

User Roles

From IT service companies to marketing agencies, businesses of all types need to ensure access to sensitive company data is secure and appropriate. With customizable, role-based permissions in LastPass, you can give users just the right level of access to do their job, and nothing more. Employees can be productive, while company data is more secure.

LastPass includes four types of roles – users, helpdesk admin, admin, and super admin – each with specific functionality so you can give appropriate levels of access to LastPass. The helpdesk admin is a customizable role, so you can choose what is appropriate for IT helpdesk staff in your organization. For example, designate the helpdesk admin role to IT team members that handle day-to-day internal support tickets on passwords, without giving them access to all of the privileged information in your LastPass Enterprise account. Or, select key team members to be admins so they can set security policies and provision new users as needed.

Overview of LastPass roles:

User

These are individual account holders – employees – who only have access to their personal vault and folders shared with them.

- Access to their own vault
- Feature usage and access limited by policies through LastPass

Helpdesk Admin

The least-privileged admin tasked with day-to-day management of LastPass and supporting employees with their IT questions.

- Resend an invitation
- Disable multifactor authentication • Require master password change • Kill a user's sessions
- Add or disable a user
- Add or remove groups

Admin

These are your IT managers and team leads that have access to all areas of the admin dashboard for ability to deploy, configure, and manage LastPass, such as user provisioning, policy setting, and more. Be sure to protect admin LastPass accounts with MFA.

All permissions of the helpdesk admin, plus:

- Access to all areas of the admin dashboard • Enable or disable policies
- Add or remove users

Super Admin

You'll likely only have one or two super admins who have the most privileged access to LastPass, particularly for crisis scenarios.

All permissions of an admin, plus:

- Master password reset on any user's vault
- Access to all shared folders across the company

Configuring a custom admin

LastPass Enterprise admins can create as many custom admin roles as needed.

1. Launch the admin dashboard from the LastPass extension, the vault, or https://lastpass.com/enterprise_home.php
2. Under “Advanced Options”, click “Roles”.
3. Designate a Name for the new role.
4. Enter a description of the new role’s purpose or permissions.
5. Use the check boxes to select which permissions should be available to the new role.
6. Click save.
7. In the Users tab, assign the role to any new users as-needed.