LastPass by LogMeIn

FACT SHEET

Quick Helpdesk Guide for LastPass Business Admins

Questions are inevitable as employees use LastPass. To help you assist users, take advantage of the resources below and follow the best practices we've developed through working with our customers.

LastPass Admin Responsibilities

- Direct support to your end users
- User lock-outs and account deletion (only the User and Super Admin can reset master passwords)
- Configure Admin roles and related policies – like Help Desk Restricted Admin
- Re-inviting users whose invitations have expired
- Software installation assistance (for the LastPass browser plugins and desktop apps)
- User education and training
- Initial troubleshooting on problem/resolution, including login issues on specific URLs

Common Issues for the Helpdesk

Signing in to LastPass through the Extension

Downloading and signing in through the browser extension is the best way to use LastPass. If you have deployed LastPass and a user still does not see the extension in their browser toolbar:

- Use the download link in the browser: LastPass.com/dl
- Check that the browser is up to date
- Go to the browser's settings, open Extensions and ensure LastPass is listed AND enabled
- Check that LastPass is not hidden behind the address bar by dragging the bar left or dropping LastPass into the browser toolbar (depending on which browser you are using)
- Temporarily disable other extensions, and then try reinstalling LastPass
- Test antivirus or security software that may be blocking LastPass – ensure LastPass is trusted
- Reset the browser to default settings and/or reinstall the browser before reinstalling

Top Learning Resources

- User Guide
- LastPass Video Tutorials
- Admin Toolkit

Getting Help from LastPass

We support Admins and Helpdesk support teams with any issues requiring escalation, including technical or usability-related issues.

If the resources above can't answer a user's question, please submit a LastPass support ticket. Sign in to your LastPass account to submit the ticket, describe the issue in detail (including URLs, browser, OS) and add usernames of any impacted users.

Using LastPass Offline

Though LastPass is a cloud-based solution, offline access is available through the browser extension and the mobile apps. The user needs to sign in at least once on a device to create a locally cached, encrypted copy of the vault. When they sign in without a connection, the app will default to offline mode and the user can sign in to view the offline copy of the vault. Note that offline access can be disabled by policy, though we do not recommend this due to user inconvenience.

Trouble Saving or Filling a Site Login

- Check that the LastPass extension in the browser toolbar is red (black in Safari)
- Go to the LastPass Icon > Preferences > General and ensure Automatically Fill Login Information is enabled
- Right-click on the site's login fields and look at the context menu information to check whether the website is built with Flash or Silverlight – LastPass doesn't support these sites
- If the login is already stored in LastPass, try deleting and re-saving the site to LastPass
- Check if the URL is in the LastPass Icon > My LastPass Vault > Settings > Never URLs
- Force-capture the login fields with the Save All Entered Data feature

Forgotten Master Password

LastPass is never sent the user's Master Password, so we can't send it to the user or the Admin or reset it. The Master Password must be reset by the user or an Admin using the available recovery options. Before deploying LastPass, we strongly recommend enabling the Super Admin Master Password Reset Policy, which allows Admins to reset a user's Master Password.

Here are steps users can take when they're having trouble with their Master Password:

- If signing in to the website at LastPass.com works, re-install the extension
- Type the Master Password in a document and copy-paste to ensure no typos
- Request the password hint at LastPass.com/forgot.php to help recall the Master Password
- Visit LastPass.com/recover.php to activate your local One Time Password. Try account recovery on all browsers and on all devices where the LastPass extension has been used, including the mobile apps
- Ask the Admin to activate Super Admin Account Recovery. The Admin needs to communicate the new temporary Master Password to the user – LastPass does not send the Master Password to the user. The Admin can request that the user be prompted to change their Master Password when they next sign in.

Updating the Master Password

LastPass cannot change the username, email address or Master Password for a user – it must be done by signing in to the user's account.

1. Sign in to LastPass via the browser extension or at LastPass.com
2. In the Account Settings, select Change Master Password and save the changes when done
3. Admins can also require by policy that the Master Password be updated on a regular basis. The user will automatically be prompted to create a new Master Password when signing in.

Resetting Multifactor Authentication (MFA)

If a user does not have access to their MFA device, the Admin can temporarily disable it from the Admin dashboard.

1. From the Admin dashboard, click through to the Users tab, locate the user in question and click their name to open the right-hand panel
2. Click the ellipsis at the top right and select the Disable Multifactor Authentication option
3. The user will be able to sign in without MFA and will be prompted to set it up again

Encouraging Strong Password Hygiene

One of the primary benefits of LastPass is the ability to create new, strong and unique passwords. It's important to educate users on how to use the password generator and how to evaluate their overall password security with the Security Challenge.

Users can find the Security Challenge under Options. They will need to enter their Master Password to view results:

- The Security Score shows overall security of all passwords in the vault (0 – 100)
- LastPass Standing ranks the user against all other LastPass users
- Master Password Score ranks strength of the Master Password (0 – 100)
- The report shows all duplicate, compromised, weak and old passwords
- Users can then launch sites with poor passwords and use the password generator to replace those passwords

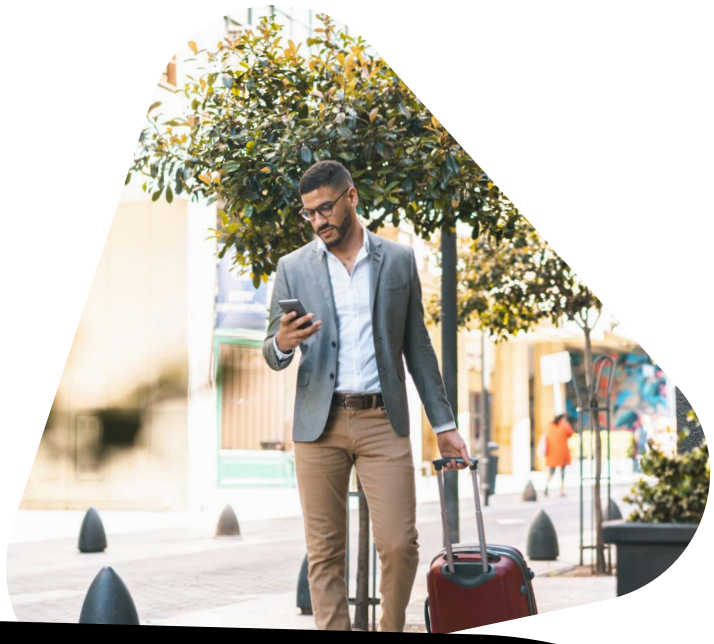
Personal Passwords and Linking Personal Accounts

Because Admins can disable or delete a user's account at any time, and because items stored in the work vault appear in reporting logs, we recommend that a user create a separate, personal LastPass account for all personal passwords.

Using the Link Personal Account option, the user can link their personal vault to their work vault so they can securely access both vaults while at work. However, the personal vault remains private, and the contents remain hidden from the Admin. Admins can enable the policy to make the personal vault Read Only if they want to ensure that no work items accidentally end up in the personal vault.

More Information about Key LastPass Features

- Sharing Center
- Mobile apps for iOS and Android
- MFA



Common Employee Objections

What's the value of LastPass?
LastPass securely stores all of your passwords and automatically signs you in to your accounts. LastPass also fills out shipping and billing forms, generates unique passwords and saves you time overall while improving security for you and your organization.

How will I get access to LastPass?
You will receive a welcome email from LastPass with next steps on creating your account and completing setup.

What if I already use LastPass?
We welcome creating a separate, personal LastPass account, so only work credentials are stored in your work account. You can link the two vaults together for easy access to both while keeping your personal account separate and private.

What if I use a different password manager?
Unless the company will allow employees to choose their password manager, we recommend Admins make it clear why LastPass was chosen and how it is used. LastPass supports importing from the most popular password managers.

What happens if I get compromised?
LastPass performs daily checks to see if LastPass account email addresses are compromised on the dark web. If a match is found, an email notification is sent to the LastPass user notifying them of the domain that was breached and the potential risk. Users can then run the LastPass Security Challenge to check for reuse of the same password and generate new passwords for all affected accounts.

Get in Touch **Contact us to learn more about LastPass Business features and tools.**