

# Introduction



The LastPass Enterprise Admin Manual is a comprehensive guide to the administration of LastPass Enterprise.

- [What is LastPass Enterprise?](#)
- [Deployment](#)
- [Admin Dashboard](#)

LastPass Enterprise offers your employees and admins a single, unified experience that combines the power of SAML SSO coupled with enterprise-class password vaulting. LastPass is your first line of defense in the battle to protect your digital assets from the significant risks associated with employee password re-use and phishing.

LastPass Enterprise is deployed in days. It automatically 'Learns' and 'Remembers' usernames and passwords for virtually all online websites and Windows applications. It 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. Your employees can familiarize themselves with LastPass' features by using our [LastPass User Manual](#).

The Admin Dashboard allows your System Administrators to install and upgrade your installation, manage policies, user configurations, applications, authentication methods and user groups. It provides centralized reporting for auditing and compliance and automated user alerts for optimizing use of the tool.

## **Not Just Websites: SAML SSO**

LastPass Enterprise supports SAML SSO for all of your essential cloud-based applications. Seamlessly onboard new users with automated provisioning and termination through our SAML dashboard.

## **Education and Outreach**

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.

## **Sharing**

The sharing of login data is impossible to avoid in many cases. The problem with sharing is that you lose accountability. With LastPass Shared Folders, administrators can easily share credentials for a single website or for a group of sites while retaining the ability to tie activity back to the individual user. Password updates automatically and seamlessly propagate to all assigned users eliminating lock-out caused by version control issues.

## **Admin Access to User Accounts**

In its default state, LastPass Administrators cannot access any data stored in an employee's LastPass account. However, there are some exceptions: (1) the end user can explicitly share data with an Administrator via an individual share or a Shared Folder, or (2) the company can choose to enable either or both of the Super Admin Policies defined here [https://lastpass.com/policy\\_doc.php](https://lastpass.com/policy_doc.php) . When the Super Admin Policies are enabled, a notification is sent automatically to every LastPass Admin in the Enterprise.

## **Integration**

Already deployed SSO or Active Directory? You can use LastPass for web logins to improve productivity logging in to apps locally, or to handle apps that haven't been integrated into your SSO/Active Directory. Many implementations require minor changes for each application to specify domain or other settings that confuse users – LastPass resolves those issues.

# Deployment

LastPass supports command line install and updates. For the automated provisioning and termination of LastPass user accounts, clients can choose between: Active Directory 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.

# Synchronization

A Web 2.0 cloud based approach allows a mobile workforce seamless access to their accounts on any computer or mobile device from any location.

# Policies

Enforce site-wide policies on password strength, security features and password expiration.

# Administration

Employee accounts can be instantly disabled when employees leave the organization.

## Reporting

Administrators can view historical data and can audit employee logins and accesses.

## Authentication

Multifactor authentication offering increased security.

## Security & Privacy Is Our Priority

We've taken every step we can think of to ensure your security and privacy. Using an evolved host-proof hosted solution, LastPass employs localized, government-level encryption (256-bit AES implemented in C++ and JavaScript) and local one-way salted hashes to give you complete security with the go-anywhere convenience of syncing through the cloud. All encrypting and decrypting happens on your computer – no one at LastPass can ever access your sensitive corporate data. The LastPass™ [Security Challenge](#) also allows your users to identify weak account data and provides suggestions for significantly improving online security.