LastPass Enterprise Recommended Policies Guide

This document will help guide you through common scenarios and selecting policies to enable on your LastPass Enterprise account.

We will not cover all policies available to you in LastPass Enterprise. To review a comprehensive list of policies please visit your **Admin Console** > **Settings** > **Policies**.

Contents

LastPass Enterprise Recommended Policies 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 manage my user's mobile experience? 8

How can I help adoption of LastPass within my organization? 8

How can I increase the amount of reporting information available? 9

Default Policies

These policies are enabled by default for your LastPass Enterprise account.

Policy	Description	Additional Notes
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.	Though a default policy it is best practice to disable this policy to keep your LastPass accounts secure.
Block TOR Access	Restrict logins to LastPass accounts from The Onion Router (TOR) exit node IPs.	
Prohibit reuse of old master passwords	Prohibit users from re-using recent master passwords. 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.	
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: Email addresses, separated by commas.	
Pre-create sharing key	When creating user accounts server-side, automatically create and encrypt the sharing key that allows users to share items with others. Without this policy, users must log in to the browser extension to generate the key and share. **Note:** The sharing key will be created server-side, as opposed to client-side upon user login. It is immediately encrypted using the user's temporary password and is never stored in plaintext.	
Log mobile activity	Gather data about password access and site fill events for use in reporting.	
Show master password strength	Collect and report data about the strength of your users' master passwords.	
Show security challenge score	Upon user login, run the security challenge in the background and report the results.	

How can I manage administrative functions?

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

Policy	Description	Additional Notes
Permit super admins to reset master passwords	Allow selected admins to reset the master password of any user in your enterprise. 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.	Without this policy enabled, your administrators will be unable to assist a user if they have been locked out of their LastPass account.
Permit super admins to access shared folders	Invisibly share all shared folders in your enterprise 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.	This maintains admin oversight of items being shared within the organization.
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 an end users 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. Example: 1,2,admin@acme.com,admin2@acme.com	
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. Enter the allowed domains, separated by commas.	

How can I manage the Master Password?

Review the policies listed below to determine if they will help you structure how your employees use the Master Password. Additional configuration information is available when editing the policy itself in the Admin Console.

Policy	Description	Additional Notes
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).	We recommend master password changes every 90 days without multi-factor authentication, or every 365 days if you require multi-factor. If you wish to specify different time frames when a user has MFA enabled, you can specify two values separated by a comma (for example, 90,365).
Prohibit reuse of old master passwords	Prohibit users from re-using recent master passwords. Value: The number of historical passwords to check against.	By default, this is set to 1. Meaning they cannot reuse their last master password. We recommend setting this to mirror your AD policy (if applicable) or setting a reasonably high number based upon whether you are using multi-factor and how often you are enforcing a master password change.
Length of master password	Force users to create a master password that includes at least this many characters. Once enabled, users with a master password using too few characters are prompted to change their master password. 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).	Typically, enterprises follow their already-established AD password policy for password length.
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 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).	Typically, enterprises follow their already-established AD password policy for password complexity.

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

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

Policy	Description	Additional Notes
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.	If a user needs to export for a valid reason, you can temporarily exempt them from the policy.
Prohibit shared folders outside enterprise	Prohibit users from sharing Shared Folders with anyone outside your Enterprise account. That is, only allow shared folders to be shared inside your organization.	You can exclude specific individuals and groups as needed.
Prohibit sharing except shared folders	Only allow sharing via the shared folders feature, which can be limited to internal sharing within your Enterprise account (Prohibit shared folders outside enterprise).	This removes the option to share an individual item. Shared items must be in shared folders and give more auditability and accountability to sharing in your organization.

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

The policies below are recommended in order to ensure security and protect your organization from common threats.

Policy	Description	Additional Notes
Require any MFA option after grace period	Require users to enable a multifactor authentication option a specified number of days after account creation. 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.	We recommend master password changes every 90 days if you do not require multifactor authentication, or every 365 days if you do require MFA.
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. Values: Number of allowed attempts, between 3 and 8. For example, a value of 3 results in lockout on the fourth failed attempt.	
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: 10-60 (minutes).	
Require MFA for admin console	Require logged in admins to complete MFA when accessing the admin console after this many minutes of inactivity.	This policy helps you provide an additional layer of security to the admin console.
Account logoff on browser idle (website)	Automatically log users out of LastPass.com after their browser remains idle for this many minutes. This also prevents users from setting this policy themselves (Account Settings > Website Auto-Logoff). Value: 5-20160 (minutes).	We recommend setting this to around 30 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.	
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).	
Allow users to skip MFA at trusted locations	Allow users to trust computers and bypass multifactor authentication when accessing LastPass from an approved location (such as your office), based on IP address. Value: Enter each allowed IP address or partial IP address, separated by white space. Example: 71.126.154. 128.8. 120.0.0.1 This allows any user located at 71.126.154.*, 128.8.*.* and 120.0.0.1 to trust their device and skip MFA. To disable trust altogether, enter 'none'. This is not retroactive. Computers previously trusted remain trusted after the policy is enabled.	You can enable this policy to allow users to skip multi-factor authentication from trusted locations (such as the office) but still require it from remote locations.

How can I manage my user's mobile experience?

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

Policy	Description	Additional Notes
Require PIN	Force users to enter a PIN code when they open the mobile app.	This policy also supports biometric authentication on mobile devices.
Override mobile lock option	Force users to log in or re-enter their PIN to unlock the app after the specified period of inactivity. Supported on LastPass for iOS 4.1.8 or higher and LastPass for Android 4.2.290 or higher. Value: 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.	
Prohibit 'Remember master password' on mobile	Prevent users from remembering their master password to the app.	We generally recommend against the "remember password" option because it reduces security and increases the likelihood a user will forget their master password.

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.

Policy	Description	Additional Notes
Recommend or require linked personal account	Force each user to create a personal account linked to their Enterprise account. Users in your Enterprise with an existing personal account are forced to link it to their personal account. Users without a personal account are prompted to create one using their personal email address as their username. The master password is the same for both accounts. Value: Forced, enter 1. Optional, enter 2.	This policy is often enabled after the initial roll-out as an added employee benefit. We recommend waiting to avoid confusion during the initial onboarding process.
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.	

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.

Policy	Description	Additional Notes
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'.	
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)'.	
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. **Important!** LastPass never stores username data unencrypted unless you activate this policy.	

	Logged in users must log in again for this policy to take effect. 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)'.	