Dashlane User Guide

Overview

This guide provides step-by-step instructions for using Dashlane within our organization. It covers logging in, enabling recovery options, saving passwords, sharing access securely, creating groups, adding secure notes, account recovery procedures, and using VPN.

1. Logging Into Dashlane

Step 1 — Open Dashlane

Go to: https://app.dashlane.com

(You may also use the Dashlane browser extension if installed.)

Step 2 — Enter Your Email

Enter your work email address and select Next.

Step 3 — Enter Your Master Password

Type your Master Password and select Log In.

Important:

- Your Master Password protects your encrypted vault.
- Administrators cannot see your Master Password.
- Never share your Master Password with anyone.

Step 4 — Complete Verification (If Prompted)

You may be asked for:

- Two-factor authentication (2FA)
- Email verification
- Device approval

---

2. Activate Admin-Assisted Recovery (Critical Step)

This step prevents permanent lockouts and must be completed by each user after logging in.

User Setup Steps

1. Open the Dashlane web app or browser extension.
2. Go to My Account or Settings.
3. Select Security Settings.
4. Locate Account recovery.
5. Click View options
6. Enable Admin-assisted recovery.

You may be asked to:

- Confirm your Master Password
- Confirm your email address

3. Saving Passwords

Dashlane can save passwords automatically or manually.

Automatic Saving (Recommended)

1. Log into a website normally.
2. Dashlane will prompt to save the password.
3. Select Save.

Manual Entry

1. Open Dashlane.
2. Select Passwords.
3. Choose Add New.
4. Enter:
   - Website name
   - URL
   - Username
   - Password
5. Select Save.

---

4. Sharing Passwords Securely

Passwords can be shared with coworkers without exposing credentials unnecessarily.

Step 1 — Select Password

1. Open Dashlane.
2. Navigate to Passwords.
3. Select the password to share.

Step 2 — Share

1. Select Share.
2. Enter the recipient’s email address.

Step 3 — Choose Permission Level

Limited Rights (Recommended)

- Can use login credentials
- Cannot view, edit, or re-share the password

Full Rights

- Can view password
- Can edit
- Can re-share

Step 4 — Send Share

Select Share. The recipient must accept the invitation.

5. Creating Groups for Password Sharing (Business Feature)

Groups allow sharing access with multiple users at once.

Step 1 — Open Sharing Center

Open Sharing Center within Dashlane.

Step 2 — Create Group

1. Select Create Group.
2. Enter a group name (example: Office Staff, AV Team).

Step 3 — Add Members

Add user email addresses and assign permissions if prompted.

Step 4 — Share with Group

1. Open a password item.
2. Select Share.
3. Choose the group instead of individual users.

Benefits:

- Easier onboarding and offboarding
- Centralized access management
- Reduced administrative effort

6. Adding Secure Notes

Secure Notes store sensitive information in encrypted form.

Examples:

- Alarm codes
- WiFi details
- Vendor contacts
- Internal procedures

Step 1 — Create Secure Note

1. Open Dashlane.
2. Navigate to Secure Notes.
3. Select Add New.

Step 2 — Enter Information

Add a title and content. File attachments are optional.

Step 3 — Save

Select Save.

Step 4 — Share Secure Notes (Optional)

1. Open the secure note.
2. Select Share.
3. Choose users or groups.

7. Account Recovery if Password Is Forgotten and Recovery Was Not Enabled

If recovery options were not enabled, the encrypted vault cannot be recovered. The account must be reset. Please let the Dashlane Admin know when you start this process.

Current Admin: Holly and Katie

Step 1 — Initiate Account Reset

1. Go to https://www.dashlane.com/
2. Enter your email and select Next.
3. Select Forgot your Master Password.
4. Choose Reset Account.
5. If you do not have the browser extension installed it will have you install it.
6. Follow instructions to reset your account.

Step 2 — Create New Account

After reset:

- Create a new account using the same email address as before.
- The vault will be empty.
- Credentials must be re-added manually.

Step 3 — Admin Removes and Reinvites User (Optional)

If issues occur:

1. Admin removes the user from the Dashlane Business Admin Console.
2. Admin reinvites the user to the organization.

8. Using the Dashlane VPN (Powered by Hotspot Shield)

Dashlane Business includes a Virtual Private Network (VPN) powered by Hotspot Shield. This VPN encrypts your internet connection to help protect sensitive information, especially when using public or unsecured WiFi networks.

The VPN service is provided through Hotspot Shield but is accessed through your Dashlane account.

When to Use the VPN

Use the Dashlane VPN when:

- Working on public WiFi (airports, hotels, coffee shops)
- Traveling
- Accessing sensitive organizational systems remotely

The VPN is typically not required when working on a secured office network.

How to Set Up the VPN (First-Time Use)

Step 1 — Open Dashlane

1. Open the Dashlane web app or browser extension.
2. Navigate to the VPN section.

Step 2 — Activate VPN Access

1. Select Enable VPN or Get Started.
2. Dashlane will prompt you to activate your VPN subscription.

3. Follow the prompts to create or link your Hotspot Shield account (this is required for VPN access).

Step 3 — Download the Hotspot Shield App The VPN runs through the Hotspot Shield application.

1. Download the Hotspot Shield app for your device (Windows, macOS, iOS, or Android) when prompted.
2. Install the application.
3. Log in using the credentials created during activation.

Step 4 — Grant Device Permissions Your device may ask you to:

- Allow VPN configuration
- Approve network permissions

Approve these to complete setup.

How to Connect to the VPN

1. Open the Hotspot Shield application.
2. Select Connect.
3. Wait for confirmation that the VPN is active.

When connected, your internet traffic is encrypted.

How to Disconnect

1. Open the Hotspot Shield application.
2. Select Disconnect.

Important Notes

- The VPN protects internet traffic but does not replace strong passwords or two-factor authentication.
- Internet speed may vary while connected.
- If you experience connectivity issues, disconnect and reconnect.
- The VPN is intended for business security use and should not be used to bypass organizational policies.

Best Practices

- Use Limited Rights sharing unless full access is required.
- Store shared organizational information in Secure Notes rather than email.
- Use groups instead of individual sharing whenever possible.
- Enable Admin-Assisted Recovery immediately after setup.
- Create and store an Account Recovery Key securely.
- Never share your Master Password.

Revision #4
Created 2026-02-11 21:14:08 CET by Holly
Updated 2026-04-26 20:45:28 CEST by Holly