MIGRATION PLAYBOOK · IDENTITY AND SECURITY

How to migrate your business to a new password manager

Set up the new organisation and its policies first, import shared vaults into collections or shared vaults, onboard users, then have each person move their own items. Attachments, passkeys and one-time codes often need to move by hand.

Updated 4 Nov 2026 4 phases 4 detailed steps 4 official sources

START HERE

How do you migrate your business to a new password manager?

SHORT ANSWER

This moves your team's saved passwords from one password manager (or from web browsers) into a new business password manager. An admin sets up the new service and its security rules, copies the shared company passwords in, then invites staff.

- **Recommended route:** Admin imports shared data into the organisation, then users import their own items
- **Order:** Policies before people, shared before personal, and clean-up straight after.
- **4 phases:** Set up the new organisation, Import shared data, Onboard users and Close the old manager.
- **You're done when:** All shared items are in the right collections or vaults with the right access.

Each person moves their own items. Files attached to entries and some special item types may need moving by hand, and every export file is deleted once imported.

RECOMMENDED ROUTE

Admin imports shared data into the organisation, then users import their own items

Keeps company data in shared collections or vaults with the right access, and keeps personal items out of shared space.

▼ **Other options and when to use them**

- **Each user imports everything themselves**
  : Very small teams with no shared folders.
- **Direct import from the old manager**
  : Bitwarden can import directly from LastPass without a file, which avoids an unencrypted export.

TOOLS FOR THIS PLAN

Are you ready?	Plan your dates	New to the jargon?
22-question readiness check	Dated countdown you can add to your calendar	Plain-English migration glossary

ORDER TO MIGRATE IN, AND WHY

Policies before people, shared before personal, and clean-up straight after.

1. **New organisation, SSO and policies**
   Bitwarden recommends configuring policies before onboarding users.
2. **Shared folders mapped to collections or vaults**
   Decides who sees what after import.
3. **Admin import of shared data**
   Bitwarden advises importing straight into the organisation, not a personal vault.
4. **Users invited and confirmed**
   They need accounts before they can see shared data or import personal items.
5. **Users import personal items and re-attach files**
   Attachments are not imported.
6. **Export files deleted, old service closed**
   Exports are unencrypted.

SETTINGS CHECKLIST: DECIDE THESE BEFORE YOU COPY

Built-in and third-party tools treat these differently. Tick each one off once you have decided.

Download this checklist (Excel)

- [ ] **Where shared folders go**

  Collections (Bitwarden) or shared vaults (1Password) and who gets access.

  ▼ How each tool handles it

Built-in method	Bitwarden: put each shared folder name in the Collection column of the organisation import CSV. Groups are the most effective way to manage access, and permissions combine as a union.
1Password	Desktop import from LastPass turns each shared folder into a vault and maps permissions; needs permission to create vaults.

  Tip: Map one shared folder per collection or vault, named after the team that owns it.

  Bitwarden: Teams and Enterprise migration guide

- [ ] **What will not import**

  Who re-adds attachments and other items.

  ▼ How each tool handles it

Built-in method	Bitwarden: file attachments are not imported and must be uploaded manually; Sends must be recreated.
1Password	Desktop import from LastPass keeps attachments; passkeys and LastPass Authenticator codes are not imported.

  Tip: Ask owners to list items with attachments or one-time codes before the move.

  Bitwarden: Import data from LastPass

- [ ] **Export safety**

  How exports are handled.

  ▼ How each tool handles it

Built-in method	Bitwarden: delete the export file after a successful import, since a compromised computer could expose it.

  Tip: Export and import on one trusted computer in one sitting, with backup and sync paused.

  Bitwarden: Import data from LastPass

- [ ] **User onboarding**

Manual invites or directory sync.

▼ How each tool handles it

Built-in method	Bitwarden: SCIM for Azure AD (Entra ID), Okta, OneLogin and JumpCloud, or Directory Connector; SSO with SAML 2.0 or OIDC.

Tip: Sync groups from your directory so access follows team membership.

Bitwarden: Teams and Enterprise migration guide

THE PLAN, PHASE BY PHASE

1 Set up the new organisation Week 1

Create the organisation and admin accounts.

Set up SSO and policies.

Create collections or shared vaults and groups.

Watch out: Free Bitwarden organisations allow only two collections.

WAYS AROUND IT

- Use a paid plan, or remove the grouping column before import.

Show the detailed steps (1) →

2 Import shared data Week 1

Export or directly import shared folders.

Remove personal items from the file.

Import into the organisation and check access.

> **Watch out:** Re-importing creates duplicates.
>
> **WAYS AROUND IT**
>
> - Import each file once; clean up duplicates before onboarding.

Show the detailed steps (1) →

3 Onboard users Week 2

Invite users or sync them from the directory.

Confirm users and check

group access.

- [ ] Ask each user to import personal items and re-attach files.

> **Watch out:** Attachments, passkeys and one-time codes may not import.
>
> **WAYS AROUND IT**
>
> - Re-add them by hand from the old manager.

Show the detailed steps (1) →

4 Close the old manager Week 3 to 4

- [ ] Confirm every team has signed off.
- [ ] Delete export files everywhere.
- [ ] Remove browser extensions and cancel the old service.

> **Watch out:** Old exports may be in backups or downloads folders.
>
> **WAYS AROUND IT**
>
> - Check Downloads and sync folders on the computers used.

Show the detailed steps (1) →

You are finished when

- All shared items are in the right collections or vaults with the right access.
- Every user has imported personal items and re-added attachments.
- All export files are deleted.
- The old manager is cancelled and its browser extensions removed.

CLICK BY CLICK

What does each step involve?

Open a part when you reach it in the plan. Each step says where to go, what to do and what you should see.

About this migration

What it covers, limits at a glance

Password manager moves are small in data but high in risk: every export is an unencrypted file of your company's secrets. Both Bitwarden and 1Password import from LastPass, browsers and CSV files. What carries over differs: Bitwarden leaves attachments behind, while 1Password's desktop import from LastPass keeps them and turns shared folders into vaults.
This playbook covers the order that keeps shared data tidy and personal data private. Tightening identity at the same time? See Essential Eight in Microsoft 365.

ORDER	SHARED FOLDERS	ATTACHMENTS
Organisation and policies, shared data, users, then personal items	**Bitwarden collections or 1Password shared vaults**	**Bitwarden: re-attach by hand; 1Password desktop import from LastPass keeps them**
1PASSWORD FROM LASTPASS	DUPLICATES	AFTER IMPORT

Shared folders become vaults; passkeys not imported

Bitwarden import does not de-duplicate

Delete the unencrypted export file

1 What do you need before you migrate your business to a new password manager?

Need	Details	Where to get it
Admin access to the old manager	A LastPass admin, not super admin, for Bitwarden direct import.	Old admin console
New organisation	Business plan with admin accounts.	New vendor's sign-up
Folder map	Shared folder to collection or vault, with owners.	The data mapping template
Trusted computer	For exports, with backup and sync paused.	IT

2 Set up the organisation and policies

1 step

1

Configure SSO and policies

Where: Bitwarden Admin Console > Settings > Single Sign-On, and Policies

Set up SSO and enable policies, such as master password requirements, before inviting anyone.

✓ **You should see:** Policies are on before the first user joins.

3 Import shared data

1 step

1

Import directly or from a file

Where: Bitwarden Admin Console > Settings > Import data; or 1Password desktop app > File > Import > LastPass (Mac)

Choose the file format (or LastPass direct import in Bitwarden), choose the file, and import into the organisation. In 1Password, shared folders you administer become vaults.

✓ **You should see:** Items appear in collections or the chosen vault.

4 Onboard users

1 step

1

Invite and confirm

Where: Admin Console > Members, or directory sync

Invite users, or sync them with SCIM or Directory Connector, then confirm them. Send the switch-over email with steps for personal items.

✓ **You should see:** Users see their team's shared items.

5 Clean up and close the old manager

1 step

1

Delete exports and remove the old service

Where: Computers used for exports; old admin console

Delete every export file, turn backups back on, remove the old browser extension through your device management, and cancel the old service once teams sign off.

✓ **You should see:** No unencrypted exports remain.

WORTH KNOWING

What can go wrong, and how do you avoid it?

The detail behind the plan: options compared, and what experienced engineers check first. Tap any item.

Compare all the ways to do this — 3 options —

Admin import, then users — MEDIUM EFFORT

Best for: Teams with shared folders

+ Clean shared structure
+ Personal items stay private
– Two stages to coordinate

Direct import (Bitwarden from LastPass) — LOW EFFORT

Best for: Avoiding unencrypted export files

+ No CSV on disk
– Not for Google Workspace or ADFS SSO
– Needs one-time codes for MFA

Users import everything

LOW EFFORT

Best for: Very small teams

+ Quick
− Shared items end up in personal vaults

OUR ADVICE

Import shared data as an admin into the organisation first, then have users import personal items. Use direct import where it fits to avoid plain-text exports.

Exports are unencrypted

REDUCES RISK

CSV exports hold every password in plain text. Bitwarden advises deleting the file after import because a compromised computer could expose it.

WHAT TO DO

Use direct import where available, or export on one trusted computer and delete straight away.

Bitwarden: Import data from LastPass

Attachments may be left behind

SAVES TIME

Bitwarden does not import file attachments; they must be uploaded to the vault manually.

WHAT TO DO

List items with attachments and re-attach them, or check whether your new manager's direct import keeps them.

Bitwarden: Import data from LastPass

Personal and shared data get mixed

COMPLIANCE

Bitwarden notes exports often mix individual and shared items.

WHAT TO DO

Remove personal items from the admin's file and have users import their own.

Bitwarden: Teams and Enterprise migration guide

Duplicates on re-import

USER IMPACT

Bitwarden does not check for duplicates when importing.

WHAT TO DO

Import each file once and check before onboarding users.

Bitwarden: Import data from LastPass

SSO limits on direct import

SAVES TIME

Bitwarden direct import from LastPass does not support Google Workspace or ADFS identity providers.

WHAT TO DO

Use a file export for those organisations.

Bitwarden: Import data from LastPass

FINISH SAFELY

How do you check it worked, or roll back?

Full validation checklist

4 checks

Run these before you declare the migration complete. Record the results in the data validation report.

Check	How to check	What good looks like
Shared items in place	Ask each team owner to check their collection or vault.	Counts match the old shared folders.
Access is right	Test as a member of each group.	Users see only their teams' items.
Attachments re-added	Check the list of items with attachments.	All re-attached.

Check	How to check	What good looks like
Exports deleted	Check computers used for export.	No export files remain.

Rollback plan

If it goes wrong

ROLL BACK IF

- Shared items are missing or visible to the wrong people
- Users cannot sign in to the new manager

POINT OF NO RETURN

Until you cancel the old manager, users can keep using it. After cancelling, its data is gone.

1

Pause onboarding

Where: New admin console

Stop inviting users and fix collection access.

✓ **You should see:** No more users see wrong items.

2

Keep the old manager live

Where: Old admin console

Tell users to keep using it until fixed.

✓ **You should see:** Nobody is locked out.

Agree the triggers and who decides before the go / no-go meeting. Use the rollback plan template.

Common problems and fixes

4 errors

`This organization can only have a maximum of two collections`

Cause: Free Bitwarden organisation with three or more groupings.

Fix: Upgrade, or remove the grouping column before import.

`Special characters look wrong after import`

Cause: The export HTML-encoded characters.

Fix: Find and replace them in a text editor before importing.

`Bitwarden direct import fails`

Cause: Super admin credentials used, or unsupported SSO.

Fix: Use a LastPass admin account, or a file export.

`Items imported twice`

Cause: The file was imported more than once.

Fix: Delete duplicates; imports do not de-duplicate.

Search the full error library →

FAQ

Frequently asked questions

Do attachments move?

Not into Bitwarden. 1Password's desktop import from LastPass keeps them.

Do LastPass shared folders keep their structure?

In Bitwarden, map them to collections. 1Password's desktop import turns each into a vault.

Should users import their own items?

Yes. It keeps personal items out of shared space.

What do I do with the export file?

Delete it as soon as the import succeeds.

SOURCES

Official sources

4 official pages this guide is based on

Vendors change limits and features, so confirm details on the source before you rely on them. Last checked 4 Nov 2026.

- Bitwarden: Teams and Enterprise migration guide
- Bitwarden: Import data from LastPass
- 1Password Support: Move to 1Password from another app
- 1Password Support: Move your data from LastPass to 1Password in the desktop app