Shared Folders

A Shared Folder is a special folder in your vault that you can use to securely and easily share sites and notes with other people in your Enterprise. Changes to the Shared Folder are synchronized automatically to everyone with whom the folder has been shared. Different access controls – such as 'Hide Passwords' – can be set on a person-by-person basis or in the form of policies. Shared Folders use the same technology to encrypt and decrypt data that a regular LastPass account uses, but are designed to accommodate multiple users for the same folder.

With Shared Folders:

- Anyone can create a shared folder.
- Simple to configure and maintain.
- You can share hundreds of passwords with hundreds of users individually or via user groups.
- Changes automatically propagate to all assigned users.

Options for managing Shared Folders

Once a folder is created and populated by the folder Admin, there are three different ways in which the folder can be assigned out to additional users:

1. **The folder Admin assigns and manages the folder manually.** In this scenario, from his/her vault the folder admin (for example, the division manager) can add and remove users, and edit user permissions on an individual by individual basis.
2. **Automate all folder assignments through the user group assignments in AD.** The creator of the folder simply assigns the folder to the appropriate user group from the existing AD groups. Once this mapping is completed,

the AD Sync Client will manage all user additions and removals for you based on any relevant changes in AD.

3. **Centralize the management function and have a dedicated person managing the groups manually through the Admin dashboard.** In this case, the designated individual would need to be a LastPass Admin. Using the 'Groups' function in the Admin dashboard, the Admin could add and delete users to groups, which would then map back to the relevant Shared Folders. The creator of the folder simply assigns the folder to the appropriate user group. In this scenario, you would typically publish the point of contact on your LastPass wiki page or internal FAQs so that users would know to whom they should direct a change request.

Limitations of Shared Folders

The current limitations of Shared Folders are:

- Each Shared Folder has a capacity of 1500 items.
- Sites can be copied to multiple folders but must be updated manually in every folder. The better option is to use 'restrict' to limit access for a specific sub-set of users, rather than copying the site into multiple folders.
- Site entries cannot be directly imported into Shared Folders.
- Form Fill Profiles cannot be shared.
- Individually shared sites cannot be added to a Shared Folder; a copy will have to be made.
- If a user is added more than once to a Shared Folder via multiple groups or individually multiple times with different permissions, the most restrictive settings take priority. If a user is added to the folder individually and via user groups, the individual permission would apply. This is important to remember when an admin is

also part of a group, as they can limit their privileges.
- A Sub-folder cannot have separate permissions from its parent Shared Folder.
- Users **MUST** generate sharing keys before being added to folders. This is done automatically by logging into the plugin at least once after creating an account. In Safari, if the plugin has not been installed yet, Sharing Keys can be created using the “Generate Sharing Keys” button in the online vault. This can only be circumvented by enabling the “Pre-Create Sharing Key” Policy. **

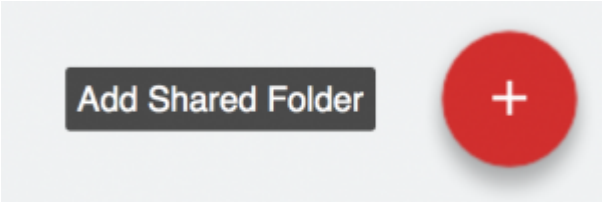
** The Pre-Create Sharing Key policy functions by creating a random password, a random sharing key, encrypting the sharing key with the password, and emailing the password to the user. This information is then flushed from our servers. Users are then required to change this password immediately on their first log in. This information is then flushed from our servers. It is less than perfectly secure as it requires you to trust us, so you are welcome to wait on creating sharing keys by having the user log into their account.

Create Shared Folders

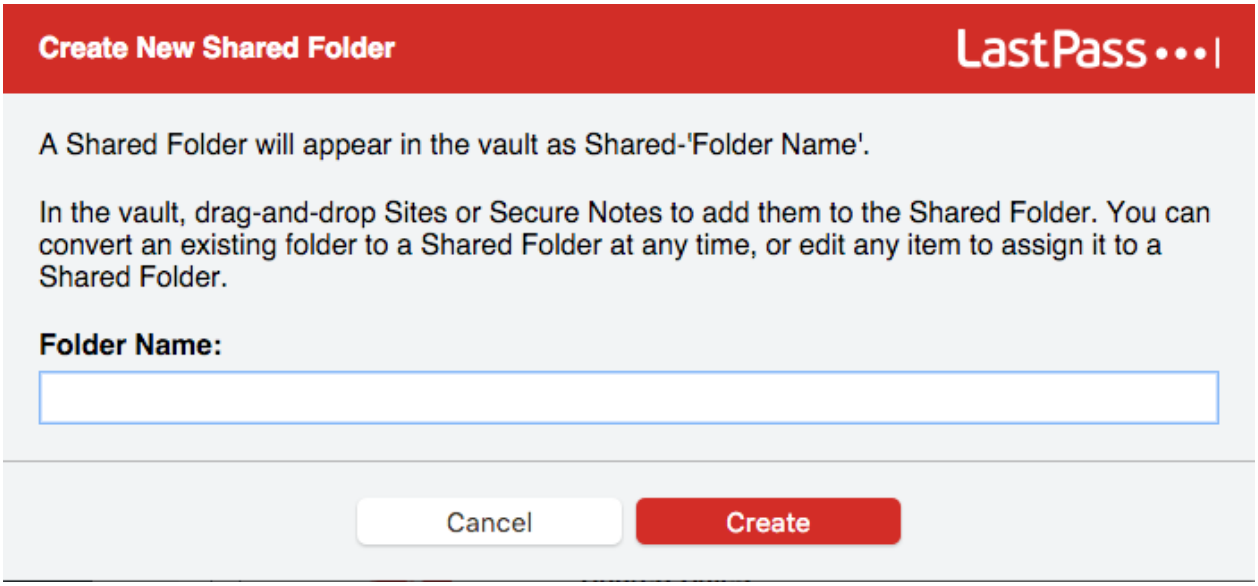
There are two main ways to create a Shared Folder: 1) Create a new one from scratch, and 2) convert an existing Folder into a Shared Folder.

- Create a Shared Folder
- Convert to a Shared Folder

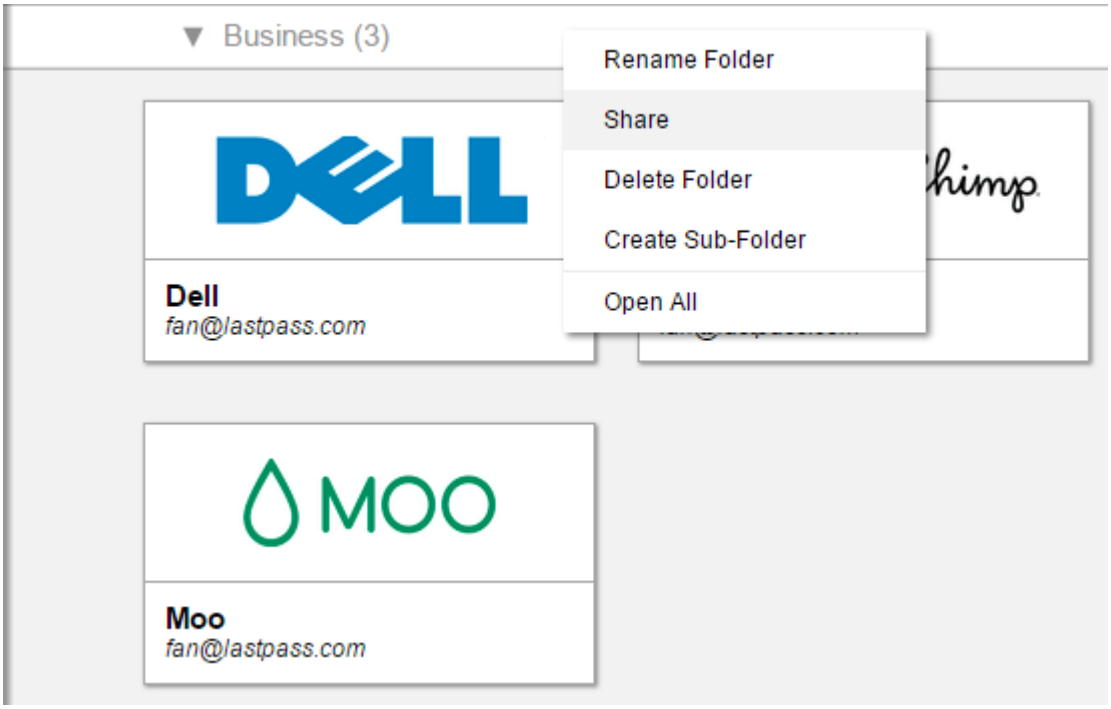
1. Navigate to the Manage Shared Folders tab in the Sharing Center.
2. Click on **Add Shared Folder**.



3. Give the Shared Folder a name and click **Create**.

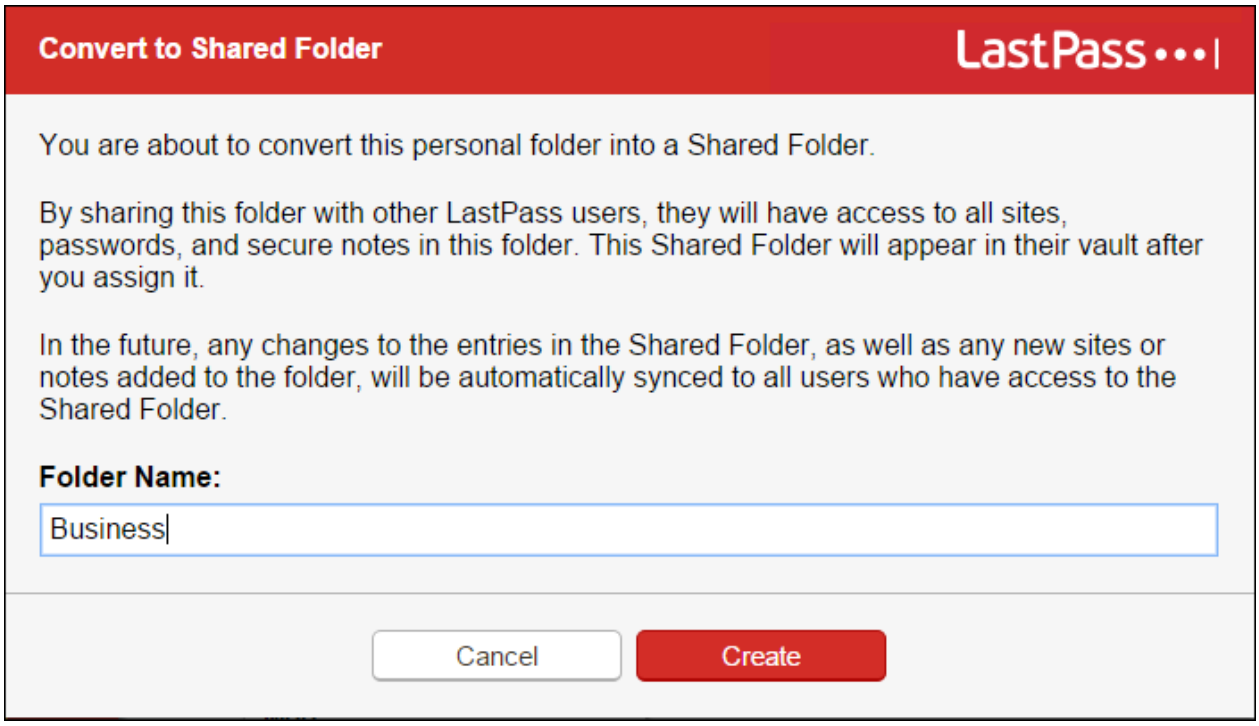


1. Right click the folder you would like to convert to bring up more options.



2. Choose **Share** in the list.
3. In the resulting window, change or confirm the name of

the Shared Folder.



4. Click **Create**.

Edit Permissions

With each user or group, you have several additional choices regarding access via the radio buttons next to each users name and when you initially add the user or group to the folder:

- **Read-only** prohibits the user from adding/removing items to/from a Shared Folder. It also prevents the user from saving any updated username, password or note information to the folder. However, we cannot block the update from transpiring at the site level. This option could, therefore, result in a lockout by the rest of the team. It is our recommendation, therefore, that you articulate a 'no update' policy outside of LastPass (if this is, in fact, your goal) and that you *do not* select 'read only'. If the user still updates the credentials, then the

change will save back to LastPass, and the event will be captured in the reports so that you are able to track it back to the owner.

- **Hide Passwords** prohibits the user from seeing the credentials. They will be able to utilize the tools via autofill or autologin, but they will be unable to see the actual credentials. *
- **Can Administer** will grant the user equal admin rights over the shared folder including: adding and removing users and restricting access to individual sites in the folder.
- **Notify User Via Email** will send the user a notification regarding their assignment to the shared folder. Please note, this is only available upon the initial addition of users to the group.

Once you have made these selections, hit ‘Share’ and the user will be added to the list of assigned users with the permissions that you designated.

Multiple Permissions

If a user is added to a Shared Folder multiple times via groups, the most restrictive permissions will apply to their access. If they are added multiple times but are added to the Shared Folder individually, the permissions established from the individual share will be reflected. Below are tables to to highlight different scenarios:

In each scenario, the user user@lastpass.com is a part of two groups: A and B.

Scenario 1:

User/User Group	Can Administer	Read-Only	Hide Password
A	Yes	No	No
B	No	Yes	

Permissions = user can edit sites, view passwords but cannot add/edit users in the Shared Folder

Scenario 2:

User/User Group	Can Administer	Read-Only	Hide Password
A	No	Yes	Yes
B	Yes	No	No

Permissions = user cannot edit sites, view passwords nor edit users in the Shared Folder.

Scenario 3:

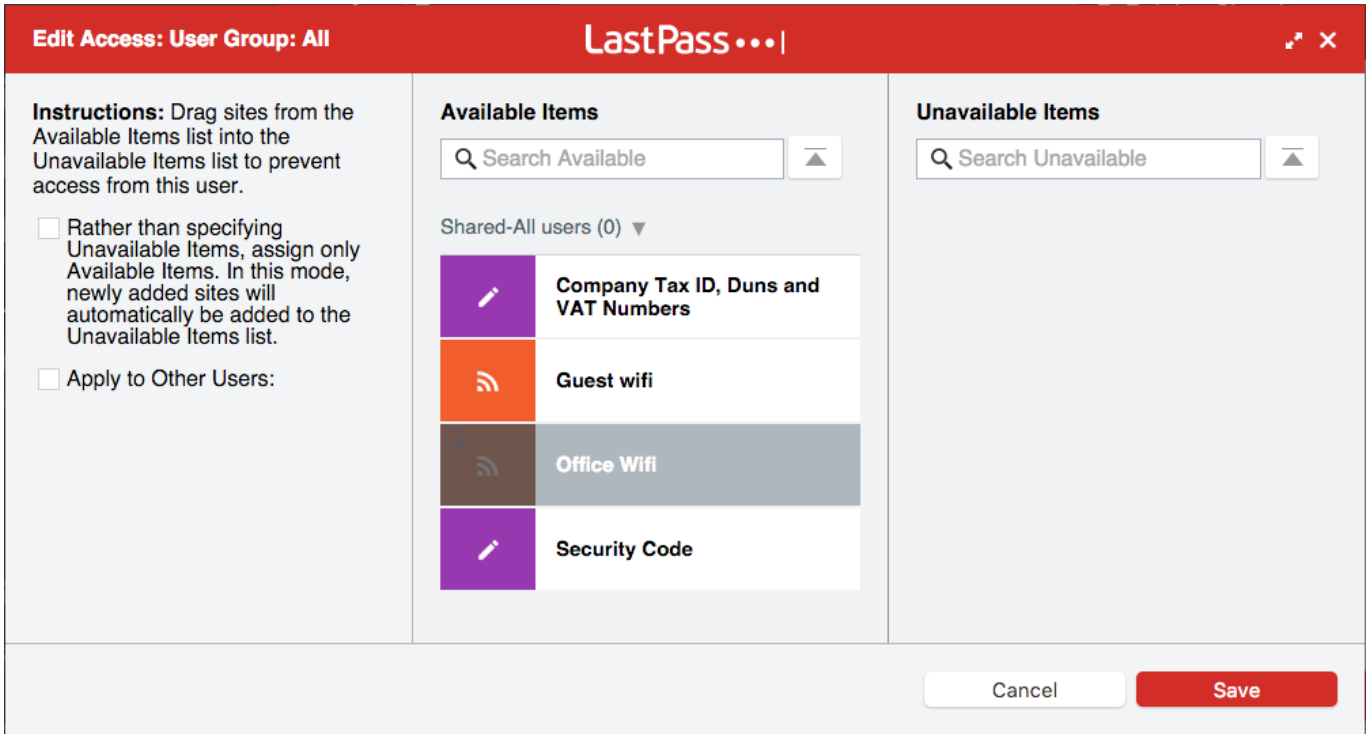
User/User Group	Can Administer	Read-Only	Hide Password
A	No	Yes	Yes
B	No	No	No
user@lastpass.com	Yes	No	

Permissions = user can edit/add users, edit sites, and view passwords. Note that in this scenario, the user's permissions ignore permissions made in groups A and B and only take into account permissions set for the user when they are added individually.

Restrict and Remove

Next to each user's name you will see the 'Restrict' and 'Remove' options.

- The **Remove** button will remove the user or groups from the shared folder. This will revoke access to the folder and any sites stored within.
- The **Restrict** feature allows you to limit access on a site-by-site, user-by-user basis. Click 'Restrict' next to the appropriate user in order to prohibit access to any number of sites within the folder. By default, all items placed in a Shared Folder will be made available to every user unless they are restricted by moving the item from column A to column B. However, on the 'Restrict' screen, the toggle below the columns will *reverse* this logic. When selected, all items in column A will be *unavailable* to the user until they are moved to column B. Many enterprises prefer this 'opt in' rather than 'opt out' approach.



Now that the folder has been created and is in your Vault, you can proceed to populate the folder with sites and Secure Notes via several methods:

- Drag and drop

- Right-click in your vault and select ‘Change Group’
- Edit site (in plugin) and select ‘Change Group’
- Add a new site and set the ‘Group’ to the Shared Folder name

Adding Users to Shared Folders

You can add users to Shared Folders using User Groups. This is a quick and easy way to add pre-made groups of users to Shared Folders. User groups are added to Shared Folders just like individuals; the groups are created in the Admin dashboard and available in the dropdown list of users when you create or edit a Shared Folder. You can set ‘Read-only’, ‘Hidden Passwords’, and ‘Can Administer’ access once for the entire group. You can also restrict what sites the group can view just like you can for an individual user. When adding groups to Shared Folders, there are a few things to keep in mind to avoid conflicts:

- If you add a user to a User Group that is assigned to a Shared Folder, they will gain access to that Shared Folder.
- If you add a user to your Enterprise via the Active Directory or LDAP sync, and the user is synced straight into a group that has already been assigned access to a Shared Folder, that user will not have access to the folder until another member of the folder logs in to LastPass. Upon this event the sharing keys are exchanged between those two user accounts, making access possible by the new user. (You must ensure that the ‘Precreate Sharing Keys’ policy is enabled in order for this to happen automatically.)
- If a user is added to a Shared Folder more than once, the most restrictive settings will take precedence. This

applies to ‘Read-only’, ‘Hidden Password’, and ‘Can Administer’ rights, as well as what restrictions are in place regarding what sites can be seen in the folder. This can also apply to other admin accounts.

- When a non-Enterprise admin creates a Shared Folder, they are able to add both individuals and groups. These non-admins do not have the ability to see who is in what group, so they should be aware who is in what user group before adding them to a Shared Folder.

Important note:

- You can share each shared folder with up to 5 users outside your enterprise with any permission except Can-Administer and they cannot manage the shared folders created in your enterprise. This is by design in attempt to protect your company data.
- Savvy end users could potentially access a hidden password if they capture it using advanced techniques during the login process such as using another password manager. LastPass recommends that you ensure that you’ve used a generated password specific to the individual site that you are sharing, and that you refrain from sharing any passwords that you are uncomfortable with the recipient obtaining. Regardless, LastPass helps facilitate the seamless update of passwords so that you can change them frequently and at a moment’s notice, without your end users even knowing that an update has taken place.

Active Directory Synced Groups and Shared Folders

You can use the LastPass Active Directory Synchronization Service to automatically provision and sync users and user groups from your Active Directory into your LastPass Enterprise. LastPass also recommends provisioning users with our simple LastPass Provisioning API.