Summary of Key LastPass Security Principles

As the leading cloud-based password vaulting and single sign-on solution, LastPass helps consumers and businesses increase productivity and decrease the likelihood of password-related breaches.

Our security measures include:

- **Reliable access to data**: We endeavor to ensure you can manage and view your passwords whenever and wherever you need to, offline and online.
- **Local-only encryption**: LastPass is a host-proof solution, meaning the system is designed to ensure that only the user can access their data. Sensitive data is encrypted locally in a 'vault' that is stored on the end user's device and on our servers.
- **Centralized control for admins**: For businesses, LastPass provides a cloud-based admin dashboard for deployment and management of the service. The dashboard includes configurable security policies, provisioning of shared credentials, and real-time auditing reports.
- **Security and encryption best practices**: Sensitive data stored with LastPass is encrypted using a key that we never have. LastPass offers industry standard cryptography that is strong enough to defend against brute-force attacks.
- **SOC-2 report**: The Service Organization Control 2 (SOC 2) Type II attestation report is widely recognized as an information security "gold standard." Completing and maintaining the SOC 2 is just one way we demonstrate our commitment to data security, safeguarding of information and service availability.
- **Top-level data centers**: LastPass uses data centers in world-class hosting facilities that follow best practices for redundancy and stability.
- **Transparent incident response:** Our team reacts swiftly to investigate, verify, and resolve reports of bugs or vulnerabilities. Our bug bounty program also incentivizes responsible disclosure and improvements to our service. Our product and customers benefit from the positive relationship we maintain with top security researchers and the attention we receive from their work.
- **Regular audits and penetration tests**: We engage trusted, world-class, third-party security firms to conduct routine audits and annual testing of the LastPass service and infrastructure.
- **Backed by leading SaaS company LogMeIn**: One of the world's top 10 public SaaS companies, LogMeIn, Inc. (NASDAQ:LOGM) is a market leader with over $1 billion in revenue, nearly 3,000 employees and millions of customers in virtually every country across the globe. LogMeIn's products simplify how people connect with each other and the world around them to drive meaningful interactions, deepen relationships, and create better outcomes for individuals and businesses. LogMeIn is headquartered in Boston with additional locations in North America, Europe, Asia and Australia.

Table of Contents

Introduction

LastPass is helping people achieve effortless security, at home and in the workplace. As our business and personal worlds intersect on an increasing scale in our cloud-centric world, a strong foundation of secure authentication and access is critical to keeping systems, data, and assets safe.

As a secure password manager trusted by millions of consumers and tens of thousands of companies worldwide, LastPass safely stores passwords and grants access to the technology and services they rely on every day.

Our core mission at LastPass is to keep customer information secure and provide a reliable service. This document shows how we accomplish this mission.

We help LastPass customers achieve better security in two ways:

1. Building security into the very foundation of the product, with additional layers of protection to safeguard customer data at all steps, and

2. Offering features, settings, and options that allow users and admins to customize LastPass to meet their specific security needs and follow best practices.

By building security and safeguards into the product, we strive to ensure that all LastPass users are protected from threats, both in the cloud and locally on their device.

And by offering configurable security features, we can equip end users and admins alike to eliminate the poor password practices that put their private information at risk. With the implementation of a password manager, businesses and consumers can strengthen their defense against attackers.

We are constantly improving the LastPass software and updating our service with the latest technology as new attack vectors and security threats emerge. We work closely with members of the LastPass community and security researchers who help improve the service for the benefit of all users. LastPass fundamentally believes in taking proactive measures to review security reports, address issues, and regularly evaluate new technologies that will strengthen our security model.

Our Privacy Statement is available here (https://lastpass.com/privacy-statement) and our Terms of Service are available here (https://secure.logmein.com/home/policies/terms-and-conditions).

Logging in

The Master Password

When a user creates their LastPass account, they also create a master password. The master password is used to authenticate in to the LastPass account through the browser extension or by logging in to www.lastpass.com.

Once logged in, the user will be able to access and input the credentials for other websites that have been stored in LastPass. The vault is the space where a user can add, view, and manage credentials and other items that have been saved to LastPass. The vault is accessed by successfully entering the correct username and master password.

A strong master password

To ensure the security of their vault, it is essential that users choose a strong master password for their LastPass account. While we enforce industry-standard minimums when creating the master password, the user should make the master password as strong as possible. Specifically, that means a master password should be long and unique, with a mix of character types – it directly

impacts the overall security of the data as other encryption keys are generated from this password.

In our business solutions, admins can also enforce policies around the strength, complexity, and regular updates of master passwords, as well as prevent master password reuse.

The master password should never be used as a password for any other website or app. Even a variation of it should never be used for any other account. For example, a breach on another website could put a LastPass account at risk if a user re-uses their master password.

Users should also never share their master password with anyone, including LastPass. No one at LastPass, including our customer care team, ever needs to know the user's master password. Any requests to share a master password should be treated as a threat and reported to the LastPass team at https://lastpass.com/supportticket.php immediately.

A moderately strong master password also ensures that a brute-force attack is unrealistic.

Protecting the master password

The encrypted vault data is meaningless to us and to anyone else without the decryption key. The key to the user's data is created from a combination of their username and master password. The master password is never sent to LastPass.

While the option to remember the master password is offered in the LastPass extension and mobile apps due to user demand, enabling it may reduce the security of the master password, and also makes it more likely that a user will forget it. LastPass Enterprise admins can enable a policy that prevents users from selecting remember master password.

New Device Verification

When a user logs in to their LastPass account from a new location and an unrecognized device, LastPass requires the user to complete a verification step to "trust" that new location/device.

The verification process involves LastPass sending a verification link to the email address used for a given LastPass account (or a designated security email address, if one has been added to the account). Once the user clicks the verification link, the new location/device is trusted.

The next time the user logs in from that device/location they will not be asked to complete the verification step.

Multifactor Authentication

LastPass encourages users to enable multifactor authentication to add an additional layer of protection to an account. Multifactor authentication requires another piece of information before access is granted. Companies can mandate use of multifactor authentication with LastPass through policies available in the admin dashboard.

Multifactor authentication requires two or more authentication factors, including something the user knows (the master password), in addition to something they have (a code, a key) and/or something they are (a fingerprint). By requiring not only the master password, but also an additional login step (like a one-time password, a fingerprint swipe, a randomly-generated 6-digit code), a user adds another layer of protection against unauthorized access to their account.

If an attacker were to discover a user's Master Password, it's unlikely that they would also have access to a valid multifactor token, therefore minimizing the chance that they would be unable to gain access to the user's account.

LastPass currently supports over a dozen multifactor authentication vendors. Learn more about the options LastPass currently supports at https://lastpass.com/multifactor-authentication/.

Admins can mandate multifactor authentication through policies in the admin dashboard, requiring use of any supported multifactor authentication option or requiring use of only specific, company-approved multifactor authentication options.

Encryption Technology

The LastPass encrypted vault is designed to prevent the ability to decrypt a vault without a user's master password.

Local-Only Encryption Model

LastPass employs local-only encryption, also known as "host-proof hosting". This type of solution is designed to allow only a LastPass user to decrypt and access their data. We call this "Local-Only Encryption", which means that all sensitive vault data is encrypted and decrypted exclusively on the user's local machine (such as Chrome, Firefox, iPhone, Android, the Web Vault, etc.), rather than after the data syncs to LastPass' servers.

Only once data is encrypted with the user's unique encryption key is the data synced to LastPass for secure storage. Sensitive data is transmitted to LastPass as a base64 encoded blob of encrypted data, and it never touches LastPass servers in a way that can be visible to LastPass. LastPass does not have access to nor does it store the master password, which prevents LastPass from having the ability to decrypt a user's sensitive vault data.

This means that LastPass, and the employees who work here, can never access the sensitive data that a user stores in their vault nor can LastPass remotely access a user's device. The data stored in LastPass is decrypted the instant it is needed on the user's device, after the master password is successfully entered, including when the user is accessing their account via the web vault and any of the mobile apps.

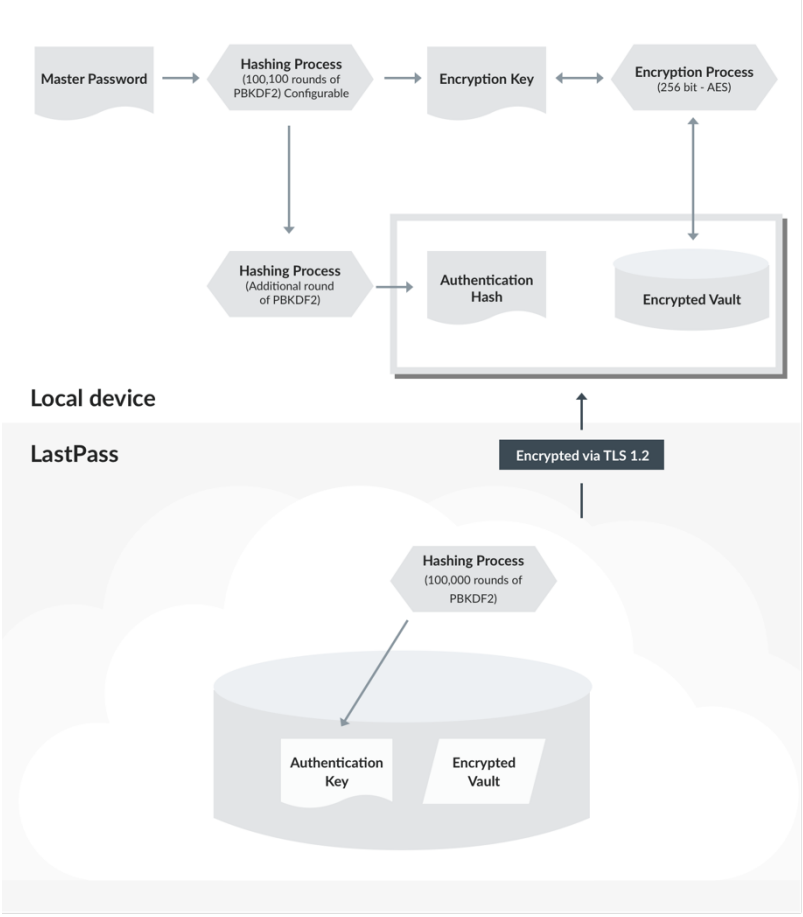
Account Lockout

LastPass also protects against brute-force attacks by locking accounts after repeated failed attempts to login. We regularly monitor accounts for signs of irregular or suspicious activity and will suspend accounts automatically when appropriate.

AES 256-bit Encryption

LastPass uses encryption and hashing algorithms of the highest standard to protect user data. Local-only encryption and locally-created, one-way salted hashes provide LastPass users with the best of both worlds: Complete security, with online accessibility, and syncing through the cloud.

LastPass encrypts user data with the trusted algorithm Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with a 256-bit key generated from each user's master password. The AES 256-bit algorithm is widely-accepted as impenetrable and is the same military-grade encryption used by banks and the US military to secure Top Secret data. We believe that our best line of defense is simply not having access to unencrypted sensitive vault data.



Key Derivation

When a user creates their account, we first do a hash of the LastPass master password using the username as the salt. This is performed on the user's device (client-side).

We use a default of 100,100 rounds of PBKDF2-SHA256 to create the encryption key, on which we perform another single round of hashing, to generate the master password authentication hash (or the "login hash"). This hash is sent to the LastPass server so that we can perform an authentication check as the user is logging in. With that value, we use a salt (a random string per user) and do another 100,100 rounds of PBKDF2 hashing, in addition to hashing with scrypt, a best-in-class hashing algorithm. When the user logs in, we compare this value to the authentication hash in our database. This is the value that LastPass stores on its servers to check against when the user next logs in.

The master password and encryption key are never sent to our servers. And because hashing is a one-way algorithm, LastPass cannot reverse the authentication hash that it receives.

In summary: With a good master password, cracking our algorithms is unrealistic, even for the strongest of computers.

Key Strengthening with PBKDF2

LastPass has implemented AES-256 with thousands of rounds of PBKDF2 SHA-256, a password-strengthening algorithm, to create the user's unique encryption key.

PBKDF2 is an adaptive one-way function which hashes a password multiple times with a hashing algorithm that can be chosen by the service provider. This makes it difficult for a computer to check that any one password is the correct master password during a brute-force attack.

LastPass has opted to use SHA-256, a slower hashing algorithm that provides more protection against brute-force attacks. LastPass performs x number of rounds of the function (100,100 by default) to create the encryption key, before a single additional round of PBKDF2 is done to create the user's login hash.

LastPass can increase this number of rounds over time to render brute-forcing the master password infeasible even as computers advance. Users also have the ability to increase the rounds of PBKDF2 in their account settings.

Increasing the number of iterations increases the work required to derive the hash. This makes verifying a password take longer, but in turn it also significantly increases the work needed to brute-force a password with a given hash.

The entire process is conducted client-side. The resulting login hash is what is communicated with LastPass. LastPass uses the hash to verify that the user is entering the correct master password when logging in to their account.

LastPass also performs 100,100 rounds of PBKDF2 server-side. This implementation of PBKDF2 client-side and server-side ensures that the two pieces of the user's data - the part that's stored offline locally and the part that's stored online on LastPass servers - are thoroughly protected.

PBKDF2 can be described as:

Derived Key = PBKDF2(PRF, Password, Salt, Iterations, Key Length)

Where:

PRF is the hash function to be used.

Password is the Master Password.

Salt consists of bits of data unique to each account used to ensure the same Master Password does not produce the same derived key.

Iterations is the desired number of iterations to run the PRF.

Key Length is the desired length of the derived key.

A vault encryption key is calculated with:

PBKDF2(SHA-256, Master Password, Username, 100,100, 256)

To create a login hash, an extra level of PBKDF2-SHA256 is run on the user's password using the user's vault encryption key to create another 256-bit hash, thus increasing the number of iterations to 100,101.

Login hash = PBKDF2(SHA-256, Master Password, Username, 100,101, 256)

This hash value is sent to LastPass and used for account authentication. Additional measures are taken to protect this hash before it is stored by LastPass, as described in Storing the Login Hash section.

Due to the number of rounds used, users may notice slowness or problems connecting to LastPass when logging in via certain browsers, such as legacy versions of Internet Explorer.

Enforcing Security Policies

LastPass Enterprise offers additional layers of control and protection to companies via the Admin Console. Admins can control the provisioning and de-provisioning of users, mandate the use of security features, and set organization-wide security policies that are customized for the unique needs of their corporate environment. A user kill switch ensures that departing or rogue employees can have their access revoked in real-time.

LastPass Enterprise allows admins to audit employee password habits and see if employees are reusing passwords, reusing their master password, and putting the organization at risk through their actions.

Companies also benefit from detailed reporting logs for auditing and compliance purposes. In addition to the data encryption and storage benefits, LastPass Enterprise allows companies to create password policies and data breach prevention practices that are manageable and enforceable.
Learn more about LastPass Enterprise here (https://www.lastpass.com/enterprise/).

Shared Folders

Public Key Cryptography

LastPass uses RSA public key cryptography to allow users to share credentials with trusted parties synced through LastPass. Admins and users can create Shared Folders to give appropriate access to individuals or groups, without the need to expose the credentials themselves. And even though it is shared through LastPass, LastPass is unable to decrypt the data.

RSA uses asymmetric key algorithms, where the key used to encrypt a message is different from the key used to decrypt it. Each user has a pair of cryptographic keys, one public, one private. The public key can be shared with anyone and can be used to encrypt data, while the private key is available only to the user and can be used to decrypt data encrypted with their public key.

When a Shared Folder is created, a 256-bit encryption key is generated and used to encrypt the data stored in the Shared Folder. This encryption key is further encrypted with the public key of anyone invited to the Shared Folder and can be decrypted only with the invitee's corresponding private key.

All users who share folders generate a 2048-bit RSA key pair locally on their own device. The user's private key is encrypted with their vault encryption key using AES-256-bit encryption then sent to LastPass along with the user's public key. The encrypted private key is sent to LastPass so that it can be attained from other devices in the future. Public keys will be used by other users to encrypt data that can only be decrypted with the original private key.

Securing Shared Credentials

Because password sharing is an inevitability in the workplace, ensuring the security of shared access to credentials is critical to maintaining compliance and safeguarding your company from threats. LastPass facilitates this in a way that provides convenient access for the employee, while maintaining accountability and tracking to meet your company's security requirements. Both private and work-related credentials can be shared through LastPass.

We strongly recommend using the password generator to create a unique, strong password for an account before sharing it.

When a user shares a credential, regardless of whether the password is "hidden" from the recipient in LastPass or made visible, the recipient can then launch the site that results in the autofill of the credentials. Once a shared credential is auto-filled on a website, it is outside of LastPass' control, and

savvy end-users may be able to obtain the password. For example, the recipient may use the browser's developer tools to reveal the password.

Linked Accounts

LastPass users can link a personal account to a LastPass Enterprise account. By linking accounts, the user's personal vault is shared with their enterprise account. This works in much the same way as Shared Folders. The difference is that this user has the Master Password for both vaults.

Account Recovery

Because LastPass does not store the master password, it does not offer the same password reset options users may be accustomed to on other web services. If a user forgets their master password, LastPass cannot look up the master password, reset the master password, or create a new master password for the user.

One Time Passwords (OTP) can be used for account recovery if a user's Master Password is lost. Recovery OTPs are created automatically on a device when logging in.

Login One Time Passwords

Users can generate and print Login One Time Passwords (OTP) on an ad hoc basis for use when logging in to LastPass on an untrusted device. A user can generate OTPs to log in on an untrusted computer in place of the master password, but they expire after first use.

They work the same way as Recovery OTPs but remain enabled until used and are not stored on a local device. Using an OTP can safeguard against keylogging on public or untrusted computers. Learn more here (https://helpdesk.lastpass.com/your-lastpass-icon/loggin-in/one-time-passwords/).

Recovery

A random recovery key is generated on the user's device at login. This key is used to encrypt the vault encryption key (which is re-generated when logging in) using AES-128 in CBC mode. The encrypted vault key is then sent to LastPass servers while the recovery key is stored locally on the device.

The encrypted vault key cannot be fetched from LastPass until account recovery is activated by the user. The encrypted vault key on LastPass' servers is secure because the recovery key is never shared with LastPass.

When Account Recovery is requested, a verification code is emailed or sent via SMS to the user. The user's identity is confirmed via access to the email account or phone number associated with the user's account. After verification, the encrypted vault key is downloaded and decrypted locally on the user's computer using the recovery key. The user specifies a new master password, generates a new vault encryption key, a new login hash, and then encrypts their vault data with the new key. The old encrypted files are wiped from LastPass servers, thus invalidating the old keys.

If for any reason the OTPs are not available, whether because of a software or system upgrade, or because the user does not have access to a previously-used device, then the only recourse is to delete the account to start over. LastPass cannot do anything in this case to recover the encrypted data or reset the master password, because that recovery data is only available client-side rather than server-side. Again, we've designed LastPass this way as a protective measure to reduce the risk of someone maliciously obtaining a user's sensitive data.

Account recovery OTPs can be disabled by the user, or disabled organization-wide with a LastPass Enterprise security policy.

A super admin security policy is available to Teams and Enterprise admins, allowing designated admins to reset the master password of employee accounts.

Securing the Client

The LastPass client is typically run as a browser extension that is supported for all major browsers on Windows, Mac and Linux. Native applications are also available for iOS, Android, Windows and OSX.

Communication between the client and LastPass servers uses TLS connections. The TLS configuration uses industry best practices, only allowing TLS 1.x connections with strong cipher suites.

Connections via browser extensions are further protected by browser security controls. HTTP Strict Transport Security (HSTS) forces all connections to TLS, thus mitigating the risks of downgrade attacks and misconfiguration. Content Security Policy headers provide further protection from injection attacks, such as cross-site scripting.

LastPass Infrastructure

High-Availability Service

LastPass is built with full redundancy of our data centers, reducing the risk of downtime and single-point-of-failure.

Even if a user does not have internet access, they can still access their account via the LastPass browser extension or app on a device where they have previously logged in. A secure, local copy of a user's vault content is stored automatically when a user connects to LastPass, which is then available offline.

The status of the LastPass service is currently reported here (https://twitter.com/lastpassstatus).

Service Architecture

LastPass operates in three active-active datacenters in the United States and another pair of active-active datacenters in Europe. This model increases service reliability as each datacenter can handle all user traffic. All datacenters are in world-class hosting facilities that constantly monitor environmental conditions and provide 24-7 physical security.

User vault data is backed up daily and stored offsite at a separate datacenter.

Automated nightly reviews are conducted to ensure the appropriate level of security.

LastPass systems run on a Linux system that updates automatically to maintain the latest available security updates. User data is stored in SQL and NoSQL databases.

Universal Availability

LastPass strives to offer users access to their data on as many platforms as possible, and keeps pace with new technology so that users can always rely on LastPass to securely sync their data where they need it. Information on supported platforms, browsers, and mobile devices can be found here (https://helpdesk.lastpass.com/downloading-and-installing/).

The LastPass web vault is also available at www.LastPass.com on all major browsers and platforms and via m.lastpass.com on mobile platforms. Although downloading the extensions and apps are recommended for the best experience, the web vault ensures secure access on devices where LastPass can't be installed.

Local and Cloud Storage

To ensure that customers have consistent access to their data, LastPass creates an encrypted copy of the vault both locally on a user's device and in the cloud on LastPass' servers.

Protecting Data at Rest

When using the LastPass browser extensions or the LastPass mobile apps, LastPass stores a locally-encrypted, cached copy of the vault on that device. If LastPass.com can't be reached because the user has no internet connection or in the unlikely event that LastPass.com is down, the user can log in via the browser extension or the mobile app to access the stored data.

The secure offline cache is only available if the user has successfully logged in to the extension or mobile app at least once before to sync with the LastPass servers.

On Windows devices, Windows Crypto APIs are used to add an extra layer of protection.

Note that offline access can be disabled in the LastPass extension preferences or disabled company-wide with a LastPass Enterprise security policy.

User Data Storage

Sensitive vault data is encrypted client-side, then received and stored by LastPass as encrypted data. Other data, such as a phone number used for SMS account recovery, is encrypted server-side using a Hardware Security Module (HSM). The HSM is a separate device purposely built to securely store cryptographic keys.

Login Hash Storage

LastPass receives the login hash from the user (following the default 5,001 iterations on the user's master password using PBKDF2-SHA256), the login hash is additionally salted with a random 256-bit salt, and an additional 100,000 rounds of PBKDF2-SHA256 are performed. That output is then hashed using scrypt to increase the memory requirements of brute-force attacks. The resulting hash stored by LastPass is the output of 105,001 rounds of SHA256 + scrypt.

LastPass System Data

EncFS is used to encrypt system data needed to run the LastPass service. EncFS is a Filesystem in Userspace (FUSE)-based encrypted filesystem that automatically encrypts all files added to the volume. A system administrator is required to manually enter the password to decrypt the filesystem.

Transport Layer Encryption

LastPass uses TLS exclusively for secure data transfer even though the vast majority of user data is already encrypted with AES-256. This protocol protects the data from any party listening in to the network traffic. TLS ensures that the user is connecting directly to LastPass to protect against man-in-the-middle attacks.

Protecting LastPass Network and Systems

LastPass protects infrastructure and customer data with best practices and regularly-upgraded systems.

Application Layer Firewalls and Filtering

LastPass utilizes a best in class application firewall and DDoS prevention service. Traffic to LastPass services is proxied through this service, which filters and blocks malicious traffic before it reaches LastPass servers.

LastPass runs a local application firewall on its web servers to provide an additional layer of protection against web application attacks. This also actively blocks malicious traffic, such as SQL injection and XSS (cross-site scripting) attacks.

Network Layer Firewalls and Filtering

All LastPass web servers are running host-based firewalls which filter inbound and outbound connections including internal connections between LastPass systems. Only ports 80 and 443 are open to the internet.

Vulnerability Testing

Vulnerability scans are run daily against LastPass servers. LastPass also uses automated tools to search for common mistakes that could result in vulnerabilities such as XSS or SQL Injection.

Third-Party Audits

We're committed to evaluating and improving LastPass through third-party audits and penetration tests, and LastPass infrastructure is tested by an industry-recognized third party on an annual basis.

Error Reporting

LastPass may also collect anonymized error reports and crash data from users to help us continually improve the service. Although users can opt-out of this when installing LastPass, no identifying information is used in these automated error reports, which are solely used by the LastPass team to improve performance and security.

Code Reviews

All changes to the code base are reviewed by the technical team for security, privacy, and compliance with company policies and procedures.

LastPass Federated Login Services

Introduction

To simplify the employee onboarding process and provide a seamless end-user experience, LastPass offers integration with Active Directory Federation Services (ADFS). With federated login, a user can log in to their LastPass account with their AD credentials, so that their AD identity becomes linked with their LastPass identity.

Enabling and configuring federated login for your deployment must be done prior to provisioning users.

The architectural design of LastPass Federated Login Services maintains the zero-knowledge model, even while the user authentication itself is performed by ADFS rather than directly by LastPass. LastPass Federated Login Services is designed to ensure that the user's AD credentials are not exposed to LastPass, and the master password is also not exposed to LastPass.

Infrastructure Elements

LastPass Federated Login Services implements the Security Assertion Markup Language 2.0 (SAML 2.0) standard. As is typical with SAML, there are three main components that make up the integration, where LastPass is the Service Provider (SP), your organization acts as the Identity Provider (IdP), and the data is made available through a user agent (the browser or app).

For LastPass Federated Login Services, the primary infrastructure components are:

Service Provider (LastPass)

lastpass.com (LP): The web and database servers where the encrypted vault and one third of the master password are stored.

accounts.lastpass.com (ALP): A separate server where authentication data and one third of the master password are stored.

Identity Provider (Company's Active Directory Infrastructure)

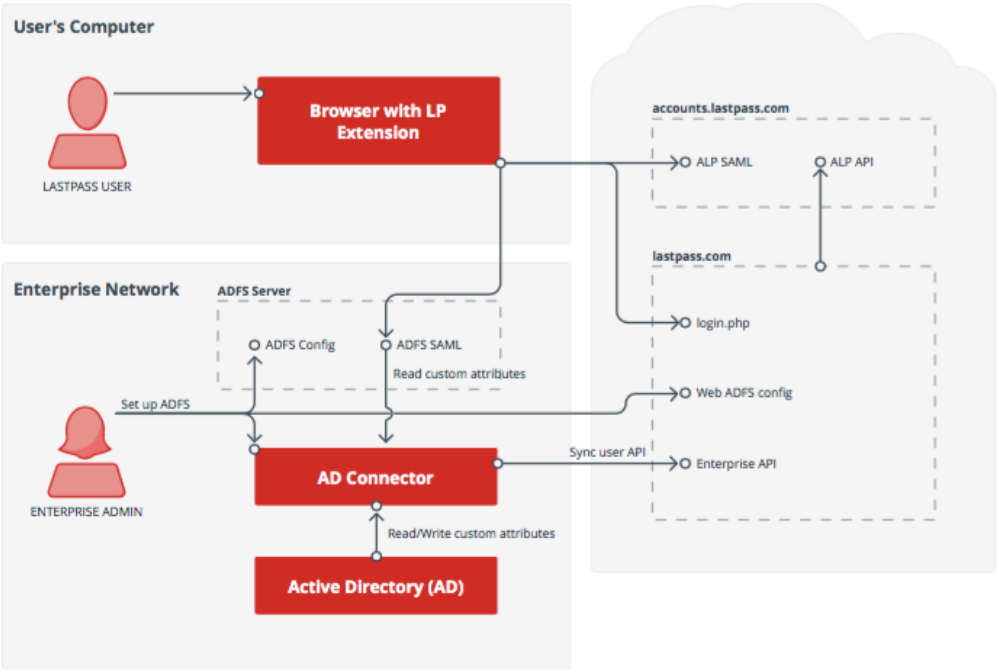
Active Directory: Hosted by the company and serves as the directory service provider. One third of the master password is stored as a user account attribute.

Active Directory Federation Services: Hosted by the company and authenticates the user as they log in to LastPass.

ADFS Custom Attribute Store: Provides a secure way for adding the encrypted K1 to the SAML response.

LastPass Active Directory Connector: A LastPass client run by the company to sync user status from their Active Directory to LastPass.

User Agent (Browser/LastPass Extension)



Creating the Master Password

By default, every LastPass user has a master password that is used to generate an encryption key for their LastPass vault and is used to log in to their LastPass account.

With LastPass Federated Login Services, the master password is created behind-the-scenes by the LastPass AD Connector. As a user is provisioned, the LastPass AD Connector generates three 256-bit keys using a cryptographically secure, pseudo-random number generator.

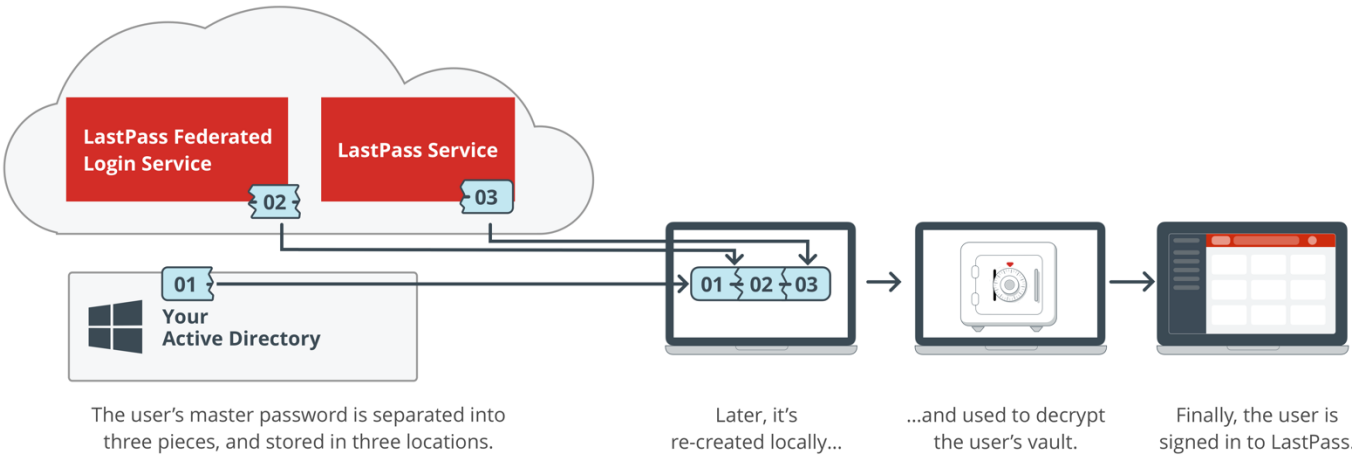
Together, the three keys (K1, K2, and K3) equal the user's master password, using the following algorithm:

MasterPassword = base64(SHA256(K1 XOR K2 XOR K3))

With the master password, the LastPass AD Connector generates a vault encryption key that is used to encrypt the user's newly-created vault. The encrypted vault and the login hash are then sent to lastpass.com to complete the user provisioning step.

K1, K2, and K3 are then stored separately, one in the company's Active Directory, one in accounts.lastpass.com, and one in lastpass.com.

As the user logs in to LastPass, they are redirected to ADFS to authenticate. After successfully authenticating, the three keys are re-combined locally on the user's machine to form the "master password" and decrypt the LastPass vault.



The three keys – K1, K2, and K3 – are only recombined locally on the user's device to form the master password and decrypt the vault.

Configuring LastPass Federated Login Services

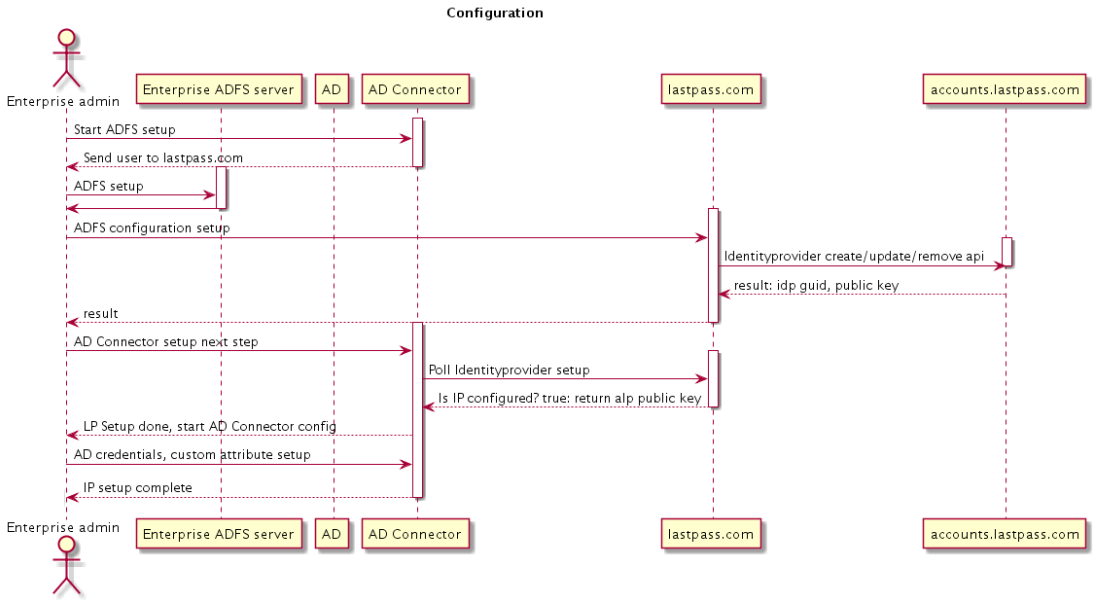
Before users can be provisioned to LastPass with LastPass Federated Login Services, each of the following steps must be completed:

- The company has configured ADFS
- The company has registered the ADFS server with LastPass
- The company has activated a LastPass Enterprise account
- An Enterprise admin account has been created (required as part of the Enterprise account activation)
- The LastPass AD Connector is installed in the company's local environment

- In the company's Active Directory, there is an attribute field created to store K1
- Super Admin Master Password Policy is enabled

Two pieces of information, the URL certificate and entity ID, must also be shared with LastPass to complete the integration.

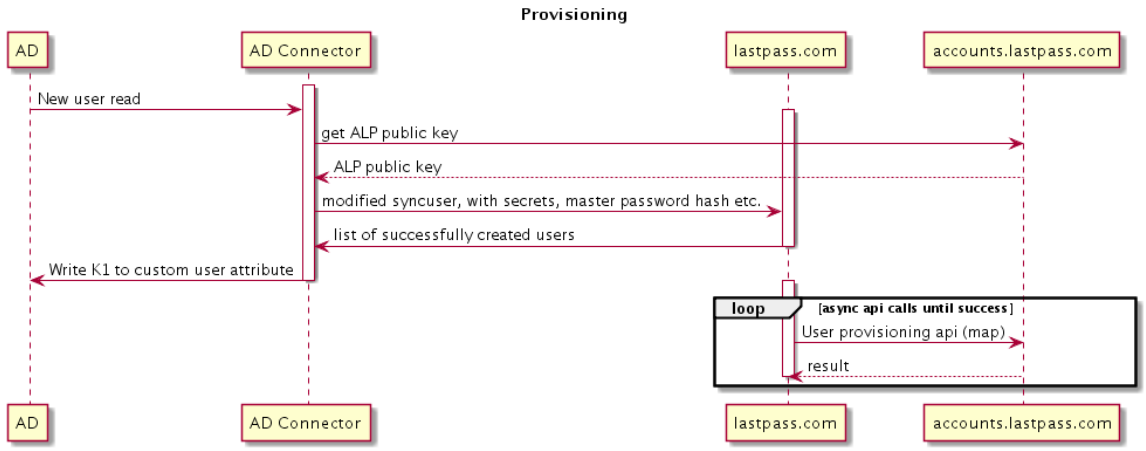
For details on the above steps, see our configuration guide here (https://support.logmeininc.com/lastpass/help/set-up-federation-services-for-lastpass-enterprise-lp010054).



User Provisioning

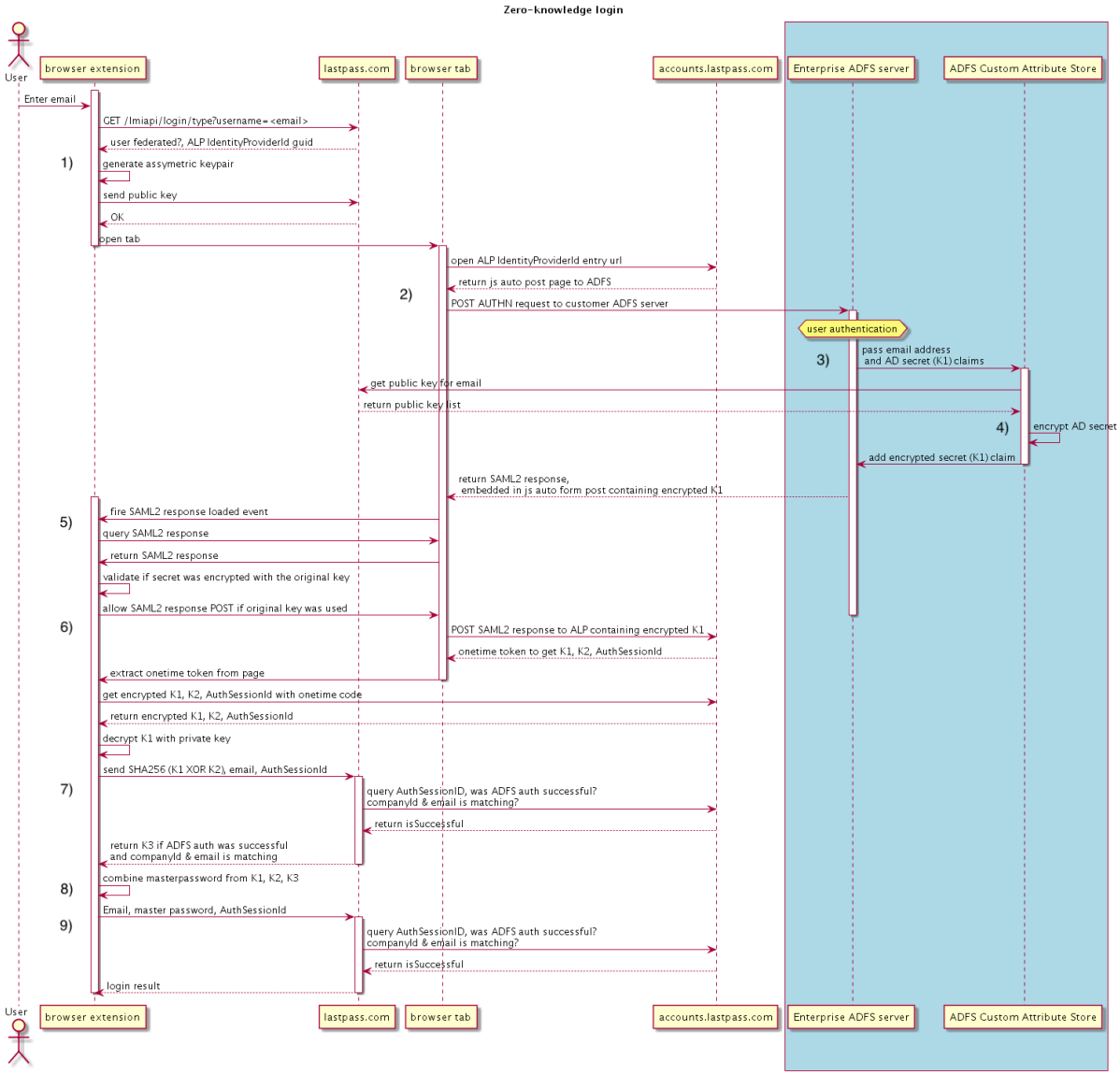
As a new user is added to a company's Active Directory, the LastPass AD Connector detects the new user and creates the new user in the LastPass directory via the following process:

1. Either the new user is added in the company's Active Directory or existing users become eligible for a LastPass account (e.g. based on group membership).
2. On the next sync, the LastPass AD Connector detects the user is new to LastPass.
3. AD Connector provisions the new user to lastpass.com (where K3 is stored) and accounts.lastpass.com (where K2 is stored).
4. If step 3 is executed successfully, K1 is stored in the company's Active Directory (in the custom attribute field specified by the admin).



Federated Login Flow

When the company has configured LastPass Federated Login Services, when the user initiates a login to the LastPass browser extension the following sequence occurs:



1. The local LastPass browser extension generates a public/private key pair (the public key is later stored on lastpass.com and used later to encrypt K1) and checks if the user requires federated login to complete authentication.
2. If the user is federated, then the login flow is redirected to accounts.lastpass.com to start federated authentication
3. The user is authenticated by the ADFS server with the user's AD credentials.
4. The ADFS Custom Attribute Store requests the public key of the browser extension (from lastpass.com) and uses it to encrypt K1 (K1 is stored in Active Directory, so the ADFS server can access it) and add the encrypted K1 to SAML Response.
5. The extension validates if the right public key is used to encrypt K1.
6. The extension receives the validated SAML Response, which includes K2.
7. The extension then requests K3 from lastpass.com providing a SHA2 hash of K1 and K2 as an additional authentication check.

8. Now the extension has all necessary key parts (K1,K2, and K3) to recreate the user's master password and retrieve the encrypted vault.
9. Now, authentication proceeds for the user and they are logged in with the master password.

Offline login

Offline login is not currently supported with our ADFS integration.

Resetting Passwords with the Super Admin Policy

We require enabling the Super Admin Master Password Reset Policy prior to deploying LastPass Federated Login Services as this is the only way to turn off federated login in LastPass.

Web login

Currently, the user must be signed in through the LastPass browser extension to connect to www.lastpass.com.

Multi-factor authentication

When allowing employees to log in to LastPass with their AD credentials, it is strongly recommended that you also require the use of multi-factor authentication. Should the AD credentials ever be phished or otherwise captured, multi-factor authentication ensures that attackers will not be able to log in to LastPass without the secondary piece of login information.

It is also recommended that you setup multi-factor authentication through your AD (rather than through LastPass) to ensure the highest level of security for your LastPass accounts.

LastPass Authenticator is included in your LastPass Enterprise purchase and provides one-tap verification to a user's smartphone for convenient multi-factor authentication. Other top multi- factor authentication solutions are also supported. See our manual to learn more:
https://support.logmeininc.com/lastpass/help/enterprise-admin-management-of-multifactor-authentication-options-lp010026
[please copy and paste URL if hyperlink doesn't work]

SOC 2 Attestation

LastPass has acquired the Service Organization Control 2 (SOC 2) Type II attestation report from an industry-recognized auditing firm. The SOC 2 report provides a rigorous audit, review, and validation of our practices as a company, and with respect to our services and systems, around data security, safeguarding of information and service availability. This includes ensuring proper safeguarding of the data our systems process and the availability of those systems. An annual review must be completed to maintain SOC 2 compliance.

As the "gold standard" for software companies that is widely recognized nationwide across industries, completing and maintaining the SOC 2 attestation is just one more way we demonstrate our commitment to security and privacy.

System Hardening

All LastPass systems are hardened and patched regularly.

All servers run an industry-leading Linux Security Module to enforce mandatory access controls to system files and objects. This kernel security module is configured to restrict the capabilities and privileges of

running processes to the minimum privilege required, which reduces the risk of vulnerabilities from other services. LastPass administrators must explicitly configure access to any files or services that a process requires to run.

Linux kernel security module configuration violations are forwarded to LastPass' centralized logging infrastructure, which helps monitor and detect possible host intrusions.

Infrastructure Access Controls

Access to LastPass infrastructure and systems is protected by multi-layer security and multifactor authentication. Employees are only granted access to LastPass production systems on an as-needed basis and as required by their role.

System access requires administrators to pass multiple identity checks, including multifactor authentication. A secure VPN connection is required for access to the LastPass network. SSH is used for console access to servers, requiring password protected SSH keys to login.

Logging and Monitoring

System logs are forwarded to a central log server and reviewed by a log management and analytics tool. Additional tools are used to monitor network bandwidth and the health of LastPass systems, alerting LastPass personnel in the event of any issues.

Bug Bounty Program

LastPass participates in a bug bounty program (https://bugcrowd.com/lastpass) hosted at BugCrowd to facilitate the important work that security researchers do to find and responsibly disclose qualifying security bugs.

Security Incidence Reporting

Security is our highest priority at LastPass, including quickly responding to and fixing reports of bugs or vulnerabilities. LastPass is in part able to achieve the highest level of security for our users by looking to our community to challenge our technology.

We appreciate the important work that the security research community provides and appreciate responsible disclosure of issues; we believe that when the security process works as designed, we all benefit.

Local-Impact vs. Broad-Impact Security Concerns

LastPass classifies security reports into two categories: A Local-Impact Security Concern that affects only the user or their account, and a Broad-Impact Security Concern, which is an issue that can impact many or all LastPass users.

A local-impact security concern should be reported in a support ticket (https://lastpass.com/supportticket.php) where it will be escalated appropriately.

A broad-impact security concern should be reported through our bug bounty program at https://bugcrowd.com/lastpass.

Reporting Security Issues

When reporting potential issues, we ask that users please try to be as thorough as possible in providing us enough information so that we can appropriately recreate their findings.

This may include exact steps to reproduce the bug, any links that were clicked on, pages that were visited, URLs, and any affected account email addresses. Please include a code sample and either images or a video recording that clearly demonstrates the exploit.

If using automated tools to find vulnerabilities, please be aware that these tools frequently report false positives.

Responding to Security Concerns

Once a security concern has been submitted and received, our team will:

1. Promptly take steps to investigate the report and determine its severity.

2. Contact the reporter directly if more information is needed.

3. Try to fix the issue, potentially with the reporter's assistance. While issues are usually fixed very quickly, deploying the fix to affected customers will be done based on the complexity and severity of the issue.

4. Once the issue is fully resolved to both the reporter's and our satisfaction, we'll close the report.