-->

Managing Passwords (and more) at Penn

Last Modified on 05/15/2025 10:28 am EDT

If you have a LastPass account from the University, please see our directions on migrating your account to Dashlane.

The University provides a premium password management service, Dashlane. Use this article to help you choose and configure the account type that is right for you, and for any Wharton-specific tips. The University also has information on setting up Dashlane.

Dashlane Business Plan

Dashlane business plan accounts are available for *University faculty, staff, and employees.* They allow you to share credentials with other colleagues securely.

You **must** use the Dashlane business plan if:

- you use credentials for University resources or work purposes.
- you need to share collections (a shared Dashlane password folder) of credentials with other employees.

Accounts in the Wharton School's Dashlane business plan is open to *Wharton faculty, staff and employees* only.

To create a Dashlane account tied to Wharton's business plan, you'll need to receive an invitation emailed to your Wharton email account. To request an invitation to use Dashlane Enterprise, please contact your Wharton Computing representative.

LastPass Enterprise users should automatically receive a Dashlane invitation to their Wharton email account with the subject: "You have been added to UPenn - Wharton on Dashlane." Follow the instructions in our University Retires LastPass Password Manager article.

If you run into issues with installing the browser plugin see Dashlane's article. We also recommend that you turn on the Account Recovery Methods to ensure you don't lose all your passwords if you forget your Master Password! See the section on enabling account recovery options, below, for details.

Dashlane Personal Account with Premium Access

Dashlane personal accounts are for *everyone in the Penn Community.*

Only personal credentials and files should be used with a Dashlane Personal plan.

To obtain a Dashlane Premium account, follow ISC's Dashlane Premium instructions.

Dashlane is available as an app for your smart phone, and as an extension for your web browser. If you run into issues with installing the browser plugin, you can use this link to install it.

Can I have 2 accounts?

You can have two separate Dashlane accounts, but they must have separate login credentials:

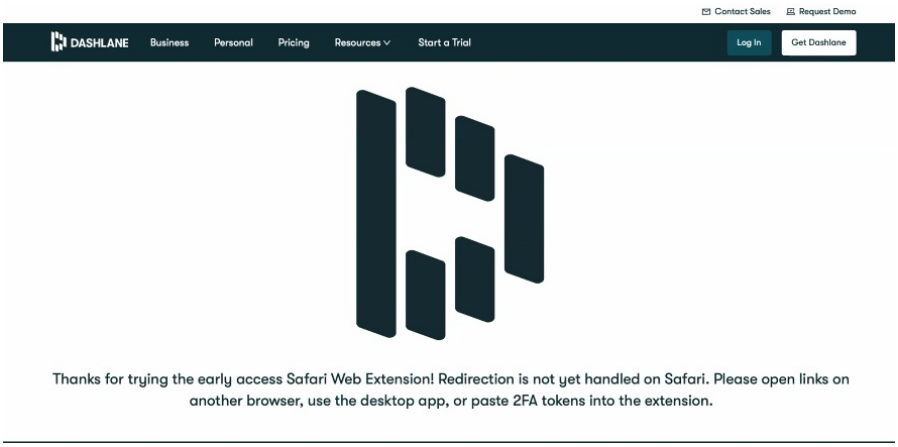
- **Dashlane Business:** Use this for Wharton and Penn work
- **Dashlane Premium:** Use this for saving personal credentials.

Additional Information and Best Practices

General

Safari Browser Does Not Work

When using Safari, accepting the invitation from email doesn't work. You will likely have to use a different browser (eg. Firefox, Chrome).



Note: the Dashlane browser plugin is **required** to interact with Dashlane. Mac OS has a Dashlane client, but it does not allow access to the full suite of sharing features available in the Mac OS client.

Account Recovery Options

We recommend enabling a password recovery option for your Dashlane account so you have another way to access your password store if you lose your master password. See Dashlane's article on Account recovery key set up .

Store Personal and Business Passwords Separately

ISC and Wharton Security recommend using distinct password manager stores (accounts) to separate your personal passwords:

- **Personal passwords:** any passwords for personal use, eg. your Netflix account, etc.

- **Work passwords**: any credentials you use to access work resources.

This is good practice so that a compromise of your personal password manager won't inadvertently expose University resources and open the University to risk. You can have two separate Dashlane accounts, but they must have separate login credentials. For example:

- **Dashlane Business:** Use this for Wharton and Penn work
- **Dashlane Premium:** Use this for saving personal credentials. (Or use a different password manager.)

If you need to store work-related credentials, ask your Wharton Computing representative for an invitation to Wharton's Dashlane plan.

Dashlane Business Users

Dashlane Business Accounts are Tied to the Wharton Dashlane plan

Using Dashlane Business accounts linked to the Wharton Dashlane Plan means you are part of the school's Dashlane account and subject to its policies. When a Dashlane Business account is separated from our Wharton Dashlane plan (for example, if you leave the university), **your account will lose all data added** when it was part of the business account.

Don't Store Personal Passwords in Dashlane Business

We recommend not storing personal passwords in Dashlane Business. If for whatever reason you simply cannot avoid it, please beware of the following:

- When you leave the University, your Dashlane business account will be removed from the Wharton Dashlane business plan. Any passwords created while part of the Dashlane business plan will be **deleted** from your Dashlane account.

- Since it is complicated to export individual passwords, and exporting any work credentials is against policy, we recommend storing all personal passwords in a separate account (either Dashlane Premium or another password manager).

Enable Account Recovery Options

We recommend that you **turn on an Account Recovery Method**: This will ensure you don't lose all your passwords if you forget your Master Password! If you forget your Master Password and haven't enabled a recovery method, you may need to reset your account, which erases all your data. Here are the options:

- Option 1: Account Recovery Key
- Option 2: Admin-Assisted Recovery
- Option 3: Biometric Recovery

Business users should enable all 3 options. They need to be set up BEFORE before you need the account recovery service, so make sure to consider this when setting up your account. If you weren't prompted to do this when you set up your account (or just didn't do it), see Dashlane's article on setting this up.

Using Dashlane Collections

A Dashlane collection is a shared Dashlane password folder. It works a little differently than in LastPass.

- In LastPass, credentials were stored inside the shared folder. Everyone with access to the shared folder could see it.
- In Dashlane, each credential first must be created in the user's Dashlane storage, and then shared to a Collection. Once each user gains access to the collection, those items then are visible in those users' Dashlane storage as well.
- When sharing collections, if you share the collection without granting anyone else full ("Manager") access, then no one else will be able to share it if your Dashlane account gets revoked from the Wharton Dashlane shared account. You should take care to always **make sure at least one other person other than yourself has Manager access to a shared collection**, otherwise you may end up with a shared collection with passwords and credentials inside it that no one can manage, edit, or delete.