Guide

# JumpCloud Password Manager Guide

# Contents

## Password Manager Overview

JumpCloud now offers a richly featured password manager fully integrated into the JumpCloud product and all single-sign-on applications. The JumpCloud Password Manager enables teams to securely manage and share passwords, 2FA (two-factor authentication) tokens, and other types of sensitive information while providing comprehensive visibility and control over passwords used across the organization. IT admins and users will have a seamless authentication experience without relying on a third-party solution.

### Key Features

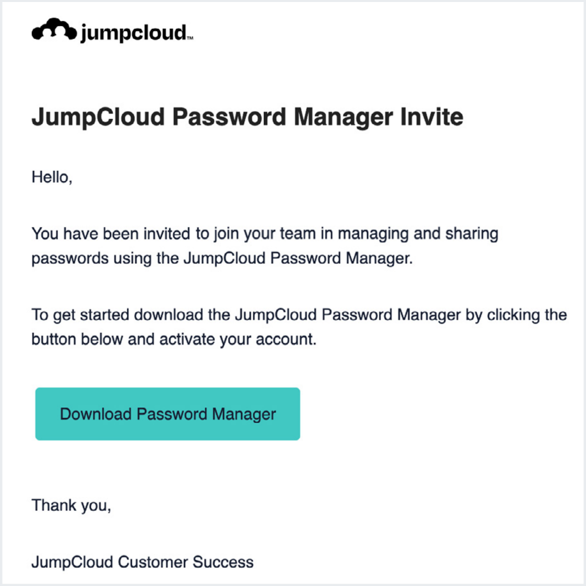
- **Store secrets locally**: passwords and other secrets are locally encrypted on devices and synced with end-to-end encryption
- **Autofill passwords**: users can store and autofill passwords and 2FA tokens
- **Securely share passwords**: users and groups can share passwords and 2FA tokens without compromising security
- **Generate strong passwords**: the JumpCloud Password generator creates strong, complex, and unique passwords
- **Administrative controls and reporting**: admins can provision and remove access to the password manager and also can generate password usage reports

## Password Manager Enrollment

Users wanting to enroll in Password Manager must be enrolled as a JumpCloud user; this also includes admin accounts. To take full advantage of Password Manager functionality, users should add JumpCloud Password Manager to their devices from the applicable app store or play store.

### End User Enrollment

1. You will receive a Password Manager Invite email, and will be prompted to **Download Password Manager**.



**JumpCloud Password Manager Invite**

Hello,

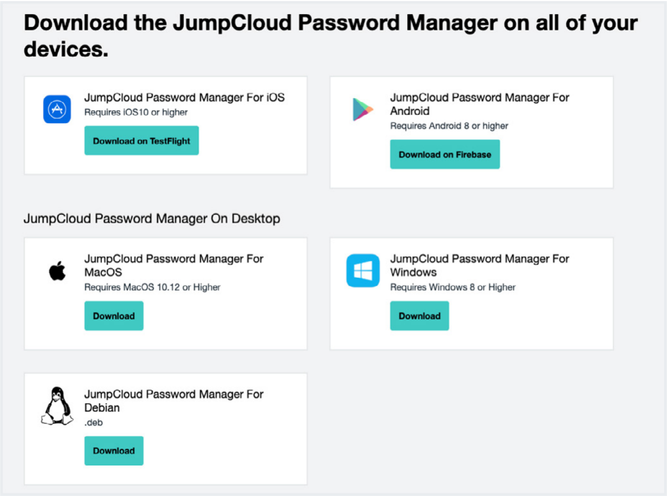
You have been invited to join your team in managing and sharing passwords using the JumpCloud Password Manager.

To get started download the JumpCloud Password Manager by clicking the button below and activate your account.

Thank you,

JumpCloud Customer Success

2. Follow prompts to download and launch the application.



**Download the JumpCloud Password Manager on all of your devices.**

JumpCloud Password Manager For iOS
Requires iOS10 or higher

JumpCloud Password Manager For Android
Requires Android 8 or higher

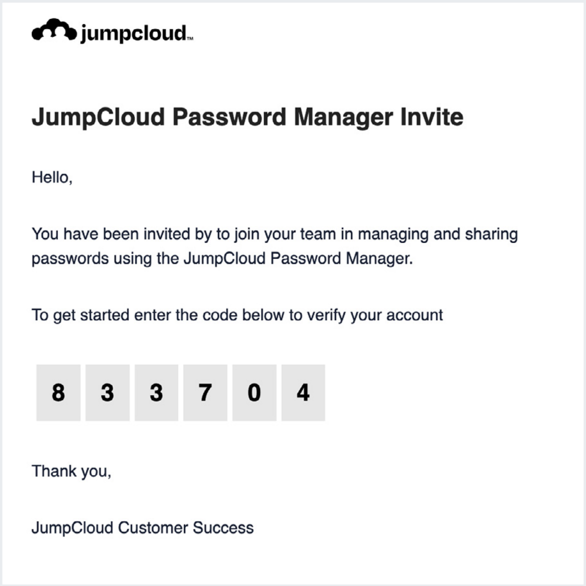
JumpCloud Password Manager On Desktop

JumpCloud Password Manager For MacOS
Requires MacOS 10.12 or Higher

JumpCloud Password Manager For Windows
Requires Windows 8 or Higher

JumpCloud Password Manager For Debian
.deb

3. Once the application is launched, you will receive another email; this one contains a verification code to enter on the **Verify Account** page in the application.



**JumpCloud Password Manager Invite**

Hello,

You have been invited by to join your team in managing and sharing passwords using the JumpCloud Password Manager.

To get started enter the code below to verify your account

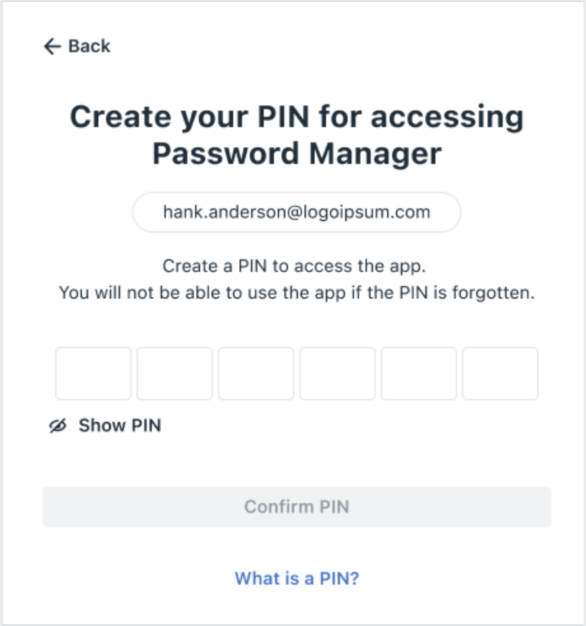
8 3 3 7 0 4

Thank you,

JumpCloud Customer Success

4. Once the account is verified, you will be prompted to create and confirm a PIN.

   **Important**: this PIN is how you will access the application, and should be something you can remember.



← Back

Create your PIN for accessing Password Manager

hank.anderson@logoipsum.com

Create a PIN to access the app.
You will not be able to use the app if the PIN is forgotten.

5. Once the PIN is confirmed enrollment is complete.

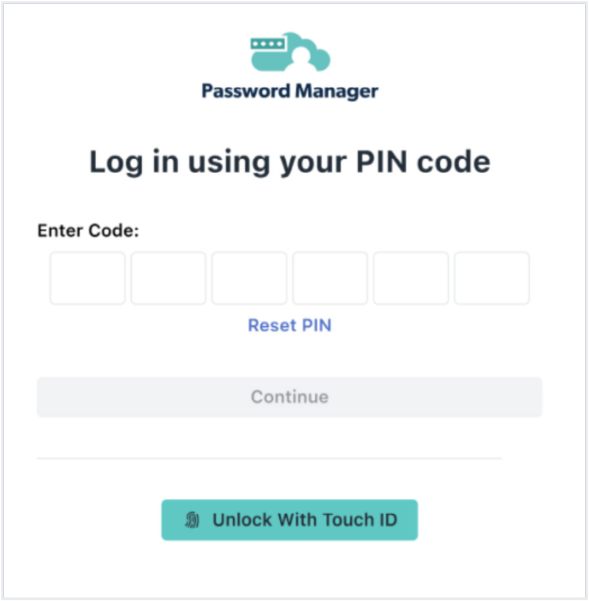
## JumpCloud Password Manager Forgotten PIN

JumpCloud Password Manager enables teams to securely manage and share passwords, 2FA (two-factor authentication) tokens, and other types of sensitive information while providing IT admins with full visibility and control over passwords used across the organization.

During the Password Manager Enrollment process you are prompted to create a 6-digit PIN, which is from that point on how you will access the application. In most cases, Password Manager is also accessible with biometrics, whether on a laptop or device. On laptops users can access the application with TouchID or Windows Hello. On iOS and Android devices, FaceID or TouchID can be used.

In the case where biometrics are not being used, and the user PIN is forgotten, follow this process:

1. When you are presented with the login page, if you do not remember your PIN and can’t access Password Manager with biometrics, select the **Reset PIN** button.



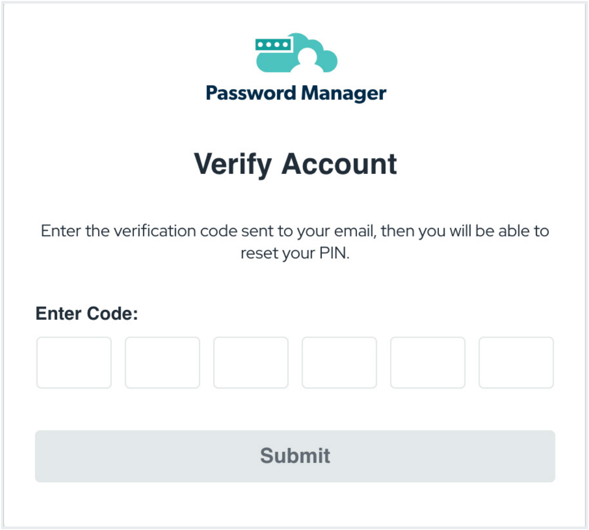
Password Manager

Log in using your PIN code

Enter Code:

2. An email with a reset code will be sent to your JumpCloud registered email address.
3. Enter the code sent via email to verify your account, after which you will be able to create a new PIN and log into Password Manager.

   **Note:** You will be asked to enter their new PIN three times: once to set the new PIN, a second time to verify the new PIN, and a third time to actually log into Password Manager.



Password Manager

Verify Account

Enter the verification code sent to your email, then you will be able to reset your PIN.

Enter Code:

# Browser Extensions and Import Tool

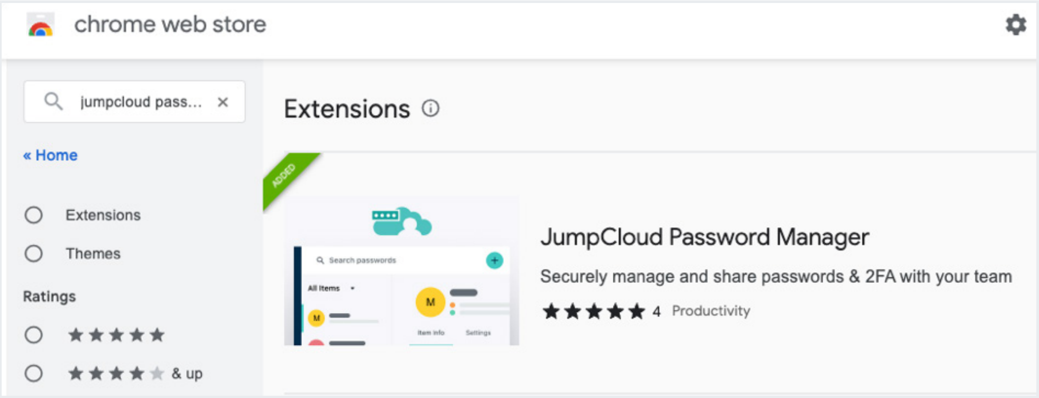
## Browser Extensions

Once you have the JumpCloud Password Manager installed as a desktop and mobile app, the next step is to install the Password Manager browser extension.

**Considerations**:
We recommend downloading the browser extension during or after installing JumpCloud Password Manager.

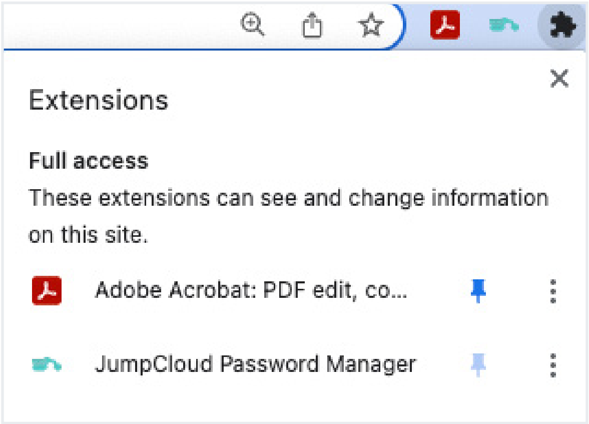
**Download your extension**:

- We offer extensions on a wide variety of browsers: Chrome, Firefox, Safari, Opera, Brave, and Edge.
- You will be prompted to download an extension during the installation of the Password Manager desktop application, but the step can be skipped and done later.
- To download an extension after the installation, navigate to the web stores for the desired browser and search for JumpCloud Password Manager. For example, https://chrome.google.com/webstore/category/extensions.



Securely manage and share passwords & 2FA with your team

- Once installed, access the extension by clicking on the puzzle piece in the upper right corner of your browser window. Select the pushpin icon next to this extension to pin it to the browser window.

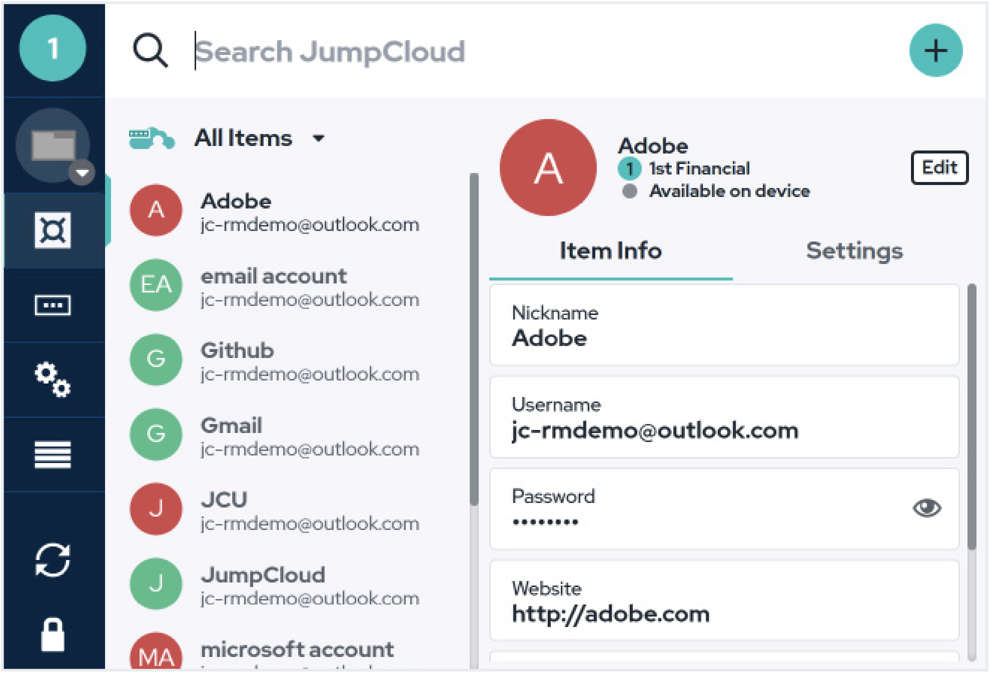


These extensions can see and change information on this site.

## Browser Extension Overview

The browser extension is broken into three parts.

The left margin shows the different sections of the extension.



A Adobe jc-rmdemo@outlook.com

EA email account jc-rmdemo@outlook.com

G Github jc-rmdemo@outlook.com

G Gmail jc-rmdemo@outlook.com

J JCU jc-rmdemo@outlook.com

J JumpCloud jc-rmdemo@outlook.com

MA microsoft account

A Adobe
1 1st Financial
Available on device

Nickname
Adobe

Username
jc-rmdemo@outlook.com

Password
••••••••

Website
http://adobe.com

The middle section shows all the vault items.

The far right section shows the details of the currently selected item.

**Profile Picture**: this is just an identifier - an initial of the user.

**Folder**: users can select which folder to view, such as All Items or other folders which have been set up for personal or work use.

**Vault**: this will show items in the selected folder, along with details of the selected item. You can select a specific type of vault item to view from the All Items dropdown menu.

**Password Generator**: you can create passwords of varying complexity.

**Settings**: you can set preferences for setting the JumpCloud Password Manager as default, unpairing on exit, and other details like behavior with forms, 2FA, and the backup schedule.

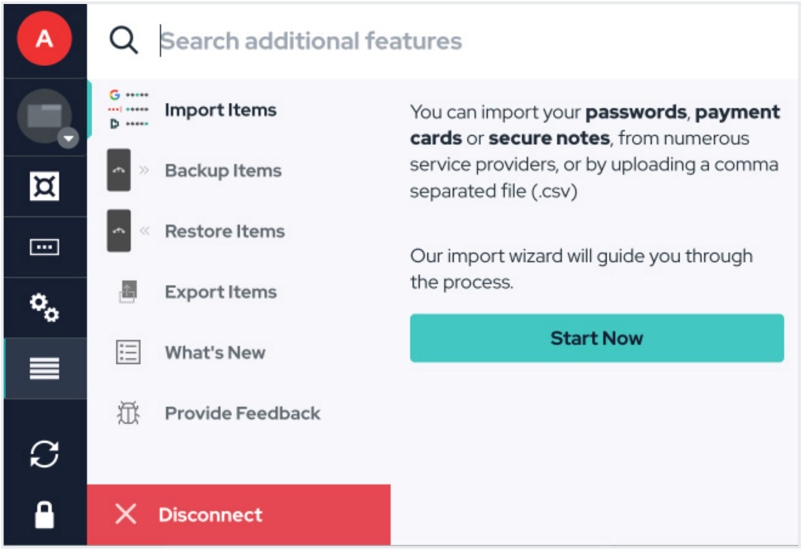
**Import Tool**: you can import passwords and other information from a previous application. See details for this in the Import Tool section below.

**Refresh Button**: click the refresh icon to force a refresh of the browser extension.

**Lock**: clicking the lock icon will lock Password Manager.

## Import Tool

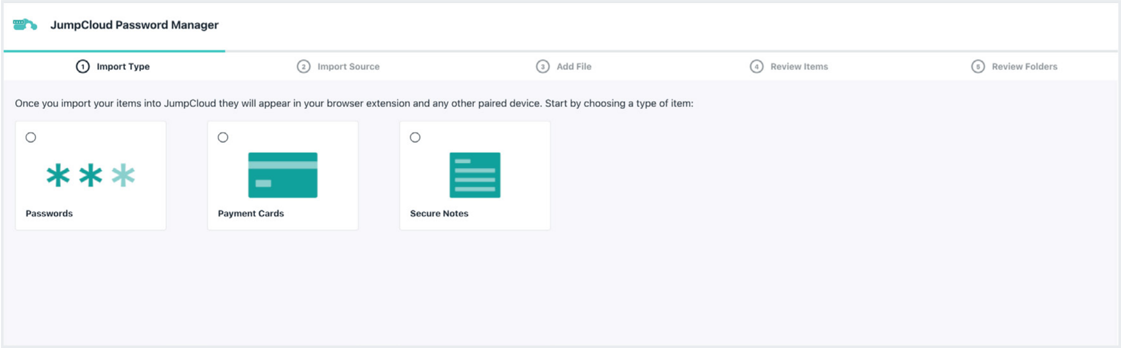
The import tool lets you bring in data from a previous data manager by importing it with a CSV or an Excel file. This can be done at any time and passwords can be imported from the Browser Extension or Desktop App. For this example we'll import passwords using the Browser Extension.



You can import your **passwords**, **payment cards** or **secure notes**, from numerous service providers, or by uploading a comma separated file (.csv)

Our import wizard will guide you through the process.

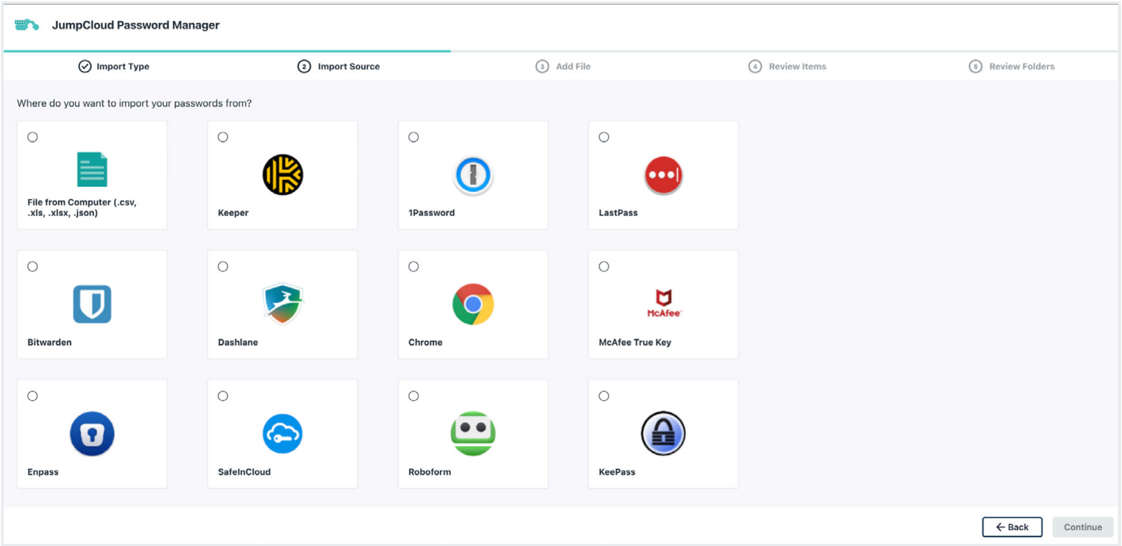
- To begin, click the **Start Now** button.
- From the import tool screen, choose which type of data you want to import. For this example, we will import passwords, so select Passwords and click the **Continue** button.



Once you import your items into JumpCloud they will appear in your browser extension and any other paired device. Start by choosing a type of item:

- From this screen you can select to import from an already existing file on your computer, or you can choose from one of the existing password manager applications. Select whichever you want, and click the **Continue** button.

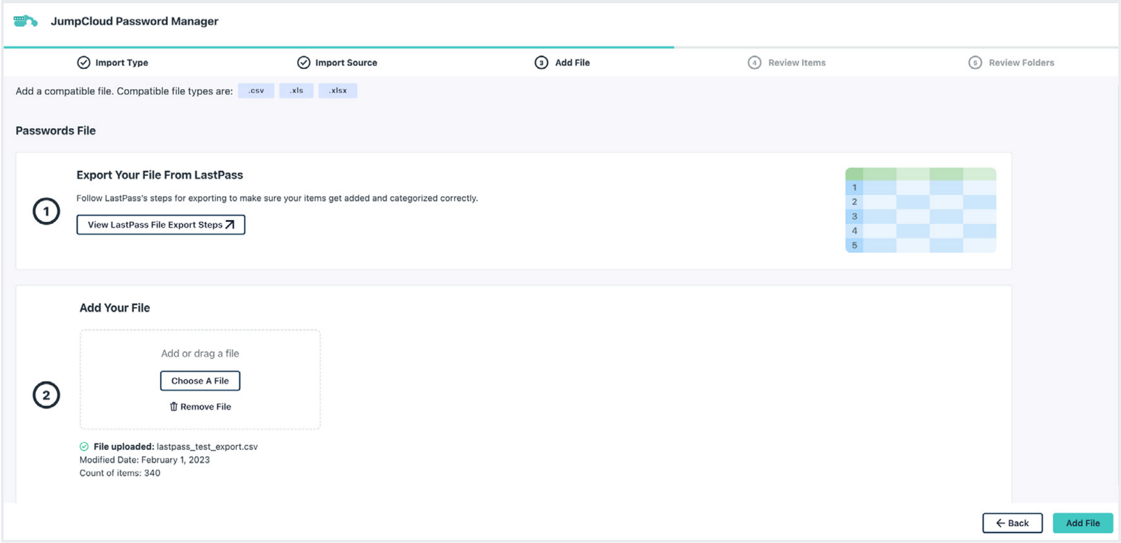
**Note:** Whichever option you choose, you will need to have exported your data from that application and know the location of that file on your computer.



Where do you want to import your passwords from?

○ File from Computer (.csv, .xls, .xlsx, .json)
○ Keeper
○ 1Password
○ LastPass
○ Bitwarden
○ Dashlane
○ Chrome
○ McAfee True Key
○ Enpass
○ SafeInCloud
○ Roboform
○ KeePass

- Follow the on screen instructions to add or drag a file, then click the **Add File** button.



Add a compatible file. Compatible file types are: .csv .xls .xlsx

Passwords File

1 Export Your File From LastPass

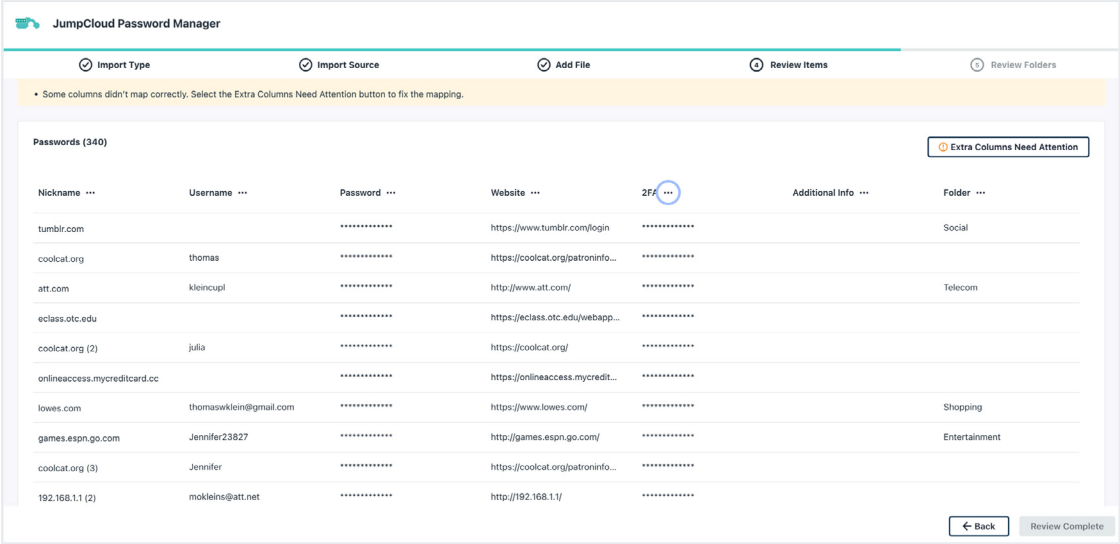
Follow LastPass's steps for exporting to make sure your items get added and categorized correctly.

2 Add Your File

Add or drag a file

File uploaded: lastpass_test_export.csv
Modified Date: February 1, 2023
Count of items: 340

- On this step, you can review your items and the column mapping. You can use the three dots to change the column mapping, or if you receive the Extra Columns Need Attention alert, select that button to edit the flagged column headers. Once done, click **Review Complete** to move to the next step.

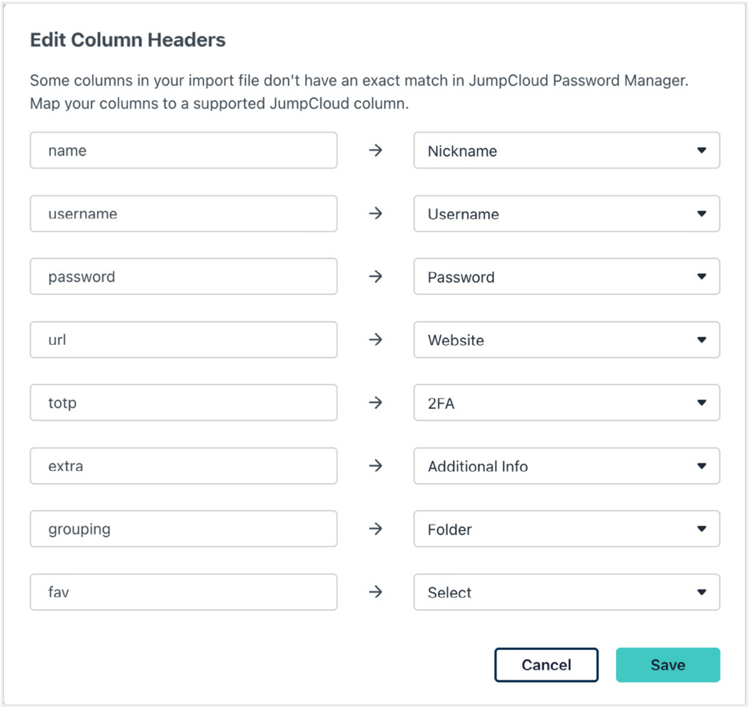


JumpCloud Password Manager

- Some columns didn't map correctly. Select the Extra Columns Need Attention button to fix the mapping.

Passwords (340)

| Nickname ··· | Username ··· | Password ··· | Website ··· | 2FA ··· | Additional Info ··· | Folder ··· |
|---|---|---|---|---|---|---|
| tumblr.com | | ************* | https://www.tumblr.com/login | ************* | | Social |
| coolcat.org | thomas | ************* | https://coolcat.org/patroninfo... | ************* | | |
| att.com | kleincupl | ************* | http://www.att.com/ | ************* | | Telecom |
| eclass.otc.edu | | ************* | https://eclass.otc.edu/webapp... | ************* | | |
| coolcat.org (2) | julia | ************* | https://coolcat.org/ | ************* | | |
| onlineaccess.mycreditcard.cc | | ************* | https://onlineaccess.mycredit... | ************* | | |
| lowes.com | thomaswklein@gmail.com | ************* | https://www.lowes.com/ | ************* | | Shopping |
| games.espn.go.com | Jennifer23827 | ************* | http://games.espn.go.com/ | ************* | | Entertainment |
| coolcat.org (3) | Jennifer | ************* | https://coolcat.org/patroninfo... | ************* | | |
| 192.168.1.1 (2) | mokleins@att.net | ************* | http://192.168.1.1/ | ************* | | |

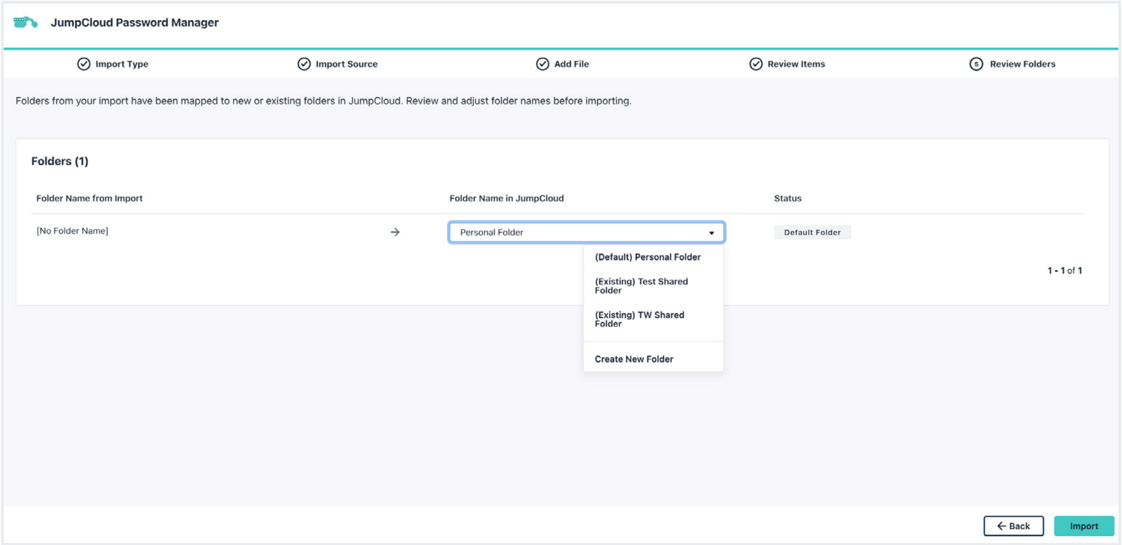


Edit Column Headers

Some columns in your import file don't have an exact match in JumpCloud Password Manager. Map your columns to a supported JumpCloud column.

| | | |
|---|---|---|
| name | → | Nickname ▾ |
| username | → | Username ▾ |
| password | → | Password ▾ |
| url | → | Website ▾ |
| totp | → | 2FA ▾ |
| extra | → | Additional Info ▾ |
| grouping | → | Folder ▾ |
| fav | → | Select ▾ |

- Review and update, if needed, your Folder name(s).



JumpCloud Password Manager

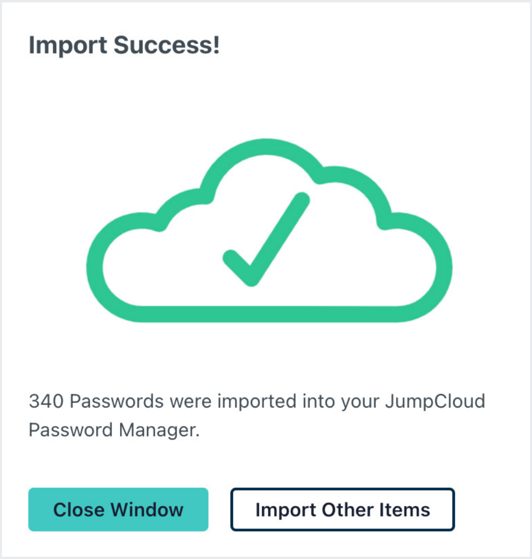
Folders from your import have been mapped to new or existing folders in JumpCloud. Review and adjust folder names before importing.

Folders (1)

| Folder Name from Import | | Folder Name in JumpCloud | Status |
|---|---|---|---|
| [No Folder Name] | → | Personal Folder | Default Folder |

(Default) Personal Folder
(Existing) Test Shared Folder
(Existing) TW Shared Folder
Create New Folder
1 - 1 of 1
← Back
Import

- Click **Import** to bring all of this data into the JumpCloud Password Manager. You should now be able to see all of the imported items in your JumpCloud Password Manager vault.

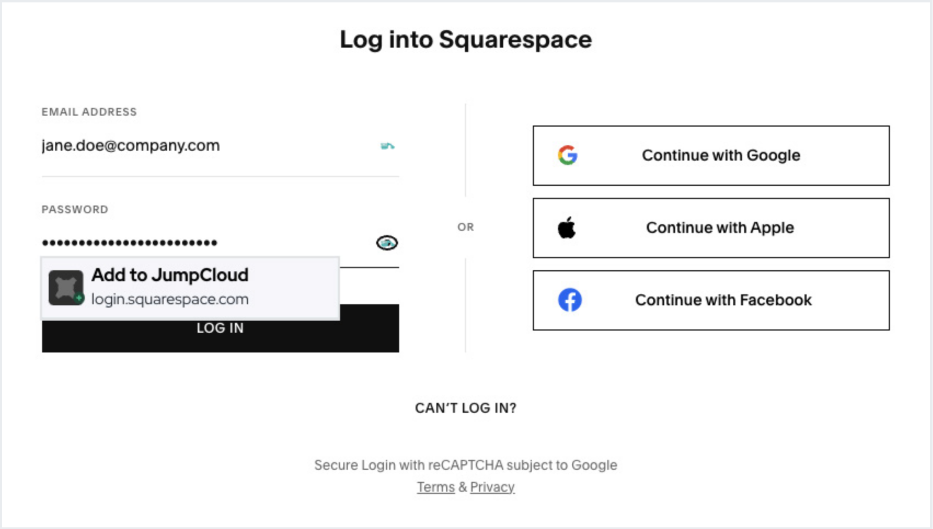


Import Success!

340 Passwords were imported into your JumpCloud Password Manager.

## Adding Passwords Manually

It is also simple to add passwords as you are logging into a site. JumpCloud Password Manager will prompt you to save passwords as you are logging in.

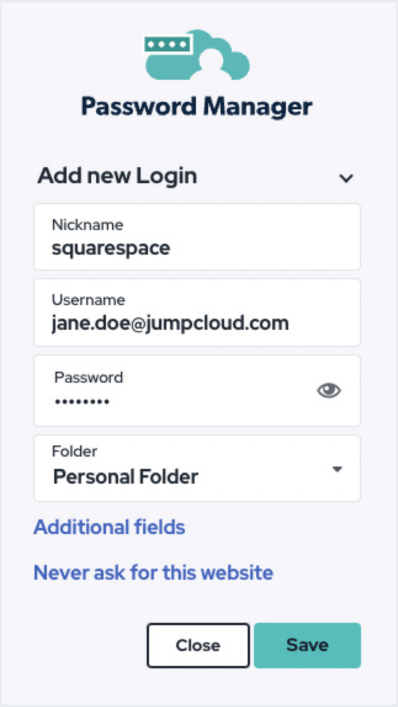


Log into Squarespace

EMAIL ADDRESS
jane.doe@company.com

PASSWORD
••••••••••••••••••••••••

- Select the Add to JumpCloud button to save the Username and Password, adding other details like a Nickname for the site and a Folder if desired.



Password Manager

Add new Login

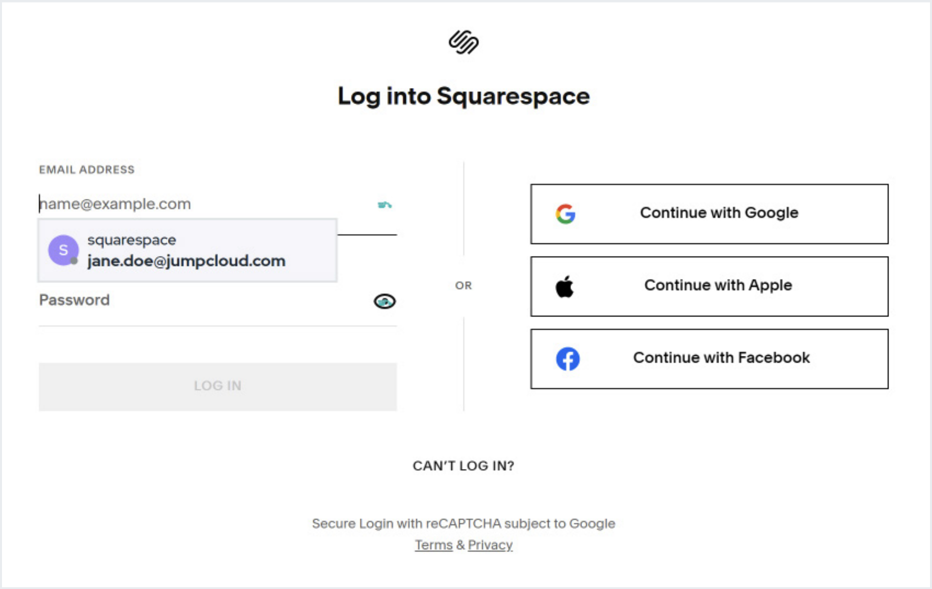
Nickname
squarespace

Username
jane.doe@jumpcloud.com

Password
••••••••

Folder
Personal Folder

- Click **Save** and continue working.
- The next time you log into this site JumpCloud Password Manager will prompt to auto-fill the Username and Password fields.



Log into Squarespace

EMAIL ADDRESS

name@example.com

squarespace
jane.doe@jumpcloud.com

Password

Secure Login with reCAPTCHA subject to Google Terms & Privacy

**Important:** If 2FA is set up for a site, JumpCloud Password Manager will offer to auto-fill that token for you as well.

# JumpCloud Password Manager Desktop App

### Supported MacOS Versions

- Big Sur 11.x
- Monterey 12.x
- Ventura 13.x

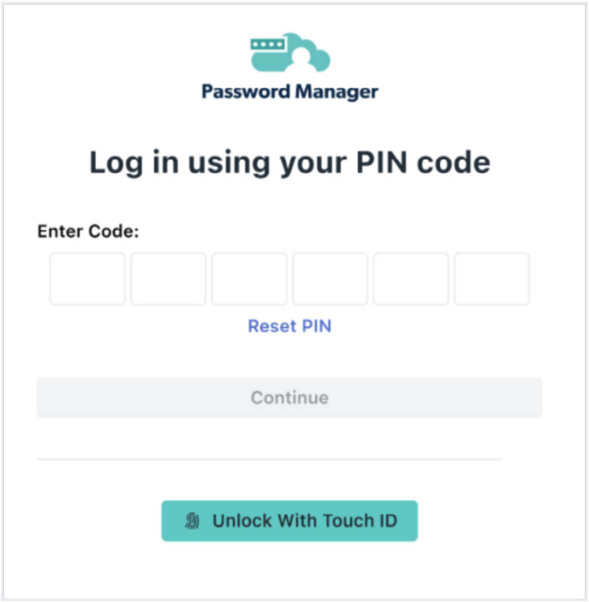
### Supported Windows Versions

- 10 (64-bit)
- 11 (64-bit)

### Supported Linux Versions

See Linux Specific Information section, below.

**Logging in:** When you open the desktop app, you will be prompted for your PIN, or the option to unlock with Touch ID.

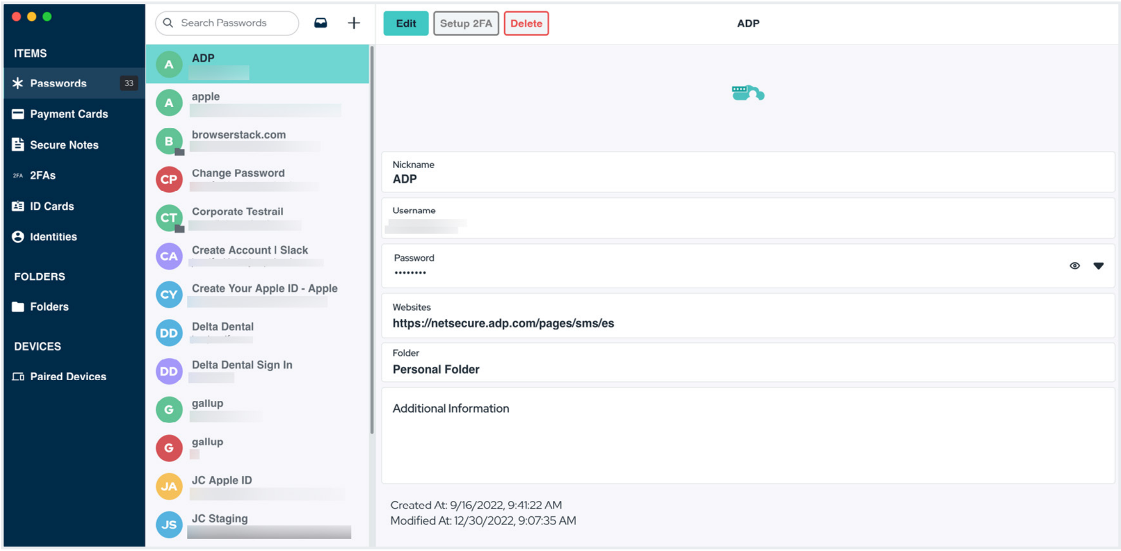


Password Manager

Log in using your PIN code

Enter Code:

- **Items**: From the left navigation menu, you can view saved/assigned passwords, payment cards, secure notes, 2FAs, ID cards, and identities.



Nickname
ADP

Username

Password
••••••••

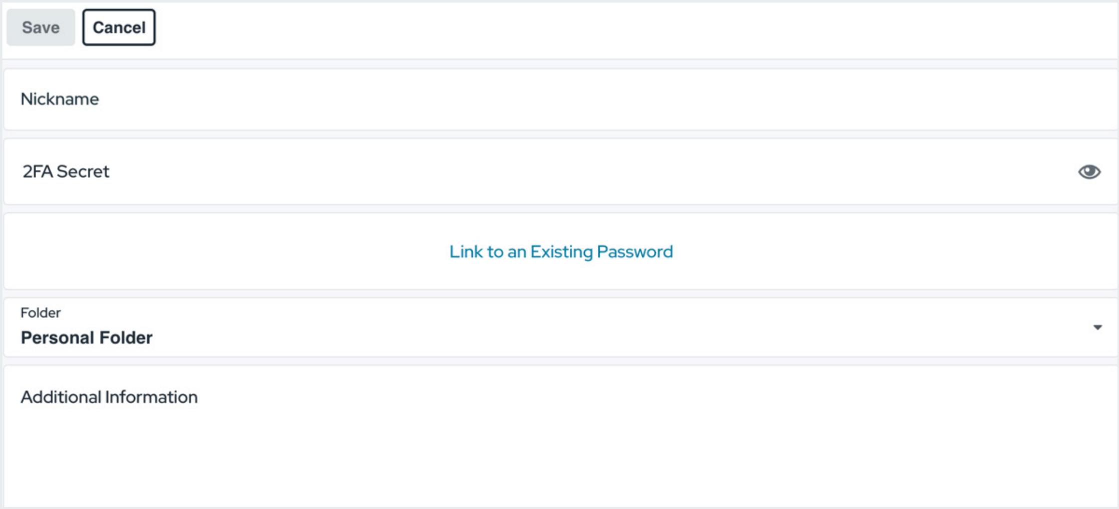
Websites
https://netsecure.adp.com/pages/sms/es

Folder
Personal Folder

Additional Information

Created At: 9/16/2022, 9:41:22 AM
Modified At: 12/30/2022, 9:07:35 AM

- For Passwords, you can select Setup 2FA, which will prompt you to add the 2FA secret (a unique code from the app or website being accessed).
- 2FA credentials can be linked to existing passwords.



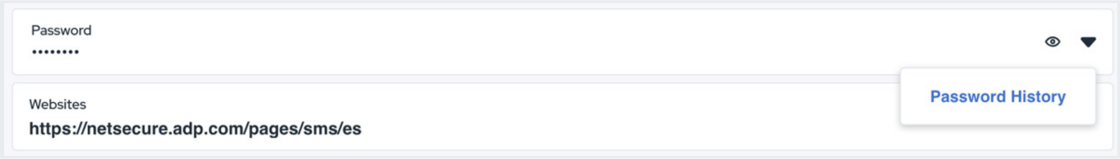
Nickname

2FA Secret

Folder
Personal Folder

Additional Information

- **Password History:** the arrow icon in the Password field opens Password History, a modal that shows past passwords, sorted by date, and the option to restore any previous password. You can also multi-select (Ctrl-click on Windows; Cmd-click on Mac) items to add to a shared folder from this list.



Password

••••••••

Websites

https://netsecure.adp.com/pages/sms/es

- **Folders**: You can add folders and share access with others. You can also assign user groups to a shared folder, if that user group has been assigned to Password Manager by an admin in the Admin Portal.

- **Devices**: Any paired devices will display here.

- **Top Navigation Bar**: From the top bar, you can search whichever area of Password Manager is currently selected, view notifications, or add any of the items with the + button.
  - One of the options from the + button is to Import Items. See Password Manager Import Tool.
  - With an item selected, and if there is content in that item, the Edit, Setup 2FA, and Delete buttons will be visible.

- **Security Dashboard**: This area displays your security score, which is calculated by your number of weak, reused, and old passwords. The passwords can be searched or you can view by selecting the Weak, Reused, and Old tabs.

- **Settings > General**:
  - **Startup and Window Behavior:** on by default; launches the app minimized when you log into the computer
  - **Debug Logs:** off by default; turning on enables verbose logging
  - **Backup Interval:** defaults to 7 days
  - **Backup Path:** click on the path to change
  - **Export Data:** location to export data as a CSV file
  - **JC Mini:** click to launch the mini onboarding screen
  - **Account Details:** click in field to see account details
  - **Synchronize:** click in field to synchronize data between all devices
  - **Install Browser Extensions:** click in the field to be redirected to a website for downloading available browser extensions
  - **Delete JC Account:** this action is irreversible

## Linux Specific Information

Linux builds do not work on ARM architecture, and do not allow for biometric authentication at this time.

- The Appimage build is not as stable as Debian and will not auto-update, but does work on all Linux distributions.
  - To install, run the `chmod a+x` command [path-to-downloaded-appimage-build] in the terminal, close the terminal, and then double-click the build you downloaded.
  - To update, download the new version build here, run the same command as above, close the terminal. Once you have double-clicked on the build you downloaded, delete the old version build.

- The Debian build is more stable than appimage and will auto-update when new versions of Password Manager are released. It works on Debian distributions (Ubuntu) but not Fedora.
  - To install on Ubuntu, right-click the downloaded build, open with Ubuntu, and click on the install button.
  - To install on all Debian distributions, open the terminal and run the `apt install -y command` [path-to-debian-build.deb].
  - Updates will download automatically, and a notification will prompt the user to restart.

- To migrate from Appimage to Debian:
  - Delete the .appimage file only (NOT the Password Manager account or any Password Manager files).
  - Then download the Debian build from the Password Manager download page and install.

## Restore JumpCloud Password Manager from Cloud Backup

Cloud Backups gives admins a secure fallback method to minimize the chance of data loss, especially in the case of a lost device. The cloud backup is encrypted and requires a private decryption key, stored by the admin, to restore the backup.

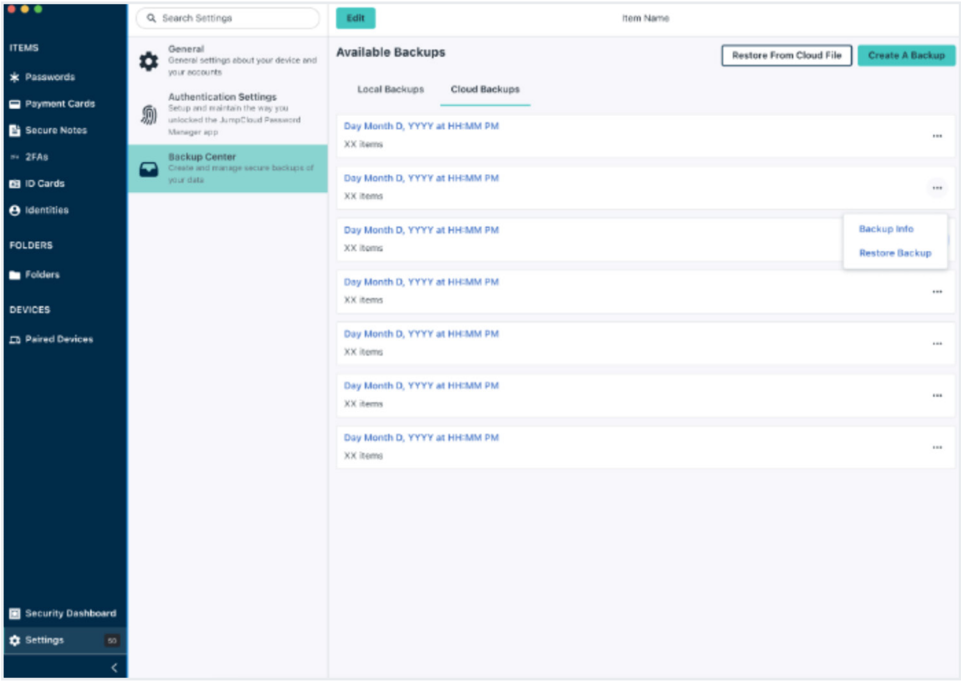
**Key Features:**

- The backup never leaves the device in plaintext.
- The decryption key is never sent in plaintext.
- There is never a scenario in which the cloud has access to both the encrypted backup file and also the decryption key.
- Admins do not have access to the data in the backup file.

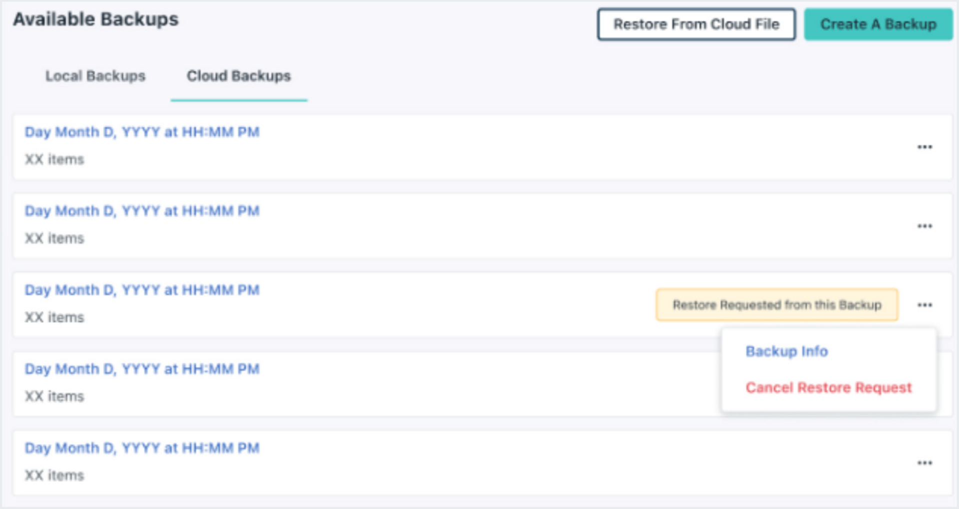
If enabled by admin, your JumpCloud Password Manager data will have a cloud backup in addition to the automatic backup stored on your device. Cloud Backups minimize the chance of data loss, especially in the case of a lost device. The cloud backup is encrypted and requires a private decryption key, stored by the admin, to restore the backup.

### In the Desktop App

- On the desktop app, go to **Settings > Backup Center > Cloud Backups** tab.
- You can select to restore from a specific backup, or use the Restore from Cloud File button and then select the specific backup to use.

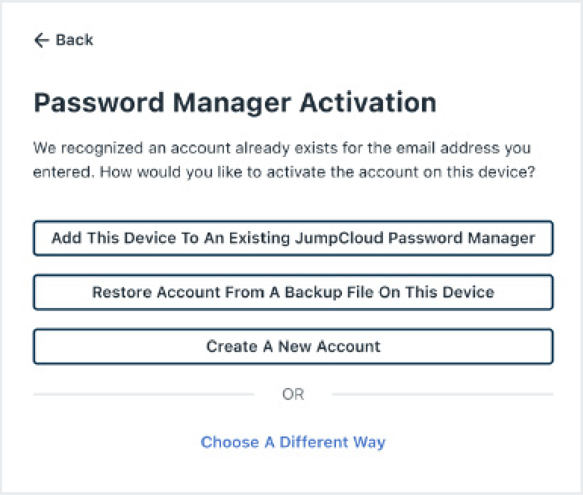


- Once a restore has been requested, a badge will indicate the request and you will have the option to cancel the request. Only one restore can be requested at a time, so if you accidentally requested the wrong backup file, you will need to cancel and initiate a new request.



### During Reactivation

When you are reactivating your Password Manager account on a device, a new option flow will be available.

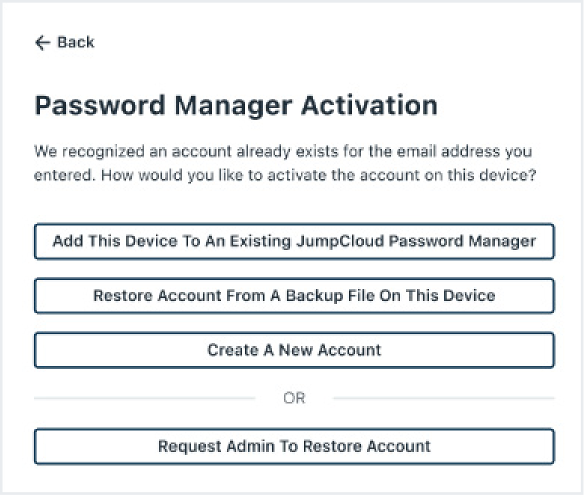


← Back

Password Manager Activation

We recognized an account already exists for the email address you entered. How would you like to activate the account on this device?

Add This Device To An Existing JumpCloud Password Manager
Restore Account From A Backup File On This Device
Create A New Account
OR
Choose A Different Way



← Back

Password Manager Activation

We recognized an account already exists for the email address you entered. How would you like to activate the account on this device?

Add This Device To An Existing JumpCloud Password Manager
Restore Account From A Backup File On This Device
Create A New Account
OR
Request Admin To Restore Account

- Continuing with the restore workflow will send a notification to your admin; you will also get a verification email and be prompted to create a new PIN.
- Navigating to **Settings > Backup Center > Cloud Backups** will show the request badge just as if you had initiated the request from the desktop app.

When an admin approves the restore request, the items will get restored on your desktop app.

# JumpCloud Password Manager Mobile App

With Password Manager, your team can manage and share passwords, 2FA secrets, secure notes, and other types of sensitive information in a secure and frictionless manner. An important part of the end user's experience is the mobile application.

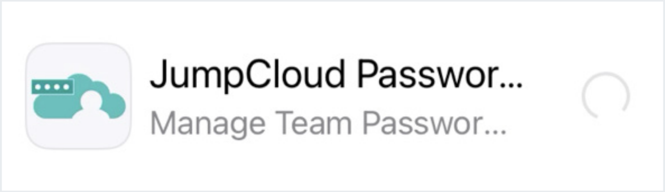
### Important Considerations

The email address you use to sign into the mobile application should be your email address for your organization.

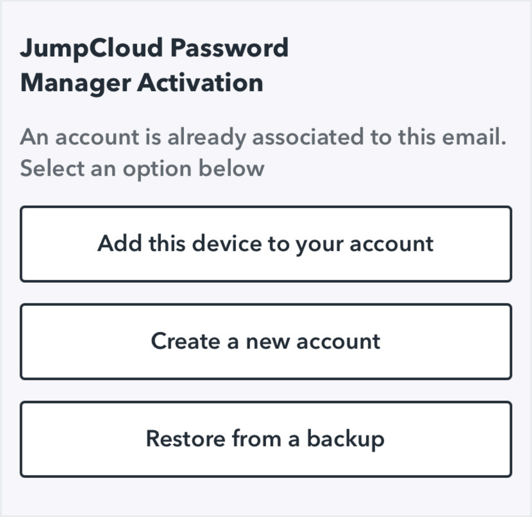
## Installing and Pairing the Mobile Application

JumpCloud Password Manager is available from the iOS App Store or the Google Play Store.

- Download and open the application.

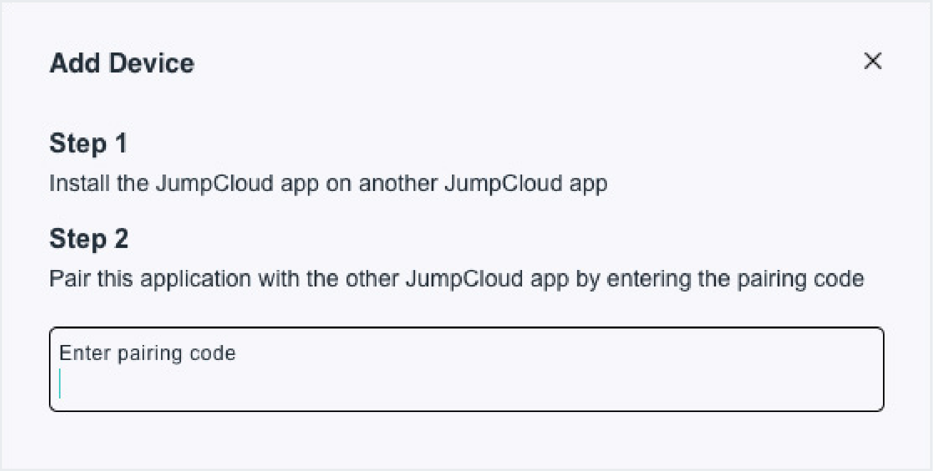

JumpCloud Passwor...
Manage Team Passwor...

- You will be prompted to sign in with your email.
- Once your email address is verified, you will see the JumpCloud Password Manager Activation screen. **Important**: If you receive an error at this step, and JumpCloud Password Manager cannot verify your email, please review the options in the Password Manager Activation Help help center article.


**JumpCloud Password Manager Activation**

An account is already associated to this email. Select an option below

- Select **Add this device to your account**
- On the desktop Password Manager app, go to **Devices > Paired Devices**, and click on (+) Add an app.



Add Device

Step 1

Install the JumpCloud app on another JumpCloud app

Step 2

Pair this application with the other JumpCloud app by entering the pairing code

- On the desktop app, add the pairing code from the mobile app. You will only receive a pairing code on a freshly installed app.
- All items from the desktop app will be synced to the mobile app, and the device will appear in the list of **Paired Devices** on the desktop app.
- After your device has been paired you will be prompted to create and confirm a PIN for accessing Password Manager. This PIN can be the same one created for the Password Manager desktop version.

**Important:** you will not be able to access the Password Manager application if your PIN is forgotten. Your admin does not have access to your PIN.

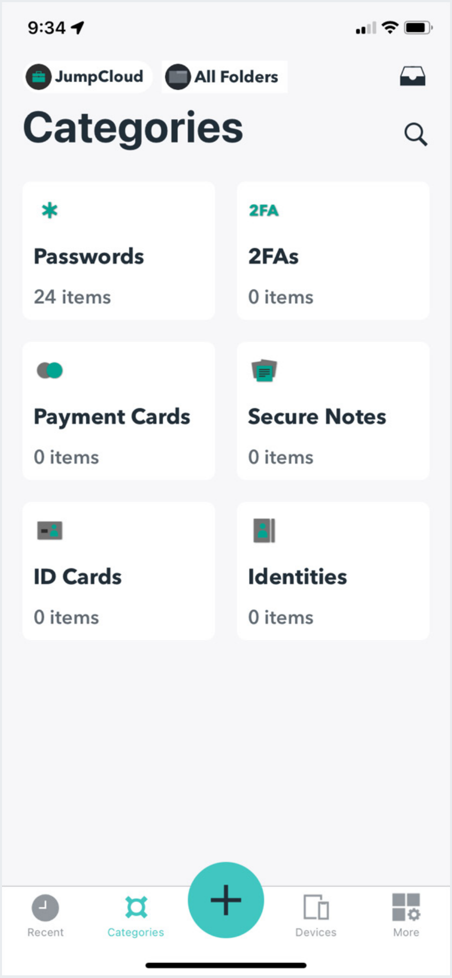
## Using the Mobile App

The Password Manager mobile app home screen, or **Categories** page, is a collection of your items.

- Selecting the **Recent** icon will display a list of recent activities.
- The **(+)** button is how you will add items to the app such as a password or payment card.
- Selecting **Devices** will show which other devices exist on this Password Manager account.
- The **More** button covers everything else:
  - Security Dashboard: you can check on the security score of your accounts, and review which passwords are weak, reused, old, or at risk.
  - Authentication Settings: options for changing the PIN, enabling Face ID, detecting Face ID change, and setting the lock schedule.
  - Backup Items: gives the steps for creating a backup file on the desktop app.
  - Restore Items: gives the steps for restoring items on the desktop browser extension.
  - Password Generator: can create passwords with editable settings.
  - Safari Autofill Extension: gives the steps for enabling AutoFill on the device.

- Apple Watch: user can select items to see on the Password Manager watch app.
- Pair Computer Browser: provides steps for enabling a browser extension on a desktop browser.
- Settings: general settings and details about the app, along with the ability to enable Quick Autofill and Delete Account.

  **Note**: on iOS, in order to set Password Manager as the default for AutoFill, go to **Settings > Passwords > Password Options**, and select JumpCloud PWM from the list.



9:34

JumpCloud | All Folders

Categories

| | |
|---|---|
| Passwords<br>24 items | 2FAs<br>0 items |
| Payment Cards<br>0 items | Secure Notes<br>0 items |
| ID Cards<br>0 items | Identities<br>0 items |

**Note:** Screens and steps may appear slightly different on an Android device.