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 ................................................................. 5
The Dashlane desktop app .............................................................. 8
The Dashlane mobile app .............................................................. 9
Dashlane browser extension ......................................................... 10
Password Health Score .............................................................. 11
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. Please note, if you’ve enabled single sign-on, employees access Dashlane with their organizational credentials instead of using a Master Password.

Core Features

PASSWORD MANAGER
Dashlane's patented security architecture ensures your passwords and other data are secure and accessible to only you. You can easily save passwords as you browse the internet 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.

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.

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

GROUP SHARING
Employees have the ability to share credentials and Secure Notes among set groups, such as specific departments or teams. Admins have the ability to disable sharing in the Admin Console settings.
Navigating the Admin Console

Your Dashlane Business 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 user’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 below.

Access the Admin Console at console.dashlane.com

To start a trial, go to dashlane.com/business
Reporting dashboard

In the Admin Console, you’ll also be able to access your reporting dashboard. The dashboard’s centralized view gives you unprecedented visibility into your company’s password security and the ability to track improvements over time. There, you’ll receive actionable insights on your employees’ Password Health Scores and be able to help at-risk employees update their weak, reused, or compromised passwords.

This means that not only can you assess employees’ password hygiene right now, but you can also better demonstrate to company leadership the effectiveness of strategies and tactics to bring your organization’s habits in line with best practices.

We recommend aiming for a company security score of 90 or above. It might take some time to get there, but don’t fret. Start by checking in with users weekly and encourage at-risk employees to update their passwords. Before long, you’ll start to see your company’s score rise and have to check in with employees less frequently.
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.

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 BUSINESS PLAN MEMBERS
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 Business 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 Business 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 Business account.

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.
Configure your account

CONFIGURE SINGLE SIGN-ON (SSO)
Single sign-on (SSO) allows your users to sign in to their Dashlane vault using their SSO credentials instead of a Master Password. Dashlane supports all SAML based identity providers, including OKTA, ADFS, G Suite, and Azure AD.

To maintain our zero-knowledge security architecture, Dashlane leverages Dashlane’s SSO Connector to authenticate users. When a user attempts to sign in using SSO, the user is redirected to the SSO Connector, which federates to the identity provider. After the user successfully signs in, the SSO Connector sends a unique key to the client that will finally decrypt the user’s data.

For full details, please visit our setup guide at https://support.dashlane.com/hc/articles/360013149040.

MANAGE SHARING GROUPS
The Group Sharing feature allows Dashlane Business 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 Business 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.
Configure your account

**ACTIVE DIRECTORY**

Dashlane's Active Directory (AD) integration automatically provisions (and optionally de-provisions) users and groups to your Dashlane Business plan. When enabled, your Dashlane Business 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.

**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.

**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.
The Dashlane web app

WEB APP
Access your secure data from the left-side navigation panel of the web app. Here, you’ll find your Passwords, Secure Notes, and Digital Wallet. You’ll also be able to share Secure Notes and passwords to individuals or groups.

Dashlane syncs passwords and other data securely across all your authenticated devices 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.

The first time you log in to Dashlane, you’ll be asked to install the browser extension. The browser extension is required for autofill and navigating to the web app (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 browser extension

BROWSER EXTENSION

Dashlane’s 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.

To navigate to the web app from your extension, click the Dashlane D icon, choose the three dots on the right hand side, and click Open the app.
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 Password Health Score in their mobile app.

Users on a Dashlane Business 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 Business 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, or go to support.dashlane.com to search the Help Center or contact our support team at support@dashlane.com.