LastPass •••|

IMPLEMENTATION GUIDE

What is the LastPass MSP Solution?

The LastPass MSP solution provides partners with the ability to sell, manage, and support LastPass password management, including single sign-on, and/or multifactor authentication solutions in a multi-tenant environment. With LastPass, MSPs can manage their customers' LastPass accounts and perform tasks, such as adding and removing users, configuring policies, creating groups and shared folders, setting up single sign-on and multifactor authentication, and much more.

Multi-Tenancy

With the LastPass MSP solution, LastPass admins of master accounts (i.e., MSP technicians) can manage multiple independent tenants or company accounts for LastPass all from one master account.

Managed Companies have all the features and functionality available to a LastPass account, including various multifactor authentication options, directory integrations, federated login, 100+ customizable policies, single sign-on capabilities, and much more.

Master Account
MSP Technician

- **Managed Company 01**
  MSP Technician
- **Managed Company 02**
  Local Administrator
- ...
- **Managed Company N**
  Local Administrator

Setting up your MSP

Setting up your own Admin Console

Please review our administrator training resources to learn how to set up your MSP Admin Console successfully. Please find these training resources here.

Review the Admin Console

First, let's dive into the LastPass admin experience to see how simple it is to manage access.

Admins can launch the admin console from their LastPass account at any time. The admin console is a web-based portal that provides centralized oversight of all employee LastPass accounts and gives the company control of employee password behavior. This allows admins to eliminate password reuse and to enforce a strong password policy throughout the organization.

Adding MSP Users to LastPass

MSP partners are encouraged to roll out LastPass across their organizations.

LastPass accounts are either "users" or "admins." Users include anyone who has been given a LastPass account. Admins are users with special privileges and access to the admin dashboard.

MSP technicians, who will need to access each managed company instance for administrative purposes, must be added as LastPass admins of the master account (MSP technicians). As a LastPass admin of the master account, they will be able to access and perform key tasks on each managed company instance, such as adding users, setting policies, managing groups, adding a single sign-on application, etc.

All LastPass admins in the master account will also be admins for all the managed companies.

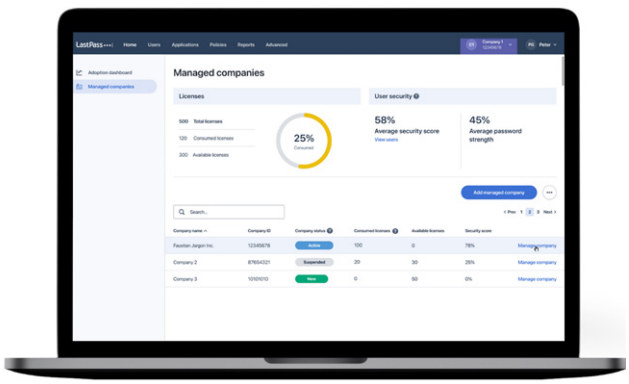
When adding technicians please refer to these resources:

Add technicians to be LastPass users of the master account by following the detailed instructions here.

Assign roles to technicians LastPass allows MSPs to give different levels of admin permissions to their technicians. Learn more about these roles here.

Grant LastPass admin access to all technicians to enable them to access the Admin Console and the managed companies with their LastPass credentials. Please find detailed instructions here.

LastPass offers Internal Use licenses for our MSP partners. These licenses must be used in the Master Account of the MSP.

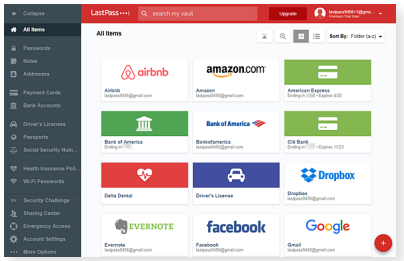


MSPs can manage their customers on the 'Managed Companies' tab in their Admin Console.

Key LastPass Features

New to LastPass?

Visit our end user training site to receive an overview of key features in more depth. Visit here.



LastPass Vault

The LastPass Vault is where all your passwords, Notes, and items are stored. They are easily accessible in the lefthand navigation. Your Vault is a locally hosted file, so you can access your stored data securely and quickly. You can organize your Vault view by folders, move or manage items in bulk, and manage your user account.

Learn more about the LastPass Vault here.

Dark-Web Monitoring

The dark-web monitoring feature evaluates all of your users' stored email addresses in their Vault items and alerts them immediately – via email notification and within the Security Dashboard – if any of their email addresses have been found in the database of breached credentials. View the Security Dashboard on the left-hand column of your LastPass vault.

Learn more about this feature here.

Browser Extension

LastPass functions primarily by virtue of the browser extensions, which you'll see in the browser toolbar. Through a single download, you'll have the LastPass extension installed on all browsers detected on the device, including IE, Firefox, Chrome, Safari, and Opera. LastPass supports Mac, Windows, and Linux, and has apps for Android, iOS, and Windows Phone. We recommend imaging the software out to all your desktops, or you can let end users download it themselves. You also decide how user accounts will be created.

Most users will download the software to their frequently used devices and download phone apps as well so they can access their data from anywhere.

If they ever find themselves needing LastPass access from a device that doesn't have LastPass installed, they can log in at LastPass.com. The LastPass account is synced automatically wherever the user logs in. We recommend adding the LastPass browser extension to all users' browsers. The LastPass browser extension is the principle mechanism for capturing, generating, and filling passwords.

Please read the detailed instructions here.

Adding Users

Administrators needn't install any new directory connector software on their on-premise Active Directory, which is a frequent comment from existing LastPass Administrators. An on prem AD connector, Azure, Okta, OneLogin, provisioning API's, and federated login integrations also sync with the LastPass as well. Again, emphasizing simplicity of leveraging existing systems and saving time to ramp-up.

Learn more about this option here.

Policies

As you prepare to deploy LastPass, in the Settings tab and then Policies you'll want to review our list of over 100 security policies that you can take advantage of to create and enforce the perfect security environment your company requires - high, medium, or low. For example, by default, LastPass is accessible anywhere, but you may want to restrict access to a set of work-related IP addresses. Or, maybe, you want to restrict access to a subset of employees but let another set of users have access from any location. In that case, you can apply the policy to an inclusive or exclusive list of users.

Here are a few questions that MSPs should discuss with their customers prior to configuring policies:

- Are you going to have to sign in or sign out to access restrictions?
- Are you going to enforce strong master passwords to log into LastPass, or will federate logins require this through your active directory?
- Are you requiring the use of multifactor authentication?
- Are you allowing the use of personal linked accounts?
- Are you allowing access on mobile devices?
- Are you allowing password sharing in LastPass?
- Are you implementing SAML Single Sign-On with LastPass?

To add a policy, just click the Add Policy button. In the dropdown list, you see all the policies, and you can customize them. For example, with the Do Not Allow Master Password Reuse, you select the policy, then enter the Value below. You can also deploy these policies to an inclusive or exclusive list of users. If you click this link, you can see a complete list of all policies with descriptions.

For more information on configuring policies, visit here.

Shared Folders

LastPass also excels at password sharing among teams. LastPass allows you to share logins and notes seamlessly and securely among groups without losing accountability.

From the left-hand menu in the vault that you'll see, we can choose to go to the "Sharing Center," where we can create a Folder and assign it to specific team members. Any passwords or notes we then add to that folder will be synced to those users automatically, with the appropriate permissions set by an admin.

Multiple people can access these single accounts, and by only sharing these passwords through LastPass, you, as an admin, can look up who last accessed a shared account.

You can see some of these folders have read-only access, while others have admin rights. Through the edit link, we can add/remove users or groups to the folder. We can also select whether to give them Read-Only, Hide, or make them an Admin.

Changes to the shared folder are synchronized automatically to everyone with whom the folder has been shared.

Learn how to create a shared folder here.

Groups

Groups can be utilized to assign policies and/or shared folders to a designated set of users all at once within your LastPass account. From the left-hand menu of the Admin Console, select Groups. You can create user groups manually (or automatically sync groups if you choose to set up the LastPass Active Directory Connector), as well as edit or delete groups, manage users within a group, and view group details.

Learn to create groups here.

Email Notifications

LastPass admins can add and manage email notifications to keep users apprised of critical user statuses, including account activation, lack of best practices being used (warranting additional education or training), and much more. Navigate to the Settings tab, then select Email Notifications to configure.

Learn about email notification options here.

Reports

What's your stance on auditing; the more the better? LastPass advanced reporting includes audits for user activity, user status, policies setting changes, access requests, security reports, and shared folder reports across both password management and single sign-on.

LastPass reporting helps you safeguard your organization's data and build compliance. Available in the password management Admin Console, the Reports feature offers admins an audit trail that can also be exported and shared with key stakeholders as needed. There are four types of Reports: the most valuable for auditing are User and Admin activity, whereas Security and Login Reports are excellent for tracking adoption and usage.

From the password management dashboard, please select Reports from the left menu, where the User Activity tab provides a comprehensive log of every login event, passwords or username update, attempted or completed Form Fills, and deleted Sites by your LastPass users. The logs include attempted (e.g., failed login attempts) and successful actions. The reports can be filtered by date range or user and can be exported to Excel for backup or sharing with others.

Learn about the different types of reports here.

Federation

Once a LastPass admin has set up federated login for an organization, new users are provisioned with a LastPass account that allows them to log into LastPass with their existing Active Directory account (AD FS, Azure AD, or Okta) – no separate Master Password required. This streamlines user access to LastPass, without requiring an additional password.

Learn more here.

Families as a Benefit

MSPs can provide their LastPass users with a complimentary LastPass Families account, which is a personal account that includes five (5) additional licenses that can be granted to anyone – family, friends, etc.– so they can also keep their digital lives secure.

Learn more here.

PSA Integrations

LastPass integrates with ConnectWise Manage and Datto Autotask to streamline provisioning and billing of clients.

Learn how to set-up the ConnectWise Manage integration here and the Datto Autotask integration here.

Single Sign-On

LastPass MSPs can access the single sign-on (SSO) Admin Console to set up a SAML-based login integration with apps and services for their users. Once set up, LastPass users can log into these apps using the same credentials they use to access their work systems. This allows users to sign into SSO apps using the same credentials that they use for LastPass.

Admins can choose from over 1,200 web app integrations. To configure a new SSO application, simply click on "Applications" in the SSO Admin Console, and then select "Add Application." Admins can follow our detailed step-by-step guides to configure each app. Once configured, the admin can assign users to the SSO app. Click on Save, locate the newly created App, click on the person icon, and assign users or groups for SSO. Finally, hit Save one last time. You'll notice a notification feed appearing on the lower-right, and a specific item notifying a successfully saved integration. Each user will see the app in their "Cloud Apps" Launchpad as soon as it is configured to their account.

PRO TIP: Make sure to assign the app to yourself for testing.

Learn how to add Single Sign-On apps here.

Multifactor Authentication

LastPass supports multifactor authentication for the LastPass vault, cloud and legacy apps, VPN, workstation, and identity providers. LastPass MFA is an adaptive authentication solution that supports various forms of authentication, including biometrics (face or fingerprint recognition), as well as pattern matching.

MFA policies allow admins to restrict access based on location. The admin can define red and green zones for both geo-location and IP address. The admin can then create policies using a combination of location and time. The policy can be configured at the app level or organizational level. The policy can also be permanent or temporary.

Learn how to set up LastPass MFA here.

Security

At every step, we've designed LastPass to protect what you store, so you can trust it with your sensitive data.

We keep your information safe with:

A proven security model, setting the standard for transparency and best practices

Local encryption, so that sensitive information is obscured before it's synced to LastPass

Powerful security features to give you tools to protect against threats and attacks

Learn more about our security standards here.

Setting up your Customer

Adding a Managed Company

When an MSP customer is ready to deploy LastPass, the first step is to add them as a Managed Company below the MSP. To add a Managed Company, follow these steps:

1. Click the active LastPass icon in your browser extension. Go to **Admin Console > Managed Companies > Add Managed Company.**
2. Enter the name of the company, and select how many licenses to allocate to the company.

   Note: When you first add a Managed Company, you must add at least 11 licenses to create the company. You will not be charged for those 11 licenses, only the licenses that you assign to a user.
3. Click **Save**. The company is added.

Learn more about Managed Companies here.

Develop a Communication Plan

We recommend aligning with your customer on the communication plan, as it is very important to build awareness of LastPass. Consider hanging posters, distributing flyers, or sending a series of emails alerting employees of this upcoming change. We recommend including an executive sponsor email in this step.

Resources

Email Templates

- Executive Welcome

Posters/Flyers

- Why LastPass Flyer
- LastPass Getting Started Flyer

Run User Trainings

LastPass offers several resources to aid with end-user training:

- LastPass End User Training Script: Use this script to train customers on LastPass.
- LastPass Self-Service Training Platform: Invite customers to view a live end-user training, a recorded training, or our self-paced learning. In each swession, we'll cover the main features and functionalities of LastPass.
- LastPass 101 Videos: These videos demonstrate LastPass's functionality.

Provision Users

We recommend rolling out LastPass initially to a cross section of employees and technical experiences to start. Be sure to conduct end-user training with this group.

For detailed instructions on how to add users, visit here.

Once you've successfully rolled out LastPass to your initial users, it is time to roll out LastPass to the rest of the organization.

Driving Adoption

Consider driving LastPass adoption through these key features:

- **Assign an Executive Sponsor.** We recommend selecting a C or V-level Executive to champion LastPass internally and request regular reports on progress of the roll out.
- **Make LastPass mandatory.** Consider creating a company policy that all employees are mandated to use LastPass. Deploy a user training portal to track employee progress.
- **Integrate with your user directory.** By integrating with your existing directory, every employee can be automatically onboarded to LastPass when they join the company, as well as offboarded when they leave. You'll simplify day-to-day management for admins while spreading usage in the organization.
- **Hardwire LastPass.** Consider pre-loading user vaults for new hires with passwords they need to do their work. When they see that the vault is set up for them and that LastPass starts filling their passwords automatically, they'll instantly see the value of the service.
- **Formalize a communication strategy.** Develop a plan for raising awareness of LastPass and training employees to use the tool. See the Communication Plan tab.
- **Invest in employee training.** Educate employees on why a password management tool is necessary and the importance of cybersecurity. Highlight how the employee will benefit. LastPass will protect the individual as an employee and as a consumer. Use metrics and statistics to communicate the value (80% of breaches are password related, and the average cost of a breach is nearly $4 million.).
- **Go mobile.** 56% of web traffic comes from a mobile device. The LastPass mobile app is not only easy to use but also increases adoption. Encourage mobile use and train on the mobile product experience.
- **Create and report on success metrics.** How can you measure success in LastPass? What metrics can LastPass help you track? What is important to you?