

RESOURCE CENTER

LastPass Migration Kit for Organizations

In this kit, we'll cover the most common LastPass to Bitwarden migration process, including step-by-step instructions on how to move systems and onboard users.

Get the full interactive view at
<https://bitwarden.com/sv-se/resources/lastpass-migration-kit/>



Introduction

Moving to a new password management system can seem like a daunting task, especially if you're in charge of handling hundreds to thousands of users in your organization. That's why we put this kit together to help you at every stage of your migration journey.

In this kit, we'll cover the most common LastPass to Bitwarden migration stages, including step-by-step instructions on how to move systems and onboard users easily and efficiently. Get started by navigating to where you are in your migration process using the table of contents.

"When we exported from LastPass and imported to Bitwarden, it was a very smooth transition. I was impressed because we had mountains of data that we migrated and it was very simple."

Andrew Nguyen
CTO, Golden Communications



Bitwarden Case Study with Golden Communications

Table of Contents

- [Introduction](#)
- [Getting started](#)
- [LastPass Enterprise Migration Guide](#)
 - [Step 1: Create and configure your Bitwarden organization](#)
 - [Step 2: Import your data into Bitwarden](#)
 - [Step 3: Onboard your users](#)
 - [Step 4: Configure access to collections and vault items](#)
- [Additional Migration Journey Resources](#)
- [Migration support](#)

Getting started

Bitwarden for business

Bitwarden enables teams and enterprises to easily facilitate secure password sharing among colleagues. Reduce cybersecurity risk by enacting strong password policies for all employees and monitor activity with audit logs. Bitwarden integrates seamlessly with your existing security stack and supports SSO and directory service integrations. Features such as passwordless authentication, biometric unlock, security key support, and credential autofill make it easy for employees to access their important accounts, ensuring productivity for your company.

Choose the right plan for your business to get started.

- [For Teams \(\\$4 per user/month*\)](#): Share private data safely with coworkers, across departments, or the entire company.
- [For Enterprise \(\\$6 per user/month*\)](#): Advanced functionalities, including enterprise policies, SSO integration, SCIM support, and more.

*pricing is based on an annual subscription

Bitwarden for you

For individuals interested in exploring Bitwarden features, we recommend starting with a free plan which includes all the bells and whistles you'll need to strengthen your online security. Leverage the [import options](#) to make your switch to Bitwarden quick and easy.

LastPass Enterprise Migration Guide

Securely migrating your passwords and other sensitive information to Bitwarden is a straightforward and secure process. This guide describes the best practices for safely migrating data from Lastpass to a Bitwarden [Teams or Enterprise organization](#), building an infrastructure for security based on simple and scalable methods. The steps in this guide are listed in the recommended order for ease of use and smooth user onboarding.

Start migrating from LastPass to Bitwarden by following these simple steps:

1. [Create and configure your Bitwarden organization](#)
2. [Import your data into Bitwarden](#)
3. [Onboard your users](#)
4. [Configure access to collections and vault items](#)

Step 1: Setup your organization

Bitwarden organizations relate users and vault items together for [secure sharing](#) of logins, notes, cards, and identities.

1. **Create your organization.** Start by creating your organization. To learn how, check out [this article](#). To self-host Bitwarden, create an organization on the Bitwarden cloud, generate a [license key](#), and use the key to [unlock organizations](#) on your server.
2. **Onboard administrative users.** With your organization created, further setup procedures can be made easier by onboarding some [administrative users](#). It's important that you **do not begin end-user onboarding** at this point, as there are a few steps left to prepare your organization. Learn how to invite admins [here](#).
3. **Configure identity services.** Enterprise organizations support [logging in with single sign-on](#) (SSO) using either SAML 2.0 or OpenID Connect (OIDC). To configure SSO, open the organization's **Settings → Single Sign-On** screen, accessible by [organization owners and admins](#).
4. **Enable enterprise policies.** [Enterprise policies](#) enable organizations to implement rules for users, for example requiring use of two-step login. It is highly recommended that you configure policies before onboarding users.

Pro Tip

If you need assistance during your migration, our [Customer Success team](#) is [here to help](#)!

Tip

It's important that you create your organization first and [import data to it directly](#), rather than importing the data to an individual account and then [moving items](#) to the organization secondarily.

Step 2: Import to your organization

Data can be imported directly from LastPass or using an [exported file](#) from LastPass. If you're a member of a team using SSO with LastPass, a LastPass administrator will need to complete a short setup procedure before you can use the **Direct import** option ([learn more](#)).

To import data to your organization using the **Direct import** method:

1. Log in to the Password Manager browser extension or desktop app.
2. In the browser extension, select the **Settings** tab and choose the **Import items** option. Or, in the desktop app, select **File > Import data**.
3. Complete the following fields from the drop down menus:
 - **Import destination:** Select the import destination, such as the organizational vault that you have access to.
 - **Folder or Collection:** Select if you would like the imported content moved to a specific collection that you have access to.
 - **File format:** Select **LastPass**.
 - In the LastPass Instructions box, choose the **Import directly from LastPass** option.
 - Enter your **LastPass email**.
4. Select the **Import data** button to trigger the import.
5. You will be prompted for your LastPass master password or, if your LastPass account uses SSO, to log in to your IdP. In either case, follow the prompts to log in to your LastPass account.

Tip

If your LastPass account has multi-factor authentication activated, you will be prompted to enter a one-time passcode from your authenticator app. If you use Duo for MFA, only in-app approval is supported to fulfill your MFA requirement.

Tip

You should also recommend to employees that they export their individually-owned data from your existing password manager and prepare it for import into Bitwarden. Learn more [here](#).

Step 3: Onboard users

Bitwarden supports manual onboarding via the web vault and automated onboarding through SCIM integrations or syncing from your existing directory service:

Manual onboarding

To ensure the security of your organization, Bitwarden applies a 3-step process for onboarding a new member, [invite](#) → [accept](#) → [confirm](#). Learn how to invite new users [here](#).

Automated onboarding

Automated user onboarding is available through SCIM integrations with [Azure AD](#), [Okta](#), [OneLogin](#), and [JumpCloud](#), or using [Directory Connector](#), a standalone application available in a [desktop app](#) and [CLI](#) tool that will synchronize users and groups from your existing directory service.

Whichever you use, users are automatically invited to join the organization and can be confirmed manually or automatically using the [Bitwarden CLI tool](#).

Step 4: Configure access to collections and items

Share vault items with your end-users by configuring access through collections, groups, and group-level or user-level permissions:

Collections

Bitwarden empowers organizations to share sensitive data easily, securely, and in a scalable manner. This is accomplished by segmenting shared secrets, items, logins, etc. into **collections**.

Collections can organize secure items in many ways, including by business function, group assignment, application access levels, or even security protocols. Collections function like shared folders, allowing for consistent access control and sharing amongst groups of users.

Shared folders from LastPass can be imported as collections into Bitwarden by using the organization import template found [here](#) and placing the name of the shared folder in the **collections** column.

Collections can be shared with both groups and individual users. Limiting the number of individual users that can access a collection will make management more efficient for admins. Learn more [here](#).

Groups

Using groups for sharing is the most effective way to provide credential and secret access. Groups, like users, can be synced to your organization using SCIM or Directory Connector.

Permissions

Permissions for Bitwarden collections can be assigned on the group or user-level. This means that each group or user can be configured with different permissions for the same collection. Collection permissions options include options:

- Can view
- Can view, except passwords
- Can edit
- Can edit, except passwords
- Grant access to all current and future collections

Learn more about permissions [here](#). Bitwarden uses a union of permissions to determine final access permissions for a user and a collection. For example:

- User A is part of the Tier 1 Support group, which has access to the Support collection, with can view permission.
- User A is also a member of the Support Management group, which has access to the Support collection, with can edit access.
- In this scenario, User A will be able to edit to the Collection.

Note

Nested collections do not inherit the permissions of the top level collection. See [using groups](#) to designate permissions.

Additional Migration Journey Resources

If you have more questions about your migration journey or need help, feel free to [reach out to us](#) or check out these additional resources below:

- [Free 7-Day Enterprise Trial](#)
- [Bitwarden Community Forums](#)
- [Reddit Community](#)
- [Contact Us](#) | [Twitter](#) | [Facebook](#) | [LinkedIn](#) | [YouTube](#)

Migration support

The Bitwarden Customer Success team is available 24/7 with priority support for your organizations. If you need assistance or have questions, please do not hesitate to [contact us](#).