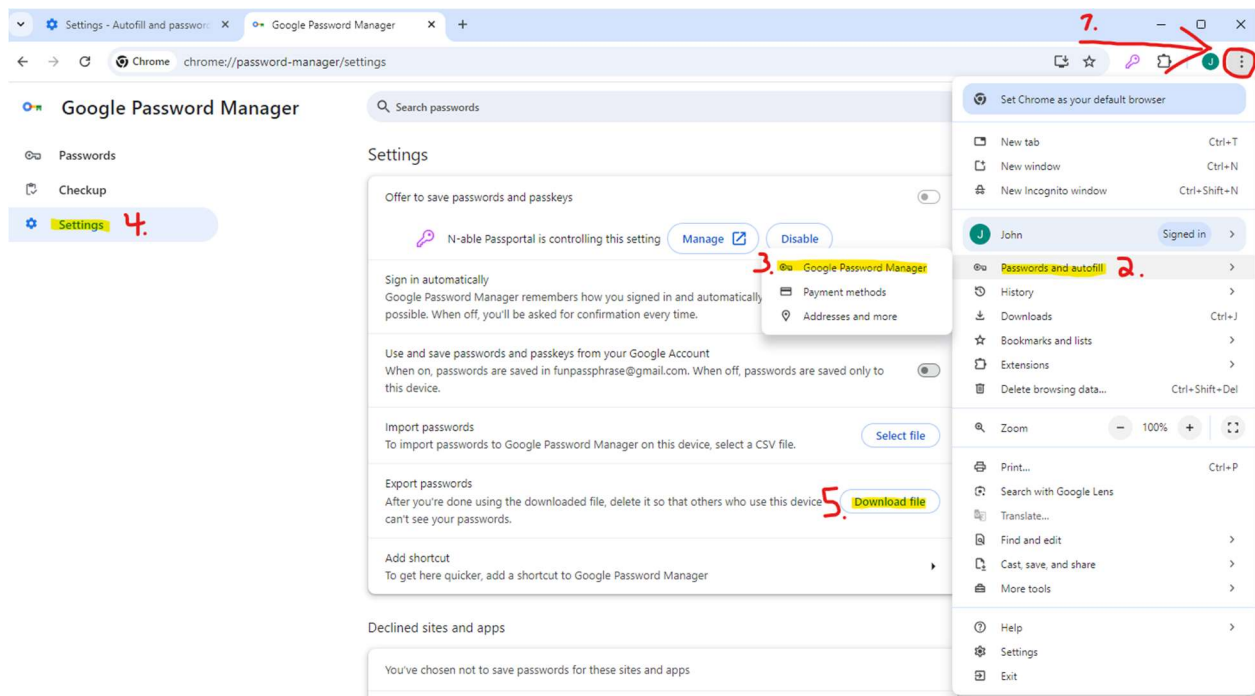
Prepping your browser

1. Navigate to your browser's settings. Typically, this is done in the top right-hand corner of your browser under 3 Dots.
2. Find your browser's settings for passwords and autofill services. (For Microsoft Edge, navigate to your "wallet" settings)
3. Turn off the browser's autofill services for Passwords, Payment methods, and Addresses.

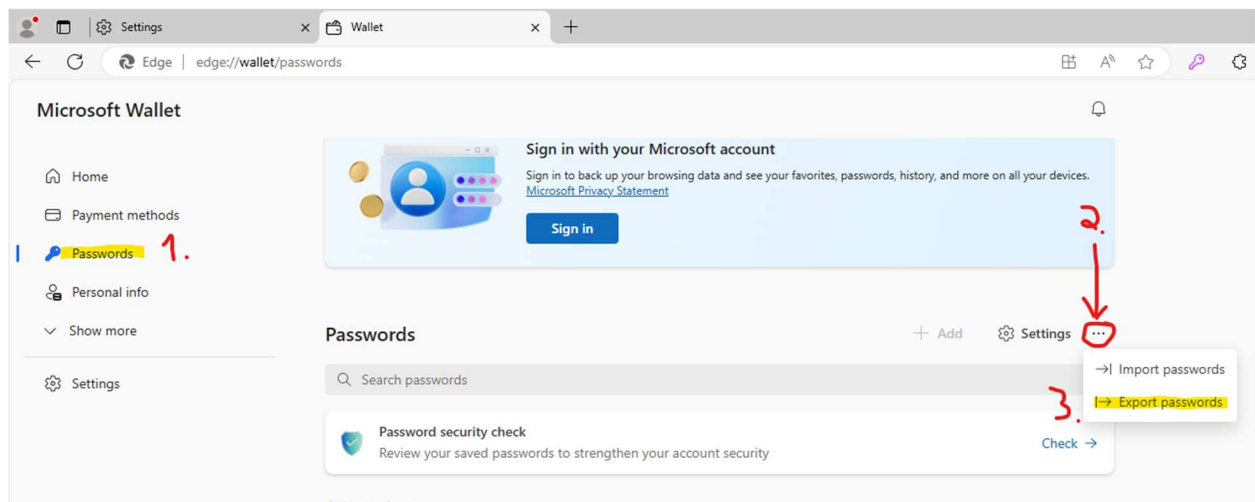
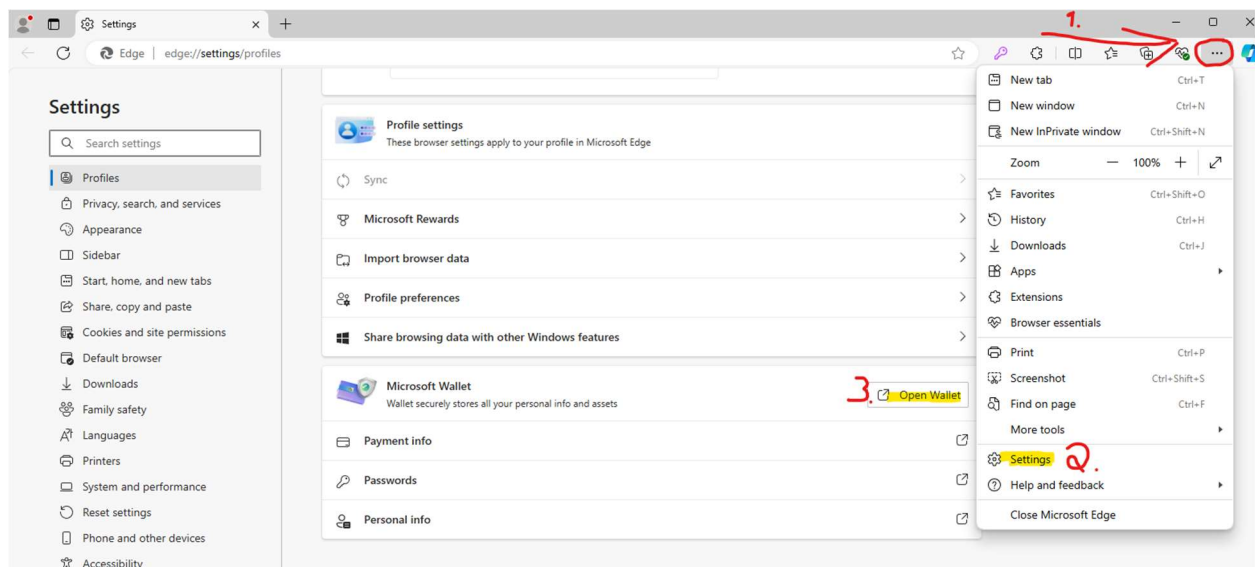
Importing Passwords

If you stored passwords previously inside a web browser like Google Chrome, or Microsoft Edge, these passwords can be exported from your browser, and imported into Passportal. Similarly, if you saved passwords from a different password management tool, you are able to import those passwords into Passportal. Passportal accomplishes this task through the use of Excel Spreadsheets, learn below:

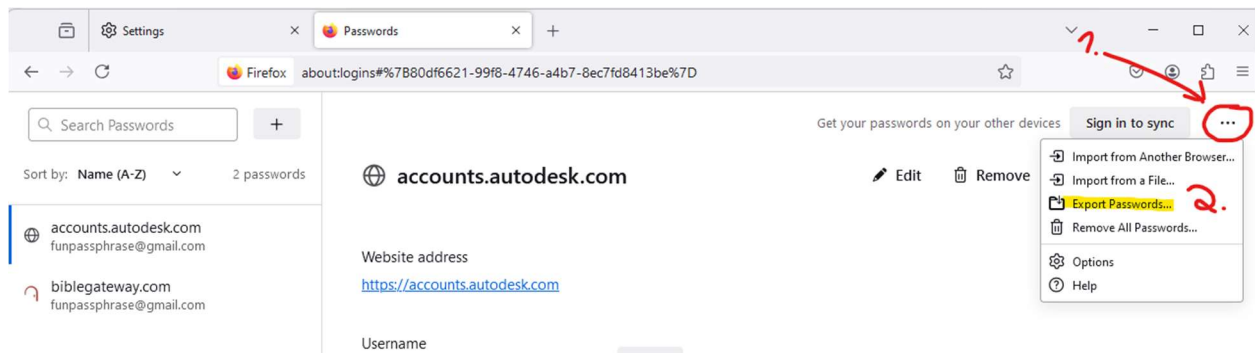
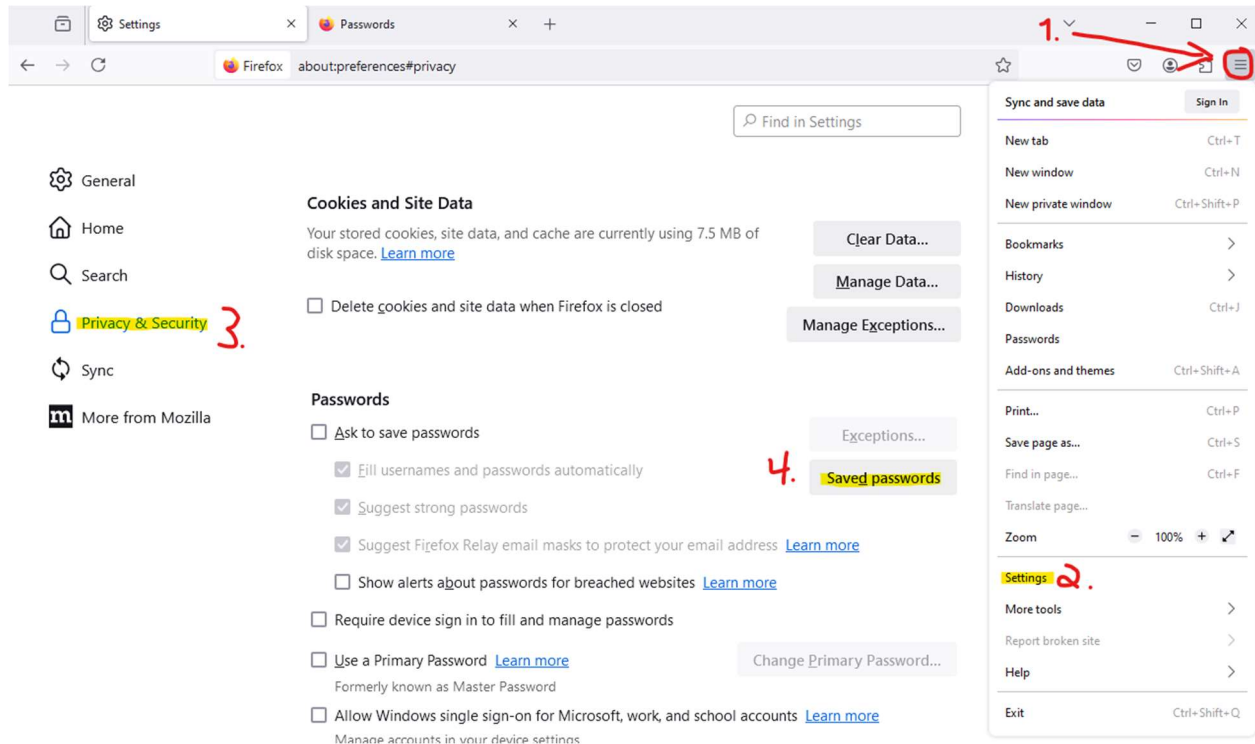
1. Acquire an exported .csv (excel spreadsheet) file from your browser or old password management tool containing all your saved passwords. If you are sourcing your passwords from an old password management tool, refer to that product's documentation on how to export passwords.
 - a. To Export passwords from Google Chrome, Navigate to:
Three Dots top right corner > Password and Autofill > Google Password Manager > Settings > Export passwords. You may be asked to type in your Windows user account password.
Save the exported .csv file to a location convenient for you.



- b. To Export passwords from Microsoft Edge, Navigate to:
Three Dots top right corner > Settings > On the “Profiles” page, scroll down and find “Microsoft Wallet” > Select “Open Wallet” > Select “Passwords” on the left hand side > Next to the “+ Add” and “Settings” buttons on the center of the the “Passwords” page, select the 3 Dots > Select “Export passwords”, you may be asked to type in your Windows user account password.
Save the exported .csv file to a location convenient for you.



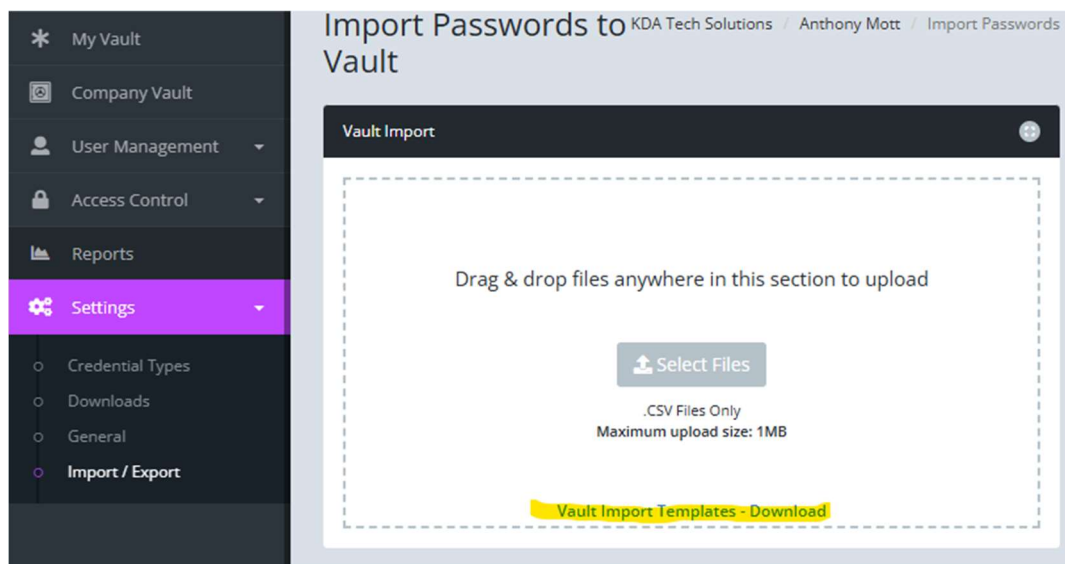
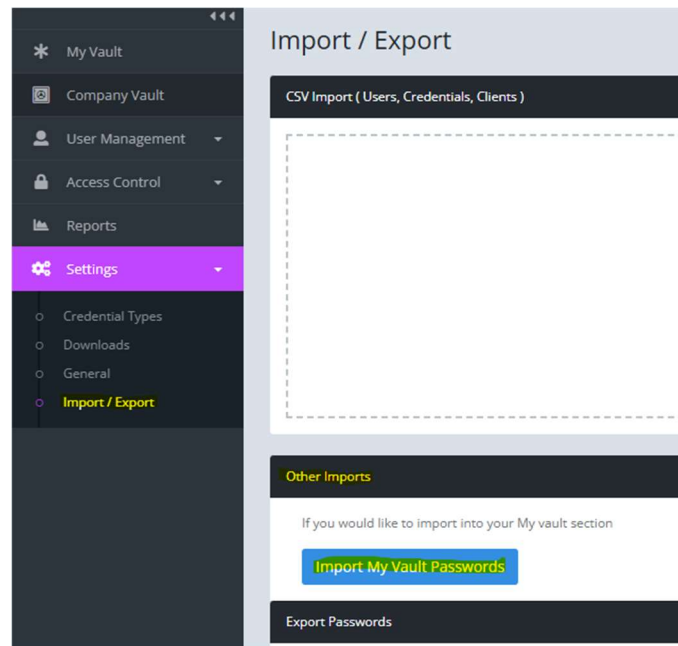
- c. To Export passwords from Firefox, Navigate to:
Three lines top right corner > Passwords > Three Dots top right corner of page >
Select “Export passwords” > Select “Continue with export”
Save the exported .csv file to a location convenient for you.



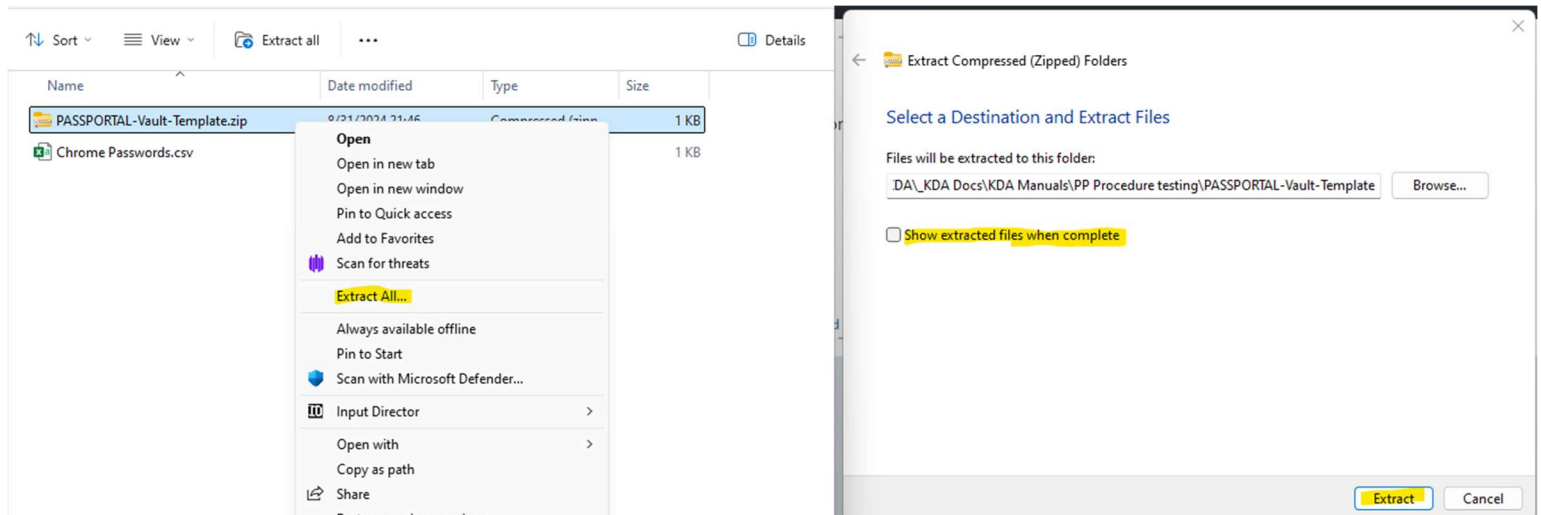
2. This exported .csv file will be used to manually copy your passwords to a Passportal template .csv file for importing your passwords.

Login to your Passportal account online at us-clover.passportalmsp.com, and navigate to: Settings > Import/Export > Other Imports > Click on “Import My Vault Passwords “ > Select “Vault Import Templates – Download”

Save the .zip file containing the template in a known location on your computer. (This file may be downloaded to your “downloads” folder by default in your PC.)



3. Navigate to the folder on your computer where you saved the zipped folder containing the “Vault Import Template” file. Right-Click on the .zip folder and select “Extract All” > An Extraction window will come up > Deselect “Show Extracted files when complete” > Select “Extract”.



4. You'll now have a regular folder labeled “PASSPORTAL-Vault-Template” that you can open to find the Passportal Vault template .csv file.

NAME	DATE MODIFIED	TYPE	SIZE
PASSPORTAL-Vault-Template	8/31/2024 21:58	File folder	
Chrome Passwords.csv	8/31/2024 21:10	Microsoft Excel C...	1 KB
PASSPORTAL-Vault-Template.zip	8/31/2024 21:46	Compressed (zipp...	1 KB

5. Double click the Extracted PASSPORTAL-Vault-Template folder, and then once more; Open the “PASSPORTAL Password Vault Template.csv” file. Also open the exported Password .csv file from your browser that you created earlier and put the two Excel sheets side-by-side. We are going to transplant columns of data from the Exported password .csv file to the Passportal Vault template file.

Notice how in both excel spreadsheets, there are several labeled columns under A, B, C... named for different categories like name, url, username, etc...

Starting in **Row 2 and below** of the Exported Passwords .csv file, contains your saved usernames and passwords associated with their URLs. Everything in Row 2 is data for one saved password, similarly in Row 3, 4, 5... The rows will go as far as the number of passwords you had saved in your browser.

We are going to highlight all the data from each Column starting every time in **row 2** and Copy (Ctrl + C) the data, and paste (Ctrl + V) the data to the corresponding column from **row 2** in the Passportal Vault template file.

Column **A** in the Exported passwords .csv file labeled “**name**” is transferred to Column **E** in the Passportal Vault Template .csv file labeled “**Description**”.

Column **B** in the Exported passwords .csv file labeled “**url**” is transferred to Column **H** in the Passportal Vault Template .csv file labeled “**URL**”.

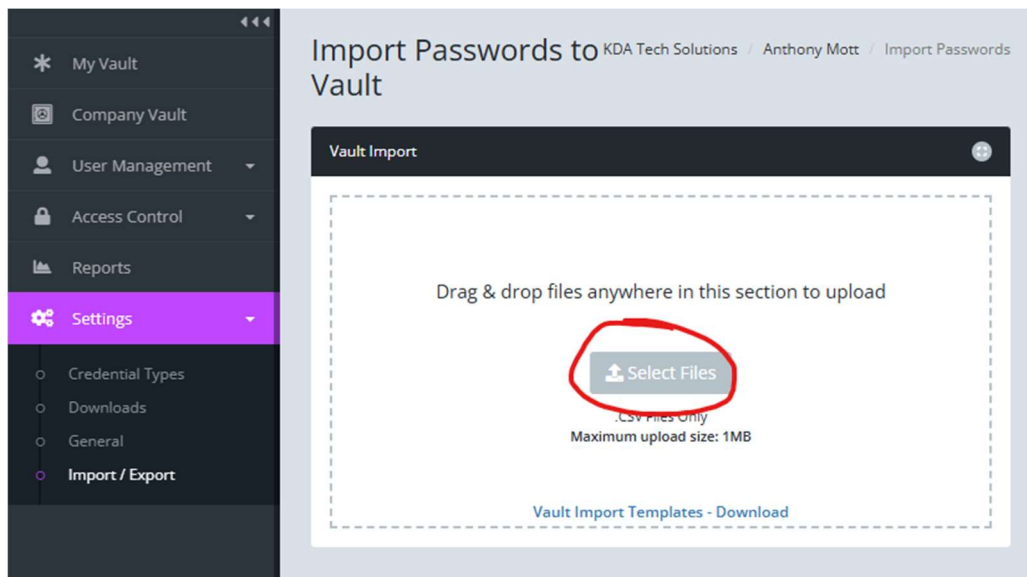
Column **C** in the Exported passwords .csv file labeled “**username**” is transferred to Column **C** in the Passportal Vault Template .csv file labeled “**Username**”.

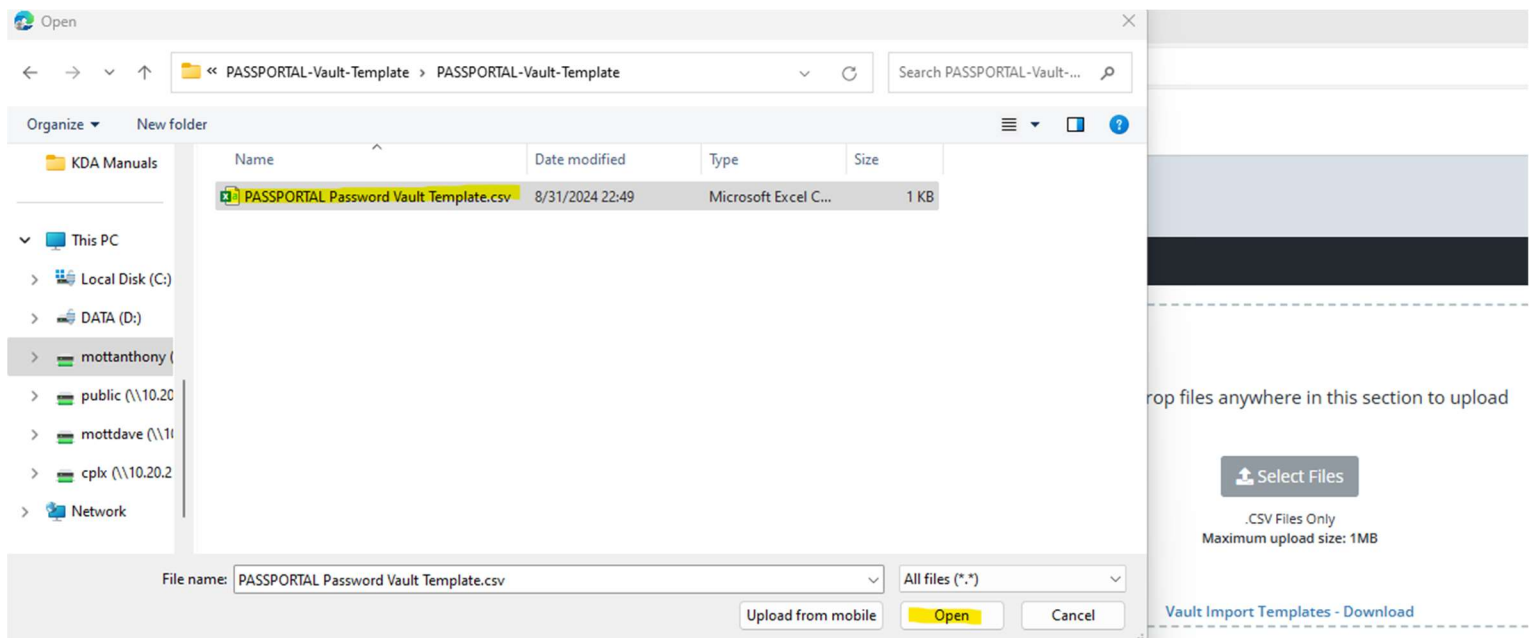
Column **D** in the Exported passwords .csv file labeled “**password**” is transferred to Column **D** in the Passportal Vault Template .csv file labeled “**Password**”.

(If Applicable) Column **E** in the Exported passwords .csv file labeled “**note**” is transferred to Column **G** in the Passportal Vault Template .csv file labeled “**Notes**”.

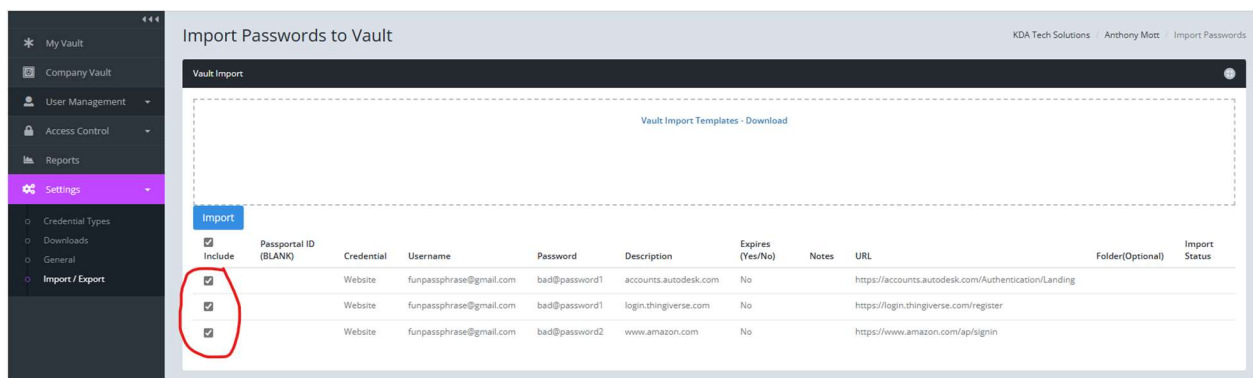
10. Navigate back to your Browser where you downloaded the Passportal Vault Template Excel file located here: Login to your Passportal account online at us-clover.passportalmsp.com, and navigate to: Settings > Import/Export > Other Imports > Click on “Import My Vault Passwords “

From this page select “Select Files” and navigate to where you saved the Passportal Vault template file you’ve just filled in with your exported passwords. Once you find the file, open it to upload the file into Passportal.

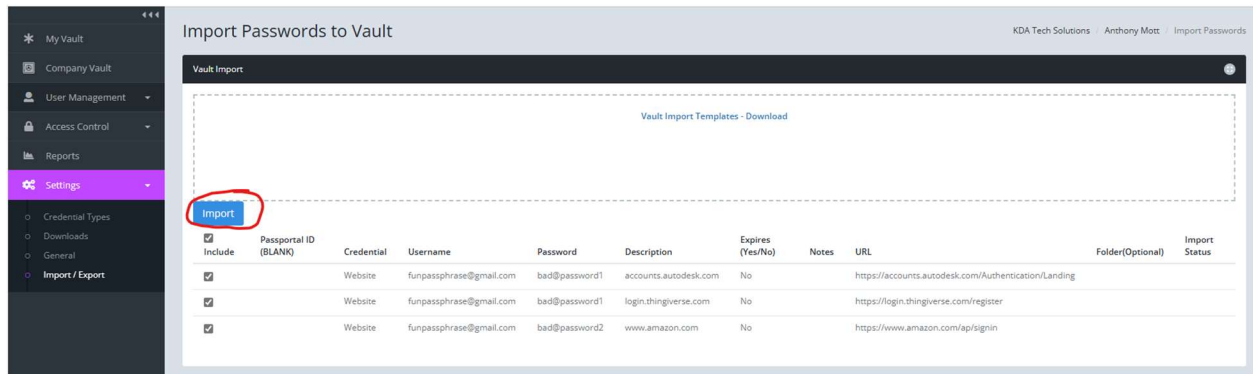




11. After you've opened the file, you'll see your passwords inside Passportal for you to review. Notice how in the list of your passwords you have a checkbox on the left-hand side allowing you to chose to not import a password that you deselect. Go through your passwords here and deselect any duplicate credentials or un-wanted credentials.



12. After you've deselected any un-wanted credentials, select "Import" to import the credentials into your account.



Import Passwords to Vault

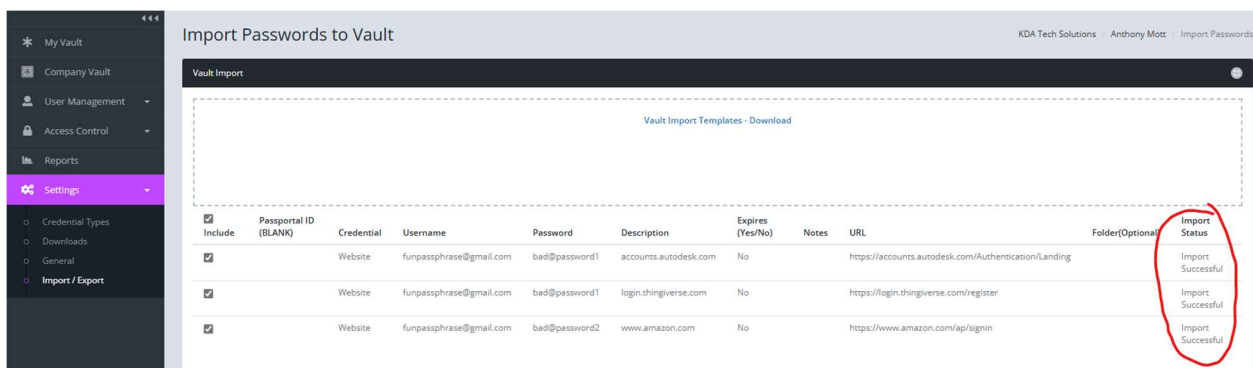
Vault Import

Vault Import Templates - Download

Import

Include	Passportal ID (BLANK)	Credential	Username	Password	Description	Expires (Yes/No)	Notes	URL	Folder(Optional)	Import Status
☒		Website	funpassphrase@gmail.com	bad@password1	accounts.autodesk.com	No		https://accounts.autodesk.com/Authentication/Landing		
☒		Website	funpassphrase@gmail.com	bad@password1	login.thingiverse.com	No		https://login.thingiverse.com/register		
☒		Website	funpassphrase@gmail.com	bad@password2	www.amazon.com	No		https://www.amazon.com/ap/signin		

13. You'll know the import is finished after you see "Import Successful" on the right-hand side of each credential in your list.



Import Passwords to Vault

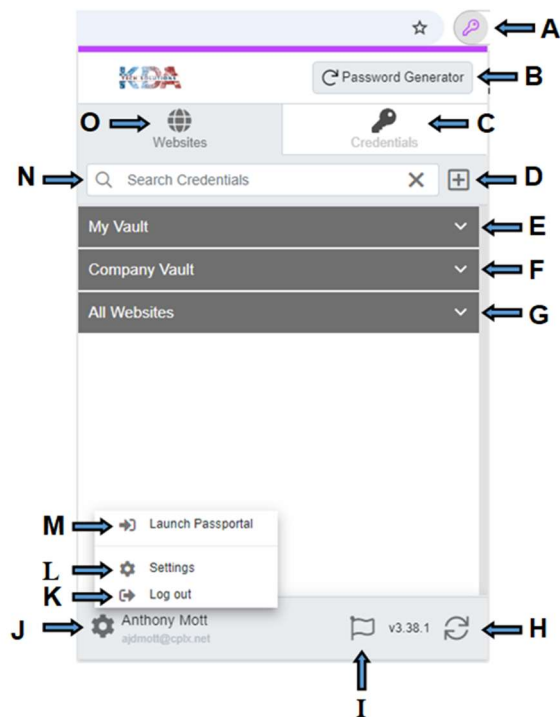
Vault Import

Vault Import Templates - Download

Include	Passportal ID (BLANK)	Credential	Username	Password	Description	Expires (Yes/No)	Notes	URL	Folder(Optional)	Import Status
☒		Website	funpassphrase@gmail.com	bad@password1	accounts.autodesk.com	No		https://accounts.autodesk.com/Authentication/Landing		Import Successful
☒		Website	funpassphrase@gmail.com	bad@password1	login.thingiverse.com	No		https://login.thingiverse.com/register		Import Successful
☒		Website	funpassphrase@gmail.com	bad@password2	www.amazon.com	No		https://www.amazon.com/ap/signin		Import Successful

Tour of Passportal Extension

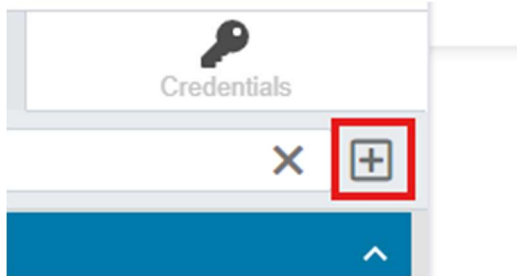
Extension Interface:



- A.** Extension button – This is to open the Passportal extension window.
- B.** Password Generator – This is one of the locations where you can generate passwords for websites.
- C.** Credentials Tab – Shows you all your saved credentials.
- D.** Add Credential Button – This is used to manually save a new credential (Username/Password) to your account.
- E.** My Vault Tab – Look through saved credentials under your personal Vault.
- F.** Company Vault Tab - Look through saved credentials under your company's vault. (Credentials shared across other members in your company)
- G.** All Websites Tab – See a list of credentials saved between your Vault and your company's Vault.
- H.** Resync Button – Resync the passwords in your extension. This is good to do after you've updated a password in the system.
- I.** Report Site Button – If there is a site that is not functioning properly for automatically filling in your username and password, use this button to report it to Passportal for them to review and implement a fix.
- J.** Settings Icon – See a list of more options for the Passportal Extension.
- K.** Log out – Use this to log out of your Passportal Extension prior to it automatically doing so.
- L.** Passportal Extension Settings – Adjust Specific settings for the Passportal Extension and how it behaves.
- M.** Launch Passportal – This will launch the Web Portal Version of Passportal for you to navigate, organize, and manage your credentials.
- N.** Search Credentials – Allows you to search for Credentials from the Website Tab or Credentials Tab.
- O.** Website Tab – Shows you all your saved credentials associated with a website.

Saving a new Password

1. To save a new password, open the extension in your browser and click the “Add Credentials” + sign button:

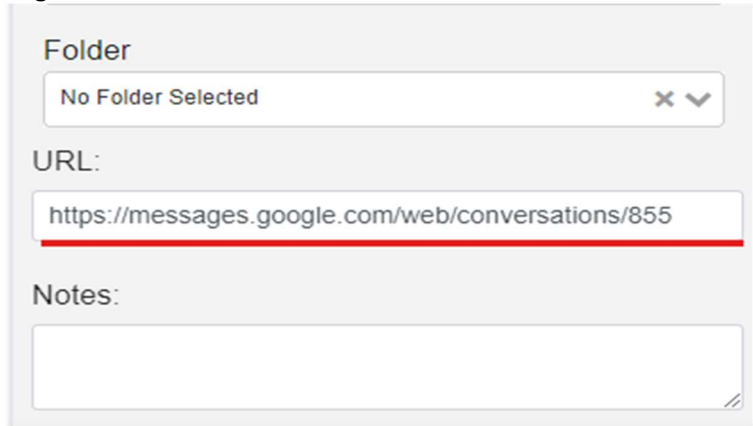


The add credentials interface will appear with the details expanded.

2. Fill out all the required fields. If you need to add a TOTP code, click the “+ Add TOTP setup code” link.

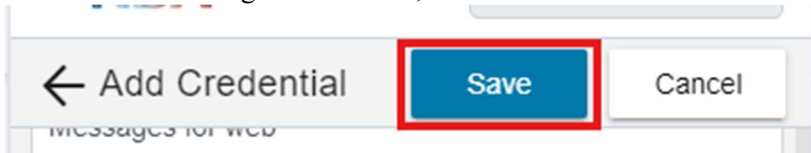
Don't forget to scroll down.

Pay attention to the URL field, this usually gets populated with a cached or tokenized temporary URL which will need to be changed to reflect the permanent login URL. E.g: “login.microsoft.com”



The screenshot shows a form with three main sections. The first section is labeled 'Folder' and contains a dropdown menu with the text 'No Folder Selected' and a small 'x' icon. The second section is labeled 'URL:' and contains a text input field with the URL 'https://messages.google.com/web/conversations/855'. The third section is labeled 'Notes:' and contains an empty text area.

3. When finished filling out the fields, click the “Save” button to save the credential



The screenshot shows the bottom of the form with three buttons: 'Add Credential' (with a left arrow), 'Save' (highlighted with a red box), and 'Cancel'.

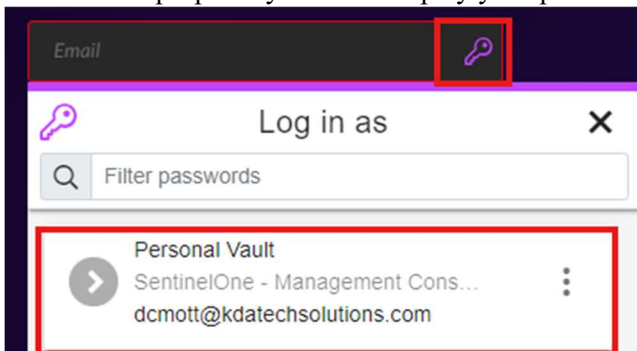
Logging into a website with auto-fill

1. Navigate to the website’s login address. Note, the web address should match the URL field in passportal:



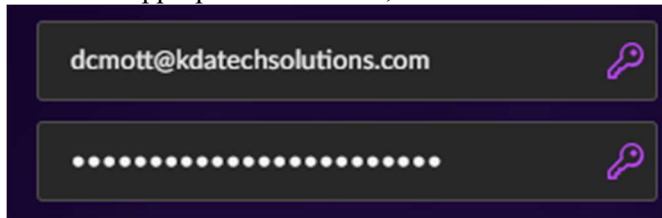
The screenshot shows a login form with two main sections. The first section is labeled 'URL:' and contains a text input field with the URL 'https://usea1-swprd2.sentinelone.net/login'. The second section is labeled 'Notes:' and contains an empty text area.

2. Click on the purple key icons to display your password options:



The screenshot shows a password manager interface. At the top, there is a search bar labeled 'Email' and a purple key icon. Below the search bar, there is a list of saved passwords. The first entry is highlighted with a red box and contains the text 'Personal Vault', 'SentinelOne - Management Cons...', and 'dcmott@kdatechsolutions.com'.

3. Select the appropriate credential, note it will fill out the field:

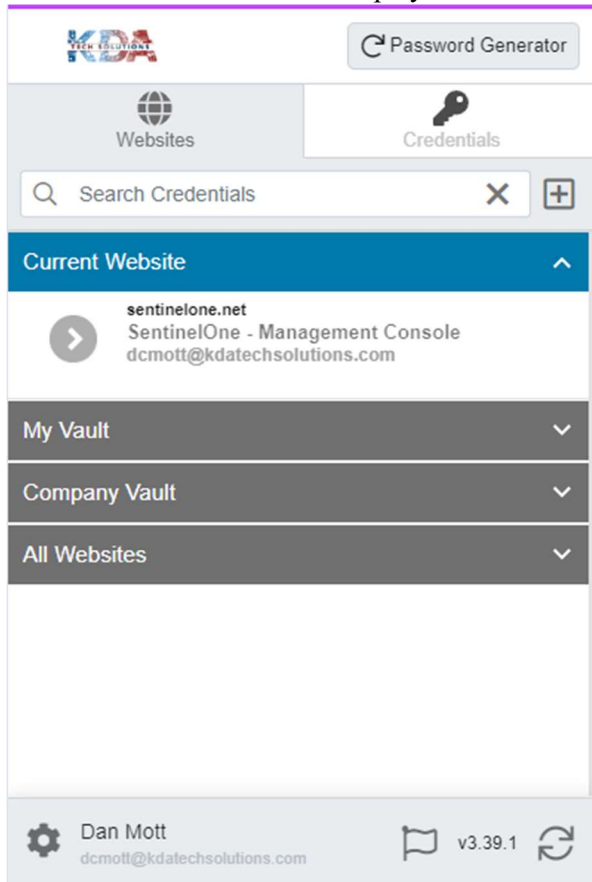


Then login

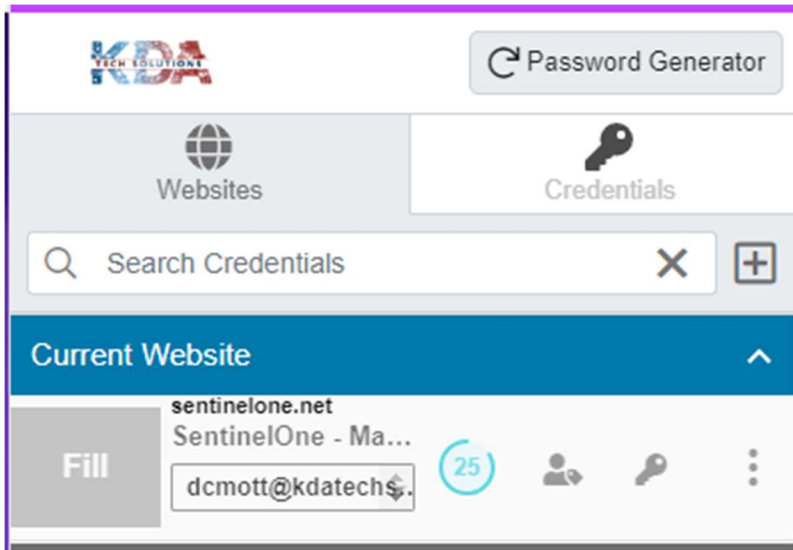
When auto-fill doesn't work as expected

Sometimes Passport doesn't properly input the username and password into the respective fields. When this happens, you will need to manually input the password:

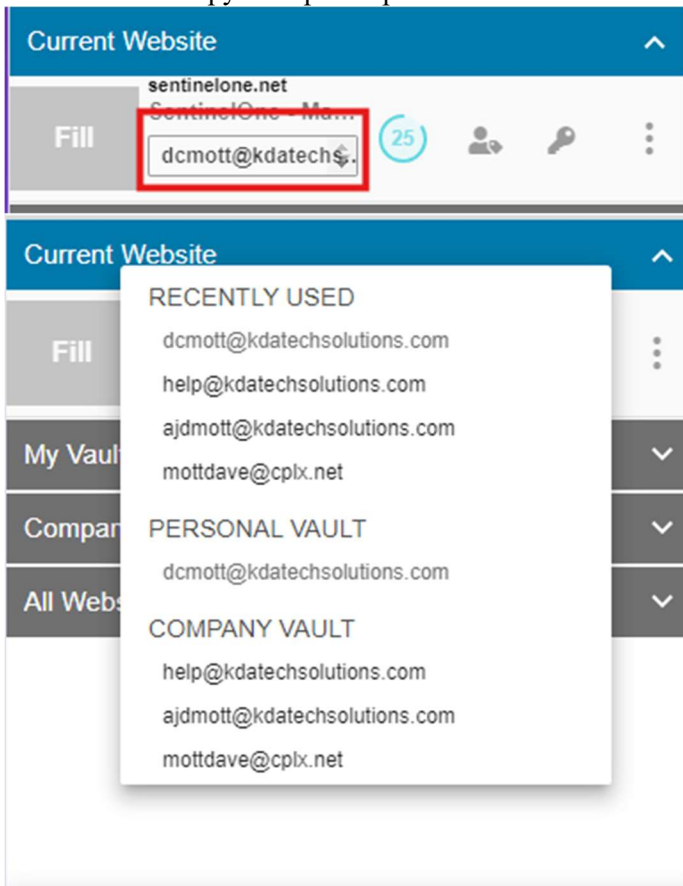
1. Click the PassPortal Icon to display the menu:



2. Hover over the displayed credential to show options. If no credential appears, you will need to manually search for it.



3. Click to either copy or expand options:



Ensure the correct username is selected, then click the button to copy the username:



Paste into the username login field:

4. Repeat the process for the password:
Click to copy the password:



Paste into the password field and login

5. If there is 2FA configured on the site, copy it and paste it on the next login screen, note the timer.

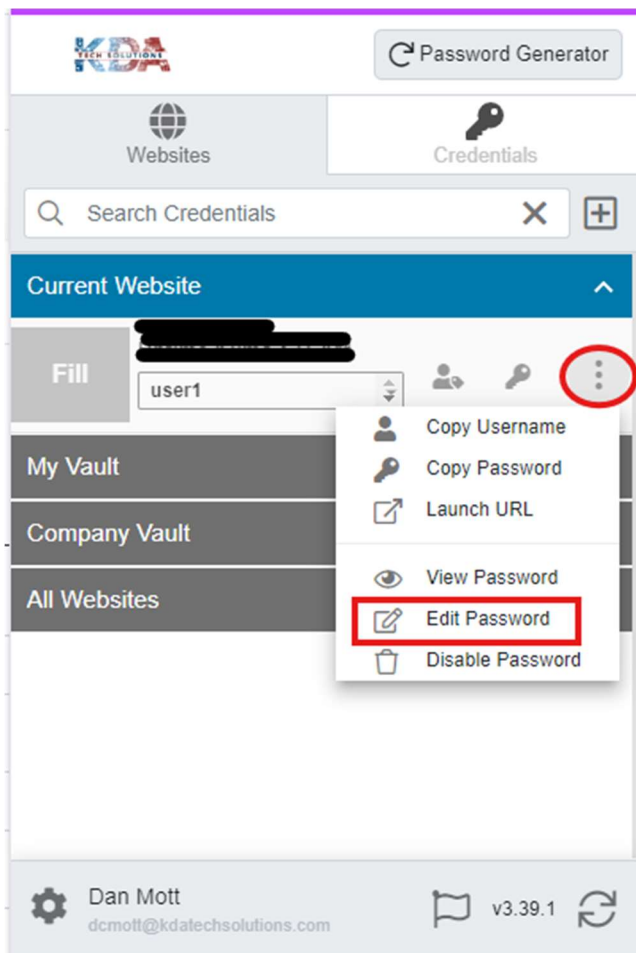


Updating a Password

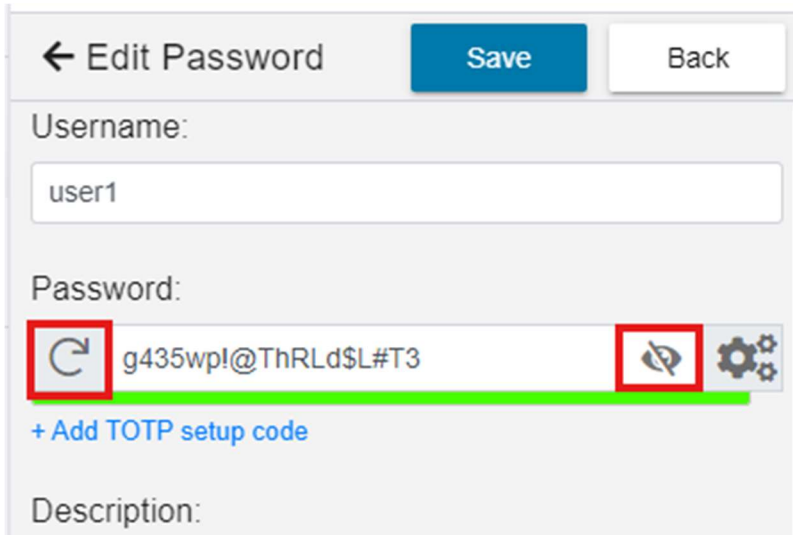
1. Navigate to the site where you wish to update your password. When prompted for a new password, click on the PassPortal Icon



Check that the correct credential is referenced and the correct username is displayed. Click the 3 dot menu and select “Edit Password”



2. Expose the password by clicking the eyeball icon, doublecheck this is the password you wish to refresh. Once confirmed, click the refresh button on the left side:



3. If you don't like the password length or characters uses, click the gears to change the settings:

Username:

Password:
  

[+ Add TOTP setup code](#)

4. Adjust the parameters to your liking:

Password:
 

Length:
 31

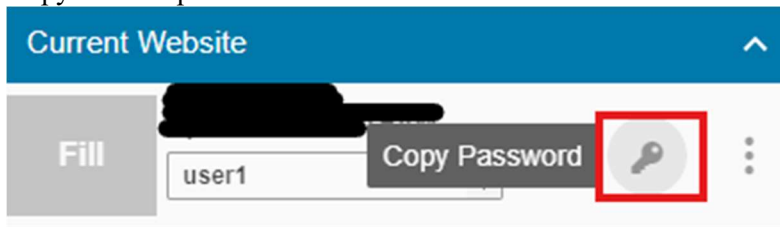
Advanced Options:

☒ a-z	☒ A-Z	☒ 0-9
☒ Special Characters	!@#\$%^&*()_+	

5. When you're happy with the selection, click the "Use" button to go back to the edit password screen:

6. Click "Save" to write the new credential to the password manager

7. Copy the new password into the website



Paste into the fields:

Current Password

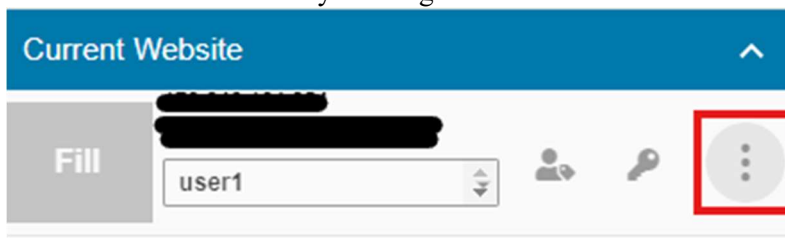
New Password

Repeat New Password

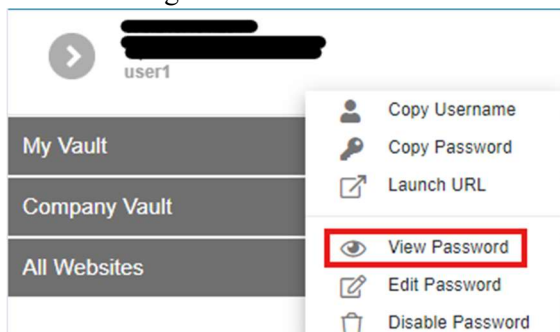
Note the length difference.

Also, I like to paste the updated password into a notepad just in case there are any issues, I then delete the text file later when I'm satisfied that the password manager has remembered the updated credential.

You can check the status by clicking the three dots menu:



Then selecting "View Password"

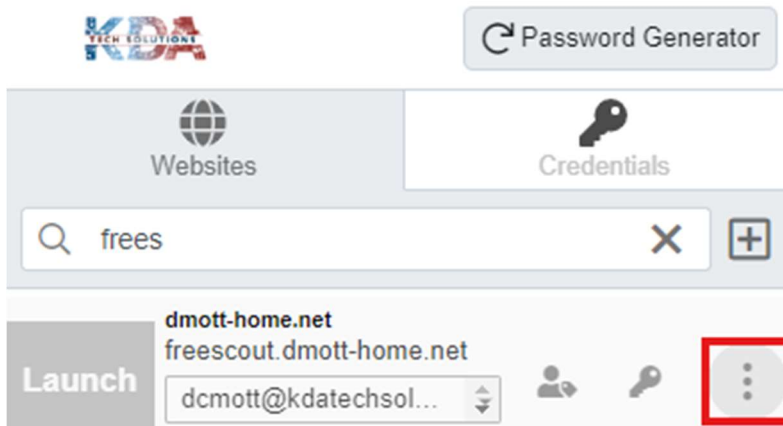


Click the eyeball icon to view the password:

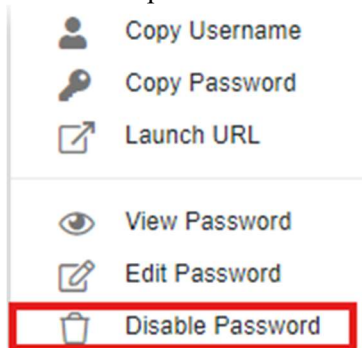


Disabling a Password

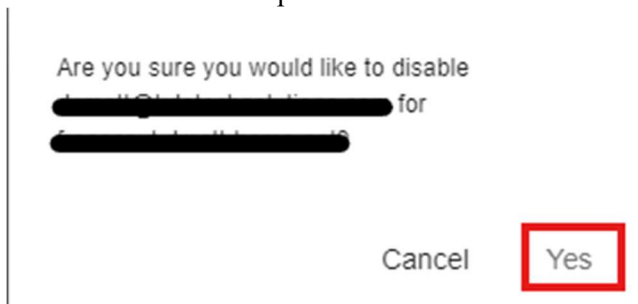
1. Either navigate to the website or search for the credential in the manager, click the 3 dots menu:



2. Disable the password:



3. Confirm to disable the password:

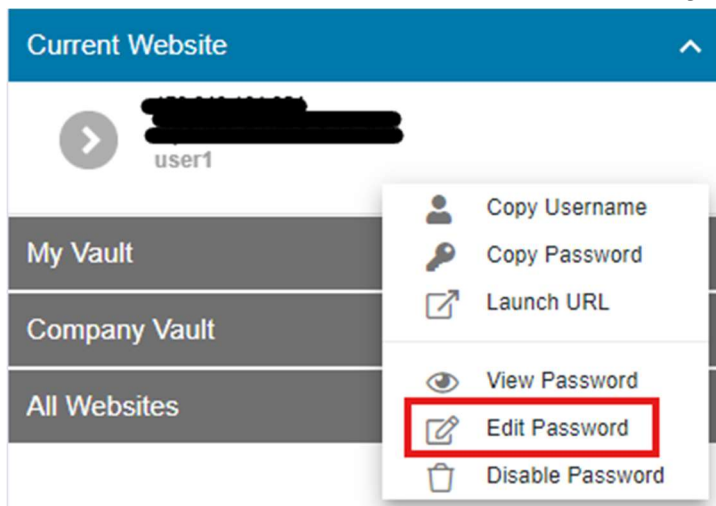


Note If you disable a credential by mistake, you may reenble the credential via the web interface.

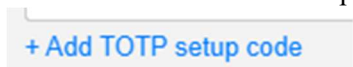
Adding TOTP To A Credential

There are many styles of two factor authentication. The type that PassPortal supports is Time-based One Time Password (TOTP). This involves adding a seed code by which a server calculates a six digit temporary password which will rotate on typically a thirty second timer.

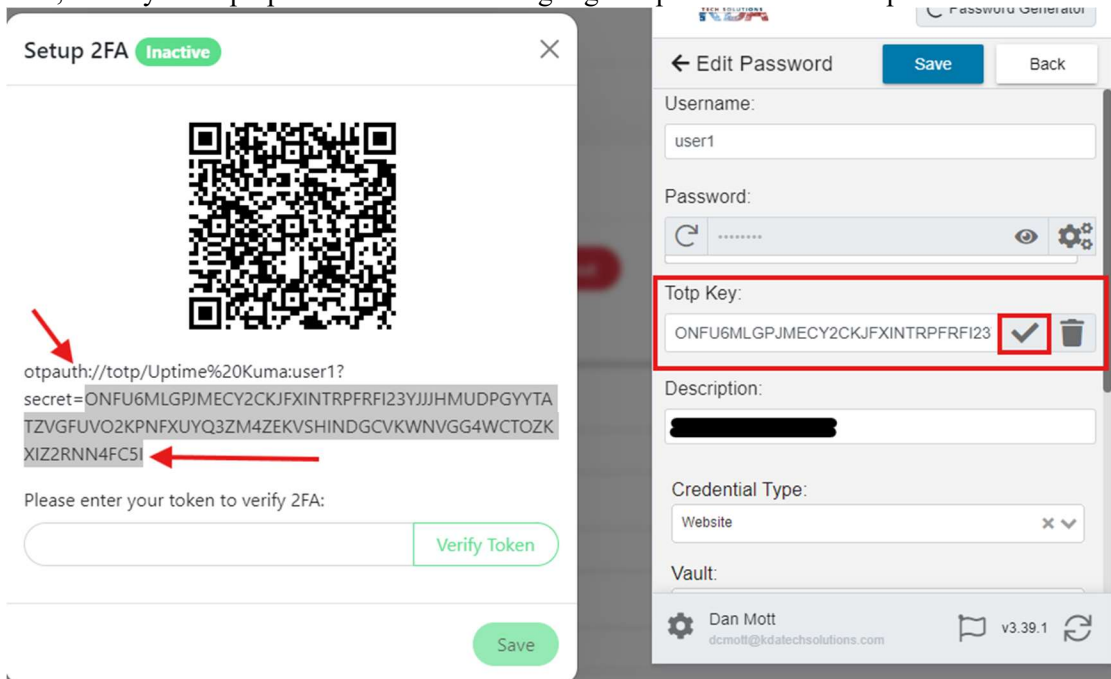
1. Find the credential in the browser extension and click the 3 dots menu and select “Edit Password”



2. Click the “+ Add TOTP setup code” link:



3. Enter the secret key in the “Totp Key:” field in the extension. Note you will only want the key data, not any URL prepended data. See the highlighted portion of the example:



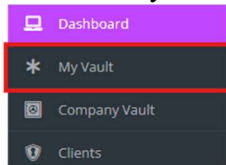
If this does not sync properly, use the web interface detailed below

Web Interface

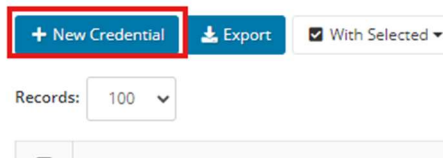
Log into the web interface at: <https://us-clover.passportalmsp.com>

Save a new password

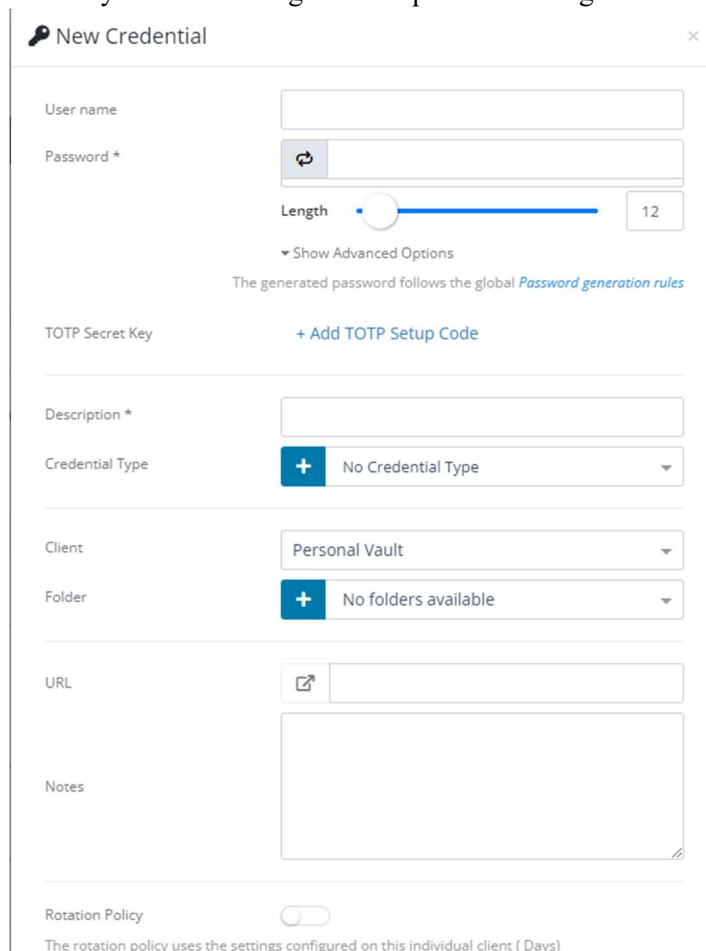
1. Click on “My Vault” on the left hand side menu



2. Click the “New Credential” button



3. Fill out the requisite fields. If the credential is a website, paste in the login page to the URL field. You may choose to categorize the password using the “Credential Type” drop down

A screenshot of the 'New Credential' form. The form is titled 'New Credential' with a key icon and a close button. It contains several fields: 'User name' (text input), 'Password *' (password input with a refresh icon and a 'Length' slider set to 12), 'TOTP Secret Key' (text input with a '+ Add TOTP Setup Code' link), 'Description *' (text input), 'Credential Type' (dropdown menu with a blue plus button and 'No Credential Type' selected), 'Client' (dropdown menu with 'Personal Vault' selected), 'Folder' (dropdown menu with a blue plus button and 'No folders available' selected), 'URL' (text input with a copy icon), 'Notes' (text area), and 'Rotation Policy' (toggle switch). A note at the bottom states: 'The rotation policy uses the settings configured on this individual client (Days)'.

4. Once all fields are filled in, click “Create” to save the credential.

Rotation Policy ☐

The rotation policy uses the settings configured on this individual client (Days)

Create Close

Updating a Credential

1. Navigate to the credential you wish to update within your vault. You can use the search query to filter your passwords:

Show Disabled: ☐ Filter:

↑	Credential Type	↕	TOTP	↑	Flags	↕	Actions
---	-----------------	---	------	---	-------	---	---------

2. Click the password, then click the “Edit” button near the bottom.

Notes

Rotation Policy No

Linked Items No Linked Items

Disable Credential Show History: ☐ **Edit** Close

3. Click the pencil icon in the password field to edit the password:

Password *****

4. Cycle the password by clicking the refresh symbol:

Password *   85YH4x+bFom@Ta7103^+V

Strength: Very Strong

Length  23

▼ Show Advanced Options

The generated password follows the global [Password generation rules](#)

Credential type  Website

Client Personal Vault

Folder  No folders available

 Disable Credential Show History:   

Note the options available to mutate the password.
Click “Save” at the bottom to write the password:

Disabling a Password

1. Search for the credential you wish to disable using the search query

Filter:

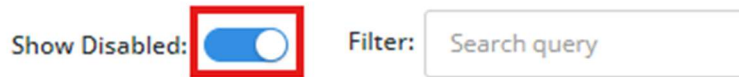
2. Click the credential to expose it then click “Disable Credential” at the bottom of the screen:

Linked Items No Linked Items

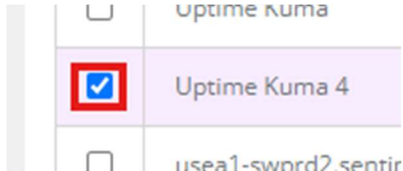
 Disable Credential Show History:   

Re-enable a Credential

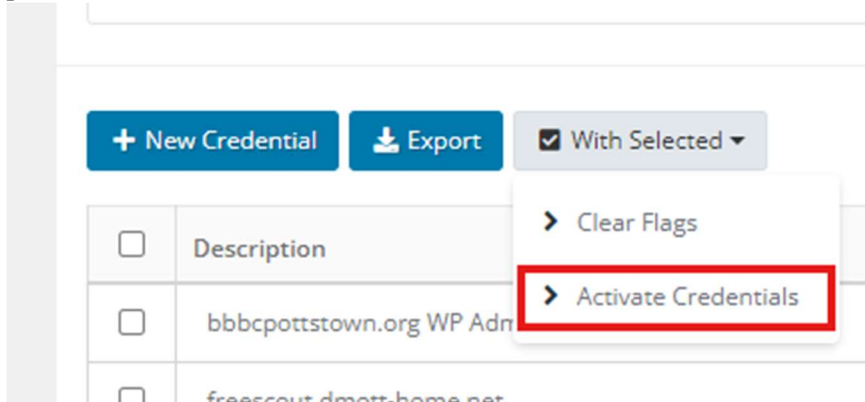
1. From your vault, click ON the “Show Disabled:” slider next to the search query to reveal all of your disabled credentials:



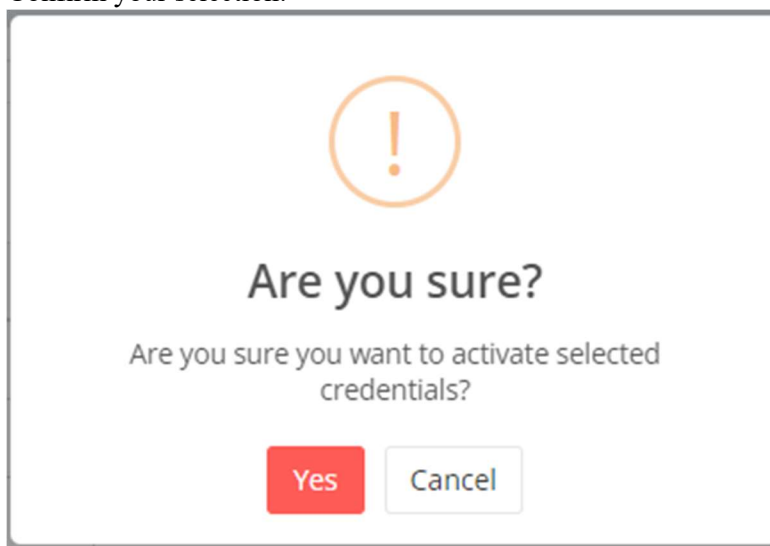
2. Search the list and select the check box next to the password you wish to re-enable



3. Click the “With Selected” Dropdown and choose “Activate Credentials” to re-enable the password:



4. Confirm your selection:



Web Interface Time-based One Time Password (TOTP)

1. Navigate to the credential you wish to add TOTP to and select the “Edit” button as if you were to update the password

View Credential

Uptime Kuma STEAM

Very Strong

3

1

Launch URL

User name

user1

Password

TOTP Secret Key

Description

Uptime Kuma STEAM

Credential Type

Website

Client

Personal Vault

Folder

URL

http://173.243.164.254:3001/dashboard

Notes

Rotation Policy

No

Linked Items

No Linked Items

Disable Credential

Show History:

Edit

Close

- At the edit screen, click the “+ Add TOTP Setup Code” link

TOTP Secret Key

[+ Add TOTP Setup Code](#)

- On the TOTP Setup screen, Add the text based key to the field, an example is given below:

 Launch URL 

Add TOTP code

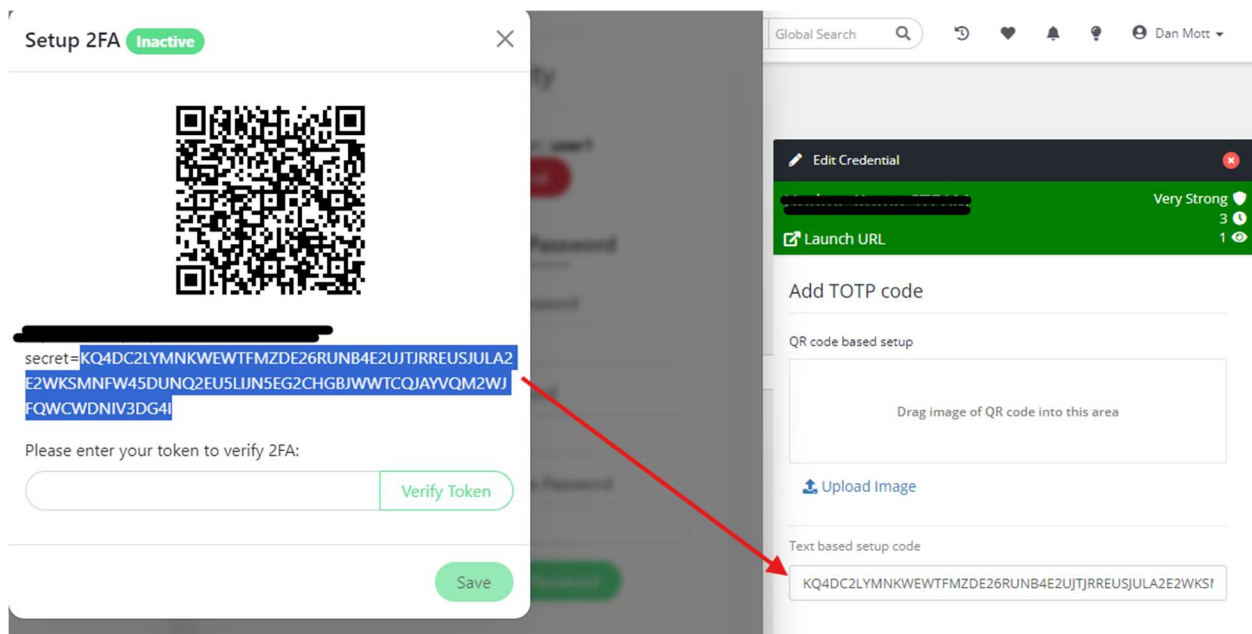
QR code based setup

Drag image of QR code into this area

 Upload Image

Text based setup code

Enter provided TOTP setup code



Text based setup code

KQ4DC2LYMNKWEWTFMZDE26RUNB4E2UJTJRREUSJULA2E2WKS!

Apply Cancel

Click apply

Click Save:

NO TARGETS available

URL   [REDACTED]

 Disable Credential Show History: ☐

Save Cancel

4. Now expose the TOTP key by clicking the eyeball icon next to the TOTP secret key section:

TOTP Secret Key  ***** 

You will reveal the key and timer, copy and paste it into the confirmation window for the TOTP verification page for the website:

TOTP Secret Key  181 725 Code expires in 18

Setup 2FA

Inactive



secret=KQ4DC2LYMNKWEWTFMZDE26RUNB4E2UJTJRREUSJULA2
E2WKSMNFW45DUNQ2EU5LIJN5EG2CHGBJWWTCQJAYVQM2WJ
FQWCWDNIV3DG4I

Please enter your token to verify 2FA:

Verify Token

Save

Verify and save the token.