

Eng Password Manager

User Guide

Version 1.8



SUMMARY

1	PURPOSE.....	3
2	MAIN FEATURES.....	3
3	IMPORTANT WARNINGS AND CONDITIONS FOR USE.....	3
3.1	TYPES OF INFORMATION THAT CAN BE STORED.....	3
3.2	TYPES OF CREDENTIALS THAT CAN BE SHARED.....	4
3.3	THE IMPORTANCE OF ORGANIZED AND CONSCIOUS SHARING.....	4
3.4	ACCESS PASSWORDS FROM DISCONNECTED ENVIRONMENTS.....	4
4	PASSWORD MANAGER ACTIVATION.....	5
4.1	ACCESSING THE PASSWORD MANAGER FROM A PC.....	5
4.1.1	MANUAL INSTALLATION OF THE EXTENSION.....	5
4.1.2	FIRST ACCESS TO ENG PASSWORD MANAGER.....	6
4.2	ACCESSING THE PASSWORD MANAGER FROM A MOBILE DEVICE.....	8
5	USING THE PASSWORD MANAGER.....	9
5.1	MAIN PAGE.....	9
5.2	APPLICATIONS.....	9
5.2.1	ADDING APPLICATIONS FROM THE CATALOG.....	10
5.2.2	MANUALLY ADDING APPLICATIONS.....	10
5.2.3	INTEGRATING APPLICATIONS VIA LAND&CATCH.....	11
5.2.4	APPLICATIONS ASSIGNED BY ADMINISTRATOR.....	12
5.2.5	CONFIGURING TOTP-BASED MULTI-FACTOR AUTHENTICATION.....	12
5.2.6	ACCESSING APPLICATIONS WITH TOTP.....	14
5.3	SECURED ITEMS (PASSWORDS AND NOTES).....	15
5.3.1	ENTERING A PASSWORD.....	15
5.3.2	ENTERING A NOTE.....	16
5.4	FOLDERS.....	17
5.4.1	ADDING APPLICATIONS OR SECURED ITEMS TO FOLDERS.....	17
5.4.2	REMOVING APPLICATIONS OR SECURED ITEMS FROM FOLDERS.....	17
5.5	VIEWING AND COPYING AVAILABLE SECRETS.....	17
5.6	ACCESSING APPLICATIONS.....	18
5.6.1	ACCESS VIA PORTAL.....	18
5.6.2	ACCESS VIA BROWSER EXTENSION.....	19
5.6.3	ACCESS VIA WEB PAGE.....	20
5.7	SHARING.....	22
5.7.1	SHARING APPLICATIONS AND SECURED ITEMS.....	22
5.7.2	SHARING FOLDERS.....	23
5.7.3	HOW TO EFFECTIVELY ORGANIZE SHARES.....	25
5.8	USING THE EXTENSION AND PASSWORD GENERATOR.....	26
5.8.1	MAIN FUNCTIONALITIES OF THE BROWSER EXTENSION.....	26
5.9	IMPORTING CREDENTIALS.....	27
5.9.1	DIRECT IMPORT VIA PLUG-IN (CURRENTLY ONLY LASTPASS SUPPORTED).....	27
5.9.2	IMPORTING FROM KEEPASS VIA KDBX FILE.....	27
5.9.3	IMPORT VIA CSV FILE.....	28
6	REQUESTING A GROUP.....	33
6.1	HOW TO REQUEST GROUP ACTIVATION OR MODIFICATION.....	33
7	CURRENT LIMITATIONS AND FUTURE DEVELOPMENTS.....	35
7.1	DIRECT IMPORT OF CREDENTIALS FROM BROWSERS IS NOT SUPPORTED.....	35



7.2	THE MOBILE APPLICATION IS CURRENTLY NOT USABLE IN ENGINEERING.....	35
7.3	THE EXTENSION ICON IS BARELY VISIBLE ON BROWSERS WITH DARK THEMES.....	35
7.4	FOLDER NUMBER AND CAPACITY LIMITS.....	35
7.5	IT IS NOT POSSIBLE TO IMPORT A FOLDER TREE.....	35
7.6	LIMIT ON SECRET IMPORTABLE WITH A SINGLE CSV FILE.....	35
7.7	LIMITATIONS ON SPECIAL CHARACTERS IN DATA IMPORTED FORM CSV	35

VERSION TABLE

VERSION	DATE	AUTHOR	DESCRIPTION OF CHANGE	CHAPTER MODIFIED
1.0	06/05/2025	Fabrizio Musilli	First Draft	/
1.1	06/06/2025	Fabrizio Musilli Nicola Barbieri	Reorganization and Integration	/
1.2	10/06/2025	Nicola Barbieri	Details on folders and import introduced	5, 7
1.3	14/07/2025	Nicola Barbieri Fabrizio Musilli	Updates on folder and import limits, Applications with MFA (TOTP)	5, 7
1.4	29/07/2025	Nicola Barbieri	General review	/
1.5	04/09/2025	Nicola Barbieri	Updates on sharing and deletion limitations	5, 7
1.6	18/09/2025	Nicola Barbieri	Main URL update	/
1.7	04/11/2025	Nicola Barbieri	Updates on limits, clarifications on features	4, 5, 7
1.8	03/02/2026	Nicola Barbieri	Removal of limitations: select multiple items, clipboard auto-clearing disabled, sharing extended to subfolders, recover deleted items, import KeePass files directly	5, 7

1 PURPOSE

The purpose of this document is to provide a guide for using the Eng Password Manager solution, the official tool of the Engineering group for storing work account credentials.

2 MAIN FEATURES

Eng Password Manager was created as a more secure and comprehensive replacement for browsers and other local password management solutions. Passwords are kept in the cloud, and the tool's functionalities are accessible:

- **from the web portal** <https://eng.cyberark.cloud> (main access point)
- **from an extension** for Microsoft Edge, Google Chrome, and Mozilla Firefox browsers
- **from a mobile application** [coming soon]

Eng Password Manager allows you to save different types of secrets:

- **Applications:** username, password, and any other access data for **websites/web apps**. These can be accessed without manually entering credentials each time, and in many cases, even without interacting with the login page.
- **Passwords:** username, password, and any other access data for **applications, systems, devices, files**, etc. You can view or copy them, then paste them into access prompts. They can also be shared.
- **Secure Notes:** **confidential** data such as PINs, serial numbers, credit card numbers, digital certificates, tax codes, etc., that you want to keep and potentially share securely.

Each Password or Secure Note item can also include attachments (maximum 10 files, up to 10 MB each).

The main operations allowed by the tool are:

- Save website login details directly while browse.
- Manually save login details, notes, and other secrets.
- Read or copy saved secrets.
- Access many web applications with one click (automatic credential entry).
- Organize secrets into folders.
- Generate complex and robust passwords.
- Share applications and other secrets with Engineering Group personnel.

Eng Password Manager is based on the commercial solution CyberArk Identity - Workforce Password Management.

3 IMPORTANT WARNINGS AND CONDITIONS FOR USE

3.1 TYPES OF INFORMATION THAT CAN BE STORED

Within Eng Password Manager, only credentials and other secrets related to work activities performed on behalf of the Engineering group are allowed to be saved, including activities carried out for Engineering's clients.

Saving, even temporarily, credentials and other secrets related to personal matters in Eng Password Manager is not permitted, even if they are related to your work (e.g., credentials for a personal account on a software development forum).



3.2 TYPES OF CREDENTIALS THAT CAN BE SHARED

With Eng Password Manager, only the sharing of credentials for accounts not assigned to natural persons is allowed. This means only accounts for which there are no individual usage restrictions due to applicable terms of use or licenses can be shared.

Sharing is not allowed for:

- **Nominal credentials or those formally assigned to a user** (e.g., `firstname.lastname@clientX.com`; `DOMAIN\EmployeeNumber`, `user1234@domain.com`, etc.).
- **Account credentials with personal use licenses** (e.g., a premium account for a service purchased with a personal license, but with the intent of using it shared among multiple users in the company).

3.3 THE IMPORTANCE OF ORGANIZED AND CONSCIOUS SHARING

The ability to share credentials and other confidential information with a secure tool like Eng Password Manager doesn't prevent users from making **incorrect or unnecessary shares**.

In line with the principles of need-to-know and least privilege, you should share a secret:

- Only when strictly necessary, and if possible, by setting an expiration date for the share.
- Only with those who genuinely need access to it.
- Only if the recipient of the share has the right to access the shared secrets and the resources accessible via those shared credentials.

Without proper organization, there's also a **risk of information loss**. When a user account is deactivated, typically at the end of an employment relationship, it results in the deletion of all secrets that user had entered Eng Password Manager, including those shared with other users. To prevent this, at least one of the recipients of the share must have been made an **owner** by the original owner.

For these reasons, **we strongly encourage those responsible for work groups to personally organize how credentials are shared among their team members**. This includes providing clear instructions on what can be shared and periodically monitoring that sharing occurs as expected.

Please see chapter 5.7.3 for directions on how to effectively organize shares.

3.4 ACCESS PASSWORDS FROM DISCONNECTED ENVIRONMENTS

Currently, the credentials available in Eng Password Manager can only be accessed from devices connected to the internet. Only in extreme cases, where it's necessary to use credentials in places where an internet connection is impossible, these credentials can be kept on a traditional password manager (e.g., KeePass). The encrypted file from the traditional password manager must be stored within Eng Password Manager and downloaded locally only for the time strictly necessary to operate in the disconnected environment.

To store an encrypted file within Eng Password Manager, we recommend creating a "Password" item. The key to open the file should be stored in the corresponding password field, while the encrypted file should be attached using the "Add attachment" button. If the encrypted file has a format that is not among those accepted, simply place it in a .zip file and upload it.



4 PASSWORD MANAGER ACTIVATION

This chapter outlines the steps necessary to activate Eng Password Manager and perform your first login.

4.1 ACCESSING THE PASSWORD MANAGER FROM A PC

The Eng Password Manager web portal is accessible from <https://eng.cyberark.cloud>

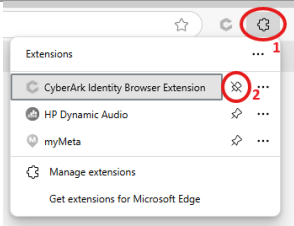
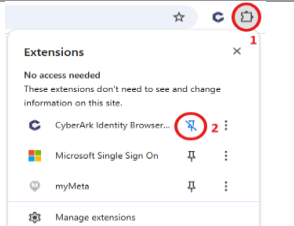
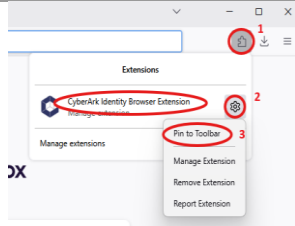
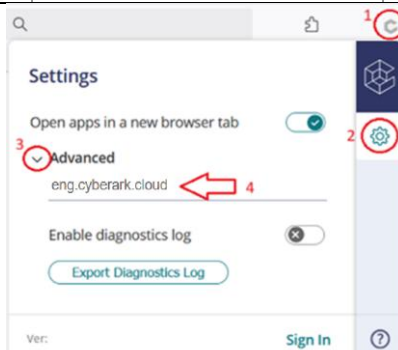
However, for full use of the solution, the user will need to connect to the Eng Password Manager web console from a browser where the specific extension "CyberArk Identity Browser Extension" (hereinafter simply "extension") has been installed.

Below are the **supported browsers**, on some of which the extension is already installed.

Browser Versions	Browser	Company PC Operating System	Type of Extension Installation
Any version released in the last 6 months.	Microsoft Edge	Windows	Pre-installed
		MacOS	Manual Installation
	Google Chrome	Windows	Pre-installed
		MacOS	Manual Installation
	Mozilla Firefox	Windows	Manual Installation
		MacOS	

4.1.1 MANUAL INSTALLATION OF THE EXTENSION

If you are using a browser on which the "CyberArk Identity Browser Extension" is not pre-installed (see table above), manually install it using the following steps:

Action	Microsoft Edge	Google Chrome	Mozilla Firefox
1. Open the extension page for the browser you're using	Extension Page	Extension Page	Extension Page
2. Click on:	Get	Add	Add to Firefox
3. Click on:	Add extension	Add extension	Installed
4. Close the confirmation pop-up	Click on X	Click on X	Click on OK
5. Pin the extension to your browser bar			
6. Insert the eng.cyberark.cloud tenant in the advanced configuration (deleting the default tenant)			



4.1.2 FIRST ACCESS TO ENG PASSWORD MANAGER

All the operations described here must be repeated for every browser you intend to use Eng Password Manager with.

Open the extension by clicking on the "C" icon and select **"Sign In."**

Please note: If the extension icon isn't visible on the bar, you can pin it as shown in paragraph 4.1.1.



FIGURE 1 - ENG PASSWORD MANAGER EXTENSION

The Password Manager login page will open. Enter your company email (e.g., john.smith@eng.it) and select "Next".

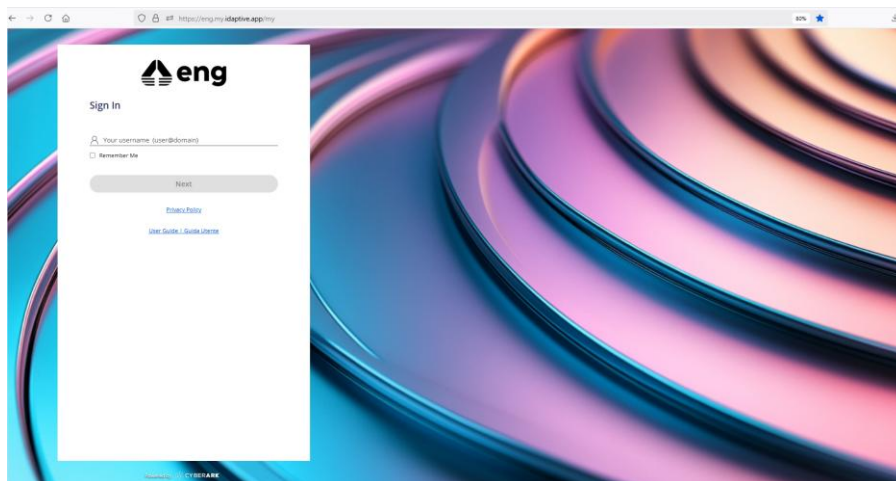


FIGURE 2 - ACCESS TO THE PORTAL

If an authenticated session with your company account isn't already active in the browser, you'll be prompted to enter your domain credentials with two-factor authentication, as shown in the following image:

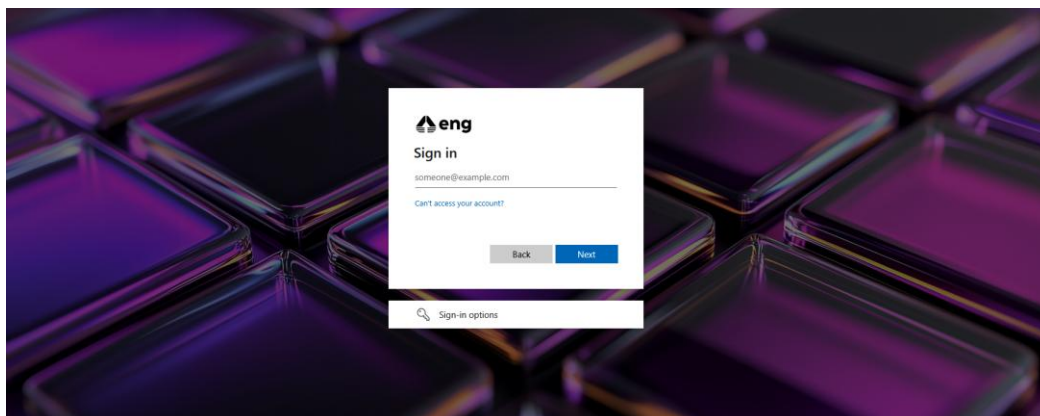


FIGURE 3 - LOGIN: ENG CORPORATE AUTHENTICATION (MAY DIFFER FOR SOME GROUP COMPANIES)

Following the entry of your credentials, you'll be prompted to authorize access either via **push notification** or by entering the code provided by the **Microsoft Authenticator** mobile app.

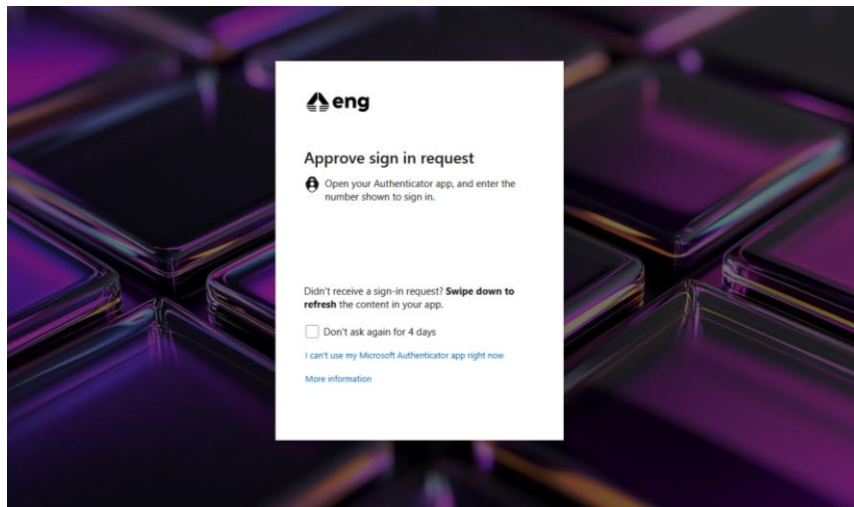


FIGURE 4 - LOGIN – MFA ENG (MAY DIFFER FOR SOME GROUP COMPANIES)

Once the authentication process is complete, you'll be asked if you want to keep the session active. By selecting "Yes," you'll be able to stay connected to the Password Manager for an extended period without needing to re-authenticate.

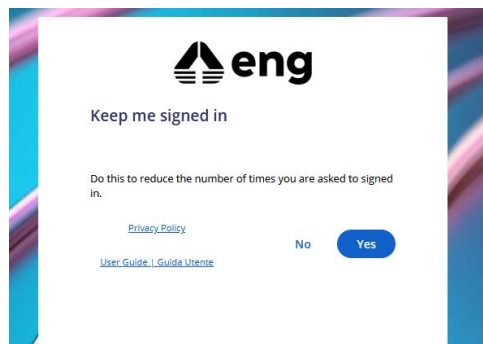


FIGURE 5 - LOGIN – MAINTAINING THE SESSION

Once this operation is complete, the user will be redirected to the user portal and can then proceed with using the Password Manager.

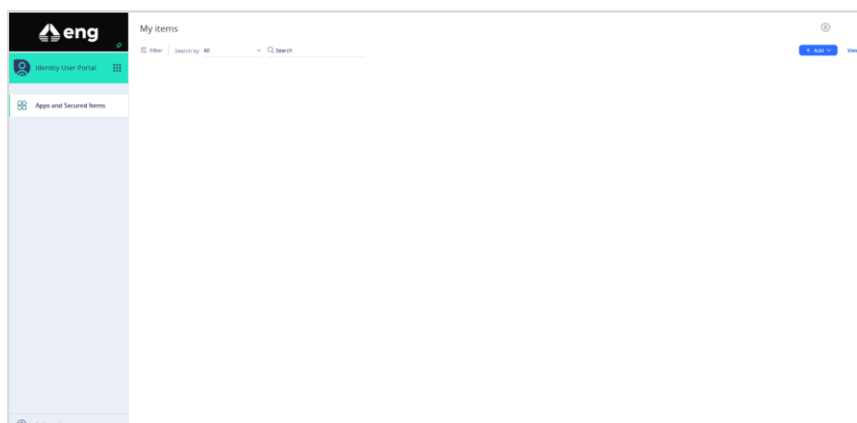


FIGURE 6 - USER PORTAL: MY ITEMS

If the access fails and redirects to the login page (Figure 2), please verify that the extension is correctly configured (see 4.1.1 step 6)

Once you've completed the login procedure for the first time, a pop-up may appear requesting authorization to access the extension. You need to select **"Sign In"**.

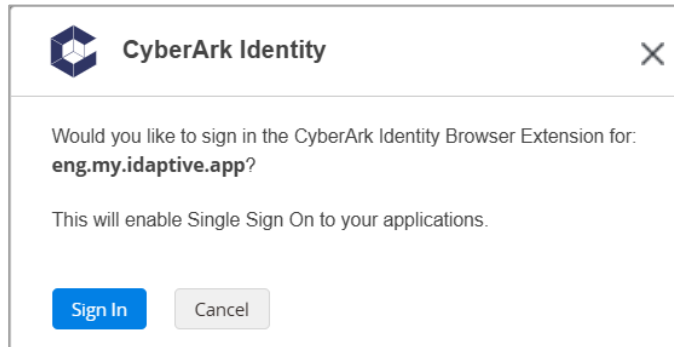


FIGURE 7 - EXTENSION ACCESS POP-UP

4.2 ACCESSING THE PASSWORD MANAGER FROM A MOBILE DEVICE

Access from mobile devices is only possible from smartphones or tablets equipped with the **company MDM solution**.

Mobile access is possible by:

- Opening the web Portal at <https://eng.cyberark.cloud> through the Microsoft Edge browser from the company profile.
- From a mobile application [available soon].

5 USING THE PASSWORD MANAGER

5.1 MAIN PAGE

Following authentication to the Eng Password Manager platform, the user will be redirected to the main page called: "Secure Access – Apps and Secured Items" (hereinafter also "Portal" or "User Portal"), always accessible at <https://eng.cyberark.cloud>. From this page, you can view, import, and create protected applications and items. The User Portal is available in over 20 languages and is displayed in the language set on the user's browser.

The page and its main functions are shown below.

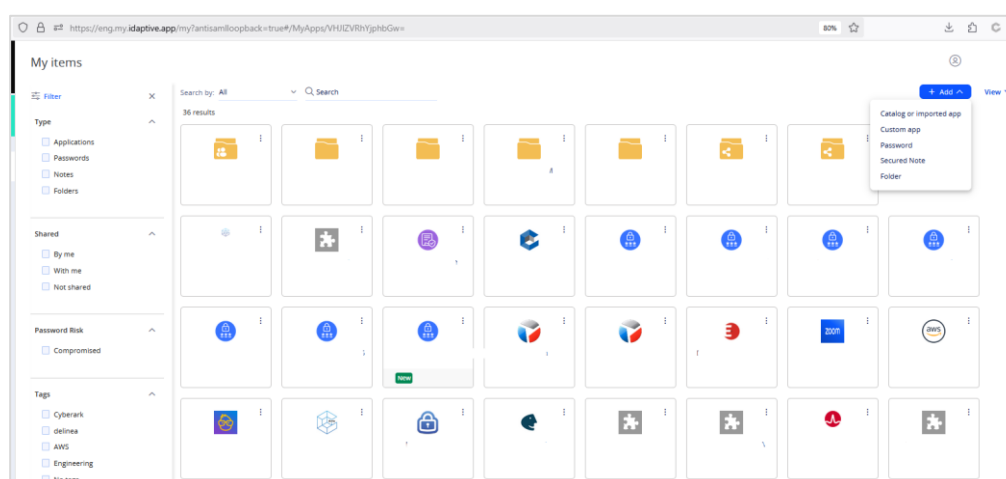


FIGURE 8 – USER PORTAL

The main page, called "My Items," displays the applications and resources you have access to. Using the "Filter" function, you can view only specific available resources:

1. **Applications:** Websites for which the system will attempt an automatic login with a simple click.
2. **Passwords:** Passwords and other credentials saved in the Password Manager.
3. **Notes:** Secrets other than credentials (e.g., PINs, serial numbers, license codes, credit card numbers, etc.).
4. **Folders:** Containers for organizing and sharing applications, secured items, and notes in bulk.

Note: The main page shows all items you can access, including those placed within folders.

5.2 APPLICATIONS

The Eng Password Manager solution allows you to add and use applications in several ways:

- Adding applications from the Catalog
- Manually adding applications
- Integrating applications via Land&Catch (while browsing the web)
- Applications assigned by the administrator



5.2.1 ADDING APPLICATIONS FROM THE CATALOG

The user portal provides a list of pre-configured applications, which correspond to well-known websites/web portals, grouped by category. The user can choose the applications they use and add them to their portal.

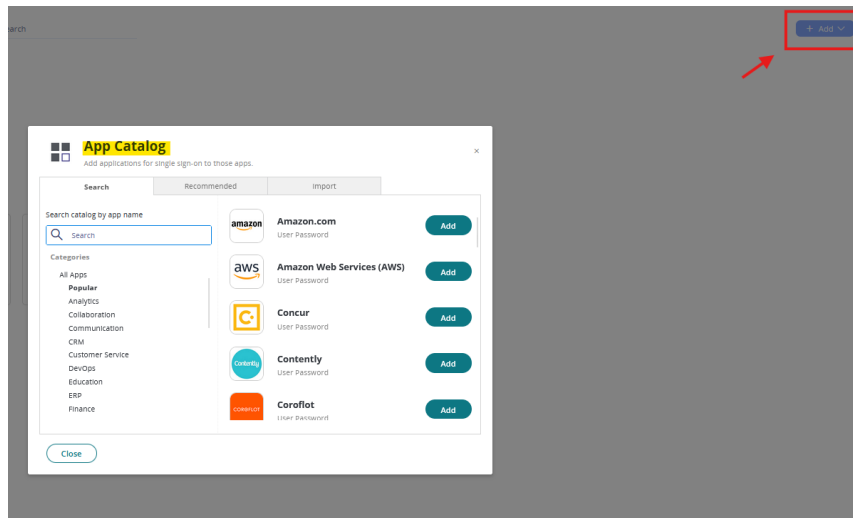


FIGURE 9 – APPLICATIONS CATALOG

1. Select the **"Add – Catalog or imported app"** option in the portal.
2. Browse or search for available applications in the catalog.
3. Select the desired application and follow the instructions to add it to your portal.

5.2.2 MANUALLY ADDING APPLICATIONS

The user manually enters the required data, including at least the application's URL and login credentials.

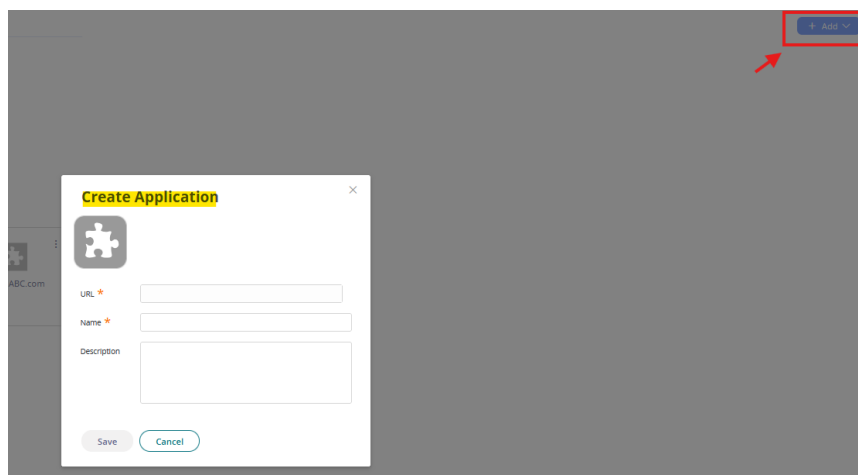


FIGURE 10 – CREATING AN APPLICATION

1. Select the **"Add – Custom App"** option.
2. Enter the application's **access URL** (e.g., <https://site.com/login>) and a **name** to easily identify it. NOTE: it is not possible to add applications with a URL containing "localhost" or "127.0.0.1", but it is possible to save their credentials in a Password item, as described in section 5.3.1.
3. Enter an optional **description** for the application and click **Save**.
4. A page will open where you can enter further details, including:

a) System or application name the password refers to.

b) Match Detection:

This parameter indicates on which application pages automatic login should be performed (function described in section 5.6.3.2). Assuming the configured URL is <https://site.com/login>, automatic access will be performed if you visit:

i. **Base Domain:** any page of the site.com domain, regardless of subdomains or paths (e.g., news.site.com or site.com/resources).

ii. **Regular Expression:** a page whose URL matches a regular expression.

iii. **Exact Match:** only the login page configured in the URL field.

iv. **Hostname:** any page that has the same hostname as the URL field, which in the example is "site.com" (e.g., site.com/resources is included, while news.site.com is excluded). The hostname is the part between the protocol (e.g., **https://**) and the first subsequent / character.

c) Add Tag: to facilitate searching and organizing applications.

d) Add to folder: Select the desired folder.

e) Any additional Notes.

f) Username.

g) Password.

h) Authentication Key: by adding the key issued by the site, multi-factor authentication is configured (function described in section 5.2.5).

5. Save the changes.

5.2.3 INTEGRATING APPLICATIONS VIA LAND&CATCH

The "Land&Catch" feature simplifies adding web applications to the Password Manager. Instead of manually configuring each application, Land&Catch automates the process when you access a website for the first time. Make sure you've enabled the Land&Catch option from the browser extension:

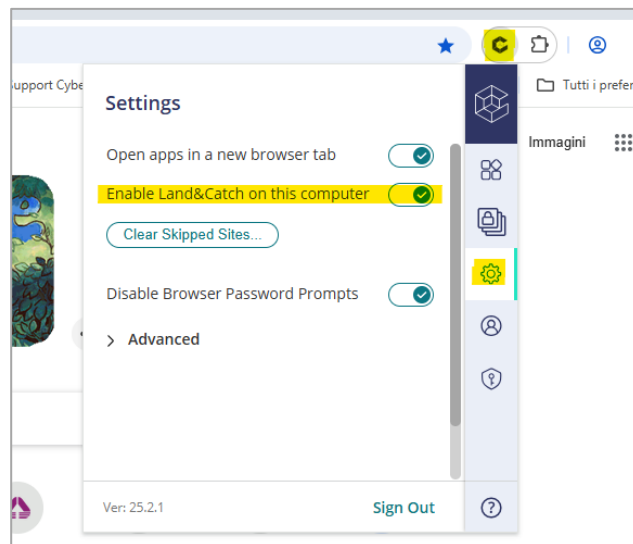


FIGURE 11 – ACTIVATING LAND&CATCH ON THE BROWSER EXTENSION

1. **Access a Website:** open a website in your browser and enter your credentials.
2. **Add Request:** The extension will detect the credential entry and prompt you to add the website as an application to your Password Manager.
3. **Automatic Addition:** The Password Manager will try to automatically retrieve the necessary information to integrate the application.

Please note: In some cases, you might need to provide additional details, such as the name you want to assign to the application in the portal.

5.2.4 APPLICATIONS ASSIGNED BY ADMINISTRATOR

Engineering can centrally configure and assign applications to specific users, who will find them on their portal along with other applications.

5.2.5 CONFIGURING TOTP-BASED MULTI-FACTOR AUTHENTICATION

For web applications that support **Time-based One-Time Password (TOTP) multi-factor authentication (MFA)**, Eng Password Manager can act as a generic authenticator app (e.g., Google Authenticator) and generate one-time codes for authentication. Adding an authentication factor to an account makes it more secure compared to traditional protection (ID + Password). Configuring MFA using Eng Password Manager allows for quicker access and enables shared access, because the one-time codes are not generated on a single user's device, but directly by the Password Manager.

To use TOTP, you need to configure them individually for each application. This configuration can be done through the **User Portal** by following the process described in the paragraphs below.

5.2.5.1 RETRIEVING THE AUTHENTICATION KEY FROM THE APPLICATION

1. Open the application from its official website and look for the menu with login / multi-factor authentication settings.
2. Locate and copy the "configuration key" for MFA, often also called "authentication key," "secret key," or "two-factor secret".

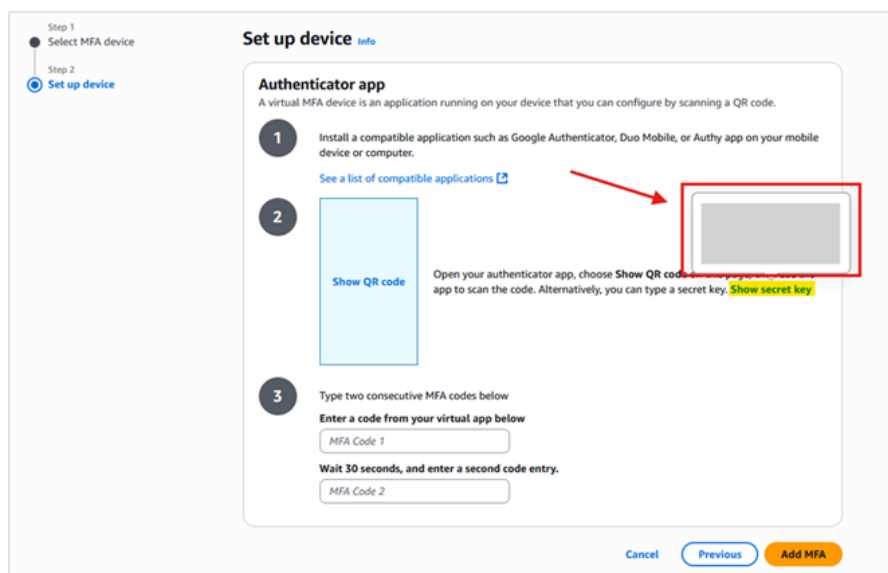


FIGURE 12 - EXAMPLE OF MFA CONFIGURATION WITH TOTP ON THE AWS.COM APPLICATION

5.2.5.2 CONFIGURING THE TOTP KEY IN THE USER PORTAL

1. In the **User Portal**, find the application tile you're configuring and open its settings (by clicking on the three dots in the top right corner of the application tile).
2. Under the **User Identity** section, paste the copied authentication key into the **Authentication Key** field.
3. Click **Apply** and then **Save**.

Application Settings

Shared with me

URL *

Match detection

Add Tags

Add to folder

Notes

☐ Auto-login at site

User Identity

Username

Password

Authentication key

[Download CyberArk Identity CLI Tools for AWS](#)

FIGURE 13 – ENTERING THE AUTHENTICATION KEY IN APPLICATION SETTINGS

- The **Verification Code (TOTP)** will be generated at regular intervals and displayed on the screen. This code should be provided to the application when requested (typically at each login).

☐ Auto-login at site

User Identity

Username

Password

Authentication key

Verification code

[Download CyberArk Identity CLI Tools for AWS](#)

FIGURE 14 – VERIFICATION CODE (TOTP) IN APPLICATION SETTINGS

Important: Some applications might require you to download and save recovery codes. These codes are crucial for accessing your account if you lose your device and must be stored in a secure location, such as a "Note" item in Eng Password Manager (see section 5.3.2).

Once this procedure is complete, multi-factor authentication will be ready to be used with the application.



5.2.6 ACCESSING APPLICATIONS WITH TOTP

Eng Password manager offers several ways to use TOTPs during the authentication process.

5.2.6.1 AUTOMATIC ACCESS WITH TOTP-BASED MFA

On compatible applications, Eng Password Manager can automatically retrieve and insert the TOTP, logging into the application, through the following methods (explained in detail in section 5.6):

- The **User Portal**
- The **contextual menu** directly on the website's login form.
- The **browser extension**.

If multiple accounts have been saved for the same application, select the desired account for auto-filling credentials.

5.2.6.2 MANUAL TOTP ENTRY

If automatic access is not available, you can manually generate and copy/paste the TOTP from the following locations:

- **Contextual Menu:**
 - On the application's login page, enter your username and password, then right-click on the field where the multi-factor authentication (MFA) code is required.
 - Select **CyberArk > Copy verification code**, click on the account you want to use, and paste it into the correct field.

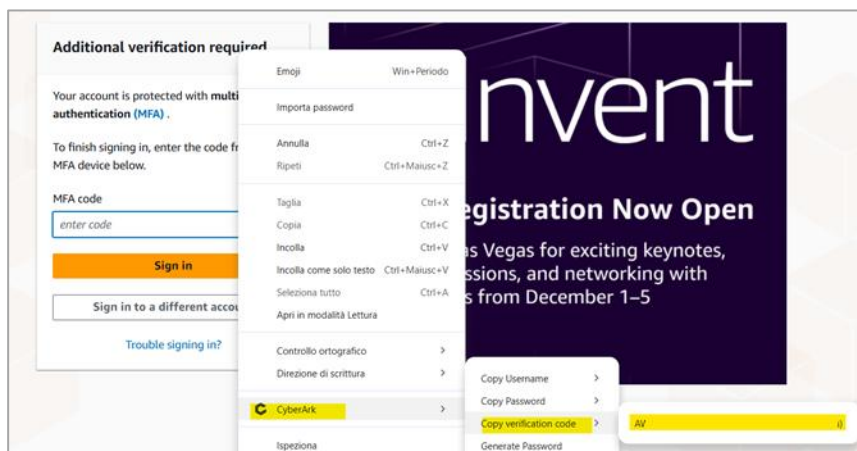


FIGURE 15 – COPYING THE TOTP CODE FROM THE CONTEXTUAL MENU

- **Browser Extension:**
 - Click on the **browser extension** icon.
 - Select the application's name, then click on the three dots and choose **"Copy verification code"**.

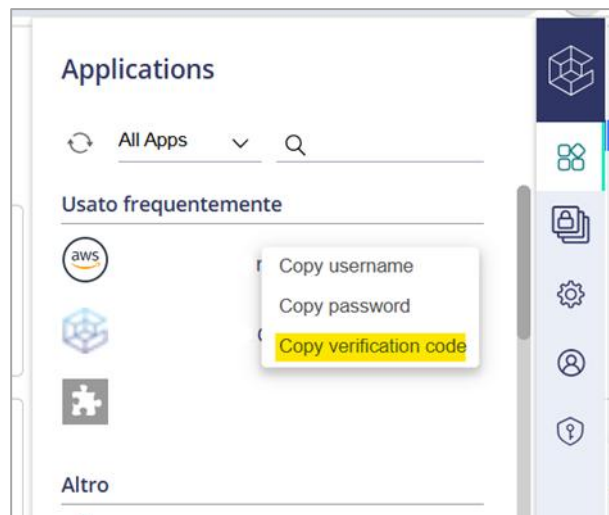


FIGURE 16 – COPYING TOTP FROM THE BROWSER EXTENSION

- **User Portal:**
 - In the **User Portal**, locate the application's tile.
 - Click on the menu with the three dots in the top right corner of the tile.
 - Select **Copy verification code**.

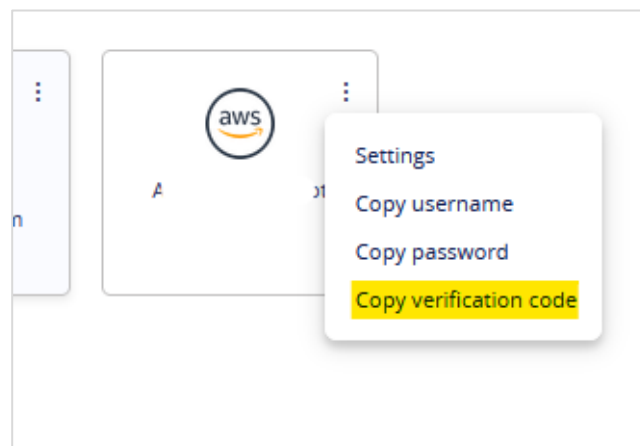


FIGURE 17 – COPYING TOTP FROM THE USER PORTAL

5.3 SECURED ITEMS (PASSWORDS AND NOTES)

Secured Items are confidential information, such as passwords, notes, personal documents, certificates, or other credentials, that the product can securely store and manage.

5.3.1 ENTERING A PASSWORD

This method is primarily useful for saving credentials for accounts not tied to web applications, but rather to other types of accounts accessed outside of the browser.

Below are the steps to add a "Password" item:

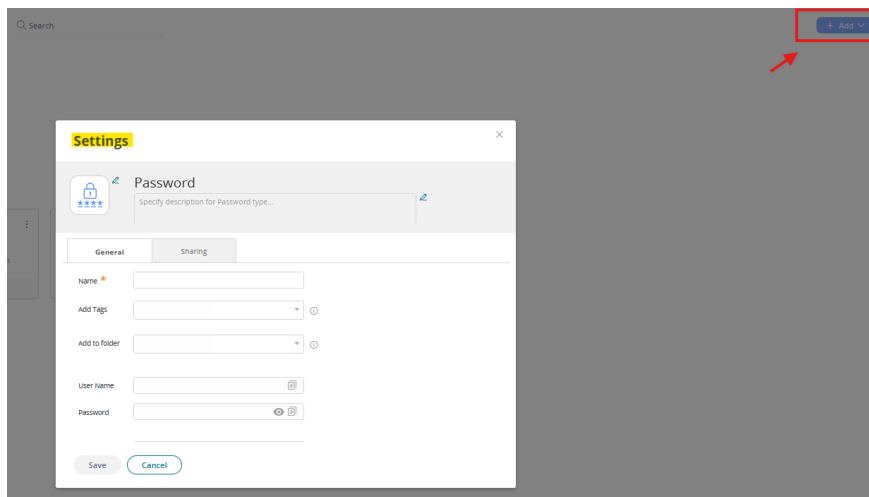


FIGURE 18 – MANUALLY ENTERING A PASSWORD

1. Select **"Add – Password"** from the User Portal.
2. Enter the item details:
 - a) Name of the system or application the password refers to.
 - b) Username.
 - c) Password.
 - d) Any additional notes.
 - e) Any files (e.g., digital certificates).
3. Save the changes.

5.3.2 ENTERING A NOTE

This method is primarily useful for saving confidential information such as PINs, credit card or bank account numbers, serial numbers, tax codes, or similar data.

Below are the steps to add a "Note" type item:

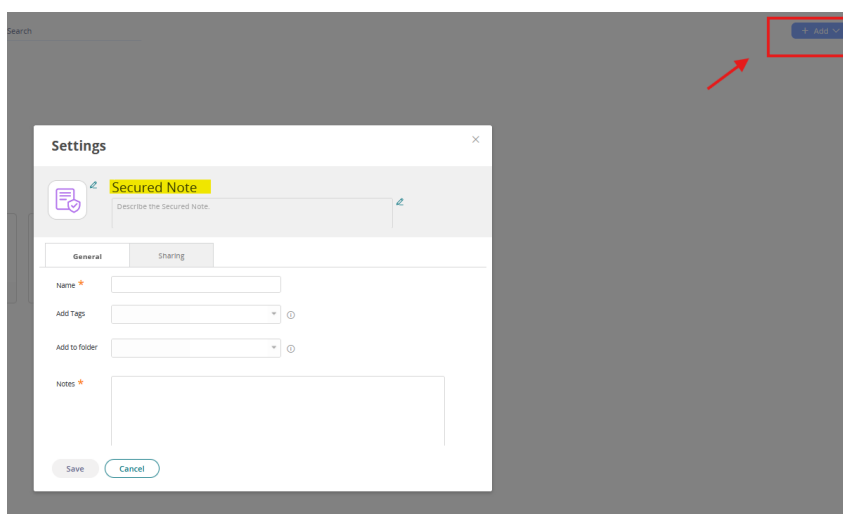


FIGURE 19 – MANUALLY ENTERING A SECURED NOTE

1. Select **"Add – Secured Note"** from the User Portal.
2. Enter the item details:

- a) Item name.
 - b) Optional item description.
 - c) Optional tags to classify the type of information.
 - d) Optional files.
 - e) The actual data to be protected, in the "Notes" field.
3. Save the changes.

5.4 FOLDERS

Folders offer an intuitive way to organize and group Applications and Secured Items. This feature is particularly useful for:

- **Organization:** Grouping related items to simplify navigation and management.
- **Quick Access:** Quickly accessing specific groups of applications or secured items.
- **Customization:** Creating personalized folders based on your needs or roles.

Note: Each user can create a maximum of 800 folders. Each folder can contain up to 800 items, including Applications, Passwords, and Notes, and up to 100 subfolders. You cannot create two folders with the same name, but you can receive a shared folder from another user that has the same name as one of your existing folders.

5.4.1 ADDING APPLICATIONS OR SECURED ITEMS TO FOLDERS

1. Create a folder by selecting the **"Add – Folder"** option and entering a name and an optional description.

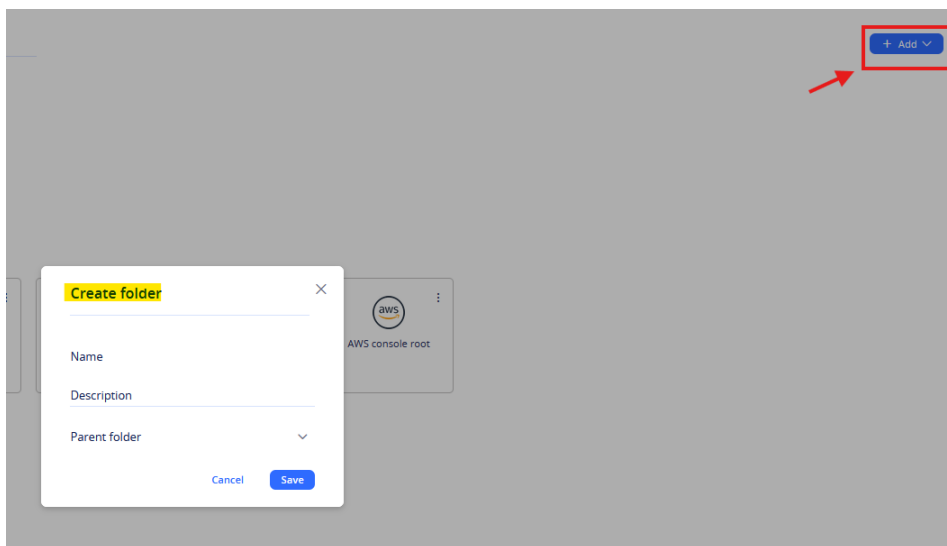


FIGURE 20 – CREATING A FOLDER

2. Drag and drop the icons of applications or secured items directly into the folders.

5.4.2 REMOVING APPLICATIONS OR SECURED ITEMS FROM FOLDERS

1. Click on the **three dots** in the top right corner of the item or application icon you want to remove.
2. Select the **"Remove from folder"** option.

5.5 VIEWING AND COPYING AVAILABLE SECRETS

You can **view** the data of saved items (applications, passwords, notes) by accessing the web interface at <https://eng.cyberark.cloud>, clicking on the three dots on the item's icon, and selecting "Settings".



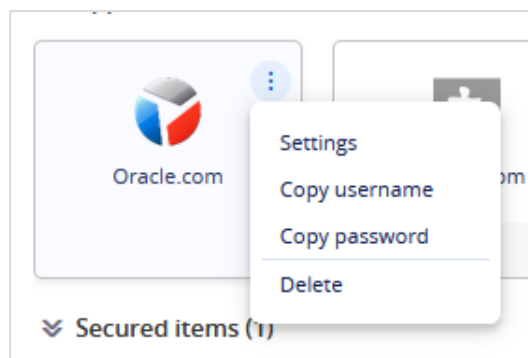


FIGURE 21 – EXAMPLE OF AN APPLICATION WITH THE CONTEXTUAL MENU OPEN

Alternatively, you can quickly copy the saved username or password by selecting the **"Copy username"** or **"Copy password"** options. For "Note" type items, the **"Copy secured note"** option will be available to transfer the content of the "Notes" field to your PC's clipboard.

Another method to retrieve credentials is to open the login page of a saved web application, select the Username and Password fields, and open the dropdown menu by right-clicking.

1. In the desired field, right-click with your mouse to open the dropdown menu.
2. Follow the path **"CyberArk" > "Copy Username"** or **"Copy Password"** > Select the account associated with the site.

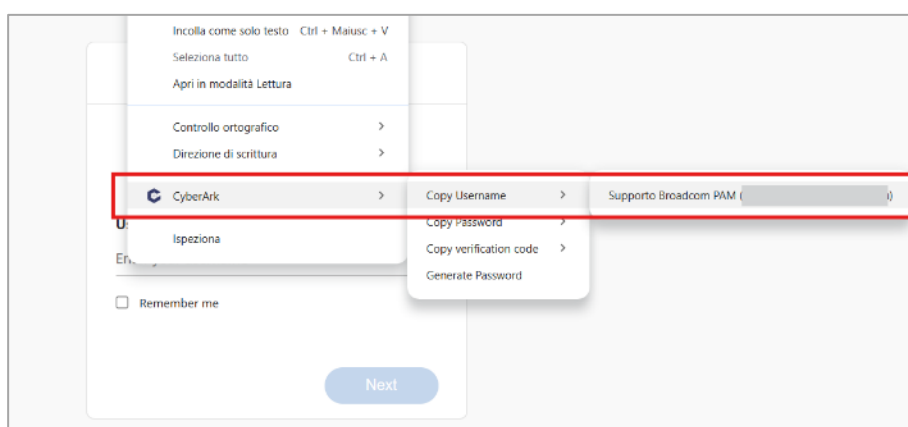


FIGURE 22 – MANUALLY COPYING A CREDENTIAL FROM THE LOGIN PAGE

3. Paste the copied information into the correct field.

5.6 ACCESSING APPLICATIONS

This section offers a comprehensive overview of the automatic login features for applications saved in Eng Password Manager.

NOTE: Due to the varying designs of websites and web applications, automatic login isn't guaranteed to work for all applications. If automatic login results in an error on the login page, you can try recreating the application in the Password Manager either via Land&Catch or manually.

5.6.1 ACCESS VIA PORTAL

Access via the User Portal requires the extension to be installed and active in your browser (see section 4.1).



Once you have logged into the portal:

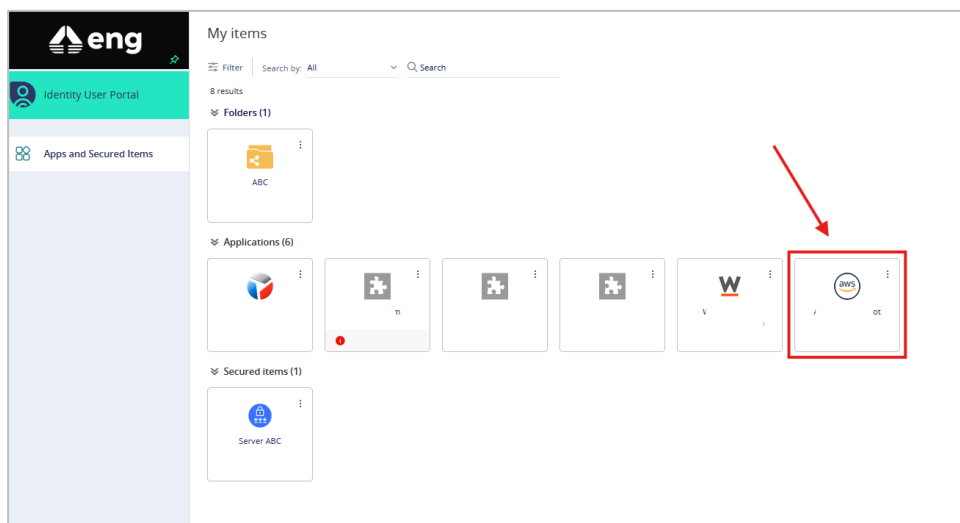


FIGURE 23 – SELECTING THE APPLICATION

1. Locate and click on the desired application.
2. The application's web access page will open in a new browser tab.
3. The extension will automatically fill in the login fields and perform the login.

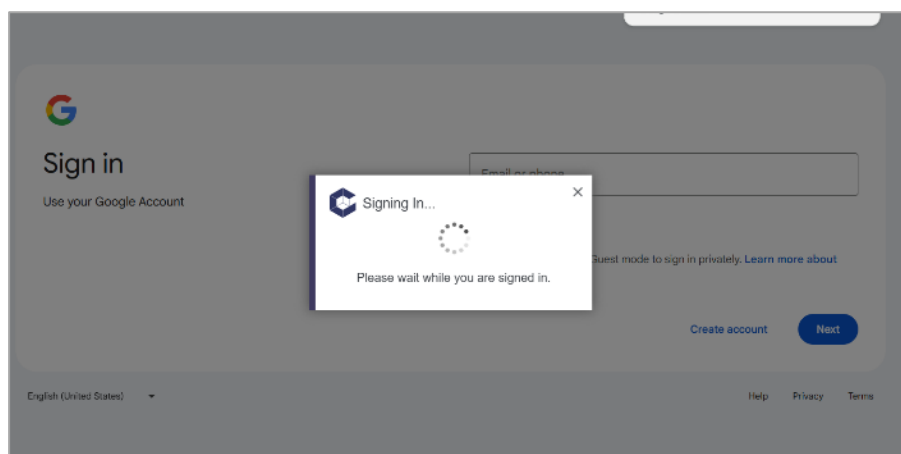


FIGURE 24 – AUTOMATIC FILLING OF LOGIN FIELDS

5.6.2 ACCESS VIA BROWSER EXTENSION

The browser extension offers an even faster and more convenient way to log into applications.

Accessing via the browser extension works identically to accessing via the portal, with the main difference being that you can start the process by clicking the icon in your browser's toolbar.

Once you have logged into the extension:

1. **Select the icon** in the browser's toolbar, where a searchable list of available applications appears.
2. **Click on the application** you wish to access.



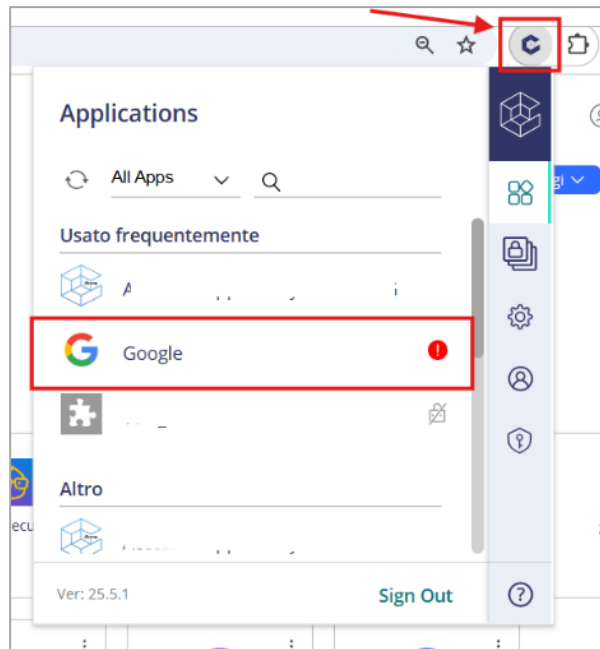


FIGURE 25 – SELECTING AN APPLICATION FROM THE BROWSER EXTENSION

3. The application's web access page will **open in a new browser tab**.
4. The extension will **automatically fill in the login fields** and perform the login.

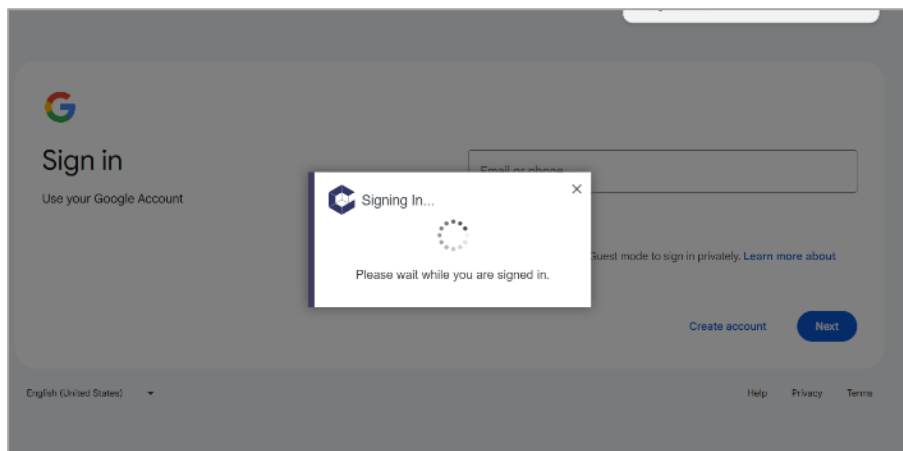


FIGURE 26 – AUTOMATIC FILLING OF LOGIN FIELDS

5.6.3 ACCESS VIA WEB PAGE

There are two different ways to access an application while browsing the web.

5.6.3.1 MANUAL LOGIN

1. Visit the login page for which credentials have been saved.
2. Eng Password Manager automatically detects the login fields, showing a "C" icon.
3. Select the icon, choose the correct account to use, and click "Go".

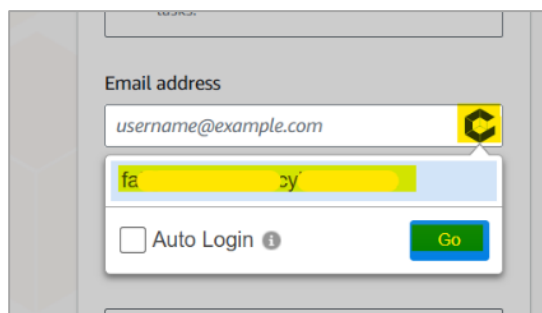


FIGURE 27 - ENG PASSWORD MANAGER ICON ON LOGIN FORM

NOTE: In the small window used to select the correct account, you'll also find the "Auto Login" flag. You can check this box to enable the automatic login feature, which will be described in the next section.

5.6.3.2 AUTOMATIC ACCESS

For all applications that support access via the portal as described in section 5.6.1, you can set up a feature called **"Auto Login."** This allows you to access the application simply by navigating to the application itself. For example, you can decide that if you open www.site.xyz in your browser, the Password Manager will automatically log in with the account for that site, saved under Applications.

1. Open the application settings by clicking on the **three dots** on the item's icon and selecting **"Settings."**
2. Select the **"Auto-login at site"** option and click **"Save"**.

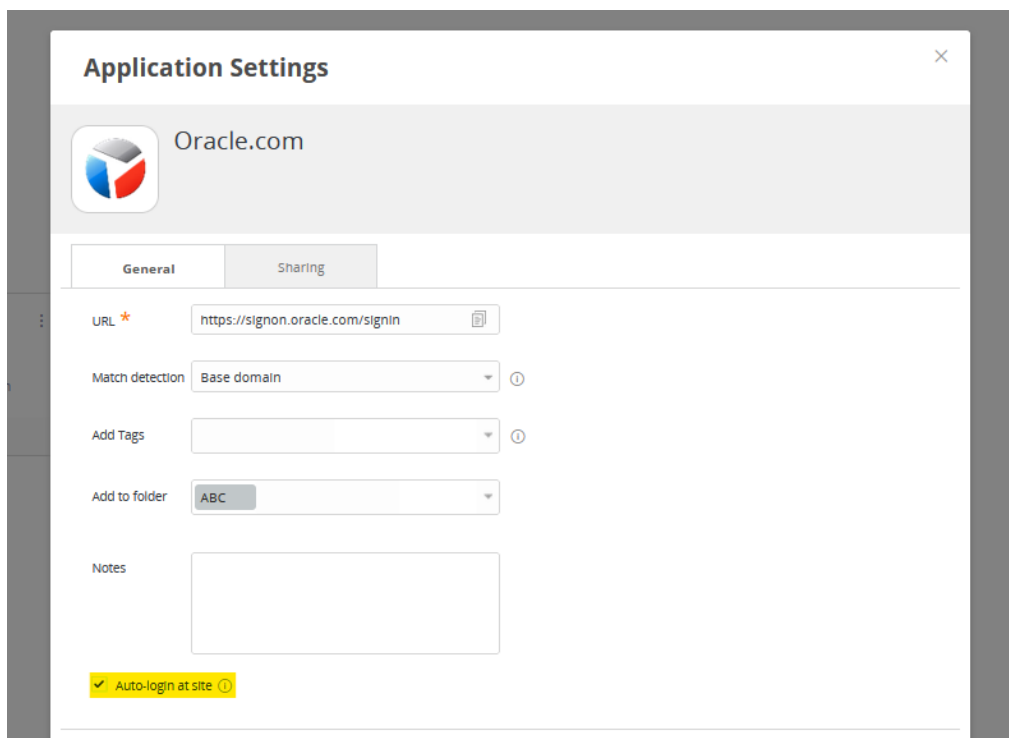


FIGURE 28 - AUTOMATIC ACCESS CONFIGURATION

Every time a browser equipped with the extension visits the site in question, Eng Password Manager will automatically log in.

5.7 SHARING

Eng Password Manager offers a secure method for sharing your items or folders with colleagues or work groups.

The "Share" feature allows Eng Password Manager users to grant other users or groups access to specific applications, secured items, or entire folders. This function is essential for secure collaboration and the controlled management of company resources.

GROUPS PREREQUISITE: in order to share an item with a group of users, that group must have been previously made visible on the Password Manager, as described in Chapter 6.

5.7.1 SHARING APPLICATIONS AND SECURED ITEMS

Sharing individual secured items allows you to grant access to specific sensitive information, such as credentials or secure notes.

How to share:

1. Select the **three dots** next to the chosen item and click on **"Settings."**

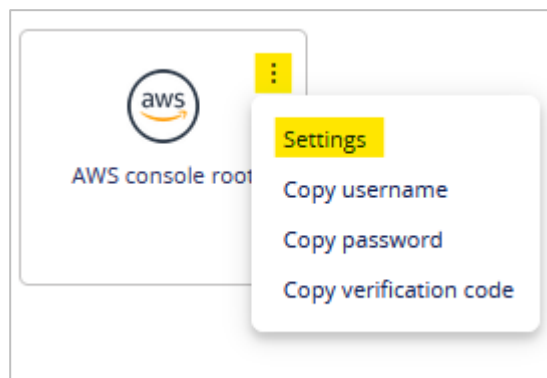


FIGURE 29 – ITEM SETTINGS

2. Move to the **"Sharing" tab** and select **"Add."**

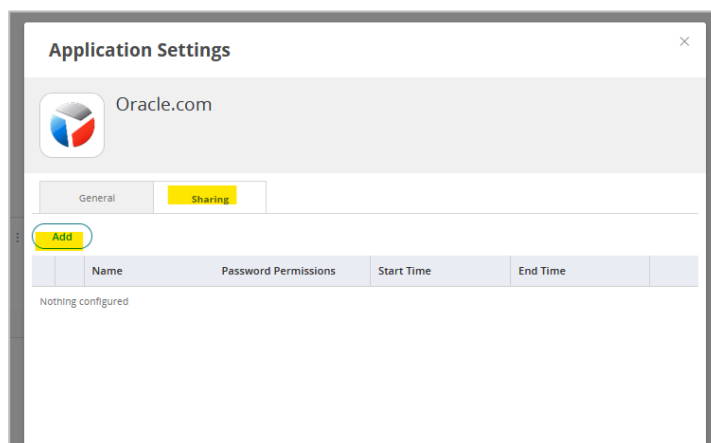


FIGURE 30 – "SHARING" TAB

3. Enter the **email addresses of the users** or the **names of the groups** with whom you want to share the item.
4. Specify the **access permissions** for each user or group with whom you want to share the item:



- a) **None** [available for applications only]: Allows the recipient of the share to automatically authenticate to the web application without being able to see the password in the Password Manager.

Important notes:

- i. Automatic login to the application in question must be supported and functional. The user is advised to test it before sharing.
 - ii. The secrecy of the password with this sharing method depends on the application being accessed. In some cases, the application recipient might use the application itself to view or modify the password after logging in with the Password Manager.
- b) **View password:** Allows only viewing or copying of the password and other fields, but not modification.
- c) **Modify password:** Allows changes to the content.
- d) **Owner:** Grants the recipient complete control over the item, including deletion and the ability to modify the original owner's permissions as well. **If any owner of a secret deletes it, it will also be removed for all other owners.**
5. If you intend to grant authorization for a limited time, you can fill in the "Start Time" and "End Time" fields with the desired days and times.
6. Click **"Save"** to confirm all changes made.

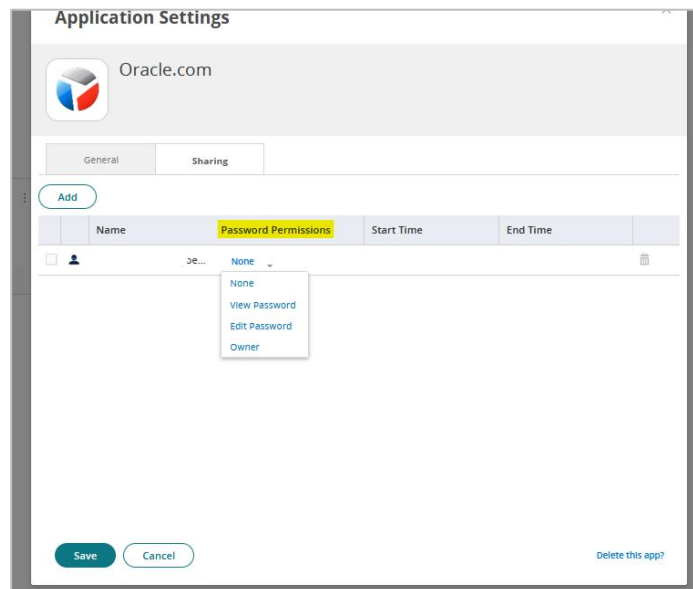


FIGURE 31 – CHOOSING THE TYPE OF SHARING FOR EACH USER OR GROUP

5.7.2 SHARING FOLDERS

Sharing folders lets you grant access to an entire group of applications or secured items all at once, which simplifies permission management.

NOTE: since January 2026, when a folder that contains subfolders is shared, any subfolders and relative items **are automatically shared**. Similarly, if an item is added to a subfolder of an already shared folder, the added item **will be shared as well**.

How to share a folder:

1. Select the **three dots** next to the chosen item and click on **"Share."**



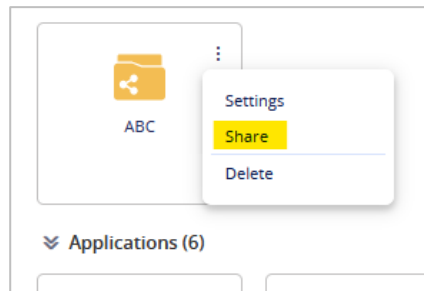


FIGURE 32 – SHARING FOLDERS

2. Select **"Add"** and enter the email addresses of the users or the names of the groups with whom you want to share the folder.
3. Specify the access permissions for each user or group with whom you want to share the folder:
 - a. **View:** This permission allows the recipient to **only view and copy** the secret and other fields of the item. They cannot modify any of the content.
 - b. **Modify:** This permission allows the recipient to **make changes** to the content of the items within the folder.
 - c. **Owner:** This permission grants the recipient **complete control** over the folder. This includes the ability to delete the folder and its contents, and crucially, to also modify the permissions of the original owner.

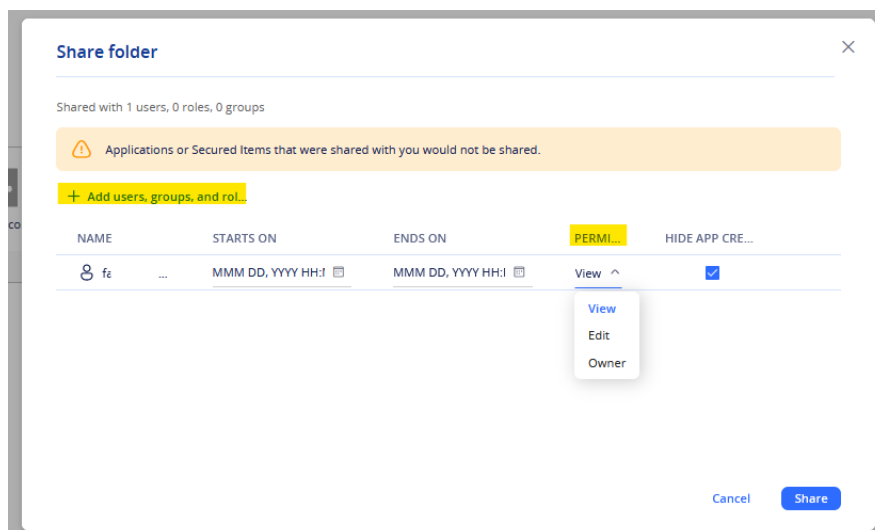


FIGURE 33 – ADDING USERS OR GROUPS

4. If you intend to grant authorization for a limited time, you can fill in the **"Starts on"** and **"Ends on"** fields with the desired dates and times.
5. By selecting **"Hide app credentials"** (a control that only applies to any applications present in the folder), you allow the recipient of the share to automatically authenticate to the web application without being able to see its password in the Password Manager.

Important notes:

- a) The automatic login to each application must be supported and functional. The user is advised to test it before sharing.
- b) The secrecy of the password with this sharing mode depends on the application being accessed. In some cases, the application recipient might use the application itself to view or modify the password after logging in with the Password Manager.
6. Click **"Share"** to confirm all changes made.

5.7.3 HOW TO EFFECTIVELY ORGANIZE SHARES

This section aims to provide some insights to all those who work with shared credentials and other secrets within one or more work groups. To maximize the efficiency of using the Password Manager so that it best meets work needs, **each group must decide how to organize the saving and potential sharing of non-strictly personal credentials.**

Please remember that **not all credentials can be shared**: refer to the warnings in Chapter 3.

Here are the main points of attention to address in each team, with some possible solutions.

5.7.3.1 WHO IS RESPONSIBLE FOR SAVING SHARED SECRETS?

It is recommended to **designate a responsible person (e.g., Team Leader, Client Manager...) who will personally enter** the secrets for the projects/clients they manage into the Password Manager. This person should also **determine how to organize them (in folders) and with which groups to share them**, thereby promoting a **culture of shared responsibility** in managing confidential data.

Anyone who inserts or imports a secret into Eng Password Manager is automatically designated as the **Owner** of that secret.

5.7.3.2 PREVENTION OF SECRET LOSS

A secret is deleted if all users who were owners of it are removed. It is therefore recommended to:

- **Assign more than one owner to every shared secret.**
- **Avoid individual users keeping critical secrets without sharing them.**
- **Ensure that if a person is about to terminate their employment with the Company, they have defined at least one alternative owner for every secret they have shared, and they do not delete delete shared secrets before leaving, otherwise they will also be deleted for the other owners.**

5.7.3.3 ORGANIZING SECRETS IN FOLDERS

We recommend the following:

- **Create shared folders for each project or client.** Optionally, within a client's folder, you can place subfolders related to all that client's projects, along with a generic folder for information that applies across all projects.
- **Establish and use a consistent naming convention** for secrets and folders.

We remind you that each folder must be shared separately, even if it is contained in an already shared folder.

5.7.3.4 LIMITING VISIBILITY AND DURATION ON SHARES

When sharing credentials, always use the principles of need-to-know and least privilege. Make sure you:

- **Don't share a secret with groups larger than necessary or with users who don't need it.**
- **Carefully consider if you should add new secrets to folders shared with many users.**
- **Share secrets in view-only mode if there's no need to grant modification rights.**
- **Share secrets for a specific period whenever a permanent access is not needed.**



5.8 USING THE EXTENSION AND PASSWORD GENERATOR

The Eng Password Manager browser extension, named "CyberArk Identity Browser Extension," simplifies and speeds up access to applications and secured items directly from the browser. It also enables the Land&Catch feature (see paragraph 5.2.3) for capturing and saving passwords entered during web browse. It acts as a bridge between the web portal and the browser, offering a more integrated and fluid user experience.

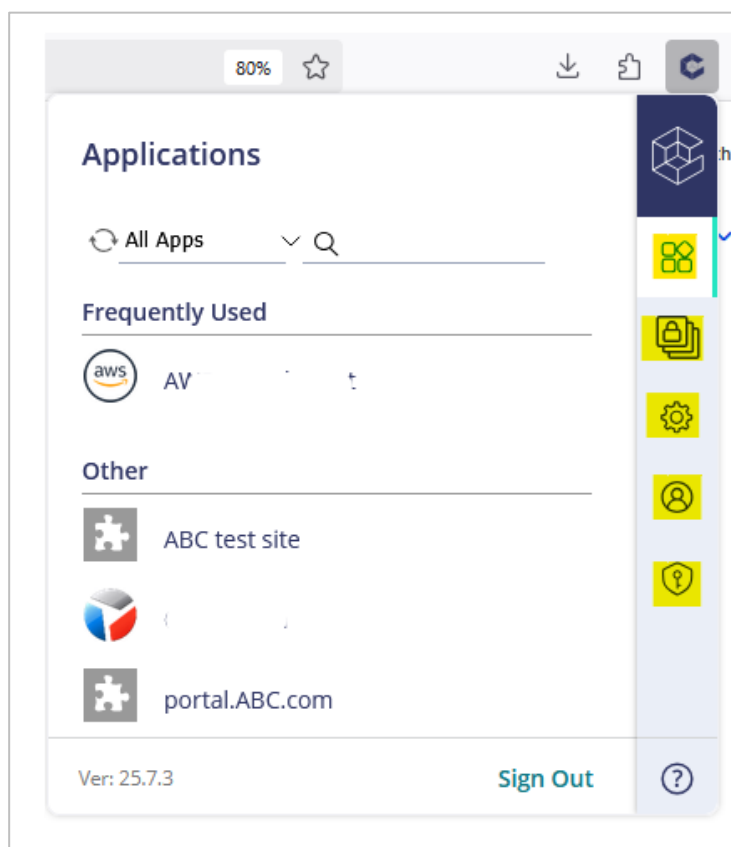


FIGURE 34 – BROWSER EXTENSION

5.8.1 MAIN FUNCTIONALITIES OF THE BROWSER EXTENSION

- **Quick Access to Applications:** By selecting the icon , the extension displays a list of your applications. Clicking on the application's name attempts an automatic connection to it. Alternatively, you can copy the application's username or password by hovering over the application name and selecting the three dots that appear to the right of the name.
- **Quick Access to Secured Items (Passwords and Notes):** By selecting the icon , the extension displays a list of saved items. You can copy the username or password (or the secret content in the case of a note) by hovering over the item name and selecting the three dots that appear to the right of the name.
- **Item Search:** Using the field marked with a magnifying glass icon, you can quickly search for the secret you wish to access.
- **Access to the User Portal:** By selecting the icon , the User Portal opens in a new browser page.
- **Password Generator:** By selecting the icon , a configurable complexity password or passphrase generator is activated, which can be copied and used on any system.

5.9 IMPORTING CREDENTIALS

The credential import function simplifies the transition to Eng Password Manager, allowing you to quickly and securely transfer credentials saved in other password managers, including browsers. This process enables you to consolidate all your sensitive information into a single platform, improving both security and accessibility.

NOTE: it is not possible to import applications with a URL containing 'localhost' or '127.0.0.1', but it is possible to save their credentials in a Password item, as described in section 5.3.1

5.9.1 DIRECT IMPORT VIA PLUG-IN (CURRENTLY ONLY LASTPASS SUPPORTED)

For some sources, the ability to directly import all saved credentials into Eng Password Manager is available (or will be available soon).

Please note that automatic login to Applications (websites or web apps) is less likely to work when they are imported from external password managers compared to when they are configured using the "Land&Catch" method.

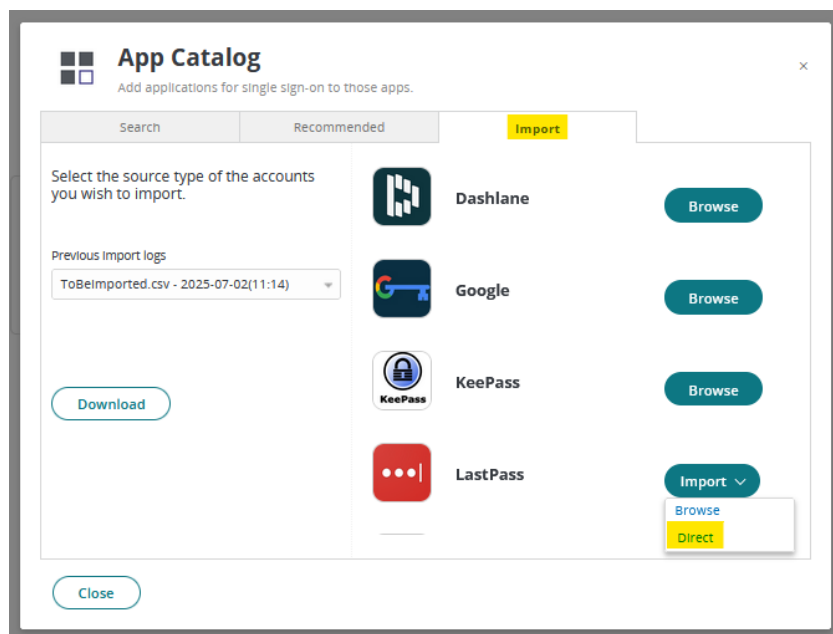


FIGURE 35 – DIRECT CREDENTIAL IMPORT

1. **Importing into Eng Password Manager:**
 - a) Access the User Portal: <https://eng.cyberark.cloud>
 - b) Select the option "Add – Catalog or imported app" and move to the "Import" tab.
 - c) Next to the applications that support direct import, the "Import" button is available. Select "Import > Direct" next to the chosen application.
 - d) Follow the on-screen instructions.
2. **Verification of imported credentials:** After importing, carefully check the number and correctness of the imported credentials.

5.9.2 IMPORTING FROM KEEPASS VIA KDBX FILE

It is possible to import an encrypted archive in KDBX format from the KeePass password manager, by uploading it directly into Eng Password Manager. If the folder structure present in KeePass does not already exist, it will be recreated.



It is also possible to import credentials exported from KeePass in CSV format (as described in the following paragraph), but importing via a KDBX file is strongly recommended as it preserves or recreates any existing folders.

NOTE: Only KDBX files protected by a master password are accepted.

1. Importing into Eng Password Manager:

- a) Access the User Portal: <https://eng.cyberark.cloud>
- b) Select the option “**Add – Catalogue or imported App**” and move to the “**Import**” tab.
- c) Next to the KeePass entry, select “Browse” and locate the KDBX file on your PC.
- d) Follow the on-screen instructions, which will require entering the master password of the uploaded file. If duplicate records are detected, you will be able to choose whether to skip or keep the duplicates during the import process.

2. Verification of imported credentials: After the import is complete, carefully check the number and accuracy of the imported credentials.

5.9.3 IMPORT VIA CSV FILE

To import secrets from sources that do not offer the “Import” function, it is necessary to extract the secrets from those sources and provide them to Eng Password Manager via a standard CSV file.

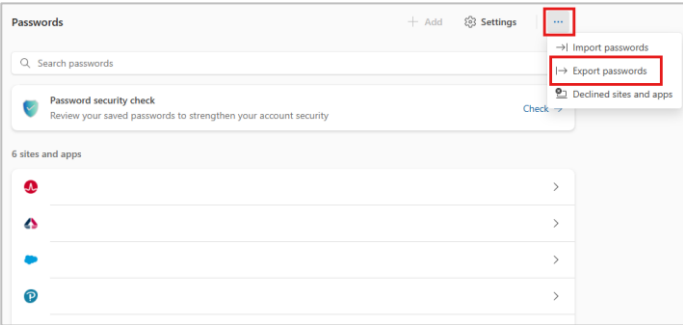
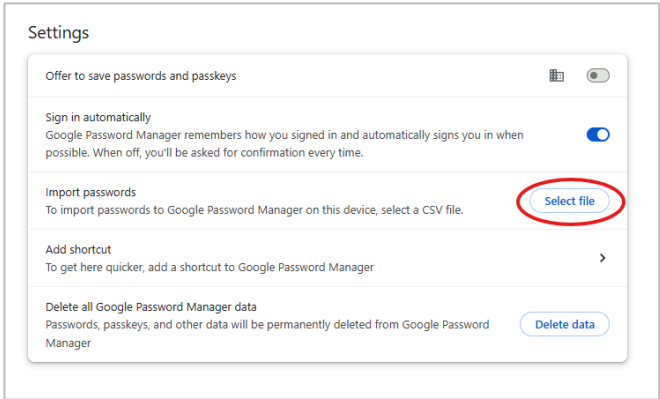
5.9.3.1 LIMITATIONS ON CSV FILES

- Each imported CSV can contain up to **1000 rows**. If you need to import a CSV with more than 1000 rows, split it into multiple files, each with a maximum of 1000 rows. Remember that the first row of each split file must contain the header from the original CSV.
- The **name**, **username**, and **notes** fields:
 - Cannot start with the character `<`
 - Cannot contain the character sequence `&#`
- The **folder** field cannot contain the characters `<` `>` `{}` nor the character sequence `&#`
- [Currently applicable only for CSV extracted from Last Pass – will be extended to all CSVs soon] The `\` character in the **folder** field is interpreted as a folder separator in a path. For example, if a secret has “father\son” in the folder field, the secret is placed in the “son” folder inside the “father” folder. Any folders specified in the CSV are created on Eng Password Manager if they do not already exist.
- The **URL** field cannot contain “localhost” or “127.0.0.1”.



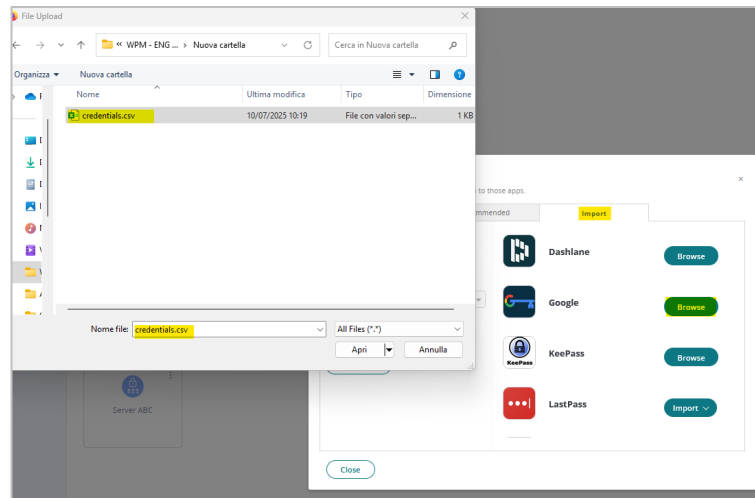
5.9.3.2 IMPORTING CREDENTIALS FROM MICROSOFT EDGE AND GOOGLE CHROME BROWSERS

Follow the instructions below for each browser:

Microsoft Edge	Google Chrome
Open the following address with Edge: edge://wallet/passwords Click on the Passwords menu (three dots) and choose "Export passwords" 	Open the following address with Chrome: chrome://password-manager/settings Click on "Download File" next to the "Export Password" option. 
The file "Microsoft Edge Passwords.csv" containing your passwords saved in Edge in plain text will be saved to your PC.	The "Chrome Passwords.csv" file containing your passwords saved in Chrome in plain text will be saved to your PC
Verify that the CSV file does not have the incompatible characteristics described in the paragraph 5.9.3.1.	

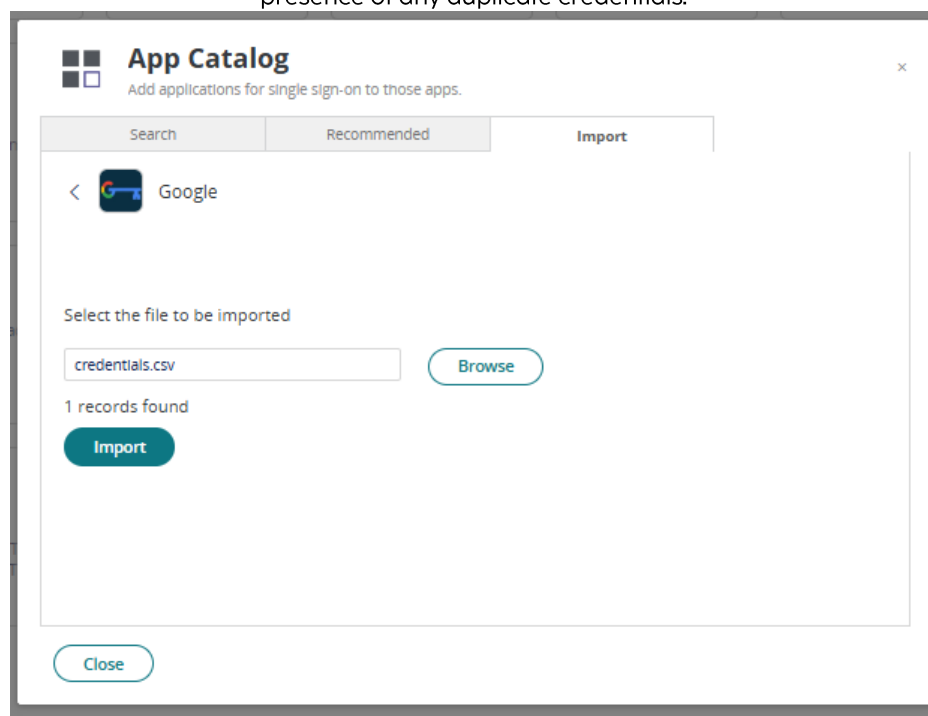


Access the Eng Password Manager User Portal, select the option **"Add – Catalog or imported app"** and navigate to the **"Import"** tab



Select **"Browse"** next to the **"Google"** entry and choose the CSV file exported from your browser.

Click on **"Import"** in the subsequent summary screen, which shows the number of credentials found in the file and the presence of any duplicate credentials.



The import activity will be executed silently and may take up to a few minutes, depending on the number of credentials to import. The credentials will progressively appear in the User Portal.

IMPORTANT: Delete the CSV file containing plain-text passwords from your PC (even from the recycle bin).

IMPORTANT: Delete the passwords transferred to Eng Password Manager from the source browser.

5.9.3.3 IMPORTING CREDENTIALS FROM MOZILLA FIREFOX BROWSER

Open **about:logins** with Firefox.

Click on the menu in the top right (three dots) and choose "Export passwords."



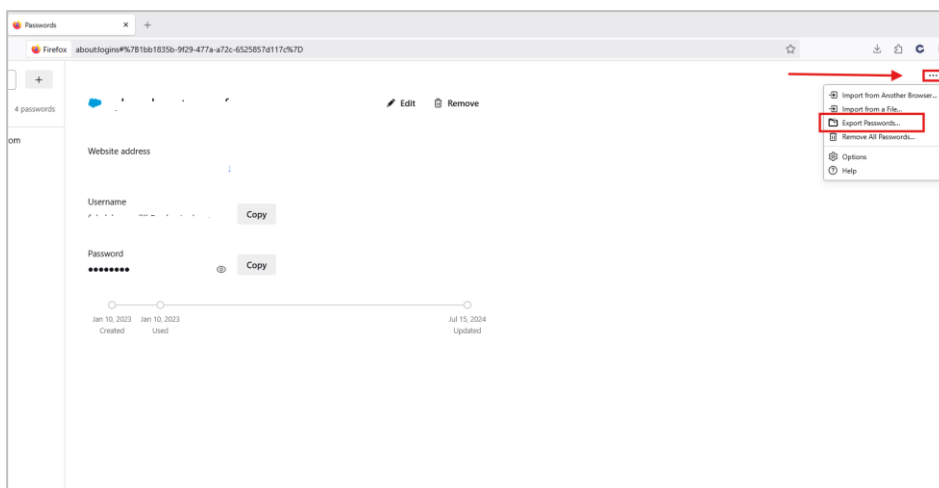


FIGURE 36 – EXPORTING CREDENTIALS FROM MOZILLA FIREFOX

Click **"Continue with Export"** to close the information pop-up:

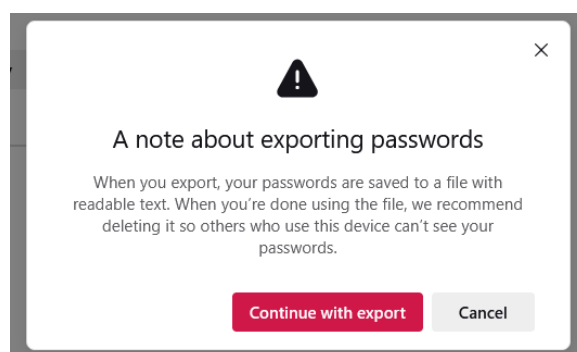


FIGURE 37 – WARNING: EXPORTING PASSWORDS FROM MOZILLA FIREFOX

The file **password.csv** containing the passwords saved in Firefox in plain text will be saved to your PC. This file does not contain names for the credentials, which Eng Password Manager requires. It is therefore necessary to modify the **password.csv** file exported from Firefox as follows:

1. Add a column at the beginning, with the value **"name"**, in the header row.
2. Add a name for each credential in the subsequent rows of the file. The name must be enclosed in double quotes and followed by a comma, for example, **"MyApp.com"**.

To quickly make this modification, you can use the **Firefox-Import-Tool.xlsx** file that has been specifically prepared, and can be downloaded from the same folder where this User Guide is located.

Alternatively, the CSV file can be modified using a text editor (e.g., Notepad on Windows) or Microsoft Excel.

Attention: If you prefer to use Microsoft Excel to modify the CSV file, be aware that in some countries (including Italy), Excel saves CSV files by replacing the comma separator "," with another separator (e.g., semicolon ";"). In this case, the CSV must then be re-adapted by replacing the alternative separator character with a comma, which is the only standard separator accepted by Eng Password Manager.

After making the modifications, verify that the CSV file does not have the incompatible characteristics described in paragraph 5.9.3.1.

Once the CSV is prepared, access the Eng Password Manager User Portal, select the option **"Add – Catalog or imported app,"** and move to the **"Import"** tab.

Select **"Browse"** next to the **"Other"** entry and select the modified CSV file.

Click on **"Import"** in the subsequent summary screen, which shows the number of credentials found in the file and the presence of any duplicate credentials.

The import activity will be executed silently and may take up to a few minutes, depending on the number of credentials to import. The credentials will progressively appear in the User Portal.

IMPORTANT: Delete the CSV files with plain-text passwords from your PC (including from the recycle bin).

IMPORTANT: Delete the passwords transferred to Eng Password Manager from Mozilla Firefox.

5.9.3.4 IMPORTING CREDENTIALS FROM OTHER SOURCES

1. Export from the source password manager:

- The first step is to export your credentials from your current password manager or browser. Most password managers allow export in CSV (Comma Separated Values) format.
- Look for the "Export" or "Export data" option in your password manager's settings.
- Choose the CSV format.
- Save the exported file to a specific location on your company PC, from which it must be deleted after the operation is complete.

2. CSV file formatting:

Some popular password managers (like Google, KeePass, Dashlane) export CSV files that are already formatted to be compatible with Eng Password Manager. In these cases, the exported file can generally be imported directly without further modifications (though it's still recommended to review the notes below).

With other password managers, you might need to reformat the CSV file to align with Eng Password Manager's requirements. This process could involve reorganizing columns, changing header names, or removing unnecessary data.

Eng Password Manager provides a **CSV template** that can be downloaded from its import interface (via the "Download template" link under the generic "Other" application). Using this template ensures the file is correctly formatted.

- **NOTE 1:** The CSV template includes a field named **url**. If this field is populated, Eng Password Manager will treat the imported credential as an **Application**; if it's empty, the credential will be imported as a **Password** item.
- **NOTE 2:** The CSV template includes a field named **folder**. In this field, you can specify the name or the path of the folder where each secret should be imported. In fact, the **** character in the **folder** field is interpreted as a folder separator in a path. For example, if a secret has "father\son" in the folder field, the secret is placed in the "son" folder inside the "father" folder.

Any folders specified in the CSV are created on Eng Password Manager if they do not already exist. It's not possible to import a secret from CSV directly into a folder shared by another user.

Before importing, ensure the CSV file does not have the incompatible characteristics described in paragraph 5.9.3.1.

3. Import into Eng Password Manager:

- Access the portal.
- Select **"Add – Catalog or imported app"** and navigate to the **"Import" tab**.
- Upload the CSV file after selecting **"Browse"** next to the source application type.



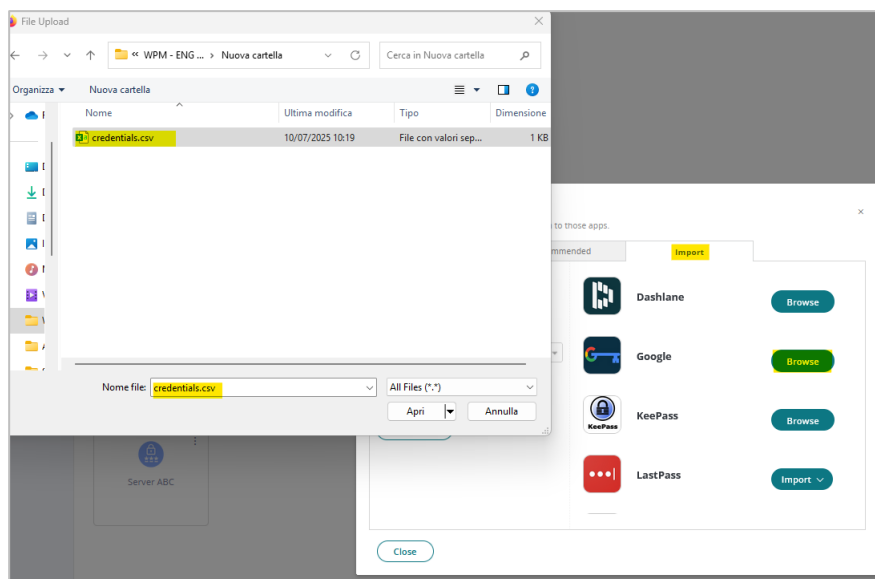


FIGURE 38 – IMPORT CREDENTIALS WITH .CSV

- Fare Click "**Import**" on the next summary screen, which shows the number of credentials found in the file and any duplicates.
 - The import process will run silently and can take a few minutes, depending on how many credentials you're importing. The credentials will progressively appear in the User Portal.
4. **Verify Imported Credentials:** After importing, carefully check the number and accuracy of the imported credentials.
 5. **Delete the Exported File:**

IMPORTANT: Delete the CSV files containing plaintext passwords from your PC (including from the recycle bin).

IMPORTANT: Delete the passwords transferred to Eng Password Manager from the source software.

6 REQUESTING A GROUP

The Eng Password Manager solution allows for the archiving and management of applications and secured items for personal use and for group (shared) use, as illustrated in paragraph 5.7.

To enable sharing applications and secured items with an entire group of people, that group must be visible on the platform. There are two possible scenarios:

- **The group already exists (or can be created) on the company's Active Directory** – the existing group can be imported into Eng Password Manager. Any modification to the group (adding or deleting members) must be done on the Active Directory.
- **The group does not exist (and it is not desired to create it) on the company's Active Directory** – the group will be created directly in Eng Password Manager. Any modification to the group (adding or deleting members) must be done within the Password Manager.

6.1 HOW TO REQUEST GROUP ACTIVATION OR MODIFICATION

Any request for the activation, modification, or deletion of a group must be submitted to the Password Manager support group by sending an email to servicedesk_internalit@eng.it with the subject line containing "ENG Password Manager – Request for the MSS CYBERTECH group". A ticket will be opened, and the request will be processed.

Every request for **group creation** must contain:

- The name of the group to be created on the Password Manager [e.g., ProjectAlphaDevelopers]



- A description of the group [e.g., Team involved in application development for Project Alpha]
- The group members:
 - If the group needs to be mapped to an existing group on the Company's Active Directory: indicate the exact name of the A.D. group [e.g., AlphaDev].
 - If the group does not need to be mapped to one on the Company's Active Directory: provide a list of the corporate email addresses of the desired members.

Every request for **group modification** must contain:

- The name of the group to be modified [e.g., ProjectAlphaDevelopers]
- Any new name or new description for the group (optional)
- [Only for groups not mapped to groups on the Company's Active Directory] Any members to be added or removed.

7 CURRENT LIMITATIONS AND FUTURE DEVELOPMENTS

7.1 DIRECT IMPORT OF CREDENTIALS FROM BROWSERS IS NOT SUPPORTED

Currently, you need to export credentials from browsers in CSV format and then import them manually.
[A planned update from the vendor will enable direct import of credentials from common browsers.](#)

7.2 THE MOBILE APPLICATION IS CURRENTLY NOT USABLE IN ENGINEERING

Currently, it is only possible to access Eng Password Manager from a mobile device by accessing the User Portal from the corporate Edge browser on an Android or iOS device equipped with an Engineering MDM solution.
[A planned update from the manufacturer will enable the use of the mobile app.](#)

7.3 THE EXTENSION ICON IS BARELY VISIBLE ON BROWSERS WITH DARK THEMES

The browser extension icon, which is dark blue, is hard to see on browsers set to a dark interface.
[The vendor is currently looking into this issue.](#)

7.4 FOLDER NUMBER AND CAPACITY LIMITS

Each user can create a maximum of 800 folders. Each folder can contain a maximum of 800 items (including applications, passwords, and notes) and up to 100 subfolders.

7.5 IT IS NOT POSSIBLE TO IMPORT A FOLDER TREE

While you can import various secrets via CSV, with each placed in a specified folder, the organization of folders into a hierarchical structure (folders within folders) must be done directly within the Password Manager, either before or after the import.

7.6 LIMIT ON SECRET IMPORTABLE WITH A SINGLE CSV FILE

Currently, you can import a maximum of 1000 secrets at once from a single CSV file. If you have more than 1000 secrets, you'll need to split them into multiple CSV files and import them separately.

7.7 LIMITATIONS ON SPECIAL CHARACTERS IN DATA IMPORTED FROM CSV

Certain characters in CSV files can prevent secrets from being imported or cause them to be placed outside their intended folders. The specific limitations you need to be aware of are described in paragraph 5.9.3.1.
Before importing secrets from a CSV file, check for incompatible characters and either remove or replace them.

