Introduction

The LastPass Enterprise Admin Manual is a comprehensive guide to testing, deploying, and administering LastPass Enterprise.

For businesses of all sizes, LastPass provides secure password storage and centralized admin oversight to reduce the risk of data breaches while removing employee password obstacles. With customizable policies, secure password sharing, and comprehensive user management, LastPass offers the control IT needs and the convenience users expect.

When 81% of data breaches are caused by poor credential management, addressing password security in your organization needs to be a top priority. From the CEO to your summer intern, every employee's passwords are a low-barrier, high-value target for attackers looking to find the easiest way in. With direct visibility into password strength for all employees, LastPass Enterprise gives businesses the control they need to change behavior across the business, with convenient automation for IT teams and an

experience employees will love.

Recommended by industry experts and tech enthusiasts for its security model, LastPass is used and trusted by over 33,000 businesses around the world.

LastPass Enterprise is deployed in days. It automatically 'learns' and 'remembers' usernames and passwords for virtually all online websites, cloud apps, and even Windows applications. LastPass provides universal access to resources, seamlessly synchronizing passwords across all platforms and browsers. Deployed on the desktop and in the cloud, your employees will love using the powerful, intuitive features and readily adopt LastPass for its productivity benefits. Your employees can familiarize themselves with LastPass' features by using our LastPass User Manual.

LastPass supports command line install and updates. For the automated provisioning and termination of LastPass user accounts, clients can choose between: Active Directly Sync client, Windows Login Integration, or an open API. Clients looking for less automation can simply add users manually in the Admin Dashboard and LastPass will take it from there with our automated welcome emails. If you need something custom to make deployment easier, let us know, we're here to help.

The LastPass admin dashboard allows your Systems Administrators to install and upgrade your LastPass installation, manage policies, user configurations, applications, authentication methods and user groups. It provides centralized reporting for auditing and compliance, plus automated user alerts for optimizing use of the tool. The admin dashboard is your "command central" for putting

your password security plan into action.

Convenience for employees

LastPass Enterprise balances the competing priorities of IT teams – and the employees they support. From safely storing passwords to managing employee permissions, LastPass Enterprise helps businesses of all sizes remove password obstacles and fix dangerous password behaviors.

- **Store everything in one place**. Give employees what they want: One easy place to save all their credentials and one-click login to their web services.
- **Remember one password**. Employees create and remember their master password, while LastPass remembers all the rest.
- **Let LastPass save and fill for you**. LastPass stores, fills, and creates passwords automatically, saving employees time and hassle.
- **Organize work and personal.** Log in with any password throughout the day, and sort passwords to the right place automatically.
- **Generate strong passwords**. Let LastPass create long passwords for employees, so every web service is protected by a unique, strong password.
- **Share passwords conveniently**. Eliminate shared spreadsheets with easy – and secure – password sharing that keeps everyone up to date.
- **Give universal access**. LastPass works everywhere employees do, with real-time sync for all desktops, laptops, mobile, and web.

Control for businesses

LastPass helps IT departments take back control of password security in their organization. Directory integration, user management, policies, reporting, and more – all are managed from a single admin dashboard that offers actionable insights and comprehensive controls.

- **Centralize admin control.** Centralize deployment and management of LastPass from a secure admin portal.
- **Integrate with user directories.** Automate user onboarding and removal by syncing with Microsoft Active Directory or a custom API.
- **Configure custom policies.** Customize over 100 policies to ensure employee access is appropriate and secure.
- **Automate reporting.** Build compliance and maintain accountability with detailed reporting logs that tie actions to individuals.
- **Assign group-level permissions.** Manage password security and shared passwords with groups created in your directory or LastPass.
- **Protect cloud apps.** Deploy cloud apps company-wide while employees have access to all apps and web services from one vault.
- **Add multi-factor authentication**. Protect every password in the business with additional authentication steps. LastPass Enterprise includes LastPass Authenticator and supports many other major MFA solutions.
- **Reset user accounts**. Enable the super admin policy to ensure employee data isn't lost if they leave or forget their master password.

Guidance for success

LastPass gives you the tools and guidance that you need to ensure a seamless launch, grateful employees, and a happy

boss. Our turnkey program includes a step-by-step Training Kit for the initial product intro, individual and aggregate Security Challenge scores to measure the impact of the program, and a status summary report (coupled with email templates) to identify (and easily act on) education opportunities among your users.

Our customer success managers are also available to bring best practices to your LastPass deployment for even higher adoption and faster results. Contact our team today to learn more.

Security is what we do

At every step, we've designed LastPass to protect what you store, so you can trust it with your business' sensitive data. Our security model includes:

- **SOC 2 Type 1 compliance**: This detailed review of our controls and processes is a gold standard for confirming the security and reliability of LastPass.
- **Strong data encryption**: Sensitive data is encrypted at the device level with AES-256 before syncing with TLS to protect from man-in-the-middle attacks.
- **Regular audits and pen tests**: We engage trusted, world-class, third-party security firms to conduct routine audits and testing of the LastPass service and infrastructure.
- **Bug bounty program**: Our bug bounty program incentivizes responsible disclosure and improvements to our service from top security researchers.
- **Reliable service**: LastPass operates out of multiple, geo-distributed facilities that can handle all customer traffic for redundancy.
- **Transparent incident response**: Our team reacts swiftly to reports of bugs or vulnerabilities and communicates

transparently with our community.

For more information, we've made the following resources available:

- The security and encryption overview [PDF], a short summary of how we provide a secure, reliable service that's perfect for sharing with non-IT management.
- The security white paper [PDF], a detailed review of the LastPass encryption model, service infrastructure, and product safeguards that's perfect for IT or security professionals.