Using LastPass Enterprise

# Using LastPass Enterprise

## What is LastPass?

LastPass is an online password management tool that we make available to you to help you create, store and share passwords. Using it means you no longer need to remember dozens of passwords, just a single primary password. It keeps all your website logins protected, helps with creating new 'strong' passwords and password sharing when required.

LastPass is available as a browser extension for popular browsers and as well as a full software suite (for use outside of browsers) for Microsoft Windows and Apple macOS.

LastPass will securely save your credentials in your own LastPass 'Vault' and then offer to autofill those credentials the next time you need them.

The Ministry of Justice (MoJ) has the Enterprise tier of LastPass.

### Who should use it?

MoJ LastPass accounts can be requested by anyone in MoJ Digital & Technology.

At the moment, rollout is limited to technical service/operation teams but we're working on license funding to make it available to everyone in D&T.

## How to get it

Email [lastpass-admins@digital.justice.gov.uk](mailto:lastpass-admins@digital.justice.gov.uk) to request access.

Make sure you include in the email:

* which team you're in
* your role in your team / why you need access
* if there were any credentials within Rattic that you need access to based on this [shared spreadsheet of old Rattic credentials](https://docs.google.com/spreadsheets/d/1xkjXApSI1yw4gSuE9-izOBjvD5MK895wt1GJ9unQdU8/edit?usp=sharing)

### What it can be used for

LastPass can be used for storing usernames and passwords that are specific to you (for example, your MoJ Google account details).

LastPass can also be used for sharing passwords within a team when individual named accounts cannot be created in the service. A good example is running a shared Twitter account.

#### Personal use

You could use your MoJ LastPass account to store personal non-work information but as it is a work account belonging to the MoJ you may lose access if you change role and will lose access entirely if you leave the MoJ.

MoJ LastPass administrators cannot routinely access the contents of LastPass Vaults but can reset accounts to gain access if there is a good reason to do so.

### What it shouldn't be used for

LastPass should not be used for storing MoJ documents - you must use existing MoJ services such as Office 365 or Google Workspace for that.

You shouldn't use LastPass for 'secrets' that belong to systems, only credentials to be used by humans. There is separate guidance on how to handle [secrets](secrets-management.html).

## How to use it

### Getting started

You will be sent an email to your MoJ work email account inviting you to create your LastPass account. LastPass have ['getting started' guides](https://support.logmeininc.com/lastpass?articleID=1194875481) on their website.

#### Creating your primary password

You need to create a primary password - this is the only password you'll need to remember.

It must be at least 12 characters long (the longer the better).

You can choose to make it pronounceable and memorable (passphrase) such as CyberSecurityRules! or Sup3rD00p3rc0Mp3X!, as long as you're comfortable remembering it and won't need to write it down.

There are [password guidance standards](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/password-standard/) on the MoJ intranet.

Your primary password **must** be unique and you should **never** use it anywhere else (including a similar version, for example, by simply adding numbers to the end)

#### Multi-Factor Authentication

You **must** setup multi-factor authentication (MFA, sometimes known as 2FA) for your MoJ LastPass account.

LastPass has a [guide on setting up MFA](https://support.logmeininc.com/lastpass/help/enable-multifactor-authentication-lp010002).

The MoJ has an 'order of preference' for [which types of MFA to use](authentication.html):

* Hardware-based (for example, Yubikeys)
* Software-based (for example, Google Prompt on a mobile device)
* TOTP-based (the code is held by a dedicated app such as Google or LastPass Authenticator on a mobile device)
* SMS-based (a one-time code sent via SMS)

If you don't have an MoJ-issued work smartphone you may use a personal device for MFA.

### Sharing passwords

To share a password [create a 'shared folder' in the LastPass Vault](https://support.logmeininc.com/lastpass/help/manage-lastpass-teams-shared-folders-users-lp010061).

You should make sure the credentials you're sharing are only available to the people who need to access them for MoJ work. It is your responsibility to remove items or people from shared folders when access to the credential(s) is no longer required.

(You must not share your LastPass main password with anyone, even your line manager or MoJ security.)

### Using it abroad

Taking a device (such as personal smartphone) that has MoJ LastPass installed counts as travelling abroad with MoJ information.

The MoJ has existing [policies on travelling abroad on the MoJ intranet](https://intranet.justice.gov.uk/guidance/security/staff-security-and-responsibilities/travelling-abroad-business-or-personal/) which require various approvals before travel.

It may be simpler to 'log out' of the LastPass applications or uninstall/delete them before travelling outside of the UK and reinstalling when you get back.

### Keeping LastPass update to date

Like all software, it is important to keep the software up to date (sometimes known as 'patching'). LastPass software generally should self-update to the latest version by itself however make sure you approve or apply any updates if LastPass asks you to.

### Need help?

If you need help *installing* LastPass contact the relevant MoJ IT Service Desk.

If you need help using LastPass such as getting access to shared folders or resetting your primary password as you have forgotten it, contact [lastpass-admins@digital.justice.gov.uk](mailto:lastpass-admins@digital.justice.gov.uk)