LastPass Business Recommended Policies Guide

Introduction

This document will help guide you through common scenarios and selecting policies to enable on your LastPass Business account. We will not cover all policies available to you in LastPass Business here. To review a comprehensive list of policies in product, please visit your **Admin Console** > **Policies**.

To review a complete list of all policy best practice considerations and recommendations please use the *General Policies* tab in the LastPass Deployment and Adoption Plan Guide.

When configuring policies consider security and usability when determining how you want users to interactive with LastPass. Here are the recommended policy best practices topics covered in this guide:

1. Default Policies
2. How can I manage administrative functions?
3. How can I manage the master password?
4. How can I protect the data my organization is sharing via LastPass?
5. How can I protect my end user accounts from an internal or external attacker?
6. How can I ensure mobile access is protected?
7. How can I help adoption of LastPass within my organization?
8. How can I increase the amount of reporting information available?

---

1. Default Policies

As a best practice we recommend you keep all default policies enabled with one exception highlighted and a couple other recommended customizations suggested below.

Policy	Description	Considerations
Remember Master Password	Permit users to allow their LastPass browser extension to remember their master password. When enabled, users have the option to 'Remember master password' upon login to LastPass.	As a best practice we recommend you delete/disable this policy. Remembering the password weakens the security for that user.
Minimum character sets in master password	Force users to create a master password that includes at least this many different character sets. Once enabled, users with a master password using too few character sets are prompted to change their master password. Value: 1 (default), 2, 3, or 4 For example: enter value of 3 to force master passwords with at least one character from any three of the four character sets: uppercase, lowercase, numeric, and special (!#$,^ and similar).	As a best practice we recommend you enable this policy and follow your established AD password policy for password complexity.
Prohibit reuse of old master passwords	Prohibit users from re-using recent master passwords.	As a best practice we recommend increasing the value from 1 to at least 5. Ideally, you want users to always use a new one, not recycle a few.

	Value: The number of historical passwords to check against.	
Apply parent account MFA policy	Apply the parent account's multifactor authentication requirements to linked personal accounts.	If you don't want your multi-factor authentication to "impose" upon an employee's linked personal LastPass account, you can disable this policy.
Notify admins upon user lockout	Send an email to the specified addresses when an account is temporarily locked out due to failed login attempts. Value: Enter email addresses, separated by commas.	We recommend keeping this policy enabled but to review the value (i.e. the email address to which user lockouts are sent). The default value is the admin who created the account so you may want to edit this value. If this policy is deleted/disabled, there is no way to unlock a user before the defined lockout period is over.

2. How can I manage administrative functions?

The policies below are recommended to add enhanced oversight and control for your account administrators.

Permit super admins to reset master passwords	Allow selected admins to reset the master password of any user in your business. Click 'Edit Users' to add admins. Users must log in to the browser extension at least once to capture the encryption key that makes admin reset possible. Security tip: Always protect accounts with 'super admin' rights with multifactor authentication. While not recommended, you can specify multiple admins by separating their usernames by comma, space, or semicolon. To disable the ability to add or change this policy, contact LastPass.	As a best practice we always recommended enabling this policy as soon as possible. This policy requires set-up before elevated password reset admin access is available. Super Admins cannot reset a user's master password if the user hasn't signed in since enabling this policy. To understand how this policy works review support article: **https://support.logmeininc.com/lastpass/help/reset-a-users-master-password-super-admin-lp010038**
Permit super admins to access shared folders	Invisibly share all shared folders in your business with authorized admins. Click 'Edit Users' to add admins. To disable the ability to add or change this policy, contact LastPass. Shared folders that existed prior to setting this policy are assigned the next time a user with 'Can Administer' access to that folder logs back in to LastPass.	As a best practice we always recommended enabling this policy. This policy requires set-up before elevated admin of all shared folder access is available.
Notify admins upon account recovery	Send an email to the specified addresses when the account recovery option is used. Value: Enter 1 to send when end user requests account recovery. Enter 2 to send when account recovery is successfully completed, and the user re-sets their master password. Enter 1,2 for both options. For example: 1,2,admin@acme.com,admin2@acme.com	As a best practice we recommended enabling this policy.

Restrict domain for LastPass username	Only allow users to use an email from an approved domain when creating a username for their LastPass account. No accounts can be created or updated using a username outside the approved domains. Value: Enter the allowed domains, separated by commas. For example: lastpass.com,xmarks.com	As a best practice we recommend enabling this policy and entering your approved domain values. When enabled this policy prevents a user from changing their company account username (email address) to any other non-AD username.

3. How can I manage the Master Password?

Review the policies listed below to determine if they can help you structure how your employees keep their Master Password secure.

Require Master Password Change	Force users to change their master password after this many days. Value: The number of days between master password resets. This is recommended to be set at 90 days if you do not require multifactor usage, and 365 days if you require multifactor. To have a different limit for multifactor, specify a second number, separated by a comma (For example: 90,365).	As a best practice we recommend you follow your established password security guidelines. The National Institute of Standards and Technology (NIST) recommends the removal of periodic password changes and emphasizes the importance of password length. Consider the "Length of Master Password" to have more characters rather than having any periodic password rotation.
Prohibit reuse of old master passwords	Prohibit users from re-using recent master passwords. Value: The number of historical passwords to check against.	As a best practice we recommend increasing the value from 1 to at least 5. Ideally, you want users to always use a new one, not recycle a few.
Length of master password	Force users to create a master password that includes at least this many characters. Any user attempting to save a master password that uses too few characters is prompted to meet the requirement. Value: The required number of characters. Values must be greater than or equal to 8. To have a different limit for multifactor, specify a second number, separated by a comma (for example, 12,9).	As a best practice we recommend you follow your established AD password policy guidelines for length.
Require master password change when reuse detected	Force users to change their master password upon detecting that it matches the password for any site in their vault. If an employee saves a site password to their vault that matches their master password, they are immediately logged out of LastPass and, upon next login, are forced to change their master password.	As a best practice we recommend enabling this policy to ensure master passwords are unique and not used as a site password.

4. How can I protect the data my organization is sharing via LastPass?

By default, LastPass users can share individual items with up to five users outside of the Enterprise as well as export data from their vault. Review the policies below to consider enabling sharing best practices.

Prohibit Export	Prohibit users from exporting their account data. Advanced tip: To hide the export option in the client software, use the installer switch -dexp. Given that this is a client-side restriction, this policy cannot fully prevent exporting. The policy makes it more difficult for users to access the export option from the product interface.	As a best practice we recommend enabling this policy. If a user has a legitimate need to export it can be temporarily disabled, or they can be excluded to allow them to do an export.
Prohibit Sharing Except for Shared Folders	Only allow sharing via the Shared Folders. This can further be limited to internal sharing within your organization's managed users when you also Enable the Prohibit Shared Folders Outside Business policy under the Account Restrictions category.	As a best practice we recommend you enable this policy. When enabled it removes the option for users to share individual items, requiring shared items to be shared in a folder. This gives more auditability and accountability to sharing in your organization, and the option to give admins elevated super admin control over shared credentials if needed.
Prohibit Shared Folders Outside Business	Prohibit users from sharing Shared Folders with anyone outside your Business account except users at permitted domains. Value: To limit all outside sharing, enter 1. To allow access from certain domains, enter permitted domains separated by comma (example: aaa.com,bbb.com)	As a best practice if there is no use case for external password sharing, we recommend enabling this policy.

5. How can I protect my end user accounts from an internal or external attacker?

The policies below are just some of the ones we recommend ensuring security and protection for your organization against common threats.

Require use of any MFA (multifactor) option	Require users to enable a multifactor authentication option. To define the list of valid multifactor options available to users, go to Advanced Options > Enterprise Options in the Admin Console. Currently available options: LastPass Authenticator, YubiKey, LastPass Sesame, Google Authenticator, Toopher, Duo Security, SecureAuth, Transakt, Salesforce Authenticator, RSA SecurID, and Symantec VIP. Note: Fingerprint and Grid cannot be managed through require use policy.	As a best practice we recommend protecting vaults with 2-factor authentication. Use this policy to offer multiple authenticator options or select one of our other multifactor policies to require a specific authenticator. This policy can be turned on after rollout, but we recommend testing prior to rollout. Communication/process awareness is important when implementing. *If your LastPass account has a Federated Login integration with LastPass (e.g. Azure, Okta, or ADFS), we recommend setting up MFA with your Identity Provider since LastPass does not support LastPass-initiated MFA for federated accounts. Please see our article for Limitations of Federated Login

Restrict login attempts before lockout	Allow this many failed login attempts before locking a user's account and preventing further attempts for the time period set in the 'Lockout period' policy. Value: Set number of allowed attempts value between 3 and 8. For example: a value of 3 results in lockout on the fourth failed attempt.	Best practice is to set a value of allowed attempts between 3 and 8. *If left disabled system value is 5*.
Lockout period	Upon exceeding the number of allowed failed login attempts, a user's account remains locked for this many minutes before they can attempt login. Value: Set number value between 10-60 (minutes).	Best practice is to set a value between 10-60 minutes. *If left disabled system value is 15 minutes*.
Account Logoff on Browser Close	Automatically log users out of their LastPass account when they close their browser. This forces users to log in each time they re-open their browser. This also prevents users from setting this policy themselves in their browser extensions.	It is a best practice to enable an account logoff policy. When this policy is enabled, you will override the user's General Security Log Off Preferences. By default, there are no log off policies configured, and users can configure their own logoff preferences if they setup up their account securely.
Account Logoff on Browser Idle (extension)	Automatically log users out of their LastPass account after their browser remains idle for this many minutes. This also prevents users from setting this policy themselves in their browser extensions. Value: 0-9999 (minutes). IMPORTANT: Your identity provider settings may override this policy for your federated users.	Best practice is to enable an account logoff policy. When this policy is enabled, you will override the user's General Security Log Off Preferences. By default, there are no log off policies configured, and user is able to configure their own logoff preferences. Consider enabling this policy to ensure users are logged out of LastPass after being idle for an extended period of time since not all users will close their browsers at the end of the day.
Account logoff (website)	Automatically log users out of LastPass.com after the selected period of time. This also prevents users from setting this policy themselves (Account Settings > Website Auto-Logoff). Value: 5-20160 (minutes). IMPORTANT: Your identity provider settings may override this policy for your federated users.	As a best practice we recommended enabling this policy. Enabling this policy and setting a value between 5-20160 minutes helps protect user's vaults. Typically, users don't use their online vault unless they are on a shared machine without the extension installed. Setting a value here ensures users will be logged out of website if they walk away.
Restrict Access by Country	Only allow login to LastPass from specified countries. Value: Enter the two-character domain abbreviation for each permitted country, separated by white space. For example: US CA This allows users to log in when the country code for their IP is in the United States or Canada. Any matching country code allows entry. A matching IP restriction or DNS restriction also allows entry. For a list of country codes, see https://lastpass.com/listcountrycodes.php	

Restrict Access by IP Address	Use IP address restriction to allow access only from approved IP addresses or ranges. Value: Enter each allowed IP address or partial IP address, separated by white space. For example: 71.126.154. 128.8. 120.0.0.1 would allow login from any address in 71.126.154.*, 128.8.*.* and 120.0.0.1. A matching DNS restriction or country restriction also allows entry. We also support CIDR Notation. For example: 61.12.56.0/24 allows any address in 61.12.56.* to log in.	

6. How can I ensure my user's mobile experience is secure?

Enable the policies below to extend your LastPass security while using LastPass on a mobile device.

Require PIN	Force users to enter a PIN code when they open the mobile app.	As a best practice we recommended enabling this policy. Requiring use of a PIN means users will be required to set up an 'alternative' unlock method. The default lock for the mobile app is 5 minutes. Once a PIN is set users can replace it with their mobile's supported biometric method.
Override mobile lock option	Force users to log in or re-enter their PIN to unlock the app after the specified period of app inactivity. Supported on LastPass for iOS 4.1.8 or higher and LastPass for Android 4.2.290 or higher. Value: Enter value for allowed period of inactivity, as follows: 0 - Immediately 1 - 1 minute 2 - 3 minutes 3 - 5 minutes 4 - 15 minutes 5 - 1 hour 6 - 8 hours 7 - 24 hours 8 - Never	As a best practice we recommend enabling this policy. Enabling the mobile lock option override will ensure users are locking the app in the background.
Prohibit 'Remember master password' on mobile	Prevent users from remembering their master password to the app on their mobile.	Remembering the password weakens the security for that user, we recommend enabling this policy as a best practice.

7. How can I help adoption of LastPass within my organization?

The policies below, if enabled, will help support adoption throughout your organization. Encouraging good password hygiene at work and at home will boost the security of your organization.

Recommend or Require Linked Personal Account	When enabled you can Require or Recommend users to create a personal account linked to their Business account. Users in your Business with an existing personal account are required to link it to their Business account. Users without a personal account are required to create one using their personal email address as their username. Value: Enter value of 1 to force or require a linked account; Enter value of 2 to recommend a linked account.	Best practice is to recommend users set up a personal linked account. If policy is not enabled users will still have option to 'Link Account' in their vault, unless linked accounts are prohibited.
Save Personal Sites to Personal Vault	By linking their personal account to their work account, users gain access to both LastPass vaults with a single login to their enterprise account. When this policy is enabled, sites with a username matching the user's linked personal account are saved directly to the personal vault. Sites with any other username are saved to the work vault.	As a best practice we recommend enabling this policy. A personal LastPass account must be linked to the user's business account for sites to auto-sort. Without this policy set, all logins will save to the work vault by default. When saving a site users can override the LastPass personal account designation by selecting 'Edit' if desired. When enabled, once a site is saved to their vault the user will not be able to move any sites that use their business account username (@company.com) from their company managed vault to their linked personal vault. Only sites with a username that doesn't match their company username can be moved to a linked personal account.
Check for Compromised User Accounts	When performing a background security scan, check each username against a database of known third-party security breaches. If the username associated with a login is potentially at risk, an email is sent to the user identifying the compromised website and recommending preventative measures.	As a best practice we recommended enabling this policy. Read more about breach detection: https://support.logmeininc.com/lastpass/help/what-is-breach-detection-in-lastpass

8. How can I increase the amount of reporting information available?

LastPass is built on a "zero-knowledge" model and by default we only capture specific events in the reporting available to your admins. If you would like to add additional reporting measures, please review the optional policies listed below.

Log full URL in reporting	Show full URL (server + path, but no HTTP parameters) in reports rather than just the domain name of the site. This is often useful to distinguish which service is being accessed if many different resources are located on the same internal server. This policy goes into effect upon next user login. EXAMPLE: If a user logs into https://def.abc.com/login.php?a=1, then by default we would display 'abc.com', but with this policy enabled we would display 'def.abc.com/login.php'.	As a best practice we recommend enabling this policy for more complete auditing logs. *https://support.logmeininc.com/lastpass/help/generate-enterprise-reports-lp010040*

Log item name in reporting	Show name of site/note in reports. The name data (which is typically never sent to LastPass in unencrypted format) is sent by the client when reporting a login event and is shown in the admin reports. This policy goes into effect upon next user login. EXAMPLE If a user logs in to the site 'alphabet' with URL https://abc.com/, then by default we display 'abc.com'. With this policy enabled, we display 'abc.com (alphabet)'. Note: If all 3 polices are enabled, the output would look similar to the following: login.salesforce.com/ (john.smith@email.com) (Customer Support Salesforce login) from Support Logins Where: login.salesforce.com/is the Full URL john.smith@email.com is the username Customer Support Salesforce Login is the name of the item, Support Logins is the name of the Shared Folder	As a best practice we recommend enabling this policy for more complete auditing logs. *https://support.logmeininc.com/lastpass/help/generate-enterprise-reports-lp010040*
Log username in reporting	By activating this policy, you allow LastPass to store username data unencrypted and to provide that data to you in reports. This policy goes into effect upon next user login. Important: LastPass never stores username data unencrypted unless you activate this policy. EXAMPLE If a user logs in to the site 'alphabet' with URL https://abc.com/, then by default we display 'abc.com'. With this policy enabled, we display 'abc.com (alphabet)'.	As a best practice we recommend enabling this policy for more complete auditing logs. https://support.logmeininc.com/lastpass/help/generate-enterprise-reports-lp010040