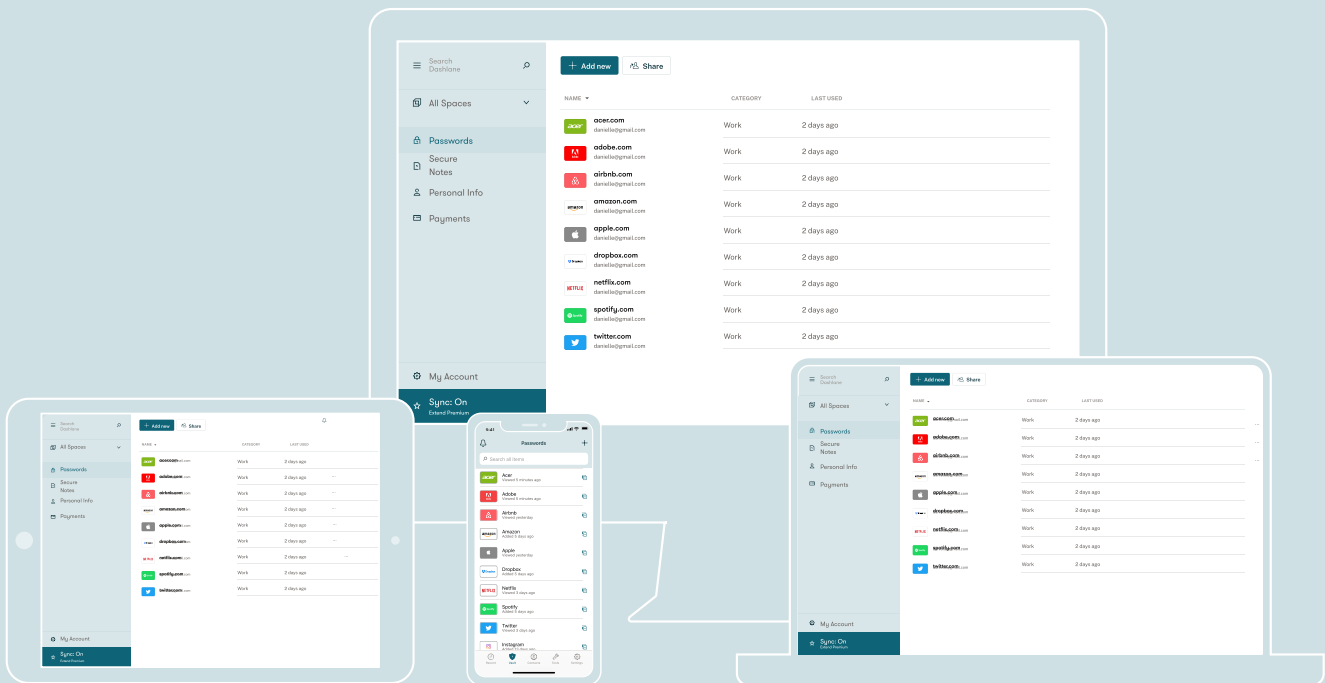


# POWER & PROTECT YOUR BUSINESS

Your guide to getting started with Dashlane



## WHAT'S INSIDE:

Introduction to Dashlane .....	2
Navigating the Admin Console .....	3
Configure your account .....	4
The Dashlane desktop app .....	6
The Dashlane mobile app .....	7
Dashlane desktop browser extension .....	8
Identity Dashboard & Password Health Score .....	9

## Introduction to Dashlane

Dashlane is the most secure password and access management app, making logins and authentication for your employees safe and simple. In the digital era, it's imperative to protect your business from the dangers of storing data online, as a single weak password puts your entire company and customer information at risk. With our universal app, passwords and data sync securely to all authenticated devices, including Mac, Windows, Linux, Chromebook, iOS, Android, and on the web.

Dashlane is the only password manager designed for easy use by both technical and not-so-technical people. Onboarding is painless, secure sharing of company logins is simple, and autofill and auto-login keep team members working faster and more efficiently.

When you create your account, you'll be asked to set a Master Password — the encryption key used to unlock the account. Dashlane never stores or transmits your Master Password, which means only you can access your vault, even in the unlikely event of a server breach. Our patented security architecture coupled with built-in, two-factor authentication means you can rest easy knowing your data is safe.

## Core features

---



### PASSWORD MANAGER

Dashlane's patented security architecture ensures your passwords and other data are secure and accessible to only you. If you've been using your browser's native password manager, you should import those passwords into Dashlane under the desktop app's **File** menu, or just save as you browse with the Dashlane extension. Credentials stored in your account must contain an email address or login, the password, and a website URL. If you want to organize your credentials, use the default categories or create your own. Passwords are encrypted locally and synced between an unlimited number of authenticated devices, so you can access your passwords anywhere.



### SECURE NOTES

Secure Notes are an easy way to store or share sensitive information. Start a blank note or use a template in the desktop app, and share privately or encrypt with a password for personal use. Secure Notes automatically sync across all your devices for handy access.



### SMART SPACES

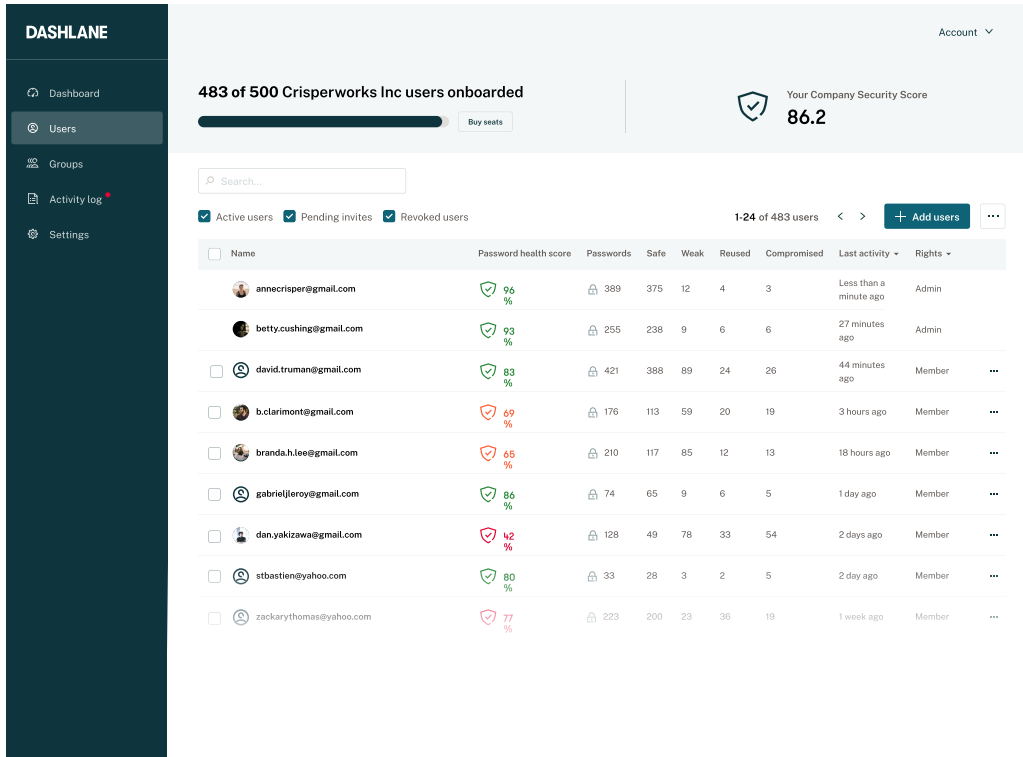
Smart Spaces allow users to securely store business and personal data in separate spaces within the same account. This means ultimate visibility and security for your business and convenience for your employees. Admins can set rules that automatically store users' work passwords in their Business Space, which allows admins to easily revoke credentials if necessary and keep company data where it belongs. Admins also have visibility into each user's security score across their Business and Personal Spaces — all without needing access to their credentials.



### SHARING CENTER

The Sharing Center allows you to view and manage all shared credentials in a single place. New sharing invitations will appear here along with any groups or existing individual shares. Admins have the ability to disable sharing in the Admin Console settings.

## Navigating the Admin Console












**DASHLANE** Account ▾

**483 of 500 Crisperworks Inc users onboarded** Buy seats

Your Company Security Score **86.2**

Search...

Active users  Pending invites  Revoked users 1-24 of 483 users < > + Add users ⋮

<input type="checkbox"/>	Name	Password health score	Passwords	Safe	Weak	Reused	Compromised	Last activity	Rights
<input checked="" type="checkbox"/>	 annecrisper@gmail.com	96 %	389	375	12	4	3	Less than a minute ago	Admin
<input checked="" type="checkbox"/>	 betty.cushing@gmail.com	93 %	255	238	9	6	6	27 minutes ago	Admin
<input type="checkbox"/>	 david.truman@gmail.com	83 %	421	388	89	24	26	44 minutes ago	Member ⋮
<input type="checkbox"/>	 b.clarimont@gmail.com	69 %	176	113	59	20	19	3 hours ago	Member ⋮
<input type="checkbox"/>	 branda.h.lee@gmail.com	65 %	210	117	85	12	13	18 hours ago	Member ⋮
<input type="checkbox"/>	 gabrieljeroy@gmail.com	86 %	74	65	9	6	5	1 day ago	Member ⋮
<input type="checkbox"/>	 dan.yakizawa@gmail.com	42 %	128	49	78	33	54	2 days ago	Member ⋮
<input type="checkbox"/>	 stbastien@yahoo.com	80 %	33	28	3	2	5	2 day ago	Member ⋮
<input type="checkbox"/>	 zackarythomas@yahoo.com	77 %	223	200	23	36	19	1 week ago	Member ⋮

Your Dashlane Team trial or paid plan provides admins with an Admin Console, where they can configure policies and settings and manage and monitor users. Admins can add/remove users, monitor Password Health Scores, and enable custom features and policies. Accessing the Admin Console requires device authentication, the admin's Master Password (used locally), and admin status.

Admins can change other users on the plan to admin status from the Admin Console. Before adding members to your plan, you should become familiar with the available policies in the Admin Console. Navigate to the **Settings** tab to view available options, which are detailed in the next section.

**Access the Admin Console at**  
[console.dashlane.com](https://console.dashlane.com)

**To start a trial, go to**  
[dashlane.com/business](https://dashlane.com/business)

## Configure your account

### ADD COMPANY DOMAINS

Add your company's email domain(s) to the Admin Console to enable Dashlane to force users' company credentials matching the domain(s) into the Business Space. When credentials are saved in a user's Business Space, admins can view details about those passwords, including the Password Health Score and breakdown of safe, reused, weak, and compromised passwords — but never the actual passwords. By default, users are able to move company passwords back to the Personal Space. This can be changed by enabling the **Move company items to Business Space** feature detailed below.

### FORCE COMPANY ITEMS TO BUSINESS SPACE

Enable this feature to force items matching your company email domains to remain in a user's Business Space. When toggled on, the option to change a work credential's space will be grayed out and inaccessible.

### REMOVE COMPANY ITEMS FOR REVOKED USERS

When an employee leaves your organization, they shouldn't leave with work passwords. When this setting is enabled and a user is revoked, Dashlane immediately hides the user's Business Space and all contents forced into it. If a user is added back to your plan, the Business Space and all contents are immediately restored. Thirty (30) days after being revoked, the user's Business Space and its contents are permanently deleted.

### AUTOMATICALLY LOG OUT IF INACTIVE FOR A DESIGNATED PERIOD OF TIME

Enable this setting to log out users when they're inactive for a designated period of time.

### SECURE SHARING FOR PASSWORDS AND NOTES

When this setting is toggled on, users have the ability to share passwords and Secure Notes with other Dashlane users. Disabling sharing will prevent any new shares from being sent; however, previously shared items will remain.

### AUTO-LOCK ON EXIT

When enabled, Dashlane will automatically lock after exiting the iOS or Android app, requiring the user to log in again.

### MANAGING USERS

To add users, go to the **Users** tab in the Admin Console and click the **Add users** button. Add users' email addresses one by one or by importing a CSV or TXT file. Then, click **Send invites** to email users their invitations.

Users will receive an email inviting them to your Dashlane Team plan. When they accept, they'll go through the account creation process which will have them create a Master Password and download the Dashlane app. Employees will appear as pending in the Admin Console until the invitation is accepted. To resend an invite, to change a user to an admin, or to revoke a user, click the ellipses by their name and make your selection.

### SAML PROVISIONING

Dashlane Team supports the SAML 2.0 protocol to help admins add team members to their account. Compatible with most SSO identity providers (IdP) such as Okta, ADFS 3.0, Microsoft Azure Active Directory, Centrify, and more, Dashlane ensures admins have an easy, secure way to provision colleagues to their Dashlane Team account.

*If you're interested in Dashlane's SAML-based single sign-on feature, you can upgrade to a Dashlane Business plan.*

## Configure your account

### MANAGE SHARING GROUPS

The Group Sharing feature allows Dashlane users to easily and efficiently share passwords and Secure Notes, making onboarding easy and secure. Admins can create groups based on departments or company needs in the Admin Console. Once created, both admins and individual users can share information with these groups via the app.

To get started, navigate to the **Groups** tab in the Admin Console and create a group. Once a group is created, admins can manage members by clicking into the group and selecting **Add members**. Admins can also remove users from this view.

A newly added group member will receive a sharing invitation in their Dashlane app. Once the invitation is accepted, any passwords that are already part of the group will be immediately provisioned to the user. If a user needs to share a password with members of the group, they can navigate to the password credential in Dashlane, click the share icon, and enter the group into the recipients field. Users already in the group will receive the new shared password immediately without having to accept another invitation.

When admins revoke a user from their Dashlane Team plan, any passwords that user had shared with a group will remain, as long as there is at least one user with full rights to the password. **The revoked user will lose access to the groups and passwords shared.**

### ACTIVE DIRECTORY

Dashlane's Active Directory (AD) integration automatically provisions (and optionally deprovisions) users and groups to your Dashlane Team plan. When enabled, your Dashlane Team plan's members will mirror the users in the Active Directory Group(s) you select to sync.

For full details, please visit our setup guide at <https://support.dashlane.com/hc/en-us/articles/115002155485-Active-Directory-Integration>.

### DISABLE AUTO-LOGIN AND AUTOFILL ON WEBSITES

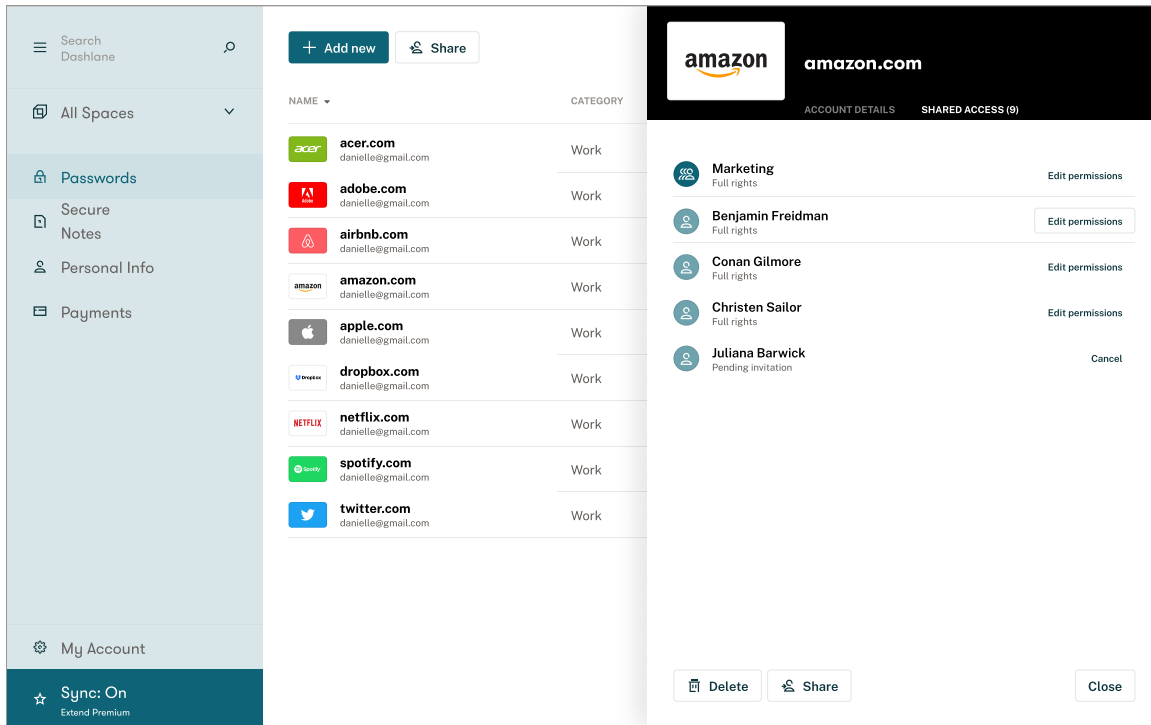
There are times when Dashlane's browser extension attempts to fill in a user's personal information when it isn't appropriate. Users can disable Dashlane from filling logins and forms for sites by navigating to the site, opening the Dashlane browser extension and navigating to the **This website** tab. Admins can disable auto-login and autofill on websites company-wide by entering them in this field.

### MSI PACKAGE

Dashlane's MSI package allows admins of Windows-based environments to deploy the Dashlane app to multiple users' computers from a single point. Our step-by-step deployment documentation teaches admins how to deploy the Dashlane Windows client via GPO or SCCM.

For full details, please visit our setup guide at [dashlane.com/business/features/deployment](https://dashlane.com/business/features/deployment).

## The Dashlane desktop app



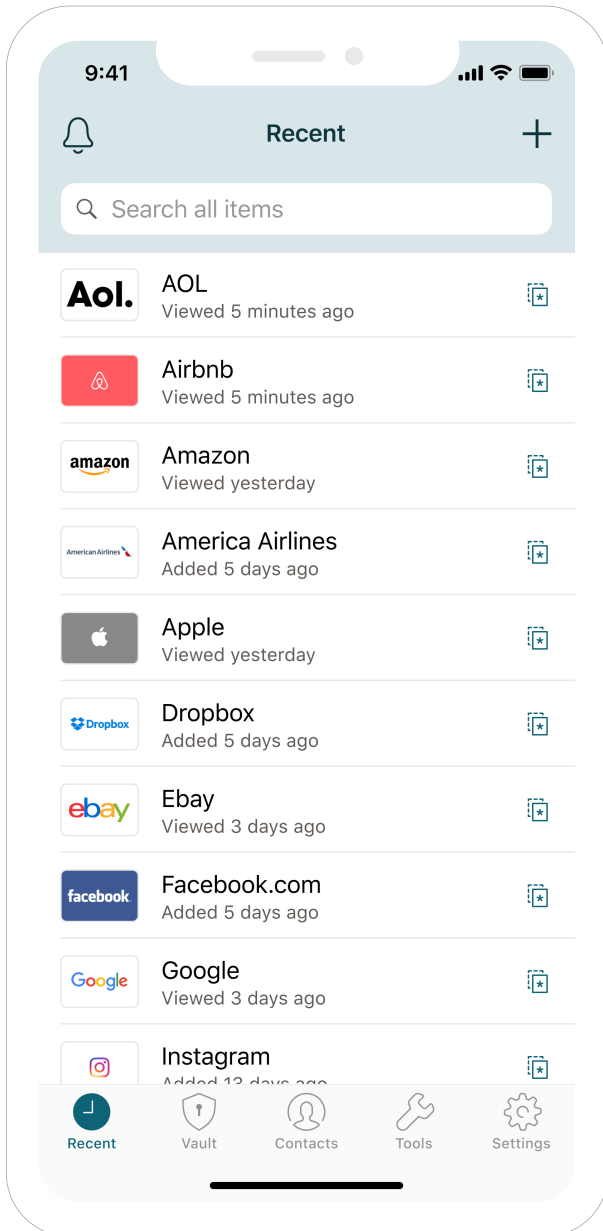
The Dashlane app syncs passwords and other data securely across all your authenticated devices, including Mac, Windows, Linux, Chromebook, iOS, Android, and on the web. Depending on your corporate environment and employee personal device policies, you should familiarize yourself with the platforms your colleagues will use.

Download our Mac and Windows applications at [dashlane.com](https://dashlane.com) or download our mobile apps from their respective app stores. To use Dashlane on Chromebook or Linux systems, install Dashlane’s browser extension via the browser store.

### DESKTOP APP

Access your secure data from the left-side navigation panel of the desktop app. Here, you’ll find your Passwords, Identity Dashboard, Secure Notes, Digital Wallet, Sharing Center, and Emergency Contacts. For the most robust Dashlane experience on desktop, make sure the browser extension is installed (explained in detail on page 8).

## The Dashlane mobile app



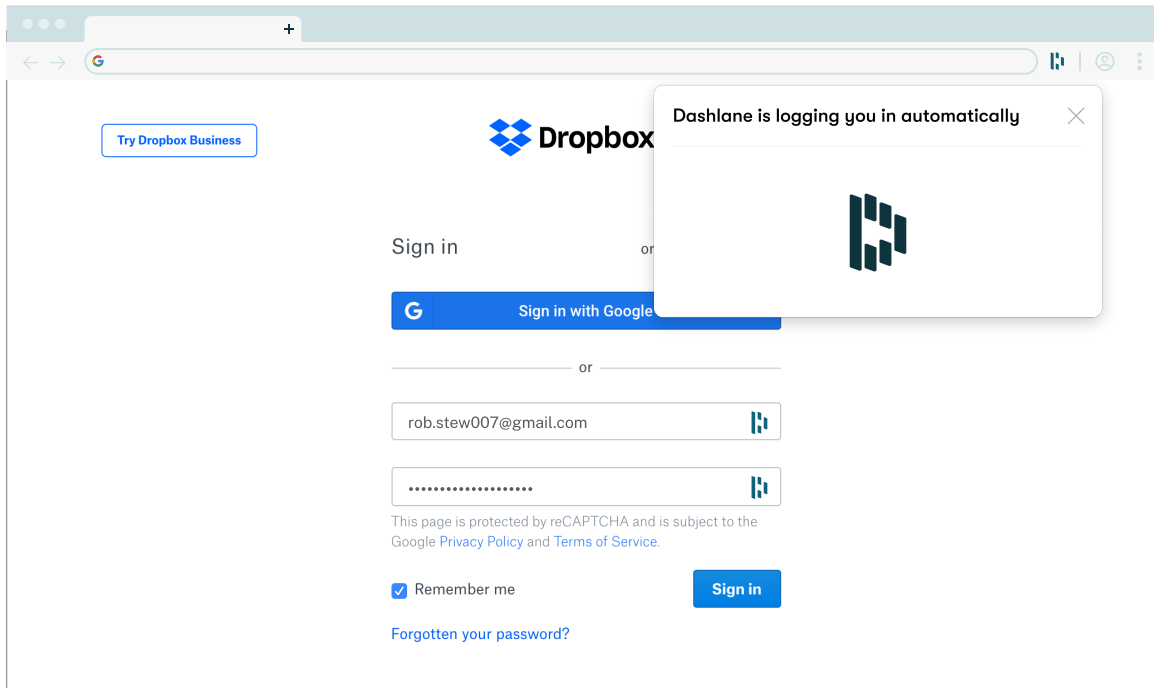
### MOBILE APP

Dashlane is available on iOS and Android and syncs seamlessly across all your authenticated devices, letting you access business and personal passwords anywhere. Passwords are stored locally on your devices, so you can access passwords even when you don't have an internet connection. Quickly find your most recently viewed items, or navigate to the **Vault** tab to see everything stored in Dashlane. Accept and view shared passwords in the **Contacts** tab.

iOS users can quickly unlock their Dashlane account with a PIN or biometrics and can autofill their passwords on most apps on their phone by going to **Settings > Passwords and Accounts > AutoFill Passwords**. Enable **AutoFill Passwords** and select Dashlane as your password manager of choice. For optimal performance, we highly recommend unselecting iCloud Keychain. For faster access to your credentials, set up biometrics or a four-digit code.

Android users can also quickly unlock their Dashlane account with biometrics. And with expanded app login capabilities, users can expect to see the Dashlane icon on all app login screens or in the Chrome browser. Activate these enhanced auto-login features in the settings of the Dashlane Android app.

## Dashlane desktop browser extension



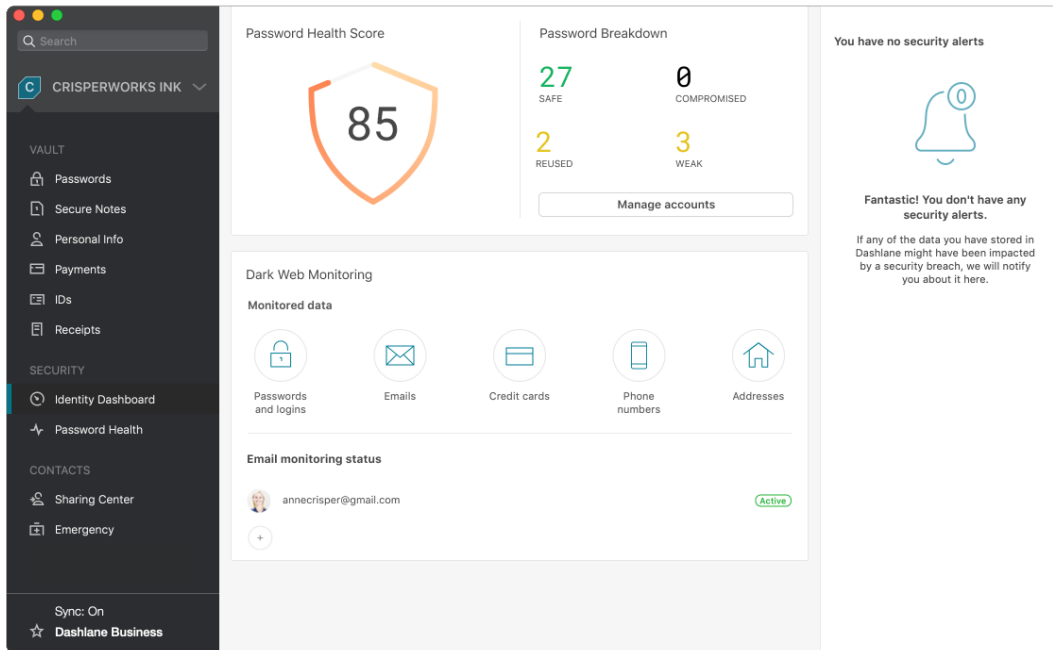
### DESKTOP BROWSER EXTENSION

Dashlane's desktop browser extension is critical to a fast and seamless experience. Available on Chrome, Firefox, Safari, and Edge, the extension enables Dashlane to automatically fill in login credentials and personal information. At page load, our semantic engine analyzes the page to identify form fields with the Dashlane D icon. Click into any field with the Dashlane D icon to autofill information. When creating a new account or updating a password, the extension's Password Generator can even create a complex password and automatically save it to your account.

Look for how to install and manage your browser extension within the Dashlane desktop app main menu.



## Identity Dashboard & Password Health Score



Dashlane's security features benefit both admins and end users. Most people who aren't using a password manager use the same or similar passwords for nearly all of their logins, which puts individuals and companies at risk. When users begin adding passwords to Dashlane, they have a view into their password hygiene for the first time through the Identity Dashboard in the desktop app.

Users on a Dashlane Team plan have access to both a Business and Personal Space, which each have their own security score. Admins can only see details on a user's Business Space, which include the overall score, and a breakdown of safe, weak, reused, and compromised passwords. However, if someone is reusing a password in both spaces, it will be included in the company's space breakdown. Admins also have the ability to view the total number of business passwords and last activity times of users from the Admin Console.

A company's overall security score is an aggregate of end users' scores on a Dashlane Team plan. In a perfect world, all users would have a 100% score. We suggest aiming for a 90% overall score with the understanding that scores will fluctuate as users are added and removed from your plan and as users add passwords into Dashlane.

## STILL HAVE QUESTIONS ABOUT DASHLANE?

Reach out to your system administrator, go to [support.dashlane.com](https://support.dashlane.com) to search the Help Center, or contact our support team at [support@dashlane.com](mailto:support@dashlane.com).