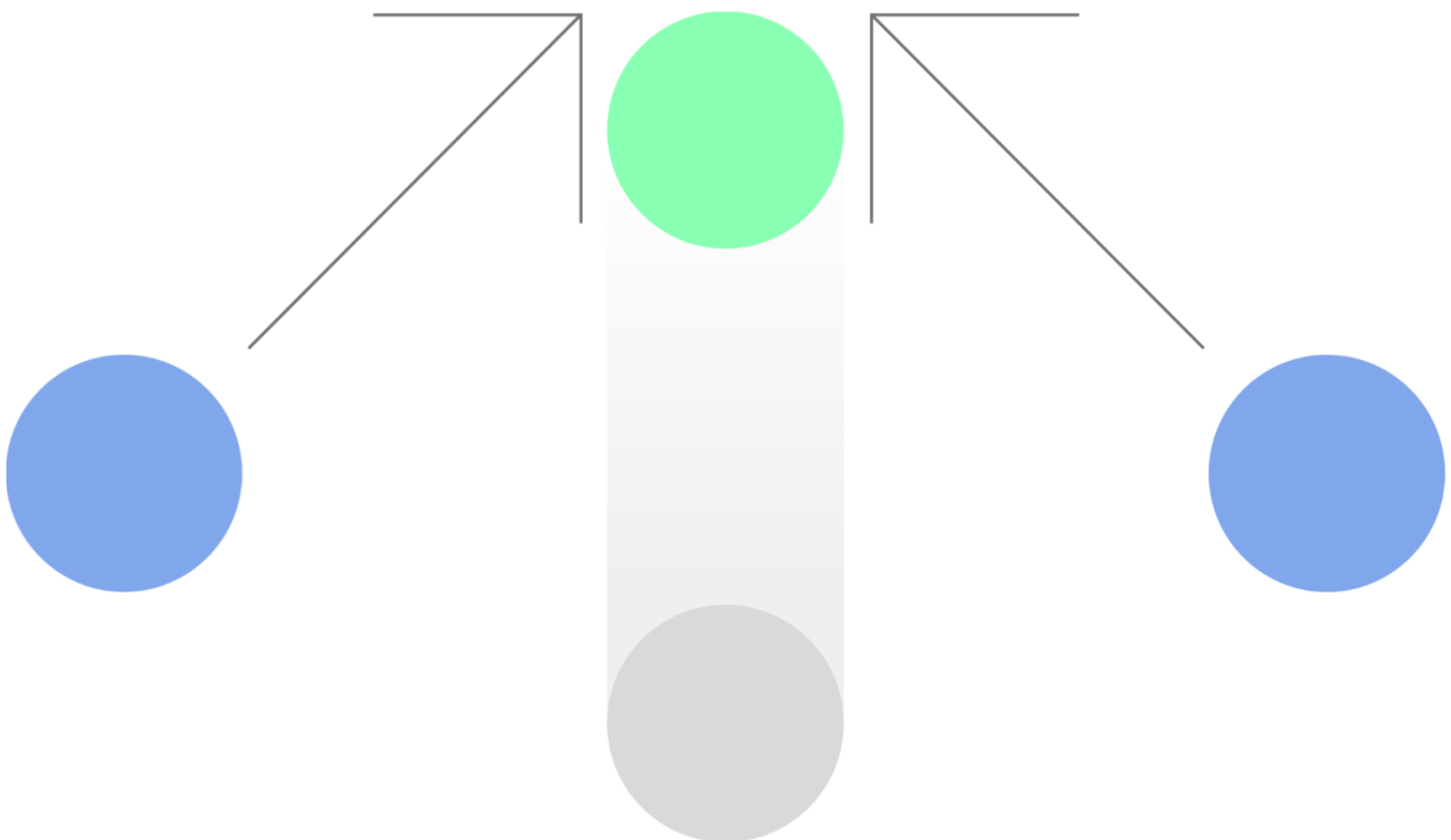


 **bitwarden**

LastPass Migration Kit



## Intro

Moving to a new password management system can seem overwhelming, especially if you're in charge of handling dozens to hundreds of users across several different tech stacks. That's why we put together this kit to help, whether you're still evaluating if Bitwarden is worth the move or if you are ready to go.

### Where You Are in Your Current Migration Journey

Navigate to where you are in the migration process and discover several resources including: point-of-view materials (case study, video, news article and blog post) from colleagues who've made the switch and industry leaders, as well as help center notes detailing step-by-step instructions on how to move systems and get users onboarded.

We'll cover the most common stages users face as they move throughout their migration journey, including:

#### [Thinking about Moving](#)

- I. [Case study of how one company accomplished a successful migration](#)
- II. [Video on how flawless moving 800 passwords was for one organization](#)
- III. [What others in the news are saying about migrating](#)

#### [Starting your Move](#)

- I. [How Moving Your Passwords is Free and Easy](#)
- II. [Importing and Migration Guide](#)

#### [Onboarding users](#)

- I. [Sharing Collections and Items](#)

#### [Additional Migration Journey Resources](#)

## Thinking About Moving

If you're reading this, it's likely because you've heard all the frenzy around LastPass changing some of their plans and Bitwarden has come up as another alternative. Here's what others have to say about their own migration journeys.

### Case Study

Read the full information below, or visit the case study on our website [here](#)



Video technology company, Alpha Video & Audio, Inc. found themselves in a similar situation.

#### Alpha Video & Audio, Inc.

Alpha Video & Audio, Inc. is a US-based integrator of audiovisual, broadcast, and IPTV technologies. John Parker (JP), an IT administrator at Alpha Video for over 20 years, says Bitwarden was the ideal solution for their company because of the open-source software approach, no-nonsense interface, and a highly responsive support staff.

Alpha Video was using a bulkier password management solution, but wanted a less-busy interface to expand to their entire employee base. "We looked at our previous solution and decided the framework of it wasn't necessary...Some people might take this as a dig, but I like the no-nonsense interface of Bitwarden. It's really easy to navigate."

When doing a stadium set up for an event, it's not uncommon for the Alpha Video field team to be managing hundreds of IP addresses, on top of logins for media equipment and switches. At this scale, it's impossible to manually manage passwords and log in information for all of the technology devices they need to operate.

Equally important, they wanted a solution that came with exceptional customer support, since they noticed support with their previous solution took days to get a response.

## Deploying a suite of Bitwarden solutions

Alpha Video retired their old solution, migrated, cleaned up the data, and implemented new best practices for how they were going to deploy Bitwarden across the organization.

### Migration to Bitwarden:

JP reports migrating to Bitwarden from their previous solution was easy. The hard part was realizing that in the prior solution, data wasn't being properly stored in the correct fields. "Yes, it was secure—but employees weren't putting information in the right place," he said. With the migration to Bitwarden, he saw an opportunity for some education.

### Company-wide training:

After the data cleanup, it was clear that employees needed additional support for using Bitwarden. JP and his team instituted a mandatory training with virtual classes and documentation. This ensured everyone was using Bitwarden to its full potential, making use of both individual and collaborative features.

### Bitwarden Directory Connector:

Alpha Video is "group heavy," according to JP, meaning they rely on organizing teams within their directory service. So, it was important that the solution they chose could leverage their existing LDAP groups to organize their Bitwarden instance. The Directory Connector made it easy to onboard users and ensure they have the right group associations.

*"It's not uncommon for us to manage 500, 600, or 800 IP addresses when we're doing stadiums. It's nice to have all that information in one secure place."*



## A Central, Secure Place for Sensitive Information

A unique use case for Alpha Video is having the ability to use Bitwarden as a secure place to hold important customer data.

As a systems integrator, the company needs to store many important credentials for dozens of clients. Bitwarden uses end-to-end encryption that allows Alpha Video to store clients' credentials in templates, be put into Collections, and then can easily be shared with those throughout the company that need access.

Beyond the client database, Alpha Video also uses Bitwarden as a central place to securely store and share vendor information and financial details for specific teams.

Bitwarden search makes it easy to find anything you're looking for. In fact, it's one of JP's favorite things about Bitwarden. "Bitwarden search allows you to put in a term and it delivers the stuff you're actually looking for."

JP offers a fun take on the password generator feature. Using the passphrase option, he says he's got some pretty good band names out of the combinations. "Believe it or not, I have a list of fictional band names that I've curated over the last four or five years."



## Balancing Security and Convenience

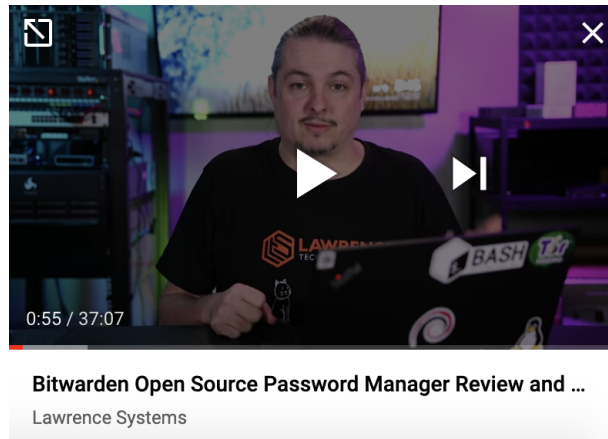
As most IT professionals can agree, JP says management typically prefers convenience while security professionals want the utmost security. But you want to find a solution that balances both—like Bitwarden.

Rolling out a new security tool can take some time, but in the end, it makes JP's life a lot easier. "Bitwarden made my life a heck of a lot easier. We're not herding cats anymore."



## Video

### Bitwarden Open Source Password Manager Review and Why We Moved From LastPass - Lawrence Systems



[YouTube Video](#)

“I have right around 700 or 800 passwords that I needed copied over. When you run and do the export you just have to export with LastPass and they link to the article How to Export From LastPass. You copy that and paste it in or you save it as a csv file and it imported flawlessly. That part was way less pain than I thought, so switching was really really easy for me.”

- Tom Lawrence

## Industry News

# Forbes

## Forbes - LastPass Breaks Free Accounts: Where To Store Your Passwords Now?

[Read Forbes Article](#)

“My recommended course of action is to switch to one of LastPass’s rivals, such as Bitwarden. I’ve written about the brilliant Bitwarden before: it’s free, open source and it works with almost any device you can name.”

-Barry Collins/Forbes

# c|net

## CNET - Need a LastPass alternative? This is the best free password manager we've found

[Read CNET Article](#)

“Bitwarden has proven a solid product, one I have no qualms about recommending.”

- Rick Broida/CNET

# c|net

## CNET- Bye, LastPass. Here's how to export your data and switch to a new password manager

[Read CNET Article](#)

“Bitwarden makes it easy to bring your LastPass credentials with you.”

- Jason Cipriani/CNET

Start a [free trial today](#) or let us know if you are [ready to make the move](#).



## Starting Your Move

### Blog Post : **Moving Password Managers is Free and Easy**

Read the full information below, or visit the blog post on our website [here](#).



Password managers are serious business. And moving password managers can be an equally serious step for long-time users.

The good news is that moving password managers can be simple and straightforward, putting you in a position to choose the tools that work best for you.

### Migrating to Bitwarden

It's easy to import data from any other password management solution to a Bitwarden Vault. Bitwarden supports a wide range of formats for import, including those used by the most popular password management solutions.

To learn how to import data, please visit this help note [bitwarden.com/help/article/import-data/](https://bitwarden.com/help/article/import-data/).

For advanced users who may have Vaults with unique items, check out a help note on troubleshooting import errors <https://bitwarden.com/help/article/import-data/#length-related-import-errors>.

For more migration information replay our Vault Hours - Migration Edition from February 26th [here](#).

## See what others are saying

If you'd like to hear from others who made the switch, check out the following presentation which includes comments from our newest users!

Here's one of our favorites:



**Jordan Crowley**

@jordanvc\_\_

Anyone looking to switch should use [@Bitwarden](#) it is open source, has a good free tier, and you can even self-host if you want. I just made the switch

8:24 AM · Feb 16, 2021 · Twitter Web App

Hear from the community about switching to Bitwarden, view presentation [here](#).

## Help Note : Import Data from LastPass

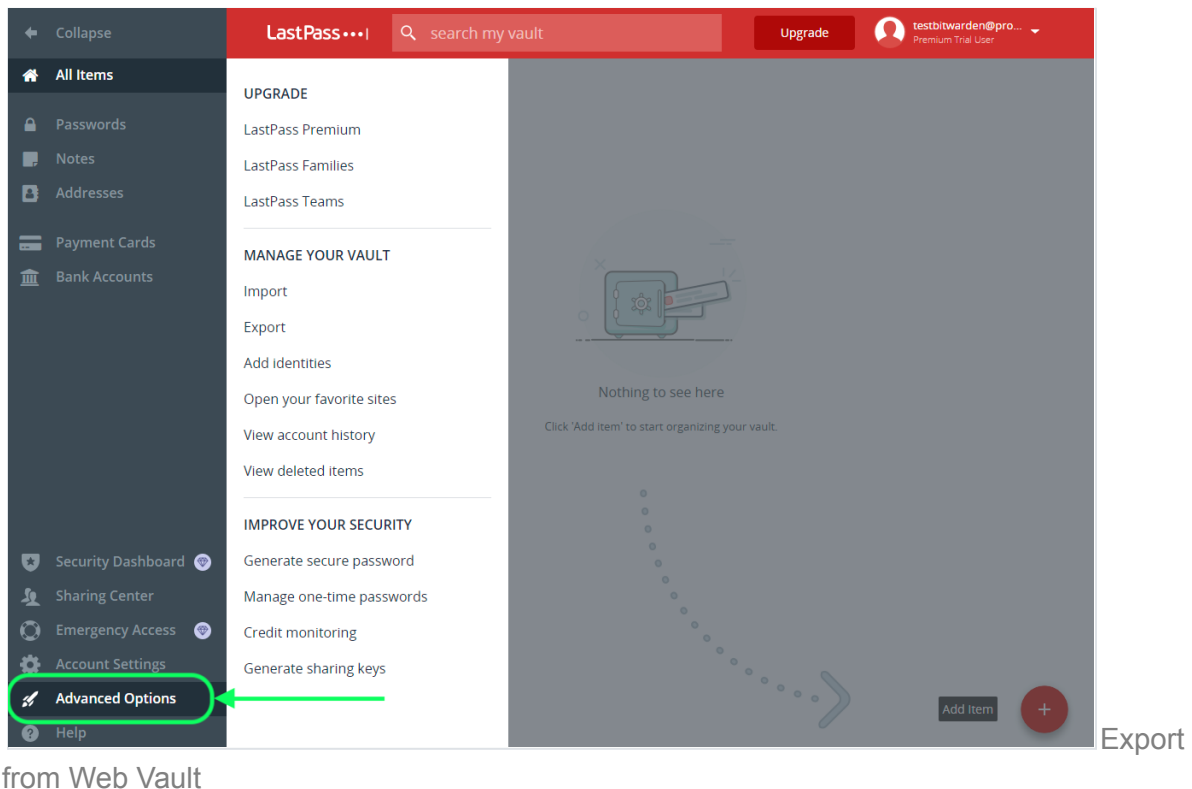
Use this article for help exporting data from LastPass and importing into Bitwarden.

Read the full information below, or visit the help note on our website [here](#).

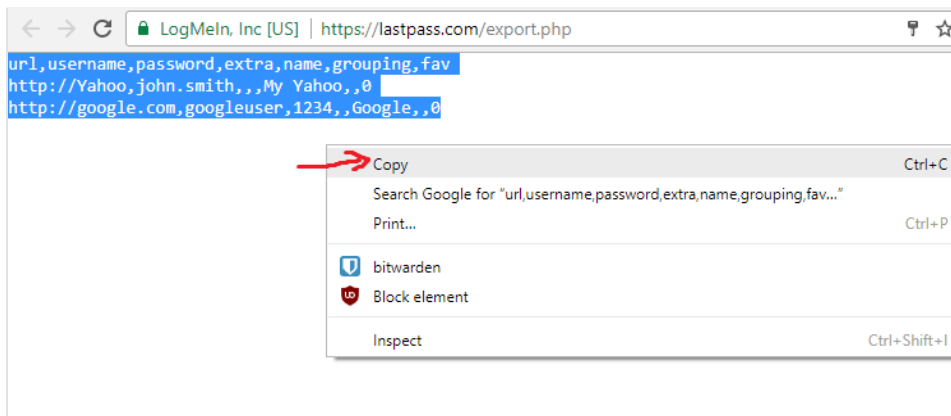
### Export from LastPass

Complete the following steps to export data from the [LastPass Web Vault](#):

1. Select the **Advanced Options** option on the left sidebar:



2. From the Manage Your Vault section, select the Export option.
3. Enter your Master Password to validate the export attempt.  
Depending on your browser, your Vault data will either be automatically saved as a **.csv** or printed to the screen in a **.csv** format:



LastPass Export

4. If your Vault data was printed to the screen, highlight the text and copy and paste it into a new **export.csv** file.

## Warning:

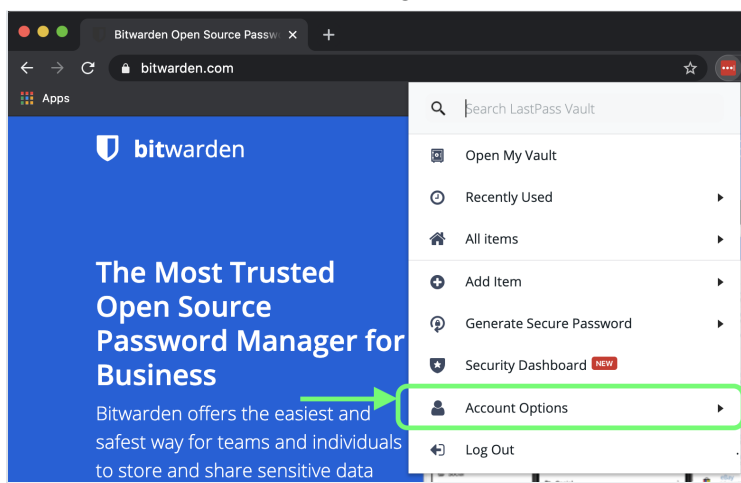
**Some users have reported a bug** which changes special characters in your password (&, <, >, etc.) to their HTML -encoded values (for example, &amp;) in the printed export.

If you observe this bug in your exported data, use a text editor to find and replace all altered values before importing into Bitwarden.

## Export with Form Fills

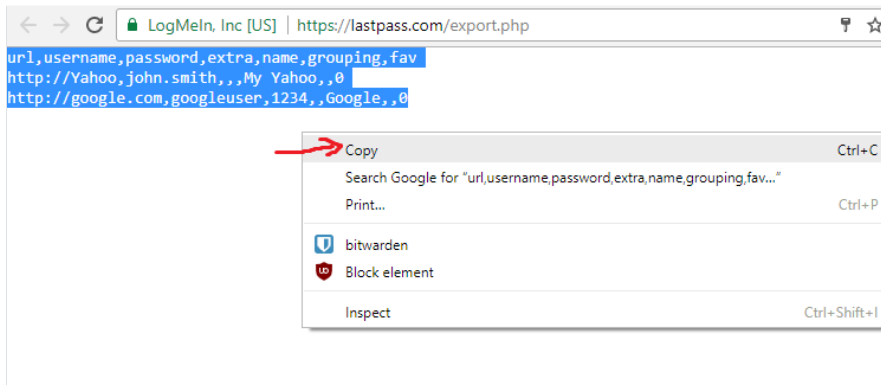
Exports from the Web Vault will not include form fills. To export form fill data from LastPass, you must do so from the Browser Extension:

1. In the Browser Extension, navigate to Account Options → Advanced → Export → Form Fills:



Export from Browser Extension

2. Enter your Master Password to validate the export attempt.  
Depending on your browser, your Vault data will either be automatically saved as a **.CSV** or printed to the screen in a **.CSV** format:



LastPass Export

3. If your Vault data was printed to the screen, highlight the text and copy and paste it into a new **export.csv** file.

## Import to Bitwarden

Complete the following steps to import data to your Bitwarden personal Vault. For help importing to an Organization Vault, see [Import Items to an Organization](#).

If you want to store File Attachments in your Bitwarden Vault, please be aware that these are currently not included in Bitwarden import operations and will need to be uploaded to your Vault manually. For more information, see [File Attachments](#).

1. Log in to the [Web Vault](#).
2. Select Tools from the top navigation bar.
3. Select Import Data from the left Tools menu.
4. Select LastPass (csv) from the format dropdown.
5. Select the Browse... button and add the file exported from LastPass.
6. Select the Import Data button to complete your import.

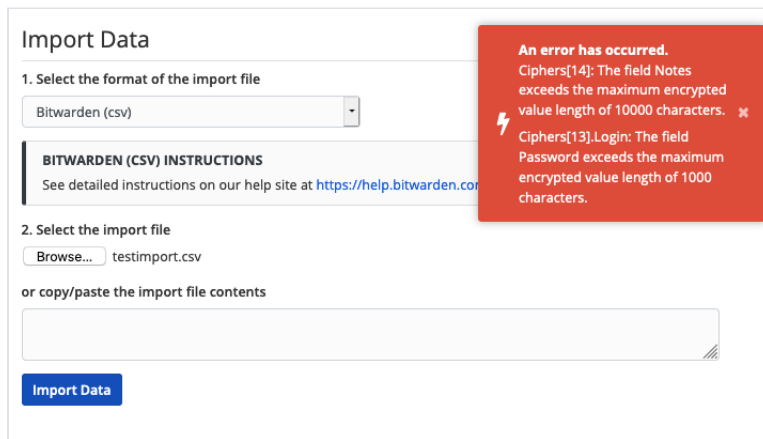
**Warning:** Importing data multiple times will create duplicates.

Congratulations! You have just transferred your data from LastPass into Bitwarden.

## Import Troubleshooting

### Character Limit Error

The following error messages, typically received when attempting to import a **.csv**, indicate that a field in your import file exceeds the allowed encrypted character limit for that field type:



The screenshot shows the 'Import Data' form in Bitwarden. It has two main sections: '1. Select the format of the import file' with a dropdown set to 'Bitwarden (csv)', and '2. Select the import file' with a 'Browse...' button and a text input containing 'testimport.csv'. Below this is a large text area for pasting contents and an 'Import Data' button. A red error box is overlaid on the right side of the form. The error message reads: 'An error has occurred. Ciphers[14]: The field Notes exceeds the maximum encrypted value length of 10000 characters. Ciphers[13].Login: The field Password exceeds the maximum encrypted value length of 1000 characters.'

### Cipher errors in the Web Vault

These error messages contain 3 pieces of pertinent data:

- **Ciphers[X]** indicates the index number where the offending item is located.
- **The field <field>** indicates the field name which is causing the offense.
- **length of <limit> characters** indicates the character limit allowed for that field.

### Note:

On import to Bitwarden, the character count of any given field is increased due to encryption, meaning that an 8000-character **note** field in your **.csv** will scale to 10,000+ characters when it comes into contact with Bitwarden, triggering this error. As a rule of thumb, character counts will grow between 30-50% when encrypted.

To solve this issue:

1. Open the **.csv** file you're attempting to import in a text editor or spreadsheet program.
2. Locate the offending item at **index[X]**. The value of **X** references a **.csv** index number, so depending on the program you use to edit your file it may not map perfectly to a spreadsheet Row or Line number.

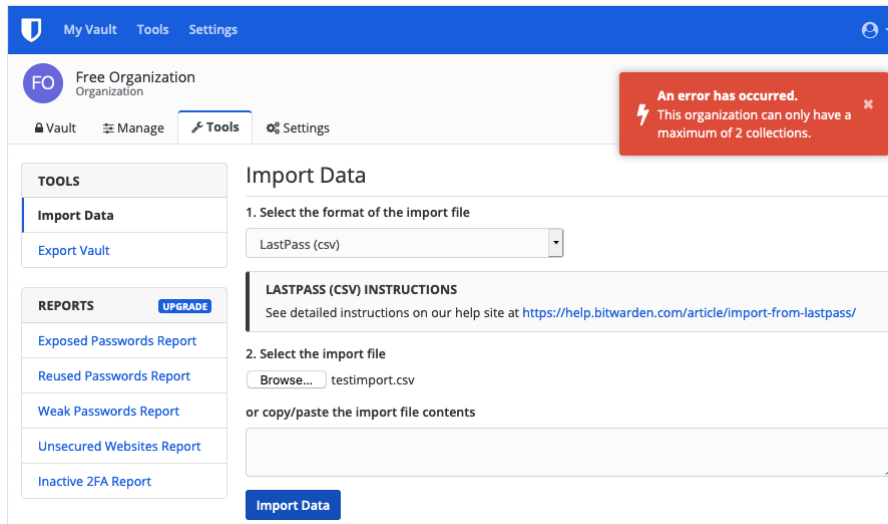
In many cases, you'll need to adjust for **.csv** header rows, which are not counted in many spreadsheet programs. It can also help to use field name (**yyyy**) and perceived character length as context clues.

*Tip: If you're having trouble locating the offending item using the data provided in the error, it may help to focus first on notes as these are frequently the cause of this error.*

3. Remove the offending item from your import file, or reduce the character count. When reducing the character count, remember that limits are placed on encrypted counts, not pre-encryption counts. As a rule of thumb, character counts will grow between 30-50% when Bitwarden attempts to encrypt a field on import.

## Maximum Collections Error

When importing Lastpass .csv exports to a [Free Organization](#), you may observe the following error:



## Free Organization Max Collections Error

This error occurs when the Lastpass export contains 3 or more **grouping** values. The values in the **grouping** field are interpreted by Bitwarden as **Collections**, however **Free Organizations** are limited to only two Collections. The following .csv, for example, would cause this error:

```
url,username,password,totp,extra,name,grouping,fav
https://www.facebook.com/login.php,login,password,,,Facebook,Social,0
https://twitter.com/login,login,password,,,Twitter,Social,0
https://asana.com/,login,password,,,Asana,Productivity Tools,0
https://github.com/login,login,password,,,Github,Productivity Tools,0
https://www.paypal.com/login,login,password,,,Paypal,Finance,0
https://www.bankofamerica.com/,login,password,,,Bankofamerica,Finance,0
```

To solve this issue, delete the **grouping** column and the **grouping** datum for each item, including the trailing comma, for example edit:

```
https://github.com/login,login,password,,,Github,Productivity Tools,0
```

down to:

```
https://github.com/login,test,test,,,Github,0`
```



## Help Note: **LastPass Enterprise Migration Guide**

Read the full information below, or visit the help note on our website [here](#).

Bitwarden-exclusive content: Making migration easy

Securing your Organization with Bitwarden is straightforward and secure.

Simply follow the below steps to migrate data and users from LastPass (or any other platform):

1. Export your data
2. Create and configure your Bitwarden Organization
3. Import your data into Bitwarden
4. Onboard your users and share

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

### Scope

This document will describe the best practices for migrating secure data from a LastPass instance to a Bitwarden Teams or Enterprise Organization, building an infrastructure for security based on simple and scalable methods.

Password management is crucial for organizational security and operational efficiency. Providing insight into the best methods to perform migration and configuration is designed to minimize the trial-and-error approach that is often needed when exchanging enterprise tools.

The below steps are listed in the recommended order for ease of use and smooth boarding for users.

### Exporting data

LastPass data may be exported inside of the web-based vault, or from a LastPass Client. For ease of manipulation, CSV is the recommended export format.

LastPass provides step-by-step instructions [here](#)

### Important notes on exported data

Data imported into Bitwarden is defined as one of four item types:

- Login (username, password, 2FA keys)
- Card (Credit Cards, Bank Cards)
- Identity (Name, address fields, personal information)
- Secure Note

Bitwarden currently limits the length of item fields to 1,000 characters, and Secure Notes to 10,000 characters. Items that exceed that criteria should be saved as separate files (text, key, pem, ssh, etc.) and added as attachments to an item.

- [More on Items](#)
- [Attaching a file to an item](#)

Gathering a full export of your data across your LastPass Organization may require assigning all shared folders to a single user, or performing multiple exports - one for each segment of shared folders.

Exported data from LastPass will contain data from both your Personal vault, as well as any Shared folders that the exporting user was assigned to. Be sure to remove any personal vault items before importing data into a Bitwarden Organization.

## Creating an Organization

Shared or company-level data is stored in a Bitwarden Organization. The best practice is to create this Organization first and import it directly, instead of importing the data into an individual account and then sharing it with the organization secondarily.

For more on creating a Bitwarden Organization, visit [this article](#).

Self-hosted instances will need to create an Organization on the Bitwarden cloud instance to generate their [license key](#) and can then proceed with [installing and configuring a Bitwarden Server instance](#).

**Note:** Self-hosting is available for Enterprise plans

## Configuring Identity services

Bitwarden Enterprise plans support Login with Single-Sign-On using either SAML 2.0 or OpenID Connect (OIDC).

Each Bitwarden Organization can configure one SSO provider. Configuration for this is located in the [Business Portal](#), accessible from the Web Vault by Organization Owners and Administrators.

For more details on Login with SSO configurations and examples of Identity Provider (IdP) settings and naming conventions, please visit [these help articles](#).

## Enabling enterprise policies

Policies are found in the [Business Portal](#)

Policies allow you to control the actions of users within your Organization. It is recommended to configure these policies prior to onboarding users. For a complete list and details for Enterprise Policies, please see our helpful article [here](#).

## Importing data

Importing information into Bitwarden can be performed in both an Individual Vault and Organization Vault. The below instructions are for Organization Imports.

There are two options to import data into your Organization:

Using the default CSV export file from LastPass. Creating a Bitwarden specific CSV from your exported data

The best practice for most Organizations is to format your data into a Bitwarden CSV, or for advanced users, a Bitwarden JSON file for import into your Organization vault.

For instructions on shaping a Bitwarden specific import file, please refer to the guide [here](#).

A collection of data import and export documentation is available [here](#). to assist with imports from additional sources.

**Note:** Importing multiple times will create duplicate records in your Bitwarden Vault.

### Individual user data import

Bitwarden supports a variety import formats from other password management platforms. Individual users can import their data into their Bitwarden Vault on their own, and does not require Administrative assistance.

For more on importing individual data, check out our helpful article [here](#).

## Onboarding Users

Bitwarden supports both manual and automated user invitation and boarding. Best practice is to manually board any necessary Administrative users during configuration and initial deployment, ensuring all Organization configurations including Enterprise Policies, Login with SSO, and Directory Connector are ready prior to automating the User invitation and boarding process.

### Manual onboarding

Manual boarding is done via the Web Vault. More information on manual user boarding can be found in this [helpful article](#)

### Automated onboarding

Automated user boarding is also available when leveraging Bitwarden Directory Connector - a standalone application available in a [Desktop app](#) and a [CLI tool](#) - synchronizing user and group information to the Bitwarden Organization. These users are automatically invited to join the Organization, and can be confirmed manually or automatically using the [Bitwarden CLI tool](#).

- Learn more about how syncing works [here](#).
- Discover how to configure user and group filters for Directory Connector [here](#).
- Documentation for multiple Directory Connector options is available [here](#).

## Sharing Collections and items

### Collections

Bitwarden empowers Teams and 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 organize secure items in many ways, including but not limited to: business function, group assignment, application access levels, or even security protocols. Collections perform the same functions as 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 Collection column.

Example LastPass Export:

| url                                | username     | password       | extra | name          | grouping        | fav |
|------------------------------------|--------------|----------------|-------|---------------|-----------------|-----|
| https://azure.microsoft.com/en-us/ | AzureUser    | 5HDXWtuAAK3SX8 |       | Azure Login   | Shared-Systems  | 0   |
| https://github.com/login           | GitHubUser   | P4JUghjRfhKrDJ |       | Github        | Shared-Systems  | 0   |
| https://adobe.com                  | AdobeUser    | T6RYSbD5mn78ab |       | Adobe Login   | Shared-Design   | 0   |
| https://shutterstock.com           | Shutterstock | 749bs2saWb3bxH |       | Shutterstock  | Shared-Design   | 0   |
| https://usps.com                   | USPSUser     | 6UmtWLkGydBMaZ |       | USPS Shipping | Shared-Shipping | 0   |
| https://ups.com                    | UPSUser      | YBD7ftBZbosS9u |       | UPS Login     | Shared-Shipping | 0   |
| https://fedex.com                  | FedexUser    | y44xgs5fiyYZNU |       | FedExUser     | Shared-Shipping | 0   |

Note: shared folders are listed in the grouping column

Example Bitwarden Organization Import

| collections     | type  | name          | notes | fields | login_uri                          | login_username | login_password | login_totp |
|-----------------|-------|---------------|-------|--------|------------------------------------|----------------|----------------|------------|
| Shared-Systems  | login | Azure Login   |       |        | https://azure.microsoft.com/en-us/ | AzureUser      | 5HDXWtuAAK3SX8 |            |
| Shared-Systems  | login | Github        |       |        | https://github.com/login           | GitHubUser     | P4JUghjRfhKrDJ |            |
| Shared-Design   | login | Adobe Login   |       |        | https://adobe.com                  | AdobeUser      | T6RYSbD5mn78ab |            |
| Shared-Design   | login | Shutterstock  |       |        | https://shutterstock.com           | Shutterstock   | 749bs2saWb3bxH |            |
| Shared-Shipping | login | USPS Shipping |       |        | https://usps.com                   | USPSUser       | 6UmtWLkGydBMaZ |            |
| Shared-Shipping | login | UPS Login     |       |        | https://ups.com                    | UPSUser        | YBD7ftBZbosS9u |            |
| Shared-Shipping | login | FedExUser     |       |        | https://fedex.com                  | FedexUser      | y44xgs5fiyYZNU |            |

Note: shared folders are now 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 Administrators.

For more information on assigning Collections to Users and Groups, please refer to our help article [here](#).

## Groups

Leveraging Groups for sharing is the most effective way to provide credential and secret access. Ideally Groups are mirrored from an LDAP service, however Bitwarden supports automatic Group synchronization via the Directory Connector application, as well as manually created ad-hoc Groups.

As a part of deployment preparations, it is possible to synchronize just groups from the LDAP directory before synchronization of Users begins, such that Collections can be assigned to Groups before users begin accessing Bitwarden.

For more information on filtering and synchronization of Users with the Bitwarden Directory Connector, please check out the article [here](#).

## Permissions

Bitwarden Collection permissions are assigned on the assignment of the Group or User to a particular Collection. This means that each Group or User can be configured with permissions for the same Collection.

Collection permissions are easily configured with options for Read Only and Hide Passwords.

Read Only prevents users from adding new items to that Collection, as well as preventing the editing or deleting of existing items. Hide Passwords prevents the users from seeing the Password field, TOTP field, and any custom field for an item that is listed as hidden. This permission is best used for Collections of items that are able to be auto-filled in a browser, since copying and pasting of credentials is disabled when this is configured.

Bitwarden uses an union of permissions to determine final access permissions for a User and a Collection Item.

### Example:

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

More information on permissions can be found on our help site [here](#).

## Migration support

The Bitwarden Customer Success team is available 24/7 with priority support for Enterprise and Teams Organizations. If you need assistance or have questions, please do not hesitate to contact us here: [bitwarden.com/contact](https://bitwarden.com/contact).

## Terms and equivalent references

### Organization

- A Bitwarden Organization is the encompassing “object” that relates all data for a given sharing entity. Click [here](#) for more information on Organizations.

### Folders for Individual Vaults

- Within Bitwarden, individual Users can create Folders and assign items to those folders to help organize their Vault. Folders function much like ‘tags’ since they are linked to your items by reference, and deleting a folder does not delete the data inside it. Organizations use Collections to group secure items that need to be shared with the same user(s) or user group(s).
- Within LastPass, folders behave in the same manner between an individual user and a business.

### Collections for Organizational Vaults

- Collections are used by Bitwarden Organizations to group secure items that need to be shared with the same user(s) or user group(s).
- Most often exported shared folders become Collections, however, you can organize Collections in a number of ways.

### User

- Any user who is a member of a Bitwarden Organization

### Group

- Bitwarden and LastPass support User Groups. When migrating to Bitwarden, you can leverage [BWDC](#) to synchronize your LDAP groups into your Bitwarden Organization.

### Read Only

- A permission that prevents users from adding new data to items within a Collection. Users can see / access all data within items but cannot add new items or modify existing data. This permission is set on a User or Group assignment to a Collection.

## Hide Password

- Permission to prevent users from seeing any part of a secure item within a Collection.

## User Type

- Users within Bitwarden can be granted a “user-type”. Users onboarded via Directory Connector are defaulted to “Users” that can only access items that they are assigned directly and do not have access to reconfigure sharing or permissions.

## Vault

- Storage area for encrypted data. Bitwarden users that are members of an Organization have an Individual and Organization Vault, encrypted with separate keys.

# 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](#)