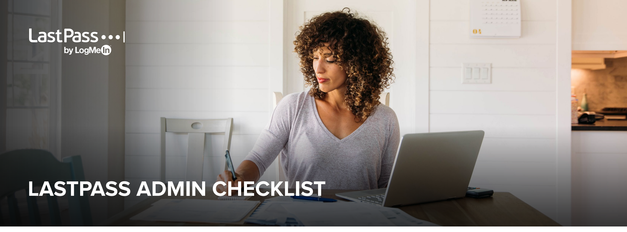

LASTPASS ADMIN CHECKLIST

What are your goals with LastPass?

- [ ] Centralize management of passwords to increase security hygiene within the organization
- [ ] Limit password resets to save the IT team time
- [ ] Increase user sign-in efficiency to improve productivity
- [ ] Improve credential sharing methods within the organization

Timeline

- [ ] What is your implementation go-live date?
  - Recommendation to deploy is 60 days
- [ ] What is your goal adoption rate at 60 days, 90 days, etc.?
  - Example: X% of users, implemented by X date

Key Considerations

- [ ] Are you making LastPass mandatory for use among employees?
  - We find making LastPass mandatory directly increases adoption rate and overall security within the organization
- [ ] Are you moving from an existing Password Manager, Single Sign-On (SSO), or Multi-Factor Authentication (MFA) provider?

Getting Started

Step 1: Add and Train Admins

- [ ] Attend Admin Training
  - Understand End User vs. Admin
- [ ] Identify and Provision LastPass Stakeholders
  - Elevate privileges – Admins
- [ ] Create a Project Plan/ Timeline
  - Review Deployment and Adoption Plan spreadsheet
  - Admin Toolkit

Stakeholders Types

Product Integration: Team responsible for configuring LastPass Admin console, reviewing security policies, setting up Automated Provisioning/ Federation, and deploying software licenses to organization.

Internal communication: Team responsible for messaging, letting employees know LastPass is coming, and where to get assistance should they need it.

Pilot Group: Consider creating a small testing group that includes technical AND non-technical people from multiple departments across your organization to create a more accurate picture of user experience and „super users" that will be able to assist other users during the full roll-out.

Step 2: Admin Console/ Technical configuration

- [ ] Create Software Installation package
- [ ] Configure Policies
  - Review our Recommended Policies
- [ ] Configure Provisioning (Optional, consider provisioning options on the right)
  - Create Groups
  - Use directory integrations for automated provisioning (optional)
- [ ] User Sign In (Federation recommended)
  - Federate logins with ADFS
  - Federate logins with Microsoft Azure
  - Federate logins with Okta

Software Installation

Manual Installation: Users download the LastPass extension themselves
Automated: Use a silent .msi installer to auto-deploy to your users using GPO, SCCM, JAMF, etc.

Provisioning

Do you plan to manually provision LastPass users, or leverage existing infrastructure, such as Active Directories to automate your provisioning?

Manual Provisioning
- Pros: Fast, easy, effortless deployment
- Cons: Difficult to scale or manage large user base

Automated Provisioning (preferred method)
Connect LastPass with your Active Directory to automate provisioning and de-provisioning of LastPass users.
- Pros:
  - Easy to scale and maintain
  - Automated, seamless user deployment and licenses provisioning /deprovisioning in conjunction with your Active Directory
- Cons:
  - More technical configuration than manual deployment
  - Must be using AD, Azure, Okta, or OneLogin for Identity Provider

User Sign In

With Federation (preferred method)
Users use their AD credentials to sign into LastPass, as opposed to unique password for LastPass. This should be decided in project planning, as it impacts baseline implementation and configuration settings.
- Pros:
  - Users can use familiar password/ sign in process to access LastPass
  - Results in higher adoption
  - Can leverage existing password and MFA policies and apply them to LastPass
- Cons:
  - Technical configuration
  - Some limitations in LastPass once enabled

Without Federation
- Pros:
  - Less technical
  - No product limitations
- Cons:
  - Lowers overall adoption rate
  - Users use a separate Master Password to log in to LastPass

Step 3: Pre-load User Vaults/ Applications

- [ ] Setup Single-Sign On (SSO) Applications
  - Add SSO Applications
  - Manage App Setting and Users
- [ ] Push Password Apps to LastPass Users

Single Sign On (SSO)

LastPass SSO apps allow users to sign in to LastPass and launch any of their web apps without having to re-enter their credentials for those apps. This reduces the number of credentials that end users need to manage in order to access their cloud applications and provides a simplified provisioning and deprovisioning experience for LastPass admins.
- SSO Admin Toolkit
- Single Sign-On App Catalog – Explore our catalog of over 1,200 pre-integrated SSO applications for which LastPass provides access

Password Applications
LastPass admins can place password apps directly in a user's Vault. This can be used to pre-populate a site in a user's Vault so that it is available when the user first logs in.

Step 4: Launch to Pilot Group

- [ ] Goals for Pilot Group:
  - Feedback on account activation/installation process
  - Feedback on training experience
  - Feedback on basic product
  - Usage day-day (adding passwords, sharing, generating passwords, etc.)
  - Optimize deployment plan based upon feedback

Step 5: Publish Training and Send Communication

- [ ] Formalize welcome/ communication materials (emails, blogs, internal messaging, events, etc.)
  - Pre-deployment communication to let users know LastPass is coming
  - Post-deployment communication to let users know how to get started and how to find help should they need it
- [ ] Create internal repository of resources /support information
  - Where can users go to find help, answer questions?
  - Encourage users to train themselves

Step 6: Deploy to Organization

- [ ] Based upon the size of your organization, consider deploying by department or moving forward with a companywide rollout.
- [ ] Consider the timing of the deployment
  - Ex: Friday afternoons tends to decrease sign up/ adoption rate

Step 7: Ongoing Management

- [ ] Run weekly Reports to measure adoption and usage
- [ ] Send milestone communication emails every 30 days with progress and training resources

Reports

Ongoing Adoption:
- Consider bi-weekly or monthly online office hours for ongoing support
- Incorporate LastPass into your employee onboarding programs

Helpful resources

For Admins:
- Admin toolkit
- Adoption and Deployment worksheet
- Recommended Policies
- Advanced Training
- Technical whitepaper
- Reporting

For End Users:
- Embark Training Portal
- End User Desk Reference guide
- End User Toolkit
- Password Generating
- Sharing
- Import

General resources:
- Support website

Features to Consider:

LastPass MFA
The LastPass MFA app is an adaptive authentication solution that supports various forms of authentication, including biometrics (face or fingerprint recognition), as well as pattern matching. You can use this authenticator to verify your login for your LastPass Vault (if you have one) and/or websites that you sign in to and use daily.

- Adaptive authentication
- Biometric authentication factors
- Contextual authentication policies
- Centralized, granular control
- Flexible integrations
- In-depth reporting
- Security Dashboard

Resources:
- Set Up Your LastPass Enterprise to Use the LastPass MFA app
- LastPass MFA app Activation (User)

01.07.2021/LM1813/PDF