unolock®

CYBVAULT

UnoLock Docs

Your Safe for everything that matters.

None

None

Table of contents

1. Overview

1.1 UnoLock Knowledge Base

Welcome to the **UnoLock Knowledge Base**. This is the main entry point for understanding how UnoLock works, how to use it, and how its security model is designed.

UnoLock is built around a few core ideas:

- your data lives in a **Safe**
- access is controlled by **registered access keys**
- Safe data is **client-side encrypted**
- messaging and protected API flows use **end-to-end encrypted payload protection**
- privacy in UnoLock is driven by **OPSEC**, metadata minimization, and separation of systems

⚠ **Public Playground**

You can explore UnoLock features in the public playground at safe.test.1two.be.

This is a **non-production test environment** used to test changes before they are promoted to safe.unolock.com. Logging is enabled, and all data is automatically purged every 24 hours.

Do **not** store sensitive, personal, financial, prohibited, or irreplaceable data there.

For payment testing, use card number `4242 4242 4242 4242` with any future expiry date, any CVC, and any postal code.

Need help or want to report something? Contact support@unolock.com or visit r/UnoLockSupport.

1.1.1 Start Here

- **Get Started**: create your first Safe and understand the basics
- **Features Overview**: see the customer-facing feature set
- **Security Overview**: understand the security model
- **Safe Setup Tutorial**: step-by-step setup guide

1.1.2 Introduction

This Knowledge Base explains UnoLock from practical use to deeper architecture. It is organized so customers can start with workflows and concepts, while security reviewers and technical users can drill into the underlying model.

? **What’s Covered?**

- **Features**: Access keys, Spaces, Shared Spaces, Vault Messaging, DPW, LegacyLink, and more.
- **Security**: Client-side encryption, end-to-end encrypted payload protection, WebAuthn access, post-quantum design, and threat controls.
- **How-To Guides**: Task-based tutorials for setup, messaging, Spaces, and recovery/inheritance flows.
- **Pricing Tiers**: Free, Inheritance, Sovereign, and HighRisk.
- **Data Self-Governance**: The principles behind UnoLock’s control model.
- **Company & Legal**: Product background, policies, and supporting information.

Continue to Application Overview

1.1.3 Core Features

UnoLock’s feature set is designed around storage, collaboration, security, continuity, and privacy.

All Features

- **Local File Encryption**: Encrypt data on-device before upload (all tiers). **Learn More**
- **Global Redundancy**: Multi-region AWS backups for reliability (all tiers). **Learn More**
- **FIDO2 & Biometric Login**: Passwordless authentication (all tiers). **Learn More**
- **Access Keys & Safe Access**: Access the same Safe from multiple devices or users through registered access keys (Inheritance, Sovereign, HighRisk tiers). **Learn More**
- **Spaces**: Compartmentalized areas inside a Safe with same-Safe access control (Sovereign, HighRisk tiers). **Learn More**
- **Shared Spaces**: Collaboration between separate Safes in the same Space (Sovereign, HighRisk tiers). **Learn More**
- **Vault Messaging**: Address-based encrypted messaging and Shared Space invites between Safes (Sovereign, HighRisk tiers). **Learn More**
- **Bitcoin Payment**: Anonymous payments via Bitcoin (all tiers). **Learn More**
- **Lifetime Safe**: Concept for prepaid credits that help prevent Safe expiration after later billing issues. **Learn More**
- **Absolute Anonymity**: OPSEC-driven privacy through metadata minimization and system separation (all tiers). **Learn More**
- **Payment Anonymity**: Payment processing designed so billing does not become Safe identity (all tiers). **Learn More**
- **End-to-End Encryption**: Client-side encrypted storage plus end-to-end protected messaging and API payloads (all tiers). **Learn More**
- **Lockout Guard**: Recover access from lost devices (all tiers). **Learn More**
- **Digital Paper Wallet (BTC, ETH, ERC-20)**: Generate and export cryptocurrency (BTC, ETH, ERC-20) keys (Sovereign, HighRisk tiers). **Learn More**
- **Duress Decoy**: Hide selected sensitive Spaces when a safeword PIN is used (Sovereign tier). **Learn More**
- **LifeSafe**: Delete selected sensitive Spaces when a safeword PIN is used (HighRisk tier). **Learn More**
- **LegacyLink**: One-time succession or recovery path after configured inactivity conditions (Inheritance, Sovereign, HighRisk tiers). **Learn More**
- **Time Lock**: Temporarily lock an individual access key for a selected number of hours (all tiers). **Learn More**
- **PIN Code**: Randomized keypad thwarts keyloggers (all tiers). **Learn More**
- **Post-Quantum Encryption**: Future-proof protection against quantum threats (all tiers). **Learn More**
- **UnoLock Drop**: Sender client for delivering messages/files to a Safe through Receive Addresses. **Learn More**

Explore All Features

1.1.4 Security Architecture

UnoLock’s security model is layered. It does not rely on one control or one secret.

Security Highlights

- **Client-Side Encryption**: Safe data is encrypted before it leaves the client.
- **End-to-End Protected Messaging and API Payloads**: protected payloads are not reduced to plain HTTPS-only confidentiality.
- **WebAuthn Access Keys**: Safe access is based on registered authenticators, not reusable passwords.
- **Protected PIN Entry**: the PIN is a brute-force and deniability control, not the root encryption secret.

- **Post-Quantum Cryptography**: quantum-resistant protections are built into the broader model.

Dive into Security

1.1.5 Data Self-Governance (DSG)

UnoLock’s **Data Self-Governance as a Service (DSGaaS)** model is about keeping control with the user instead of turning the platform into the ultimate trust anchor.

DSG Principles

- **Security & Privacy**: client-side protected data and minimized service-side knowledge
- **Autonomy & Control**: control access with access keys, Spaces, and Shared Spaces
- **Continuity & Succession**: plan for recovery, inheritance, and high-risk scenarios without abandoning the core security model

Understand DSG

1.1.6 How-To Guides

The how-to section is task-oriented. Start there if you want practical steps instead of conceptual overviews.

Popular Tutorials

- **Safe Setup Tutorial**: Create your first Safe.
- **Local File Encryption**: Secure files on-device.
- **Granting an Access Key Access to Spaces in the Same Safe**: Share one Safe correctly.
- **Sharing a Space Between Safes**: Use Shared Spaces for collaboration.
- **Setting Up LegacyLink**: Plan for inheritance.
- **Receive Addresses**: Create addresses and share UnoLock Drop links for anonymous intake.

View All Tutorials

1.1.7 Pricing Tiers

UnoLock offers four tiers built around different continuity, collaboration, and protection needs.

Tiers

- **Free**: core Safe storage and protection
- **Inheritance**: adds succession and same-Safe multi-access-key support
- **Sovereign**: adds Spaces, Vault Messaging, collaboration, and advanced privacy/security tooling
- **HighRisk**: adds the strongest coercion-resistance and long-term protection features

Explore Pricing

1.1.8 Our Company

TechSologic Inc., creators of UnoLock, is committed to privacy-first innovation. Learn about our mission, Beta Program, and community.

Highlights

- **Mission**: Build tools for digital sovereignty, user protection, and data self-governance.
- **Beta Program**: Shape UnoLock's future with early feature access.
- **Reddit Community**: Engage at r/UnoLock.

Meet TechSologic

1.1.9 Application Overview

UnoLock CybVault is a cloud-based digital Safe platform for sensitive records, secure messaging, private collaboration, digital inheritance, and high-risk protection scenarios.

Why UnoLock?

- **Access Keys, Not Passwords**: Safe access is controlled by registered passkeys and hardware-backed authenticators.
- **Same-Safe Sharing and Shared Spaces**: support both shared access inside one Safe and collaboration between separate Safes.
- **Client-Side + End-to-End Protection**: stored data, messaging, and protected API flows are covered by layered encryption.
- **OPSEC-Driven Privacy Model**: payment, messaging, metadata, and Safe access are designed to reduce linkability.

Learn More

1.1.10 Getting Started

Begin your UnoLock journey with these steps:

- **Create Your Safe**: Start with the **Safe Setup Tutorial** and understand how Safe creation and access-key registration work.
- **Register Access Keys**: Use passkeys, hardware security keys, or compatible authenticators for WebAuthn-based Safe access.
- **Choose Your Collaboration Model**: Use **same-Safe access keys** when multiple users share one Safe, or **Shared Spaces** when separate Safes need to collaborate.
- **Protect and Organize Your Data**: Use client-side encryption, Spaces, Vault Messaging, and continuity features such as LegacyLink or Lockout Guard where appropriate.

Start Now

2. Features

2.1 Features Overview

2.1.1 Overview

UnoLock CybVault is a state-of-the-art digital Safe designed to provide **complete control** over your digital assets and sensitive information. With cutting-edge features like post-quantum encryption, LegacyLink inheritance, and UnoLock Drop, UnoLock ensures unparalleled security, privacy, and autonomy across the Free, Inheritance, Sovereign, and HighRisk tiers. Backed by **Data Self-Governance as a Service (DSGaaS)**, UnoLock guarantees no third-party intervention, empowering you to manage cryptocurrencies (BTC, ETH, ERC-20), documents, and more with confidence.

2.1.2 Key Features

UnoLock’s comprehensive feature set empowers you with unmatched security, privacy, and control.

All Features

- **Local File Encryption**: Encrypt data on-device before upload, ensuring privacy (all tiers). **Learn More**
- **Global Redundancy**: Multi-region AWS backups for reliability (all tiers). **Learn More**
- **FIDO2 & Biometric Login**: Passwordless authentication for secure access (all tiers). **Learn More**
- **Access Keys & Safe Access**: Access the same cloud-based Safe through multiple registered access keys, including passkeys and hardware keys (Inheritance, Sovereign, HighRisk tiers). **Learn More**
- **Bitcoin Payment**: Anonymous payments via Bitcoin (all tiers). **Learn More**
- **Lifetime Safe**: Concept for prepaid credits that help prevent Safe expiration after later billing issues. **Learn More**
- **Absolute Anonymity**: No personal data or tracking (all tiers). **Learn More**
- **Payment Anonymity**: Transactions without identity linkage (all tiers). **Learn More**
- **End-to-End Encryption**: AES-256-GCM secures data from creation to access (all tiers). **Learn More**
- **Lockout Guard**: Recover access from lost devices (all tiers). **Learn More**
- **Digital Paper Wallet (BTC, ETH, ERC-20)**: Generate and export Bitcoin and Ethereum keys for cold-like storage (Sovereign, HighRisk tiers). **Learn More**
- **SeedSafe**: High-security Safe for backing up BIP-39 mnemonic seed phrases (All tiers). **Learn More**
- **DPW VaultSign**: Secure transaction signing within the Digital Paper Wallet ecosystem (Sovereign, HighRisk tiers). **Learn More**
- **DPW Portability**: Cross-Safe migration of Digital Paper Wallets (Sovereign, HighRisk tiers). **Learn More**
- **Duress Decoy**: Hide selected sensitive Spaces when a safeword PIN is used (Sovereign tier). **Learn More**
- **LifeSafe**: Delete selected sensitive Spaces when a safeword PIN is used (HighRisk tier). **Learn More**
- **LegacyLink**: One-time succession or recovery path after configured inactivity conditions (Inheritance, Sovereign, HighRisk tiers). **Learn More**
- **Time Lock**: Temporarily lock an individual access key for a selected number of hours, typically when closing a Safe before a risky situation (all tiers). **Learn More**
- **Vault Messaging**: Address-based messaging for sending messages, files, and Shared Space invites between Safes through Receive Addresses (Sovereign, HighRisk tiers to create addresses). **Learn More**
- **Spaces**: Compartmentalized areas inside a Safe, with support for same-Safe access control through access keys (Sovereign, HighRisk tiers). **Learn More**
- **Shared Spaces**: Collaboration Spaces shared between separate Safes so participants can work in the same Space without sharing the rest of their Safes (Sovereign, HighRisk tiers). **Learn More**
- **PIN Code**: Randomized keypad thwarts keyloggers (all tiers). **Learn More**
- **Post-Quantum Encryption**: Future-proof protection against quantum threats (all tiers). **Learn More**
- **UnoLock Drop**: Sender client for delivering messages/files to a Safe through Receive Addresses. **Learn More**
- **Threat Detection**: Runtime security monitoring and tamper detection (all tiers). **Learn More**

2.1.3 Why It Matters

UnoLock’s features address the full lifecycle of digital asset protection, from creation to inheritance. By combining post-quantum encryption, absolute anonymity, and specialized tools like Digital Paper Wallet (BTC, ETH, ERC-20) and UnoLock Drop, UnoLock ensures digital sovereignty in an era of rising cyber threats and surveillance. Whether securing cryptocurrencies (BTC, ETH, ERC-20), managing sensitive documents, or planning your digital legacy, UnoLock empowers you with unparalleled control and peace of mind.

Back to Knowledge Base

2.2 Local File Encryption

2.2.1 Overview

Local File Encryption transforms your sensitive data into a portable Safe in your hands, encrypting files client-side into a **ULF (UnoLock Encrypted File)** that you can download and send to any cloud storage provider, with only you holding the key to decrypt it. Available across all tiers, Free, Inheritance, Sovereign, and HighRisk, this feature ensures that your files, from personal documents to Bitcoin and Ethereum keys, remain private and secure, untouchable by UnoLock or third-party services. UnoLock's zero-knowledge design guarantees that your data's sovereignty travels with you, wherever you store or share it.

2.2.2 How It Works

- **Client-Side Encryption**: Files are encrypted on your device using **AES-256 GCM**, ensuring confidentiality and integrity before any transmission or storage.
- **ULF File Creation**: Encrypted files are saved as a **ULF (UnoLock Encrypted File)**, downloaded locally to your device, ready for secure sharing or storage.
- **Cloud Storage Flexibility**: ULF files can be sent or uploaded to **any cloud storage provider** (e.g., Dropbox, Google Drive, OneDrive), with only you able to decrypt them using your locally stored key.
- **Zero-Knowledge Key Management**: Unique encryption keys are generated and stored on your device, never shared with UnoLock or third parties, ensuring exclusive user control.

2.2.3 Security Implications

- **Zero-Knowledge Privacy**: UnoLock has no access to your encryption keys or unencrypted data, ensuring complete privacy, even when ULF files are stored externally.
- **Portable Security**: ULF files remain encrypted and secure on any cloud storage platform, protected from unauthorized access by third parties or service providers.
- **End-to-End Protection**: From local encryption to secure transmission via TLS 1.3-encrypted channels (for UnoLock uploads), your data is safeguarded at every stage.

2.2.4 Use Cases

- **Personal Data Sharing**: Encrypt sensitive documents (e.g., tax records, medical files) as ULF files and store them on Google Drive or share via email, with only you able to decrypt.
- **Business Collaboration**: Companies can distribute encrypted client contracts or proprietary data as ULF files on Dropbox, ensuring only authorized recipients with keys can access them.
- **Cryptocurrency Safety**: Securely store wallet seed phrases as ULF files on OneDrive or a USB drive, protected from theft or exposure, with user-only decryption.

2.2.5 Why It Matters

Local File Encryption empowers you with a portable fortress of privacy, creating ULF files that safeguard your data across any cloud storage platform, accessible only by you. In a world of data breaches and surveillance, this feature ensures your sensitive information remains yours alone, wherever it resides.

2.2.6 FAQs

? What is a ULF file, and how can I use it?

A ULF (UnoLock Encrypted File) is a locally encrypted file downloadable to your device, which you can store or send to any cloud provider (e.g., Dropbox, Google Drive), decryptable only with your key.

Can UnoLock or cloud providers decrypt my ULF files?

No, UnoLock’s zero-knowledge model ensures only you have the encryption key, and ULF files remain unreadable to cloud providers or third parties.

How secure is it to store ULF files on external cloud storage?

ULF files are encrypted with AES-256 GCM, ensuring they remain secure on any platform, as only you can decrypt them with your locally stored key.

2.2.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Local File Encryption supports GDPR and HIPAA by encrypting data client-side and ensuring only the user can access it, maintaining privacy across any storage platform.

2.2.8 Integration with Other Features

- **Post-Quantum Encryption Security**: Enhances Local File Encryption with quantum-resistant AES-256 GCM, ensuring ULF files remain secure against future threats.
- **FIDO2 Authentication with WebAuthn**: Secures access to encryption keys with passwordless, phishing-resistant authentication, protecting the decryption process.

Back to Features Overview

2.3 Global Redundancy

2.3.1 Overview

Global Redundancy is a global bastion of data resilience, enabling Free and Inheritance tier users to select a single region from multiple locations to meet data residency requirements, while Sovereign and HighRisk tiers harness multi-region replication through Spaces for unmatched availability and disaster recovery. By securely replicating encrypted data across AWS S3 data centers, UnoLock ensures your Safe remains accessible and protected against outages, disasters, or regional failures, all while upholding the highest standards of privacy and security. Available across all tiers, Free, Inheritance, Sovereign, and HighRisk, this feature guarantees your data's safety, tailored to your tier's needs.

2.3.2 How It Works

- **Single-Region Choice for Free and Inheritance Tiers**: Users in Free and Inheritance tiers select one region (e.g., US, EU, Asia) from multiple location options to comply with data residency requirements, storing encrypted data securely in the chosen region.
- **Multi-Region Replication for Sovereign and HighRisk Tiers**: Sovereign and HighRisk tiers, enabled by Spaces, replicate encrypted data across multiple AWS S3 data centers globally, ensuring maximum availability and resilience.
- **Real-Time Synchronization**: Changes to your Safe are synchronized in real-time across all designated regions, ensuring the latest data version is accessible from any data center.
- **Encrypted Storage**: Data is encrypted with **AES-256 GCM** client-side and stored with server-side encryption (SSE) in each data center, remaining unreadable without your decryption keys.

2.3.3 Security Implications

- **Tailored Data Residency**: Free and Inheritance tier users meet regional compliance (e.g., GDPR) with single-region selection, while Sovereign and HighRisk tiers benefit from multi-region redundancy for enhanced availability.
- **Disaster Recovery Assurance**: Single and multi-region replication ensures data access even if a region faces outages, natural disasters, or cyberattacks, with greater resilience for paid tiers.
- **Uncompromised Security**: Encrypted data remains secure during replication and at rest, protected by AES-256 GCM and SSE, ensuring no unauthorized access.

2.3.4 Use Cases

- **Regulatory Compliance**: Free tier users in the EU can select an EU region to comply with GDPR, ensuring data residency while maintaining security and accessibility.
- **Global Business Operations**: Enterprises in Sovereign or HighRisk tiers can rely on multi-region redundancy for fast, secure data access, ensuring continuity during regional disruptions.
- **Personal Data Protection**: Individuals in any tier can store critical files (e.g., legal documents, Bitcoin and Ethereum keys) with confidence, knowing single or multi-region replication prevents loss from localized failures.

2.3.5 Why It Matters

Global Redundancy delivers a fortress of availability and compliance, blending Free and Inheritance tier flexibility with Sovereign and HighRisk tier resilience to ensure your encrypted data is always safe and accessible. In a digital world prone to disruptions, UnoLock's region-aware replication safeguards your Safe with unmatched reliability and privacy.

2.3.6 FAQs

Can Free or Inheritance tier users choose multi-region storage?

No, Free and Inheritance tiers select a single region (e.g., US, EU, Asia) for data residency, while multi-region redundancy is exclusive to Sovereign and HighRisk tiers via Spaces.

What happens if a data center in my chosen region goes offline?

Free and Inheritance tier data in a single region may be temporarily inaccessible, but Sovereign and HighRisk tiers’ multi-region replication ensures access from other data centers.

Is my data secure during replication across regions?

Yes, data is encrypted with AES-256 GCM before replication and stored with server-side encryption, ensuring it remains unreadable without your keys.

2.3.7 Compliance & Privacy Regulations

- **GDPR Compliance**: Global Redundancy supports GDPR by allowing Free and Inheritance tier users to select a region for data residency and ensuring encrypted replication for Sovereign and HighRisk tiers meets privacy standards.
- **Data Sovereignty**: Single and multi-region options enable compliance with regional data laws, maintaining security and user control across all tiers.

2.3.8 Integration with Other Features

- **Local File Encryption**: Complements Global Redundancy by encrypting files as ULFs client-side with AES-256 GCM, ensuring replicated data remains secure in any region.
- **Post-Quantum Encryption Security**: Enhances redundancy with quantum-resistant encryption, protecting data across regions against future threats.

Back to Features Overview

2.4 Biometric and FIDO2 Access

2.4.1 Overview

Biometric and FIDO2 Access offers secure, passwordless authentication for accessing users' UnoLock Safes, utilizing biometric data (e.g., fingerprints, facial recognition) and FIDO2 hardware tokens. This feature enhances both security and convenience, reducing reliance on traditional passwords, which are vulnerable to theft or hacking. The use of strong, cryptographic-based authentication methods minimizes the risks associated with phishing and password attacks.

2.4.2 How It Works

- **Biometric Authentication**: Users can unlock their Safes using biometric data such as fingerprints or facial recognition. This data is securely stored and processed locally on the user's device, ensuring privacy and security.
- **FIDO2 Authentication**: FIDO2 is an open authentication standard that uses public-key cryptography to enable secure, passwordless access. Users authenticate using a FIDO2 hardware token (e.g., YubiKey) or a biometric device that supports WebAuthn (the web authentication protocol).
- **Public-Private Key Pair**: During the registration process, a public-private key pair is generated. The private key is stored on the hardware token or biometric device, while the public key is registered with UnoLock. During authentication, the device signs a challenge using the private key, and the signature is verified with the public key, granting access without transmitting sensitive information.
- **Primary Authentication Model**: In UnoLock, WebAuthn-based access keys are the primary authentication factor for Safe access. Users can register more than one authenticator for continuity and recovery, but WebAuthn itself is not treated as a secondary factor.

2.4.3 Security Implications

- **Passwordless Security**: Passwordless login eliminates the risks associated with weak or stolen passwords. Since authentication is based on public-key cryptography, FIDO2 is inherently resistant to phishing, credential stuffing, and replay attacks.
- **Local Biometric Data Processing**: Biometric data never leaves the user's device, as all authentication occurs locally. This means that UnoLock never sees or stores biometric information, ensuring user privacy.
- **Resistance to Phishing Attacks**: FIDO2 protects against phishing by verifying the origin of the login request, ensuring that authentication only occurs on legitimate websites or applications.

2.4.4 Use Cases

- **High-Security Access**: Users who handle sensitive data or financial assets can use biometric or FIDO2 authentication for more secure Safe access.
- **Convenience for Daily Use**: Individuals looking for both convenience and security can quickly access their Safe without relying on passwords, reducing login friction while maintaining high security.
- **Enterprise and Business**: Organizations can implement FIDO2 authentication to secure employee access to company Safes, reducing the risks of password theft and improving overall access management.

2.4.5 Why It Matters

Passwords are a common target for cyberattacks and are often the weakest link in account security. By replacing passwords with biometric and FIDO2 authentication, UnoLock provides stronger protection for user Safes, making them highly resistant to attacks such as phishing, brute force, and credential theft. This feature enhances both security and user experience, aligning with UnoLock's commitment to robust, user-centric privacy solutions.

2.4.6 FAQs

How does FIDO2 authentication improve security?

FIDO2 uses public-key cryptography, meaning only the private key stored on your device can authenticate a login attempt. Since no passwords are involved, it prevents phishing, credential stuffing, and man-in-the-middle attacks.

Can UnoLock access my biometric data?

No, biometric data is processed locally on your device and never transmitted to or stored by UnoLock.

What happens if I lose my FIDO2 hardware token?

If you lose one authenticator, access should continue through another registered access key or configured recovery method rather than relying on a single device.

2.4.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: By using local biometric processing and secure FIDO2 authentication, UnoLock ensures compliance with data privacy regulations, protecting user data and minimizing exposure to potential breaches.

2.4.8 Integration with Other Features

- **End-to-End Encryption (E2EE)**: Biometric and FIDO2 Access work alongside E2EE to ensure that Safe access is secured and encrypted, providing comprehensive protection from login to data retrieval.
- **Access Keys & Safe Access**: Users can register multiple passkeys, phones, or hardware authenticators to access the same Safe from different devices while maintaining the same strong security protocols.

2.5 Access Keys & Safe Access

2.5.1 Overview

UnoLock is **cloud-based**, so your Safe is not tied to a single device. Your encrypted Safe data can be accessed from different devices, but access is controlled by your **registered access keys**.

That means the real question is not "Can UnoLock work on multiple devices?" It can. The important question is:

Which access keys are allowed to open this Safe?

2.5.2 What an Access Key Means in UnoLock

In UnoLock, an **access key** is the authentication credential a person uses to unlock a Safe. An access key can be:

- a **passkey** stored by your device platform,
- a **hardware security key** such as a **YubiKey**,
- a **mobile phone acting as a passkey authenticator**,
- or another supported **FIDO2 / WebAuthn** authenticator.

Each user can have their **own** access key. A Safe can have multiple access keys registered to it.

2.5.3 How Access Keys & Safe Access Actually Works

- Your Safe data is stored in UnoLock's cloud architecture.
- You open that Safe from a device by using a **registered access key** on that device.
- If you want access from another device, you register another access key for the same Safe.
- That second access key can belong to:
- you, on another device,
- or another person who needs access to the same Safe.

So this feature is really **multi-access-key access to the same cloud-based Safe**.

2.5.4 What This Looks Like for Users

Examples:

- You use a **passkey on your laptop** and another **passkey on your phone** to open the same Safe.
- You use a **YubiKey** as one access key and a **phone-based passkey** as another.
- A second user gets their **own access key** to the same Safe, with either:
- limited access to selected Spaces,
- or full administrative rights to the Safe.

2.5.5 Why This Matters

This makes the system clearer:

- **The Safe is cloud-based**: your data is available wherever you securely authenticate.
- **The access key controls entry**: a device alone is not what matters.
- **Multiple devices work because multiple access keys can be registered**.
- **Multiple users can share the same Safe** if each has their own registered access key.

2.5.6 Security Implications

- **No shared password model**: access is based on registered authenticators, not a reusable password.
- **Per-user accountability**: each person can have their own access key.
- **Granular control**: access keys can be limited to selected Spaces or elevated to full Safe administration.
- **Phishing-resistant authentication**: WebAuthn / FIDO2 access keys provide stronger protection than traditional passwords.

2.5.7 Use Cases

- **Personal multi-device use**: use your Safe from a phone, tablet, laptop, or desktop with your own registered access keys.
- **Backup access**: register more than one access key so you are not dependent on a single authenticator.
- **Family or team access**: allow multiple users to access the same Safe, each with their own access key and permission level.

2.5.8 Relationship to Shared Spaces

Access-key based Safe access is **not** the same as **Shared Spaces**.

- **Multi-device / multi-user access keys**: multiple users can access the **same Safe**.
- **Shared Spaces**: multiple **separate Safes** collaborate in the same Space.

See **UnoLock Spaces** and **Shared Spaces**.

2.5.9 FAQs

? Can I access my Safe from more than one device?

Yes. UnoLock is cloud-based, so you can access the same Safe from multiple devices as long as you have a registered access key available on those devices.

? Is a device the same thing as an access key?

No. The important thing is the access key, not the device itself. A device may hold a passkey, use a phone-based authenticator, or work with a hardware key such as a YubiKey.

? Can more than one person access the same Safe?

Yes. Multiple users can share one Safe if each person has their own registered access key. Those keys can be limited to selected Spaces or granted full administrative access.

? What if I want collaboration without sharing the same Safe?

Use **Shared Spaces** instead. Shared Spaces are for collaboration between separate Safes.

2.5.10 Integration with Other Features

- **FIDO2 & Biometric Access**: access keys are based on passkeys, WebAuthn, and compatible hardware authenticators.
- **Spaces**: access keys can be limited to selected Spaces or granted full Safe administration.
- **Shared Spaces**: use Shared Spaces when the goal is collaboration between separate Safes rather than shared access to one Safe.

2.6 Bitcoin Payment

2.6.1 Overview

Bitcoin Payment enables users to make secure, anonymous manual payments, renewals, and upgrades using Bitcoin, ensuring transactions are crypto-native and unlinkable to their identity. By leveraging Bitcoin's decentralized blockchain, UnoLock provides a privacy-first payment method that protects financial data from third-party tracking. Available in all tiers (Free, Inheritance, Sovereign, HighRisk), this feature supports one-time transactions without the need for recurring subscriptions.

2.6.2 How It Works

- **Manual Payment Processing**: Users initiate one-time payments, renewals, or tier upgrades using Bitcoin, with no option for recurring subscriptions, ensuring full control over transactions.
- **Anonymous Transaction Design**: Payments require no personal information, using Bitcoin wallet addresses to maintain user anonymity throughout the payment process.
- **Secure Payment Channels**: Transactions are processed via encrypted channels (TLS 1.3), protecting against interception or tampering during transmission to UnoLock's payment system.
- **Blockchain Confirmation**: UnoLock integrates with Bitcoin's decentralized network to verify transactions quickly, enabling prompt activation of services like renewals or upgrades.
- **Flexible Wallet Support**: Users can pay from any Bitcoin wallet, with UnoLock generating a unique payment address for each transaction to enhance privacy.

2.6.3 Security Implications

- **Unlinkable Transactions**: Bitcoin Payment ensures no personal or identifiable data is collected, making transactions untraceable and protecting user financial privacy.
- **Decentralized Blockchain Security**: Bitcoin's cryptographic protocols secure payments, reducing risks of fraud or unauthorized access inherent in centralized payment systems.
- **Zero-Knowledge Payment Model**: UnoLock has no access to the user's Bitcoin wallet or transaction details, ensuring a privacy-first payment process.

2.6.4 Use Cases

- **Anonymous Renewals**: Users can renew their Inheritance, Sovereign, or HighRisk tier services without revealing their identity, ideal for privacy-conscious individuals.
- **Secure Upgrades**: Businesses or individuals can upgrade to higher tiers (e.g., HighRisk for LifeSafe) using Bitcoin, avoiding traditional payment methods that require personal data.
- **Crypto-Native Payments**: Cryptocurrency enthusiasts can make manual payments for UnoLock services, aligning with the platform's decentralized, privacy-focused ethos.

2.6.5 Why It Matters

Bitcoin Payment provides a secure, anonymous alternative to traditional payment methods, empowering users to maintain financial privacy for manual transactions, renewals, and upgrades. In an era of increasing financial surveillance, this feature ensures users can access UnoLock's services without compromising their identity.

2.6.6 FAQs

Can UnoLock track my Bitcoin payments?

No, UnoLock operates under a zero-knowledge model, collecting no personal data and ensuring payments are unlinkable to your identity.

What if my Bitcoin payment is intercepted?

Payments are transmitted via TLS 1.3-encrypted channels, ensuring intercepted data remains secure and unreadable without decryption keys.

Can I use Bitcoin Payment for recurring subscriptions?

No, Bitcoin Payment supports only manual payments, renewals, and upgrades, not recurring subscriptions like credit card payments.

2.6.7 Compliance & Privacy Regulations

- **GDPR Compliance**: Bitcoin Payment aligns with GDPR by collecting no personal data, ensuring user privacy during financial transactions.

2.6.8 Integration with Other Features

- **Payment Anonymity**: Enhances Bitcoin Payment by ensuring all financial transactions remain unlinkable, reinforcing UnoLock's privacy-first approach.
- **Absolute Anonymity**: Complements Bitcoin Payment by eliminating personal information requirements across all UnoLock interactions, including payments.

Back to Features Overview

2.7 LifetimeSafe

2.7.1 Overview

LifetimeSafe is a concept for giving users a way to prepay for Safe coverage by purchasing credits in advance. In this model, those credits would be applied if later subscription payments fail, so a Safe would not expire just because of billing issues down the road. Users could purchase as many credits as they want, making LifetimeSafe a flexible idea for long-term Safe protection without depending entirely on future recurring payments.

2.7.2 How It Works

- **Prepaid Credits**: Users would buy credits ahead of time and could add more whenever they want. There is no fixed 10-year increment model.
- **Protection Against Billing Failures**: If a subscription renewal later failed, available credits would be used so the Safe stays active instead of expiring because of a payment problem.
- **Flexible Long-Term Coverage**: Users could purchase as many credits as they like, making it possible to plan for short-term or long-term protection based on their needs.
- **Unused Value Is Not Lost**: If a user later deleted the Safe, they would be offered a promo code valued at the remaining credits.
- **Works with Safe Features**: LifetimeSafe would preserve access to the Safe and its supported tier-specific capabilities while credit coverage remained available.

2.7.3 Security Implications

- **Reduced Risk from Payment Interruptions**: Prepaid credits could help avoid accidental Safe expiration caused by failed cards, expired payment methods, or other subscription billing issues.
- **Zero-Knowledge Protection Remains**: This concept would not change UnoLock's zero-knowledge architecture or encryption model.
- **More Predictable Long-Term Access**: Users could fund future coverage in advance instead of relying entirely on successful recurring payments over time.

2.7.4 Use Cases

- **Inheritance Planning**: Keep an inheritance Safe protected even if billing details change years later.
- **Long-Term Asset Storage**: Prepay coverage for Safes holding recovery phrases, legal records, or other critical files that should not lapse because of subscription issues.
- **Set-and-Forget Backup Coverage**: Add credits in advance for users who want extra confidence that important Safes remain active over time.

2.7.5 Why It Matters

LifetimeSafe is intended as a financial safety-net concept for long-lived Safes. Instead of depending entirely on future subscription payments succeeding, users could prepay credits in advance and keep protection in place even if billing problems happen later.

2.7.6 FAQs

? Can I add more credits to my Safe?

In the LifetimeSafe concept, yes. Users would be able to purchase additional credits at any time, with no limit to how many credits they can add.

What do credits do?

Credits would be held in reserve and applied if a later subscription payment failed, helping prevent the Safe from expiring because of billing issues.

Will my Safe expire if a later subscription payment fails?

In this concept, available credits would help keep the Safe from expiring due to later subscription payment problems.

What happens to unused credits if I delete my Safe?

In this concept, deleting the Safe would trigger an offer for a promo code valued at the remaining credits.

2.7.7 Compliance & Privacy Regulations

- **GDPR Compliance**: As a concept, LifetimeSafe is aligned with privacy-preserving operation by working within UnoLock's existing zero-knowledge architecture and minimizing the effect of future billing interruptions on Safe availability.

2.7.8 Integration with Other Features

- **LifeSafe**: Would work alongside LifetimeSafe for users who want strong deletion and deniability options while still prepaying future Safe coverage.

Back to Features Overview

2.8 Absolute Anonymity

2.8.1 Overview

Absolute Anonymity in UnoLock is the result of a broader design philosophy: reduce linkable identity, reduce linkable metadata, and avoid turning operational data into ownership data.

This is not one isolated feature. It is an **OPSEC-driven** platform design choice applied across:

- Safe access,
- storage architecture,
- Vault Messaging,
- payment handling,
- and metadata minimization.

The goal is simple: using UnoLock should not require building a usable identity profile around a particular Safe.

2.8.2 How It Works

- **No account-identity model**: UnoLock does not center Safe access around names, email addresses, usernames, or password-based accounts.
- **Access-key based Safe access**: access is controlled through registered access keys rather than a traditional identity-and-password login model.
- **Metadata minimization**: the platform is designed to reduce how much linkable operational data is created or retained.
- **Address-based messaging**: Vault Messaging uses Receive Addresses and compartmentalized message routing instead of global social or contact graphs.
- **Payment separation**: payment processing is kept separate from Safe identity so payment knowledge does not become Safe knowledge.
- **Minimal logging posture**: logging is kept intentionally narrow so operational telemetry does not become a user-tracking system.

2.8.3 Security Implications

- **Harder to profile**: reducing linkable metadata makes it harder to build relationship graphs around ownership, usage, or collaboration.
- **Lower-value records**: if systems are separated correctly, logs, payment records, and routing data reveal less about a specific Safe.
- **Defense beyond encryption**: encryption protects content, but anonymity also depends on limiting metadata, linkability, and operational correlation.

2.8.4 Use Cases

- **High-risk users**: journalists, activists, investigators, and others who need stronger protection against profiling and targeting.
- **Privacy-conscious users**: people who want secure storage and communication without feeding identity graphs.
- **Operational compartmentalization**: users who want payments, messaging, and Safe usage to stay separated instead of collapsing into one profile.

2.8.5 Why It Matters

Most systems leak identity through side channels long before content encryption matters. UnoLock is designed to resist that pattern. Absolute anonymity in UnoLock is really about making identity linkage operationally difficult by design, not just promising that data is encrypted.

2.8.6 FAQs

? Does UnoLock track any of my actions?

UnoLock is designed to minimize logging and linkable metadata rather than operate as a tracking platform. The goal is to avoid turning operational data into a user identity graph.

? Is this just about anonymous payments?

No. Payment separation is one part of the model, but absolute anonymity in UnoLock also includes access-key based Safe access, metadata minimization, and address-based messaging that avoids global identity graphs.

? Will any of my data be linked to my identity?

UnoLock is designed to avoid tying Safe access and normal platform use to personal identity fields like names, email addresses, or traditional accounts.

2.8.7 Compliance & Privacy Regulations

- **Privacy by design**: minimizing identity linkage and unnecessary metadata supports stronger privacy handling.
- **GDPR Alignment**: reducing unnecessary personal-data collection and linkage supports GDPR-style data-minimization principles.

2.8.8 Integration with Other Features

- **Payment Anonymity**: keeps payment records separated from Safe identity.
- **Vault Messaging**: reduces relationship-graph exposure through address-based encrypted messaging.
- **End-to-End Encryption (E2EE)**: protects message and protected API payload content while the anonymity model reduces metadata linkage.
- **DuressDecoy & Plausible Deniability**: help protect the user when anonymity pressure becomes coercion pressure.

2.9 Payment Anonymity

2.9.1 Overview

Payment Anonymity in UnoLock means the payment system is designed so UnoLock cannot link a payer or payment record to a particular Safe as part of normal operations.

This is not just about offering Bitcoin. It is about architectural separation:

- payment processing is kept separate from Safe cryptographic state,
- billing data is not used as a Safe identity layer,
- and UnoLock is designed so that payment knowledge does not become Safe knowledge.

This reflects a broader UnoLock design principle: **operational security (OPSEC)** underpins the user-protection philosophy applied throughout the platform.

2.9.2 How It Works

- **Billing isolation**: payment processing is kept separate from Safe content and Safe cryptographic material.
- **No payment-to-Safe linkage by design**: UnoLock is designed so a payment record cannot be used to determine which specific Safe it funded.
- **External card handling**: when a user pays through Stripe, the card and billing workflow are handled by the payment processor rather than being turned into internal Safe identity data.
- **Bitcoin support**: Bitcoin provides an additional privacy-preserving option for users who want stronger payment-side separation.
- **Privacy-focused metadata minimization**: the system avoids turning payment events into a map of Safe ownership.

2.9.3 Security Implications

- **Reduced coercion risk**: if payment data cannot be tied back to a specific Safe, payment records become less useful as an attack surface.
- **Lower profiling value**: separating billing from Safe identity makes it harder to build relationship graphs around ownership and usage.
- **Consistent OPSEC posture**: the same defensive thinking used for Safes, messaging, and metadata minimization is applied to payments.

2.9.4 Use Cases

- **Privacy-conscious users**: reduce the chance that a payment trail becomes a Safe trail.
- **High-risk users**: add another layer of operational separation so billing data is less useful to adversaries.
- **Bitcoin users**: pay with a privacy-preserving method while still benefiting from the same Safe-side isolation model.

2.9.5 Why It Matters

Many systems claim privacy while quietly turning billing records into an ownership index. UnoLock is designed to avoid that. Payment anonymity in UnoLock is really about preserving separation between financial events and Safe identity, which is a core part of the platform’s overall OPSEC-driven protection model.

2.9.6 FAQs

? **What does payment anonymity mean in UnoLock?**

It means the payment system is designed so UnoLock cannot link a payment record to a particular Safe during normal operation.

? **If I pay with Stripe, does UnoLock know which Safe I paid for?**

The system is designed to keep payment processing separate from Safe identity so UnoLock cannot map a payment record back to a specific Safe as a normal platform capability.

? **Is Bitcoin the only reason this feature exists?**

No. Bitcoin improves payment privacy, but the more important design point is architectural separation between payments and Safe identity.

2.9.7 Compliance & Privacy Regulations

- **Privacy by design**: minimizing payment-to-Safe linkage supports a data-minimization approach to financial privacy.
- **GDPR Compliance**: reducing unnecessary linkage between billing data and Safe identity supports stricter privacy handling.

2.9.8 Integration with Other Features

- **Absolute Anonymity**: extends UnoLock’s broader commitment to minimizing linkable identity and metadata.
- **Bitcoin Payment**: provides a privacy-preserving payment option within the same separation-first model.
- **Access Keys & Safe Access**: payment events are not meant to become another identity or ownership key for Safe access.

2.10 End-to-End Encryption

2.10.1 Overview

End-to-End Encryption (E2EE) in UnoLock protects data while it moves between intended endpoints so that intermediaries, including UnoLock infrastructure, do not get plaintext access.

This is related to, but not identical to, **client-side encryption**:

- **Client-side encryption** means the data is encrypted on your device before it leaves your device.
- **End-to-end encryption** means the encrypted data stays protected all the way to the intended recipient or endpoint.

UnoLock does **both**:

- Safe data is encrypted client-side before upload.
- Messaging payloads are end-to-end encrypted between the sending and receiving endpoints.
- API payloads are protected with end-to-end encrypted application-layer security in addition to transport security.

2.10.2 How It Works

- **Encryption starts on the client**: Safe data is encrypted on the client before upload, so plaintext is not handed to the server as part of normal storage flows.
- **Endpoint-only decryption**: for messaging and protected API exchanges, only the intended endpoints perform decryption of the protected payloads.
- **Transport protection still applies**: TLS 1.3 protects network transport, but it is not the whole security story. UnoLock also protects payloads above the transport layer.
- **Client-held key material**: cryptographic key material used for data protection stays under client control rather than being exposed to UnoLock as reusable plaintext secrets.
- **Access via WebAuthn, not passwords**: normal Safe access relies on WebAuthn-based access keys rather than passwords.

2.10.3 Security Implications

- **Protection from intermediaries**: end-to-end encryption reduces trust in the transport path and in service intermediaries because ciphertext remains protected between endpoints.
- **Server compromise resistance**: encrypted payloads and client-held key material limit what a server-side breach can expose.
- **Separation of concerns**: WebAuthn authenticates access, encryption protects data, and the PIN adds brute-force resistance and deniability controls. These are different layers, not one blended secret.

2.10.4 Use Cases

- **Safe storage**: personal or business records are encrypted client-side before being stored in UnoLock.
- **Vault Messaging**: messages and files exchanged through UnoLock are protected end-to-end between sender and recipient endpoints.
- **API use on hostile networks**: application-layer protection plus TLS helps preserve confidentiality even when the network path is untrusted.

2.10.5 Why It Matters

People often use "end-to-end encrypted" and "client-side encrypted" as if they mean the same thing. They do not. UnoLock uses both, and that matters because it gives stronger protection for stored data, messaging flows, and API communications without relying on passwords as the root of trust.

2.10.6 FAQs

Is UnoLock only client-side encrypted, or also end-to-end encrypted?

Both. Safe data is encrypted on the client before upload, and UnoLock also uses end-to-end encrypted protection for messaging and protected API payloads.

Does TLS by itself make something end-to-end encrypted?

No. TLS protects transport between network peers. End-to-end encryption means the payload remains protected all the way between the intended application endpoints.

Does UnoLock use passwords for normal Safe encryption?

No. Normal Safe access is based on WebAuthn access keys, not passwords. The main password-style exception is optional Space backup files, which are intended for controlled migration and are not the recommended default operating model.

2.10.7 Compliance & Privacy Regulations

- **GDPR & HIPAA**: client-side encryption and end-to-end encrypted payload protection help reduce unnecessary plaintext exposure of personal and sensitive data.

2.10.8 Integration with Other Features

- **Local File Encryption**: extends the client-side encryption model to portable encrypted files.
- **Vault Messaging**: applies end-to-end encrypted delivery to messages and files between endpoints.
- **Access Keys & Safe Access**: uses WebAuthn-based access keys for authentication rather than password-based Safe access.

2.11 LockoutGuard Access Assurance

2.11.1 Overview

LockOutGuard ensures that users can regain access to their UnoLock Safe even if they lose access to their primary authentication method, such as their FIDO2 device or biometric login. This feature provides multiple backup mechanisms and layers of protection to prevent accidental lockouts, enabling secure recovery while maintaining the integrity of the Safe.

LockoutGuard Access Assurance is a recovery and continuity feature designed to prevent permanent lockout from your UnoLock digital Safe. By providing a secure, user-controlled alternative recovery method, LockoutGuard ensures that users can regain access to their Safe in case of lost credentials or device issues, without compromising the zero-knowledge security model. In UnoLock, LockoutGuard is not a permanent parallel login path. It is a recovery path that is intended to be used, then replaced by fresh WebAuthn registration.

2.11.2 How It Works

- **Alternative Recovery Method Setup**: Users configure LockoutGuard as an alternative recovery path, such as an offline recovery code or related recovery material, stored securely by the user.
- **Encrypted Recovery Keys**: LockoutGuard generates encrypted recovery keys or mnemonic phrases, which are stored locally or on trusted devices, encrypted with AES-256 GCM, ensuring only the user can access them.
- **Inactivity Monitoring**: The system monitors user activity and can trigger recovery prompts after a user-defined inactivity period, guiding users to restore access securely.
- **Client-Side Recovery Process**: Recovery operations are processed client-side, maintaining UnoLock’s zero-knowledge architecture. Users authenticate using the configured recovery path to regain access without server intervention.
- **One-Time Recovery Flow**: After LockoutGuard is used, the user is required to register again with WebAuthn. The alternative recovery path is then removed, making LockoutGuard effectively a one-time recovery mechanism rather than a standing second login method.

2.11.3 Security Implications

- **Prevention of Permanent Lockout**: LockoutGuard ensures users can recover access to their Safe without relying on third-party intervention, reducing the risk of data loss.
- **Zero-Knowledge Security**: Recovery processes are handled client-side, ensuring that UnoLock servers never access user keys or data, maintaining privacy and security.
- **Controlled Recovery Lifecycle**: Recovery access is temporary. By forcing fresh WebAuthn registration after use, UnoLock restores the Safe to its normal primary-authentication model and removes the temporary recovery path.

2.11.4 Use Cases

- **Individual Users**: Protects access to personal Safes containing Bitcoin and Ethereum keys, financial records, or sensitive documents, ensuring recovery in case of lost credentials.
- **Business Continuity**: Companies can use LockoutGuard to ensure key personnel can recover access to critical data, maintaining operations despite credential issues.
- **High-Risk Scenarios**: Users in unstable environments can configure LockoutGuard to safeguard against coerced access attempts, using secure recovery options to regain control.

2.11.5 Why It Matters

Losing access to a digital Safe can result in permanent data loss, especially for critical assets like Bitcoin and Ethereum keys or legal documents. LockoutGuard provides a user-controlled, secure recovery mechanism that prevents such scenarios while upholding UnoLock’s commitment to privacy and security. As discussed in the context of secure key management, LockoutGuard ensures users can always regain access to their digital assets, offering peace of mind in an increasingly digital world.

2.11.6 FAQs

What happens if I lose my primary authentication method?

LockoutGuard allows you to use the configured recovery method to regain access. After that recovery succeeds, you must register again with WebAuthn, and the temporary recovery path is removed.

Can UnoLock access my recovery keys?

No, all recovery keys are encrypted and managed client-side, ensuring UnoLock has no access to them.

How does LockoutGuard protect against unauthorized recovery?

Recovery verification methods, like biometrics or FIDO2 authenticators, ensure only authorized users can initiate the recovery process.

Is LockoutGuard a permanent second way to log in?

No. LockoutGuard is an alternative recovery method, not a permanent parallel login method. Once it is used, UnoLock forces WebAuthn registration again and removes the alternative recovery path.

2.11.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: LockoutGuard supports compliance with GDPR, HIPAA, and other regulations by ensuring that recovery processes are secure, private, and do not expose sensitive data on servers.

2.11.8 Integration with Other Features

- **End-to-End Encryption (E2EE)**: Ensures that all recovery keys and data remain encrypted throughout the recovery process.
- **Access Keys & Safe Access**: LockoutGuard integrates with access-key based Safe access, allowing recovery methods to coexist with multiple registered authenticators.

2.12 Digital Paper Wallet

2.12.1 Overview

Digital Paper Wallet (DPW) is an impregnable fortress for your cryptocurrency (BTC, ETH, ERC-20) keys, empowering Sovereign and HighRisk tier users to generate, encrypt, and store private keys with cold-like storage-like security without the risk of loss that cold wallets have, exporting them as BIP-39 mnemonic seed phrases via the coercion-resistant Key Extraction Protocol (KEX) when needed. Designed exclusively for secure key management, DPW does not transact or hold keys, enabling seamless transfer to transaction wallets like Ledger or MetaMask for spending. Available only in Sovereign and HighRisk tiers, DPW ensures your Bitcoin and Ethereum assets remain under your sole, unassailable control.

2.12.2 How It Works

- **Offline Key Generation**: Sovereign and HighRisk tier users generate private and public key pairs for Bitcoin and Ethereum offline-like in their browser, ensuring no third-party access, including UnoLock.
- **Client-Side Encryption**: Keys are encrypted on the user’s device with **AES-256 GCM**, stored securely in the Safe, and backed up to AWS S3 with pre-signed URLs, remaining unreadable without the decryption key.
- **BIP-39 Mnemonic Export via KEX**: Keys are exported as 24-word BIP-39 mnemonic seed phrases using the **Key Extraction Protocol (KEX)**, splitting phrases across two offline devices with optional multi-device authentication and self-destructing sessions for secure transfer to transaction wallets.
- **Cold-like Storage-Like Security**: Encrypted keys are stored in a state of the art Safe environment, mirroring cold storage principles with extreme loss prevention techniques, ensuring protection from online threats without transaction capabilities.

2.12.3 Security Implications

- **Zero-Knowledge Sovereignty**: Client-side key generation and encryption ensure only you access your private keys, with UnoLock maintaining a zero-knowledge model, eliminating custodial risks.
- **Coercion Resistance**: KEX’s split-device mnemonic retrieval, paired with DuressDecoy (Sovereign) and LifeSafe (HighRisk), protects keys against physical or legal coercion, ensuring attacker deception.
- **Cold-like Storage Resilience**: Offline-like key management and encrypted storage shield keys from online threats like phishing or malware, providing cold-like storage security with digital flexibility.

2.12.4 Use Cases

- **Crypto Investors**: Sovereign and HighRisk tier users generate Bitcoin or Ethereum keys offline-like, exporting mnemonics via KEX to Ledger or MetaMask for secure trading or long-term storage.
- **High-Security Asset Management**: HighRisk tier users export Ethereum keys to MetaMask via KEX, protected by LifeSafe against coercion in high-risk scenarios.
- **Enterprise Bitcoin and Ethereum Protection**: Sovereign tier businesses generate and store corporate Bitcoin and Ethereum keys, using KEX to securely integrate with hardware wallets, ensuring robust security for financial operations.

2.12.5 Why It Matters

Digital Paper Wallet redefines cryptocurrency (BTC, ETH, ERC-20) security by offering Sovereign and HighRisk tier users a cold-like storage-like Safe for key management, with secure KEX export to transaction wallets, ensuring self-sovereign control. In a world of cyber threats and physical risks, DPW’s zero-knowledge design safeguards your digital wealth with unmatched resilience.

2.12.6 FAQs

? Can UnoLock access my DPW private keys?

No, DPW’s zero-knowledge model ensures keys are generated and encrypted client-side, inaccessible to UnoLock or any third party.

? How does KEX secure mnemonic export?

KEX splits BIP-39 mnemonics across two offline devices with optional multi-device authentication and self-destructing sessions, preventing exposure to coercion, keyloggers, or malware.

? Can DPW be used for cryptocurrency (BTC, ETH, ERC-20) transactions?

No, DPW is designed for secure key generation and storage, not transactions; keys are exported via KEX to transaction wallets like Ledger or MetaMask for spending.

2.12.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: DPW supports GDPR and HIPAA by encrypting keys client-side, ensuring user privacy and control during storage and export in Sovereign and HighRisk tiers.

2.12.8 Integration with Other Features

- **Local File Encryption**: Complements DPW by encrypting keys client-side with AES-256 GCM, ensuring robust protection during storage and backup.
- **Post-Quantum Encryption Security**: Enhances DPW with quantum-resistant AES-256 GCM encryption, safeguarding keys against future quantum threats.

Back to Features Overview

2.13 SeedSafe

2.13.1 Overview

SeedSafe provides a specialized, high-security Safe for backing up existing BIP-39 mnemonic seed phrases from any standard wallet. Built on UnoLock's zero-knowledge architecture, it offers military-grade protection for your most critical cryptocurrency recovery keys without any active wallet functionalities. Designed purely for secure storage and recovery, SeedSafe ensures your seed phrases remain completely inaccessible to UnoLock servers while providing resilient cloud backup capabilities.

2.13.2 How It Works

- **Split-Entry Protocol**: Enter your mnemonic in two halves (e.g., words 1-12 and 13-24) to mitigate single-device compromise risks, with support for 12, 18, and 24-word phrases validated against canonical BIP-39 wordlists in real-time.
- **Cryptographic Verification**: Client performs full BIP-39 checksum verification after both halves are entered, guaranteeing mathematical validity and error-free entry.
- **Independent Encryption**: Each mnemonic half is encrypted separately using AES-256-GCM with your Client Data Master Key (CDMK), creating two distinct ciphertext records.
- **Zero-Knowledge Storage**: Encrypted halves stored as opaque records within your Space, with servers having zero knowledge of content type or relationship between records.
- **Authenticated Split-Retrieval**: Recovery requires full authentication to decrypt either half independently or both together, enabling secure two-device recovery that prevents full reconstruction on any single endpoint.

2.13.3 Security Implications

- **Distributed Trust Model**: Split-entry and split-storage architecture ensures no single compromised device or session can expose your complete seed phrase.
- **Server-Blind Architecture**: UnoLock servers handle only encrypted ciphertexts with no metadata revealing mnemonic content, maintaining absolute zero-knowledge guarantees.
- **Multi-Device Recovery**: Independent decryption of halves allows recovery across two trusted devices, preventing single-point-of-failure scenarios.

2.13.4 Use Cases

- **Hardware Wallet Backup**: Store Ledger or Trezor recovery phrases with bank-vault security while maintaining cloud resilience against physical loss.
- **Exchange Wallet Protection**: Secure backup for MetaMask, Trust Wallet, or other software wallet mnemonics without exposing them to online threats.
- **Multi-Wallet Management**: Safely store multiple seed phrases from different wallets in isolated, encrypted Safes with granular access control.

2.13.5 Why It Matters

SeedSafe transforms the dangerous practice of physical seed phrase storage into a cryptographically secure digital solution. By combining split-entry protocols with zero-knowledge encryption, it eliminates the traditional trade-off between security and accessibility, ensuring your recovery keys remain both utterly inaccessible to attackers and reliably available when needed.

2.13.6 FAQs

Can UnoLock access my stored seed phrases?

No, SeedSafe's zero-knowledge architecture ensures seed phrases are encrypted client-side before transmission. UnoLock servers only store encrypted ciphertexts without any ability to decrypt or relate the stored halves.

What happens if I lose access to one device during split-device entry?

You can still complete the entry on a single trusted device. The split-device option provides enhanced security but isn't mandatory for storage or retrieval.

Is SeedSafe compatible with all wallet types?

SeedSafe supports all standard BIP-39 compliant wallets with 12, 18, or 24-word mnemonic phrases, covering virtually all modern cryptocurrency wallets.

2.13.7 Compliance & Privacy Regulations

- **GDPR & Privacy Compliance**: SeedSafe maintains complete data sovereignty through client-side encryption, ensuring compliance with GDPR's data protection principles.
- **Zero-Knowledge Guarantee**: Server infrastructure cannot access, decrypt, or correlate stored mnemonic data, exceeding standard compliance requirements.

2.13.8 Integration with Other Features

- **Post-Quantum Encryption Security**: Leverages quantum-resistant AES-256 GCM encryption to protect seed phrases against future cryptographic threats.
- **Spaces**: Enables isolated storage environments for organizing multiple seed phrases with distinct access controls and security policies.

Back to Features Overview

2.14 DPW VaultSign

2.14.1 Overview

DPW VaultSign governs the controlled execution of cryptocurrency transactions within UnoLock's Digital Paper Wallet ecosystem. This feature provides a hardened, zero-knowledge process that ensures private keys never leave the client browser sandbox and never persist beyond active signing operations. By coupling multi-layered decryption with an air-gapped broadcasting model, VaultSign guarantees that funds cannot be exfiltrated even in scenarios involving fully compromised servers or applications.

2.14.2 How It Works

- **Four-Layer Decryption Protocol**: Access requires reversing DPW's encryption layers with explicit user consent at each stage - wallet document decryption, server envelope removal, authentication-bound release, and in-memory reconstruction.
- **Browser Sandbox Execution**: All signing operations occur within the hardened browser environment, protected by Content Security Policy (CSP) enforcement and runtime memory purging.
- **Balance Inquiry**: Submit only public addresses to UnoLock's API for blockchain queries, with private keys never requested or exposed during balance checks.
- **Raw Transaction Generation**: Users with appropriate permissions generate raw signed transactions entirely within their Safe's secure environment.
- **Air-Gapped Broadcasting**: Signed transactions are intentionally not broadcast by UnoLock, requiring manual submission through independent third-party services to create a functional air-gap against unauthorized transmission.

2.14.3 Security Implications

- **Memory-Only Key Exposure**: Private keys exist solely in volatile memory during signing operations, with immediate purging preventing any persistent exposure.
- **Multi-Factor Authentication Chain**: Each decryption layer requires distinct authentication ceremonies, creating defense-in-depth against compromise.
- **Broadcast Isolation**: The air-gap between signing and broadcasting ensures no automated path for fund exfiltration, even with complete infrastructure compromise.

2.14.4 Use Cases

- **High-Value Transaction Signing**: Execute large cryptocurrency transfers with bank-vault security, ensuring keys remain protected throughout the signing process.
- **Multi-Signature Coordination**: Generate signed transactions for multi-sig wallets, with each participant using their own VaultSign instance for maximum security.
- **Institutional Asset Management**: Enterprise users leverage VaultSign for corporate treasury operations, maintaining audit trails while ensuring key security.

2.14.5 Why It Matters

DPW VaultSign represents the pinnacle of secure transaction execution, combining the convenience of digital signing with security guarantees that exceed even hardware wallets. By enforcing strict separation between key access, transaction signing, and broadcast mechanisms, VaultSign ensures that your cryptocurrency assets remain under absolute control even in adversarial scenarios.

2.14.6 FAQs

❓ **Why doesn't UnoLock broadcast transactions directly?**

The air-gap design is a critical security feature. By requiring manual broadcast through external services, we ensure that even a fully compromised UnoLock system cannot autonomously move your funds.

❓ **How long are keys held in memory during signing?**

Keys exist in memory only for the milliseconds required to sign the transaction. Immediately after signing, all key material is cryptographically wiped from memory.

❓ **Can signing operations be performed offline?**

While the UnoLock interface requires connectivity, the actual signing occurs entirely client-side. Keys never traverse the network during signing operations.

2.14.7 Compliance & Privacy Regulations

- **Regulatory Compliance**: VaultSign's audit trail capabilities support compliance requirements while maintaining zero-knowledge privacy guarantees.
- **Transaction Privacy**: Raw transaction generation ensures complete control over what information is shared with blockchain networks.

2.14.8 Integration with Other Features

- **Digital Paper Wallet**: VaultSign operates exclusively on DPW-generated keys, leveraging the full security architecture of the DPW ecosystem.
- **Spaces**: Transaction signing permissions can be segregated across different Spaces, enabling role-based access control for organizational use.

Back to Features Overview

2.15 DPW Portability

2.15.1 Overview

DPW Portability extends UnoLock's Digital Paper Wallet architecture by enabling secure migration of mnemonics between Spaces within a Safe, or across different Safes entirely. This feature provides unparalleled flexibility for cryptocurrency key management without compromising sovereignty, ensuring that DPWs generated within UnoLock can be reused, shared, or redundantly stored in other controlled contexts without ever exposing plaintext seeds.

2.15.2 How It Works

- **Split-Entry Import Protocol**: Import DPW mnemonics in two halves with real-time BIP-39 validation, optionally using separate trusted devices to mitigate endpoint compromise.
- **Authentication-Bound Encryption**: Each mnemonic half is independently encrypted using AES-256-GCM, bound to fresh FIDO2/WebAuthn ceremonies for phishing-resistant security.
- **Zero-Knowledge Migration**: Encrypted halves transfer as opaque ciphertexts between Safes, with servers handling only encrypted data and no metadata revealing content type.
- **Authenticated Split-Retrieval**: Reconstruction requires separate WebAuthn ceremonies for each half, enforcing distributed trust where no single session can expose the full seed.
- **Cross-Context Flexibility**: Seamlessly move DPWs between personal and organizational Safes, or distribute across multiple Spaces with granular access controls.

2.15.3 Security Implications

- **Transit Security**: Mnemonics remain encrypted throughout migration, with zero-knowledge guarantees maintained across Safe boundaries.
- **Consent-Based Transfer**: Every import, export, or reconstruction requires explicit FIDO2/WebAuthn verification, preventing silent or automated migrations.
- **Distributed Trust Architecture**: Split-storage across Safes enables multi-party custody scenarios without requiring key sharing or compromise.

2.15.4 Use Cases

- **Cross-Space Import**: Migrate DPWs between Spaces for granular access control, enabling admin rights in one Space while maintaining read-only access in another.
- **Cross-Safe Portability**: Import the same DPW into personal and organizational Safes, ensuring business continuity without breaking security boundaries.
- **Inheritance Planning**: Copy DPWs into designated LegacyLink Safes for estate planning, maintaining survivability without key exposure.
- **Shared Custody**: Distribute encrypted halves across Safes controlled by different trustees, providing multi-party assurance for high-value assets.

2.15.5 Why It Matters

DPW Portability solves the critical challenge of key management flexibility in cryptocurrency custody. By enabling secure migration and distribution of DPWs across multiple contexts, it provides the redundancy and accessibility needed for real-world asset management while maintaining the uncompromising security standards that define UnoLock's zero-knowledge architecture.

2.15.6 FAQs

Can migrated DPWs be traced between Safes?

No, each Safe operates independently with no correlation possible between encrypted records. Servers cannot determine that the same DPW exists in multiple locations.

What happens if migration is interrupted?

The atomic nature of the migration ensures that incomplete transfers leave no partial data. You can safely retry the migration without risk of corruption or exposure.

Can I limit who can import my DPW?

Yes, import operations require both the encrypted DPW data and appropriate Safe permissions. You maintain complete control over distribution and access rights.

2.15.7 Compliance & Privacy Regulations

- **Data Portability Compliance**: Satisfies GDPR Article 20 requirements for data portability while maintaining encryption throughout the transfer process.
- **Custody Chain Documentation**: Migration events create auditable logs without exposing key material, supporting compliance and governance requirements.

2.15.8 Integration with Other Features

- **SeedSafe Architecture**: Leverages SeedSafe's split-entry and authenticated retrieval mechanisms for consistent security across all mnemonic operations.
- **LegacyLink**: Enables seamless integration with inheritance planning by allowing DPW copies in designated successor Safes.
- **Spaces**: Provides granular control over DPW access across different organizational contexts within the same Safe.

Back to Features Overview

2.16 DuressDecoy: Protection Against Coercion

2.16.1 Overview

DuressDecoy: Protection Against Coercion is a safeword-PIN behavior for Spaces that a user has marked as sensitive. When the safeword PIN is entered, those sensitive Spaces are either hidden or deleted, depending on the tier. The PIN is received by the server and the feature is applied server-side so a compromised device does not reveal, through different local behavior, that a safeword PIN was entered instead of the normal access PIN.

2.16.2 How It Works

- **Sensitive Spaces Selection**: The user marks selected Spaces as sensitive.
- **Safeword PIN Entry**: The user enters the safeword PIN instead of the normal PIN.
- **Server-Side Handling**: The entered PIN is sent to the server, which applies the duress behavior there rather than relying on the local device to do something observably different.
- **Tier-Dependent Outcome**: Sensitive Spaces are then either hidden or deleted, depending on the tier.
- **Scoped Behavior**: The feature applies to the Spaces marked as sensitive. It is not a silent-alert system and it does not open a separate decoy Safe.

2.16.3 Security Implications

- **Protection for Sensitive Spaces**: The feature helps protect selected Spaces when a user needs to open the Safe under pressure.
- **Plausible Deniability on a Compromised Device**: Because the server receives the PIN and applies the outcome server-side, an adversary watching the compromised device should not be able to tell from local behavior whether the normal PIN or safeword PIN was entered.
- **Simple Duress Response**: The safeword PIN directly affects only the Spaces marked as sensitive.
- **Tier-Specific Severity**: Depending on the tier, the result is either concealment or deletion of those sensitive Spaces.

2.16.4 Use Cases

- **Checkpoint or Search Scenarios**: A user can enter the safeword PIN if they are being pressured to open the Safe and want sensitive Spaces protected.
- **Personal Safety Situations**: Sensitive records can be hidden or deleted rather than exposed during a coercive interaction.
- **Compartmentalized Protection**: Users can decide in advance which Spaces should be treated as sensitive if the safeword PIN is ever used.
- **Shared Space Caution**: If a sensitive Space is also a Shared Space, ownership matters for whether deletion affects every participating Safe or only one Safe loses access.

2.16.5 Why It Matters

DuressDecoy keeps the coercion response simple and focused. By tying the safeword PIN to Spaces marked as sensitive, UnoLock lets users predefine what should be concealed or removed if they are forced to open the Safe under pressure.

2.16.6 FAQs

? How does DuressDecoy differ from LifeSafe?

DuressDecoy acts on Spaces marked as sensitive when the safeword PIN is entered. Depending on the tier, those Spaces are hidden or deleted.

Can UnoLock detect when I use the duress PIN?

The server receives the entered PIN and applies the DuressDecoy behavior server-side. That is necessary so a compromised device does not visibly behave differently when the safeword PIN is used.

What if I accidentally trigger the duress PIN?

The effect depends on the tier because sensitive Spaces are either hidden or deleted when the safeword PIN is used.

What if the sensitive Space is a Shared Space?

Ownership matters. If the owner Safe deletes the Shared Space, it is deleted for every participating Safe. If a non-owner Safe loses access to the Shared Space, the data remains for the owner and other participants.

2.16.7 Compliance & Privacy Regulations

- **Plausible-Deniability-Oriented Processing**: DuressDecoy is implemented so the server can apply the safeword outcome without exposing a distinct local signal on a compromised device.

2.16.8 Integration with Other Features

- **Spaces**: DuressDecoy applies to Spaces that the user has marked as sensitive.
- **PIN Code**: The feature is activated through the safeword PIN rather than the normal Safe PIN.

Back to Security Overview

2.17 LifeSafe

2.17.1 Overview

LifeSafe is the HighRisk-tier safeword behavior for Spaces that a user has marked as sensitive. When the safeword PIN is entered, those sensitive Spaces are deleted. The PIN is received by the server and the feature is applied server-side so a compromised device does not reveal, through different local behavior, that the safeword PIN was used instead of the normal access PIN.

2.17.2 How It Works

- **Sensitive Spaces Selection**: Users mark selected Spaces as sensitive.
- **Safeword PIN**: Users set a safeword PIN distinct from the normal Safe PIN.
- **Server-Side Handling**: The entered PIN is sent to the server, which applies the deletion behavior there so the compromised device does not expose a distinct local signal.
- **Sensitive Space Deletion**: When the safeword PIN is used, the Spaces marked as sensitive are deleted.
- **HighRisk Scope**: This deletion behavior is the HighRisk-tier version of the safeword response.

2.17.3 Security Implications

- **Protection for Sensitive Spaces**: LifeSafe helps protect selected Spaces when a user must open the Safe under pressure.
- **Plausible Deniability on a Compromised Device**: Because the server applies the outcome, an adversary watching the device should not be able to distinguish safeword entry from normal PIN entry through local behavior.
- **Irreversible Tradeoff**: In HighRisk, the marked Spaces are deleted rather than hidden.

2.17.4 Use Cases

- **High-Risk Operatives**: Whistleblowers or activists can delete selected sensitive Spaces under threat.
- **Cryptocurrency Security**: Investors can protect particularly sensitive wallet material if their threat model justifies deletion.
- **Corporate Data Protection**: Executives can mark critical Spaces as sensitive and have them deleted if coerced.
- **Shared Space Caution**: If a marked sensitive Space is also a Shared Space, the result depends on whether the acting Safe is the owner.

2.17.5 Why It Matters

LifeSafe is the irreversible version of UnoLock's safeword response. It exists for users whose threat model calls for deletion of selected sensitive Spaces rather than merely hiding them.

2.17.6 FAQs

❓ **Can any data be recovered after LifeSafe is triggered?**

The Spaces marked as sensitive are intended to be deleted when the safeword PIN is used.

❓ **How does LifeSafe differ from Duress Decoy?**

LifeSafe deletes selected sensitive Spaces. DuressDecoy hides selected sensitive Spaces instead.

? Is the LifeSafe safeword PIN secure from attackers?

The server receives the entered PIN and applies the LifeSafe behavior server-side so the compromised device does not visibly branch when the safeword PIN is used.

? What if a sensitive Space is also a Shared Space?

If the owner Safe deletes the Shared Space, it is deleted for every participating Safe. If a non-owner Safe loses access to that Shared Space, the data remains for the owner and other participants.

2.17.7 Compliance & Privacy Regulations

- **Privacy-Preserving Operation**: LifeSafe is implemented to support plausible deniability without exposing a distinct local signal on a compromised device.

2.17.8 Integration with Other Features

- **Spaces**: LifeSafe applies to Spaces that the user has marked as sensitive.
- **PIN Code**: The feature is activated through the safeword PIN rather than the normal Safe PIN.

Back to Features Overview

2.18 LegacyLink Inheritance

2.18.1 Overview

LegacyLink Inheritance is UnoLock's succession-oriented recovery path for a Safe. A user configures it in connection with LockoutGuard, sets a delay, and generates a dormant LegacyLink credential that can be stored or given to a trusted person. If the configured inactivity conditions are later met, that credential can be used to take custody of the Safe, register a new access key, and continue from UnoLock's normal access-key model. It is best understood as a one-time succession or recovery path, not as a permanent second login method.

2.18.2 How It Works

- **Configured from LockoutGuard**: LegacyLink is set up through the LockoutGuard area and depends on that inactivity-based continuity model.
- **Delayed Activation**: The user chooses a delay that applies after LockoutGuard has been triggered.
- **Dormant Credential**: Setup generates a LegacyLink credential, including an access ID and passphrase, which stays dormant until the configured conditions are met.
- **Stored Outside Daily Access**: That credential can be printed, saved, or handed to a trusted person for future use if succession or recovery becomes necessary.
- **One-Time Recovery or Succession Flow**: When the conditions are met, the LegacyLink credential is used to begin recovery of the Safe.
- **New Access Key Required**: The recovering person must register a new access key and set a new PIN before continuing normal Safe access.
- **Temporary Path Is Removed After Use**: Once LegacyLink has been used, the old dormant credential is no longer the ongoing access method. If future succession coverage is still wanted, it should be configured again.

2.18.3 Security Implications

- **No Immediate Secondary Access**: LegacyLink does not create a standing second login path for everyday use.
- **Bound to Inactivity Conditions**: The dormant credential is intended to become useful only when the configured inactivity path has been triggered.
- **One-Time Transition**: After the credential is used, access is moved back into UnoLock's normal access-key model with a newly registered key.
- **Zero-Knowledge Model Remains**: LegacyLink fits within UnoLock's client-side and zero-knowledge security model rather than bypassing it.

2.18.4 Use Cases

- **Family Succession Planning**: A user can prepare a trusted person to recover the Safe if the owner is gone or permanently unable to access it.
- **Emergency Continuity**: Important records can remain recoverable after prolonged inactivity without turning LegacyLink into a normal everyday login path.
- **Single-Safe Handover**: LegacyLink can support a planned transfer of custody for the Safe itself rather than day-to-day multi-user collaboration.

2.18.5 Why It Matters

LegacyLink addresses a difficult continuity problem: how to make a Safe recoverable by a successor after prolonged inactivity without weakening UnoLock into a permanent alternative-login system. It provides a bounded succession path and then returns the Safe to the standard access-key model.

2.18.6 FAQs

Does LegacyLink give someone a permanent second way into my Safe?

No. LegacyLink is a one-time succession or recovery path, not a permanent parallel login method.

What do I store during LegacyLink setup?

LegacyLink setup generates a dormant credential that includes an access ID and passphrase, along with a QR code representation for storage or transfer.

What happens when LegacyLink is used?

The recovering person uses the LegacyLink credential to begin the recovery flow, then registers a new access key and sets a new PIN for ongoing use.

What happens after the Safe has been recovered through LegacyLink?

The temporary LegacyLink path is no longer the ongoing access method. If continued succession coverage is needed, it should be configured again.

2.18.7 Compliance & Privacy Regulations

- **Privacy-Preserving Operation**: LegacyLink is designed to support succession and recovery without changing UnoLock's underlying zero-knowledge privacy model.

2.18.8 Integration with Other Features

- **LockoutGuard**: LegacyLink is configured through the LockoutGuard flow and depends on its inactivity-triggered continuity model.
- **Access Keys**: After LegacyLink recovery, the Safe returns to the standard access-key model by registering a new key.

2.19 TimeLock

2.19.1 Overview

TimeLock is a simple time-based lock for an individual access key. A user sets it when closing their Safe, usually for a selected number of hours, so that specific key cannot be used to open the same Safe until the time expires. It is intended for short, uncomfortable situations, such as going through security checkpoints or other moments when a device might be temporarily at risk. TimeLock is available in all tiers.

2.19.2 How It Works

- **Per-Key Only**: TimeLock applies to a single access key. It does not lock the entire Safe.
- **Set When Closing the Safe**: A user enables TimeLock as they close the Safe if they expect to be in a vulnerable situation for a while.
- **Fixed Short Duration**: The lock is set for some number of hours, during which that key cannot reopen the Safe.
- **Automatic Expiry**: Once the selected time has passed, the key becomes usable again.
- **Separate from Key Management**: TimeLock does not disable or revoke a key. If a user wants to disable an access key, they should use UnoLock's key management features instead.

2.19.3 Security Implications

- **Short-Term Protection**: TimeLock helps reduce the risk of someone using a key during a brief period when the user's device may be exposed or under pressure.
- **Useful Under Coercion or Inspection**: A time-locked key cannot immediately reopen the Safe, which can help in situations like checkpoints or other uncomfortable encounters.
- **Narrow Scope by Design**: Because TimeLock affects only one key, it provides a focused delay mechanism without changing the Safe's broader key-management setup.

2.19.4 Use Cases

- **Security Checkpoints**: Lock the access key for a few hours before going through airport security, border control, or similar inspections.
- **Temporary Device Exposure**: Add a delay when carrying a device through an environment where access pressure or opportunistic compromise is a concern.
- **Short-Term Personal Safety**: Close the Safe with a time lock before entering a situation where immediate access to the Safe should not be possible from that device.

2.19.5 Why It Matters

TimeLock is intentionally simple. It gives users a way to make one access key temporarily unusable for a short period, much like the time lock on a physical safe. That can be enough to get through a risky window without changing the rest of the Safe's configuration.

2.19.6 FAQs

Can I access my Safe while TimeLock is active?

TimeLock only affects the specific key that was time-locked. It does not lock the entire Safe.

What happens if I lose a device with a TimeLocked key?

TimeLock does not disable the key. If you need to disable or revoke an access key, use UnoLock's key management features.

Can I change the TimeLock period after activation?

TimeLock is meant to cover a selected number of hours after the Safe is closed. During that time, the affected key remains unusable until the time expires.

Does TimeLock work on all tiers?

Yes. TimeLock is available in all tiers.

2.19.7 Compliance & Privacy Regulations

- **Privacy-Preserving Operation**: TimeLock adds a temporary access delay to a key without changing UnoLock's underlying privacy and encryption model.

2.19.8 Integration with Other Features

- **Access Keys & Safe Access**: TimeLock applies at the access-key level, so it works naturally alongside UnoLock's multi-key access model.
- **Key Management**: If a key needs to be disabled or revoked, that should be handled through key management rather than TimeLock.

Back to Features Overview

2.20 Vault Messaging

2.20.1 Overview

Vault Messaging is Unolock’s secure data-movement system for address-based exchange. It is **not a chat app**. Messages move between cryptographic endpoints, not identities. Unlike conventional “private” messengers that stop at content encryption, Vault Messaging minimizes metadata that can be used to construct relationship graphs over time.

- **Receive Address**: a shareable address with its own keypair and policy controls.
- **UnoLock Drop**: the anonymous sender client for Receive Addresses.
- **Known Addresses**: a local address book (saved addresses + names) inside your Safe.

Unolock lets Safe owners create multiple independent Receive Addresses, each acting as a separate compartment for intake. Addresses are isolated from one another and are not tied to identities, inboxes, or accounts. Each address can be configured with its own limits—attachments, usage count, and throttling—so you can control exposure, reduce abuse, and limit correlation. If an address is leaked or abused, it can be disabled or discarded without impacting other addresses.

2.20.2 How It Works

- **Address-based sending**: messages and files are sent to a Safe through an address, not to a global identity.
- **Client-side hashing**: Receive Addresses are hashed on the client and sent as `vaultxAddressHash`.
- **Per-address keys**: each Receive Address has its own keypair, limiting blast radius.
- **Address policies**: set usage limits, throttling, and attachment permissions per Receive Address.
- **Address authenticity hint**: set a sender message (code word) so senders can confirm they reached the intended Receive Address.
- **Policy enforcement**: limits are enforced server-side and reflected in the client before send.
- **Reply-only addresses**: replies are bound to a specific sender to prevent reuse.
- **Anonymous intake**: external senders can use the UnoLock Drop client to message a Receive Address without creating a Safe.

2.20.3 Security Implications

- **Zero-knowledge routing**: the server routes encrypted payloads and sees only hashed Receive Addresses.
- **Post-quantum ready**: messages use ML-KEM-1024 for key encapsulation and AES-256-GCM for payload encryption.
- **Compartmentalization**: per-address keys prevent one leaked key from exposing other conversations.
- **Metadata hardening**: outbox destination addresses are encrypted at rest; receive-side linkage is hashed.

2.20.4 Use Cases

- **Secure coordination**: exchange sensitive files and messages between Safes without exposing a global identity.
- **Anonymous intake**: publish a Receive Address for tips or disclosures via UnoLock Drop.
- **One-off communications**: create short-lived addresses with strict limits for high-risk interactions.

2.20.5 Why It Matters

Most messaging tools protect content but not anonymity, exposing relationships. Vault Messaging is built to eliminate those relationship graphs by default. By making addresses disposable, policy-driven, and compartmentalized, you can move messages and files between Safes without building a map of real-world relationships.

2.20.6 Tiering Summary

- **Sovereign / HighRisk**: create and manage Receive Addresses with policies.
- **Free / Inheritance**: receive messages and reply using bound reply-only addresses; cannot create new Receive Addresses.

2.20.7 FAQs

? **Do senders need a Safe account?**

No. The UnoLock Drop client lets anyone send to a Receive Address without creating a Safe. https://drop.unolock.com

? **Can I revoke a Receive Address?**

Yes. You can disable or delete a Receive Address at any time to stop new messages.

2.20.8 Compliance & Privacy Regulations

- **GDPR Alignment**: Vault Messaging avoids storing raw destination addresses and keeps message contents client-side encrypted.

2.20.9 Integration with Other Features

- **Post-Quantum Encryption**: ML-KEM-1024 + AES-256-GCM protect messages against future cryptographic threats.
- **Threat Detection**: Runtime monitoring helps detect tampering during sensitive messaging flows.

Back to Features Overview

2.21 UnoLock Spaces

2.21.1 Overview

Spaces let you organize information inside your Safe into separate compartments. A Space can be used for personal records, business material, family planning, project data, or any other category you want to keep isolated from the rest of your Safe.

Spaces now support **two different access models**, and they are not the same:

- **Access keys for the same Safe**: multiple users can have their own access key, such as a passkey or hardware-backed key, and those keys can be granted either limited access to selected Spaces or full administrative access to the Safe.
- **Shared Spaces between Safes**: a Space can be shared with another Safe so both Safes can collaborate on the same records and cloud files.

That distinction matters:

- **Access keys** mean more than one user can have their own access key and open parts of **one Safe**.
- **Shared Spaces** mean two or more **separate Safes** can work together in the same Space without sharing the rest of their data.

2.21.2 How It Works

- **Private Spaces** keep records separated inside one Safe.
- **Access-key allocation** lets the Safe owner decide whether a specific access key has limited access to selected Spaces or full administrative rights to the Safe.
- **Shared Spaces** let a Safe owner create a collaboration Space and send an invite to another Safe through **Vault Messaging**.
- **Per-Space encryption** keeps each Space logically separated from the others.

2.21.3 Two Ways to Collaborate

1. Sharing access inside the same Safe

This is the original model:

- You stay within **one Safe**.
- You register additional **access keys** for that Safe.
- You choose which Spaces those keys can open.

This is useful for:

- Adding another access key for yourself, such as a passkey or hardware-backed key on another device.
- Giving a family member or teammate their own access key for selected Spaces in the **same Safe**.
- Giving a trusted administrator full Safe access through their own access key.
- Separating limited-access and full-admin roles within one Safe.

See **Granting an Access Key Access to Spaces in the Same Safe**.

2. Sharing a Space between separate Safes

This is the new collaboration model:

- Each person keeps their **own Safe**.
- A Space owner creates a **Shared Space**.
- The owner sends a **Vault Messaging** invite to another Safe.
- The recipient imports the invite and gains access to that shared collaboration space only.

This is useful for:

- Team collaboration between separate Safes.
- Secure family coordination without merging Safes.
- Sharing one project workspace while keeping the rest of each Safe private.
- Ownership-based deletion, where the owner can delete the Shared Space for every participant, while a non-owner can only remove that Shared Space from their own Safe.

See **Shared Spaces** and **Sharing a Space Between Safes**.

2.21.4 Security Implications

- **Compartmentalization**: each Space remains separate from the rest of your Safe.
- **Selective exposure**: sharing a Space does not share the rest of your Safe.
- **Collaboration without Safe merging**: Shared Spaces allow cooperation while preserving Safe-level separation.
- **Owner-controlled shared deletion**: if the owner deletes a Shared Space, it is deleted for all participating Safes; if a non-owner deletes it, only that Safe loses access.
- **Key-scoped access**: same-Safe access keys can be limited to specific Spaces or elevated to full Safe administration.
- **Multi-user same-Safe access**: multiple people can share one Safe when each person has their own access key and only the Spaces intended for them.

2.21.5 Use Cases

- **Personal and work separation**: keep business records apart from personal material.
- **Family organization**: use one Space for estate planning, another for household records.
- **Same-Safe delegated access**: allow a trusted person to use their own access key to open only selected Spaces in one Safe.
- **Cross-Safe collaboration**: share one project Space with another Safe while keeping all other Spaces private.

2.21.6 Why It Matters

Spaces are not just folders. They are a control layer for privacy, organization, and collaboration. They let you decide whether you want:

- compartmentalization inside one Safe,
- limited access through selected access keys,
- or collaboration between entirely separate Safes.

That makes Spaces useful for both personal security and operational teamwork.

2.21.7 FAQs

? Does sharing a Space mean sharing my whole Safe?

No. A Shared Space exposes only that collaboration Space, not the rest of your Safe.

? Are access keys and Shared Spaces the same thing?

No. Access keys apply to one Safe. Shared Spaces connect separate Safes to the same collaboration area.

When should I use access keys instead of a Shared Space?

Use access keys when multiple users should have their own access key to the same Safe, either with limited access to selected Spaces or with full administrative rights. Use a Shared Space when different people should keep separate Safes but collaborate in one Space.

What happens if a Shared Space is deleted?

If the owner deletes it, it is deleted for every participating Safe. If a non-owner deletes it, only that Safe loses access and the data remains for the owner and other participants.

2.21.8 Integration with Other Features

- **Vault Messaging**: Shared Space invites are delivered through Vault Messaging.
- **Cloud File Storage**: shared collaboration includes cloud-stored files in the shared Space.
- **Access Keys & Safe Access**: this remains the right model when the goal is to let one or more users open the same Safe using their own passkey or hardware-backed key.

Back to Features Overview

2.22 Shared Spaces

2.22.1 Overview

Shared Spaces let separate Safes collaborate inside the same Space without sharing the rest of their Safes. This is different from giving additional access keys to one Safe. In a Shared Space, each participant keeps their own Safe, but they can work together on the same notes and cloud files inside one shared workspace.

2.22.2 How It Works

1. A Safe owner creates a **Shared Space**.
2. The owner sends a **Shared Space invite** through **Vault Messaging**.
3. The recipient opens the message and selects **Add Shared Space**.
4. The imported Space appears in the recipient's Safe.
5. Both Safes can then work in the same shared collaboration area.

2.22.3 What Shared Spaces Are For

Shared Spaces are designed for collaboration between Safes, such as:

- project work between separate operators,
- family coordination across separate Safes,
- secure document collaboration,
- controlled sharing of one workspace without exposing unrelated Safe data.

2.22.4 What Gets Shared

- notes and records stored in that Space,
- labels and organization inside that Space,
- cloud-stored encrypted files attached to records in that Space.

2.22.5 What Does Not Get Shared

- the rest of either participant's Safe,
- unrelated Spaces,
- wallet functions in that Space,
- local-only encrypted files for that Space.

> **Important**
>
> Shared Spaces are for collaboration between **separate Safes**. If you want one or more users to share the **same Safe**, give each user their own access key, such as a passkey or hardware-backed key, and grant either limited Space access or full Safe administration as needed.

2.22.6 Security and Privacy

- **Safe separation remains intact**: each participant keeps their own Safe.
- **Space-limited collaboration**: only the shared Space is exposed to collaborators.
- **Invite-based access**: access is added by importing a Shared Space invite through Vault Messaging.

- **End-to-end encryption model**: the collaboration data remains encrypted and compartmentalized at the Space level.

2.22.7 Collaboration Behavior

- Shared Spaces are designed for live collaboration between Safes.
- Updates made by one participant can appear to other participants after refresh or when reopening shared content.
- Shared Spaces assume that more than one Safe may edit the same workspace over time.

2.22.8 Ownership and Deletion Behavior

- A Shared Space has an owner Safe.
- If the owner deletes the Shared Space, that Shared Space is deleted for every Safe that was participating in it.
- If a non-owner Safe deletes the Shared Space from its own Safe, that Safe only loses access to the Shared Space.
- When a non-owner loses access this way, the Shared Space data is not deleted for the owner or for other participating Safes.

2.22.9 Limits and Operational Notes

- Wallet tools are not available inside Shared Spaces.
- Local-only encrypted file storage is not supported inside Shared Spaces.
- Shared Space invites are sent through Vault Messaging, not through access-key setup.
- Deleting a Shared Space has different results depending on whether the deleting Safe is the owner or only a participant.

2.22.10 Use Cases

- **Operations room**: share one secure workspace across separate team Safes.
- **Family coordination**: keep separate Safes while working together in a single family Space.
- **Advisor or assistant workflows**: collaborate on one defined area without granting access to the rest of a Safe.

2.22.11 FAQs

? Do both people need their own Safe?

Yes. Shared Spaces are specifically for collaboration between separate Safes.

? Does a Shared Space replace access keys?

No. Access keys are for one Safe and can let multiple users access that same Safe with their own keys, either with limited Space access or full administration. Shared Spaces are for collaboration between multiple separate Safes.

? Can I share files in a Shared Space?

Yes, cloud-stored files in that Space can be used for collaboration. Local-only file storage is not supported in Shared Spaces.

? What happens if the owner deletes a Shared Space?

If the owner deletes it, the Shared Space is deleted for every Safe that has access to it.

What happens if a participant deletes a Shared Space?

If a non-owner Safe deletes it, that Safe loses access to the Shared Space, but the data remains available to the owner and other participating Safes.

2.22.12 Related Guides

- **UnoLock Spaces**
- **Sharing a Space Between Safes**
- **Granting an Access Key Access to Spaces in the Same Safe**

2.23 Pin Code

2.23.1 Overview

Pin Code protects PIN entry with a randomized keypad and mouse click-based input to outsmart keyloggers and safeguard user access. This system ensures that PINs are never typed or exposed, delivering strong protection with seamless usability across all tiers, Free, Inheritance, Sovereign, and HighRisk.

In UnoLock, the PIN is **not** the main authentication factor and it is **not** the password that encrypts your Safe data. WebAuthn access keys are the primary authentication model. The PIN is an additional control that helps resist brute-force access attempts and supports deniability-related features.

2.23.2 How It Works

- **Randomized Keypad Generation**: For each login session, the server generates a unique keypad image with numbers 0-9 and letters A-F, randomized in position to prevent predictable input patterns.
- **Mouse Click-Based Input**: Users enter their pin by clicking the keypad’s characters on-screen, bypassing keyboard input to render keyloggers ineffective.
- **Server-Side Decoding**: Clicked positions are sent to the server, which decodes them using the session’s randomized keypad layout, ensuring the pin itself is never transmitted or exposed.
- **Secure Transmission**: Click data is transmitted via TLS 1.3-encrypted channels, protecting against interception during the authentication process.
- **Intuitive User Interface**: The keypad’s visual design is user-friendly, allowing seamless pin entry through clicks, balancing advanced security with effortless usability.
- **Brute-Force Control Layer**: PIN handling adds rate-limiting and attempt-friction around local access flows, which matters because the cryptographic model does not depend on a reusable password.

2.23.3 Security Implications

- **Keylogger Protection**: By eliminating keyboard input, Pin Code ensures keyloggers cannot capture pins, thwarting malware-based attacks in risky environments.
- **Session-Specific Randomization**: The ever-changing keypad layout prevents attackers from mapping inputs across sessions, enhancing authentication security.
- **PIN Is Not the Root Secret**: the PIN is not the cryptographic key that encrypts Safe data and is not a substitute for WebAuthn access keys.
- **Brute-Force Resistance**: controlled PIN entry and throttling help block repeated guessing attempts against protected local access flows.
- **Deniability Support**: PIN-based controls also support related features such as duress and deletion flows where different PIN behavior has security meaning.

2.23.4 Use Cases

- **High-Risk Environments**: Users in malware-prone settings (e.g., public or compromised devices) can authenticate securely without exposing their pin to keyloggers.
- **Corporate Security**: Businesses can protect employee access to sensitive Safes, ensuring robust authentication even on potentially infected systems.
- **Everyday Privacy**: Privacy-conscious individuals can log into their UnoLock Safe with confidence, knowing their pin is shielded from cyber threats.

2.23.5 Why It Matters

Pin Code matters because UnoLock does not fall back to a normal password-centric model. WebAuthn authenticates access, client-side encryption protects data, and the PIN adds a separate barrier against brute-force attempts and coercion-related workflows.

2.23.6 FAQs

Can keyloggers capture my Pin Code input?

No, Pin Code uses mouse click-based input on a randomized keypad, ensuring keyloggers cannot record your pin, as no keystrokes are involved.

Is the PIN my Safe password?

No. UnoLock does not use a normal password as the main secret for Safe access. WebAuthn access keys are the primary authentication factor, and the PIN is a separate protective control.

Is the Pin Code system easy to use for non-technical users?

Yes, the visual keypad and click-based interface are designed for simplicity, making secure authentication intuitive for all users.

How does UnoLock ensure the Pin Code remains secure during transmission?

Clicked positions are transmitted via TLS 1.3-encrypted channels and decoded server-side using the session’s unique keypad layout, protecting the pin from exposure.

2.23.7 Compliance & Privacy Regulations

- **GDPR Compliance**: Pin Code supports GDPR by avoiding cleartext pin storage and using encrypted transmission, ensuring user authentication data remains private and secure.

2.23.8 Integration with Other Features

- **FIDO2 & Biometric Login**: Complements Pin Code by providing the primary passwordless authentication model for Safe access.
- **End-to-End Encryption**: protects messaging and protected API payloads independently of the PIN.
- **Client-Side Encryption**: keeps Safe data encrypted without turning the PIN into the cryptographic root secret.

Back to Features Overview

2.24 Post-Quantum Encryption

2.24.1 Overview

Post-Quantum Encryption is a vanguard of quantum-proof security, arming UnoLock with advanced cryptographic defenses to shield your data, identity, and digital assets against future quantum computing threats. Integrated across all tiers, Free, Inheritance, Sovereign, and HighRisk, this feature employs lattice-based algorithms like Kyber and Dilithium, alongside AES-256 GCM, to ensure your Safe remains an impregnable fortress for decades. UnoLock's forward-thinking encryption delivers unmatched protection, securing your digital sovereignty today and tomorrow.

2.24.2 How It Works

- **Post-Quantum Key Exchange**: UnoLock uses Kyber-based Key Encapsulation Mechanism (KEM) to negotiate secure session keys for API communication, replacing vulnerable elliptic curve methods with quantum-resistant cryptography.
- **Quantum-Safe Authentication**: API servers authenticate with Dilithium digital signatures, ensuring clients connect only to legitimate UnoLock backends, immune to quantum-powered Man-in-the-Middle attacks.
- **Client Data Master Key Protection**: The Client Data Master Key (CDMK) is generated and wrapped using a FIDO2 WebAuthn authenticator, safeguarded on-device with quantum-resistant encryption and biometric verification.
- **End-to-End Data Encryption**: All user data, files, archives, and metadata, is encrypted client-side with AES-256 GCM, maintaining a 128-bit security margin against quantum attacks like Grover's algorithm.
- **Dual-Layer Cloud Storage**: Data is encrypted client-side with AES-256 before cloud storage, supplemented by AWS S3 server-side encryption, ensuring quantum-safe protection at rest.

2.24.3 Security Implications

- **Quantum-Resistant Defense**: Kyber and Dilithium algorithms protect against quantum attacks (e.g., Shor's algorithm), ensuring your data remains secure as quantum computing advances.
- **Forward Secrecy**: Per-session key negotiation and re-keying prevent retroactive decryption, safeguarding past communications even if future keys are compromised.
- **Zero-Knowledge Privacy**: Client-side key management and stateless servers ensure UnoLock cannot access your data, maintaining privacy against both classical and quantum threats.

2.24.4 Use Cases

- **Long-Term Data Protection**: Individuals can secure sensitive files (e.g., legal documents, Bitcoin and Ethereum keys) with confidence that they'll remain safe against future quantum decryption.
- **Corporate Data Security**: Businesses can protect proprietary information or client data, ensuring compliance and security in a quantum future.
- **High-Risk Asset Management**: Cryptocurrency investors can safeguard wallet seeds or financial records, leveraging quantum-hardened encryption for enduring protection.

2.24.5 Why It Matters

Post-Quantum Encryption fortifies UnoLock with a shield against the quantum future, ensuring your digital assets and privacy endure beyond today's threats. This feature delivers peace of mind, securing your Safe with cryptography that outpaces the evolution of computing itself.

2.24.6 FAQs

❓ **How does Post-Quantum Encryption protect against quantum computers?**

It uses lattice-based algorithms like Kyber and Dilithium, which resist quantum attacks (e.g., Shor’s algorithm), unlike traditional cryptography vulnerable to quantum decryption.

❓ **Does Post-Quantum Encryption affect UnoLock’s usability?**

No, the advanced cryptography is seamlessly integrated, delivering enterprise-grade security without complicating the user experience.

❓ **Will my data remain secure decades from now?**

Yes, Post-Quantum Encryption’s forward secrecy and AES-256 GCM ensure your data stays protected against future quantum and classical threats.

2.24.7 Compliance & Privacy Regulations

- **GDPR Compliance**: Post-Quantum Encryption supports GDPR by using zero-knowledge, client-side encryption and stateless servers, ensuring no personal data is exposed or stored.

2.24.8 Integration with Other Features

- **End-to-End Encryption**: Complements Post-Quantum Encryption by ensuring all Safe data is encrypted with AES-256 GCM, reinforced by quantum-resistant key management.
- **FIDO2 & Biometric Login**: Enhances Post-Quantum Encryption by securing the Client Data Master Key with WebAuthn-based authentication, adding a quantum-safe layer to user access.

Back to Features Overview

2.25 UnoLock Drop

2.25.1 Overview

UnoLock Drop is the sender client for Vault Messaging **Receive Addresses**. A recipient creates a Receive Address inside their Safe and shares it (or a shareable link). Anyone can use **UnoLock Drop** to send encrypted messages and files to a Safe through that address without creating an account or Safe.

UnoLock Drop is built for first-contact scenarios: whistleblowing, legal intake, investigative tips, and sensitive disclosures where minimizing metadata matters.

2.25.2 How It Works

- **Recipient creates a Receive Address**: each address has its own keypair and policy controls.
- **Share the address or link**: the link opens UnoLock Drop with the address prefilled.
- **Sender message (optional)**: a public note shown before submission.
- **Sender uses UnoLock Drop**: no login required; the client encrypts locally and uploads the sealed payload.
- **Hashed addressing**: the Receive Address is hashed client-side and sent as `vaultxAddressHash`.
- **Recipient decrypts in Messaging**: drops appear in the Safe's inbox and are decrypted client-side.
- **Optional local address book**: senders can save frequently used Receive Addresses in a **local, password-encrypted** address book (stored on their device only).

2.25.3 What It Is (and isn't)

- **UnoLock Drop is sender-only**: it does not have an inbox and cannot receive replies.
- **Receive Addresses are the same format** for Safe-to-Safe exchange and UnoLock Drop senders. The difference is the sender client, not the address type.
- **Tier behavior**: Sovereign and HighRisk can create Receive Addresses. Free and Inheritance can still send messages/files and can optionally allow replies per message.

2.25.4 Security Implications

- **No account required**: senders do not need a Safe to deliver a message.
- **Address privacy**: the server never receives raw Receive Addresses, only hashes.
- **Per-address keys**: each Receive Address isolates risk to a single conversation stream.
- **Policy controls**: enforce usage limits, throttling, and attachment rules per address.
- **Optional extra anonymity**: access the Drop Client via Tor for additional network privacy.
- **Local-only address book**: saved addresses are encrypted with a user password and never synced.

2.25.5 Use Cases

- **Whistleblowing and tips**: enable anonymous submissions without creating accounts.
- **Legal and journalism intake**: publish a single-use or rate-limited Receive Address for sensitive sources.
- **High-risk one-off exchanges**: rotate addresses after a short window to reduce exposure.

2.25.6 Why It Matters

UnoLock Drop makes anonymous first contact practical. It reduces setup friction for senders, keeps raw addresses off the server, and gives recipients control over exposure with per-address limits and throttles.

2.25.7 FAQs

? Do I need a Safe to send with UnoLock Drop?

No. UnoLock Drop is designed for senders who do not have a Safe.

? What is a Receive Address?

A Receive Address is a shareable messaging address with its own keypair and policy limits. The server stores only the hashed version.

? Can I save addresses for later?

Yes. UnoLock Drop can store addresses locally in a password-encrypted address book.

? Can I revoke or rotate an address?

Yes. Receive Addresses can be disabled or deleted at any time to prevent new messages.

2.25.8 Compliance & Privacy Regulations

- **GDPR Alignment**: UnoLock Drop avoids storing raw sender identities and keeps content client-side encrypted.

2.25.9 Integration with Other Features

- **Post-Quantum Encryption**: ML-KEM-1024 + AES-256-GCM protect payloads against future cryptographic threats.
- **Threat Detection**: Runtime monitoring helps detect tampering in the Drop Client and Safe workflows.

Back to Features Overview

2.26 Threat Detection

2.26.1 Overview

Threat Detection (Runtime Security Monitoring and Tamper Detection) is UnoLock's comprehensive browser runtime security service that continuously audits your environment to detect and block malicious behavior before it can compromise your data. By combining API-blocking, event-listener auditing, DOM mutation inspection, overlay detection, and extension probing—all running client-side in Angular—it ensures that any injected code, unauthorized extensions, or clickjacking attempts are caught and neutralized in real time.

2.26.2 How It Works

- **API Access Blocking**: Overrides localStorage/sessionStorage methods and indexedDB.open to throw on any attempt to read or write, logging and flagging each unauthorized call immediately.
- **WebSocket Block**: Replaces the global WebSocket constructor so any socket connection attempt is halted and reported, preventing data exfiltration channels.
- **Event Listener Auditing**: After Angular stabilizes, intercepts addEventListener to count sensitive handlers (click, input, keydown, etc.) and detect listeners injected by browser extensions via stack-trace analysis, triggering alerts when configurable thresholds are exceeded.
- **UI Overlay & Clickjacking Checks**: Every few seconds (outside Angular's zone), scans for full-screen, low-opacity overlays with high z-index, flagging or removing elements that could hijack user clicks.
- **API Tampering Detection**: Compares window.fetch and other core APIs against snapshots taken at initialization; any override by third-party code is immediately flagged.
- **DOM Mutation Inspection**: Uses a debounced MutationObserver to watch for newly added script or iframe nodes, stripping unauthorized elements (those without the data-unolock attribute or not from location.origin).
- **Extension Presence Probing**: Loads hidden manifests for known banned extensions and alerts immediately if any are detected in the browser environment.

2.26.3 Security Implications

- **Proactive Tamper Detection**: Identifies and blocks meddling scripts and API overrides before they can execute malicious operations.
- **Clickjacking Protection**: Stops hidden overlays and rogue iframes that could hijack user interactions or steal credentials.
- **Extension Threat Awareness**: Detects malicious or unapproved extensions at runtime, warning users to remove them before continuing.
- **Real-Time Client-Side Alerts**: Escalating alerts inform users of repeated or severe anomalies, guiding them to switch to a clean profile or incognito mode.
- **Zero-Trust Browser Environment**: By enforcing strict controls on every aspect of the browser API, UnoLock maintains a hardened, trust-no-one runtime posture.

2.26.4 Use Cases

- **Secure Banking Operations**: Users accessing financial accounts benefit from real-time detection of keyloggers, screen capture attempts, and malicious browser extensions.
- **Cryptocurrency Management**: Protection against clipboard hijacking and transaction manipulation when managing digital assets within the Safe.
- **Corporate Data Protection**: Enterprise users gain defense against targeted attacks attempting to steal sensitive corporate information through browser exploits.
- **High-Risk Environments**: Journalists and activists operating in hostile digital environments receive alerts about surveillance extensions and tracking attempts.

2.26.5 Why It Matters

Threat Detection provides a best-effort, client-side defense layer that enforces strict API controls, audits runtime behavior, and neutralizes unauthorized code or extensions—all in real time. While this zero-trust approach significantly raises the bar against browser-based threats, no client-side guard can guarantee 100% protection. Users must also exercise caution by avoiding untrusted browser extensions and keeping their environment secure. Together, UnoLock's monitoring features and responsible user practices maintain the integrity of your data against evolving risks.

2.26.6 FAQs

? Can Threat Detection prevent all browser-based attacks?

While Threat Detection provides comprehensive runtime monitoring and blocking capabilities, no client-side solution can guarantee 100% protection. It significantly raises the security bar but should be combined with safe browsing practices and avoiding untrusted extensions.

? Does Threat Detection slow down my browser?

The monitoring service is optimized to run efficiently outside Angular's change detection zone, using debounced observers and selective API hooks to minimize performance impact while maintaining comprehensive protection.

? What happens when a threat is detected?

Depending on the severity, the system will either block the action silently, display a warning notification, or in severe cases, recommend switching to a clean browser profile or incognito mode to ensure continued security.

2.26.7 Compliance & Privacy Regulations

- **Client-Side Only Operation**: All threat detection occurs within your browser, with no external reporting or data collection, maintaining complete privacy compliance.
- **GDPR & Privacy Compliance**: Threat detection data never leaves your device, ensuring compliance with data protection regulations.

2.26.8 Integration with Other Features

- **Post-Quantum Encryption**: Works in tandem with encryption layers to ensure that even if threats bypass detection, encrypted data remains protected.
- **FIDO2 Authentication**: Complements hardware-based authentication by ensuring the browser environment is secure before authentication ceremonies.
- **Client Application Isolation**: Reinforces browser sandbox isolation by actively monitoring for sandbox escape attempts.

Back to Features Overview

3. Security

3.1 Security Overview

3.1.1 Overview

UnoLock's security architecture is built around providing maximum protection for digital assets and sensitive information, ensuring complete privacy and control for users. UnoLock uses both **client-side encryption** and **end-to-end encrypted payload protection**, alongside WebAuthn-based authentication, post-quantum cryptography, and multi-layered data redundancy. Key management is handled client-side, meaning only the user can access decryption keys, and critical data is encrypted before leaving the device, while features like TimeLock, DuressDecoy, Plausible Deniability, and protected PIN handling provide robust defenses against unauthorized access, brute-force attempts, or coercion.

3.1.2 Security Architecture

UnoLock CybVault’s security architecture is a multi-layered framework designed to protect your digital assets at every stage of their lifecycle. Operating as a **Progressive Web App (PWA)**, UnoLock ensures that sensitive operations such as encryption, decryption, and key management are performed client-side, adhering to a **zero-knowledge** model where only the user holds the decryption keys. Safe data is encrypted locally using **AES-256 GCM** before being transmitted for storage, where it is further protected by storage-layer controls and global redundancy.

The architecture emphasizes **privacy by design**, collecting no personally identifiable information (PII), avoiding browser local storage or cookies, and anonymizing all transactions to prevent tracking. **FIDO2 and biometric authentication** provide passwordless, phishing-resistant access, while **post-quantum cryptography** ensures resilience against future quantum threats. UnoLock also protects **messaging** and protected **API payloads** with end-to-end encrypted application-layer security, instead of relying only on transport encryption. For high-risk scenarios, features like **TimeLock**, **DuressDecoy**, and **Plausible Deniability** offer robust defenses against coercion or unauthorized access. The **serverless infrastructure** minimizes attack surfaces, and **AWS CloudTrail** auditing ensures all cloud operations are traceable, supporting compliance with **GDPR**, **HIPAA**, and other regulations.

This comprehensive approach, combining client-side encryption, end-to-end encrypted payload protection, cloud resilience, WebAuthn-based access, and privacy-first principles, makes UnoLock a sovereign solution for protecting digital assets, ensuring users retain full control under all circumstances.

3.1.3 Key Security Features

UnoLock CybVault’s security is bolstered by a suite of advanced features, each designed to address specific threats and enhance user control. Below is the full list of security features, each with a brief description and a link to its detailed page:

- **Security Overview**: Introduces UnoLock's comprehensive security architecture for protecting digital assets. Learn More
- **Client Application Isolation in Web Browser**: Isolates the UnoLock web app in a sandboxed browser environment to prevent cross-site attacks. Learn More
- **Benefits of Browser Isolation**: Enhances protection by preventing malicious sites or extensions from accessing UnoLock sessions. Learn More
- **Cross-Platform Compatibility and Consistent Performance**: Ensures consistent security and performance across devices and operating systems. Learn More
- **Browser Content Security Policy (CSP) Isolation**: Enforces strict CSP to block unauthorized scripts and mitigate XSS attacks. Learn More
- **Secure Hashing and Signing of PWA Updates**: Verifies the integrity and authenticity of PWA updates using cryptographic hashing and signing. Learn More
- **FIDO2 Authentication with WebAuthn for Secure Access**: Provides passwordless, phishing-resistant access using FIDO2 and WebAuthn. Learn More
- **Enhanced PIN Entry Security**: Strengthens PIN entry protection with a randomized keypad and keylogger resistance. Learn More
- **Client-Side Encryption Using AES-256 GCM**: Encrypts data locally with AES-256 GCM for zero-knowledge security. Learn More
- **Secure Direct Storage of Encrypted Data in AWS S3**: Stores encrypted data in AWS S3 with secure, direct access. Learn More
- **Dual-Layer Encryption with AWS S3 Server-Side Encryption (SSE)**: Adds server-side encryption to client-side encrypted data in AWS S3. Learn More
- **Advanced Key Management with Client-Side Keyring**: Manages encryption keys securely on the client side. Learn More
- **Advanced Data Deletion and Perfect Forward Secrecy**: Ensures secure data deletion with perfect forward secrecy for privacy. Learn More
- **SHA-256 Hash Verification of Uploaded Data**: Verifies data integrity using SHA-256 hashes during uploads. Learn More
- **Robust Data Redundancy with AWS S3**: Replicates encrypted data across global AWS S3 data centers for reliability. Learn More
- **No Browser Local Storage or Cookies Used**: Avoids local storage and cookies to enhance privacy and reduce tracking risks. Learn More
- **Commitment to Anonymity and Data Privacy**: Prioritizes user anonymity by avoiding PII and anonymizing transactions. Learn More
- **Advanced API Security with AES-256 GCM and ECDHE_ECDSA**: Secures API communications with advanced encryption and key exchange. Learn More
- **Secure Deletion of Safes and Encrypted File Records**: Permanently deletes safes and records to prevent recovery. Learn More
- **Plausible Deniability with Safeword-PIN Space Protection**: Hides or deletes selected sensitive Spaces under coercion, depending on tier. Learn More
- **Robust Key Management with Multi-Key Registration and WebAuthn**: Supports multiple keys with secure WebAuthn registration. Learn More
- **Access Keys, Limited Access, and TimeLock**: Explains the difference between key permissions and temporary per-key TimeLock behavior. Learn More
- **Secure Viewing of Supported File Types Within the Client Application**: Safely views files within the UnoLock app without external exposure. Learn More
- **Inactivity-Triggered Safe Access Methods - LockoutGuard and LegacyLink**: Manages access during inactivity with recovery and succession options. Learn More
- **Serverless Infrastructure for Enhanced Security**: Uses serverless architecture to minimize attack surfaces. Learn More
- **Advanced AWS Account Management**: Secures AWS accounts with RBAC, MFA, and CloudTrail auditing. Learn More

- **Stateless Multi-Account Build System with AWS CodePipeline**: Isolates builds across AWS accounts for secure CI/CD. Learn More
- **Digital Paper Wallet (DPW) for Bitcoin and Ethereum Management**: Stores Bitcoin and Ethereum keys offline-like for maximum security. Learn More
- **Spaces: Granular Data Access and Control**: Segments data into isolated environments with fine-grained permissions. Learn More
- **Quadruple Encryption & WebAuthn Digital Paper Wallet (DPW)**: Applies four encryption layers and WebAuthn for ultimate key security. Learn More
- **Post-Quantum Encryption Security**: Employs quantum-resistant cryptography (Kyber, Dilithium) to protect data and communications. Learn More
- **Vault Messaging Security**: Enables zero-trust, post-quantum encrypted vault-to-vault messaging with metadata anonymity. Learn More
- **UnoLock VaultX Security**: Provides anonymous, post-quantum encrypted messaging via Receive Addresses and the Drop Client. Learn More

3.2 Client Application Isolation in Web Browser

3.2.1 Overview

Client Application Isolation ensures that the UnoLock web application runs in a fully isolated environment within the user's browser, providing additional layers of protection. This feature prevents the web application from interacting with other browser processes or tabs, reducing the risk of cross-site attacks, such as cross-site scripting (XSS) or man-in-the-middle (MITM) attacks. By containing the UnoLock client within a secure environment, this feature guarantees that sensitive operations, such as encryption and decryption, remain shielded from potential browser vulnerabilities or malicious extensions.

3.2.2 How It Works

- **Sandboxed Environment**: UnoLock runs in a secure, sandboxed browser environment, separating its processes from other open tabs or extensions. This minimizes exposure to threats arising from other web applications.
- **Process Isolation**: The browser allocates a separate process to UnoLock, preventing data leakage or cross-interaction with other browser processes.
- **Secure Handling of Data**: All cryptographic functions (e.g., key generation, encryption) are handled locally and within the isolated browser context, ensuring that no sensitive data is shared across browser processes or with external websites.
- **Content Security Policy (CSP)**: UnoLock enforces a strict CSP to limit the sources of executable scripts, reducing the risk of XSS and other injection-based attacks.

3.2.3 Security Implications

- **Reduced Attack Surface**: By isolating the UnoLock client within its own browser environment, the risk of browser-based attacks, such as cross-site scripting or unauthorized data access, is significantly reduced.
- **Protection Against Malicious Extensions**: Browser extensions are prevented from accessing the UnoLock application or interacting with its data, enhancing the overall security of the platform.
- **Secure Local Operations**: All sensitive operations (such as encryption and key management) are performed locally within the isolated context, reducing exposure to browser vulnerabilities.

3.2.4 Use Cases

- **Web-Based Vault Access**: Users accessing their UnoLock vault through a web browser can securely manage their digital assets, knowing that their session is isolated from other websites and browser activities.
- **High-Security Environments**: Individuals in sensitive roles (e.g., executives, journalists) who require strong browser isolation can benefit from additional protection against web-based attacks.
- **Cross-Platform Use**: Users accessing UnoLock from different devices can rely on consistent security, thanks to the isolated client environment across all web browsers.

3.2.5 Why It Matters

Client Application Isolation ensures that sensitive operations and data within the UnoLock vault are protected from common browser vulnerabilities. In a world where phishing, malware, and browser-based exploits are rampant, isolating the UnoLock client reduces the risk of unauthorized access and ensures secure vault management.

3.2.6 FAQs

Can browser extensions interact with my UnoLock session?

No, UnoLock’s Client Application Isolation prevents browser extensions from interacting with your vault or accessing sensitive data.

❓ **How does this isolation protect my data?**

By running in a sandboxed environment, UnoLock isolates its processes from the rest of the browser, ensuring that no data leaks occur and no unauthorized access is possible.

❓ **What happens if another website tries to access my UnoLock session?**

The isolation prevents any cross-site interaction, ensuring that no other websites or browser tabs can access your UnoLock vault or session data.

3.2.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: By ensuring secure data handling within an isolated browser context, Client Application Isolation helps users comply with strict data privacy regulations such as GDPR and HIPAA.

3.2.8 Integration with Other Features

- **Content Security Policy (CSP) Isolation**: Works in conjunction with strict CSP enforcement to further limit potential attack vectors within the browser.
- **Client-Side Encryption**: All cryptographic operations are securely handled within the isolated environment, ensuring end-to-end encryption integrity.

3.3 Benefits of Browser Isolation

3.3.1 Overview

The **Benefits of Browser Isolation** feature enhances UnoLock's security by protecting user data and application processes from potential browser-based vulnerabilities. Browser isolation ensures that UnoLock's web application runs in a controlled environment, isolating it from other web content and browser activities. This prevents malicious sites, tabs, or extensions from accessing or manipulating sensitive information in the UnoLock vault. It also mitigates the risk of attacks such as cross-site scripting (XSS), phishing, and man-in-the-middle (MITM) attacks by limiting how web content can interact with the UnoLock session.

3.3.2 How It Works

- **Isolated Browser Session**: UnoLock uses browser isolation techniques to create a sandboxed environment, ensuring that sensitive operations are executed in isolation from other web applications.
- **Cross-Site Interaction Prevention**: This feature blocks other sites and browser tabs from accessing or interacting with UnoLock's session, preventing the possibility of unauthorized data leaks.
- **Security Layer in Browser**: Browser isolation acts as an additional security layer, filtering out malicious content before it can impact the UnoLock environment.
- **Protection from Malicious Content**: Any potentially harmful scripts or code from other browser windows are blocked from interacting with the UnoLock session.

3.3.3 Security Implications

- **Enhanced Protection Against Browser Attacks**: By isolating UnoLock from other browser content, users are protected from cross-site attacks and malware injections. This drastically reduces the risk of web-based threats like XSS and MITM attacks.
- **Reduced Risk from Malicious Extensions**: Browser extensions, which are often vulnerable to exploitation, are blocked from accessing or modifying UnoLock's secure session.
- **Safer Browser Interaction**: Users can confidently use UnoLock's web application without worrying about browser vulnerabilities, especially when accessing sensitive information.

3.3.4 Use Cases

- **Sensitive Data Access**: Users handling sensitive data, such as financial records or cryptocurrency wallets, can use UnoLock in a browser without worrying about interaction with malicious web content.
- **Secure Web Browsing**: Those who access their UnoLock vault from public or unsecured networks (e.g., cafés, airports) benefit from browser isolation, which protects their data from potential attacks.
- **Cross-Platform Users**: Whether on desktop, mobile, or other devices, browser isolation ensures a consistent and secure browsing experience for UnoLock users.

3.3.5 Why It Matters

Browser isolation prevents the UnoLock application from being compromised by common web-based threats like phishing and malware. By ensuring that sensitive operations within the vault are shielded from other web content, this feature offers a significant security advantage. It is especially critical in environments where users frequently interact with other websites or are at risk of phishing attacks.

3.3.6 FAQs

? Can websites track my UnoLock session through cookies or scripts?

No, UnoLock’s browser isolation prevents other sites and browser tabs from interacting with your vault session, blocking unauthorized access.

? How does browser isolation protect my data?

By sandboxing the UnoLock web application, it ensures that no malicious scripts or browser tabs can access or modify your data during your session.

? Is browser isolation applied to mobile browsers as well?

Yes, browser isolation is implemented across all supported browsers, including mobile devices, ensuring consistent protection.

3.3.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: By protecting user data from external browser vulnerabilities and interactions, browser isolation helps maintain compliance with privacy regulations like GDPR and HIPAA.

3.3.8 Integration with Other Features

- **Client Application Isolation**: Works alongside Client Application Isolation to ensure that the UnoLock client is secured in the browser and that sensitive data is protected from external threats.
- **End-to-End Encryption**: Complements browser isolation by ensuring that any data being processed or transmitted remains encrypted, adding another layer of security.

3.4 Cross-Platform Compatibility and Consistent Performance

3.4.1 Overview

The **Cross-Platform Compatibility and Consistent Performance** feature ensures that UnoLock can be seamlessly accessed across multiple devices and operating systems while maintaining the highest security standards. Whether users are accessing their vault from desktop computers, mobile devices, or tablets, UnoLock delivers a consistent experience without sacrificing performance or security. This feature ensures that all cryptographic operations, data management, and security measures function identically across platforms, making UnoLock versatile and secure, regardless of the device being used.

3.4.2 How It Works

- **Unified User Experience**: UnoLock provides a consistent interface and user experience across all devices, ensuring that users can access their vault seamlessly, whether on desktop, mobile, or tablet.
- **Cross-Platform Cryptography**: Cryptographic operations, such as encryption, decryption, and key management, are handled uniformly across platforms, ensuring that security protocols remain intact regardless of the device.
- **Device-Specific Optimizations**: UnoLock automatically optimizes performance for different devices, ensuring that mobile users experience fast, secure access without compromising on encryption or data integrity.
- **Real-Time Synchronization**: Vault data is synchronized across all devices in real-time, ensuring that changes made on one platform are immediately reflected on others, without sacrificing security or performance.

3.4.3 Security Implications

- **Consistent Security Standards**: UnoLock ensures that all devices adhere to the same security protocols, such as end-to-end encryption and FIDO2 authentication, ensuring that users experience consistent protection across all platforms.
- **Protection Against Device-Specific Threats**: Each device’s operating system and security vulnerabilities are considered, ensuring that users are protected against platform-specific threats, such as mobile-based malware or phishing on desktops.
- **Real-Time Data Integrity**: Data synchronized across platforms remains encrypted and secure at all times, ensuring that users can switch between devices without exposing their data to potential breaches.

3.4.4 Use Cases

- **Multi-Device Users**: Users who access their vault from various devices, such as a laptop at work, a phone while traveling, and a tablet at home, benefit from a consistent and secure experience across all platforms.
- **Businesses with Remote Teams**: Remote teams can securely access and manage company vaults across different devices and operating systems, ensuring data integrity and security without limiting access.
- **Traveling Professionals**: Individuals on the move can securely switch between devices, knowing that their sensitive data is protected and synchronized in real-time.

3.4.5 Why It Matters

Cross-platform compatibility is essential in today’s multi-device world. UnoLock ensures that users can access their vaults securely, no matter which device they are using. With consistent performance and stringent security protocols in place across platforms, this feature is crucial for both individual users and businesses that require flexibility without sacrificing security.

3.4.6 FAQs

? Can I access my UnoLock vault from multiple devices simultaneously?

Yes, you can access your vault from multiple devices, and all changes will be securely synchronized in real-time across platforms.

❓ **Does the security level change when switching between desktop and mobile?**

No, UnoLock ensures that the same security protocols are applied consistently across all devices, maintaining end-to-end encryption and other security measures.

❓ **What happens if I lose one of my devices?**

If a device is lost, you can revoke its access from another device to ensure the vault remains secure. Multi-factor authentication ensures that unauthorized access is prevented.

3.4.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: UnoLock's cross-platform security features help ensure that users' sensitive data remains protected, no matter what device they are using. This supports compliance with data privacy regulations, such as GDPR and HIPAA, by maintaining encryption and secure access across platforms.

3.4.8 Integration with Other Features

- **Access Keys & Safe Access**: Works hand-in-hand with the access-key model to ensure consistent security and Safe access across supported devices.
- **End-to-End Encryption**: All data synchronized across platforms is protected by end-to-end encryption, ensuring that security is never compromised when switching between devices.

3.5 Browser Content Security Policy (CSP) Isolation

3.5.1 Overview

The **Browser Content Security Policy (CSP) Isolation** feature ensures that UnoLock's web application is protected from malicious content and unauthorized code execution. By enforcing a strict Content Security Policy, UnoLock limits which resources (scripts, stylesheets, and media) can be executed by the browser, minimizing the risk of attacks such as cross-site scripting (XSS) and data injection. This feature isolates UnoLock's application from potentially harmful web content, ensuring a secure environment for all cryptographic and data operations.

3.5.2 How It Works

- **Strict CSP Rules**: UnoLock enforces a Content Security Policy that restricts the types of resources the browser can load and execute, allowing only trusted sources to run within the web application.
- **Script and Resource Whitelisting**: Only trusted scripts, styles, and media from verified sources are allowed to execute within the UnoLock application. External scripts and unauthorized resources are blocked by default.
- **Prevention of Code Injection**: By restricting the types of scripts that can be executed, CSP Isolation protects against malicious code injections, safeguarding user data from unauthorized modifications or theft.
- **Inline Script Blocking**: UnoLock's CSP prevents the execution of inline scripts, further reducing the risk of XSS attacks by disallowing the execution of untrusted code directly within the application.

3.5.3 Security Implications

- **Mitigates Cross-Site Scripting (XSS)**: By blocking untrusted scripts from being executed in the browser, CSP Isolation significantly reduces the risk of XSS attacks, which are a common vector for injecting malicious code.
- **Protection Against Malicious Resources**: CSP ensures that only resources from authorized domains are allowed, preventing external entities from injecting malicious code into the UnoLock application.
- **Enhances Browser Security**: CSP Isolation adds another layer of security within the browser, protecting users from external web vulnerabilities that could compromise their vault's security.

3.5.4 Use Cases

- **Web-Based Vault Access**: Users who access UnoLock through a browser benefit from the enhanced security that CSP provides, ensuring their data is protected from malicious content.
- **Enterprise-Level Security**: Businesses using UnoLock for sensitive data management can rest assured that the application is isolated from potentially harmful web content or scripts that could otherwise compromise the security of their data.
- **Protection in High-Risk Environments**: Users who access their UnoLock vault from public or unsecured networks benefit from additional protection provided by CSP Isolation, safeguarding their sessions against malicious interference.

3.5.5 Why It Matters

In today's web environment, attacks like cross-site scripting (XSS) and code injection are common. By enforcing a strict Content Security Policy, UnoLock ensures that its web application is shielded from untrusted sources and malicious scripts, reducing the attack surface and enhancing the overall security of user data.

3.5.6 FAQs

How does CSP Isolation protect against XSS attacks?

CSP Isolation prevents unauthorized scripts from being executed within the UnoLock web application, blocking any attempts to inject malicious code and reducing the risk of XSS attacks.

Can external websites inject scripts into my UnoLock session?

No, UnoLock’s strict CSP ensures that only whitelisted resources and scripts can run, preventing external websites from injecting unauthorized code.

Does CSP affect the performance of the UnoLock application?

No, CSP is designed to enhance security without affecting the performance of the application. It works in the background to block harmful content without impacting the user experience.

3.5.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: By ensuring that only authorized scripts and resources are executed, CSP Isolation helps maintain the privacy and security of user data, supporting compliance with GDPR and HIPAA regulations.

3.5.8 Integration with Other Features

- **Client Application Isolation**: CSP Isolation works in tandem with Client Application Isolation to ensure that UnoLock’s web application is secure from unauthorized access and malicious interference.
- **End-to-End Encryption**: CSP complements end-to-end encryption by preventing unauthorized scripts from compromising encrypted data during transmission or processing.

3.6 Secure Hashing and Signing of PWA Updates

3.6.1 Overview

The **Secure Hashing and Signing of PWA Updates** feature ensures the integrity and authenticity of Progressive Web App (PWA) updates in UnoLock. By applying cryptographic hashing and digital signing, this feature verifies that the updates delivered to the user’s browser or device are legitimate and untampered. This process prevents the installation of malicious or altered updates that could compromise the security of the UnoLock vault. Secure hashing guarantees that the content has not been modified, while signing ensures that only authorized updates from trusted sources are applied.

3.6.2 How It Works

- **Cryptographic Hashing**: Every update to the UnoLock PWA is hashed using a secure cryptographic hash function (e.g., SHA-256). The hash value acts as a fingerprint of the update, ensuring that any changes to the content can be detected.
- **Digital Signing**: Once hashed, the update is digitally signed using UnoLock’s private key, guaranteeing its authenticity. The digital signature is verified against UnoLock’s public key, ensuring that only updates from authorized sources are accepted.
- **Integrity Verification**: When a user’s device receives a PWA update, the application checks the hash of the update against the original hash value. If the hashes match, the update is verified as unchanged.
- **Authenticity Check**: The digital signature is also verified to ensure that the update comes from a trusted source, preventing unauthorized updates from being installed.

3.6.3 Security Implications

- **Protection Against Malicious Updates**: By ensuring that updates are hashed and signed, UnoLock prevents the delivery of malicious or tampered updates that could introduce vulnerabilities or compromise user data.
- **Data Integrity Assurance**: Hashing ensures that any alteration in the update content will be detected, safeguarding users from corrupted or altered updates.
- **Trusted Source Verification**: Digital signatures confirm that updates originate from UnoLock’s trusted sources, protecting users from potential man-in-the-middle (MITM) attacks or unauthorized changes during transmission.

3.6.4 Use Cases

- **Secure PWA Updates for All Devices**: Users who access UnoLock’s PWA from various devices benefit from the assurance that every update is authenticated and verified, keeping their vault secure and up-to-date without fear of malicious interference.
- **Protection for Sensitive Data**: Individuals or businesses that rely on UnoLock for managing sensitive data, such as financial records or private documents, can ensure that the PWA remains secure through trusted updates.
- **Enterprise-Level Security**: Organizations using UnoLock’s PWA for managing internal data can rely on secure hashing and signing to protect against potential supply chain attacks that might introduce vulnerabilities via updates.

3.6.5 Why It Matters

Software updates are a common target for attackers, who may try to inject malicious code during the update process. By implementing secure hashing and signing, UnoLock ensures that every update is verified for integrity and authenticity before being applied. This protects users from unknowingly installing compromised software and keeps their sensitive data secure.

3.6.6 FAQs

How does secure hashing prevent malicious updates?

Hashing generates a unique fingerprint for each update. If any part of the update is altered, the hash will no longer match, and the update will be rejected, preventing tampered updates from being installed.

What role does digital signing play in securing updates?

Digital signing ensures that only updates coming from UnoLock’s trusted sources can be applied. The signature is verified using UnoLock’s public key, preventing unauthorized updates from being installed.

What happens if an update fails the integrity check?

If an update’s hash or signature verification fails, the update is rejected, and the user is notified. This ensures that only legitimate and secure updates are applied.

3.6.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Secure hashing and signing of PWA updates help ensure data integrity and prevent unauthorized software changes, supporting compliance with GDPR and HIPAA by protecting sensitive user information from malicious or tampered software.

3.6.8 Integration with Other Features

- **End-to-End Encryption**: Secure hashing and signing work alongside end-to-end encryption to ensure that both data and updates are protected from tampering or unauthorized access.
- **Client-Side Encryption**: This feature complements client-side encryption by ensuring that the application performing encryption remains secure and unmodified, guaranteeing the safety of users' encrypted data.

3.7 FIDO2 Authentication with WebAuthn for Secure Access

3.7.1 Overview

This page explains the **security role** of **FIDO2 / WebAuthn** in UnoLock.

UnoLock uses FIDO2 / WebAuthn to authenticate **access keys** securely without relying on traditional passwords. That gives UnoLock phishing-resistant, public-key based authentication for Safe access while keeping the authenticator's private key on the user's device or hardware key.

For the customer-facing explanation of access keys, passkeys, hardware keys, and multi-device use, see **Access Keys & Safe Access**.

3.7.2 What FIDO2 / WebAuthn Provides

- **Public-key authentication**: UnoLock verifies signed challenges using a registered public key instead of a reusable password.
- **Private key isolation**: the authenticator keeps the private key on-device or in dedicated hardware.
- **Origin binding**: WebAuthn is tied to the correct origin, which helps prevent phishing.
- **Local biometric mediation**: when biometrics are used, the biometric check stays local to the authenticator or device.

3.7.3 How It Works in UnoLock

At a high level:

1. A user registers an access key for a Safe.
2. The authenticator creates or exposes a WebAuthn credential.
3. UnoLock stores the public-key side needed for verification.
4. During Safe access, the authenticator signs a challenge.
5. UnoLock verifies the response and allows the authenticated operation to continue.

3.7.4 Security Properties

- **Passwordless authentication**: no reusable password secret is transmitted or stored for login.
- **Phishing resistance**: origin-aware challenge signing makes credential phishing materially harder.
- **Replay resistance**: challenge-response authentication reduces replay risk.
- **Hardware-backed protection**: dedicated authenticators such as YubiKeys can harden key protection.
- **Biometric privacy**: UnoLock does not receive or store fingerprint or face data.

3.7.5 Why It Matters

FIDO2 / WebAuthn strengthens UnoLock’s security model by replacing weak shared-secret authentication with device-bound or hardware-bound authenticators. This reduces exposure to:

- stolen-password attacks,
- phishing,
- credential stuffing,
- replay of intercepted credentials.

It also supports a stronger access-control model because each person can authenticate with their **own** registered access key rather than sharing one secret.

3.7.6 Scope in UnoLock

FIDO2 / WebAuthn secures **authentication**. It is one part of a larger system that also includes:

- encrypted Safe data storage,
- per-user access keys,
- Space-level permissions,
- recovery and continuity controls such as **Lockout Guard**.

3.7.7 FAQs

What is the difference between FIDO2 / WebAuthn and an access key?

FIDO2 / WebAuthn is the authentication standard and protocol. An access key is the user-facing credential registered in UnoLock, such as a passkey or hardware key, that uses that security model.

Can UnoLock access my biometric data?

No. Biometric checks happen locally on the device or authenticator. UnoLock does not receive or store biometric data.

Does this page explain how users access the same Safe from multiple devices?

Not in detail. That topic is covered in **Access Keys & Safe Access**.

3.7.8 Related Pages

- **Access Keys & Safe Access**
- **Biometric and FIDO2 Access**
- **Spaces**
- **Shared Spaces**
- **Lockout Guard**

3.8 Enhanced PIN Entry Security

3.8.1 Overview

Enhanced PIN Entry Security protects UnoLock PIN entry with a randomized keypad and mouse click-based input to ensure strong resistance to keyloggers. Available across all tiers, Free, Inheritance, Sovereign, and HighRisk, this feature safeguards your Safe by preventing PIN capture through malware while fitting into UnoLock’s broader access-key authentication model.

The important security distinction is that the PIN is **not** the primary authentication factor and is **not** the password that encrypts Safe data. UnoLock’s primary authentication model is WebAuthn-based access keys. The PIN is a separate control used to slow brute-force attempts and support PIN-based deniability and recovery-related behaviors.

3.8.2 How It Works

- **Randomized Keypad Generation**: Each login session generates a unique keypad image with numbers 0-9 and letters A-F in randomized positions, preventing predictable input patterns.
- **Mouse Click-Based Input**: Users enter their pin by clicking keypad characters on-screen, bypassing keyboard input to nullify keylogger threats.
- **Server-Side Decoding**: Clicked positions are sent to the server and decoded using the session’s randomized keypad layout, ensuring the pin is never transmitted in cleartext.
- **Encrypted Transmission**: Click data is transmitted via TLS 1.3-encrypted channels, protecting against interception during authentication.
- **Brute-Force Control**: Protected PIN handling adds friction and rate limits around repeated access attempts, which is important in a WebAuthn-plus-client-side-encryption model.

3.8.3 Security Implications

- **Keylogger Neutralization**: Mouse click input eliminates keyboard data, rendering keyloggers ineffective and safeguarding pins from malware capture.
- **Dynamic Input Protection**: Randomized keypad layouts per session prevent attackers from mapping inputs, enhancing authentication resilience.
- **Zero-Knowledge Pin Security**: The pin is never typed or stored in cleartext, with server-side decoding ensuring UnoLock cannot access it.
- **Non-Password Architecture**: PIN protection exists alongside WebAuthn and client-side encryption; it does not replace them or act as the main cryptographic secret.

3.8.4 Use Cases

- **High-Risk Device Access**: Users on public or compromised devices can authenticate securely, protected from keyloggers lurking in untrusted environments.
- **Corporate Vault Security**: Businesses can ensure employee logins remain safe from malware, maintaining vault integrity in sensitive operations.
- **Privacy-First Authentication**: Individuals can access their vault with confidence, knowing their pin is shielded from cyber threats in any setting.

3.8.5 Why It Matters

Enhanced PIN Entry Security strengthens UnoLock login by blending keylogger protection with brute-force resistance. That matters because UnoLock does not rely on normal passwords for Safe access or for the main Safe encryption model.

3.8.6 FAQs

Can keyloggers capture my UnoLock pin?

No, mouse click-based input on a randomized keypad ensures keyloggers cannot record your pin, as no keystrokes are used.

Is the PIN the same as my Safe password?

No. UnoLock’s primary authentication model is WebAuthn-based access keys, not passwords. The PIN is a separate security control.

Is the randomized keypad difficult to use?

No, the visual keypad is designed for simplicity, allowing easy click-based entry while maintaining robust security.

How secure is the pin during transmission?

Clicked positions are sent via TLS 1.3-encrypted channels and decoded server-side, ensuring the pin remains protected from interception.

3.8.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Enhanced PIN Entry Security supports GDPR and HIPAA by preventing unauthorized access to authentication data, ensuring user privacy through encrypted, zero-knowledge PIN handling.

3.8.8 Integration with Other Features

- **FIDO2 Authentication with WebAuthn**: Complements protected PIN entry by providing the primary phishing-resistant authentication model for Safe access.
- **Client-Side Encryption**: keeps Safe data encrypted independently of the PIN.

Back to Security Overview

3.9 Client-Side Encryption Using AES-256 GCM

3.9.1 Overview

Client-Side Encryption Using AES-256 GCM means UnoLock encrypts Safe data on the client before it is uploaded or stored remotely. This is the core of UnoLock's zero-knowledge storage model.

This page is about **where encryption happens**. It is not the same as the separate question of **whether a payload is end-to-end encrypted while moving between endpoints**.

In UnoLock:

- Safe data is encrypted on the client.
- Encryption keys used for data protection remain under client control.
- Normal Safe access does not depend on a password-derived encryption secret.
- WebAuthn access keys handle authentication.
- The PIN is a separate control for access throttling, brute-force resistance, and deniability-related flows.

3.9.2 How It Works

- **Local encryption first**: records, files, and other protected Safe data are encrypted before leaving the client.
- **AES-256 GCM**: UnoLock uses authenticated encryption so ciphertext is protected for both confidentiality and integrity.
- **Client-controlled key material**: key material needed to protect data stays under client control rather than being exposed as reusable server-side plaintext.
- **Encrypted storage**: once uploaded, UnoLock stores ciphertext rather than plaintext user data.
- **Transport protection on top**: TLS protects the transport path, but the main privacy guarantee for stored data begins with client-side encryption.

3.9.3 Security Implications

- **Zero-knowledge storage model**: the server stores encrypted data rather than plaintext user content.
- **Reduced trust in infrastructure**: client-side encryption limits what storage systems, operators, or attackers can learn from stored data.
- **Tamper detection**: AES-256 GCM helps detect unauthorized modification of protected ciphertext.

3.9.4 Use Cases

- **Sensitive Safe records**: store legal, financial, operational, or personal records without exposing plaintext to UnoLock servers.
- **Crypto key protection**: seed phrases and related recovery material are encrypted before storage.
- **Shared infrastructure with private data**: cloud delivery and redundancy can be used without turning the server into the plaintext trust anchor.

3.9.5 Why It Matters

Client-side encryption answers a basic trust question: does the provider ever receive your data in plaintext as part of normal storage? In UnoLock's design, the answer is no for normal Safe storage flows.

3.9.6 FAQs

What is client-side encryption?

It means data is encrypted on your device before it is sent to the cloud or stored remotely.

Is client-side encryption the same as end-to-end encryption?

No. Client-side encryption describes where encryption happens. End-to-end encryption describes how protected data stays encrypted between intended endpoints. UnoLock uses both in different parts of the system.

Can UnoLock access my encrypted data?

Not as plaintext in the normal client-side encrypted storage model. UnoLock stores encrypted Safe data, not your unencrypted content.

Does UnoLock use passwords to derive the main Safe encryption?

No. Normal Safe access relies on WebAuthn access keys, not password-derived encryption. The main password-style exception is optional Space backup files used for controlled backup and restore workflows.

3.9.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: client-side encryption reduces plaintext exposure of personal and sensitive data and supports privacy-focused handling.

3.9.8 Integration with Other Features

- **FIDO2 Authentication with WebAuthn**: authenticates access to the Safe without turning passwords into the main trust anchor.
- **Advanced API Security**: protects application communication in addition to client-side protected storage.
- **Enhanced PIN Entry Security**: adds access throttling and brute-force resistance around local access flows without replacing the underlying cryptographic model.

3.10 Secure Direct Storage of Encrypted Data in AWS S3

3.10.1 Overview

The **Secure Direct Storage of Encrypted Data in AWS S3** feature ensures that all data stored in UnoLock CybVault is securely uploaded to **Amazon Web Services (AWS) Simple Storage Service (S3)**, leveraging robust encryption and direct access controls to maintain privacy and integrity. By integrating with UnoLock's client-side encryption, this feature guarantees that data remains encrypted during transit and at rest, accessible only to the user with the decryption key. AWS S3's scalable, durable infrastructure provides a reliable foundation for storing sensitive information, such as cryptocurrency keys, documents, or personal records, while UnoLock's security measures prevent unauthorized access, even in the event of a server breach.

3.10.2 How It Works

- **Client-Side Encryption**: Data is encrypted locally on the user's device using AES-256 GCM before being uploaded to AWS S3, ensuring that only encrypted data is transmitted and stored.
- **Secure Upload Process**: UnoLock uses direct, authenticated API calls to upload encrypted data to AWS S3 buckets, protected by TLS to prevent interception during transit.
- **AWS S3 Bucket Security**: Data is stored in private S3 buckets with strict access controls, including IAM policies and bucket-level encryption, to prevent unauthorized access.
- **Data Durability**: AWS S3's high durability (99.999999999% annually) ensures that encrypted data remains intact and available, with automatic replication across multiple availability zones.

3.10.3 Security Implications

- **Zero-Knowledge Storage**: Since data is encrypted client-side, AWS S3 servers cannot access or decrypt user data, maintaining UnoLock's zero-knowledge model.
- **Protection Against Server Breaches**: Even if AWS S3 servers are compromised, the encrypted data remains inaccessible without the user's decryption key.
- **Reliable Data Availability**: AWS S3's durability and redundancy ensure that encrypted data is always available, protecting against data loss due to hardware failures or disasters.

3.10.4 Use Cases

- **Cryptocurrency Key Storage**: Users can securely store encrypted private keys or mnemonic phrases in AWS S3, ensuring they are protected and accessible only to the owner.
- **Confidential Document Archiving**: Businesses or individuals can archive sensitive documents, such as legal or financial records, with confidence in their security and availability.
- **Global Data Access**: Users who need to access their vault from multiple locations benefit from AWS S3's global infrastructure, ensuring fast and secure data retrieval.

3.10.5 Why It Matters

Secure storage is critical for protecting digital assets in the cloud, where server breaches and unauthorized access are constant threats. By combining client-side encryption with AWS S3's robust infrastructure, UnoLock provides a secure, reliable, and scalable solution for storing sensitive data, ensuring user privacy and data integrity in all scenarios.

3.10.6 FAQs

How does UnoLock ensure data security in AWS S3?

UnoLock encrypts data client-side with AES-256 GCM before uploading it to private S3 buckets, ensuring that only the user can decrypt and access their data.

What happens if AWS S3 is hacked?

Since data is encrypted client-side, a breach of AWS S3 would not expose user data, as it remains inaccessible without the user's decryption key.

Can I access my data if an AWS data center goes offline?

AWS S3's replication across multiple availability zones ensures that your encrypted data remains available, even if a single data center experiences an outage.

3.10.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Secure direct storage in AWS S3, combined with client-side encryption, supports compliance with GDPR, HIPAA, and other data protection regulations by ensuring data privacy and security.

3.10.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: Works seamlessly with client-side encryption to ensure that all data stored in AWS S3 is encrypted locally, maintaining zero-knowledge privacy.
- **Dual-Layer Encryption with AWS S3 Server-Side Encryption (SSE)**: Enhances security by adding server-side encryption to client-side encrypted data, providing an additional layer of protection.

3.11 Dual-Layer Encryption with AWS S3 Server-Side Encryption (SSE)

3.11.1 Overview

The **Dual-Layer Encryption with AWS S3 Server-Side Encryption (SSE)** feature enhances UnoLock CybVault's security by combining **client-side encryption** with **AWS S3 Server-Side Encryption (SSE)**, providing an additional layer of protection for data stored in the cloud. While client-side encryption using AES-256 GCM ensures that data is encrypted before leaving the user's device, SSE applies a second encryption layer managed by AWS, safeguarding data at rest in S3 buckets. This dual-layer approach ensures that even if one encryption layer is compromised, the data remains secure, maintaining UnoLock's **zero-knowledge** model and protecting sensitive information like cryptocurrency keys, documents, or personal records.

3.11.2 How It Works

- **Client-Side Encryption**: Data is encrypted locally on the user's device using AES-256 GCM, ensuring that only the user with the decryption key can access the plaintext data.
- **Secure Transmission**: Encrypted data is transmitted to AWS S3 over TLS, protecting it from interception during transit.
- **AWS S3 Server-Side Encryption (SSE)**: Upon reaching S3, the encrypted data is further encrypted using AWS-managed keys (SSE-S3) or customer-provided keys (SSE-C), adding a second encryption layer at rest.
- **Key Management**: Client-side keys are managed locally by the user, while AWS S3 SSE keys are handled by AWS or the user (for SSE-C), ensuring separation of key control and enhancing security.

3.11.3 Security Implications

- **Enhanced Data Protection**: The dual-layer encryption ensures that data remains secure even if one encryption layer is compromised, as both client-side and server-side keys are required to access the plaintext.
- **Zero-Knowledge Integrity**: Client-side encryption maintains UnoLock's zero-knowledge model, while SSE adds an additional safeguard without compromising user privacy.
- **Resilience Against Server Breaches**: Even if AWS S3 servers are breached, the client-side encryption ensures that the data remains inaccessible without the user's key, and SSE provides an extra barrier.

3.11.4 Use Cases

- **High-Security Data Storage**: Users storing highly sensitive data, such as cryptocurrency keys or medical records, benefit from the added security of dual-layer encryption.
- **Regulatory Compliance**: Businesses subject to strict data protection regulations (e.g., GDPR, HIPAA) can use dual-layer encryption to ensure compliance with encryption requirements.
- **Global Enterprises**: Organizations with data stored across multiple regions can leverage AWS S3's infrastructure and UnoLock's encryption to maintain consistent security standards.

3.11.5 Why It Matters

In a cloud-based world, data breaches and unauthorized access are significant risks. The dual-layer encryption approach combines the strengths of client-side and server-side encryption, providing an extra layer of security that ensures user data remains protected, even in worst-case scenarios like server compromises. This feature reinforces UnoLock's commitment to privacy and security, making it a trusted solution for safeguarding digital assets.

3.11.6 FAQs

How does dual-layer encryption differ from client-side encryption alone?

Dual-layer encryption combines client-side AES-256 GCM encryption with AWS S3 SSE, adding a second encryption layer at rest to enhance security beyond client-side encryption.

Can AWS access my data with SSE?

No, AWS cannot access your data, as client-side encryption ensures that only you have the decryption key, and SSE is an additional layer managed by AWS or you (with SSE-C).

What happens if my client-side key is lost?

If your client-side key is lost, the data cannot be decrypted, as AWS S3 SSE alone cannot access the plaintext. UnoLock’s LockOutGuard feature can help recover access in such cases.

3.11.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Dual-layer encryption supports compliance with GDPR, HIPAA, and other regulations by ensuring that data is encrypted both client-side and server-side, minimizing the risk of unauthorized access.

3.11.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: Forms the foundation of the dual-layer approach, ensuring that data is encrypted locally before being sent to AWS S3.
- **Secure Direct Storage of Encrypted Data in AWS S3**: Works in tandem to securely upload and store client-side encrypted data in S3, where SSE is applied for additional protection.

3.12 Advanced Key Management with Client-Side Keyring

3.12.1 Overview

The **Advanced Key Management with Client-Side Keyring** feature lets UnoLock users securely generate, store, and manage encryption keys entirely on their local device, reinforcing the **zero-knowledge** security model. By maintaining a client-side keyring, UnoLock ensures that cryptographic keys, used for encrypting sensitive data like cryptocurrency wallets, documents, or personal records, never leave the user's device or are exposed to servers. This feature provides robust key management capabilities, including key generation, rotation, and backup, while protecting against unauthorized access and ensuring user control over their digital assets.

3.12.2 How It Works

- **Key Generation**: The client-side keyring generates cryptographic keys (e.g., AES-256 keys) locally on the user's device, using secure random number generation to ensure key strength.
- **Local Storage**: Keys are stored in a secure client-side keyring, protected by device-level security (e.g., secure enclave or encrypted storage), ensuring they never leave the device.
- **Key Rotation**: Users can periodically rotate keys to enhance security, with UnoLock facilitating seamless re-encryption of data using new keys without exposing them to servers.
- **Backup and Recovery**: The keyring supports secure key backup options, such as encrypted exports or integration with hardware tokens, allowing users to recover keys without compromising security.

3.12.3 Security Implications

- **Zero-Knowledge Privacy**: By keeping keys client-side, UnoLock ensures that servers, third parties, or attackers cannot access or misuse encryption keys, maintaining user privacy.
- **Protection Against Server Breaches**: Since keys are never stored on UnoLock's servers, a server compromise cannot expose user keys or decrypt data.
- **User Control**: The client-side keyring gives users full control over their keys, enabling secure management without reliance on external systems.

3.12.4 Use Cases

- **Cryptocurrency Wallet Security**: Users can manage encryption keys for cryptocurrency wallets within the client-side keyring, ensuring secure storage and access.
- **Sensitive Data Protection**: Individuals or businesses handling confidential data, such as legal or financial records, can use the keyring to securely manage encryption keys.
- **Multi-Device Key Management**: Users accessing their vault from multiple devices can synchronize encrypted keyring backups, maintaining consistent security across platforms.

3.12.5 Why It Matters

Effective key management is critical to maintaining the security of encrypted data. The client-side keyring ensures that users retain full control over their cryptographic keys, protecting against server-side vulnerabilities and reinforcing UnoLock's commitment to **zero-knowledge** privacy. This feature provides a robust, user-centric solution for safeguarding digital assets in an increasingly threat-prone environment.

3.12.6 FAQs

? What is a client-side keyring?

A client-side keyring is a secure, local repository on the user’s device that stores and manages cryptographic keys, ensuring they never leave the device or are exposed to servers.

? Can UnoLock access my encryption keys?

No, UnoLock operates a zero-knowledge model, meaning that all keys are generated and stored locally in the client-side keyring, inaccessible to UnoLock’s servers.

? What happens if I lose access to my device?

The keyring supports secure backup options, such as encrypted exports or hardware token integration, allowing key recovery without compromising security.

3.12.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: The client-side keyring ensures that encryption keys remain private and secure, supporting compliance with GDPR, HIPAA, and other data protection regulations by preventing unauthorized access.

3.12.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: The keyring manages the keys used for client-side encryption, ensuring secure encryption and decryption of data locally.
- **FIDO2 Authentication with WebAuthn**: Integrates with FIDO2 authentication to protect access to the keyring, ensuring only authorized users can manage or use the keys.

3.13 Advanced Data Deletion and Perfect Forward Secrecy

3.13.1 Overview

The **Advanced Data Deletion and Perfect Forward Secrecy** feature ensures that data removed from UnoLock CybVault is permanently deleted and cannot be recovered, while also guaranteeing that past communications and data remain secure even if future keys are compromised. By implementing secure data deletion protocols and **perfect forward secrecy (PFS)**, UnoLock protects user privacy by ensuring that deleted data, such as cryptocurrency keys, documents, or personal records, is irretrievable and that historical data sessions are isolated from future security breaches. This feature reinforces UnoLock's commitment to **zero-knowledge** privacy and robust data protection.

3.13.2 How It Works

- **Secure Data Deletion**: When a user deletes data (e.g., a safe, file, or record) from their vault, UnoLock employs cryptographic wiping techniques to overwrite and permanently remove the data from AWS S3 storage, ensuring it cannot be recovered.
- **Perfect Forward Secrecy (PFS)**: UnoLock uses ephemeral session keys for each data transaction or communication session, generated using Diffie-Hellman key exchange or similar protocols. These keys are discarded after use, ensuring that a compromised future key cannot decrypt past sessions.
- **Key Rotation**: The client-side keyring regularly rotates encryption keys, and deleted data is re-encrypted with new keys before removal, further isolating it from future access.
- **Audit and Verification**: UnoLock logs deletion requests securely using AWS CloudTrail, allowing users to verify that data has been permanently removed without retaining recoverable copies.

3.13.3 Security Implications

- **Irreversible Data Removal**: Secure deletion ensures that deleted data cannot be recovered by attackers, administrators, or forensic tools, protecting user privacy.
- **Protection Against Future Breaches**: PFS guarantees that even if a future encryption key is compromised, past data sessions remain secure, as each session uses unique, ephemeral keys.
- **Compliance with Privacy Standards**: The combination of secure deletion and PFS supports adherence to strict data protection regulations, ensuring that deleted data is unrecoverable and past communications are protected.

3.13.4 Use Cases

- **Sensitive Data Disposal**: Users handling sensitive information, such as cryptocurrency keys or legal documents, can permanently delete data with confidence that it cannot be recovered.
- **Privacy-Conscious Individuals**: Individuals in high-risk roles (e.g., journalists, activists) can use this feature to ensure that deleted data and past communications remain private, even in the event of a future breach.
- **Regulatory Compliance**: Businesses subject to data retention and deletion requirements (e.g., GDPR, HIPAA) can use UnoLock to securely delete data and maintain compliance.

3.13.5 Why It Matters

Data deletion and forward secrecy are critical for maintaining user trust and privacy in a digital world where data breaches and surveillance are prevalent. By ensuring that deleted data is permanently gone and past sessions are isolated from future compromises, UnoLock provides a robust solution for protecting digital assets and communications, aligning with its **zero-knowledge** and privacy-first principles.

3.13.6 FAQs

How does UnoLock ensure deleted data is unrecoverable?

UnoLock uses cryptographic wiping techniques to overwrite and permanently remove data from AWS S3, ensuring it cannot be recovered by any means.

What is perfect forward secrecy, and why is it important?

Perfect forward secrecy uses ephemeral session keys to ensure that past data sessions remain secure, even if future keys are compromised, protecting historical data from breaches.

Can deleted data be audited to confirm removal?

Yes, UnoLock logs deletion requests using AWS CloudTrail, allowing users to verify that data has been permanently removed without retaining recoverable copies.

3.13.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Advanced data deletion and PFS support compliance with GDPR, HIPAA, and other regulations by ensuring that deleted data is irretrievable and past communications are protected from future breaches.

3.13.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: Secure data deletion works with client-side encryption to ensure that only encrypted data is stored, and deletion removes all traces of the plaintext.
- **Advanced Key Management with Client-Side Keyring**: The keyring facilitates key rotation and secure key management, supporting PFS by generating and discarding ephemeral session keys.

3.14 SHA-256 Hash Verification of Uploaded Data

3.14.1 Overview

The **SHA-256 Hash Verification of Uploaded Data** feature ensures the integrity of data uploaded to UnoLock CybVault by using the **SHA-256** cryptographic hash function to verify that files, cryptocurrency keys, or records remain unchanged during transit and storage. By generating a unique hash for each piece of data on the client side and validating it against the stored data in AWS S3, UnoLock guarantees that uploaded content has not been tampered with or corrupted. This feature provides users with confidence that their sensitive information, such as financial records or digital assets, is stored exactly as intended, reinforcing UnoLock's commitment to **zero-knowledge** security and data reliability.

3.14.2 How It Works

- **Client-Side Hash Generation**: Before uploading data, UnoLock generates a SHA-256 hash, a unique 256-bit fingerprint, of the data on the user's device, ensuring the hash is computed locally.
- **Secure Upload**: The data, encrypted with AES-256 GCM, is uploaded to AWS S3 along with its SHA-256 hash, transmitted over TLS to prevent interception.
- **Server-Side Verification**: Upon receipt, AWS S3 recomputes the SHA-256 hash of the uploaded data and compares it to the client-provided hash to verify integrity.
- **Ongoing Validation**: When data is retrieved or accessed, UnoLock re-verifies the SHA-256 hash to ensure the stored data remains unaltered, alerting users to any discrepancies.

3.14.3 Security Implications

- **Data Integrity Assurance**: SHA-256 hash verification ensures that uploaded data remains unchanged, detecting any tampering or corruption during transit or storage.
- **Protection Against Malicious Alterations**: If an attacker attempts to modify uploaded data, the hash mismatch will flag the alteration, preventing compromised data from being used.
- **User Trust**: By verifying data integrity, UnoLock provides users with confidence that their sensitive information, such as cryptocurrency keys or documents, is stored exactly as intended.

3.14.4 Use Cases

- **Cryptocurrency Key Storage**: Users storing private keys or mnemonic phrases can verify that their data is uploaded and stored without alterations, ensuring secure access to digital assets.
- **Confidential File Transfers**: Businesses uploading sensitive documents, such as contracts or financial records, can confirm that files remain intact throughout the upload process.
- **Data Auditing**: Organizations requiring audit trails for data integrity can use SHA-256 verification to ensure that stored records match their original state.

3.14.5 Why It Matters

Data integrity is critical in a cloud-based environment where tampering, corruption, or transmission errors can compromise sensitive information. The SHA-256 hash verification feature provides a robust mechanism to detect and prevent such issues, ensuring that users' digital assets remain secure and reliable. This feature strengthens UnoLock's **zero-knowledge** architecture by guaranteeing that stored data is an exact replica of the user's original content.

3.14.6 FAQs

What is SHA-256 hash verification?

SHA-256 hash verification generates a unique fingerprint for data using the SHA-256 algorithm, allowing UnoLock to confirm that uploaded data remains unchanged during transit and storage.

How does UnoLock detect tampered data?

UnoLock compares the SHA-256 hash generated on the client side with the hash of the data received or stored in AWS S3, flagging any mismatches as potential tampering or corruption.

Can SHA-256 verification protect against all data alterations?

SHA-256 verification detects any changes to data, but it relies on secure upload processes (e.g., TLS) to prevent tampering during transit; UnoLock's architecture ensures this security.

3.14.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: SHA-256 hash verification supports compliance with GDPR, HIPAA, and other regulations by ensuring data integrity and protecting against unauthorized modifications.

3.14.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: Hash verification complements client-side encryption by ensuring that encrypted data remains unaltered, maintaining both confidentiality and integrity.
- **Secure Direct Storage of Encrypted Data in AWS S3**: Works with secure S3 storage to verify that uploaded data matches the original, enhancing trust in the storage process.

3.15 Robust Data Redundancy with AWS S3

3.15.1 Overview

The **Robust Data Redundancy with AWS S3** feature ensures that data stored in UnoLock CybVault is highly available and protected against loss by leveraging **Amazon Web Services (AWS) Simple Storage Service (S3)**'s advanced replication and durability capabilities. By distributing encrypted data across multiple geographic regions and availability zones, UnoLock guarantees that sensitive information, such as Bitcoin and Ethereum keys, documents, or personal records, remains accessible and intact, even in the face of hardware failures, natural disasters, or regional outages. This feature reinforces UnoLock's commitment to **zero-knowledge** security and reliable data preservation.

3.15.2 How It Works

- **Multi-Region Replication**: UnoLock stores encrypted data in AWS S3 buckets replicated across multiple geographic regions, ensuring that data is preserved even if a single region experiences an outage.
- **Availability Zone Redundancy**: Within each region, data is distributed across multiple availability zones (physically separate data centers), providing high availability and fault tolerance.
- **High Durability**: AWS S3 offers 99.999999999% (11 nines) durability, achieved through redundant storage and error correction, ensuring that data loss is virtually impossible.
- **Automated Recovery**: In the event of a failure, AWS S3 automatically redirects requests to redundant copies, ensuring seamless access to encrypted data without user intervention.

3.15.3 Security Implications

- **High Availability**: Multi-region and availability zone replication ensures that users can access their vault at any time, even during regional disruptions, maintaining operational continuity.
- **Data Loss Prevention**: AWS S3's extreme durability protects against data loss due to hardware failures, natural disasters, or other catastrophic events, safeguarding critical assets.
- **Zero-Knowledge Integrity**: Redundant data remains encrypted with client-side AES-256 GCM, ensuring that UnoLock's zero-knowledge model is preserved across all copies.

3.15.4 Use Cases

- **Bitcoin and Ethereum Asset Protection**: Users storing Bitcoin and Ethereum keys or Bitcoin and Ethereum digital paper wallets can rely on AWS S3 redundancy to ensure their assets are always accessible, even in the face of regional outages.
- **Business Continuity**: Enterprises managing sensitive records, such as financial or legal documents, benefit from uninterrupted access and protection against data loss.
- **Global Access**: Users who travel or operate across multiple regions can access their vault seamlessly, with data replicated globally for low-latency retrieval.

3.15.5 Why It Matters

Data availability and resilience are critical in a cloud-based environment where outages, hardware failures, or disasters can disrupt access to sensitive information. By leveraging AWS S3's robust redundancy, UnoLock ensures that users' digital assets remain secure, accessible, and protected against loss, providing peace of mind and reinforcing the platform's reliability within its **zero-knowledge** framework.

3.15.6 FAQs

How does AWS S3 redundancy protect my data?

AWS S3 replicates encrypted data across multiple regions and availability zones, ensuring that it remains accessible and protected against hardware failures or regional outages.

What happens if an AWS region goes offline?

UnoLock’s multi-region replication ensures that your data is available from other regions, with AWS S3 automatically redirecting requests to redundant copies.

Does redundancy compromise my data’s security?

No, all redundant copies are encrypted with client-side AES-256 GCM, maintaining UnoLock’s zero-knowledge model and ensuring that only you can decrypt the data.

3.15.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Robust data redundancy supports compliance with GDPR, HIPAA, and other regulations by ensuring data availability and integrity while maintaining client-side encryption for privacy.

3.15.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: Redundant data is encrypted client-side, ensuring that all copies remain secure and accessible only to the user with the decryption key.
- **Secure Direct Storage of Encrypted Data in AWS S3**: Works with secure S3 storage to replicate encrypted data across regions, enhancing availability without compromising security.

3.16 No Browser Local Storage or Cookies Used

3.16.1 Overview

The **No Browser Local Storage or Cookies Used** feature enhances UnoLock CybVault's privacy by eliminating the use of browser local storage and cookies, which are common vectors for tracking and data exposure. By avoiding these mechanisms, UnoLock ensures that no sensitive data, such as session information, user preferences, or cryptographic keys, is stored in the browser, reducing the risk of unauthorized access via browser vulnerabilities or malicious extensions. This feature reinforces UnoLock's **zero-knowledge** model, ensuring that user interactions with the vault leave no traceable footprint on the client device, providing maximum privacy for sensitive data like cryptocurrency keys, documents, or personal records.

3.16.2 How It Works

- **No Local Storage**: UnoLock does not use browser local storage (e.g., `localStorage` or `sessionStorage`) to store any data, ensuring that no session tokens, keys, or user information persist on the device after the session ends.
- **No Cookies**: The application avoids HTTP cookies, preventing any tracking mechanisms or session identifiers from being stored in the browser, which could be exploited by attackers or third parties.
- **Stateless Sessions**: UnoLock employs stateless session management, where session data is handled server-side with encrypted tokens that expire after use, leaving no trace in the browser.
- **Client-Side Processing**: All sensitive operations, such as encryption and key management, are performed in memory during the session and cleared upon logout, ensuring no residual data remains in the browser.

3.16.3 Security Implications

- **Reduced Attack Surface**: By eliminating local storage and cookies, UnoLock minimizes the risk of data exposure through browser vulnerabilities, malicious extensions, or cross-site scripting (XSS) attacks.
- **Enhanced Privacy**: Avoiding cookies prevents tracking by third parties, ensuring that user interactions with the vault are not linked to their browsing activity or identity.
- **Protection Against Device Compromise**: Even if a user's device is compromised, no sensitive data is stored in the browser, reducing the likelihood of key or session theft.

3.16.4 Use Cases

- **High-Privacy Users**: Individuals in privacy-sensitive roles, such as journalists or activists, can use UnoLock without leaving traceable data in their browser, protecting against surveillance or tracking.
- **Public or Shared Devices**: Users accessing their vault from public computers (e.g., libraries, internet cafés) benefit from the absence of local storage, ensuring no data is left behind.
- **Enterprise Security**: Businesses can deploy UnoLock for employees, confident that no sensitive session data is stored in browsers, reducing risks on corporate devices.

3.16.5 Why It Matters

Browser local storage and cookies are common targets for attackers seeking to steal session data, track users, or exploit vulnerabilities. By completely avoiding these mechanisms, UnoLock significantly enhances user privacy and security, ensuring that no sensitive information is left vulnerable on the client side. This feature is a critical component of UnoLock's **zero-knowledge** architecture, aligning with its mission to provide a secure, untraceable vault experience.

3.16.6 FAQs

Why does UnoLock avoid browser local storage and cookies?

UnoLock avoids these mechanisms to prevent tracking, reduce the risk of data exposure through browser vulnerabilities, and ensure no sensitive information remains on the device after a session.

How does UnoLock manage sessions without cookies?

UnoLock uses stateless session management with encrypted, server-side tokens that expire after use, ensuring secure sessions without storing data in the browser.

Is it safe to use UnoLock on a public computer?

Yes, the absence of local storage and cookies ensures that no session data or keys are left behind, making it safe to use UnoLock on public or shared devices.

3.16.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: By avoiding local storage and cookies, UnoLock minimizes the risk of unintended data collection or exposure, supporting compliance with GDPR, HIPAA, and other privacy regulations.

3.16.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: Ensures that all sensitive operations are performed in memory and cleared after use, complementing the absence of local storage for maximum security.
- **No Browser Local Storage or Cookies Used**: Works with stateless session management to maintain privacy and security during user interactions, leaving no traceable data in the browser.

3.17 Commitment to Anonymity and Data Privacy

3.17.1 Overview

UnoLock approaches anonymity as an OPSEC problem, not just a marketing claim. Safe access is built around registered access keys, client-side encryption, end-to-end protected messaging and API payloads, and a payment model designed to stay separated from Safe contents and normal Safe identity. The result is a system that minimizes the amount of information UnoLock needs in order to operate.

3.17.2 How It Works

- **No Conventional Safe Accounts**: Safe creation and Safe access do not depend on usernames, email logins, or stored passwords.
- **Access Keys Instead of Passwords**: Users authenticate with passkeys, hardware keys, or compatible device authenticators through WebAuthn.
- **Client-Side Encryption**: Safe data is encrypted before it leaves the client, so UnoLock does not hold the plaintext needed to read records or files.
- **End-to-End Protected Messaging and API Calls**: Messaging payloads and protected API traffic are encrypted in addition to normal transport security.
- **Minimal Client Traces**: UnoLock avoids browser storage patterns that are commonly used for tracking or session persistence.
- **Payment Separation**: Billing is handled separately from Safe contents so routine payment operations do not need to expose what is inside a Safe.

3.17.3 Security Implications

- **Reduced Identity Coupling**: Because Safe access is not built around a normal account/password model, there is less identity linkage to attack or subpoena in ordinary use.
- **Reduced Server Exposure**: Client-side encryption and encrypted payloads limit what a server-side compromise can reveal.
- **Lower Tracking Surface**: Fewer identifiers and less persistent client storage reduce the amount of correlation data available across sessions.

3.17.4 Use Cases

- **Privacy Advocates**: Users can manage sensitive records without adopting a conventional cloud identity model.
- **High-Risk Professions**: Journalists, activists, or whistleblowers can reduce identity linkage while protecting sensitive material.
- **Operational Security Workflows**: Users who care about payment separation, minimal metadata, and device-bound access keys can keep those properties aligned in one system.

3.17.5 Why It Matters

Privacy in UnoLock is not one feature. It is the combined result of access-key authentication, client-side encryption, end-to-end protected payloads, limited browser traces, and payment separation. That approach gives users a stronger base for anonymity than simply hiding a username behind an encrypted database.

3.17.6 FAQs

? Does UnoLock require an email address or password to open a Safe?

No. Safe access is based on registered access keys such as passkeys or hardware keys, not on a conventional email-and-password account model.

Is anonymity only about encryption?

No. Encryption is part of it, but UnoLock also relies on metadata minimization, limited client traces, and separation between billing and Safe contents.

Can UnoLock read what is inside my Safe?

No. Safe data is encrypted client-side before syncing, so UnoLock does not receive the plaintext needed to read the contents.

3.17.7 Compliance & Privacy Regulations

- **Privacy by Design**: The architecture supports privacy-focused operation by minimizing plaintext exposure and reducing unnecessary identity coupling.

3.17.8 Integration with Other Features

- **No Browser Local Storage or Cookies Used**: Reduces persistent browser traces.
- **Client-Side Encryption Using AES-256 GCM**: Keeps Safe contents encrypted before sync.
- **Advanced API Security with AES-256 GCM and ECDHE_ECDSA**: Protects sensitive client-server payloads in addition to transport security.

3.18 Advanced API Security

3.18.1 Overview

Advanced API Security explains how UnoLock protects application traffic between the client and the UnoLock service.

This page matters because there is often confusion between:

- **TLS transport encryption**
- **client-side encrypted stored data**
- **end-to-end encrypted application payloads**

UnoLock does not rely on TLS alone as the full explanation of API confidentiality. API traffic also uses application-layer protection so that protected payloads are not treated as ordinary plaintext requests moving over HTTPS.

3.18.2 How It Works

- **TLS 1.3 transport security**: the network channel is protected against passive interception and standard transport-layer attacks.
- **Protected application payloads**: sensitive API data is protected at the application layer rather than relying only on HTTPS transport.
- **Client-side encryption before storage**: when the API is carrying Safe data for storage, that data has already been encrypted client-side before upload.
- **Endpoint-oriented design**: the API exists to move protected data between the UnoLock client and service boundary without turning the server into a plaintext trust anchor for normal storage flows.
- **Authentication separate from encryption**: WebAuthn access keys authenticate users, while encryption protects data payloads.

3.18.3 Security Implications

- **Transport plus payload protection**: attackers do not get ordinary plaintext API data simply because they can observe the network path.
- **Lower server trust requirements**: protected payload handling reduces unnecessary plaintext exposure in backend systems.
- **Cleaner threat separation**: transport encryption, application payload encryption, authentication, and client-side stored-data encryption each do a different job.

3.18.4 Use Cases

- **Normal Safe sync and access**: records and files move through the API without requiring plaintext trust in the transport path alone.
- **Untrusted network access**: the combination of TLS and protected application payloads hardens communication over hostile or shared networks.
- **Regulated environments**: security teams can distinguish between storage encryption, transport encryption, and endpoint-to-endpoint payload protection.

3.18.5 Why It Matters

If people hear "the data is client-side encrypted" they may still ask what protects API traffic. If they hear "the API uses HTTPS" they may still ask whether payloads are protected beyond transport. This page answers that gap: UnoLock protects API traffic as part of a layered model, not as a single control.

3.18.6 FAQs

Is UnoLock API security just HTTPS?

No. TLS is one layer, but UnoLock also protects sensitive API payloads at the application level and uses client-side encryption for stored Safe data.

Is API encryption the same thing as client-side encryption?

No. Client-side encryption protects data before upload and at storage time. API encryption protects the communication path and protected payload exchange.

Does UnoLock use passwords as the main secret for API security?

No. UnoLock uses WebAuthn-based authentication for normal Safe access. Password-style secrets are not the normal root of trust for Safe data or API protection.

3.18.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: layered transport and payload protection help reduce unnecessary exposure of personal and sensitive data during transmission.

3.18.8 Integration with Other Features

- **Client-Side Encryption Using AES-256 GCM**: protects stored Safe data before it is sent through the API.
- **End-to-End Encryption**: explains the broader endpoint-to-endpoint protection model used across messaging and protected API flows.
- **Commitment to Anonymity and Data Privacy**: reduces linkable exposure while protected data moves through the service.

3.19 Secure Deletion of Safes and Encrypted File Records

3.19.1 Overview

The **Secure Deletion of Safes and Encrypted File Records** feature ensures that when users delete safes or encrypted file records from UnoLock CybVault, the data is permanently and irretrievably removed from all storage locations, leaving no recoverable traces. By employing cryptographic wiping techniques and secure deletion protocols, UnoLock guarantees that sensitive information, such as cryptocurrency keys, confidential documents, or personal records, cannot be restored by unauthorized parties, even with advanced forensic tools. This feature reinforces UnoLock's **zero-knowledge** security model, providing users with confidence that their deleted data is truly gone, enhancing privacy and compliance with stringent data protection standards.

3.19.2 How It Works

- **Cryptographic Wiping**: When a user deletes a safe or file record, UnoLock overwrites the encrypted data with random cryptographic patterns, ensuring that the original data is unrecoverable from AWS S3 storage.
- **Multi-Pass Deletion**: UnoLock employs multi-pass deletion techniques, repeatedly overwriting data to prevent recovery, adhering to industry standards for secure data destruction.
- **Metadata Removal**: All associated metadata, such as file names or access logs, is also securely deleted, leaving no trace of the safe or file's existence on the server.
- **Audit Logging**: Deletion operations are logged securely using AWS CloudTrail, providing an auditable record of the deletion process without retaining recoverable data.

3.19.3 Security Implications

- **Permanent Data Removal**: Secure deletion ensures that deleted safes and files cannot be recovered by attackers, administrators, or forensic tools, protecting user privacy.
- **Protection Against Data Breaches**: Even if a server is compromised, no residual data or metadata remains, reducing the risk of exposure for deleted information.
- **Compliance Readiness**: The feature supports adherence to data protection regulations requiring secure data destruction, ensuring that deleted data is irretrievable.

3.19.4 Use Cases

- **Sensitive Data Management**: Users handling sensitive information, such as cryptocurrency keys or legal documents, can permanently delete data to prevent unauthorized recovery.
- **Regulatory Compliance**: Businesses subject to data retention and deletion requirements (e.g., GDPR, HIPAA) can use secure deletion to meet compliance obligations.
- **Privacy-Conscious Individuals**: Users in high-risk environments, such as activists or journalists, can delete safes or files with confidence that no traces remain.

3.19.5 Why It Matters

In a digital world where data breaches and forensic recovery pose significant risks, secure deletion is essential for protecting user privacy and ensuring compliance. UnoLock's secure deletion feature guarantees that deleted safes and encrypted file records are permanently removed, leaving no opportunity for unauthorized access. This feature strengthens UnoLock's **zero-knowledge** architecture, providing users with control over their data's lifecycle and peace of mind that their sensitive information is truly gone when deleted.

3.19.6 FAQs

How does UnoLock ensure deleted data is unrecoverable?

UnoLock uses cryptographic wiping and multi-pass deletion to overwrite encrypted data and metadata, ensuring no traces remain that could be recovered with forensic tools.

Can deleted safes or files be restored by UnoLock?

No, once a safe or file is deleted, it is permanently removed from all storage locations, and UnoLock's zero-knowledge model ensures that no recovery is possible.

Is there a record of deletion activities?

Yes, UnoLock logs deletion operations securely using AWS CloudTrail, providing an auditable trail without retaining any recoverable data.

3.19.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Secure deletion supports compliance with GDPR, HIPAA, and other regulations by ensuring that deleted data is irretrievable, meeting strict data protection and destruction requirements.

3.19.8 Integration with Other Features

- **Advanced Data Deletion and Perfect Forward Secrecy**: Complements broader data deletion protocols by focusing specifically on safes and file records, ensuring comprehensive data removal.
- **Client-Side Encryption Using AES-256 GCM**: Ensures that only encrypted data is stored, and secure deletion removes all traces of this data, maintaining zero-knowledge privacy.

3.20 Plausible Deniability with Safeword Wipe

3.20.1 Overview

Plausible Deniability with Safeword Wipe is UnoLock's HighRisk coercion-response feature. Users mark selected Spaces as sensitive, then configure a safeword PIN. When that safeword PIN is entered, the server applies the feature so the sensitive Spaces are deleted rather than shown. This is designed for users whose threat model values removing those sensitive Spaces over preserving them.

3.20.2 How It Works

- **Separate Safeword PIN**: Users configure a PIN that is distinct from the normal Safe PIN.
- **Sensitive Spaces Selection**: Users choose which Spaces should be treated as sensitive.
- **Server-Side Handling**: The entered PIN is received by the server, which applies the safeword outcome there rather than relying on the local device to branch visibly.
- **Sensitive Space Deletion**: When the safeword PIN is used, the Spaces marked as sensitive are deleted.

3.20.3 Security Implications

- **Maximum Protection for Marked Spaces**: The selected sensitive Spaces are removed rather than merely hidden.
- **Plausible Deniability on a Compromised Device**: Because the server applies the outcome, the local device should not visibly reveal that the safeword PIN was used.
- **Permanent Loss Tradeoff**: Security is gained by accepting irreversible deletion of the Spaces marked as sensitive.

3.20.4 Use Cases

- **Journalists and Whistleblowers**: For situations where specific sensitive Spaces could endanger sources or lives.
- **Activists in Hostile Environments**: For scenarios where continued existence of certain Spaces creates unacceptable risk.
- **Executives Handling Critical Secrets**: For threat models where deletion of selected Spaces is preferable to exposure.
- **Shared Space Caution**: If a marked sensitive Space is also a Shared Space, ownership determines whether deletion propagates to every participant.

3.20.5 Why It Matters

Some users need more than hiding. They need the option to delete the most sensitive Spaces if the alternative is catastrophic exposure. Safeword Wipe exists for that narrower but serious category of risk.

3.20.6 FAQs

How is this different from DuressDecoy?

DuressDecoy hides selected sensitive Spaces. HighRisk Plausible Deniability deletes selected sensitive Spaces.

Can UnoLock restore a Safe after Safeword Wipe?

Deleted sensitive Spaces are not meant to be recoverable through UnoLock.

Should everyone use this feature?

No. It is appropriate only for users whose threat model justifies permanent loss of data.

What if a sensitive Space is also a Shared Space?

If the owner Safe deletes the Shared Space, it is deleted for every participating Safe. If a non-owner Safe loses access to it, the data remains for the owner and other participants.

3.20.7 Compliance & Privacy Regulations

- **High-Risk Disclosure Control**: The feature is designed for users who need a decisive response to coercion or seizure.

3.20.8 Integration with Other Features

- **Spaces**: Plausible Deniability acts on Spaces that have been marked as sensitive.
- **DuressDecoy**: Provides the hiding-based alternative for users who do not want deletion.

3.21 DuressDecoy: Protection Against Coercion

3.21.1 Overview

DuressDecoy is UnoLock's coercion-response feature for the Sovereign tier. Users mark selected Spaces as sensitive, then configure a safeword PIN. When that safeword PIN is entered, the server applies the DuressDecoy behavior so those sensitive Spaces are hidden rather than shown. The server-side handling is important because a compromised device should not reveal, through distinct local behavior, that the safeword PIN was used instead of the normal PIN.

3.21.2 How It Works

- **Sensitive Spaces Selection**: Users choose which Spaces should be treated as sensitive.
- **Safeword PIN**: Users configure a safeword PIN that is different from the normal Safe PIN.
- **Server-Side Handling**: The entered PIN is received by the server, which applies the duress behavior there rather than relying on the local device to behave differently.
- **Hidden Sensitive Spaces**: When the safeword PIN is used, the Spaces marked as sensitive are hidden.

3.21.3 Security Implications

- **Coercion Resistance**: Users can open the Safe under pressure without exposing Spaces that were premarked as sensitive.
- **Plausible Deniability on a Compromised Device**: Because the server applies the outcome, an adversary watching the device should not be able to distinguish the safeword path from the normal path through local signals.
- **Recoverability**: In the Sovereign tier, the sensitive Spaces are hidden rather than deleted.

3.21.4 Use Cases

- **Journalists and Activists**: Hide selected Spaces when forced to open a Safe under pressure.
- **Crypto Users**: Protect seed phrases or wallet records without accepting permanent deletion.
- **Professionals Under Travel Risk**: Use the safeword PIN in checkpoint or device-search scenarios so sensitive Spaces do not appear.
- **Shared Space Caution**: If a marked sensitive Space is also a Shared Space, owner-versus-participant behavior matters.

3.21.5 Why It Matters

Not every threat model justifies permanent deletion. DuressDecoy gives users a narrower response: hide the Spaces that matter most while keeping the broader Safe intact.

3.21.6 FAQs

? How is DuressDecoy different from Plausible Deniability?

DuressDecoy hides selected sensitive Spaces. HighRisk Plausible Deniability deletes selected sensitive Spaces instead.

? Does DuressDecoy create a fake or decoy Safe?

No. DuressDecoy acts on Spaces marked as sensitive. It does not create a separate decoy Safe.

Why is DuressDecoy handled server-side?

It is handled server-side so a compromised device does not expose, through different local behavior, that the safeword PIN was entered.

What if a marked sensitive Space is also a Shared Space?

If the owner Safe deletes the Shared Space, it is deleted for every participating Safe. If a non-owner Safe loses access to it, the data remains for the owner and other participants.

3.21.7 Compliance & Privacy Regulations

- **Protected Disclosure Model**: DuressDecoy helps users reduce exposure of sensitive Spaces during coercive events.

3.21.8 Integration with Other Features

- **Plausible Deniability with Safeword Wipe**: Provides the deletion-based alternative for higher-risk scenarios.
- **TimeLock**: Can complement coercion resistance with time-based access restrictions.

3.22 LockoutGuard: Anti-Lockout Protection and One-Time Recovery

3.22.1 Overview

LockoutGuard helps users regain access to a Safe after losing a key or device without turning recovery into a permanent second login system. It is designed as a one-time alternative recovery path that returns the Safe to the normal WebAuthn access-key model after use.

3.22.2 How It Works

- **Recovery Material**: Users create recovery material that is stored outside the normal day-to-day Safe access flow.
- **One-Time Recovery Access**: LockoutGuard supports a controlled recovery flow that restores access temporarily so the user can recover the Safe.
- **Client-Side Verification**: Recovery processes are executed client-side, with no decryption keys or sensitive data sent to UnoLock's servers, maintaining the zero-knowledge model.
- **Inactivity Trigger and Warning Window**: LockoutGuard uses a configured inactivity interval and warning period before the recovery path becomes relevant.
- **Forced WebAuthn Re-Registration**: After recovery is used, the user must register again with WebAuthn. That registration replaces the temporary recovery route.

3.22.3 Security Implications

- **Anti-Lockout Protection**: LockoutGuard reduces the risk of permanent data loss due to lost keys or devices.
- **Maintained Privacy**: Client-side encryption and verification ensure that recovery processes do not expose sensitive data, preserving UnoLock's zero-knowledge architecture.
- **Protection Against Abuse**: The inactivity trigger, warning period, and recovery verification mechanisms help prevent malicious actors from exploiting recovery processes.
- **Recovery Boundaries**: Because the recovery route is removed after use, LockOutGuard does not remain as a standing parallel access channel.

3.22.4 Use Cases

- **Individual Users**: Crypto investors or individuals storing sensitive documents can recover access to their Safe if they lose their primary key or device.
- **Enterprise Teams**: Businesses can implement recovery protocols for employees, ensuring access to shared Safes is restored securely.
- **High-Risk Scenarios**: Users in unstable regions can use LockOutGuard for continuity planning without turning recovery into a standing second login path.

3.22.5 Why It Matters

Losing access to a secure Safe can be catastrophic. LockoutGuard provides a recovery path without redefining recovery as a permanent alternative login method. That distinction matters because UnoLock treats WebAuthn access keys as the normal authentication model and recovery as the exception.

3.22.6 FAQs

How does LockoutGuard prevent lockouts without compromising security?

LockoutGuard uses recovery material and client-side verification to restore access securely without exposing data to servers. After recovery is used, the user must register again with WebAuthn and the temporary recovery route is removed.

What happens if I lose all my recovery keys?

If all recovery options are lost, access may be unrecoverable due to UnoLock’s zero-knowledge model, emphasizing the importance of securely storing backups.

Can the inactivity timing be bypassed in an emergency?

LockoutGuard depends on the configured inactivity and warning settings. Users should choose those settings carefully based on their recovery needs.

3.22.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: LockoutGuard supports compliance with GDPR, HIPAA, and other regulations by ensuring recovery processes are secure, private, and do not expose sensitive data on servers.

3.22.8 Integration with Other Features

- **Robust Key Management with Multi-Key Registration and WebAuthn**: Complements multi-key registration by providing recovery options for registered keys, enhancing access redundancy.
- **Client-Side Encryption Using AES-256 GCM**: Ensures that recovery keys and processes are encrypted locally, maintaining zero-knowledge privacy throughout the recovery workflow.

3.23 Robust Key Management with Multi-Key Registration and WebAuthn

3.23.1 Overview

UnoLock allows one Safe to be opened by multiple registered access keys. Each key can be a passkey, hardware key, phone-based authenticator, or other supported WebAuthn authenticator. This gives users redundancy across devices and also allows multiple people to share the same Safe while each person keeps their own key.

3.23.2 How It Works

- **Multiple Registered Access Keys**: A Safe can have more than one registered access key, up to the limits of the user’s tier.
- **WebAuthn Authentication**: Each key uses phishing-resistant public-key authentication rather than a shared password.
- **Independent User Keys**: Multiple people can access the same Safe with their own keys instead of sharing one credential.
- **Permission Control**: Access keys can be granted full Safe administration or narrower rights such as selected Spaces.
- **Key Revocation**: Lost or retired keys can be removed without changing every other key on the Safe.

3.23.3 Security Implications

- **No Shared Password Secret**: Users do not need to pass around a common login secret to collaborate.
- **Phishing Resistance**: WebAuthn reduces exposure to replay, credential stuffing, and fake login pages.
- **Operational Redundancy**: Losing one key does not have to mean losing the Safe if other authorized keys remain.

3.23.4 Use Cases

- **Multiple Devices**: One person can register a laptop passkey, phone passkey, and hardware key for the same Safe.
- **Family or Team Access**: Several people can share one Safe while each retains their own access key.
- **Granular Collaboration**: An admin can keep full control while granting another access key limited access to selected Spaces.

3.23.5 Why It Matters

Because UnoLock is cloud-based, the real control point is not the device, it is the access key. Multi-key registration makes that model practical by letting users spread access safely across devices and people without weakening the Safe into a shared-password workflow.

3.23.6 FAQs

What kinds of access keys can I register?

Supported WebAuthn authenticators such as passkeys, hardware keys, and compatible device authenticators.

Can multiple people share the same Safe?

Yes. Each person can have their own access key for the same Safe, with either limited rights or full administration depending on what is granted.

What happens if one access key is lost?

Other authorized keys can still be used, and the lost key can be revoked from the Safe.

3.23.7 Compliance & Privacy Regulations

- **Secure Authentication**: WebAuthn-based key registration supports strong authentication without requiring shared passwords.

3.23.8 Integration with Other Features

- **FIDO2 Authentication with WebAuthn**: Provides the underlying authentication model.
- **Access Keys, Limited Access, and TimeLock**: Explains the difference between key permissions and temporary per-key TimeLock behavior.

3.24 Access Keys, Limited Access, and TimeLock

3.24.1 Overview

UnoLock access keys can be granted different levels of authority. Some keys can fully administer the Safe, while others can be limited to narrower access such as selected Spaces. TimeLock is a separate feature: it temporarily locks an individual access key for a selected period of time. It does not define admin or read-only permissions.

3.24.2 How It Works

- **Admin Access Keys**: Admin keys can manage the Safe, register or revoke other keys, and change access settings.
- **Limited-Access Keys**: Other keys can be constrained to narrower Safe or Space permissions.
- **Separate TimeLock Feature**: TimeLock can be applied to an individual access key for a selected number of hours when the Safe is closed.
- **Different Purposes**: Key permissions define what a key is allowed to do. TimeLock defines when a specific key can next be used.

3.24.3 Security Implications

- **Granular Delegation**: Users can share the same Safe without making every participant a full administrator.
- **Reduced Change Risk**: Read-only or limited keys lower the chance of accidental or malicious modification.
- **Short-Term Delay Option**: TimeLock can make a specific key temporarily unusable during a brief high-risk period.

3.24.4 Use Cases

- **Family Safes**: One person keeps admin rights while another person receives limited access to selected areas.
- **Team Operations**: A collaborator can be given visibility without full administrative control.
- **Checkpoint Protection**: A specific access key can be time-locked for a few hours before a risky situation such as a checkpoint or search.

3.24.5 Why It Matters

The important distinction in UnoLock is not just who can open a Safe, but what each access key is allowed to do once inside. Key permissions and TimeLock solve different problems and should not be treated as the same feature.

3.24.6 FAQs

? What is the difference between admin and limited access?

Admin access can manage the Safe and other keys. Limited access applies narrower permissions such as selected Spaces.

? Can access be restricted to only some Spaces?

Yes. UnoLock can grant narrower access to selected Spaces instead of full Safe administration.

? Is TimeLock the feature that creates admin or read-only access?

No. TimeLock is a temporary per-key delay. Access levels are handled by key management and Space permissions.

3.24.7 Compliance & Privacy Regulations

- **Controlled Access Management**: Key permissions and temporary key delays help users apply least-privilege access in sensitive environments.

3.24.8 Integration with Other Features

- **Robust Key Management with Multi-Key Registration and WebAuthn**: Supplies the registered access keys.
- **Spaces Granular Data Access and Control**: Works with Space-level boundaries inside the same Safe.
- **TimeLock**: Temporarily locks a specific access key without changing its underlying permission level.

3.25 Secure File Viewing

3.25.1 Overview

Secure File Viewing lets users preview supported attachments directly inside the authenticated UnoLock client instead of forcing export to external apps. This keeps sensitive content inside the same browser security boundary used by the vault and messaging flows.

The goal is to reduce accidental disclosure while preserving usability: render in-app when possible, decrypt client-side, and avoid unnecessary persistence.

3.25.2 How It Works

- **Client-side decryption**: Files are decrypted in the browser during an authenticated session; plaintext is not sent back to the server.
- **In-app rendering**: Supported formats (including PDF, images, audio/video, text-like files, and DOCX) can be viewed inside the client UI.
- **Sandboxed text/DOCX preview**: Text and converted DOCX content render in a sandboxed iframe (`sandbox="allow-scripts"`), isolating preview content from the main app context.
- **Hardened PDF controls**: PDF viewer download/print/open-file and editor tools are disabled in the embedded viewer configuration.
- **Ephemeral object URLs**: Blob URLs created for inline previews are revoked when the viewer closes, reducing leftover in-memory references.

3.25.3 Security Implications

- **Reduced exposure surface**: Keeping previews in-app lowers the need to open files in third-party software.
- **Zero-knowledge alignment**: Content remains encrypted at rest and is decrypted only on the client at view time.
- **Compartmentalized execution**: Sandboxed preview rendering and CSP help limit the blast radius of malformed content.

3.25.4 Important Limits

- **No web app can guarantee screenshot prevention**: OS-level screenshots, cameras, or compromised endpoints remain possible.
- **Endpoint trust still matters**: If a device or browser is compromised, viewed data may still be exposed.
- **Use operational controls for high-risk material**: Combine secure viewing with hardened devices, short sessions, and least-privilege sharing policies.

3.25.5 Use Cases

- **Reviewing sensitive attachments** without immediately exporting to local disk.
- **Validating inbound files in Vault Messaging** before deciding whether to save or process them.
- **Handling one-off disclosures from UnoLock Drop** while minimizing additional handling steps.

3.25.6 FAQs

Does Secure File Viewing block screenshots?

Not reliably at the OS level. Secure File Viewing reduces exposure inside the web app, but no browser application can fully prevent endpoint capture.

❓ Does UnoLock decrypt files server-side for viewing?

No. Viewing is client-side; the server does not need plaintext file content for preview.

❓ What is the current UnoLock Drop URL?

The sender-only Drop client URL is `https://drop.unolock.com` (legacy `vaultx.unolock.com` links should be migrated).

3.25.7 Compliance & Privacy

- **Privacy-first design**: In-app viewing supports data-minimization goals by reducing unnecessary file exports and keeping decryption client-side.

3.25.8 Integration with Other Features

- **Vault Messaging**: Securely review received attachments before save/import workflows.
- **UnoLock Drop**: Receive Address submissions can be inspected in-app after decryption.
- **FIDO2/WebAuthn authentication**: Viewing happens inside an authenticated Safe session.

3.26 Inactivity-Triggered Safe Access Methods: LockoutGuard and LegacyLink

3.26.1 Overview

LockoutGuard and LegacyLink are UnoLock's inactivity-triggered continuity features. They exist to handle the exception cases where a user loses access or where a Safe must pass to a successor after prolonged inactivity. In both cases, the temporary path is removed after use and the Safe is returned to the normal WebAuthn access-key model.

3.26.2 How It Works

- **LockoutGuard Recovery**:
- **Inactivity Detection**: Monitors user activity and triggers recovery options after a user-defined inactivity period.
- **Recovery Material**: Users set up recovery material that is stored outside the normal day-to-day Safe access flow.
- **One-Time Recovery Flow**: Provides a temporary alternative recovery method for access restoration, processed client-side.
- **Return to Primary Access Model**: After recovery succeeds, the user must register again with WebAuthn, and the temporary recovery path is removed.
- **LegacyLink Inheritance**:
- **Configured Through LockoutGuard**: Users set LegacyLink from the LockoutGuard area and choose a delay after LockoutGuard has been triggered.
- **Dormant Credential**: Setup creates a dormant LegacyLink credential with an access ID and passphrase that can be stored or given to a trusted person.
- **One-Time Succession Access**: When the configured conditions are met, the LegacyLink credential can be used to begin recovery of the Safe.
- **Return to Primary Access Model**: After LegacyLink is used, the recovering person must register a new access key, replacing the temporary succession path.
- **Zero-Knowledge Privacy**: Both features process sensitive operations client-side, with no decryption keys or data stored on UnoLock’s servers, maintaining user privacy.

3.26.3 Security Implications

- **Preventing Permanent Lockouts**: LockoutGuard ensures users can recover access without server intervention, reducing data loss risks while preserving zero-knowledge security.
- **Secure Succession Path**: LegacyLink provides a bounded succession route without turning succession into a permanent second login method.
- **Temporary Recovery Paths**: Both mechanisms are bounded alternatives, not permanent secondary login methods.
- **WebAuthn Restoration**: After either method is used, UnoLock restores the Safe to the primary WebAuthn access-key model.
- **Robust Privacy**: Client-side encryption and authentication ensure that inactivity-triggered actions remain private, with no server-side visibility, aligning with UnoLock’s zero-knowledge model.

3.26.4 Use Cases

- **Personal Asset Protection**: Individuals can use LockoutGuard to recover access to cryptocurrency keys or documents if they lose access, and LegacyLink to prepare a trusted person for succession after prolonged inactivity.
- **Corporate Continuity**: Businesses can prepare a successor to recover access to critical records after executive inactivity.
- **High-Risk Scenarios**: Users in unstable regions can combine inactivity-based continuity planning with their normal access-key model rather than relying on a standing backup login.

3.26.5 Why It Matters

Inactivity can lead to permanent data loss or blocked inheritance. LockoutGuard and LegacyLink address those failure cases without weakening UnoLock into a standing alternative-login system. They preserve continuity while keeping WebAuthn access keys as the primary model.

3.26.6 FAQs

? How does LockoutGuard detect inactivity and initiate recovery?

LockoutGuard monitors login activity and triggers its recovery flow after a user-defined inactivity period. Once that recovery flow is used, the user must register again with WebAuthn and the temporary recovery method is removed.

? Can someone use LegacyLink immediately after it is created?

No. The LegacyLink credential is dormant and intended to become usable only when the configured conditions have been met.

? What happens after LockoutGuard or LegacyLink is used?

After either method is used, UnoLock requires WebAuthn registration again. The temporary recovery or inheritance path is then removed, making these effectively one-time alternative access methods.

? Does UnoLock have access to my recovery or succession keys?

No, recovery and succession material remain within UnoLock's zero-knowledge architecture rather than becoming a normal server-side login path.

3.26.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: LockoutGuard and LegacyLink support compliance with GDPR, HIPAA, and other regulations by ensuring that recovery and inheritance processes are secure, private, and do not expose sensitive data on servers.

3.26.8 Integration with Other Features

- **Robust Key Management with Multi-Key Registration and WebAuthn**: Enhances recovery and succession with secure, multi-key authentication, ensuring robust access control.
- **Client-Side Encryption Using AES-256 GCM**: Ensures that recovery and LegacyLink material remain protected within UnoLock's privacy model.

3.27 Serverless Infrastructure for Enhanced Security

3.27.1 Overview

The **Serverless Infrastructure for Enhanced Security** feature leverages a serverless architecture to bolster UnoLock CybVault’s security, scalability, and resilience. By utilizing serverless computing services, such as AWS Lambda and API Gateway, UnoLock minimizes the attack surface, eliminates traditional server management vulnerabilities, and ensures that sensitive operations, like data encryption and authentication, are performed in isolated, ephemeral environments. This approach enhances security by reducing persistent infrastructure risks and aligns with UnoLock’s **zero-knowledge** model, ensuring that no sensitive data is stored or processed on persistent servers, protecting user assets like cryptocurrency keys, confidential documents, or personal records.

3.27.2 How It Works

- **Serverless Computing**: UnoLock employs AWS Lambda to execute functions in stateless, short-lived environments, triggered only when needed, eliminating persistent server vulnerabilities.
- **API Management**: AWS API Gateway securely handles client requests, enforcing authentication and rate limiting, ensuring that only authorized operations reach the serverless backend.
- **Ephemeral Environments**: Each serverless function runs in an isolated container, destroyed after execution, preventing data persistence or unauthorized access to residual information.
- **Zero-Knowledge Integration**: Sensitive operations, like encryption and key management, are performed client-side, with serverless functions handling only non-sensitive tasks, maintaining UnoLock’s zero-knowledge architecture.

3.27.3 Security Implications

- **Reduced Attack Surface**: Serverless architecture eliminates traditional server management, reducing vulnerabilities like misconfigurations or unpatched software, enhancing overall security.
- **Isolated Execution**: Ephemeral, isolated function environments prevent lateral movement by attackers, ensuring that breaches in one function cannot affect others.
- **Enhanced Resilience**: Automatic scaling and fault tolerance in serverless services ensure high availability and protection against denial-of-service (DoS) attacks, safeguarding user access.

3.27.4 Use Cases

- **Secure Data Operations**: Individuals managing cryptocurrency keys or sensitive documents benefit from serverless functions that process requests securely without persistent server risks.
- **Enterprise Scalability**: Businesses can leverage UnoLock’s serverless backend to handle variable workloads securely, ensuring robust data protection during peak usage.
- **High-Security Environments**: Users in regulated industries, like finance or healthcare, can rely on serverless infrastructure to meet stringent security and compliance requirements without server management overhead.

3.27.5 Why It Matters

Traditional server-based architectures expose persistent vulnerabilities that attackers can exploit, such as outdated software or misconfigured systems. UnoLock’s serverless infrastructure, as part of its cloud integration strategy, eliminates these risks by using stateless, ephemeral functions that minimize the attack surface. This feature ensures robust security and scalability, aligning with UnoLock’s commitment to **zero-knowledge** privacy and providing users with confidence that their digital assets are protected in a modern, resilient environment.

3.27.6 FAQs

How does serverless infrastructure improve security over traditional servers?

Serverless architecture uses ephemeral, isolated functions that eliminate persistent server vulnerabilities, reducing the attack surface and preventing data leakage.

Can serverless functions access my sensitive data?

No, UnoLock’s zero-knowledge model ensures that sensitive operations occur client-side, with serverless functions handling only non-sensitive tasks, maintaining user privacy.

What happens if a serverless function is compromised?

Each function runs in an isolated, short-lived environment, limiting the impact of any compromise and preventing attackers from accessing other functions or persistent data.

3.27.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: The serverless infrastructure supports compliance with GDPR, HIPAA, and other regulations by minimizing data persistence and ensuring secure, audited operations, protecting sensitive user information.

3.27.8 Integration with Other Features

- **Advanced API Security with AES-256 GCM and ECDHE_ECDSA**: Serverless functions integrate with advanced API security to ensure secure, encrypted communication between clients and the backend.
- **Client-Side Encryption Using AES-256 GCM**: Ensures that sensitive data remains encrypted client-side, complementing the serverless architecture’s stateless processing.

3.28 Advanced AWS Account Management

3.28.1 Overview

TechSologic runs UnoLock across multiple isolated AWS accounts with centralized identity and strict separation of duties. Account access is controlled through AWS Organizations and AWS IAM Identity Center, with tightly scoped permissions for developers, approvers, and operations.

This model is designed to reduce blast radius, prevent unauthorized production changes, and keep security-critical access paths narrow and auditable.

UnoLock runs on a fully serverless architecture with no customer-managed servers or host OS instances, which materially reduces host and network administration attack surface.

3.28.2 Account and Identity Model

- **Parent account governance**: A parent AWS account managed through AWS Organizations controls identity and permission boundaries for child accounts.
- **IAM Identity Center control plane**: Workforce identities and role assignments are managed centrally through IAM Identity Center.
- **Strong MFA posture**: Access to AWS Access Portal requires physical YubiKeys.
- **Temporary credentials only**: CLI/API access uses short-lived credentials from AWS Access Portal. No long-term AWS credentials are used.
- **No root-account operations**: Day-to-day access is through users and roles only.
- **Root account lock-down**: Root access is locked down and reserved for emergency use only.

3.28.3 Multi-Account Segmentation

UnoLock operations are segmented across account types:

- **Developer accounts**: Each developer has their own AWS account and can deploy the full UnoLock app for end-to-end testing.
- **Build account**: Hosts CodeCommit repositories and build pipeline infrastructure. Developers do not have access to this account.
- **Test account**: Receives deployment from the approved pipeline and hosts the public test environment.
- **Production account**: Hosts production deployment and is isolated from developer and approver access.

3.28.4 Regional Architecture and Recovery Model

- **Multi-region runtime**: UnoLock production services are deployed across Canada and Ireland.
- **Multi-region public endpoints**: UnoLock public application endpoints and API endpoints are deployed in both regions.
- **API Gateway scope**: API Gateway is deployed multi-region for UnoLock API traffic.
- **Multi-region data layer**: DynamoDB is configured for multi-region operation.
- **Multi-region key management**: Root customer KMS keys used by the API server are configured for multi-region use.
- **PITR enabled**: Point-in-time recovery is configured for 7 days and is part of the multi-region recovery model.
- **Disaster scope**: Due to UnoLock's architecture, individual-account recovery is not the recovery target. Recovery procedures are designed for full multi-region disaster scenarios.

3.28.5 Access Boundaries and Separation of Duties

- **Branch-level write restrictions**: Developers can push only to their own branches.
- **Protected master branch**: Developers cannot write directly to master.

- **Pull request controls**: Deployment updates begin with pull requests.
- **Independent approvers**: Separate approvers in the build account control PR approvals.
- **Production isolation**: Neither developers/operations nor approvers have direct access to the production account.
- **Highly restricted parent control**: Access to the parent governance account is tightly restricted.

3.28.6 Logging and Retention Boundaries

- **Application operational logs (troubleshooting only)**: Retained for 3 days and limited to error/trouble-detection data used for production troubleshooting. These are not user activity logs.
- **AWS account audit logs (TechSologic access only)**: Organization-wide CloudTrail is configured in the parent account and delivered to Amazon S3, with a 365-day retention policy. This trail is used to audit TechSologic workforce access and AWS account activity, not customer application content.

3.28.7 Operational Benefits

- **Lower insider risk** through role separation and minimal privileged access.
- **Reduced blast radius** by account-level isolation.
- **Controlled change flow** through protected branches and approval gates.
- **Credential risk reduction** by eliminating long-lived credentials.
- **No direct infrastructure drift** by routing all changes through pipeline controls.
- **Continuous dependency visibility** through a separate nightly lockfile vulnerability scan with S3 reporting and SNS/SQS notifications.

3.28.8 FAQs

How is AWS access authenticated for TechSologic staff?

Access is authenticated through AWS Access Portal with physical YubiKeys, and sessions use temporary credentials.

Can developers modify production directly?

No. Developers are limited to their own branches and their own developer accounts. Production changes must pass through the approved pipeline and separate approval stages.

Where are identities and permissions managed?

Identities and permissions are centrally managed through IAM Identity Center in the AWS Organizations parent-account model.

Is the AWS root account used for normal operations?

No. Root is locked down and reserved for emergency access only. Routine operations are performed through role-based access with temporary credentials.

3.28.9 Integration with Other Features

- **Stateless Multi-Account Build System with AWS CodePipeline**: Account management enforces the boundaries used by the deployment pipeline.

- **Serverless Infrastructure**: Account controls complement UnoLock's serverless runtime model by limiting who can change infrastructure and deployment state.

3.29 Stateless Multi-Account Build System with AWS CodePipeline

3.29.1 Overview

TechSologic operates UnoLock with a stateless, multi-account CI/CD model built around AWS CodeCommit and AWS CodePipeline. The pipeline enforces branch protections, independent approvals, environment isolation, and staged promotion from development to test to production.

The goal is straightforward: deployment authority flows through controlled approvals, not direct account access.

UnoLock deployment targets are fully serverless, with no customer-managed servers or host OS instances, reducing host and network administration attack surface.

3.29.2 Pipeline Architecture

- **Source control in build account**: UnoLock repositories are hosted in CodeCommit in a dedicated build account.
- **Developer workflow**: Each developer works in a dedicated branch and can push only to that branch.
- **Protected master**: Developers do not have write access to master.
- **PR-gated promotion**: A pull request is required to promote changes toward deployment.

3.29.3 Deployment Flow

1. A developer pushes commits to their own branch.
2. The developer opens a pull request to master.
3. Separate approvers with PR approval rights review and approve.
4. Approval to master triggers a pipeline build and deploy to a separate AWS test account.
5. The test environment is public at `https://safe.test.1two.be` and is used as a feature playground and broad validation target.
6. A separate team has limited test-account access for troubleshooting.
7. The pipeline includes an additional approval stage before production.
8. A second approval is required for production promotion into a separate production account.

3.29.4 Security Controls in the Build System

- **No long-lived credentials**: Build and operator access rely on temporary credentials, not static keys.
- **Identity hardening**: Access to AWS Access Portal requires physical YubiKeys.
- **Centralized permissions**: Identity and authorization are managed through IAM Identity Center and AWS Organizations.
- **Environment isolation**: Build, test, and production run in separate AWS accounts.
- **Secrets handling**: Build parameters are sourced from AWS Systems Manager Parameter Store (SSM), not committed to source.
- **Dependency control**: Build dependencies are resolved through AWS CodeArtifact in the build account.
- **Default deny for new dependencies**: New dependencies fail by default until explicitly approved and added to CodeArtifact.
- **Production access isolation**: Developers, operations, and approvers do not have direct access to the production account.
- **Pipeline-only change path**: No code or infrastructure changes are applied directly in accounts.
- **100% Infrastructure as Code**: Infrastructure updates are defined as code and deployed through pipeline-managed CloudFormation changes.
- **Single controlled deployment plane**: Code deployment and CloudFormation deployment are both enforced through the same approval pipeline.
- **Multi-region deployment target**: Pipeline promotions deploy runtime components across Canada and Ireland.

- **Multi-region resiliency components**: UnoLock public endpoints, multi-region API Gateway (for API traffic), DynamoDB, and API-server root customer KMS keys are managed through the same controlled deployment process.
- **PITR policy**: DynamoDB point-in-time recovery is configured for 7 days as part of the multi-region disaster recovery model.
- **Nightly dependency monitoring**: A separate nightly security scan analyzes production npm lockfile dependencies (`--omit=dev`) for server, client, payments, serviceWorker, and EyesOnly.
- **Security reporting channels**: Nightly scan outputs are written to S3 and summarized through SNS (with optional SQS fan-out and email subscription).

3.29.5 Why This Matters

Traditional CI/CD pipelines often fail at separation of duties, secret handling, or account segmentation. UnoLock's pipeline model is designed to:

- keep deployment authority gated through independent approval,
- prevent direct production manipulation by day-to-day contributors,
- ensure consistent parameterized builds without embedding secrets in code,
- reduce supply-chain risk through controlled dependency intake,
- and enforce a single, auditable route for both application and infrastructure change.

3.29.6 FAQs

? **Can a developer deploy directly to production?**

No. Developers can only push to their own branch and deploy in their own development account. Production promotion requires pipeline approvals and account-level isolation.

? **Where do build-time parameters come from?**

Build parameters come from AWS SSM Parameter Store. Secrets and environment settings are not stored in source code.

? **How are dependencies controlled?**

Dependencies are sourced from CodeArtifact in the build account. New dependencies are blocked by default until approved.

? **Can infrastructure be changed outside the pipeline?**

No. Infrastructure and application changes are both controlled through the same CodePipeline approval flow and deployed as Infrastructure as Code.

? **How long are logs retained?**

Application operational logs are retained for 3 days and are limited to error/trouble-detection data used for production troubleshooting, not user activity logging. Organization-wide AWS CloudTrail audit logs are configured in the parent account, stored in Amazon S3, and retained for 365 days. CloudTrail in this context is for TechSologic workforce/account access auditing, not customer application content.

How are newly disclosed dependency vulnerabilities monitored?

TechSologic runs a separate nightly lockfile vulnerability scan focused on production dependencies (`npm audit --omit=dev --package-lock-only`) for server, client, payments, serviceWorker, and EyesOnly. Reports are stored in S3 and summary alerts are distributed through SNS (and optional SQS/email subscriptions).

What is the recovery model for data?

UnoLock uses a multi-region recovery design. Individual-account recovery is not the target model; recovery procedures are designed for full multi-region disaster scenarios.

3.29.7 Integration with Other Features

- **Advanced AWS Account Management**: Account-level identity and authorization boundaries enforce pipeline separation of duties.
- **Serverless Infrastructure**: The pipeline deploys into isolated serverless environments across test and production accounts.

3.30 Space Backup and Restore Technical White Paper

3.30.1 Abstract

UnoLock Space Backup is a client-side encrypted, stream-oriented export/import mechanism for moving Space data across Safes or restoring into an existing Space. The format is designed for:

- large-file streaming without full in-memory buffering,
- authenticated per-frame processing,
- archive-ID remapping on restore.

This document describes the protocol, cryptography, restore semantics, and security boundaries as implemented in the current client.

3.30.2 Scope

Included in backup:

- Space records and labels metadata,
- non-Records archives belonging to the Space (`Cloud`, `Msg`, `Local`),
- optional wallet secret material (when explicitly selected).

Not included:

- Safe-global policy/configuration not part of Space data model,
- keys/credentials of the source Safe,
- server-side operational metadata not required to reconstruct Space content.

Current UI access path:

- `Configuration -> Backup / Restore` (admin-only config action),
- available to free and paid tiers,
- restore destination behavior is tier-aware (detailed below).

3.30.3 Design Goals

- Maintain zero-knowledge handling (all backup payloads encrypted client-side).
- Preserve streaming behavior for large archives.
- Ensure record attachment references remain valid after restore in create-new and merge flows.
- Keep restore behavior compatible with tier capabilities (cloud-capable tiers vs non-cloud tiers).

3.30.4 Threat Model

Defended

- Passive storage adversary reading `.usbk` contents without password.
- In-transit tampering of backup bytes (detected by AES-GCM authentication).
- Frame reordering/substitution attacks (frame index and type bound into AAD).
- Malformed input classes that attempt oversize frame/KDF allocation denial of service (bounded in restore parser).

Not Defended

- Endpoint compromise on source or destination client.

- Offline brute-force against weak backup passwords.
- Operational leakage from insecure handling of exported backup files.

3.30.5 Backup File Format (v2)

Header

Header fields:

- Magic: `USBK2STR` (8 bytes)
- Format version: `2`
- KDF type: `Argon2id`
- Salt
- Nonce prefix (8 bytes)
- Serialized KDF params (JSON)

The header carries all required metadata for deterministic restore.

Frame Stream

Backup body is a sequence of encrypted frames:

- `MANIFEST`
- `ARCHIVE_START`
- `ARCHIVE_CHUNK`
- `ARCHIVE_END`
- `ARCHIVE_ABORT`
- `DONE`

Each frame has:

- frame type (1 byte),
- frame index (uint32 LE),
- ciphertext length (uint32 LE),
- ciphertext bytes.

Parser protections include:

- valid frame-type enforcement,
- minimum/maximum ciphertext bounds,
- strict monotonic index matching,
- single `DONE` marker and no trailing data after `DONE`.

3.30.6 Cryptography

KDF

Current default for v2 backups:

- Argon2id with explicit parameters in header.

Restore hardening validates KDF parameters against bounded ranges before derivation to reduce crafted-input DoS risk.

Encryption

Each frame payload is encrypted with AES-256-GCM.

- Nonce: 12 bytes = random 8-byte nonce prefix + 4-byte frame index.
- AAD: frame type + frame index.
- Authentication tag: GCM standard tag.

This binds ciphertext integrity to frame position and type, preventing silent frame permutation.

3.30.7 Streaming Architecture

Backup

- Manifest and control frames are emitted incrementally.
- Archive content is streamed chunk-by-chunk from archive URLs (and local-file path for `Local` archives).
- No full archive buffering is required.

Restore

- Frames are read and decrypted sequentially.
- For each archive stream, a destination archive is created and chunk data is piped into upload stream.
- Failures convert to explicit skipped/archive-abort semantics where possible.

3.30.8 Restore Destination and Tier Semantics

Restore supports two primary destination modes:

- `CREATE_NEW_SPACE` : creates a new destination Space named `<source> (Restored)` .
- `MERGE_CURRENT_SPACE` : merges restored content into the selected/current destination Space.

Config UI behavior:

- Sovereign and High Risk tiers: user is prompted to choose merge vs create-new.
- other tiers (including free tier): restore defaults to merge into the current Space.

Service default behavior (when caller does not pass an explicit mode):

- cloud-capable tiers (Sovereign/High Risk) default to `CREATE_NEW_SPACE` ,
- other tiers default to `MERGE_CURRENT_SPACE` .

3.30.9 Records and Attachment Remap Semantics

Restored archive objects are created in the destination Safe and receive new archive IDs.

The restore pipeline builds a source→destination archive ID map, then rewrites record attachment references before writing restored Records data. In merge mode, remapped records/labels are merged with existing destination records data; in create-new mode, restored records data is written as the new Space payload.

Supported reference forms:

- `record.archives[]` .

Unmapped references are dropped, and the record attachment field is normalized accordingly.

3.30.10 Local Archive Handling

`Local` archives are included when corresponding `.ulf` files are provided during backup.

Selection/matching behavior:

- local file header is used to match archive ID,
- strict mode can block backup if required local archives are missing,
- unresolved local files are reported as skipped.

On restore, destination archive storage type is tier-aware:

- tiers with cloud archive support restore to cloud-backed destination archives,
- tiers without cloud archive support restore archives as `Local` data.

3.30.11 Wallet Portability Path

When wallet inclusion is enabled:

- wallet protected secret parts are decrypted via WebAuthn-assisted flow,
- decryption is batched to reduce ceremonies,
- plaintext wallet material is included only inside encrypted backup payload,
- on restore, secrets are re-encrypted using destination Safe WebAuthn-protected encryption,
- plaintext wallet fields are removed from restored records.

Length consistency checks are enforced on decrypt/encrypt batch results to fail closed on partial responses.

3.30.12 Integrity and Failure Semantics

- Archive stream failures during backup can emit `ARCHIVE_ABORT`.
- Restore tracks skipped archives with reason codes.
- Terminal `DONE` frame required for successful restore completion.
- Password mismatch or authenticated decryption failure returns corruption/password error.

3.30.13 Format Validation

- Unknown KDF type or unsupported version is rejected.
- Frame order and frame type validity are enforced.

3.30.14 Operational Guidance

- Prefer normal Safe redundancy and key hygiene over routine exported backups.
- Use backups for controlled migration workflows.
- Use the config flow at `Configuration -> Backup / Restore` so destination mode prompts and tier defaults are applied correctly.
- Enforce high-entropy backup passphrases and secure storage handling.
- Audit skipped archive counts during restore verification.

3.30.15 Security Limitations and Future Work

- Password-derived backups are intrinsically susceptible to offline guessing if passphrase quality is weak.
- Local archive matching can be further strengthened with additional content integrity checks at selection time.
- Memory-hard KDF defaults should be periodically recalibrated to target hardware baselines and UX constraints.

3.30.16 Conclusion

The Space backup/restore design provides practical portability with strong client-side authenticated encryption and streaming for large archives. With strict parser/KDF bounds, explicit frame integrity, deterministic attachment remapping, and tier-aware restore destinations, it is suitable for controlled migration while preserving UnoLock’s zero-knowledge posture.

3.31 Digital Paper Wallet Security

3.31.1 Overview

Digital Paper Wallet Security is an unbreachable citadel for your Bitcoin and Ethereum keys, fortifying Sovereign and HighRisk tier users with zero-knowledge, offline-like key generation and BIP-39 mnemonic export via the coercion-resistant Key Extraction Protocol (KEX). By leveraging AES-256 GCM encryption and cold-like storage-like principles, DPW ensures Bitcoin and Ethereum keys remain inaccessible to third parties, including UnoLock, while integrating with DuressDecoy and LifeSafe for duress protection. Exclusively available in Sovereign and HighRisk tiers, this feature delivers ironclad self-sovereignty, safeguarding your digital wealth against all threats.

3.31.2 How It Works

- **Offline Key Generation**: Sovereign and HighRisk tier users generate private keys for Bitcoin and Ethereum offline-like in their browser, ensuring no third-party access, including UnoLock.
- **Client-Side Encryption**: Keys are encrypted on the user’s device with **AES-256 GCM**, stored securely in the vault, and backed up to AWS S3 with pre-signed URLs, remaining unreadable without the decryption key.
- **Coercion-Resistant KEX Export**: Keys are exported as BIP-39 mnemonic seed phrases via the **Key Extraction Protocol (KEX)**, splitting phrases across two offline devices with optional multi-device authentication and self-destructing sessions.
- **Cold-like Storage-Like Vault**: Encrypted keys are stored in a vault-like environment, mirroring cold-like storage security, designed for key management without transaction capabilities or key holding for transactions.

3.31.3 Security Implications

- **Zero-Knowledge Privacy**: UnoLock’s zero-knowledge model ensures no access to unencrypted keys, guaranteeing user-only control and eliminating custodial risks in Sovereign and HighRisk tiers.
- **Cold-like Storage Protection**: Offline-like key generation and encrypted storage shield keys from online threats like phishing, malware, or cloud breaches, providing cold-like storage-like resilience.
- **Coercion Defense**: KEX’s split-device retrieval, combined with DuressDecoy (Sovereign) and LifeSafe (HighRisk), protects keys against physical or legal coercion, ensuring deception or denial of access.

3.31.4 Use Cases

- **High-Stakes Crypto Security**: Sovereign tier users generate Ethereum keys offline-like, exporting mnemonics via KEX to MetaMask, protected by DuressDecoy against coercion in volatile regions.
- **Ultra-Secure Key Management**: HighRisk tier users store Bitcoin and Ethereum keys in DPW's vault, using KEX to export to hardware wallets, safeguarded by LifeSafe for maximum coercion resistance.
- **Corporate Crypto Protection**: HighRisk tier businesses generate and export Bitcoin keys to hardware wallets via KEX, ensuring corporate assets are secure from cyberattacks and insider threats.

3.31.5 Why It Matters

Digital Paper Wallet Security delivers an unyielding shield for Sovereign and HighRisk tier users, combining zero-knowledge encryption, offline-like key management, and coercion-resistant KEX export to ensure unparalleled Bitcoin and Ethereum security. In a world of relentless threats, DPW fortifies your digital wealth with absolute sovereignty and resilience.

3.31.6 FAQs

Can UnoLock access my DPW private keys?

No, DPW’s zero-knowledge model ensures keys are generated and encrypted client-side, inaccessible to UnoLock or any third party.

? How does KEX secure mnemonic export against coercion?

KEX splits BIP-39 mnemonics across two offline devices with optional multi-device authentication and self-destructing sessions, thwarting coercion, keyloggers, and malware.

? Does DPW support cryptocurrency transactions?

No, DPW is designed for secure key generation and storage in Sovereign and HighRisk tiers, exporting keys via KEX to transaction wallets for spending.

3.31.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: DPW supports GDPR and HIPAA by encrypting keys client-side, ensuring user privacy and control during storage and export in Sovereign and HighRisk tiers.

3.31.8 Integration with Other Features

- **Post-Quantum Encryption Security**: Enhances DPW with quantum-resistant AES-256 GCM encryption, safeguarding keys against future quantum threats.
- **DuressDecoy**: Complements DPW in the Sovereign tier by allowing users to hide sensitive Spaces under coercion.

Back to Security Overview

3.32 Spaces: Granular Data Access and Control

3.32.1 Overview

The **Spaces: Granular Data Access and Control** feature enables users to create isolated, segmented environments within their UnoLock vault, called "Spaces," where different data sets can be stored and managed separately. This feature allows for precise control over who has access to specific data, ensuring that sensitive information is shared only with authorized individuals or groups. With Spaces, users can assign varying levels of permissions, such as read-only or admin rights, and implement granular access policies, making it ideal for collaborative work environments or for organizing personal data across different security needs.

3.32.2 How It Works

- **Creating Spaces**: Users can create multiple Spaces within their vault, each designed to hold a separate set of files, documents, or data. These Spaces act as distinct compartments with their own access controls and permissions.
- **Granular Access Control**: For each Space, users can define who has access and what permissions they have (e.g., read-only, read-write, or admin). This allows for fine-tuned control over who can view or edit the content within that Space.
- **Permission Management**: Users can easily modify permissions for each Space, adding or removing collaborators as needed. Admins of each Space can invite others to collaborate while maintaining full control over the access level granted.
- **Role-Based Access**: Permissions within Spaces can be assigned based on roles, ensuring that only authorized individuals can modify sensitive data or perform administrative tasks.

3.32.3 Security Implications

- **Data Isolation**: Each Space is isolated from the others, ensuring that access to one Space does not grant access to another. This compartmentalization minimizes the risk of unauthorized access to unrelated data.
- **Controlled Collaboration**: Users can collaborate on specific projects or datasets within a Space without exposing other sensitive data. Only authorized individuals can access the Space they are assigned to, ensuring confidentiality and data integrity.
- **Granular Permissions**: The ability to assign different permissions (e.g., read-only, full access) provides additional security by limiting what users can do within each Space, reducing the risk of accidental modifications or data leaks.

3.32.4 Use Cases

- **Team Collaboration**: Organizations working on different projects or departments can create separate Spaces for each project. Team members can be assigned to individual Spaces with specific roles, ensuring that sensitive information is only accessible to the relevant people.
- **Personal Data Segmentation**: Users who manage different types of personal data, such as financial records, legal documents, or medical information, can organize these datasets into different Spaces, each with its own level of security and access control.
- **Shared Family or Business Vaults**: Families or businesses that share a vault can use Spaces to separate private data from shared information. Each family member or employee can have access to their designated Space while being restricted from others.

3.32.5 Why It Matters

In environments where sensitive data is being managed, fine-tuned control over access is essential for security. **Spaces** offer a powerful way to compartmentalize data and limit who can view or edit information, reducing the risk of unauthorized access or accidental sharing. This feature is particularly valuable for businesses, organizations, or individuals who need to collaborate on specific projects without exposing other unrelated data. By controlling access at a granular level, Spaces provide both flexibility and security, ensuring that data is only accessible to the right people.

3.32.6 FAQs

Can I assign different permissions to different users within the same Space?

Yes, you can assign different permission levels (read-only, read-write, or admin) to individual users within a Space, ensuring that each user has the appropriate level of access.

Can someone with access to one Space see other Spaces in my vault?

No, each Space is isolated. Users who are granted access to one Space cannot see or access other Spaces unless specifically authorized.

Can I change the access permissions for a Space after it’s created?

Yes, you can update permissions at any time, allowing you to add or remove collaborators or change their roles within the Space as needed.

3.32.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Spaces allow for strict control over who has access to personal or sensitive data, supporting compliance with data privacy regulations such as GDPR and HIPAA by ensuring that only authorized individuals can view or modify protected data.

3.32.8 Integration with Other Features

- **Advanced Key Management**: Spaces work alongside UnoLock’s **advanced key management**, ensuring that each Space is protected by its own encryption keys and that only authorized users can access the data.
- **Safeword-PIN Protection for Sensitive Spaces**: Spaces can be marked as sensitive so safeword-PIN features can hide or delete them, depending on the tier.

3.33 Quadruple Encryption & WebAuthn Digital Paper Wallet (DPW)

3.33.1 Overview

UnoLock introduces the most advanced security measures for safeguarding your cryptocurrency private keys. The **Quadruple Encryption & WebAuthn Digital Paper Wallet (DPW)** feature ensures unmatched security for your private keys, protecting them from even the most advanced threats through **quadruple encryption** and **WebAuthn-based authentication**. This feature enhances UnoLock's Digital Paper Wallet (DPW) by applying multiple layers of AES-256 encryption and FIDO2-compliant authentication, ensuring that private keys remain secure at rest, in transit, and during access, providing robust protection for cryptocurrency assets.

3.33.2 How It Works

1. **Private Key Generation and Initial Client-Side Encryption**
2. **Local Generation**: Private keys are generated locally within the UnoLock client, ensuring they never leave your device in plaintext.
3. **Client-Side Encryption**: Upon generation, the private key is encrypted using AES-256 GCM with your unique encryption keys, providing immediate protection.
4. **Server-Side Encryption of the Client-Encrypted Private Key**
5. **Secure Transmission**: The client-side encrypted private key is securely transmitted to UnoLock servers.
6. **Additional Encryption Layer**: On the server, the private key undergoes a second encryption layer using a client-specific AES-256 key managed by AWS KMS (Key Management Service).
7. **Client-Side Encryption of the Entire Wallet Document**
8. **Comprehensive Encryption**: The entire wallet document, including the doubly encrypted private key, is encrypted on your device with AES-256 GCM encryption.
9. **Data Integrity**: Ensures all wallet data remains confidential, tamper-proof, and protected against unauthorized access.
10. **AWS Storage with Server-Side Encryption (SSE)**
11. **Secure Storage**: The encrypted wallet document is stored in AWS S3 with AES-256 encryption and replicated across multiple data centers for redundancy, ensuring resilience against data loss.
12. **WebAuthn Authentication for Access**
13. **FIDO2-Compatible Devices**: Access requires a FIDO2-compatible device, such as YubiKeys, biometric scanners, or secure mobile devices.
14. **Public-Key-Based Authentication**: This ensures only you, with your registered device, can decrypt and access the private key.

Decryption Process:

1. **Authentication**
2. **WebAuthn Challenge**: Access begins with a secure WebAuthn challenge through your registered FIDO2 device.
3. **Verification**: Public-key cryptography securely verifies your identity without exposing sensitive information.
4. **Server-Side Decryption**
5. **Decrypting Server Layer**: The server decrypts the private key using the server-side AES-256 key managed by AWS KMS.
6. **Secure Transmission**: The encrypted private key is securely sent back to your device for final decryption.
7. **Local Decryption**
8. **Client-Side Final Decryption**: Your client decrypts the private key using your unique encryption keys, ensuring it remains accessible only within your secure environment.
9. **Operational Security**: The private key is stored only in memory and is never saved in plaintext.

3.33.3 Security Implications

- **Unparalleled Security Layers**: Four layers of AES-256 encryption protect private keys at rest and in transit, minimizing exposure to cyber threats.
- **End-to-End Protection**: Private keys are never exposed in plaintext, mitigating risks of unauthorized access or interception.
- **Controlled Access**: WebAuthn authentication ensures only the authorized user with a registered FIDO2 device can decrypt the private key, preventing access even in compromised systems.
- **Data Resilience**: Secure AWS S3 storage with multi-region redundancy protects against data loss, ensuring availability of encrypted wallet documents.
- **Tamper-Proof Integrity**: Multiple encryption layers and client-side processing ensure wallet data remains confidential and unaltered.

3.33.4 Use Cases

- **Cryptocurrency Security**: Individual investors can store private keys with maximum protection, using quadruple encryption and WebAuthn for secure access to digital assets.
- **Enterprise Asset Management**: Businesses managing cryptocurrency holdings can leverage this feature for cold-like-storage-like security with controlled access, ensuring compliance with high-security standards.
- **High-Risk Environments**: Users in sensitive roles, such as financial executives or crypto traders, can protect private keys against advanced threats, with robust authentication and encryption.

3.33.5 Why It Matters

UnoLock’s **Quadruple Encryption & WebAuthn** security feature represents a significant advancement in cryptocurrency key management. By combining client-side encryption, multi-layered security, and modern WebAuthn-based authentication, UnoLock ensures that private keys remain fully protected from generation to use. This comprehensive approach provides peace of mind for users managing sensitive digital assets, safeguarding them against evolving cyber threats while maintaining ease of access and usability.

3.33.6 FAQs

How does quadruple encryption enhance private key security?

Four layers of AES-256 encryption ensure that private keys are protected at every stage, generation, transmission, storage, and access, making unauthorized access nearly impossible.

What happens if I lose my FIDO2 device?

You can register multiple FIDO2 devices or use backup authentication methods configured in UnoLock, but without a registered device, access may be restricted to ensure security.

Can UnoLock access my private key?

No, UnoLock’s zero-knowledge architecture ensures that private keys are encrypted client-side and never accessible to UnoLock servers or staff.

3.33.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: The feature ensures that no personal data or sensitive information is exposed online or shared with third parties, supporting compliance with GDPR, HIPAA, and other data protection regulations by maintaining user control over encrypted keys.

3.33.8 Integration with Other Features

- **Digital Paper Wallet (DPW) for Cryptocurrency Management**: Enhances the standard DPW by adding quadruple encryption and WebAuthn, providing advanced security for offline-like key storage.
- **Client-Side Encryption Using AES-256 GCM**: Leverages UnoLock’s client-side encryption framework to ensure all key operations remain secure and private.

3.34 Post-Quantum Encryption Security

3.34.1 Overview

Post-Quantum Encryption Security is an indomitable fortress against the quantum future, embedding UnoLock with lattice-based cryptography to safeguard your data, communications, and identity from emerging quantum threats. Available across all tiers, Free, Inheritance, Sovereign, and HighRisk, this feature harnesses Kyber and Dilithium algorithms alongside AES-256 GCM to ensure your vault remains impervious to quantum decryption. UnoLock's visionary encryption delivers a shield of enduring privacy, securing your digital sovereignty for generations.

3.34.2 How It Works

- **Quantum-Resistant Key Exchange**: UnoLock employs Kyber's Key Encapsulation Mechanism (KEM) to negotiate secure session keys for API communication, replacing vulnerable elliptic curve methods with lattice-based cryptography.
- **Dilithium-Based Authentication**: API servers authenticate with Dilithium digital signatures, ensuring clients connect only to legitimate UnoLock backends, thwarting quantum-powered Man-in-the-Middle attacks.
- **Client-Side Key Security**: The Client Data Master Key (CDMK) is generated and wrapped using a FIDO2 WebAuthn authenticator, stored on-device with quantum-safe encryption and biometric verification.
- **Robust Data Encryption**: All user data, files, archives, and metadata, is encrypted client-side with AES-256 GCM, maintaining a 128-bit security margin against quantum attacks like Grover's algorithm.

3.34.3 Security Implications

- **Quantum-Proof Protection**: Kyber and Dilithium algorithms resist quantum attacks (e.g., Shor's algorithm), ensuring your data and communications remain secure in a quantum future.
- **Forward Secrecy Assurance**: Per-session key negotiation prevents retroactive decryption, protecting past data even if future keys are compromised.
- **Zero-Knowledge Privacy**: Client-side key management ensures UnoLock cannot access your data, preserving privacy against both classical and quantum threats.

3.34.4 Use Cases

- **Future-Proof Data Storage**: Individuals can secure sensitive files (e.g., Bitcoin and Ethereum keys, legal documents) with confidence that quantum computers won't decrypt them decades later.
- **Secure Corporate Operations**: Businesses can protect proprietary or client data, ensuring compliance and resilience against quantum-enabled breaches.
- **High-Stakes Asset Management**: Cryptocurrency investors can safeguard wallet seeds with quantum-hardened encryption, ensuring long-term asset security.

3.34.5 Why It Matters

Post-Quantum Encryption Security pioneers an unbreakable defense against quantum threats, ensuring your UnoLock vault remains a sanctuary of privacy and protection. This feature empowers users with the confidence that their digital assets are secure, no matter how technology evolves.

3.34.6 FAQs

? **How does Post-Quantum Encryption protect against quantum computers?**

It employs Kyber and Dilithium algorithms, which resist quantum attacks like Shor's algorithm, unlike traditional cryptography vulnerable to quantum decryption.

Does Post-Quantum Encryption slow down UnoLock’s performance?

No, the cryptography is optimized for seamless integration, delivering quantum-grade security without impacting user experience.

Can my vault data be compromised by future quantum attacks?

No, AES-256 GCM and lattice-based cryptography provide a robust security margin, ensuring your data remains protected against quantum threats.

3.34.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: Post-Quantum Encryption ensures secure data handling with zero-knowledge, client-side encryption, supporting compliance with GDPR and HIPAA privacy standards.

3.34.8 Integration with Other Features

- **Client-Side Encryption**: Works in tandem to encrypt all vault data with AES-256 GCM, reinforced by quantum-resistant key exchange and authentication.
- **FIDO2 Authentication with WebAuthn**: Enhances security by protecting the Client Data Master Key with quantum-safe WebAuthn, ensuring robust access control.

Back to Security Overview

3.35 Vault Messaging Security

3.35.1 Overview

Vault Messaging Security describes the protection model behind UnoLock's address-based messaging. It supports legacy Safe-to-Safe (EyesOnly) and Receive Address flows, with per-address keys, policy controls, and reply-only protections for Free and Inheritance tiers. The design goal is simple: minimize metadata, maximize compartmentalization, and keep trust boundaries tight.

In short, it is zero-knowledge by design, end-to-end encrypted for message payloads, and ruthless about limiting relationship graphs.

3.35.2 How It Works

- **Hashed Receive Addresses**: Receive Addresses are hashed client-side and sent as `vaultxAddressHash`, keeping raw addresses off the server.
- **End-to-end encrypted payloads**: Messages are encrypted locally before upload and decrypted only at the intended receiving endpoint.
- **Per-address keys**: Each Receive Address has its own keypair to limit blast radius.
- **Reply-only binding**: Reply addresses are bound to a specific sender to prevent reuse or abuse.
- **Anonymous intake**: External senders can use the VaultX Drop Client without creating a Safe.
- **Policy enforcement**: usage limits and throttles reduce abuse and flooding at the address level.

3.35.3 Security Implications

- **Metadata hardening**: Servers route encrypted payloads and see only hashed addresses for Receive Address flows.
- **Compartmentalization**: Compromising one address does not expose other conversations.
- **Tier separation**: Sovereign/HighRisk can create Receive Addresses; Free/Inheritance can receive and reply via bound addresses.
- **No plaintext message handling by design**: the service moves protected payloads rather than treating message bodies as ordinary server-readable application content.

3.35.4 Use Cases

- **Secure coordination**: Two-way messaging between trusted Safes with address-based compartmentalization.
- **Anonymous intake**: Receive tips or disclosures via a shareable Receive Address link.
- **Controlled exposure**: Use short-lived or rate-limited addresses for high-risk interactions.

3.35.5 FAQs

? Can UnoLock read Vault messages?

No. Vault Messaging payloads are end-to-end encrypted and decrypted only inside the recipient's Safe.

? How are Receive Addresses protected?

Receive Addresses are hashed on the client, and each address has its own keypair and policy controls.

❓ **Can Free tier users send new messages?**

Free and Inheritance tiers can receive and reply using bound reply-only addresses, but cannot create new Receive Addresses.

3.35.6 Compliance & Privacy Regulations

- **GDPR Alignment**: Vault Messaging avoids storing raw recipient addresses and keeps content client-side encrypted.

3.35.7 Integration with Other Features

- **Post-Quantum Encryption Security**: ML-KEM-1024 + AES-256-GCM protect message confidentiality.
- **Threat Detection**: Runtime monitoring helps detect tampering during sensitive messaging flows.

Back to Security Overview

3.36 UnoLock VaultX Security

3.36.1 Overview

VaultX Drop is the anonymous sender client for **Receive Addresses**. Recipients create a Receive Address inside their Safe, then share the address (or a shareable link). Senders use the VaultX Drop Client with no account to deliver encrypted payloads. The result is anonymous intake without account creation or identity linkage, designed for high-risk environments and first-contact safety.

3.36.2 How It Works

- **Hashed addressing**: Receive Addresses are hashed client-side and sent as `vaultxAddressHash`, so raw addresses are never transmitted.
- **Client-side encryption**: The Drop Client encrypts payloads locally with ML-KEM-1024 + AES-256-GCM before upload.
- **Per-address keys**: Each Receive Address has its own keypair, limiting blast radius between conversations.
- **Policy enforcement**: Usage limits, throttling, and attachment permissions are enforced per address.
- **Sender-facing context**: A public sender message can be displayed in the Drop Client before submission.
- **Client-side decryption**: Only the recipient's Safe can decrypt the payload.
- **Sender-only**: VaultX Drop has no inbox and cannot receive replies.
- **Local address book**: The Drop Client can store addresses locally in a password-encrypted address book.

3.36.3 Security Implications

- **Sender anonymity**: No account or login is required for senders. For additional network privacy, access the Drop Client via Tor.
- **Metadata hardening**: Servers only see hashed addresses and encrypted payloads, not raw Receive Addresses.
- **Compartmentalization**: Per-address keys prevent one compromised address from exposing other conversations.

3.36.4 Use Cases

- **Whistleblower communications**: Anonymous intake without creating accounts or linking identities.
- **Legal and journalism workflows**: Share a rate-limited Receive Address for sensitive sources.
- **High-risk one-off drops**: Rotate addresses after use to reduce exposure.

3.36.5 FAQs

Can UnoLock see message contents or raw addresses?

No. Payloads are encrypted client-side, and Receive Addresses are hashed before they are sent to the server.

Can anyone decrypt a VaultX Drop payload?

Only the recipient's Safe with the matching private key can decrypt the payload.

How does VaultX Drop protect against quantum attacks?

VaultX Drop uses ML-KEM-1024 for key encapsulation and AES-256-GCM for payload encryption.

3.36.6 Compliance & Privacy Regulations

- **GDPR Alignment**: VaultX Drop avoids storing raw addresses and keeps message content encrypted client-side.

3.36.7 Integration with Other Features

- **Post-Quantum Encryption**: ML-KEM-1024 + AES-256-GCM protect VaultX Drop payloads against future cryptographic threats.
- **Threat Detection**: Runtime monitoring helps detect tampering in sensitive messaging flows.

Back to Security Overview

3.37 UnoLock Security Monitoring Service

3.37.1 Overview

UnoLock's **Security Monitoring Service** is a proactive, client-side background service that runs automatically in all UnoLock vaults, continuously auditing the browser runtime to detect and block malicious behavior before it can compromise your data. By combining API-blocking, event-listener auditing, DOM mutation inspection, overlay detection, and extension probing, it helps ensure that any injected code, unauthorized extensions, or clickjacking attempts are caught and neutralized in real time. This feature enforces strict controls on every aspect of the browser API, maintaining a hardened, trust-no-one runtime posture across all tiers.

3.37.2 How It Works

- **Automated Malicious-Extension Detection**: On every app launch, UnoLock attempts to fetch each known "bad" extension's manifest.json URL across Chrome, Firefox, and Safari schemes.
- **API-Tampering & Storage-Access Alerts**: UnoLock snapshots native browser APIs (fetch, WebSocket, localStorage, IndexedDB) at startup and continually verifies they haven't been overridden or wrapped by an external script. It overrides localStorage/sessionStorage methods and indexedDB.open to throw on any attempt to read or write, logging and flagging each call immediately.
- **DOM-Injection & Clickjacking Guardrails**: A mutation observer flags any unexpected `<script>` or `<iframe>` insertions that aren't explicitly whitelisted, using a debounced MutationObserver to watch for newly added nodes and stripping unauthorized elements. A periodic overlay scan finds full-screen, transparent elements that could intercept clicks, flagging or removing elements that could hijack clicks. It also scans for UI overlays and clickjacking checks every few seconds (outside Angular's zone).
- **Event-Listener Auditing**: UnoLock wraps addEventListener to log when any code (including extensions) registers handlers on sensitive events (click, input, copy/paste). After Angular stabilizes, it intercepts addEventListener to count sensitive handlers (click, input, keydown, etc.) and detect listeners injected by browser extensions via stack-trace analysis. Exceeding configurable thresholds triggers an alert.
- **Configurable Whitelisting & Minimal Overhead**: UnoLock only probes once per known extension ID, minimizing network overhead. Continuous monitoring runs outside Angular's change-detection zone and debounces mutations to avoid performance impact. Developers can mark legitimate, app-generated scripts/iframes (data-unolock-*), so it never blocks its own functionality. Extension presence probing loads hidden manifests for known banned extensions (from BANNED_EXTENSIONS) and alerts immediately if any are present.

3.37.3 Security Implications

- **Proactive Tamper Detection**: Identifies and blocks meddling scripts and API overrides before they execute.
- **Clickjacking Protection**: Stops hidden overlays and rogue iframes that could hijack user interactions.
- **Extension Threat Awareness**: Detects malicious or unapproved extensions at runtime, warning the user to remove them.
- **Real-Time Client-Side Alerts**: Escalating alerts inform users of repeated or severe anomalies, guiding them to switch to a clean profile or incognito mode.
- **Zero-Trust Browser Environment**: By enforcing strict controls on every aspect of the browser API, UnoLock maintains a hardened, trust-no-one runtime posture.

3.37.4 Use Cases

- **Cryptocurrency Security**: Protects crypto users from extension-based theft by detecting and blocking keyloggers or API hijacks in real time.
- **High-Risk Environments**: Journalists or activists can operate safely, with alerts for tampering that could expose sensitive communications.

- **Everyday Privacy**: Privacy-conscious individuals benefit from automatic detection of unwanted extensions, ensuring their vault remains secure.
- **Enterprise Data Protection**: Businesses managing sensitive assets receive warnings about runtime threats, preventing data leaks.

3.37.5 Why It Matters

UnoLock's Security Monitoring Service provides a best-effort, client-side defense layer that enforces strict API controls, audits runtime behavior, and detects and neutralizes unauthorized code or extensions, all in real time. While this zero-trust approach significantly raises the bar against browser-based threats, no client-side guard can guarantee 100% protection. Users must also exercise caution by avoiding untrusted or unsafe browser extensions and keeping their environment secure. Together, UnoLock's monitoring features and responsible user practices maintain the integrity of your data against evolving risks.

3.37.6 FAQs

? **What happens if a malicious extension is detected?**

The service alerts you immediately and prompts removal, preventing potential data compromise.

? **How does the service impact performance?**

It runs efficiently with debounced checks and minimal overhead, ensuring smooth operation without noticeable slowdowns.

? **Can I customize the monitoring thresholds?**

Yes, configurable whitelisting and thresholds allow adjustments for specific needs, such as marking trusted app elements.

? **What if I ignore an alert?**

Ignoring alerts increases risk; the service continues monitoring but recommends action to maintain security.

3.37.7 Compliance & Privacy Regulations

- **GDPR & HIPAA Compliance**: The service collects no personal data or metadata, focusing solely on runtime threats within the browser. It supports compliance by preventing unauthorized access or tampering, aligning with stringent privacy and security standards like GDPR and HIPAA.

3.37.8 Integration with Other Features

- **Post-Quantum Encryption**: Complements the service by ensuring encrypted data remains secure even if tampering is attempted, as runtime monitoring blocks threats before they reach sensitive operations.
- **Client-Side Encryption Using AES-256 GCM**: Enhances protection by auditing APIs and DOM elements that could interfere with encryption processes, maintaining a tamper-proof environment.
- **Vault Messaging Security**: Works alongside messaging by detecting injections or overlays that could intercept communications, ensuring secure, untraceable exchanges.

3.38 SeedSafe Security

3.38.1 Overview

SeedSafe Security represents an impenetrable vault architecture for BIP-39 mnemonic seed phrase protection, implementing military-grade split-storage cryptography and zero-knowledge protocols to safeguard existing wallet recovery keys. Through independent encryption of mnemonic halves, distributed trust models, and authenticated split-retrieval mechanisms, SeedSafe ensures that seed phrases remain cryptographically inaccessible to all parties—including UnoLock servers—while maintaining resilient cloud backup capabilities. Available in Sovereign and HighRisk tiers, this security framework transforms vulnerable seed phrase storage into an unassailable digital fortress.

3.38.2 How It Works

- **Split-Entry Security Protocol**: Enforces mnemonic entry in two independent halves, preventing single-device compromise vectors while validating against canonical BIP-39 wordlists with real-time checksum verification.
- **Independent Cryptographic Isolation**: Each mnemonic half undergoes separate AES-256-GCM encryption with unique initialization vectors, creating mathematically unrelated ciphertexts that cannot be correlated even if intercepted.
- **Zero-Knowledge Server Architecture**: Encrypted halves stored as opaque binary objects within isolated Spaces, with servers maintaining zero metadata about content type, relationships, or cryptographic purpose.
- **Authenticated Multi-Factor Retrieval**: Recovery requires cascading authentication ceremonies—FIDO2/WebAuthn verification, PIN entry, and explicit consent—with optional split-device reconstruction preventing full mnemonic assembly on any single endpoint.

3.38.3 Security Implications

- **Distributed Trust Enforcement**: Split-storage architecture ensures mathematical impossibility of seed phrase reconstruction without authenticated access to both encrypted halves, eliminating single points of failure.
- **Server-Blind Cryptography**: Zero-knowledge design prevents server-side correlation attacks, with encrypted payloads indistinguishable from random noise without client-side decryption keys.
- **Memory Sanitization**: Client-side implementation enforces immediate cryptographic erasure of plaintext mnemonics from memory after viewing, preventing residual data extraction.

3.38.4 Use Cases

- **Hardware Wallet Recovery Protection**: Sovereign tier users secure Ledger and Trezor recovery phrases with split-encryption, maintaining cloud resilience while preventing physical theft vulnerabilities.
- **Multi-Wallet Security Management**: HighRisk tier cryptocurrency traders isolate multiple seed phrases across segregated Spaces with distinct access controls and authentication requirements.
- **Estate Planning Integration**: Combined with LegacyLink, enables secure seed phrase inheritance without exposing keys during the owner's lifetime or requiring technical expertise from beneficiaries.

3.38.5 Why It Matters

SeedSafe Security revolutionizes cryptocurrency recovery key protection by eliminating the traditional vulnerability trade-off between accessibility and security. Through cryptographic splitting, zero-knowledge storage, and authenticated retrieval, it provides bank-vault protection for seed phrases while maintaining the convenience of cloud access—ensuring your recovery keys remain both utterly inaccessible to attackers and reliably available when legitimately needed.

3.38.6 FAQs

Can quantum computers break SeedSafe encryption?

SeedSafe employs AES-256-GCM encryption which remains quantum-resistant for symmetric cryptography. The split-storage architecture adds an additional layer of quantum resilience by requiring multiple independent breaches.

What happens if one device is compromised during split-entry?

Even with one device fully compromised, attackers cannot reconstruct the complete mnemonic without authenticated access to the second half, maintaining security through distributed trust.

How does SeedSafe prevent insider threats at UnoLock?

Zero-knowledge architecture ensures UnoLock employees cannot access, decrypt, or correlate stored mnemonics, as all encryption occurs client-side with keys never transmitted to servers.

3.38.7 Compliance & Privacy Regulations

- **Cryptographic Sovereignty**: Client-side encryption ensures complete user control over seed phrases, exceeding GDPR Article 25 requirements for data protection by design and default.
- **Regulatory Audit Trail**: Maintains encrypted access logs without exposing seed phrase content, supporting compliance requirements while preserving zero-knowledge guarantees.

3.38.8 Integration with Other Features

- **Post-Quantum Encryption Security**: Leverages quantum-resistant symmetric encryption to future-proof seed phrase protection against emerging cryptographic threats.
- **Threat Detection**: Runtime monitoring ensures malicious extensions or injected scripts cannot intercept seed phrases during entry or viewing.
- **Spaces**: Enables isolated storage environments with granular permission models for organizing multiple seed phrases with role-based access.

Back to Security Overview

3.39 DPW VaultSign Security

3.39.1 Overview

DPW VaultSign Security implements an unbreachable transaction signing architecture that enforces absolute key isolation through four-layer encryption, browser sandbox containment, and air-gapped broadcasting protocols. By ensuring private keys exist only in volatile memory during millisecond signing windows—protected by cascading authentication ceremonies and Content Security Policy enforcement—VaultSign delivers unprecedented transaction security for Sovereign and HighRisk tier users. This zero-trust signing framework guarantees that cryptocurrency assets remain immutable even under scenarios of complete infrastructure compromise, establishing a new paradigm for digital asset control.

3.39.2 How It Works

- **Four-Layer Decryption Cascade**: Transaction signing requires sequential reversal of wallet document encryption (Layer 3), server envelope removal (Layer 2), WebAuthn-bound decryption (Layer 1), and in-memory reconstruction—each gated by explicit user authentication.
- **Browser Sandbox Containment**: All cryptographic operations execute within hardened browser environment protected by strict Content Security Policy headers, preventing key exfiltration through XSS, code injection, or malicious extensions.
- **Millisecond Key Exposure Window**: Private keys materialize in volatile memory exclusively during transaction signing, with immediate cryptographic erasure ensuring zero persistent exposure across browser sessions.
- **Air-Gap Broadcasting Architecture**: Signed transactions intentionally lack network transmission capability within UnoLock, requiring manual export and broadcast through independent third-party services, creating physical separation between signing and transmission.

3.39.3 Security Implications

- **Compromise-Resistant Design**: Even with complete server and application compromise, attackers cannot initiate unauthorized transactions due to air-gap isolation and lack of automated broadcasting mechanisms.
- **Memory Forensics Protection**: Cryptographic key erasure employs secure memory wiping patterns that prevent recovery through memory dumps, cold boot attacks, or browser debugging interfaces.
- **Authentication Chain Integrity**: Multi-ceremony authentication requirements create temporal separation between access attempts, enabling detection and prevention of automated attack sequences.

3.39.4 Use Cases

- **High-Value Transaction Execution**: Sovereign tier users sign million-dollar cryptocurrency transfers with bank-grade security, ensuring keys remain protected throughout the entire signing lifecycle.
- **Multi-Signature Orchestration**: HighRisk tier organizations coordinate complex multi-sig transactions with each participant's keys isolated in separate VaultSign instances, preventing collusion attacks.
- **Regulatory Compliance Signing**: Enterprises leverage VaultSign's audit trail capabilities for regulatory reporting while maintaining zero-knowledge privacy for actual key material.

3.39.5 Why It Matters

DPW VaultSign Security represents the apex of transaction signing protection, surpassing hardware wallet security through its unique combination of multi-layer encryption, air-gap isolation, and zero-persistence architecture. By enforcing strict separation between key access, transaction creation, and broadcast mechanisms, VaultSign ensures that your cryptocurrency assets remain under absolute control even when facing nation-state level adversaries or insider threats.

3.39.6 FAQs

Why is air-gap broadcasting more secure than integrated transmission?

Air-gap design ensures that even with complete UnoLock compromise, attackers cannot programmatically broadcast transactions. This physical separation requires explicit human action, preventing automated theft.

Can browser exploits compromise VaultSign signing?

VaultSign's CSP enforcement, sandbox isolation, and millisecond key exposure window create multiple defensive layers. Even sophisticated browser exploits cannot persist keys or automate transaction broadcasts.

How does VaultSign compare to hardware wallet security?

VaultSign exceeds hardware wallet security by combining their offline signing benefits with cloud resilience, multi-layer encryption, and air-gap broadcasting—eliminating single device failure risks.

3.39.7 Compliance & Privacy Regulations

- **Transaction Privacy**: Raw transaction generation ensures complete control over blockchain privacy, with no metadata leakage through UnoLock's infrastructure.
- **Regulatory Auditability**: Cryptographically signed transaction logs provide immutable audit trails without exposing private keys, satisfying financial compliance requirements.

3.39.8 Integration with Other Features

- **Digital Paper Wallet**: VaultSign operates exclusively on DPW-generated keys, inheriting the full security architecture including quadruple encryption and zero-knowledge storage.
- **Threat Detection**: Runtime monitoring ensures transaction signing occurs in clean browser environments, detecting and blocking malicious extensions attempting to intercept signing operations.
- **Spaces**: Transaction permissions segregated across Spaces enable role-based signing controls, preventing unauthorized access even with partial vault compromise.

Back to Security Overview

3.40 DPW Portability Security

3.40.1 Overview

DPW Portability Security establishes an unbreachable migration framework for Digital Paper Wallet mnemonics, enabling cross-vault and cross-Space transfers while maintaining absolute zero-knowledge guarantees throughout the entire portability lifecycle. Through authentication-bound encryption, opaque ciphertext migration, and distributed trust architectures, this security model ensures that mnemonics remain cryptographically protected during transit, storage, and reconstruction—even when crossing organizational boundaries. Available in Sovereign and HighRisk tiers, DPW Portability delivers unprecedented flexibility without compromising the fundamental sovereignty principles that define UnoLock's security architecture.

3.40.2 How It Works

- **Transit Encryption Envelope**: Mnemonics wrapped in multiple encryption layers during migration—base AES-256-GCM encryption, authentication-bound WebAuthn layer, and ephemeral transit keys—ensuring zero plaintext exposure across vault boundaries.
- **Opaque Ciphertext Migration**: Encrypted halves transfer as indistinguishable binary blobs with no metadata revealing content type, source vault, or destination purpose—servers process only encrypted payloads without correlation capability.
- **Atomic Transfer Protocol**: Migration operations execute as atomic transactions with automatic rollback on failure, preventing partial transfers that could compromise security or create orphaned key fragments.
- **Multi-Vault Isolation**: Each vault maintains independent encryption contexts with unique key derivation paths, ensuring compromise of one vault cannot decrypt mnemonics migrated to another vault.

3.40.3 Security Implications

- **Cross-Boundary Protection**: Mnemonics remain encrypted throughout inter-vault transfers, with re-encryption at destination using new vault-specific keys, preventing transit interception or replay attacks.
- **Consent-Enforced Migration**: Every portability operation requires explicit FIDO2/WebAuthn ceremonies at both source and destination, preventing silent or automated key transfers even with compromised sessions.
- **Distributed Custody Security**: Split-storage across multiple vaults enables trustless multi-party arrangements where no single entity can reconstruct complete mnemonics without coordinated authentication.

3.40.4 Use Cases

- **Organizational Key Distribution**: Sovereign tier enterprises distribute corporate wallet mnemonics across department vaults with role-based permissions, ensuring business continuity without centralized key exposure.
- **Inheritance Planning Architecture**: HighRisk tier users replicate DPWs into LegacyLink vaults for estate planning, maintaining encryption throughout the inheritance chain without requiring technical expertise from beneficiaries.
- **Multi-Jurisdiction Redundancy**: International organizations maintain DPW copies across geographically distributed vaults, ensuring regulatory compliance while preventing single-jurisdiction seizure risks.

3.40.5 Why It Matters

DPW Portability Security solves the critical challenge of key management flexibility in adversarial environments, enabling secure mnemonic distribution across trust boundaries without violating zero-knowledge principles. By maintaining encryption throughout migration, enforcing authentication at every step, and supporting distributed custody models, it provides the operational flexibility required for real-world asset management while preserving the uncompromising security standards demanded by high-value cryptocurrency holdings.

3.40.6 FAQs

Can UnoLock track mnemonics across different vaults?

No, each vault operates with independent encryption contexts and zero correlation capability. Servers cannot determine that identical mnemonics exist in multiple locations or track migration patterns.

What prevents unauthorized vault-to-vault transfers?

Multi-factor authentication requirements at both endpoints, combined with cryptographic proof of vault ownership, ensure only authorized parties can initiate or receive mnemonic transfers.

How does portability maintain security during network transmission?

Triple-layer encryption (base encryption, authentication binding, transit envelope) ensures that even complete network compromise cannot expose mnemonic content during migration.

3.40.7 Compliance & Privacy Regulations

- **Data Portability Compliance**: Satisfies GDPR Article 20 requirements while maintaining encryption, enabling compliant data transfers without exposing sensitive cryptographic material.
- **Cross-Border Privacy**: Encrypted migration ensures compliance with data localization requirements while preventing governmental access to plaintext mnemonics during international transfers.

3.40.8 Integration with Other Features

- **SeedSafe Architecture**: Inherits split-entry and authenticated retrieval mechanisms, ensuring consistent security model across all mnemonic operations regardless of vault location.
- **LegacyLink**: Seamless integration enables secure inheritance planning with mnemonics pre-positioned in successor vaults without premature key exposure.
- **Threat Detection**: Runtime monitoring validates migration endpoints, detecting and blocking attempts to transfer mnemonics to compromised or suspicious destinations.

Back to Security Overview

3.41 Threat Detection Security

3.41.1 Overview

Threat Detection Security (Runtime Security Monitoring and Tamper Detection) represents an impenetrable defensive perimeter that transforms the browser into a hardened, zero-trust execution environment through continuous runtime auditing, API hijacking prevention, and malicious code neutralization. By implementing comprehensive monitoring across seven attack vectors—API tampering, event injection, DOM manipulation, overlay attacks, socket exfiltration, extension infiltration, and storage breaches—this client-side security framework creates an active defense system that identifies and eliminates threats before they can compromise cryptographic operations. Available across all tiers, Threat Detection ensures that UnoLock's zero-knowledge architecture remains inviolate even in hostile browser environments.

3.41.2 How It Works

- **API Surface Lockdown**: Overwrites critical browser APIs (localStorage, sessionStorage, indexedDB, WebSocket) with security-enforced proxies that throw exceptions on access attempts, creating an impenetrable barrier against data exfiltration.
- **Event Stream Analysis**: Intercepts addEventListener calls post-Angular stabilization, analyzing stack traces to identify extension-injected listeners and enforcing configurable thresholds for sensitive event types (click, keydown, input).
- **DOM Mutation Sentinel**: Deploys debounced MutationObserver outside Angular's zone to detect unauthorized script/iframe injection, automatically purging elements lacking data-unolock attributes or originating from external domains.
- **Overlay Attack Prevention**: Executes periodic scans for transparent, high z-index overlays that could facilitate clickjacking, automatically removing suspicious elements before user interaction occurs.
- **Extension Fingerprinting**: Probes for banned extension manifests through resource loading patterns, immediately alerting users to remove detected threats while maintaining operational security.
- **API Integrity Verification**: Captures cryptographic snapshots of native APIs at initialization, continuously comparing against runtime state to detect third-party overrides or monkey-patching attempts.
- **Escalating Alert System**: Implements tiered response protocols—silent blocking for minor threats, user warnings for moderate risks, and session termination recommendations for critical compromises.

3.41.3 Security Implications

- **Zero-Day Exploit Mitigation**: Behavioral detection identifies novel attack patterns without requiring signature updates, providing protection against previously unknown browser exploits.
- **Supply Chain Attack Defense**: Detects compromised dependencies or malicious code injection through continuous API integrity monitoring and unauthorized script detection.
- **Credential Harvesting Prevention**: Blocks keyloggers, form grabbers, and clipboard monitors through event stream analysis and input handler restrictions.

3.41.4 Use Cases

- **Financial Transaction Protection**: Sovereign tier users executing high-value cryptocurrency transfers receive real-time protection against transaction manipulation and private key theft attempts.
- **Corporate Espionage Defense**: HighRisk tier enterprises gain protection against targeted attacks using sophisticated browser exploits designed to exfiltrate sensitive corporate data.
- **Journalist Security Operations**: Activists and journalists in hostile environments receive alerts about surveillance extensions and state-sponsored malware attempting to compromise their communications.
- **Healthcare Data Protection**: Medical professionals handling patient data benefit from comprehensive protection against HIPAA-violating data breaches through browser vulnerabilities.

3.41.5 Why It Matters

Threat Detection Security acknowledges a fundamental truth: the browser is both UnoLock's execution environment and its primary attack surface. By implementing comprehensive runtime monitoring that spans from low-level API hooks to high-level behavioral analysis, this security framework transforms the browser from a potential vulnerability into a fortified stronghold. While no client-side solution can guarantee absolute protection, Threat Detection's multi-layered approach significantly elevates the effort required for successful attacks, making UnoLock users unprofitable targets for all but the most determined adversaries.

3.41.6 FAQs

? Can Threat Detection prevent zero-day browser exploits?

While not infallible, Threat Detection's behavioral monitoring often identifies zero-day exploits through anomalous API usage patterns, providing defense against unknown vulnerabilities without requiring updates.

? Does continuous monitoring impact browser performance?

Monitoring operations execute outside Angular's change detection cycle using efficient observers and debounced checks, maintaining sub-millisecond overhead for typical operations.

? What happens if Threat Detection itself is compromised?

Multiple redundant detection mechanisms ensure that compromising one monitoring component triggers alerts from others, creating defense-in-depth against targeted bypass attempts.

3.41.7 Compliance & Privacy Regulations

- **Client-Only Operations**: All threat detection occurs within the browser sandbox with no external reporting, ensuring complete privacy compliance and preventing surveillance concerns.
- **GDPR Article 32 Compliance**: Continuous security monitoring satisfies requirements for appropriate technical measures to ensure ongoing confidentiality, integrity, and resilience.

3.41.8 Integration with Other Features

- **Post-Quantum Encryption**: Threat Detection ensures the browser environment remains secure for cryptographic operations, preventing key material extraction before quantum-resistant encryption is applied.
- **DPW VaultSign**: Validates signing environment integrity before private key operations, ensuring transaction signing occurs only in verified clean browser contexts.
- **SeedSafe**: Monitors for clipboard hijacking and screen recording attempts during seed phrase entry, preventing mnemonic theft through browser-based attacks.

Back to Security Overview

4. Data Self-Governance (DSG)

4.1 DSG Overview

4.1.1 Overview

Data Self-Governance (DSG) is a foundational concept in UnoLock, a platform designed to give individuals and organizations full control over their digital assets and personal data. Unlike traditional data systems that rely on third-party management, UnoLock’s DSG model ensures that only the user has authority over their information, deciding who can access, share, or modify it. At the heart of UnoLock's DSG approach is user autonomy, where every aspect of data management is controlled by the individual, with no interference from external entities. UnoLock incorporates end-to-end encryption, ensuring that all data remains private and secure at all times, with even the platform itself having no access to user data. Key features include granular access control, where users manage permissions on a highly detailed level, and legacy planning, allowing users to plan for the transfer or deletion of data in the event of incapacity or death. UnoLock also enables users to opt out of data sharing agreements or delete their data entirely when desired. In an age of increasing data breaches and privacy concerns, UnoLock’s DSG platform offers a secure and autonomous solution, empowering users with full ownership and control over their digital footprint.

4.1.2 Why It Matters

In an era where data breaches and privacy violations are increasingly common, DSG provides a transformative approach to data management by prioritizing user autonomy and security. By empowering users to control every aspect of their digital assets, UnoLock’s DSG model ensures privacy, compliance with global regulations like GDPR and HIPAA, and protection against unauthorized access. This aligns with the growing demand for digital sovereignty, where individuals and organizations retain full ownership of their data, as emphasized in discussions about UnoLock’s privacy-focused approach.

4.1.3 Integration with Other Features

- **End-to-End Encryption (E2EE)**: DSG leverages UnoLock’s E2EE to ensure that all data remains encrypted and inaccessible to third parties, including UnoLock, throughout its lifecycle.
- **Granular Access Control**: DSG’s user-centric model integrates with UnoLock’s access control features, allowing users to set precise permissions for data access and sharing.
- **Legacy Planning**: DSG supports UnoLock’s LegacyLink feature, enabling users to plan for the secure transfer or deletion of their data after incapacity or death.

4.2 What is DSG?

4.2.1 Overview

Data Self-Governance (DSG) is a framework that empowers users with full ownership and control over their personal data and digital assets. DSG shifts the control of data away from third-party entities and places it entirely in the hands of the individual or organization. Unlike traditional models, DSG eliminates reliance on external parties for data management, ensuring that users decide how their data is accessed, shared, and maintained, while remaining fully compliant with global data privacy standards such as GDPR and HIPAA. DSG aims to provide **autonomy, transparency**, and **security** in managing data, making it ideal for those who prioritize privacy and control over their digital identity.

4.2.2 Key Features

- **User-Centric Control**: Users are given the tools to directly manage all aspects of their data, including access permissions, data sharing, and modification rights.
- **End-to-End Encryption**: DSG ensures that data is encrypted from the moment it is created to the moment it is shared or deleted, preventing unauthorized access at all times.
- **Opt-Out and Deletion**: Users can opt out of data-sharing agreements and permanently delete data at any time, ensuring that their digital footprint remains under their control.
- **Legacy Management**: DSG provides mechanisms for legacy planning, allowing users to determine what happens to their data after death or incapacity.

4.2.3 Why It Matters

- **Data Ownership**: DSG fundamentally shifts the power dynamic in data management by ensuring that users maintain complete control of their digital assets, protecting against unauthorized access and misuse.
- **Data Privacy and Security**: With rising concerns over data breaches and surveillance, DSG guarantees that sensitive information remains protected and private, with no third parties involved.
- **Regulatory Compliance**: DSG ensures that users remain compliant with global data regulations, helping avoid legal risks associated with improper data handling or unauthorized access. This aligns with the growing demand for digital sovereignty, where users retain full authority over their data, as emphasized in discussions about UnoLock’s privacy-focused framework.

4.2.4 Use Cases

- **Personal Data Management**: Individuals who want to manage their personal data with full transparency and control can use DSG to ensure that no data is shared or accessed without their explicit consent.
- **Corporate Data Handling**: Businesses that handle sensitive customer information can implement DSG to provide clients with the highest standards of data privacy and control.
- **Estate Planning**: DSG allows users to plan for the future, determining how their data will be managed, transferred, or deleted after death.

4.2.5 Benefits

- **Enhanced Data Security**: DSG provides users with secure, end-to-end encryption, ensuring that data is safe from unauthorized access or tampering.
- **User Empowerment**: With DSG, individuals and organizations have the power to control every aspect of their data lifecycle, from access to deletion.
- **Increased Privacy**: By eliminating third-party involvement, DSG ensures that sensitive data is never exposed to external entities or unauthorized actors.

4.2.6 FAQs

How does DSG differ from traditional data management?

Traditional data management often involves third parties who store and manage data on behalf of users. DSG eliminates third-party involvement, giving users full control over how their data is handled, shared, or deleted.

Can DSG help with regulatory compliance?

Yes, DSG is designed to ensure compliance with global privacy standards, such as GDPR and HIPAA, by providing full control over data access, sharing, and deletion.

What happens to my data if I opt out or delete it under DSG?

If you opt out or delete data using DSG, it is permanently removed from all systems and cannot be recovered or accessed by any third party.

4.2.7 Integration with Other Features

- **Legacy Planning and Opt-Out**: DSG’s control mechanisms extend to legacy planning, allowing users to decide how their data will be handled after their passing.
- **Autonomy and Control**: DSG works in tandem with UnoLock’s **Autonomy and Control** features to ensure that users can dictate every action taken with their data.

4.3 DSG Core Pillars

4.3.1 Overview

The **Core Pillars of Data Self-Governance (DSG)** are the foundational principles that define how DSG operates within UnoLock. These pillars ensure that users have complete autonomy over their data, prioritize security and privacy, and allow for long-term data management through legacy planning and opt-out features. By adhering to these pillars, UnoLock guarantees a robust and user-centric data governance model, where individuals control every aspect of their digital assets and sensitive information.

4.3.2 Key Features

- **Security and Privacy**: DSG guarantees the highest level of security with end-to-end encryption, ensuring that only the user has access to their data. No third parties, including UnoLock, can decrypt or access the data, providing complete privacy.
- **Autonomy and Control**: Users have full authority over their data, deciding who can access, share, modify, or delete it. This pillar reinforces the user’s ownership of their digital footprint, preventing any unauthorized actions.
- **Legacy Planning and Opt-Out**: DSG offers long-term planning features, allowing users to establish what happens to their data after they are no longer able to manage it. This includes data inheritance, deletion, or transfer options, ensuring control beyond the user's lifetime.

4.3.3 Why It Matters

- **Holistic Data Management**: The core pillars of DSG ensure that every aspect of data management is addressed, from securing the data to determining who can access it and how it is handled long-term.
- **Uncompromised Security**: By focusing on security and privacy, DSG ensures that users’ sensitive information remains protected from breaches and unauthorized access.
- **Lifelong Control**: The inclusion of legacy planning ensures that data control doesn't stop with the user's death or incapacitation, offering peace of mind that their digital assets will be handled according to their wishes. This aligns with the concept of digital sovereignty, where users maintain full ownership and authority over their data throughout its lifecycle.

4.3.4 Use Cases

- **Data Governance for Businesses**: Companies that handle large volumes of sensitive client data can implement DSG’s core pillars to ensure that each client's data is handled securely and with full transparency.
- **Personal Data Autonomy**: Individuals concerned with maintaining control over their digital footprint can use DSG’s autonomy and control features to limit data sharing and enforce strict access permissions.
- **Estate and Legacy Planning**: Users can plan for the future of their data by using DSG’s legacy planning features to ensure their data is either transferred to trusted individuals or deleted after death.

4.3.5 Benefits

- **Enhanced Data Security**: The Security and Privacy pillar ensures all user data is protected by state-of-the-art encryption.
- **Full Autonomy**: The Autonomy and Control pillar guarantees that users have complete decision-making authority over their data.
- **Long-Term Data Planning**: Legacy Planning allows users to determine the future of their data, ensuring their digital assets are handled according to their wishes.

4.3.6 FAQs

What are the key pillars of DSG?

DSG is built around three core pillars: Security and Privacy, Autonomy and Control, and Legacy Planning and Opt-Out. These pillars ensure that users have full control, long-term management, and protection of their data.

How does DSG’s Security and Privacy pillar protect my data?

DSG uses end-to-end encryption to secure your data, meaning that only you can access it, and no third parties, including UnoLock, can decrypt it.

What happens to my data after I’m gone?

DSG’s Legacy Planning pillar allows you to decide what happens to your data after your death or incapacity, whether that involves transferring it to trusted parties or having it deleted.

4.3.7 Integration with Other Features

- **End-to-End Encryption**: The Security and Privacy pillar is integrated with UnoLock’s encryption systems, ensuring that all data remains protected throughout its lifecycle.
- **Legacy Planning Tools**: The Legacy Planning and Opt-Out pillar works alongside UnoLock’s tools for secure inheritance and long-term data management.

4.4 Security and Privacy in DSG

4.4.1 Overview

The **Security and Privacy** pillar of Data Self-Governance (DSG) is designed to ensure that all user data is protected by state-of-the-art security measures and remains private at all times. UnoLock guarantees that only the user has access to their data, with no involvement from third parties. Through **end-to-end encryption**, **zero-knowledge architecture**, and strict privacy protocols, DSG ensures that sensitive information is safeguarded from unauthorized access, breaches, or misuse, giving users full confidence in their data's safety and privacy.

4.4.2 Key Features

- **End-to-End Encryption**: All data managed under DSG is encrypted from the moment it is created, through transmission, and while stored, ensuring that only the user holds the decryption keys. No third parties, including UnoLock, can access this data.
- **Zero-Knowledge Architecture**: UnoLock operates on a zero-knowledge model, meaning that even the platform cannot view or access user data. This guarantees maximum privacy, as only the user controls access to the information.
- **No Third-Party Data Sharing**: DSG does not permit third-party access or sharing of user data unless explicitly authorized by the user. This ensures that data remains strictly private and under the user’s control.

4.4.3 Why It Matters

- **Protection Against Data Breaches**: In a world where data breaches are common, DSG’s security and privacy measures offer a robust defense, ensuring that unauthorized parties can never access sensitive user data.
- **Complete Privacy**: With zero-knowledge architecture and strong encryption, users are assured that their data is never accessed or monitored by external entities or even by UnoLock itself. This aligns with UnoLock’s commitment to prioritizing user privacy in an era of growing distrust in centralized data systems.
- **Compliance with Global Standards**: DSG’s security and privacy features ensure compliance with global data privacy laws like **GDPR** and **HIPAA**, making it a trusted solution for users who must adhere to strict regulatory frameworks.

4.4.4 Use Cases

- **Personal Data Protection**: Individuals who manage highly sensitive personal data, such as health records or financial documents, can trust DSG to keep this information private and protected from unauthorized access.
- **Enterprise-Level Security**: Businesses dealing with confidential information or intellectual property can leverage DSG’s security measures to ensure their data is encrypted and inaccessible to external threats.
- **Cross-Border Compliance**: For organizations that operate across regions with strict data privacy laws, DSG’s comprehensive security and privacy protocols ensure that data remains compliant with international standards.

4.4.5 Benefits

- **End-to-End Data Protection**: From creation to deletion, data is protected by strong encryption, preventing unauthorized access at all stages.
- **Privacy Assurance**: DSG guarantees that users maintain full control over their data, with no third-party or platform access, ensuring maximum privacy.
- **Risk Mitigation**: The security measures in place reduce the risk of data breaches, leaks, or unauthorized sharing, safeguarding users’ sensitive information.

4.4.6 FAQs

❓ **How does DSG ensure my data is fully secure?**

DSG uses **end-to-end encryption** to protect your data, ensuring that it remains encrypted during transmission and storage. Only you have access to the decryption keys, making your data fully secure.

❓ **What is zero-knowledge architecture, and how does it protect my privacy?**

Zero-knowledge architecture means that UnoLock, as the platform provider, cannot access or view your data. All encryption keys remain with you, ensuring complete privacy.

❓ **Can anyone, including UnoLock, access my data without my permission?**

No, UnoLock operates on a strict privacy model where no external parties, including UnoLock itself, can access your data without your explicit consent.

4.4.7 Integration with Other Features

- **Client-Side Encryption**: DSG’s **client-side encryption** ensures that all data is encrypted on the user’s device before being transmitted or stored, enhancing the privacy and security of data management.
- **Granular Data Access Control**: DSG’s **granular access controls** allow users to define exactly who can view or edit their data, ensuring full compliance with privacy requirements.

4.5 Autonomy and Control in DSG

4.5.1 Overview

The **Autonomy and Control** pillar of Data Self-Governance (DSG) empowers users to maintain full authority over how their data is accessed, shared, and managed. In the UnoLock platform, DSG gives individuals and organizations the ability to dictate every aspect of their data's lifecycle, from creation to deletion, without relying on third parties. This user-centric approach ensures that all decisions about data usage are made solely by the owner, giving users unparalleled freedom to manage their digital assets.

4.5.2 Key Features

- **Granular Access Permissions**: Users have the ability to set precise permissions for who can access or modify their data, whether it's granting full access, read-only rights, or no access at all. These permissions can be tailored for individual users or groups.
- **Data Ownership**: DSG ensures that the user retains full ownership of their data. This means that only the user has the authority to share, modify, or delete their data, with no intervention from third parties.
- **Real-Time Access Control**: Users can adjust data access permissions in real-time, allowing them to revoke or grant access instantly if the situation changes. This ensures ongoing flexibility and control over sensitive information.

4.5.3 Why It Matters

- **User Empowerment**: DSG's autonomy and control features empower users by giving them complete authority over their digital information, ensuring that no external party can override their decisions about data usage.
- **Transparency in Data Management**: With full control over who accesses their data, users can maintain transparency, knowing exactly who can see or modify their sensitive information at any given time.
- **Reduced Dependency on Third Parties**: Traditional data systems often place control in the hands of external entities, such as cloud providers or service platforms. DSG reverses this dynamic, placing full control in the hands of the user, aligning with the principle of digital sovereignty, defined as a party's right to control its own digital data.

4.5.4 Use Cases

- **Personal Data Control**: Users managing sensitive personal documents, such as legal, health, or financial records, can use DSG's autonomy features to ensure that only authorized individuals or services have access.
- **Corporate Data Governance**: Businesses can use DSG to maintain strict control over internal data, setting granular permissions for different departments or teams, ensuring that sensitive company information remains confidential.
- **Temporary Access for Collaborators**: In collaborative projects, users can grant temporary access to files or folders, allowing collaborators to view or edit data only for a limited time before the access is revoked.

4.5.5 Benefits

- **Complete Control**: Users are fully in charge of their data, including decisions on access, sharing, and deletion, without relying on third-party platforms or services.
- **Flexibility in Permissions**: Real-time access control allows users to adapt their permissions based on changing circumstances, granting or revoking access as needed.
- **Data Sovereignty**: Users are the sole owners of their data and can enforce strict access rules, ensuring that unauthorized individuals or services can never access their sensitive information.

4.5.6 FAQs

How can I control who accesses my data with DSG?

DSG allows you to set granular access permissions, enabling you to control who can view, edit, or share your data. You can modify these permissions in real-time through UnoLock's interface.

Can I revoke access once I've shared my data?

Yes, you can revoke access to your data at any time. DSG's real-time access control features allow you to immediately stop others from accessing your files.

Does DSG require third parties to manage or oversee my data?

No, DSG ensures that you are the only one in control of your data. Third parties, including UnoLock, do not have access unless explicitly authorized by you.

4.5.7 Integration with Other Features

- **Spaces for Granular Data Control**: The **Spaces** feature in UnoLock works alongside DSG's autonomy and control features, allowing users to manage permissions for specific groups or datasets within their vaults.
- **Legacy Planning**: DSG's control mechanisms extend to **Legacy Planning**, where users can assign trusted individuals to manage or inherit their data after death or incapacity, maintaining control beyond their lifetime.

4.6 Legacy Planning and Opt-Out in DSG

4.6.1 Overview

The **Legacy Planning and Opt-Out** feature of Data Self-Governance (DSG) enables users to plan for the future of their data, ensuring that they can decide what happens to their digital assets after death or incapacitation. In UnoLock's DSG model, users have the flexibility to designate trusted individuals who will inherit their data or opt to delete their information upon a certain condition, such as prolonged inactivity. Additionally, DSG provides users with full **opt-out** capabilities, allowing them to withdraw from data-sharing agreements and permanently delete their data whenever they choose.

4.6.2 Key Features

- **Legacy Planning**: Users can establish a comprehensive plan for their digital assets, deciding whether to transfer their data to trusted individuals (via **LegacyLink**) or permanently delete it. This planning ensures that their data is handled according to their wishes after they are no longer able to manage it.
- **Automatic Data Deletion**: Users can set up predefined triggers for data deletion, such as inactivity over a specified period. Once triggered, their data will be securely and permanently removed from UnoLock's system.
- **Opt-Out Capability**: DSG allows users to opt out of data-sharing agreements at any time, ensuring they have the right to revoke access, stop participating in any data-sharing programs, and delete data as necessary.

4.6.3 Why It Matters

- **Future-Proof Data Management**: Legacy planning allows users to ensure their data is handled according to their preferences even after they are gone, providing peace of mind that their digital assets won't fall into the wrong hands.
- **Data Privacy Control**: With the opt-out feature, users can withdraw from data-sharing agreements or revoke previously granted access whenever they feel it's necessary, maintaining control over their data throughout its lifecycle.
- **Compliance and Ethical Data Handling**: By giving users the power to delete or transfer their data, DSG ensures compliance with global regulations like **GDPR**, where users have the right to be forgotten, and supports ethical data management principles. This feature addresses critical needs for secure asset transfer, as highlighted in discussions about UnoLock's LegacyLink, ensuring users' digital legacies are protected and managed as intended.

4.6.4 Use Cases

- **Estate Planning**: Individuals who want to plan for the future of their digital assets can use DSG's legacy planning tools to designate trusted individuals who will gain access to important files, financial records, or sensitive data after their passing.
- **Inactivity-Based Deletion**: Users who wish to keep their data only while actively managing it can set automatic deletion triggers based on inactivity, ensuring their data doesn't remain accessible indefinitely.
- **Full Data Withdrawal**: Users concerned about privacy or no longer wanting to share their data with certain services can leverage DSG's opt-out feature to immediately revoke access and delete their data from UnoLock's platform.

4.6.5 Benefits

- **Peace of Mind**: Legacy planning ensures that users have full control over what happens to their data in the event of death or incapacity, guaranteeing their wishes are honored.
- **Control Over Data Lifecycle**: The opt-out feature and automatic deletion triggers allow users to manage their data throughout its lifecycle, ensuring they can withdraw or erase data when it's no longer needed.
- **Regulatory Compliance**: DSG's legacy and opt-out features align with data privacy laws like GDPR, offering users the right to be forgotten and full control over their data at any stage.

4.6.6 FAQs

? What happens to my data after I pass away or become incapacitated?

Through DSG’s **Legacy Planning**, you can designate trusted individuals to inherit your data or opt to have it permanently deleted based on your wishes.

? Can I delete my data if I no longer want to participate in data-sharing programs?

Yes, DSG’s **opt-out** feature allows you to revoke access and permanently delete your data from UnoLock’s systems at any time.

? How does automatic data deletion work?

You can set triggers based on inactivity (e.g., no logins for a set period), which will automatically initiate secure deletion of your data if the criteria are met.

4.6.7 Integration with Other Features

- **Inactivity-Triggered Safe Access (LockoutGuard and LegacyLink)**: DSG’s legacy planning integrates with **LegacyLink**, allowing designated individuals to securely inherit vault access after a period of inactivity or based on specific conditions set by the user.
- **Granular Access Control**: Legacy planning and opt-out features work alongside DSG’s **granular access control** to ensure that users maintain full control over who has access to their data, both during their lifetime and after.

4.7 Why DSG is Important?

4.7.1 Overview

Data Self-Governance (DSG) is crucial in today's data-driven world because it places control of personal and organizational data back into the hands of users. As data privacy concerns continue to grow, with frequent data breaches, misuse, and third-party surveillance, DSG ensures that individuals and businesses maintain full control over their sensitive information. DSG is a transformative framework that allows users to manage their data's entire lifecycle, dictating access, privacy, and security, without relying on third-party systems or facing the risks of unauthorized access.

4.7.2 Key Features

- **User-Centric Control**: DSG shifts data control entirely to the user, ensuring that they can manage who accesses, modifies, and shares their information. This prevents unauthorized access and gives users peace of mind that their data is always under their control.
- **Enhanced Privacy and Security**: With **end-to-end encryption** and **zero-knowledge architecture**, DSG ensures that no third party, including UnoLock, can access or view users' data. This secures data against breaches, hacking, and unauthorized sharing.
- **Compliance with Global Regulations**: DSG supports compliance with data privacy laws like **GDPR** and **HIPAA**, allowing users to meet strict regulatory standards by ensuring full control, protection, and rights over their data.

4.7.3 Why It Matters

- **Rising Data Privacy Concerns**: As personal and corporate data is increasingly at risk from breaches, surveillance, and third-party misuse, DSG provides a solution by ensuring that only authorized individuals can access sensitive information.
- **Empowerment Through Control**: DSG allows users to be fully empowered when it comes to managing their digital identity. This is vital in a landscape where companies often monetize or misuse personal data without proper consent.
- **Protection Against Data Exploitation**: Many users are unaware of how their data is shared or exploited by third parties. DSG puts an end to this by ensuring that data usage is entirely transparent and under the control of the owner, aligning with the principle of digital sovereignty, defined as a party's right to control its own digital data.
- **Future-Proofing Data Management**: DSG's ability to evolve with new regulations and security standards makes it a future-proof solution, ensuring users are always ahead in terms of privacy and compliance.

4.7.4 Use Cases

- **Personal Data Protection**: Individuals seeking to protect their personal data from being misused by third-party services or platforms can use DSG to retain full control, ensuring their data is only accessed or shared when they explicitly allow it.
- **Corporate Data Security**: Businesses that handle sensitive customer or internal data can implement DSG to ensure full compliance with data regulations and provide transparency for customers about how their data is used.
- **Global Compliance and Privacy Standards**: Organizations operating in multiple regions can benefit from DSG's alignment with international data privacy laws, ensuring that they meet regulatory requirements without compromising on security.

4.7.5 Benefits

- **Complete Control Over Data**: DSG allows users to manage every aspect of their data, ensuring they are the only ones who control access, sharing, and deletion.
- **Enhanced Privacy and Security**: With DSG, users' data is protected from unauthorized access through encryption and strict privacy protocols, offering enhanced protection in an age of increasing data breaches.
- **Compliance and Future-Proofing**: DSG ensures organizations and individuals are compliant with current privacy laws and prepared for future regulations by maintaining the highest standards of data control and security.

4.7.6 FAQs

Why is DSG necessary in today’s digital world?

DSG is essential because it returns control of data to the user in a world where data privacy breaches and misuse are increasingly common. It ensures that users can dictate who accesses, shares, and manages their data.

How does DSG protect my data from third-party misuse?

DSG uses end-to-end encryption and zero-knowledge architecture, meaning that even UnoLock, the platform itself, cannot access or share your data without your explicit consent.

Can DSG help me comply with data privacy regulations?

Yes, DSG aligns with privacy regulations such as **GDPR** and **HIPAA**, ensuring that you have full control over your data and are compliant with data protection laws.

4.7.7 Integration with Other Features

- **Security and Privacy**: DSG integrates with **end-to-end encryption** and **zero-knowledge architecture**, providing the backbone for data security by ensuring that all data remains private and protected at all times.
- **Autonomy and Control**: DSG’s emphasis on user control works hand-in-hand with features like **granular access permissions**, ensuring that users are the only ones who manage access to their data.

4.8 DSG Implementation Challenges

4.8.1 Overview

Data Self-Governance (DSG) is a transformative framework that empowers individuals and organizations to take full control over their data, aligning with the principle of digital sovereignty, where users maintain authority over their digital assets. However, implementing DSG effectively comes with several challenges that must be addressed to achieve its full potential. These challenges span technical, regulatory, and user adoption aspects. Understanding these obstacles is crucial for ensuring that DSG systems like UnoLock function smoothly and deliver the promised autonomy, security, and privacy, particularly in a landscape where user control is both a technical necessity and a competitive differentiator.

4.8.2 Technical Complexity

One of the primary challenges of implementing DSG is the technical complexity involved in building a secure, user-centric data platform. DSG systems must be designed to provide **end-to-end encryption** and operate within a **zero-knowledge architecture**, where even the platform itself cannot access user data. This requires sophisticated encryption protocols, robust key management, and seamless user interfaces that allow non-technical users to securely manage their own data.

- **Key Management**: Ensuring users can securely store and manage their encryption keys without losing access to their data is a significant hurdle. If a user loses their key, they could lose access to their entire data vault, which complicates the user experience and requires secure, reliable backup solutions.
- **Real-Time Access Control**: Implementing fine-grained, real-time access control mechanisms requires integrating flexible permission systems that allow users to easily grant and revoke access without compromising security.
- **Scalability**: DSG systems must handle large volumes of data and users across various platforms and devices, which poses scalability challenges. Ensuring that DSG infrastructure can scale without compromising performance or security is critical.

4.8.3 User Adoption and Education

A major barrier to the widespread adoption of DSG lies in user education and understanding. Most users are accustomed to relying on third-party platforms for data management, where they have minimal control. Transitioning to a DSG model, where users are responsible for controlling their own data, requires a significant mindset shift.

- **Understanding Data Ownership**: Users must understand the implications of true data ownership, including the responsibility that comes with managing access permissions, encryption keys, and legacy planning. Educating users about the benefits of DSG, such as enhanced security, privacy, and compliance, while also addressing the complexities involved, is a key challenge.
- **Simplifying the User Experience**: DSG systems need to be user-friendly, ensuring that even non-technical users can easily manage their data. If the platform is too complex, it risks alienating users who may revert to traditional, more familiar data management systems.
- **Trust in the System**: Convincing users to trust a DSG platform requires transparency in how their data is handled. Users need to be confident that they have true ownership and control of their data without hidden third-party access.

4.8.4 Compliance and Legal Considerations

While DSG systems provide enhanced privacy and security, they must also navigate complex regulatory environments. Compliance with global data protection laws, such as **GDPR** (General Data Protection Regulation) and **HIPAA** (Health Insurance Portability and Accountability Act), adds another layer of complexity.

- **Regulatory Conflicts**: DSG platforms operate on the premise that users control their data. However, certain jurisdictions may have conflicting laws that require businesses to provide access to user data under specific conditions, such as government or legal requests. DSG systems must reconcile the balance between user control and legal obligations.
- **Data Localization and Residency**: In some regions, regulations require that data be stored within specific geographical boundaries. DSG platforms must ensure that user data remains compliant with local data residency requirements while still providing global access to the platform.
- **Right to Be Forgotten**: DSG systems must ensure that users can fully delete their data in compliance with privacy laws, such as GDPR's “right to be forgotten.” However, ensuring complete deletion across all storage systems and backups can be technically challenging.

4.8.5 Security Risks

Although DSG provides enhanced security through user-centric control and encryption, it also introduces new security risks.

- **Key Loss**: If a user loses their encryption key, they may lose permanent access to their data. This necessitates secure backup and recovery solutions that don't compromise the privacy-first principles of DSG.
- **Insider Threats**: Even with DSG's autonomy and privacy guarantees, insider threats, such as users with granted access who misuse the data, remain a concern. Monitoring and auditing access without infringing on user privacy is a delicate balance.
- **Data Fragmentation**: DSG systems may store data across multiple encrypted environments or devices. Ensuring that this distributed data remains secure and accessible to authorized users without introducing vulnerabilities is a complex challenge.

4.8.6 Legacy Planning and Continuity

Legacy planning in DSG systems requires careful consideration, especially in scenarios where a user becomes incapacitated or passes away. Implementing secure inheritance mechanisms, such as **LegacyLink** in UnoLock, ensures that trusted individuals can access or delete data based on the user's instructions. However, ensuring this process is both secure and seamless presents challenges.

- **Trust and Verification**: Verifying the identity of a user's designated heirs or trusted individuals in a secure manner without exposing data to unauthorized parties requires robust verification mechanisms.
- **Automation vs. Control**: Users must balance the automation of legacy planning (e.g., triggering access after inactivity) with their desire to retain control over every aspect of their data. The challenge lies in designing a system that automates data handling under certain conditions while still allowing for flexibility and control.

4.8.7 System Maintenance and Updates

DSG platforms must remain up to date with the latest security protocols and technologies. This includes regular updates to encryption standards, bug fixes, and protection against newly discovered vulnerabilities.

- **Maintaining User Control**: Ensuring that users retain control of their data even during platform updates or system-wide changes is crucial. This involves providing transparent update processes and ensuring that updates don't interfere with user access or data integrity.
- **Managing Backups and Redundancy**: Implementing secure, encrypted backups that don't compromise user control or privacy is essential. The challenge lies in maintaining redundancy while ensuring that backups are stored securely and are accessible only to authorized individuals.

4.9 The Future of DSG and DSGaaS

4.9.1 Overview

The future of **Data Self-Governance (DSG)** is inherently tied to the concept of **digital sovereignty**, the right and ability of individuals, organizations, and even nations to control and manage their data autonomously. As we move deeper into the digital age, the rise of DSG highlights a shift away from traditional centralized data management models, where users' data is controlled by third-party platforms, toward a decentralized, user-first approach that empowers individuals to exercise true sovereignty over their digital assets. **DSG platforms** like UnoLock, built on principles of user autonomy, end-to-end encryption, and zero-knowledge architecture, are setting a new standard for data management, particularly in a landscape marked by increasing global concerns around privacy breaches, data exploitation, and surveillance. These platforms are designed to safeguard not only personal privacy but also the broader concept of **digital freedom**, the right of users to decide how their data is shared, stored, and accessed without interference from third parties.

4.9.2 DSGaaS: Data Self-Governance as a Service

As the demand for privacy-first solutions grows, we are witnessing the rise of **Data Self-Governance as a Service (DSGaaS)**, a service-oriented model that allows organizations and individuals to implement DSG principles without the technical burden of developing such systems in-house. DSGaaS platforms are becoming increasingly common, providing businesses with pre-built, scalable solutions that enable them to offer their users DSG functionality as part of their product or service offerings.

This move toward DSGaaS reflects a broader trend in technology: the **democratization of privacy and security**. Just as cloud services revolutionized the way businesses handle infrastructure by making it accessible and scalable, DSGaaS platforms are making data self-governance accessible to a wider audience. Companies that integrate DSGaaS into their operations are not only empowering their users but also positioning themselves as **leaders in data privacy**, setting themselves apart in an era where trust in digital services is paramount.

4.9.3 Digital Sovereignty and Regulatory Alignment

The growing popularity of DSG and DSGaaS is also aligned with the global push toward **data sovereignty**. Many countries, particularly in the European Union with frameworks like **GDPR**, are emphasizing the importance of keeping data within national boundaries and ensuring that individuals retain control over their information. DSG perfectly complements these regulations, allowing users to exercise their right to privacy and control, and offering organizations a way to meet regulatory requirements without compromising on user autonomy.

Moreover, as DSGaaS platforms become more widespread, they will likely serve as a key component of broader **data sovereignty strategies** for both private companies and governments. By adopting DSGaaS, organizations can ensure they are compliant with global privacy regulations while also offering users the freedom and security associated with self-governed data management.

4.9.4 Conclusion: A New Paradigm for Data Management

In conclusion, **DSG and DSGaaS** represent a fundamental shift in the way data is managed, governed, and protected. These frameworks put control back into the hands of users, allowing them to safeguard their personal information in a way that aligns with the principles of digital sovereignty, defined as a party’s right to control its own digital data. As DSGaaS platforms become more common, we can expect them to play an integral role in reshaping data governance across industries, transforming not only how data is secured but also how trust is built in the digital world.

In the future, **DSGaaS** will likely become the default solution for organizations seeking to offer privacy-first services to their customers, enabling seamless, decentralized data governance across a wide range of applications. This evolution will strengthen digital sovereignty on both an individual and national level, helping to create a more secure and privacy-focused internet for all. UnoLock’s pioneering role in this space positions it as a leader in fostering a user-centric digital future.

5. Pricing Tiers

5.1 Payment & Pricing Overview

5.1.1 Overview

UnoLock offers four pricing tiers for different levels of storage, collaboration, recovery, and coercion-resistance needs. Across all tiers, Safe access is controlled by registered access keys such as passkeys or hardware keys, not by conventional username and password accounts. Payments can be made by credit card or Bitcoin, and the payment flow is designed to keep billing operations separate from Safe contents and normal Safe identity.

5.1.2 Key Features

- **Flexible Billing Models**: Choose monthly billing or annual prepayment, with annual discounts on Sovereign and HighRisk.
- **Payment Separation by Design**: Billing is handled separately from Safe contents and normal Safe access, supporting UnoLock's OPSEC-first model.
- **Scalable Storage**: Paid tiers support additional encrypted storage at $1 per GB per month.
- **Access Key Expansion**: Paid tiers support multiple access keys so one Safe can be used across devices or by multiple people, each with their own key.
- **Clear Tier Progression**: Each tier adds storage and higher-risk operational features without changing the underlying client-side encryption model.
- **Predictable Downgrade Rules**: Downgrades require creating a new Safe, with unused balances returned as promo credit.

5.1.3 Why It Matters

The pricing model needs to do more than assign storage limits. It also needs to preserve UnoLock's privacy model while giving users a clean path from a simple personal Safe to multi-key family access, Shared Space collaboration, and high-risk protection features. These tiers are structured to scale that way without changing the core access-key and client-side encryption model.

5.1.4 Billing Details

- **Monthly Subscription**: Charged at the start of each billing cycle. Storage overages and extra access keys are applied to the next cycle.
- **Annual Prepayment**: One-time annual purchase with the published yearly discount where applicable. Storage overages are still billed monthly.
- **Bitcoin Payments**: The payment flow generates a one-time payment reference and amount. Once confirmed, credit is applied without turning Safe access into an identity-bound account workflow.
- **Prepaid Credit Model**: Bitcoin users can pre-load credit and let the balance cover time, storage overages, and extra access keys.
- **Tier Transition Rules**:
- **Upgrades**: Apply immediately, with proration where supported by the billing flow.
- **Downgrades**: Require creating a new Safe so the resulting state matches the lower tier cleanly.
- **Storage Expansion**: Inheritance, Sovereign, and HighRisk support additional storage at $1/GB/month.
- **Privacy by Design**: Billing data is processed separately from encrypted Safe contents. Safe access continues to rely on access keys, not on stored passwords.

5.1.5 Pricing Tiers Overview

UnoLock’s four-tier structure scales from simple seed storage to high-risk operational security:

- **Free ($0/month)**: 1MB Safe with one included access key, core encryption, and reply-only messaging.
- **Inheritance ($3/month or $36/year)**: 1GB base storage, LegacyLink, and one included access key expandable up to 10.
- **Sovereign ($8/month or $86.40/year)**: 5GB base storage, three included access keys, Spaces, Shared Spaces collaboration, DuressDecoy, and advanced messaging.
- **HighRisk ($14/month or $151.20/year)**: 5GB base storage, three included access keys, Shared Spaces collaboration, and the most aggressive coercion-response features.

Each paid tier builds on the previous with more storage, more access-key capacity, and more advanced collaboration or threat-response features.

5.2 How payments work

5.2.1 Overview

This section explains how billing works across UnoLock's four tiers: Free, Inheritance, Sovereign, and HighRisk. It covers subscriptions, Bitcoin payments, prepaid credit, upgrades, downgrades, storage overages, and extra access keys. It does not change how your Safe is unlocked; Safe access still depends on registered access keys.

5.2.2 Who Is This For?

This section is relevant for any UnoLock user choosing a paid tier, managing prepaid credit, or planning around storage and access-key limits.

5.2.3 What Does It Explain?

This section covers: - How **subscription payments** (monthly or yearly) are processed and adjusted for storage or key overages. - How **Bitcoin payments** are validated and credited through the separate payment flow. - How users manage **upgrades**, **downgrades**, and **storage/key expansion**, with a cap of 10 access keys on paid tiers. - How billing is kept separate from encrypted Safe contents and normal Safe access.

5.2.4 Why Is This Important?

Understanding how payments work is critical to: - **Prevent service interruptions** from lapsed payments on paid plans. - **Understand payment privacy boundaries** and how UnoLock separates billing from Safe contents. - **Manage upgrades and downgrades** effectively, aligning with your evolving security needs. - **Predict cost increases** from storage overages ($1/GB/month) or additional access keys (up to 10 maximum). - **Maintain continuity** for estate planning, family use, or high-risk workflows.

5.2.5 How Does the Payment Process Work?

Subscription Model

- **Billing**: Charged at the start of each billing cycle (monthly: $3 for Inheritance, $8 for Sovereign, $14 for HighRisk; yearly: $36 for Inheritance, $86.40 for Sovereign, $151.20 for HighRisk with 10% discount on Sovereign and HighRisk).
- **Overages**: Additional storage beyond the base tier (1GB for Inheritance, 5GB for Sovereign/HighRisk) is billed at $1/GB/month, added to the next cycle. Additional access keys (beyond 1 for Inheritance, 3 for Sovereign/HighRisk, capped at 10) incur charges, applied in the next cycle.
- **Upgrade Anytime**: Tier upgrades are immediate and seamless, with prorated adjustments for remaining time.
- **Downgrade Requires a New Safe**: To keep the lower-tier state clean and predictable, downgrades require creating a new Safe. Unused balances are returned as promotional codes for future use.

Bitcoin Payments

- The app generates a one-time payment reference and payment amount for the transaction.
- Once the transaction is detected and confirmed, credit is applied to the billing flow for the target plan or prepaid balance.
- Bitcoin payments are available for monthly subscriptions, annual plans, or adding credits for storage/key expansion (e.g., up to 10 keys maximum).
- The payment path is designed to keep payer records separated from Safe contents and normal Safe identity in day-to-day operation.

Prepaid Credit Model

- Available for Bitcoin users to pre-load credits for long-term use, covering tier costs, storage overages, or additional keys (capped at 10).
- Credits are consumed based on the tier, time, and storage usage (e.g., $1/GB/month for overages).
- If credits run out, the Safe gracefully reverts to the Free tier (1MB storage, 1 included access key) with no data loss.
- Promotional codes from refunds or downgrades can be applied toward future plans.

Tier Transition Rules

- **Upgrades**: Immediate, with prorated adjustments for the remaining billing period. For example, upgrading from Inheritance ($3/month) to Sovereign ($8/month) adjusts the cost based on time left.
- **Downgrades**: Require new Safe creation to prevent privilege loss or unsafe state rollback. Unused balances are issued as promotional codes.
- **Access Key Expansion**: Inheritance includes 1 key, Sovereign and HighRisk include 3 keys, with expansion up to 10 keys maximum across all paid tiers. Additional keys incur charges, reflected in the next billing cycle or deducted from prepaid credits.

Privacy by Design

- Billing data is handled separately from encrypted Safe contents.
- Bitcoin payments use one-time payment references instead of turning Safe access into a conventional account/password model.
- The payment process supports UnoLock’s privacy-first architecture while remaining distinct from client-side encryption and access-key authentication.

5.3 How storage cost is calculated

5.3.1 Overview

This section details how storage costs are calculated for UnoLock's four-tier pricing model, Free, Inheritance, Sovereign, and HighRisk. Each tier offers a baseline storage allocation, with paid tiers supporting expandable storage at $1 per GB per month. Understanding storage costs helps you budget for growth and maintain uninterrupted paid-tier service.

5.3.2 Who Is This For?

This section is for all UnoLock users, especially those on paid tiers who may exceed their baseline storage limits and want to understand how additional charges are calculated.

5.3.3 What Does It Explain?

This section covers: - How storage costs are calculated based on the **amount of encrypted data** stored in your Safe. - The **baseline storage allocation** for each tier: 1MB (Free), 1GB (Inheritance), 5GB (Sovereign/HighRisk). - How **extra storage** beyond the baseline is charged at $1 per GB per month for paid tiers. - Differences in handling storage costs between **subscription** and **prepaid credit** models. - Real-time **storage usage tracking** within the Safe interface.

5.3.4 Why Is This Important?

Understanding storage cost calculation is critical to: - **Avoid surprise charges** from exceeding baseline storage limits, ensuring predictable budgeting. - **Plan storage needs** effectively, whether for minimal seed phrases or extensive files. - **Maintain uninterrupted paid-tier service** by managing credits (prepaid model) or anticipating billing adjustments (subscription model). - **Scale securely** without performance or pricing issues, aligning with UnoLock's streamlined four-tier model that supports user growth and privacy. This transparency fosters trust and adoption in a privacy-conscious market.

5.3.5 How Does Storage Cost Work?

Baseline Storage per Tier

Each tier includes a fixed or expandable storage allocation: - **Free**: 1MB (fixed, non-expandable), suitable for passwords, seed phrases, or backup codes. - **Inheritance**: 1GB (expandable at $1/GB/month), ideal for family Safes or digital legacies. - **Sovereign**: 5GB (expandable at $1/GB/month), designed for professionals or crypto users. - **HighRisk**: 5GB (expandable at $1/GB/month), tailored for high-risk users with sensitive data.

Additional Storage Logic

- **Overages**: For paid tiers, storage exceeding the baseline (1GB for Inheritance, 5GB for Sovereign/HighRisk) is charged at $1 per GB per month, calculated in real-time based on compressed, encrypted data.
- **Billing**: Overages are reflected in the next billing cycle for subscription users (monthly or yearly) or deducted from credits for prepaid users.
- **Free Tier**: No expansion is available; storage is capped at 1MB.

Prepaid Users

- **Credit Consumption**: Credits are consumed based on the tier's base cost, time, and storage usage. Exceeding the baseline accelerates credit usage (e.g., $1/GB/month for overages).
- **Low Balance**: If credits run out, the Safe reverts to the Free tier (1MB storage, 1 included access key) with no data loss until credits are added.
- **Monitoring**: Users can track storage usage in real-time via the Safe interface to manage credits effectively.

Subscription Users

- **Overage Billing**: Additional storage fees are added to the next billing cycle’s invoice (e.g., $1/GB/month beyond 5GB for Sovereign).
- **Real-Time Tracking**: The Safe interface displays current storage usage, helping users stay below thresholds or expand consciously.
- **Flexibility**: Users can adjust storage needs without changing tiers, with costs reflected in monthly or annual billing.

Storage Usage Tracking

- The UnoLock Safe interface provides real-time monitoring of storage usage, showing encrypted data size (compressed) and alerting users when approaching or exceeding baseline limits.
- This transparency ensures users can budget for overages or adjust data to stay within their tier’s allocation, maintaining control over costs and service level.

5.4 Free: Entry-Level Tier

5.4.1 Overview

The Free tier is UnoLock’s entry-level Safe. It gives individuals a no-cost place to protect critical records such as seed phrases, passwords, recovery codes, and short notes with client-side encryption and WebAuthn-based access. The Free tier includes 1MB of fixed storage and one registered access key.

5.4.2 Who Is This For?

The Free tier is designed for individuals who want a lightweight but serious Safe without committing to a paid plan. It fits seed phrase holders, privacy-focused users, and anyone who wants to learn the UnoLock model before expanding to more storage or additional access keys.

5.4.3 What Does It Offer?

The Free tier provides essential security features at no cost, including: - **WebAuthn Access Keys**: Safe access through a passkey, hardware key, or compatible device authenticator. - **Client-Side Local File Encryption**: Data is encrypted on-device before syncing, ensuring servers never see plaintext. - **Post-Quantum Encryption**: Protection against future quantum decryption threats. - **LockoutGuard**: One-time recovery path that gets you back in and then returns you to the normal WebAuthn registration model. - **Vault Messaging (Reply-Only Model)**: Receive secure messages from paid-tier Safes and reply once a contact is initiated. - **1MB Storage (Fixed)**: Suitable for encrypted text like passwords, keys, or short notes. - **1 Included Access Key**: One registered access key for the Safe, non-expandable on the Free tier. - **Single-Region Redundancy**: Data is stored securely in one region, not globally replicated.

5.4.4 Why Is This Important?

The Free tier is crucial because it: - Offers a **zero-cost entry** to sovereign-grade encryption, making privacy accessible to all. - Keeps the **access model simple**: one Safe, one access key, no conventional password account. - Provides a **functional sandbox** to explore UnoLock’s ecosystem, fostering trust and adoption among new users. - Supports **secure communication** via reply-only messaging without forcing the user into a paid workflow on day one.

5.4.5 How Does It Work?

- **Sign-In**: Register one access key using your device passkey flow, a hardware key, or another supported authenticator.
- **Encryption**: All Safe contents are encrypted client-side before syncing, ensuring zero-knowledge handling of plaintext.
- **Storage**: Store up to 1MB of text-based data, such as passwords, seed phrases, or recovery codes, with no expansion option.
- **Access**: Limited to 1 registered access key, unlike paid tiers which support additional keys for more devices or more users of the same Safe.
- **Messaging**: Receive messages from paid-tier Safes and reply once a contact is initiated.
- **Recovery**: LockoutGuard protects against device loss using offline QR codes or fallback tokens, requiring no support tickets.
- **Redundancy**: Data is stored in a single secure region, ensuring protection without global replication.

5.4.6 Use Cases

- **Crypto Users**: Secure cold-like wallet seed phrases without cloud exposure, ideal for Bitcoin or Ethereum holders needing a private, offline-like storage solution.
- **Developers**: Store API keys, SSH credentials, or development secrets anonymously, ensuring no linked identity.
- **Privacy Seekers**: Lock away PINs, 2FA recovery codes, or sensitive notes in a secure, no-cost Safe while learning the UnoLock workflow.

5.5 Inheritance: Intermediate Tier

5.5.1 Overview

The Inheritance tier is designed for individuals and families who want a larger Safe plus a controlled inheritance and inactivity model. It adds 1GB of base storage, one included access key expandable up to 10, and LegacyLink for succession planning.

5.5.2 Who Is This For?

The Inheritance tier is ideal for estate planning, family record keeping, and long-term custody of important data that should survive device loss, incapacity, or death.

5.5.3 What Does It Offer?

The Inheritance tier provides enhanced security and inheritance features, including: - **All Free Tier Features**: WebAuthn access keys, client-side encryption, post-quantum protection, LockoutGuard, and single-region redundancy. - **LegacyLink Inheritance System**: Controlled release of recovery access after the configured inactivity conditions are met. - **Vault Messaging (Reply-Only Model)**: Receive secure messages from paid-tier Safes and reply once initiated. - **1GB Base Storage**: Expandable at $1/GB/month, suitable for family records or digital assets. - **1 Included Access Key (Expandable to 10)**: Starts with 1 key and can be expanded for additional family members, devices, or trusted parties. - **Single-Region Redundancy**: Secure data storage in one region, ensuring protection without global replication.

5.5.4 Why Is This Important?

The Inheritance tier is critical because it: - **Ensures Digital Continuity**: LegacyLink provides a clear succession path for important records and digital assets. - **Offers Scalable Storage**: 1GB base storage, expandable at $1/GB/month, supports growing digital estates without complexity. - **Maintains Privacy and Control**: Family members or trusted people can each have their own access key rather than sharing one credential. - **Simplifies Estate Planning**: It gives users a practical middle tier before moving to collaboration or high-risk features.

5.5.5 How Does It Work?

- **LegacyLink Inheritance System**: Users designate successors and set inactivity conditions. When the release path activates, the successor uses the LegacyLink credential and then registers a new WebAuthn access key.
- **Storage**: 1GB base storage supports encrypted files like legal records or seed phrases, with real-time expansion at $1/GB/month for additional needs.
- **Access Keys**: Includes 1 access key and can be expanded up to 10, letting multiple people or devices use the same Safe with their own key.
- **Messaging**: Receive messages from paid-tier Safes and reply once a contact is initiated.
- **Encryption and Redundancy**: Data is encrypted client-side with post-quantum protection and stored in a single secure region, balancing security and simplicity.
- **Recovery**: LockoutGuard ensures recovery via offline QR codes or fallback tokens, preventing lockouts without compromising privacy.

5.5.6 Use Cases

- **Families**: Securely store wills, financial instructions, and digital asset records with a planned succession path.
- **Solo Professionals**: Plan digital succession for business-critical data like client contracts or API keys, enabling trusted colleagues to inherit access securely.
- **Crypto Investors**: Safeguard seed phrases or private keys while planning how heirs can recover access later.

5.6 Sovereign: Advanced Tier

5.6.1 Overview

The Sovereign tier is UnoLock’s advanced collaboration and operational privacy tier. It is built for professionals, crypto users, and families or teams who need more storage, more access keys, Spaces inside the same Safe, and collaboration between separate Safes through Shared Spaces.

5.6.2 Who Is This For?

The Sovereign tier is designed for crypto holders, developers, privacy advocates, and small teams who need secure communication, compartmentalization, and controlled collaboration without moving to irreversible wipe features.

5.6.3 What Does It Offer?

The Sovereign tier provides comprehensive security and privacy features, including: - **All Inheritance Tier Features**: Access keys, client-side encryption, post-quantum protection, LockoutGuard, LegacyLink, and single-region redundancy. - **Vault Messaging (Two-Way)**: Send and receive encrypted text, files, and requests with other Safes. - **Spaces**: Partition one Safe into isolated working areas with separate permissions. - **Shared Spaces**: Collaborate between separate Safes by sharing a Space instead of giving another Safe access to your whole Safe. - **DuressDecoy Access**: Use a safeword PIN to hide selected sensitive Spaces under coercion. - **Digital Paper Wallet Tools (CybVault DPW)**: Offline-like, air-gapped digital paper wallet generator for Bitcoin and Ethereum, producing secure QR codes for cold-like storage. - **5GB Base Storage**: Expandable at $1/GB/month, suitable for documents, Bitcoin and Ethereum keys, and backups. - **3 Included Access Keys (Expandable to 10)**: Starts with 3 keys and can be expanded for more people or more devices on the same Safe. - **Multi-Region Redundancy**: Safe data mirrored across separate global regions for enhanced resilience.

5.6.4 Why Is This Important?

The Sovereign tier is critical because it: - **Enables Safe Collaboration**: It covers both models, multiple access keys for the same Safe and Shared Spaces between separate Safes. - **Provides Coercion Resistance**: DuressDecoy hides selected sensitive Spaces under pressure instead of exposing them. - **Supports Bitcoin and Ethereum Operations**: CybVault DPW offers secure, offline-like Bitcoin and Ethereum digital paper wallet generation, protecting high-value assets without exposure. - **Scales Flexibly**: 5GB base storage and up to 10 access keys support growing operational needs without changing the Safe model.

5.6.5 How Does It Work?

- **Spaces**: Create isolated environments inside one Safe for projects, family data, or operational needs.
- **Shared Spaces**: Send a Shared Space invite through Vault Messaging so another Safe can collaborate without merging access to the full Safe.
- **DuressDecoy Access**: Mark selected Spaces as sensitive and configure a safeword PIN so those Spaces are hidden if the safeword PIN is used.
- **Vault Messaging**: Send and receive encrypted messages or files with other UnoLock users, including Shared Space invites.
- **Digital Paper Wallet Tools**: Generate offline-like digital paper wallets for Bitcoin and Ethereum using CybVault DPW. Export keys as QR codes for cold-like storage, securely stored within Spaces.
- **Storage**: 5GB base storage supports encrypted files, with real-time expansion at $1/GB/month for additional needs.
- **Access Keys**: Includes 3 access keys, expandable to 10 maximum, enabling multiple people or multiple devices to use the same Safe with their own key.
- **Redundancy and Encryption**: Data is encrypted client-side with post-quantum protection and mirrored across multiple regions for resilience.

5.6.6 Use Cases

- **Crypto Professionals**: Manage digital paper wallets, protect against coercion with DuressDecoy, and keep related documents in the same Safe.
- **Remote Teams**: Use Spaces for internal compartmentalization and Shared Spaces for collaboration between separate Safes.
- **Privacy Advocates**: Operate across devices or users with separate access keys while keeping a 5GB Safe under strong privacy controls.

5.7 HighRisk: Maximum Security Tier

5.7.1 Overview

The HighRisk tier is UnoLock’s most aggressive security tier. It is built for journalists, activists, whistleblowers, executives, and others who face serious coercion or seizure risk and who may need irreversible response options rather than merely hiding selected sensitive Spaces.

5.7.2 Who Is This For?

The HighRisk tier is designed for users whose threat model justifies permanent loss of data in exchange for stronger coercion response. It is not simply a bigger Sovereign plan; it is a different operational choice.

5.7.3 What Does It Offer?

The HighRisk tier provides maximum security features, including: - **All Sovereign Tier Features**: Access keys, client-side encryption, post-quantum protection, Spaces, Shared Spaces, Vault Messaging, DPW tools, and multi-region redundancy. - **Plausible Deniability (Safeword Wipe)**: Enter a secret Safeword PIN to delete Spaces that were marked as sensitive. - **5GB Base Storage**: Expandable at $1/GB/month, suitable for sensitive documents, Bitcoin and Ethereum keys, and backups. - **3 Included Access Keys (Expandable to 10)**: Starts with 3 keys and can be expanded if multiple people or multiple devices still need access to the same Safe.

5.7.4 Why Is This Important?

The HighRisk tier is critical because it: - **Delivers Irreversible Protection**: Plausible Deniability with Safeword Wipe deletes selected sensitive Spaces under coercion. - **Empowers High-Risk Users**: Offers unmatched security for journalists, activists, and executives, addressing extreme threats where data exposure could be catastrophic. - **Maintains Operational Flexibility**: Keeps Spaces, Shared Spaces, messaging, and DPW tools available even in the highest-risk tier. - **Aligns with Digital Sovereignty**: Gives the user final control over whether selected sensitive Spaces survive a coercive event.

5.7.5 How Does It Work?

- **Plausible Deniability (Safeword Wipe)**: Mark selected Spaces as sensitive and set a Safeword PIN in advance. If that PIN is entered, those sensitive Spaces are deleted.
- **Spaces**: Create isolated environments for sensitive data, each with separate keyrings and permissions (Read-Only or Admin), allowing compartmentalization of investigative files or corporate secrets.
- **Shared Spaces**: Continue to collaborate between separate Safes where needed, while still preserving the HighRisk coercion model for your own Safe.
- **Vault Messaging**: Send and receive encrypted text, files, requests, and Shared Space invites with other Safes.
- **Digital Paper Wallet Tools**: Generate offline-like digital paper wallets for Bitcoin and Ethereum using CybVault DPW, exporting keys as QR codes for cold-like storage within secure Spaces.
- **Storage**: 5GB base storage supports encrypted files, with real-time expansion at $1/GB/month for additional needs.
- **Access Keys**: Includes 3 access keys, expandable to 10 maximum, enabling multi-device or trusted-party access where appropriate.
- **Redundancy and Encryption**: Data is encrypted client-side with post-quantum protection and mirrored across multiple regions for resilience.

5.7.6 Use Cases

- **Investigative Journalists**: Securely store sensitive sources, research, or media files in a 5GB Safe and delete marked sensitive Spaces if coerced.

- **Activists and Whistleblowers**: Safeguard life-critical records in hostile environments with Safeword Wipe, ensuring no data remains under threat, while using Spaces to separate personal and organizational data across up to 10 keys.
- **Executives**: Protect trade secrets or financial data with post-quantum encryption and multi-region redundancy, using Plausible Deniability to eliminate leaks during corporate espionage, supported by Two-Way Vault Messaging for secure coordination.
- **Crypto Custodians**: Manage high-value cryptocurrency portfolios with CybVault DPW, storing keys in a 5GB Safe and erasing them permanently under duress if that matches the threat model.

5.8 Sovereign vs. HighRisk: A Critical Comparison

5.8.1 Overview

Both the Sovereign and HighRisk tiers offer advanced security, multiple access keys, Spaces, and strong coercion-resistance features. The critical difference is what happens to Spaces that the user has marked as sensitive when a safeword PIN is used: Sovereign hides them, while HighRisk deletes them.

5.8.2 Sovereign: DuressDecoy Mode

- **How It Works**: Sovereign users mark selected Spaces as sensitive and set a safeword PIN. If that PIN is entered, the sensitive Spaces are hidden.
- **Ideal Use Cases**:
- Crypto investors managing significant assets, needing to protect seed phrases without risking permanent loss.
- Professionals handling proprietary data, such as business contracts or client records, where data must remain accessible post-coercion.
- Teams or families requiring the same Safe to remain recoverable after a coercive event.
- **Key Benefit**: Sensitive Spaces are concealed without deleting them.
- **Reversibility**: The Spaces are hidden rather than deleted.

5.8.3 HighRisk: Plausible Deniability (Safeword Wipe)

- **How It Works**: HighRisk users mark selected Spaces as sensitive and set a safeword PIN. If that PIN is entered, the sensitive Spaces are deleted.
- **Ideal Use Cases**:
- Investigative journalists protecting confidential sources or research, where exposure could endanger lives.
- Activists or whistleblowers in hostile regimes, needing to eliminate data to avoid persecution.
- Executives safeguarding trade secrets or financial data, where leaks could cause irreparable harm.
- **Key Benefit**: Eliminates the selected sensitive Spaces rather than merely hiding them.
- **Reversibility**: No, deletion of the marked sensitive Spaces is the HighRisk tradeoff.

5.8.4 Crucial Difference: Hidden vs. Destroyed Data

The fundamental distinction between Sovereign and HighRisk lies in their approach to Spaces marked as sensitive: - **Sovereign**: Hides those Spaces. - **HighRisk**: Deletes those Spaces.

This difference reflects two philosophies of survival: Sovereign prioritizes preservation, while HighRisk prioritizes deletion of the marked sensitive Spaces. Choosing the wrong tier could result in either unnecessary data loss or insufficient protection.

5.8.5 Scenarios Where Plausible Deniability May Not Be Suitable

HighRisk’s irreversible deletion behavior is powerful but risky in certain contexts: - **Crypto Users**: If a sensitive Space contains the only copy of a Bitcoin or Ethereum seed phrase, marking it for deletion may be too dangerous. - **Families or Teams**: Spaces storing important shared records may need to remain recoverable. - **Ongoing Projects**: Professionals or teams relying on continued access may find deletion too disruptive.

In these cases, Sovereign’s DuressDecoy offers protection without the same deletion risk.

5.8.6 Who Should Use HighRisk?

The HighRisk tier is intended for users facing extreme threats where data exposure could lead to catastrophic consequences: - **Journalists and Whistleblowers**: Those handling sensitive information that could endanger lives or reputations if exposed, requiring the ability to erase data permanently. - **Activists in Hostile Environments**: Individuals operating under authoritarian regimes or surveillance, where data seizure could lead to persecution. - **Executives with Critical Secrets**: Professionals whose businesses could face irreparable harm from leaked trade secrets or financial data, needing a fail-safe deletion mechanism.

HighRisk's Plausible Deniability ensures that selected sensitive Spaces are deleted, but users must be prepared for that permanent loss.

5.8.7 The Responsibility of the User

HighRisk's Plausible Deniability with Safeword Wipe is irreversible for the Spaces that are marked as sensitive. Users must carefully consider: - **Data Criticality**: Ensure only data that can be sacrificed is marked for deletion, or maintain external backups for essential records. - **Backup Strategy**: Critical data, such as cryptocurrency seed phrases or legal documents, should be backed up outside UnoLock if their Space is marked as sensitive. - **Threat Assessment**: Evaluate whether deletion aligns with your threat model, as accidental or coerced use of the safeword PIN removes the marked Spaces without recourse.

Choosing HighRisk requires a clear understanding of these risks, because the responsibility for deletion of marked sensitive Spaces sits with the user.

5.8.8 Conclusion: Choose Wisely

The Sovereign and HighRisk tiers both serve advanced users, but they solve different problems. Sovereign is for hiding marked sensitive Spaces. HighRisk is for deleting them. Both support 5GB storage (expandable at $1/GB/month) and up to 10 access keys (3 included).

Users must weigh their risk tolerance and data criticality when choosing. Sovereign preserves the marked Spaces by hiding them. HighRisk accepts permanent deletion of the marked Spaces to eliminate later exposure.

5.8.9 Summary Table

Feature	Sovereign (DuressDecoy)	HighRisk (Plausible Deniability)
Price (Monthly)	$8	$14
Price (Yearly)	$86.40 (10% discount)	$151.20 (10% discount)
Storage	5GB (expandable at $1/GB/month)	5GB (expandable at $1/GB/month)
Access Keys (Included/ Max)	3 included, up to 10	3 included, up to 10
Sensitive Space Status	Hidden	Deleted
Safe Behavior	Safe opens without sensitive Spaces shown	Safe opens after sensitive Spaces are deleted
Trigger	Safeword PIN	Safeword PIN

6. Howto

6.1 Tutorials Section Overview

6.1.1 Overview

Welcome to the UnoLock Howto section. These tutorials walk through the main customer workflows, from creating a Safe and registering access keys to working with Spaces, Shared Spaces, recovery options, and higher-tier security features.

6.1.2 List of Tutorials

- Safe Creation: Set up your first UnoLock Safe and first access key.
- Create First Record: Add and manage your first note in the Safe.
- More Record Functions: Explore additional actions for managing Safe records.
- Changing Your PIN: Update your Safe access PIN.
- Local File Encryption: Encrypt and decrypt files in the Free tier.
- Installation and Data Shield: Install the UnoLock app and enable DataShield.
- Upgrade Safe: Upgrade your Safe from the Free tier to a higher tier.
- Managing Subscriptions: Cancel your subscription payment.
- Downgrading Safe: Prepare for a Safe-tier downgrade.
- Uploading Files to the Cloud: Upload encrypted files to multi-region redundancy.
- LockoutGuard Setup: Configure LockoutGuard to protect your Safe after inactivity.
- Setting Up LegacyLink: Configure LegacyLink for emergency access by a trusted person.
- Gaining Access with LockoutGuard: Recover your Safe using LockoutGuard credentials.
- Gaining Access with LegacyLink: Access and recover a Safe using LegacyLink credentials.
- Using Duress Decoy Mode: Set up Duress Decoy to protect data under coercion.
- Plausible Deniability Setup: Configure Plausible Deniability to delete sensitive data.
- Wallet Setup: Create a digital paper wallet for cryptocurrencies or tokens.
- Register Another Access Key for the Same Safe: Register another person or device for the same Safe.
- Creating Spaces in Your Safe: Create and manage Spaces to organize data.
- Granting an Access Key Access to Spaces: Give another access key permission to selected Spaces or full Safe administration.
- Sharing a Space Between Safes: Collaborate in a Shared Space between separate Safes.
- Deleting a Safe: Permanently delete your UnoLock Safe.

6.1.3 FAQ

How do I get started with UnoLock?

Begin with the Safe Creation tutorial to set up your first Safe. From there, explore tutorials like Create First Record to start adding data securely.

Why can’t I find some features in my UnoLock app?

Some features, such as Spaces, Shared Spaces, Duress Decoy, and Plausible Deniability, are available only in specific tiers. Check the Upgrade Safe tutorial to upgrade your tier if needed.

What if the app’s interface doesn’t match the tutorial instructions?

UnoLock’s UI may change with updates. If buttons or options differ, look for similar labels or functions, and ensure your app is updated to the latest version.

6.1.4 Get Started

Start with the Safe Creation tutorial to set up your Safe and begin securing your sensitive data.

6.2 Safe Creation

6.2.1 Overview

This guide explains how to create and configure a UnoLock Safe using the Progressive Web App (PWA). A Safe is cloud-based, but access is controlled by registered access keys such as passkeys, hardware keys, or compatible device authenticators.

6.2.2 Prerequisites

- A supported device (e.g., smartphone, tablet, or computer) with the UnoLock PWA installed or accessible via a modern browser.
- A stable internet connection.
- Familiarity with your device's authentication methods (for example, fingerprint, facial recognition, a platform passkey, or a FIDO2-compatible hardware key).

6.2.3 Create a New Safe

1. Open the UnoLock PWA and go to the home page.
2. Select the option to create a new Safe.
3. If **Create Safe** is not visible, check the main menu for the equivalent option and ensure the app is updated.

6.2.4 Accept Terms and Conditions

1. Review the terms and conditions displayed on the welcome screen.
2. Read the terms carefully and click **Accept Terms** or the equivalent button to proceed.

6.2.5 Configure Safe Security

1. Choose a security method:
2. **Current Device**: Use the device you are on to register the first access key for this Safe.
3. **Another Device**: Register the first access key from another device if that better matches your workflow.
4. Enter a unique, memorable name for your Safe.
5. Click **Next** to continue.
6. Complete the WebAuthn prompt shown by the device or browser.

6.2.6 Set Up PIN Security

1. Read the information about PIN security to understand its role in brute-force protection and, where applicable, deniability workflows.
2. Acknowledge the information as prompted.
3. Choose a strong personal identification number (PIN), avoiding repetitive or predictable numbers.
4. Confirm the PIN if the app asks you to do so.

6.2.7 Test Your Login Credentials

1. Authenticate using your device's standard method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).
2. Select your Safe's name from the list of available Safes.
3. Enter the PIN you set in the previous step to confirm access.
4. If the interface differs, follow the current prompts to verify that both the access key and PIN are working.

6.2.8 Choose Data Storage Location

1. Select your preferred storage option:
2. **Single Region** (Free and Inheritance tiers): Choose one region to comply with local data regulations.
3. **Multi-Region Redundancy** (Sovereign and HighRisk tiers): Opt for multiple regions for enhanced reliability.
4. Click **Next** or **Confirm** to finalize your selection.
5. If the option names differ slightly in the current UI, select the storage layout that matches your tier.

6.2.9 Explore Your Safe

1. Open your newly created Safe in the Free tier or the tier you selected.
2. Explore the interface for notes, files, Spaces, and other tools available in your tier.
3. Consider upgrading later if you need more storage, more access keys, Shared Spaces, or higher-risk security features.

6.2.10 Next

Next: Create First Record

6.3 Create First Record

6.3.1 Overview

This guide provides step-by-step instructions for accessing your secure UnoLock vault, creating and managing notes, and securely logging out. Follow these steps to organize and protect your critical data effectively.

6.3.2 Prerequisites

- A configured secure UnoLock vault (see the "Safe Creation" guide for setup instructions).
- A supported device with the UnoLock PWA installed or accessible via a modern browser.
- Your access key name and secure PIN, set during vault creation.
- Familiarity with your device’s authentication methods (e.g., fingerprint, facial recognition, or FIDO2-compatible hardware key).

6.3.3 Access Your Vault

1. Launch the UnoLock PWA on your device.
2. Authenticate using your device’s standard method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).
3. Note: If the authentication method label differs (e.g., “Device Authentication”), verify the terminology in the current UI.
4. Choose your vault’s access key name from the list of available keys.
5. Recommendation: A screenshot of the access key selection screen would clarify this step, especially if multiple keys are listed.
6. Input the secure PIN you set during vault setup.
7. Note: The PIN may be referred to as a “secure PIN” in the app. Confirm the correct term in the current UI.

6.3.4 Create a New Note

1. Inside your vault, locate and click the **New Note** button.
2. Note: If the “New Note” button is not visible, check for alternative labels like “Add Record” or “Create Note” in the current UI.
3. Enter a meaningful title for your note (e.g., “Meeting Notes” or “Password List”).
4. Ensure the title is descriptive to facilitate future retrieval.
5. Populate the text area with your critical data or notes (e.g., text, lists, or other information).
6. Click **Save** to securely store the note in your vault.
7. Recommendation: A screenshot of the note creation interface, showing the title field, text area, and “Save” button, would enhance clarity.

6.3.5 Manage Saved Notes

1. Access management options via the note’s interface or an associated menu (e.g., a “More Options” menu).
2. Pin the note by selecting the **Pin** option to keep it easily accessible at the top of your vault’s list (useful for frequently accessed records).
3. Customize the background by selecting the **Customize Background** option (or similar, e.g., “Change Theme”) and choosing a color (e.g., blue for work notes, green for personal).
4. Note: If background customization is unavailable, verify the current UI.
5. Access additional options by clicking the “More Options” menu (often represented by three dots) on the note:
6. **Delete**: Remove the note if no longer needed, confirming deletion to avoid accidental data loss.
7. **Lock for Immutability**: Lock the note to prevent further edits, preserving its integrity (ensure no further edits are needed before locking).

8. **Add Files**: Attach files (e.g., documents, images) by selecting a file from your device and confirming the upload.
9. **Assign a Label**: Categorize the note with a label (e.g., “Work,” “Personal”) by entering or selecting a label as prompted.
10. Recommendation: A screenshot of the “More Options” menu with all options visible would help users locate these features.
11. Note: The term “ellipses menu” may be outdated and could now be labeled as “More Options” or “Actions.” Confirm the current menu name.

6.3.6 Exit the Vault

1. Find the lock symbol in the top right corner of the vault interface.
2. Note: If the lock symbol is not visible or has been replaced (e.g., with a “Log Out” button), check the current UI for the logout option.
3. Click the lock symbol.
4. Select **Exit Now** to securely log out of your vault.
5. Recommendation: A screenshot highlighting the lock symbol and “Exit Now” option would clarify this step.

6.3.7 Next

Next: More Record Functions

6.4 More Record Functions

6.4.1 Overview

This guide provides step-by-step instructions for performing additional actions on records in your UnoLock vault, including hiding the note body, deleting a record, locking and unlocking a record, adding a file attachment, and assigning a label.

6.4.2 Hide the Note Body

1. Navigate to the **Configuration** section in the left-hand menu.
2. Select **Options**.
3. Check the box labeled **Hide Note Body**.
4. Click **Save** to apply the setting.
5. Note: With this option enabled, only the title of your records will be visible, enhancing their security.

6.4.3 Delete a Record

1. Locate the record you want to delete.
2. Click the **More Options** menu on the record.
3. Select **Delete**.
4. Confirm the prompt to permanently delete the record from your vault.

6.4.4 Lock a Record

1. Locate the record you want to protect.
2. Click the **More Options** menu on the record.
3. Select **Lock**.
4. Note: Once locked, the record cannot be modified or deleted until it is manually unlocked.

6.4.5 Unlock a Record

1. Open the locked record.
2. Click the **More Options** menu within the note.
3. Select **Unlock**.
4. Note: You may need to click a button on the left-hand side of the screen to initiate unlocking, depending on the interface.

6.4.6 Add a File Attachment

1. Locate the record you want to attach a file to.
2. Click the **More Options** menu on the record.
3. Select **File**.
4. Choose whether the file is already in the app or is new by selecting the appropriate option.
5. Confirm your selection to attach the file to the record.
6. Note: The file will appear as an attachment for future access. Free tier users may face storage limits (1MB).

6.4.7 Add a Label

1. Locate the record you want to categorize.

2. Click the **More Options** menu on the record.
3. Select **Label**.
4. Enter your desired label name.
5. Click **Save** to save the label.
6. Note: The label will appear as a menu item in the left-hand menu, allowing you to categorize and organize your notes.

6.4.8 Next

Next: Changing Your PIN

6.5 Changing Your PIN

6.5.1 Overview

This guide explains how to update the access PIN for your UnoLock Safe. The PIN is a separate security control used alongside your WebAuthn access key.

6.5.2 Access the Configuration Menu

1. Open your UnoLock Safe.
2. From the main left-hand menu, select the **Configuration** menu item.

6.5.3 Set a New PIN

1. In the Configuration section, click the **Set Access PIN** menu item.
2. Enter your desired new PIN.
3. Confirm the new PIN by clicking **Next**.

6.5.4 Authenticate with the New PIN

1. Wait for a success window to appear, prompting you to authenticate again using the new PIN.
2. Enter the new PIN to authenticate.
3. Note: If the authentication fails, the PIN change will not proceed, and your current PIN will remain unchanged.

6.5.5 Confirm the PIN Update

1. Navigate to the Safe access screen.
2. Click **Open**.
3. Complete the authentication using your device’s standard method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).
4. Enter your new access PIN to confirm the update.

6.5.6 Next

Next: Local File Encryption

6.6 Local File Encryption

6.6.1 Overview

This guide provides step-by-step instructions for securely adding, encrypting, and decrypting files in the Free tier of your UnoLock vault.

6.6.2 Access the Files Menu

1. Open your UnoLock vault.
2. Navigate to the **Files** section on the left-hand side of the main menu.

6.6.3 Add Files to Your Vault

1. In the Files section, choose one of the following methods to add files:
2. Drag and drop your files into the drag-and-drop area.
3. Select files from your device.
4. Review the informational window explaining the encryption process.
5. Click **OK** to begin the encryption process.

6.6.4 Encrypt the File

1. Wait for a file selection prompt to load, allowing you to select the file.
2. Select the file and click **Start** to encrypt it directly on your device.
3. After encryption, the file will be downloaded to your device with a .ulef extension (indicating a UnoLock encrypted file).
4. Click **Done** to complete the process.
5. Note: The encrypted file will appear in the list of files with a symbol indicating it is stored locally as an encrypted file.

6.6.5 Decrypt a .ulef File

1. To decrypt a .ulef file stored on your device, either:
2. Click **Open Local** and select a local file.
3. Select the file from the list in the Files section.
4. Upload the corresponding .ulef file into the app when prompted.
5. Once decrypted, choose one of the following options:
6. Download the file unencrypted.
7. View the file directly within the app for maximum security (if it’s a supported file type).

6.6.6 Next

Next: Installation and Data Shield

6.7 Installation and Data Shield

6.7.1 Overview

This guide provides step-by-step instructions for installing the UnoLock Progressive Web App (PWA) on your device and using the DataShield feature to protect your vault’s contents from unwanted modifications.

6.7.2 Install the UnoLock App

1. Open the UnoLock PWA and navigate to the **Configuration** section in the left-hand navigation.
2. Click the **Install** option.
3. When prompted for confirmation, select **Yes**.
4. Note: The app will install on your device, allowing you to access UnoLock like a native app for convenience.

6.7.3 Enable DataShield

1. Navigate to the **Configuration** section in the left-hand navigation.
2. Select **Enable DataShield**.
3. When prompted, click **Yes** to activate the feature.
4. Note: A lock symbol will appear on all items within your vault, indicating that they are now protected and cannot be edited or deleted.

6.7.4 Disable DataShield

1. Navigate to the **Configuration** section in the left-hand navigation.
2. Select **Disable DataShield**.
3. When prompted, click **Yes**.
4. Note: Your vault’s contents will return to their standard state, allowing for modifications and deletions as needed.

6.7.5 Next

Next: Upgrade Safe

6.8 Upgrade Safe

6.8.1 Overview

This guide explains how to upgrade your UnoLock Safe from the Free tier to a higher tier.

6.8.2 Access Upgrade Options

1. Navigate to the main menu in the UnoLock app.
2. Select **Upgrade Safe**.
3. Review the information window explaining the upgrade process.
4. Click **Next** to proceed.

6.8.3 Select an Upgrade Tier

1. Review the available upgrade tiers displayed on the screen.
2. Select the tier you wish to upgrade to.
3. Read the pricing notice and any warnings shown by the app.
4. Click **OK** to continue, or select **Cancel** if you do not wish to proceed.

6.8.4 Initiate the Payment Process

1. After confirming the upgrade, wait for the app to redirect you to the payment system.
2. Click **Next** to begin the payment process.
3. If you have a promo code, enter it now; otherwise, click **Continue** to proceed.

6.8.5 Choose a Payment Method

1. Review the information screen outlining the two payment methods:
2. **Credits**: One-off purchases for specific durations.
3. **Subscribe**: Automated payments for continuous paid-tier service without manual renewals.
4. Depending on your selection:
5. For one-off credit purchases, use the slider to select the number of months to prepay.
6. For a subscription, enable automatic payments via the Stripe payment flow.

6.8.6 Complete the Payment

1. Click **Purchase**.
2. Select your payment method:
3. **Bitcoin** for cryptocurrency transactions.
4. **Credit card** via the Stripe payment processor.
5. Click **Continue** and confirm your payment details.
6. For credit card payments, enter your card information and press **Pay**.
7. Once payment is completed, choose to view the receipt or return to your Safe.
8. Note: Your Safe may automatically relock so the upgrade or credits can be applied cleanly.

6.8.7 Next

Next: Managing Subscriptions

6.9 Managing Subscriptions

6.9.1 Overview

This guide provides step-by-step instructions for canceling your subscription payment in the UnoLock app.

6.9.2 Access Subscription Management

1. Navigate to the main menu in the UnoLock app.
2. Select **Configuration**.
3. Click the subscription management option to access the settings.

6.9.3 Review Subscription Information

1. Read the informational dialog that appears, providing details about the subscription process.
2. Click **Next** to proceed.

6.9.4 Navigate to the Payment Gateway

1. Wait for the app to redirect you to the Payment Gateway.
2. Click **Continue** to move forward.

6.9.5 Cancel the Subscription

1. On the Payment Gateway page, review the details displayed.
2. Click **Manage Subscription**.
3. Within the Stripe Payment Gateway, click **Cancel Subscription**.
4. When a confirmation message appears, click **Cancel Subscription** again to finalize the cancellation.

6.9.6 Provide Feedback (Optional)

1. If prompted, provide feedback regarding your decision to cancel, if required.
2. Choose to complete the feedback, delete your request, or proceed without providing feedback.

6.9.7 Next

Next: Downgrading Safe

6.10 Downgrading Safe

6.10.1 Overview

This guide explains how to prepare for a UnoLock Safe-tier downgrade, including backing up data, deleting the current Safe, creating a new Safe with the same credentials, and applying any promotional credit from the old plan.

6.10.2 Back Up All Safe Data

1. Review every Space within your Safe, checking for records, notes, files, and cryptocurrency wallets.
2. Examine all notes stored in each Space.
3. Decrypt and download locally encrypted files to your device.
4. Download cloud-stored files to your device.
5. Back up all cryptocurrency wallets by securely saving your private keys or mnemonics.
6. Navigate through each Space individually to locate and back up all data, ensuring no files, records, or wallets are overlooked.
7. Store your backups in a secure location.
8. Double-check every Space, record, and file to confirm all data is backed up.
9. Note: Due to UnoLock's client-side encryption, the app cannot automatically back up or export your Safe. All data will be permanently deleted during the downgrade process, so this step is critical.

6.10.3 Delete Your Safe

1. From the main menu, go to **Configuration**.
2. Select **Options**.
3. Click the **Delete Safe and All Data** button.
4. Read the warning message explaining that this action is permanent and non-recoverable.
5. Click **Delete** to proceed.
6. Type the word **Regret** into the provided field to confirm your decision.
7. Click **Next** to permanently delete your Safe.
8. Copy the promotional code displayed on the screen for reimbursing unspent credits.
9. Save the promotional code for future use.
10. Click **Next** to return to the Home screen.
11. Note: Deleting your Safe is irreversible, and all data will be lost permanently.

6.10.4 Create a New Safe with Old Credentials

1. Navigate to the UnoLock Home screen.
2. Click to access the Safe.
3. Select the access key associated with your previous Safe from the list.
4. Authenticate using your device's usual method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).
5. When a screen appears stating that the Safe associated with the credential cannot be found, choose **Yes** to associate the credential with a new Safe.
6. Re-authenticate using the old Safe credentials when prompted.
7. Enter your original Safe name for continuity, if desired.
8. Click **Next** to proceed.
9. Read and acknowledge the information about PIN security.

10. Choose a secure personal identification number (PIN) for your new Safe.
11. Test your login credentials:
    - Respond to the authentication prompt using your device's usual method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).
    - Select your Safe's name from the list.
    - Enter your UnoLock PIN.
12. Choose single-region storage to comply with local regulations.

6.10.5 Upgrade the New Safe with Promotional Credits

1. Navigate to the main menu and select **Upgrade Safe**.
2. Review the information window explaining the upgrade process.
3. Click **Next** to proceed.
4. Review the available upgrade tiers displayed.
5. Select the tier you wish to upgrade to.
6. Read the pricing notice and any warnings shown by the app.
7. Click **OK** to continue, or select **Cancel** if you do not wish to proceed.
8. Wait for the app to redirect you to the payment system.
9. Click **Next** to begin the payment process.
10. Click **Use Promo Code** to enter the promotional code saved after deleting the old Safe.
11. Click **Submit**.
12. Verify the message indicating that the code has been applied to the Safe.
13. Click **Return to Safe** to go to the Safe access screen.
14. Enter the Safe to access your newly upgraded tier with the promotional credits applied.

6.10.6 Next

Next: Uploading Files to the Cloud

6.11 Uploading Files to the Cloud

6.11.1 Overview

This guide provides step-by-step instructions for uploading encrypted files to multi-region redundancy in the UnoLock app after upgrading to the Inheritance, Sovereign, or HighRisk tier, and accessing those files.

6.11.2 Access the Files Menu

1. Upgrade your UnoLock vault to the Inheritance, Sovereign, or HighRisk tier.
2. Navigate to the **Files** section in the main menu.

6.11.3 Upload Files

1. Choose one of the following methods to upload files:
2. Drag and drop multiple files into the designated upload area.
3. Click to select a file from your device.
4. After selecting your file, review the dialog box that appears, asking where you want to store it.
5. Select the **Cloud** option for multi-region redundancy.
6. Note: Selecting **Local** will keep the encrypted file on your device.

6.11.4 Confirm and Upload

1. Review the confirmation dialog showing the file details.
2. Rename the file if necessary.
3. Click **Upload**.
4. Wait for a message confirming that the file has been successfully uploaded.
5. Note: The file will appear in your file list, indicated by a cloud icon, distinguishing it from locally stored encrypted files.

6.11.5 Access a Cloud-Stored File

1. Locate the file in the file list and click on its name.
2. Choose one of the following options:
3. Click **Download** to retrieve a copy of the file.
4. Click **View** to securely open the file directly within the app for maximum security.

6.11.6 Next

Next: LockoutGuard Setup

6.12 LockoutGuard Setup

6.12.1 Overview

This guide explains how to set up and configure LockoutGuard for your UnoLock Safe.

6.12.2 Access Lockout Guard Settings

1. From the main menu, select **Configuration**.
2. Navigate to the Lockout Guard configuration.
3. Read the information prompt carefully.
4. Click **Next** to proceed.

6.12.3 Set a PIN for Lockout Guard

1. Respond to the prompt asking whether the PIN should match your current PIN or be different.
2. Choose **Yes** (to match) or **No** (to use a different PIN) based on your preference.

6.12.4 Enable Notifications

1. Review the notification prompt asking if notifications should be enabled on your device.
2. If you choose to enable notifications (recommended), follow the on-screen prompts to allow them on your device.
3. Wait for a confirmation prompt indicating that notifications have been set.
4. Click **Next** to continue.
5. Note: Enabling notifications is optional but highly recommended for Lockout Guard to function effectively.

6.12.5 Set the Minimum Safe Access Interval

1. Choose the minimum Safe access interval, which defines the period of inactivity after which LockoutGuard will trigger.
2. Click **Next**.

6.12.6 Specify the Warning Period

1. Set the number of days for LockoutGuard to send warning notifications before fully activating.
2. Click **Next**.

6.12.7 Authenticate and Store Credentials

1. Authenticate using your device’s usual method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).
2. Review the QR code and Lockout Guard credential displayed.
3. Print, save, or securely store the QR code and credential.
4. Note: These are critical for recovering your Safe if LockoutGuard is triggered.
5. Click **Done** once the QR code and credential are securely stored.

6.12.8 Confirm Lockout Guard Activation

1. Review the confirmation prompt indicating that Lockout Guard is active.
2. Wait for a test notification to be sent to verify functionality.
3. Click **Close** to exit the Lockout Guard window.

6.12.9 Update Lockout Guard Settings (Optional)

1. To change Lockout Guard settings in the future, navigate back to the Lockout Guard configuration.
2. Click **Generate New QR Code** to update the guard settings and credentials.
3. Securely store the new QR code and credentials.

6.12.10 Ensure Safe Expiry Alignment

1. Verify that your Safe’s expiry date does not fall within the LockoutGuard trigger time frame.
2. Extend your Safe lifetime as needed to maintain proper functionality.

6.12.11 Next

Next: Setting Up LegacyLink

6.13 Setting Up LegacyLink

6.13.1 Overview

This guide explains how to configure LegacyLink for your UnoLock Safe. LegacyLink is available on the Inheritance, Sovereign, and HighRisk tiers and is designed as a one-time succession or recovery path, not as a permanent parallel login method.

6.13.2 Access Lockout Guard Settings

1. From the main menu, navigate to **Configuration**.
2. Select **Lockout Guard**.
3. Note: Ensure that Lockout Guard is enabled and your Safe lifetime is set to at least 31 days before proceeding.

6.13.3 Begin LegacyLink Setup

1. Click to start the LegacyLink setup process.

6.13.4 Set the Trigger Time

1. Use the slider to set the delay after Lockout Guard has been triggered for the LegacyLink feature.
2. Click **Next** to continue.

6.13.5 Reauthenticate

1. Reauthenticate using your device’s usual method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey).

6.13.6 Store the LegacyLink Credential

1. Review the screen displaying the following:
2. A QR code
3. An access ID
4. A passphrase
5. Note: This credential is dormant, does not require the current PIN, and can be used only if the LegacyLink conditions are triggered.
6. Save, print, or securely store the credential information in a safe location or provide it to a trusted person who may need to recover the Safe in an emergency.
7. Click **Done** to finalize this step.

6.13.7 Confirm LegacyLink Setup

1. Review the message confirming that the dormant credential has been created successfully.
2. Click **Next**.
3. Read the notice reminding you to keep the credential stored carefully.
4. Click **Next** to complete the LegacyLink configuration process.

6.13.8 Next

Next: Gaining Access with LockoutGuard

6.14 Gaining Access with LockoutGuard

6.14.1 Overview

This guide explains how to recover your UnoLock Safe using the saved Lockout Guard access ID and passphrase.

6.14.2 Retrieve Lockout Guard Credential

1. Retrieve your saved access ID and passphrase generated during Lockout Guard setup.

6.14.3 Initiate Recovery

1. Open the UnoLock app splash screen.
2. Start the recovery process.
3. Enter your access ID and click **Next**.
4. Input your passphrase when prompted and click **Next**.
5. Enter the PIN configured during Lockout Guard setup.
6. Click **Next** to proceed.

6.14.4 Register a New Key

1. Read the prompt asking you to register a new access key for the Safe carefully.
2. Click **Next**.
3. Enter a new name for your recovered key.
4. Note: Ensure the name differentiates it from your old key to avoid confusion.
5. Click **Next** after entering the key name.

6.14.5 Associate the Key with a Device

1. Decide which device the key will be associated with:
2. Select **This Device** to tie the key to your current device.
3. Choose **Another Device** based on your requirements.
4. For this example, select **This Device**.
5. Review the prompt confirming that the access key has been successfully registered.
6. Click **Next** to proceed.

6.14.6 Restart the App

1. Review the prompt advising that a restart of the app is required to activate the new access key.
2. Restart the UnoLock app.

6.14.7 Access the Safe with the New Key

1. Return to the UnoLock app splash screen.
2. Click to access the Safe.
3. Authenticate using the newly created key from Lockout Guard recovery.
4. Upon entering the Safe, review the message notifying you that the Lockout Guard credential used for recovery is now invalid.

6.14.8 Configure a New Lockout Guard Credential

1. Follow the Lockout Guard setup screens to configure a new credential based on your recovery needs.

6.14.9 Next

Next: Gaining Access with LegacyLink

6.15 Gaining Access with LegacyLink

6.15.1 Overview

This guide explains how to recover a UnoLock Safe using a LegacyLink credential and then register a new access key for ongoing use.

6.15.2 Retrieve LegacyLink Credential

1. Retrieve your saved access ID and passphrase generated during LegacyLink setup.

6.15.3 Initiate Recovery

1. Open the UnoLock app splash screen.
2. Start the recovery process.
3. Enter your access ID and click **Next**.
4. Input the corresponding passphrase when prompted and click **Next**.

6.15.4 Review Recovery Information

1. Read the informational screen detailing the process of taking custody of the Safe via the LegacyLink credential carefully.
2. Click **Next** to continue.

6.15.5 Register a New Key

1. Enter a name for your recovered access key when prompted.
2. Click **Next**.
3. Select the device to associate with the new access key:
4. Choose **This Device** to tie the key to your current device.
5. Select **Another Device** based on your needs.
6. For this example, select **This Device**.
7. Review the prompt confirming that the access key has been successfully registered.
8. Click **Next**.

6.15.6 Restart the App

1. Review the prompt advising that a restart of the app is required to activate the new access key.
2. Restart the UnoLock app.

6.15.7 Access the Safe with the New Key

1. Return to the UnoLock app splash screen.
2. Click to access the Safe.
3. Authenticate using the newly created access key from the LegacyLink recovery process.

6.15.8 Set a New PIN

1. Review the message prompting you to set a new PIN for the Safe.
2. Click **Yes** to begin the PIN setup process.

3. Review best practices for PIN creation and check the acknowledgement boxes.
4. Click **Next**.
5. Choose your new UnoLock PIN and click **Next**.
6. Authenticate using the new PIN to confirm it has been set successfully.

6.15.9 Verify Access with New Key and PIN

1. Return to the UnoLock app splash screen.
2. Click to access the Safe.
3. Authenticate using your recovered key name and the new PIN.
4. Upon entering the Safe, review the notification confirming that the old recovery credential is now invalid and that you should configure a fresh recovery option if needed.

6.15.10 Reconfigure Recovery Options

1. Set up Lockout Guard and LegacyLink again if you want to maintain recovery options for the Safe.

6.15.11 Next

Next: Using Duress Decoy Mode

6.16 Using Duress Decoy Mode

6.16.1 Overview

This guide provides step-by-step instructions for configuring the Duress Decoy feature for your UnoLock Safe to protect sensitive Spaces in situations of coercion. In the Duress Decoy model, entering the safeword PIN hides the Spaces that were marked as sensitive.

6.16.2 Access Duress Decoy Settings

1. Navigate to the main menu in the UnoLock app.
2. Select **Configuration**.
3. Click to access the Duress Decoy configuration.

6.16.3 Create a Safe Word PIN

1. Enter a safe word PIN in the provided prompt.
2. Note: This PIN is different from your normal access PIN and is used for the duress response.
3. Click **Next**.

6.16.4 Review Duress Decoy Information

1. Read the information screen about UnoLock spaces and how they relate to the Duress Decoy feature carefully.
2. Click **Yes** to proceed.

6.16.5 Confirm Duress Decoy Setup

1. Type **I am sure** into the provided field to confirm the setup of the Duress Decoy feature.
2. Click **Next**.

6.16.6 Select Spaces to Protect

1. Choose the space or spaces containing sensitive data you want to keep hidden.
2. If one of those spaces is a Shared Space, remember that Shared Space ownership rules still apply: owner-side deletion affects every participating Safe, while non-owner loss of access does not delete the data for other Safes.
3. Click **OK**.
4. Carefully review the selected spaces to ensure they contain the data you wish to protect.
5. Click **Next**.

6.16.7 Finish Setup

1. Review your selected sensitive Spaces carefully.
2. Complete the configuration flow.
3. Keep in mind that the safeword PIN acts on the Spaces you marked as sensitive.

6.16.8 Next

Next: Plausible Deniability Setup

6.17 Plausible Deniability Setup

6.17.1 Overview

This guide provides step-by-step instructions for setting up the Plausible Deniability feature in the UnoLock app, available exclusively on the HighRisk tier, to permanently delete sensitive data when a safe word PIN is used.

6.17.2 Access Plausible Deniability Settings

1. Navigate to the main menu in the UnoLock app.
2. Select **Configuration**.
3. Click to access the Plausible Deniability configuration.

6.17.3 Create a Safe Word PIN

1. Enter your desired safe word PIN in the provided prompt.
2. Note: This PIN will trigger the permanent deletion of sensitive data when used instead of your regular access PIN.
3. Click **Next**.

6.17.4 Review Plausible Deniability Information

1. Read the informational warning explaining how the Plausible Deniability feature works with UnoLock spaces carefully.
2. Click **Yes** to continue.

6.17.5 Select Sensitive Spaces for Deletion

1. Select the spaces containing sensitive data that you want to be permanently deleted if the safe word PIN is used.
2. Note: Be thorough and ensure all sensitive spaces are marked. Marked data will be irrecoverably deleted if the safeword PIN is used.
3. Note: If one of those spaces is a Shared Space, owner-side deletion affects every participating Safe, while non-owner loss of access does not delete the data for other Safes.
4. Click **OK** to complete the configuration.

6.17.6 Verify and Finalize Setup

1. Review the screen displaying the spaces marked as sensitive for deletion if Plausible Deniability is triggered.
2. Verify that all selections are correct.
3. Click **Next** to finalize the Plausible Deniability feature setup.
4. Note: This feature is designed for high-risk individuals who prefer to have sensitive data deleted rather than compromised in a hostile situation.

6.17.7 Next

Next: Wallet Setup

6.18 Wallet Setup

6.18.1 Overview

This guide provides step-by-step instructions for creating a digital paper wallet for cryptocurrencies or tokens in the UnoLock app.

6.18.2 Access the Wallet Section

1. From the main menu, navigate to the **Wallet** section.
2. Click to create a new wallet.

6.18.3 Select a Cryptocurrency or Token

1. Review the list of supported cryptocurrencies and tokens that appears.
2. Click on the coin or token you wish to create a wallet for.
3. Review the message confirming that a new crypto wallet has been created in the Wallet section and attached to a note.
4. Click **OK** to proceed.

6.18.4 Manage the Wallet Address

1. Review the wallet address window displaying your public key, which is the wallet address used for receiving funds.
2. To copy the wallet address, click the **Copy** icon.
3. To check the wallet's balance, click the **Balance** button.

6.18.5 Access the Private Key

1. Click **Show Private Key**.
2. Read the warning message carefully to understand the importance of keeping your private key secure.
3. Click **Show Private Key** to proceed.
4. Review the private key displayed as a QR code.
5. Use the **Copy** button to save the private key.
6. Alternatively, click **Mnemonic** to view the private key in a 24-word mnemonic format.
7. Note: The private key can be used to import the digital paper wallet into external wallets outside of the UnoLock app. Ensure it is securely stored to prevent unauthorized access.

6.18.6 Next

Next: Register Another Access Key for the Same Safe

6.19 Importing a Mnemonic with SeedSafe

6.19.1 Overview

This guide provides step-by-step instructions for importing an existing BIP-39 mnemonic seed phrase into your UnoLock vault using SeedSafe. SeedSafe provides military-grade protection for your recovery phrases through split-storage cryptography and zero-knowledge protocols, ensuring mathematical impossibility of seed phrase reconstruction without authenticated access to both encrypted halves.

6.19.2 Access the Wallet Section

1. From the main menu, navigate to the **Wallet** section in your selected Space.
2. Click the **Import** button in the wallet area.

6.19.3 Select Backup Seed Option

1. Click the **Backup Seed** option.
2. Choose the number of words your mnemonic contains from the available options.

6.19.4 Enter the First Half of the Mnemonic

1. Enter the first half of your mnemonic seed phrase in the field provided.
2. Click **Submit**.
3. Review the confirmation that shows your mnemonic and the number of words you selected appearing in the wallet area.

6.19.5 Enter the Second Half of the Mnemonic

1. Click **View** on the newly imported mnemonic entry.
2. When prompted, enter the second half of your seed phrase.
3. Follow the prompts to complete the second half entry.
4. Authenticate when requested using your configured authentication method.

6.19.6 Verify the Imported Mnemonic

1. Review the wallet now appearing in your crypto wallet area with a validated status.
2. Note: Each half of your mnemonic is independently encrypted using AES-256-GCM. The split-storage architecture ensures your seed phrase cannot be reconstructed without authenticated access to both encrypted halves, eliminating single points of failure while maintaining cloud resilience against physical loss.

6.19.7 Next

Next: Wallet Setup

6.20 Importing Digital Paper Wallet with DPW Portability

6.20.1 Overview

This guide provides step-by-step instructions for importing an existing UnoLock Digital Paper Wallet (DPW) into another Space or vault using DPW Portability. DPW Portability enables secure migration of Digital Paper Wallet mnemonics between Spaces and vaults while maintaining absolute zero-knowledge guarantees. Through authentication-bound encryption and opaque ciphertext migration, mnemonics remain cryptographically protected during transit with consent-enforced operations requiring explicit FIDO2/WebAuthn ceremonies. Perfect for inheritance planning, organizational distribution, and multi-jurisdiction redundancy.

6.20.2 Access the Wallet Import Function

1. Navigate to the **Wallet** area in your selected Space.
2. Click the **Import** button.
3. Review the menu that appears.

6.20.3 Select Import DPW Option

1. Click **Import DPW** from the menu options.
2. Select the cryptocurrency type (Bitcoin or Ethereum) for the DPW you are importing.

6.20.4 Enter the First Half of the Mnemonic

1. Paste the first half of the DPW seed phrase into the mnemonic fields.
2. Click **Submit**.
3. Review the confirmation that the first half has been added successfully.
4. Note: You will see the chosen crypto wallet appear in your wallet area.

6.20.5 Enter the Second Half of the Mnemonic

1. Click on the newly appearing wallet entry.
2. When prompted, enter the second half of the mnemonic.
3. Follow the authentication prompts to complete the process.

6.20.6 Complete the Import with Authentication

1. Authenticate when requested using your configured FIDO2/WebAuthn method.
2. Note: You will be asked to authenticate twice as the system securely pieces together the entire seed phrase for your newly imported DPW.
3. Review the confirmation that the DPW has been successfully imported and is now available in your wallet area.

6.20.7 Verify the Imported DPW

1. Review the imported Digital Paper Wallet now appearing in your crypto wallet area.
2. Click **Balance** to verify the wallet is functioning correctly.
3. Note: The mnemonic remains cryptographically protected throughout the entire migration process, with zero-knowledge guarantees maintained at every step.

6.20.8 Next

Next: Signing Transactions with DPW VaultSign

6.21 Signing Transactions with DPW VaultSign

6.21.1 Overview

This guide provides step-by-step instructions for securely signing and broadcasting cryptocurrency transactions using DPW VaultSign. DPW VaultSign implements an unbreachable transaction signing architecture with four-layer encryption, browser sandbox containment, and air-gapped broadcasting. Private keys exist only in volatile memory during millisecond signing windows, with immediate cryptographic erasure preventing persistent exposure. The air-gap design ensures that even with complete infrastructure compromise, attackers cannot autonomously broadcast transactions, requiring manual export for ultimate security.

6.21.2 Access Your Wallet

1. Navigate to the **Crypto Wallet** menu icon area.
2. Choose the wallet you want to use for the transaction.
3. Click on **Balance** to view your current wallet balance.

6.21.3 Initiate a Transaction

1. Review the balance displayed for your Bitcoin or Ethereum wallet.
2. Click the **Send** button to begin creating a transaction.

6.21.4 Enter Transaction Details

1. Enter the recipient's address in the **Destination Address** field.
2. Select the amount of BTC or ETH you want to send.
3. Note: Click **Max** to send the maximum available amount in your wallet.

6.21.5 Authenticate and Review

1. Authenticate when prompted using your configured authentication method.
2. Review the transaction details showing the amount you're sending and the available balance.
3. Click **Generate** to create the raw signed transaction.

6.21.6 Copy the Raw Signed Transaction

1. Review the raw signed transaction that has been generated.
2. Click **Copy Raw** to copy the raw signed transaction to your clipboard.
3. Note: The private key used for signing has already been cryptographically erased from memory at this point.

6.21.7 Broadcast via Blockchain Explorer

1. Navigate to your preferred blockchain explorer. Examples are listed in the information modal, such as:
2. Blockchain.com
3. Blockchair.com
4. Mempool.space
5. Locate the **Broadcast Transaction** or **Push Transaction** feature.
6. Click to import the raw transaction.
7. Paste the raw signed transaction from your clipboard.
8. Click **Broadcast** to submit the transaction to the network.

6.21.8 Verify Transaction Success

1. Review the confirmation message indicating whether the transaction broadcast was successful.
2. Use the transaction ID provided to track your transaction's progress on the block explorer.
3. Wait for network confirmations as the transaction is processed.
4. Note: It is advisable to use a VPN during this process for enhanced privacy.

6.21.9 Next

Next: Wallet Setup

6.22 Register Another Access Key for the Same Safe

6.22.1 Overview

This guide explains how to register another access key for the same UnoLock Safe. The new key can belong to another device or another person. After registration, that key can later be granted access to selected Spaces or full Safe administration.

6.22.2 Access Key Management

1. Navigate to the main menu in the UnoLock app.
2. Select **Configuration**.
3. Open the access key management settings.

6.22.3 View Current Key Properties

1. Click your current key to view its properties.
2. Review whether the key is enabled and whether it has admin rights.
3. Optionally, rename the key for clarity or organization.

6.22.4 Register a New Access Key

1. Click to create a new key.
2. Provide a name for the new key.
3. Click **Next**.
4. If prompted, choose whether the new key should use the same PIN flow as your current Safe access or a different PIN.
5. Re-authenticate using your current access key (for example, fingerprint, facial recognition, passkey, or hardware key).

6.22.5 Connect the New Access Key

1. Review the prompt informing you about QR code generation.
2. Click **Next** to continue.
3. Review the temporary QR code displayed, valid for 10 minutes.
4. Connect the new access key by either:
5. Scanning the QR code.
6. Entering the URL displayed with the QR code.
7. On the target device, complete the passkey or hardware-key registration flow shown by the app.
8. Once the new access key is successfully connected to your Safe, click **Done**.
9. Note: The new key will appear in your list of keys.

6.22.6 Review Permissions

1. Open the new key from the key list.
2. Review whether it should remain an admin key or have narrower permissions.
3. If this key should have access only to selected Spaces, use the Spaces access controls documented separately.

6.22.7 Delete a Key (Optional)

1. Select the key you wish to delete from the list of keys.

2. Uncheck the **Enable** checkbox.
3. Click **Delete**.
4. Confirm the deletion when prompted.
5. Note: The key will be removed from your list of keys.

6.22.8 Next

Next: Creating Spaces in Your Safe

6.23 Creating Spaces in Your Safe

6.23.1 Overview

This guide provides step-by-step instructions for creating and managing Spaces in your UnoLock Safe to organize and separate data. Spaces are available in tiers that support same-Safe compartmentalization.

6.23.2 Access Manage Spaces

1. Navigate to the main menu in the UnoLock app.
2. Select **Configuration**.
3. Click to access space management settings.
4. Review the Spaces currently available in your Safe.

6.23.3 Rename a Space

1. Go to the Notes section of your vault.
2. Locate the available spaces at the bottom of the screen.
3. Type a new name into the field to rename a space.
4. Use the right arrow to navigate to the next default space and rename it as needed.

6.23.4 Create a New Space

1. Click the plus icon in the space management or Notes section to create a new space.
2. Note: This is useful for categorizing vault data into separate compartments.

6.23.5 Add Content to the Space

1. Open the Space you want to use.
2. Return to the Notes section.
3. Create a new note.
4. Add the records, files, or other content you want to keep in that Space.
5. Repeat this process for any additional Spaces you want to organize.

6.23.6 Next

Next: Granting an Access Key Access to Spaces

6.24 Sharing a Space Between Safes

6.24.1 Overview

This guide explains how to use **Shared Spaces** for collaboration between **separate Safes**. If your goal is to let another person use their own access key, such as a passkey or hardware-backed key, to access selected Spaces inside the **same Safe** or to have full administrative rights to that Safe, use **Granting an Access Key Access to Spaces in the Same Safe** instead.

6.24.2 Before You Start

- You need a Safe that supports Spaces and Vault Messaging.
- The recipient must also have their **own Safe**.
- You need the recipient's **Vault Messaging address**.
- The Space you want to share must be created as a **Shared Space**.

6.24.3 Step 1. Create a Shared Space

1. Open the **Notes** area in your Safe.
2. Use the **plus icon** to create a new Space.
3. Enter a name for the Space.
4. When prompted for the Space type, choose **Shared**.
5. Open the new Shared Space and confirm it appears as a collaboration Space.

6.24.4 Step 2. Prepare the Shared Space

1. Add any starting notes or cloud files you want collaborators to see.
2. Keep in mind that Shared Spaces are intended for shared records and cloud-stored files.
3. Do not expect wallet features or local-only file storage inside the Shared Space.

6.24.5 Step 3. Send the Shared Space Invite

1. Open **Vault Messaging**.
2. Start a new message to the recipient's address.
3. Click **Share Space**.
4. Select the Shared Space you want to send.
5. Review the draft message.
6. Click **Send**.

> **Important**
>
> The Shared Space invite is sent through Vault Messaging. This is different from adding a key to the same Safe.

6.24.6 Step 4. Recipient Imports the Shared Space

The recipient should:

1. Open the message in **Vault Messaging**.
2. Read the Shared Space notice in the message.
3. Click **Add Shared Space**.
4. Wait for the import to complete.
5. Open the imported Space in their Safe.

6.24.7 Step 5. Collaborate

After import:

- both Safes can work in the same shared workspace,
- notes and cloud files in that Space can be used collaboratively,
- changes may require refresh or reopening content to see the latest state.

6.24.8 Step 6. Understand Ownership and Deletion

1. Keep in mind that the Safe that created the Shared Space is the owner.
2. If the owner deletes the Shared Space, it is deleted for every Safe that has access to it.
3. If a non-owner deletes the Shared Space from their own Safe, only that Safe loses access.
4. In the non-owner case, the Shared Space data remains available to the owner and any other participating Safes.

6.24.9 When to Use This vs Access Keys

Use **Shared Spaces** when:

- each person should keep their own Safe,
- you want collaboration without exposing unrelated Safe contents,
- the goal is a shared workspace between Safes.

Use **access keys** when:

- the goal is for multiple users to open the **same Safe** using their own access keys,
- one Safe owner wants to assign certain Spaces to another user's access key,
- one Safe owner wants another user's access key to have full administrative rights to the Safe,
- you are not creating collaboration between separate Safes.

6.24.10 Troubleshooting

- **No Share Space option**: confirm your tier supports the feature and that you are using Vault Messaging.
- **Recipient cannot import**: confirm the recipient opened the correct message and used **Add Shared Space**.
- **Files not behaving as expected**: Shared Spaces support cloud collaboration, not local-only file storage.
- **Shared Space disappeared for everyone**: check whether the owner Safe deleted the Shared Space.
- **Shared Space disappeared only for one Safe**: that Safe may have removed its own access while the owner and other participants still retain the Shared Space.

6.24.11 Related Guides

- **Shared Spaces**

- **UnoLock Spaces**
- **Granting an Access Key Access to Spaces in the Same Safe**

6.25 Granting an Access Key Access to Spaces in the Same Safe

6.25.1 Overview

This guide explains how to let another person use their **own access key** with the **same Safe**.

That access key can be given:

- access to **selected Spaces only**, or
- **full administrative access** to the Safe.

This is for sharing **one Safe** with another user. It is **not** the same as a Shared Space between separate Safes. If you want collaboration between separate Safes, use **Sharing a Space Between Safes** instead.

6.25.2 When to Use This

Use this guide when:

- another person should use their **own passkey, phone, or hardware key** to open the same Safe,
- you want to limit that person to selected Spaces,
- or you want to give that person full administrative control of the Safe.

6.25.3 Before You Start

- You must already have access to the Safe with an **admin access key**.
- The person you are adding will need their **own authenticator**, such as a passkey or hardware key.
- Decide in advance whether they should have:
- **limited access** to selected Spaces, or
- **full admin access** to the Safe.

6.25.4 Step 1. Create or Review the Spaces

1. Open the **Notes** area of your Safe.
2. Confirm which Space or Spaces the new access key should be allowed to open.
3. If needed, create a new Space first.

If you need help creating Spaces, see **Creating Spaces in Your Safe**.

6.25.5 Step 2. Open Key Management

1. Open the main menu in UnoLock.
2. Select **Configuration**.
3. Open **key management**.

6.25.6 Step 3. Create the New Access Key

1. Choose the option to create a new key.
2. Enter a name for the new key.
3. Continue through the prompts.
4. Choose whether the new key should use the same PIN or its own PIN.
5. Re-authenticate with your current access method when prompted.

6.25.7 Step 4. Choose the Permission Level

1. Select the permission level for the new key.
2. Choose one of these:
3. **Selected Spaces only**
4. **Full administrative access**
5. If you selected limited access, choose the specific Space or Spaces the key should be allowed to open.
6. Confirm the assignment.

6.25.8 Step 5. Register the New User's Access Key

1. Continue to the QR code step.
2. Review the temporary QR code shown on screen.
3. Have the other user scan the QR code or follow the displayed registration flow.
4. Complete the registration of their passkey, phone, or hardware key.
5. Finish the setup.

After this step, the other user has **their own access key** for the same Safe.

6.25.9 Step 6. Verify the Result

1. Open the new key in key management.
2. Confirm the assigned permissions.
3. Test access with the newly registered key.
4. Confirm that:
5. the user can open only the allowed Spaces, or
6. the user has full admin access, depending on what you selected.

6.25.10 Important Difference from Shared Spaces

- **Same Safe + access keys**: multiple users can open **one Safe**, each with their own access key.
- **Shared Spaces**: multiple **separate Safes** collaborate in one shared Space.

6.25.11 Related Guides

- **Creating Spaces in Your Safe**
- **Sharing a Space Between Safes**
- **Shared Spaces**
- **UnoLock Spaces**

6.26 Deleting a Safe

6.26.1 Overview

This guide provides step-by-step instructions for permanently deleting your UnoLock vault.

6.26.2 Access Safe Deletion Options

1. From the main menu, go to **Configuration**.
2. Select **Options**.

6.26.3 Initiate Safe Deletion

1. Click to initiate vault deletion.
2. Read the warning message explaining the action and emphasizing the non-recoverability of your data.
3. Click **Delete** to proceed.
4. Note: Deleting your vault is a permanent and irreversible action. All data will be lost.

6.26.4 Confirm Deletion

1. Type the word **Regret** into the provided field to confirm your decision.
2. Click **Next**.
3. Note: Your vault will be permanently deleted.

6.26.5 Save Promotional Code

1. Copy the promotional code displayed on the screen for reimbursing any unspent credits assigned to the vault.
2. Save the code for future use to create a new vault with the remaining credits.
3. Click **Next** to return to the home screen.

6.26.6 Next

Next: Tutorials Overview

6.27 Using Receive Addresses

6.27.1 Overview

Receive Addresses are shareable inbox addresses for **Vault Messaging**. They let you receive messages and files to a Safe through an address.

Each Receive Address has: - Its own keypair - Its own intake policy (usage limit, throttle, attachments) - Client-side hashed routing (`vaultxAddressHash`) so the raw address is not sent to the server

This makes intake compartmentalized and easy to revoke.

6.27.2 Capabilities by Tier

- **Sovereign / HighRisk**
- Can create and manage Receive Addresses.
- **Free / Inheritance**
- Cannot create Receive Addresses.
- Can still send messages/files and optionally allow replies.
- Can receive on legacy messaging paths and use bound reply flows.

6.27.3 Create a Receive Address

Prerequisites: - **Sovereign or HighRisk tier** - **Authenticated Safe session**

1. **Open Messaging** In the Safe app, open the **Messaging** section.
2. **Go to Receive Addresses** Select the **Receive Addresses** (or **Addresses**) tab.
3. **Create a new address** Click **New Receive Address**.
4. **Configure address settings** Set optional controls:
5. **Sender message**: public note shown to senders in **UnoLock Drop**. You can use this as a pre-shared code word so senders can verify they are using the correct address.
6. **Private label/description**: internal-only label for your inbox.
7. **Usage limit**: cap how many times the address can be used.
8. **Throttle**: rate limit incoming drops.
9. **Attachments**: allow or block file uploads.
10. **Save and generate** The app generates a Receive Address and a shareable URL.

6.27.4 Share a Receive Address

- **Copy the address** and share it directly, or
- **Share the URL** to open the UnoLock Drop client with the address prefilled.

6.27.5 Manage Address Lifecycle

- **Disable** an address to stop new messages while keeping it visible.
- **Delete** an address to revoke it entirely.
- **Rotate** by creating a new address for a new source or project.

6.27.6 Where Messages Appear

Messages sent to a Receive Address appear in **Messaging**, grouped by address. Decryption happens client-side inside your Safe.

Operational tip

Use a different Receive Address per source, campaign, or project. This minimizes cross-linking and keeps revocation simple.

Code-word check

For higher assurance, agree on a short code word with the sender and place it in the Receive Address sender message. The sender should only send if that code word is displayed in UnoLock Drop.

⚠ **High-risk sender guidance**

If you share a Receive Address publicly, advise senders to use Tor Browser with UnoLock Drop for stronger network anonymity.

If you are looking for anonymous sending instructions, see **How to Send a Message with UnoLock Drop**.

6.28 How to Send a Message with UnoLock Drop

This guide explains how to send an anonymous message or file using **UnoLock Drop**. UnoLock Drop is a standalone sender client that lets anyone send encrypted payloads to a **Receive Address** without creating a Safe. It is built for first-contact and high-risk disclosure workflows where identity exposure is unacceptable. UnoLock Drop is **sender-only** (no inbox or replies).

UnoLock Drop uses client-side encryption (ML-KEM-1024 + AES-256-GCM) and hashes the Receive Address (`vaultxAddressHash`) before sending it to the server.

6.28.1 Why Use UnoLock Drop?

- **Anonymous first contact**: no account or login required.
- **Post-quantum security**: ML-KEM-1024 + AES-256-GCM protect the payload.
- **Address privacy**: the server receives only the hashed Receive Address.
- **Optional Tor access**: use Tor Browser for extra network privacy.

> ⚠ **Security Note**
>
> Always verify the Receive Address or shareable link provided by the recipient. If you are in a high-risk environment, use a trusted device and consider Tor.

6.28.2 Prerequisites

- **Receive Address or shareable URL** from the recipient.
- **Modern browser** with JavaScript enabled.
- **Tor Browser (recommended for high-risk use)**.

6.28.3 Step-by-Step: Send with UnoLock Drop

1. **Open the Drop Client** Open the shareable URL from the recipient, or visit `https://drop.unolock.com`.
2. **Confirm the Receive Address** If you opened a shareable URL, the address will be prefilled and a sender message may appear. Review usage limits and attachment rules shown in the client. If you and the recipient agreed on a code word, verify it appears in the sender message before sending.
3. **Compose your message** Add a subject and message content.
4. **Add attachments (optional)** Attach files if the address allows attachments. If attachments are disabled, the Drop Client will block file uploads.
5. **Send the drop** UnoLock Drop encrypts locally and uploads the sealed payload.
6. **Save the address (optional)** You can store frequently used Receive Addresses in a local, password-encrypted address book on your device.

6.28.4 Troubleshooting

- **Invalid address**: re-check the Receive Address or link.
- **Throttled**: the address is rate-limited; try again later.
- **Usage exhausted**: the address has hit its usage limit.
- **Attachments blocked**: the recipient disabled attachments for this address.
- **Network instability**: on slow or censored networks, retry via Tor Browser.

6.28.5 What Happens Next

The recipient receives the message in their Safe inbox under the corresponding Receive Address. Decryption occurs client-side, and no account is required for the sender.

If you are a recipient and want to manage Receive Addresses, see **Using Receive Addresses**.

6.29 How to Open Messages (Recipient)

Messages arrive in your Safe inbox when someone sends a drop to one of your **Receive Addresses**. Decryption happens client-side, and the server never sees the plaintext. This keeps sensitive intake inside your Safe, not on the wire.

6.29.1 Prerequisites

- **Authenticated Safe session**
- **Receive Address created** (Sovereign or HighRisk tier)

6.29.2 Step-by-Step: Open a Message

1. **Sign in to your Safe** Authenticate using your FIDO2 key or biometric method.
2. **Open Messaging** Go to the **Messaging** section in the left-hand menu.
3. **Select the Receive Address inbox** Messages are grouped by Receive Address or label. Open the relevant thread.
4. **Read and decrypt** Messages decrypt automatically in the client. View the subject, body, and any attachments.
5. **Save content (optional)** Save the message as a note or store attachments in your Safe if needed.

Attachment rules

If the Receive Address disallows attachments, only message content will be present.

6.29.3 Troubleshooting

- **No messages appear**: confirm the sender used the correct Receive Address.
- **Decryption fails**: try reloading the app and confirm your Safe is fully authenticated.
- **Address disabled**: if the address was revoked, new messages will not arrive.

If you need to create or manage Receive Addresses, see **Using Receive Addresses**.

6.30 How to Use Vault Messaging in UnoLock

Vault Messaging is UnoLock's in-app system for secure, address-based communication. It is designed to keep conversations compartmentalized and metadata minimized, even in high-risk environments. Think of it as Safe-to-Safe communication without a global identity trail.

It supports two ways to send:

Receive Addresses are recommended for new conversations and anonymous intake because they keep raw addresses off the server and allow per-address controls.

6.30.1 Why Use Vault Messaging?

- **Address-based privacy**: send to an address, not a global identity.
- **Post-quantum security**: ML-KEM-1024 + AES-256-GCM protect messages.
- **Per-address control**: usage limits, throttling, and attachment rules.
- **Anonymous intake**: external senders can use the UnoLock Drop client.

⚠ **Security Note**

Always verify the destination address before sending. If available, verify a pre-shared code word shown in the Receive Address sender message.

6.30.2 Prerequisites

- **Sending**: Sovereign or HighRisk tier.
- **Receiving**: all tiers can receive; Free/Inheritance can reply using bound reply-only addresses.
- **Destination address**: a Receive Address (recommended) or a compatibility Safe address (`eyesAddr`).

6.30.3 Step-by-Step: Sending a Message (Safe App)

1. **Sign in** Authenticate into your Safe.
2. **Open Messaging** Click **Messaging** in the left-hand menu.
3. **Start a new message** Click **New Message**.
4. **Enter the destination address** Paste a **Receive Address**
5. **Check address policies** The app will show attachment rules and any rate limits. If you use a pre-shared code word workflow, confirm the expected code word is shown.
6. **(Optional) Save to Known Addresses** Save the address locally with a name so you can reuse it later.
7. **Compose and attach** Write your message and add attachments if allowed.
8. **Send** Click **Send**. The message encrypts client-side and is routed by the server.

6.30.4 Step-by-Step: Receiving a Message

1. **Open Messaging** Incoming messages appear in your inbox, grouped by address.
2. **Open the thread** Select the conversation or Receive Address label.
3. **Read and decrypt** Messages decrypt locally inside your Safe.
4. **Save content (optional)** Save messages as notes or store attachments in your Safe.

6.30.5 Anonymous Senders (UnoLock Drop client)

If you want to receive messages from outside Safes, create a Receive Address and share the **UnoLock Drop client** link. UnoLock Drop is sender-only (no inbox). See **Using Receive Addresses**.

Reply-only behavior

If a known address sends you a message and you reply, your reply address is bound to that sender. This prevents address reuse and keeps trust boundaries tight.

6.30.6 Troubleshooting

- **Invalid address**: confirm the destination address through a trusted channel.
- **Throttled or expired**: the Receive Address may be rate-limited or out of uses.
- **Attachments blocked**: the destination address has attachments disabled.
- **Free tier cannot send**: Free and Inheritance tiers can receive and reply only.

For a deeper dive, see **Vault Messaging**.

6.31 Backup and Restore a Space

6.31.1 Overview

This guide explains how to create an encrypted Space backup (`.usbk`) and restore it using the current **Backup / Restore** config flow.

Use this primarily for controlled data migration. UnoLock Safe storage is already highly redundant, and password-protected backups reduce your security posture if the password is weak.

6.31.2 Before You Start

- Open **Configuration** and use **Backup / Restore** (not **Manage Spaces**) to start.
- Use a strong, unique passphrase for backup encryption.
- Perform backup and restore in a trusted environment.
- Ensure you have local archive files (`.ulf`) available if the Space contains local archives.
- Decide whether to include wallets. Wallet export requires WebAuthn verification.

6.31.3 Create a Space Backup

1. Open **Configuration**.
2. Click **Backup / Restore**.
3. In the first prompt, choose **Backup**.
4. Read the warning and continue only if needed.
5. If your Safe has multiple Spaces, select which Space to back up.
6. Enter and confirm your backup password.
7. Choose whether to include wallets.
8. If prompted, select the matching local archive files (`.ulf`) for that Space.
9. Choose where to save the `.usbk` file.
10. Wait for completion in the backup progress modal.

6.31.4 Restore a Space Backup

1. Open **Configuration**.
2. Click **Backup / Restore**.
3. In the first prompt, choose **Restore Backup**.
4. Select the `.usbk` file.
5. Enter the backup password.
6. Choose restore destination mode when prompted:
7. **Sovereign** and **High Risk** tiers: choose **Merge Into Existing Space** or **Create New Space**.
8. Other tiers (including free tier): restore defaults to merge into the current Space.
9. Wait for completion in the restore progress modal.

6.31.5 What Gets Restored

- Records and labels from the source Space.
- Cloud, message, and local archives that are present in the backup.

- Optional wallet secrets if wallet inclusion was selected during backup.

6.31.6 Archive ID Remapping

Restored archives receive new archive IDs in the destination Safe. Record attachments are automatically remapped so notes still point to the correct restored files.

If you choose **Create New Space**, the destination Space is named with a **(Restored)** suffix (for example, `Project X (Restored)`). If you choose merge mode, data is merged into the selected/current Space.

6.31.7 Local Archive Notes

- Local archives are included only when matching `.ulf` files are provided during backup.
- If required `.ulf` files are missing, backup prompts you to retry selection or cancel.
- On tiers without cloud archive support, restored archives are written as local archives.

6.31.8 Wallet Notes

- Wallet inclusion is optional.
- Wallet secret parts are decrypted in one batched WebAuthn-assisted request during backup.
- On restore, wallet secrets are re-encrypted using the destination Safe’s WebAuthn-protected encryption flow.

6.31.9 Security Warnings

- Backup files are encrypted, but still vulnerable to offline password guessing if a weak password is used.
- Do not store backup files in untrusted locations.
- Do not treat backups as a replacement for normal Safe key hygiene (multiple keys, LockoutGuard, and operational controls).

6.31.10 Troubleshooting

Restore fails with password/corruption error

- Verify password exactly.
- Verify backup file integrity and full file transfer.

Some files are missing after restore

- Check the skipped archive count in completion details.
- Re-run backup with all required local `.ulf` files selected.
- For merge restores, verify you are viewing the destination/current Space.

Wallets did not restore as expected

- Confirm wallet inclusion was selected during backup.
- Complete required WebAuthn verification prompts during backup and restore.

6.32 How to Export Your DPW Seed Phrase to Transaction Wallets

6.32.1 Overview

This guide provides step-by-step instructions for exporting your Digital Paper Wallet (DPW) seed phrase from UnoLock to a transaction wallet, allowing you to access your cryptocurrency funds externally.

6.32.2 Access Your DPW

1. Navigate to the **Wallet** section in the UnoLock app.
2. Select the Digital Paper Wallet (DPW) you wish to export.
3. Note: Ensure you are in a secure environment, as exporting your seed phrase requires careful handling to prevent unauthorized access.

6.32.3 View the Seed Phrase

1. Click **Show Private Key** or **Show Seed Phrase** for the selected DPW.
2. Read the warning message about keeping your seed phrase secure.
3. Authenticate using your device’s usual method (e.g., fingerprint scan, facial recognition, or FIDO2 passkey) to proceed.
4. Review the 24-word seed phrase displayed.
5. Note: Do not take screenshots or store the seed phrase digitally to avoid risks of hacking.

6.32.4 Export the Seed Phrase

1. Manually write down the 24-word seed phrase on a piece of paper.
2. Optionally, click **Copy** to copy the seed phrase to your clipboard, but ensure you paste it securely and clear your clipboard afterward.
3. Store the written seed phrase in a secure, offline location (e.g., a safe or lockbox).

6.32.5 Import into a Transaction Wallet

1. Open the external transaction wallet where you wish to import the DPW funds.
2. Select the option to **Import Wallet** or **Restore Wallet**.
3. Enter the 24-word seed phrase exactly as recorded.
4. Follow the wallet’s instructions to complete the import process.
5. Verify that your funds are accessible in the transaction wallet.
6. Note: Once imported, manage the transaction wallet securely, as it now controls access to your cryptocurrency funds.

6.32.6 Secure Your Seed Phrase

1. Ensure the written seed phrase is stored in a safe, offline location.
2. Do not share the seed phrase with anyone, as it grants full access to your funds.
3. Optionally, create multiple offline copies and store them in separate secure locations.
4. Note: If your seed phrase is compromised, your funds may be at risk of theft.

6.32.7 Next

Next: Tutorials Overview

6.33 How to Export Your DPW Seed Phrase

Welcome to the guide on exporting a seed phrase from a Digital Paper Wallet (DPW) in UnoLock CybVault. The DPW is a non-custodial, multi-currency cryptocurrency wallet generator designed with a strict zero-knowledge principle, ensuring UnoLock never has access to your private keys or mnemonic seed phrases. Exporting your seed phrase is a deliberate security ceremony known as the Key Extraction Protocol (KEX), which protects against risks like malware, coercion, and unauthorized access.

This process involves splitting the 24-word mnemonic phrase into two 12-word halves, requiring authentication and offline mode for each half to minimize exposure. It's essential for importing your DPW into external transaction wallets (e.g., Ledger, MetaMask) while maintaining security.

6.33.1 Why Exporting a DPW Seed Phrase Is Important

- **Non-Custodial Control**: UnoLock's DPW ensures you remain the sole custodian of your secrets. Exporting allows safe transfer to hardware wallets for transactions, without exposing plaintext keys to the internet.
- **Security Against Threats**: The KEX protocol mitigates risks like keyloggers or man-in-the-middle attacks by enforcing offline decryption and multi-layered encryption.
- **Compatibility**: Exported seed phrases (BIP-39 compliant) can be imported into supported wallets like Ledger Nano S/X, Trezor, Trust Wallet, or MetaMask (ETH/ERC-20).
- **Resilience**: Built with post-quantum preparedness and quadruple encryption, this process aligns with UnoLock's defense-in-depth model, protecting against current and future threats.

⚠ **Important Security Note**

Never export your seed phrase on a compromised device or while online. Always perform this in a secure environment. Once exported, store the full phrase offline and never share it. UnoLock cannot recover lost phrases.

6.33.2 How the DPW Seed Phrase Export Works

The DPW architecture uses a multi-layered security model: - **Secret Splitting**: The 24-word mnemonic is split into two independent 12-word halves, preventing a single exposure from compromising the full phrase. - **Quadruple Encryption**: Each half is protected by four layers: client-side master key encryption, server-side re-encryption, envelope encryption, and AWS S3 server-side encryption (SSE) with AES-256. - **KEX Protocol**: Decryption requires FIDO2/WebAuthn authentication, PIN entry, and offline mode. The system validates key-pairs internally using standards like BIP-39 and BIP-32. - **Ephemeral Handling**: After viewing, the app forces a reload to purge memory traces.

This ensures zero-knowledge: UnoLock servers store encrypted blobs but cannot decrypt them.

6.33.3 Prerequisites

- An authenticated UnoLock session on a Sovereign or HighRisk tier (DPW is available in these tiers).
- A secure, trusted device (e.g., no malware).
- A hardware wallet ready for import (e.g., Ledger).
- Backup paper and pen for writing the phrase (do not store digitally).

6.33.4 Step-by-Step Guide

Follow these steps carefully to export your DPW seed phrase.

1. **Authenticate into UnoLock**
   Open the UnoLock app and authenticate using your biometric or FIDO2 method. Ensure you're in a secure environment.
2. **Open Your Safe**
   Navigate to "Open Safe" and authenticate in to access your vault.
3. **Access the Wallet Menu**
   In the main menu, go to "Wallet" and select the Digital Paper Wallet (DPW) you want to export the seed phrase from.
4. **View the Wallet**
   Click "View" to open the wallet details.
5. **Initiate Seed Phrase Recovery**
   Click "Show Recovery Phrase," then confirm by clicking "Show Recovery Phrase" again. You'll be presented with the Key Extraction Protocol (KEX) overview.
6. **Export the First Half of the Seed Phrase**
7. Select "First Half."
8. Authenticate using your FIDO2/WebAuthn key and enter your UnoLock PIN.
9. Go offline: Disconnect your internet connection or enable airplane mode on your device.
10. Confirm you're offline by clicking "I am Offline."
11. The first 12 words of your seed phrase will appear. Write them down securely on paper.
12. Click "Close" to exit the view.
13. **Go Back Online and Re-Authenticate**
    Reconnect to the internet and log back into UnoLock. Authenticate into your safe again to continue.
14. **Export the Second Half of the Seed Phrase**
    Repeat steps 3–5 to return to the wallet view.
15. Select "Second Half."
16. Authenticate with FIDO2 and PIN.
17. Go offline again and confirm.
18. The second 12 words will appear. Write them down to complete the full 24-word phrase.
19. Click "Close."
20. **Import the Seed Phrase into Your Transaction Wallet**
    Use the full 24-word phrase to import into a compatible wallet (e.g., Ledger Nano S/X, Trezor, Trust Wallet, or MetaMask for ETH/ERC-20). Follow the wallet's import instructions carefully.
21. **Secure Your Phrase**
    Store the written phrase in a safe, offline location (e.g., a physical vault). Never store it digitally or share it.

6.33.5 Troubleshooting

- **Offline Confirmation Fails**: Ensure your device is fully disconnected (check Wi-Fi and cellular). The app enforces this to prevent online exposure.
- **Authentication Errors**: Verify your FIDO2 key is registered. Use LockoutGuard if locked out (see LockoutGuard Setup).
- **Wallet Not Visible**: Ensure you're on Sovereign or HighRisk tier. Upgrade if needed (see Upgrade Safe).
- **Phrase Validation**: After import, verify the wallet address matches your DPW to confirm accuracy.

6.33.6 Security Considerations

- **Why Offline Mode?**: Prevents real-time attacks like malware capturing the phrase during display.

- **Split-Trust Recovery**: Viewing halves separately on different devices adds protection against single-device compromise.
- **No Recovery by UnoLock**: Due to zero-knowledge design, UnoLock cannot reconstruct or recover your phrase, responsibility lies with you.
- **Post-Quantum Resilience**: The KEX protocol uses lattice-based encryption, safeguarding against future quantum threats.

For more on DPW security, see Digital Paper Wallet (DPW) Security. If issues persist, join our Reddit community or contact support. Own your digital destiny with UnoLock.

6.34 Verify Client-Side Encryption

6.34.1 Overview

This guide shows non-technical users how to verify that encryption truly happens client-side in your browser before files leave your computer. A zero-knowledge service encrypts your data in your browser, meaning the provider never sees plaintext—only encrypted ciphertext.

This verification takes about 15 minutes using only your browser's built-in tools.

6.34.2 Why This Matters

A service claiming "zero-knowledge encryption" means:

- Your files or secrets are **encrypted in your browser** before they leave your computer.
- The company **never sees plaintext**—only ciphertext (random data).

If encryption happens server-side, the provider could decrypt it. This guide teaches you how to see that encryption really occurs before upload.

6.34.3 What You Need

- **Chrome, Edge, Brave, or Firefox** (desktop version)
- A **free or test account** in UnoLock
- A small text file (e.g., `test123.txt`) containing obvious text like:

```
Hello, this is my secret.
```

- About **15 minutes**

6.34.4 Step 1: Open Developer Tools

1. Visit `https://safe.unolock.com` and log into your vault.
2. Right-click anywhere on the page and select **Inspect**.
3. In the DevTools panel, choose the **Network** tab.
4. Enable **"Preserve log"** so traffic isn't cleared when pages change.

6.34.5 Step 2: Start Recording and Upload a File

1. Ensure the Network tab is recording (red dot active).
2. Upload your sample file to the vault (or create a note with the text).
3. Wait until the upload finishes, then review the recorded requests.

You'll now see many requests in the Network list.

6.34.6 Step 3: Find the Upload Request

1. In the search box above the request list, type `upload`, `file`, or `api`.
2. Click the request that looks like the file upload (often a `POST` or `PUT` request).
3. Select the **Payload** tab (in Firefox it may be labeled **Request Body**).

6.34.7 Step 4: Inspect What Was Sent

Look at the payload contents:

- **Good**: You see **gibberish** (long random text, base64 strings, or binary bytes like `JFk4s9ds/7x...`)—this is ciphertext.
- **Bad**: You can still read `Hello, this is my secret.`—this is not encrypted client-side.

The contents should look like pure entropy: no words, no filenames, no JSON fields named "content".

6.34.8 Step 5: Check Filename and Metadata

Still in that request:

- **Filename** should be hashed (e.g., `7e2a9d6f...`) or absent entirely.
- **Headers** may include `Content-Type: application/octet-stream` or `binary/octet-stream`—that's a good sign.
- There should be **no readable text** in either the request URL or body.

6.34.9 Step 6: View Response Headers (Optional)

Select the **Headers** tab and confirm:

```
Request Method: POST
Status Code: 200
```

If the server only responds "OK" without echoing your plaintext back, that's good. If the server response body contains your text file contents, it's not zero-knowledge.

6.34.10 Step 7: Spot-Check with Another File

Repeat Steps 2–6 using a different file or secret. Ciphertext should change completely each time (due to encryption randomness). If it looks identical each time, that's a weak sign indicating non-random encryption.

6.34.11 Step 8: Entropy Test (Advanced, Optional)

1. Copy a small chunk of the Payload data (around 1 KB).
2. Paste it into an **entropy calculator** such as https://www.browserling.com/tools/entropy.
3. A score above **7.5 bits/byte** indicates strong randomness—typical of real ciphertext.

6.34.12 Step 9: Confirm No Plaintext Storage Locally

1. In DevTools, go to the **Application** tab.
2. Check **Local Storage** and **IndexedDB**.
3. Make sure your secret text isn't stored there in clear. Zero-knowledge apps keep only random tokens, not actual content.

6.34.13 Step 10: Document What You Found

Create a simple record:

Check	Result	Notes
Payload unreadable	/	
Filenames hidden	/	
No plaintext in local storage	/	
Randomness high	/	

Keep screenshots—they're useful evidence if you later audit or report results.

6.34.14 What "Good" Looks Like

- Upload request shows random bytes (ciphertext).
- No readable content anywhere in network tab.
- No plaintext remnants in local storage.
- Every upload looks different.

6.34.15 What "Bad" Looks Like

- Your text or filename appears in the upload payload.
- The server echoes your data back.
- Plaintext stored in browser storage.
- Identical ciphertext across uploads.

6.34.16 Optional Deeper Checks (For Technical Users)

- Use **Fiddler**, **Burp Suite**, or **mitmproxy** with your own test cert to intercept HTTPS locally (never do this with real secrets).
- Confirm ciphertext before TLS encryption is identical to what you saw in the browser.
- Compare with open-source zero-knowledge tools (Tresorit, Proton Drive) for baseline behavior.

6.35 How to Set Up the Affiliate Program

This guide walks you through setting up the UnoLock Affiliate Program in your CybVault account. The UnoLock Affiliate Program empowers privacy-conscious individuals, influencers, and partners to promote our zero-knowledge, post-quantum encrypted vault while earning commissions. As an affiliate, you contribute to the mission of digital sovereignty by helping others secure their data, legacy, and freedom. This step-by-step tutorial covers the process, based on UnoLock's commitment to trustless security.

6.35.1 Prerequisites

Before starting, ensure you meet the following requirements: - **Account Tier**: The affiliate program is available only on the Sovereign or HighRisk tiers. Upgrade your account if you're on Free or Inheritance. - **Upgrade Process**: Navigate to your account settings, select a qualifying tier, and complete the payment via Stripe, or Bitcoin. The affiliate option unlocks immediately after upgrade. - **Email Address**: An email is required for onboarding (creating a separate, non-anonymous affiliate account for payment purposes). - **Payout Method**: You must have a PayPal account, as UnoLock currently pays commissions via PayPal.

If you haven't upgraded yet, refer to the Upgrade Safe guide.

6.35.2 Step-by-Step Guide to Creating and Configuring Your Affiliate Link

Follow these steps to join the program and set up your unique referral link.

1. **Authenticate into the UnoLock App**
   Log in to your UnoLock CybVault account using your biometric or FIDO2 authentication. Ensure you're on a Sovereign or HighRisk tier for access to the affiliate features.
2. **Access the Options Menu**
   Click on the left-hand menu and navigate to "Options." This section allows you to customize your vault settings.
3. **Enable the Affiliate Program**
   Locate and click the "Affiliate Program" checkbox. Then, click "Save." This action launches the Affiliate Program menu in the Configuration section.
4. **Navigate to the Affiliate Program Menu**
   Return to the Configuration menu and click on the "Affiliate Program" menu item. Read the program overview, which highlights earning a perpetual 20% commission and promoting UnoLock's cutting-edge security.
5. **Join the Program**
   Click "Join Program" to begin onboarding. Read the Terms and Conditions carefully, then click "I Agree" to proceed.
6. **Provide Your Email Address**
   Enter your email address when prompted. This is required for affiliate onboarding and payment processing, creating a separate account for commissions while maintaining your vault's anonymity.
7. **Complete Onboarding with Trolley**
   Click "Next" to be redirected to the UnoLock portal at Trolley.com, our affiliate vendor. Fill out the general information: account type, first and last name, email (pre-filled), date of birth, country, and address. Click "Next."
8. **Add a Payout Method**
   Enter your PayPal account details as the payout method (UnoLock currently supports only PayPal). Complete the setup, and you'll be redirected back to UnoLock, where your affiliate account links to your vault.
9. **Configure Your Affiliate Link**
   In the Affiliate Program dashboard, choose a unique suffix for your referral link (e.g., unolock.com/affiliate/your-suffix). The system checks for availability and duplicates. Once set, the suffix cannot be changed (future updates may allow modifications).
10. **Save and Start Promoting**
    Click "Save" to finalize your link. Your dashboard will now show the referral link, ready for sharing on social media, blogs, or communities.

6.35.3 Affiliate Dashboard Overview

After setup, the dashboard becomes your hub for tracking performance.

- **How It Works**: Access it via the "Affiliate" option in your account menu. It displays transaction dates, amounts, commissions, and is paginated for high-volume referrals.
- **Why It's Important**: Provides transparent insights without compromising anonymity, empowering you to monitor earnings in real time.
- **Features**: View referrals, commissions, and link usage, all integrated with UnoLock's zero-knowledge architecture.

6.35.4 Commission Structure and Discounts

- **Affiliate Commission**: Earn a perpetual 20% on all recurring payments from referred users.
- **User Discount**: Referred users get a 10% perpetual discount, applied automatically via your link.
- **Net Revenue**: UnoLock retains ~60% per sale, ensuring profitability while rewarding affiliates.
- **Visibility**: Discount messaging is being enhanced for clearer signup notifications, reducing inquiries.

6.35.5 Payment Processing and Frequency

- **How It Works**: Commissions are paid monthly via PayPal (future support for bank transfers). Trolley handles processing through APIs and webhooks.
- **Why It's Important**: Consistent payments encourage long-term promotion, with global accessibility via PayPal.
- **Integration**: Server-side communication keeps your data private.

6.35.6 Eligibility and Account Creation

- **Tier Requirement**: Sovereign or HighRisk only, to promote premium features.
- **Account Separation**: Your affiliate account is separate (requires email) for payment compliance, preserving vault anonymity.
- **Virality**: Share your link to earn while spreading digital sovereignty.

6.35.7 Getting Started Tips

- **Upgrade First**: If not on a qualifying tier, see Upgrade Safe.
- **Promote Effectively**: Use your link on Reddit, blogs, or forums. Referred users enjoy 10% off, boosting conversions.
- **Questions?**: Join our Reddit community or contact support.

Own your digital destiny, and help others do the same through the UnoLock Affiliate Program. For more on earnings, see the Affiliate Overview.

7. Affiliate Program

7.1 UnoLock Affiliate Program

Welcome to the UnoLock Affiliate Program documentation. This program is designed to empower privacy-conscious individuals, influencers, and partners to promote UnoLock CybVault while earning commissions. As a participant, you contribute to the mission of digital sovereignty by helping others secure their data, legacy, and freedom. This guide covers the dashboard, onboarding, commission structure, and more, based on UnoLock's commitment to trustless, zero-knowledge security.

7.1.1 Affiliate Program Overview

The UnoLock Affiliate Program allows you to earn a perpetual 20% commission on sign-ups through your unique referral link. It's available exclusively on the main paid tiers: Sovereign and HighRisk, ensuring affiliates promote premium features like post-quantum encryption, DuressDecoy, and Plausible Deniability. Users who sign up via your link receive a perpetual 10% discount, creating a win-win for security advocates. The program is built for virality, enabling you to spread UnoLock's antidote to techno-feudalism while generating revenue.

Why Join the Affiliate Program?

- **Earn Passive Income**: Receive 20% of all recurring payments from referred users, fostering long-term earnings.
- **Promote Digital Sovereignty**: Align with UnoLock's values of anonymity, resilience, and legacy protection, helping users escape data exploitation.
- **Easy Setup**: No complex requirements, just upgrade to a paid tier, configure your link, and start sharing.
- **Transparency and Security**: All processes are integrated with UnoLock's zero-knowledge architecture, ensuring your data and payments remain private.

7.1.2 Affiliate Dashboard

The affiliate dashboard is your central hub for managing referrals and tracking earnings. It provides real-time insights into your program's performance while maintaining UnoLock's privacy-first design.

How It Works

1. **Access the Dashboard**: After upgrading to a Sovereign or HighRisk tier, the "Affiliate" option appears in your account menu. Log in to view your unique dashboard.
2. **Choose Your Suffix**: Select a custom suffix for your referral link (e.g., unolock.com/affiliate/your-suffix). The system checks for duplicates to ensure uniqueness. Once set, the suffix cannot be changed (though future updates may allow modifications).
3. **View Transactions**: The dashboard displays transaction dates, amounts, and commissions. It's paginated to handle high volumes of referrals efficiently. Detailed financial data is available internally if needed for reconciliation.

Why It's Important

The dashboard empowers affiliates with transparent, actionable insights without compromising anonymity. In a world of opaque affiliate programs, UnoLock's trustless design ensures you control your earnings data, aligning with our sovereignty ethos.

7.1.3 Payment Processing and Frequency

Payments are processed securely and automatically, with flexibility for privacy-focused users.

How It Works

- **Frequency**: Commissions are paid monthly via PayPal, with potential future support for bank transfers.

- **Calculation**: Earnings are based on 20% of referred users' recurring payments (after their 10% discount). The system handles all calculations in the background.
- **Integration**: Payments are managed through APIs and webhooks with Trolley, ensuring seamless, background processing without user intervention.

Why It's Important

Monthly payments provide consistent income, while the PayPal integration offers global accessibility. This structure encourages long-term promotion, as UnoLock's perpetual commissions reward affiliates for users' ongoing security needs.

7.1.4 Onboarding Process for Affiliates

Onboarding is straightforward but requires minimal verification to ensure compliance and payment accuracy.

How It Works

1. **Upgrade Requirement**: The program is available only on Sovereign and HighRisk tiers. Upgrade your account to unlock the affiliate option.
2. **Trolley Setup**: New affiliates complete a secure onboarding flow via Trolley, confirming your account and adding payout methods (e.g., PayPal). An email address is required for this step, creating a separate, non-anonymous affiliate account.
3. **Link Configuration**: After onboarding, set your unique link suffix in the dashboard.
4. **Start Promoting**: Share your link and track referrals immediately.

Why It's Important

Onboarding balances ease with security, ensuring affiliates can receive payments reliably. While UnoLock emphasizes anonymity in vaults, the affiliate account's email requirement complies with payment regulations, protecting both you and the platform.

7.1.5 Commission Structure and Discounts

The structure is simple and incentive-driven, benefiting both affiliates and users.

How It Works

- **Affiliate Commission**: 20% perpetual commission on all payments from referred users.
- **User Discount**: Referred users receive a 10% perpetual discount, applied automatically via your link.
- **Net Revenue**: UnoLock retains approximately 60% of revenue per sale after commissions and discounts, ensuring profitability while rewarding affiliates.
- **Visibility**: The 10% discount is automatically applied, but messaging is being updated to make it more visible during signup, reducing customer inquiries.

Why It's Important

This structure fosters virality and loyalty, aligning with UnoLock's mission to make digital sovereignty accessible. Affiliates earn meaningfully, while users save on premium tiers, creating a sustainable ecosystem.

7.1.6 Eligibility and Account Creation

The program is tailored for users committed to UnoLock's premium features.

How It Works

1. **Tier Eligibility**: Available only on Sovereign and HighRisk tiers, not Free or Inheritance, to promote advanced features like Spaces and post-quantum encryption.

2. **Account Creation**: Create or upgrade your UnoLock account to a paid tier. The affiliate option appears post-upgrade.
3. **Upgrade Process**: Navigate to the upgrade section, select your tier, and complete payment. The dashboard unlocks immediately.

Why It's Important

Limiting eligibility to paid tiers ensures affiliates are genuine advocates, enhancing program quality and UnoLock's focus on high-value security.

7.1.7 Program Description and Virality

The program emphasizes earning while promoting privacy and security.

How It Works

- **Description**: "Earn a perpetual 20% commission by sharing your unique link. Promote UnoLock CybVault's cutting-edge security and help others protect what matters most."
- **Virality Component**: Encourage sharing on social media, blogs, or communities (e.g., Reddit). The 10% user discount incentivizes referrals, creating network effects.

Why It's Important

Virality amplifies UnoLock's reach, spreading the antidote to techno-feudalism. Affiliates become partners in the mission, earning while advancing digital freedom.

7.1.8 API Integration with Trolley

All backend processes are secure and automated.

How It Works

- **Trolley Integration**: Handles all affiliate onboarding and commission payments via APIs and webhooks. Communication is server-side, keeping your data private.
- **PayPal Requirement**: Affiliates must have a PayPal account to receive commission payouts. Trolley processes payments directly to your PayPal account monthly.

Why It's Important

The Trolley-only integration ensures a streamlined, secure payout process while maintaining UnoLock's privacy standards. Requiring PayPal accounts provides global accessibility and reliable payment processing for affiliates worldwide.

7.1.9 Customer Discount Visibility

To enhance user experience, discounts are automatic but clearly communicated.

How It Works

- **Application**: The 10% discount applies instantly on signup via your link.
- **Visibility**: Messaging is being updated to notify users during signup (e.g., "Enjoy 10% off forever via affiliate link"). This prevents confusion and inquiries.

Why It's Important

Clear visibility builds trust and encourages conversions, maximizing virality. It reinforces UnoLock's transparency, distinguishing it from opaque affiliate programs.

7.1.10 Getting Started as an Affiliate

1. **Upgrade**: Move to Sovereign or HighRisk tier.
2. **Onboard**: Complete Trolley setup with your email and payout method.
3. **Configure Link**: Choose a suffix in the dashboard.
4. **Promote**: Share your link and track earnings.
5. **Earn**: Receive monthly commissions via PayPal.

If you have questions, join our Reddit community or contact support. Own your digital destiny, and help others do the same.

8. UnoLock Company & Legal

Welcome to the **UnoLock Company & Legal Section**! This resource provides a comprehensive overview of TechSologic Inc., the creators of UnoLock CybVault, and the legal policies that govern our platform. Learn about our mission, engage with our community, and understand the terms that ensure transparency, privacy, and security for all users across the Free, Inheritance, Sovereign, and HighRisk tiers.

8.1 Company Overview

UnoLock, developed by TechSologic Inc., is committed to transparency, community engagement, and upholding the highest standards in ethics and legal practices. This section outlines our mission, legal policies, and community initiatives, empowering you with the knowledge to navigate UnoLock’s ecosystem confidently.

8.1.1 What You’ll Learn

- **About the Company**: TechSologic’s mission, vision, and dedication to privacy-first technology.
- **Terms and Conditions**: The policies governing UnoLock services.
- **Beta Program**: How to participate in UnoLock’s development and provide feedback.
- **Reddit Community**: Ways to connect with users and stay updated via our Reddit forums.

8.2 About the Company

TechSologic Inc., founded in 2010 and headquartered in Ottawa, Canada, is a pioneering software company focused on empowering digital sovereignty. Our flagship product, UnoLock CybVault, delivers unmatched security and control for digital assets across all tiers, Free, Inheritance, Sovereign, and HighRisk.

8.2.1 Core Specializations

- **Data Security**: Zero Trust architecture and advanced encryption protect your data.
- **Identity Management**: Secure multi-factor authentication and access governance.
- **Data Encryption**: Client-side encryption ensures privacy in transit and at rest.

8.2.2 Why UnoLock Works

- **Security**: Anonymity, encryption, and Zero Trust architecture ensure robust protection.
- **Inheritance**: LegacyLink enables secure data transfer to heirs (available in Inheritance, Sovereign, HighRisk tiers).
- **Protection**: Duress Decoy and Plausible Deniability modes safeguard data in high-risk scenarios (Sovereign and HighRisk tiers).

8.2.3 Our Vision

Guided by Data Self-Governance, TechSologic empowers users to autonomously manage and protect their digital assets, fostering a future of digital freedom.

Founding Principles and Milestones

Since 2010, TechSologic has been driven by: - **Advanced Security**: Delivering reliable solutions for data protection. - **Global Expertise**: Combining insights from Canada, Australia, and Germany. - **Transparency**: Building trust through open communication.

Milestones: - **2010**: Founded by Mike Stapleton, focusing on open-source encryption. - **2024**: Launched UnoLock CybVault with contributions from Robert Galambos and Max Boehm. - **Today**: A global leader in privacy-first digital solutions.

8.2.4 Contact Information

TechSologic Inc.
150 Elgin Street, 8th Floor
Ottawa, ON K2P 1L4
info@techsologic.com
www.techsologic.com

8.3 Terms and Conditions

UnoLock's legal policies ensure fair usage, data protection, and compliance with global regulations, prioritizing your privacy and security.

Key Legal Policies

- **Terms of Service**: Governs your use of UnoLock's platform and services.
- **Privacy Policy**: Details how we collect, use, and protect your personal information.
- **GDPR Policy**: Ensures compliance with EU data protection rights.
- **Cookie Policy**: Explains cookie usage for enhanced user experience.
- **Acceptable Use Policy**: Guidelines for acceptable platform behavior.

Additional Policies

- **Refund/Cancellation Policy**: Clarifies refund and subscription cancellation processes.
- **Data Retention Policy**: Outlines data retention and secure deletion practices.
- **Security Policy**: Describes measures to safeguard your data.
- **Fair Use Policy**: Ensures equitable resource access.
- **Disclosure Policy**: Protocols for reporting vulnerabilities.

8.4 Beta Program

The UnoLock Beta Program invites users to test early-access features, provide feedback, and shape the platform's future, enhancing security and usability across all tiers.

8.4.1 Why Join?

- **Early Access**: Test new features like enhanced LegacyLink or Spaces (Inheritance, Sovereign, HighRisk tiers).
- **Shape UnoLock**: Your feedback drives platform improvements.
- **Exclusive Benefits**: Enjoy extended trials or discounts.

- **Community Collaboration**: Connect with privacy advocates.

8.4.2 Survey Initiative

Surveys gather user preferences on features, usability, and innovations, ensuring UnoLock meets your needs.

How to Participate

- **Beta Program**: Register at survey.unolock.com to access beta features.
- **Surveys**: Complete surveys at survey.unolock.com to share feedback on features like CybVault or Duress Decoy Mode.

8.5 Reddit Community

UnoLock fosters a vibrant community on Reddit, where users discuss features, share insights, and get support.

8.5.1 Forums

- **r/UnoLock**: Stay updated on announcements, discuss privacy, and share feedback.
- **r/UnoLockSupport**: Get troubleshooting tips and community-driven support.

8.5.2 Get Involved

Join the conversation at r/UnoLock or seek help at r/UnoLockSupport to engage with the UnoLock community and team.