Dropbox Security Whitepaper

A Dropbox Whitepaper

Dropbox

Table of Contents

Table of Contents

Table of Contents

Dropbox Trust Program

Trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you've put in us and take the responsibility of protecting your information seriously. To be worthy of your trust, we built and will continue to grow Dropbox with an emphasis on security, privacy, transparency, and compliance.

The Dropbox Trust Program policy establishes a risk assessment process, which is designed to address environmental, physical, user, third party, applicable laws and regulations, contractual requirements, and various other risks that may affect system security, confidentiality, integrity, availability, or privacy. Performance reviews occur at least annually. More information about the Dropbox Trust Program is available at: dropbox.com/business/trust.

Dropbox has established a Trust Center to provide self-serve access to information related to the security, privacy, compliance, and reliability of our products. Visit the Trust Center at trust.dropbox.com to learn more.

We follow a multilayered approach to secure the enterprise, infrastructure, applications, and products that impact your organization.

Dropbox has established an information security management framework describing the purpose, direction, principles, and basic rules for how we maintain trust. This is accomplished by assessing risks and continually improving the security, confidentiality, integrity, availability, and privacy of the Dropbox for Teams systems. We regularly review and update security policies, provide security training, perform application and network security testing (including penetration testing), monitor compliance with security policies, and conduct internal and external risk assessments.

Our policies

We've established a thorough set of security policies that are enforced by the Dropbox Security Team. All security policies are reviewed and approved at least annually. Employees, interns, and contractors participate in mandatory security training when joining the company and through ongoing security awareness education.

- ***Information security***

  Keeping user and Dropbox information secure.

- ***Authentication***

  Describes how Dropbox employees authenticate themselves to access information systems and data.

- ***Device security***

  The minimum security requirements for mobile devices used to access company information.

- ***Logical access control***

  Keeping access to Dropbox systems, users, and information secure. Covers access control to both corporate and production environments.

- ***Data security***

  Describes how Dropbox protects data through specific storage, access, and use requirements.

- ***Travel security***

  Describes what Dropbox employees should do before traveling overseas.

- ***Sales and Customer Experience (CX) security guidelines***

  Keeping user information secure, protecting our employees, and providing support to our users.

- ***Physical security***

  Maintaining a safe and secure environment for people and property at Dropbox.

- ***Production physical security guidelines***

  Managing physical access to production facilities.

- ***Incident response***

  Outlines the way Dropbox handles reported security, privacy, and site events and documents incident response plans for each.

- ***Unauthorized copyrighted materials***

  Prohibiting employees from using Dropbox or Dropbox systems to store or share unauthorized content.

- ***Change management***

  Managing changes to production systems. Intended for all Dropbox employees, contractors, and interns with access to systems.

- ***User data privacy***

  Protecting and handling user information and user data at Dropbox in compliance with our Privacy Policy.

- ***Business continuity policy and emergency management***

  Describes preservation, protection, and the safety of people (Dropbox employees), property, and (business) processes.

- ***Dropbox Privacy Program***

  The purpose, principles, and accountability for the Dropbox Privacy Program.

- ***Dropbox Trust Program***

  Describes how Dropbox operates and is Worthy of Trust.

- ***Payments environment security***

  Securing and maintaining the dedicated payments environment used at Dropbox in order to accept credit card payments.

Dedicated and experienced security team

Our security program is designed to assess risks and build a culture of security at Dropbox. Every single employee at Dropbox is dedicated to security and protecting our customer data in all that we do. All products and services are in alignment with the information security program in place under the Head of Security at Dropbox. As part of our formal risk management program, security risks are reviewed periodically, resulting in security-related initiatives at the product, infrastructure, and company level.

The Privacy Team is responsible for operating the Privacy Program. They implement our key privacy initiatives and champion privacy-by-design in our data lifecycle.

To ensure all Dropbox employees are able to foster customer data protection, we work to ensure security and privacy are embedded in our company culture from day one. Employees undergo comprehensive background checks, sign and follow a code of conduct and acceptable use policies, and undergo annual security awareness and privacy training. Continuous information security awareness is maintained via monthly information security newsletters and security relevant notifications.

Employee policy, personnel security, and access

Upon hire, each Dropbox employee is required to complete a background check, sign a security policy acknowledgment and non-disclosure agreement, and receive security training. Only individuals that have completed these procedures are granted physical and logical access to the corporate and production environments, as required by their job responsibilities. In addition, all employees are required to complete annual security and privacy training, and they receive regular security awareness training via informational emails, talks and presentations, and resources available on our intranet.

Employee access to the Dropbox environment is maintained by a central directory and authenticated using a combination of strong passwords, passphrase-protected SSH keys, and two-factor authentication. Remote access requires the use of VPN protected with two-factor authentication, and any special access is reviewed and vetted by the Security team. Access to corporate and production networks is strictly limited based on defined policies. For example, production network access is SSH key-based and restricted to engineering teams requiring access as part of their duties. Firewall configuration is tightly controlled and limited to a small number of administrators.

In addition, our internal policies require employees accessing production and corporate environments to adhere to best practices for the creation and storage of SSH private keys. Access to other resources, including data centers, server configuration utilities, production servers, and source code development utilities is granted through explicit approval by appropriate management. A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals.

Dropbox employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about user accounts. In order to protect end user privacy and security, only a small number of engineers responsible for developing core Dropbox services have access to the environment where user files are stored. Employee access is promptly removed when an employee leaves the company.

As Dropbox products and services become an extension of our customers' infrastructure, they can rest assured that we are responsible custodians of their data. See the Privacy section for more details.

Security training & awareness

We empower our software development teams with the best practices and techniques for building secure applications. In an ever-evolving digital landscape, ensuring the security of our software is of paramount importance, and we are committed to equipping our teams with the knowledge and skills needed to safeguard our products and protect our users.

Corporate offices

- ***Physical security***

  The Dropbox Physical Security Team is responsible for enforcing physical security policy and overseeing the security of our offices.

- ***Visitor and access policy***

  Physical access to corporate facilities, other than public entrances and lobbies, is restricted to authorized Dropbox personnel and registered visitors who are accompanied by Dropbox personnel. A badge access system ensures only authorized individuals have access to restricted areas within the corporate facilities.

- ***Server access***

  Access to areas containing corporate servers and network equipment is restricted to authorized personnel via elevated roles granted through the badge access system. The lists of authorized individuals approved for physical access to corporate and production environments are reviewed at least quarterly.

Vulnerability management

Our security team carries out regular automated and manual security testing and patch management, and works with third-party specialists to identify and remediate potential security vulnerabilities and bugs.

As a necessary component of our information security management system, findings and recommendations that result from all of these assessments are communicated to Dropbox management, evaluated, and appropriate action is taken, as determined to be necessary. Issues with high severity are documented, tracked, and resolved by assigned security engineers.

Physical security

Infrastructure

Physical access to sub-service organization facilities where production systems reside is restricted to personnel authorized by Dropbox, as required to perform their job function. Any individuals requiring additional access to production environment facilities are granted that access through explicit approval by appropriate management.

A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals. Once approval is received, an authorized member of the infrastructure team will contact the appropriate sub-service organization to request access for the approved individual. The sub-service organization enters the user's information into their own system and grants the approved Dropbox personnel badge access and, if possible, biometric scan access. Once access is granted to approved individuals, it is the data center's responsibility to ensure that access is restricted to only those authorized individuals.

Notes:

Dropbox for Teams, Dropbox Sign, and Dropbox DocSend services utilize Amazon Web Services for SaaS and IaaS, which operates state-of-the-art facilities independently evaluated by third-party assurance assessments (e.g., SOC 1, SOC 2, ISO 27001). Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Additionally, PaaS through Heroku, which services Dropbox DocSend, is also independently evaluated by third-party assurance assessments (e.g., SOC 1, SOC 2, ISO 27001).

Further detail on the AWS Compliance Program can be found here.

Incident response

We have incident response policies and procedures to address service availability, integrity, security, privacy, and confidentiality issues. As part of our incident response procedures, we have dedicated teams who are trained to:

- Promptly respond to alerts of potential incidents.
- Determine the severity of the incident.
- If necessary, execute mitigation and containment measures.
- Communicate with relevant internal and external stakeholders, including notification to affected customers to meet breach or incident notification contractual obligations and to comply with relevant laws and regulations.
- Gather and preserve evidence for investigative efforts.
- Document a postmortem and develop a permanent triage plan.

The incident response policies and processes are audited as part of our SOC 2, ISO/IEC 27001, and other security assessments.

Infrastructure security

Dropbox uses off-the-shelf and custom services hosted on Dropbox and AWS infrastructure. AWS is operated with shared responsibility between Dropbox and AWS. Logical and network security of AWS infrastructure is provided by AWS.

Note: Currently, all AWS infrastructure used for Dash is located within the United States and is distributed across multiple availability zones. As product development progresses for Dash and as customer demand expands, additional worldwide regions may be added to support data residency requirements.

Network security

Dropbox diligently maintains the security of our back-end network. Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We employ industry-standard protection techniques, including firewalls, network vulnerability scanning, network security monitoring, and intrusion detection systems to ensure only eligible and non-malicious traffic is able to reach our infrastructure.

Our internal private network is segmented according to use and risk level. The primary networks are:

- Internet-facing DMZ
- Priority infrastructure DMZ
- Production network
- Corporate network
- Dropbox services and applications are isolated via containers when possible

Access to the production environment is restricted to authorized IP addresses and requires multi-factor authentication on all endpoints. IP addresses with access are associated with the corporate network or approved Dropbox personnel. Authorized IP addresses are reviewed on a quarterly basis to ensure a secure production environment. Access to modify the IP address list is restricted to authorized individuals.

Traffic from the internet destined to our production network is protected using multiple layers of firewalls and proxies.

Strict limitation is maintained between the internal Dropbox network and the public internet. Internet-bound traffic to and from the production network is carefully controlled through a dedicated proxy service and this, in turn, is protected by restrictive firewall rules.

Dropbox instruments sophisticated tool sets to monitor laptops and desktops with Mac and Windows operating systems, and production systems, for malicious events. Security logs are collected in a centralized location for forensic and incident response following the industry standard retention policy.

Dropbox identifies and mitigates risks via regular network security testing and auditing by both dedicated internal security teams and third-party security specialists.

Points of Presence (PoPs)

To optimize website performance for users, Dropbox leverages third-party content delivery networks (CDNs) and Dropbox-hosted points of presence (PoPs) in 31 locations around the world. No user data is cached at these locations, and all user data being transferred is encrypted with SSL/TLS. Physical and logical access to Dropbox-hosted PoPs are restricted to authorized Dropbox personnel only. Dropbox performs optimizations at both the transport (TCP) layer and the application (HTTP) layer.

Peering

Dropbox has an open peering policy, and all customers are welcome to peer with us. For details, please see dropbox.com/peering.

Security monitoring

Dropbox uses cloud native security platforms to monitor the security of its production environment and actively monitors for suspicious user activity. This includes direct alert escalation for Dropbox Security.

Reliability

When you're doing business, you need us to be there for you. That's why we strive to hit the highest uptime possible. We develop Dropbox products and services with multiple layers of redundancy to guard against data loss and ensure availability.

Data centers and managed service providers

Dropbox corporate and production systems are housed at third-party sub-service organization data centers and managed service providers located in different regions of the United States. Sub-service organization data center SOC reports and / or vendor security questionnaires and contractual obligations are reviewed at a minimum annually for sufficient security controls. These third-party service providers are responsible for the physical, environmental, and operational security controls at the boundaries of Dropbox infrastructure. Dropbox is responsible for the logical, network, and application security of our infrastructure housed at third-party data centers.

Our managed service provider for processing and storage, Amazon Web Services (AWS), is responsible for the logical and network security of Dropbox services provided through their infrastructure. Connections are protected through their firewall, which is configured in a default deny-all mode. Dropbox restricts access to the environment to a limited number of IP addresses and employees.

Dash's intelligent data analysis and decisioning capabilities are powered by the ElasticSearch platform, which provides a complete managed SaaS solution with security demonstrated through their ISO certification and SOC attestation reports.

Infrastructure in Germany, Australia, Japan, and the United Kingdom

Dropbox offers storage of file blocks in regions outside the United States for qualified customers. Our infrastructure is hosted by Amazon Web Services (AWS) in Germany, Australia, Japan, and the United Kingdom and replicated within the respective region to ensure redundancy and protect against data loss. File metadata is stored in the United States on Dropbox's proprietary servers. Paper docs and previews are currently stored in the United States for all customers.

Business continuity

Dropbox has established a business continuity management system (BCMS) to address how to resume or continue providing services to users—as well as how to function as a company—if business-critical processes and activities are disrupted. We conduct a cyclic process consisting of the following phases:

- ***Business impact and risk assessments***

  We conduct a business impact assessment (BIA) at least annually to identify processes critical to Dropbox, assess the potential impact of disruptions, set prioritized timeframes for recovery, and identify our critical dependencies and suppliers. We also conduct a company-wide risk assessment at least annually. The risk assessment helps us systematically identify, analyze, and evaluate the risk of disruptive incidents to Dropbox. Together, the risk assessment and BIA inform continuity priorities, and mitigation and recovery strategies for business continuity plans (BCPs).

- ***Business continuity plans***

  Teams identified by the BIA as critical to Dropbox's continuity use this information to develop BCPs for their critical processes. These plans help the teams know who is responsible for resuming processes if there's an emergency, who in another Dropbox office or location can take over their processes during a disruption, and which methods for communications should be used during a continuity event. These plans also help prepare us for a disruptive incident by centralizing our recovery plans and other important information, such as when and how the plan should be used, contact and meeting information, important apps, and recovery strategies. Dropbox's continuity plans are tied into our company-wide crisis management plan (CMP), which establishes Dropbox's crisis management and incident response teams.

- ***Plan testing/exercising***

  Dropbox tests selected elements of its business continuity plans at least annually. These tests are consistent with the BCMS's scope and objectives, are based on appropriate scenarios, and are well-designed with clearly defined aims. The tests may range in scope from tabletop exercises to full-scale simulations of real-life incidents. Based on the results of the testing, as well as experience from actual incidents, teams update and improve their plans to address issues and strengthen their response capabilities.

- ***Review and approval of BCMS***

  At least annually, our executive staff reviews the BCMS as part of reviewing Dropbox's Trust Program.

Disaster recovery

The company is aware that disasters can strike at any time and in any region or location. The infrastructure is designed for resilience and contingency plans are in place in case of service-impacting events. We use Amazon Web Services (AWS), which is dispersed across multiple data centers for data and processing redundancy. Critical data related to the system is backed up on a daily basis. Engineering is notified in the event of backup failure and issues are resolved as appropriate.

To address information security requirements during a major crisis or disaster impacting Dropbox for Teams operations, we maintain a disaster recovery plan. The Dropbox Engineering Team reviews this plan annually and tests selected elements at least annually. Relevant findings are documented and tracked until resolution.

Our Disaster Recovery Plan (DRP) addresses both durability and availability disasters, which are defined as follows:

- A durability disaster consists of one or more of the following:
  - A complete or permanent loss of a primary data center that stores metadata, or of multiple data centers that store file blocks.
  - Lost ability to communicate or serve data from a data center that stores metadata, or from multiple data centers that store file content.
- An availability disaster consists of one or more of the following:
  - An outage greater than 10 days.
  - Lost ability to communicate or serve data from a storage service / data center that stores metadata, or from multiple storage services / data centers that store file blocks.

We define a Recovery Time Objective (RTO), which is the duration of time and a service level in which business process or service must be restored after a disaster, and a Recovery Point Objective (RPO), which is the maximum tolerable period in which data might be lost from a service disruption. We also measure the Recovery Time Actual (RTA) during Disaster Recovery testing, which is performed at least annually.

Dropbox incident response, business continuity, and disaster recovery plans are subject to being tested at planned intervals and upon significant organizational or environmental changes.

Application security

Scanning and security penetration testing (internal and external)

Our security team performs automated and manual application security testing on a regular basis to identify and patch potential security vulnerabilities and bugs on our desktop, web, and mobile applications.

All Dropbox applications are fully integrated with the Dropbox Application Security program. We perform design and architecture reviews of new features through our intake process. All Dropbox code is scanned for security related issues using static code analysis tools like Semgrep & CodeScan.

Additionally, Dropbox contracts with third-party vendors to perform periodic penetration and vulnerability tests on the production environment. We work with third-party specialists, other industry security teams, and the security research community to keep our applications secure. We also leverage automatic analysis systems to identify vulnerabilities. This process includes systems that we develop internally, open source systems we modify for our needs, as well as external vendors we hire for continuous automated analysis.

Keeping harmful content off Dropbox

We have scanning capabilities that aim to prevent the storage and distribution of harmful content in Dropbox. Our scanners leverage home grown technology as well as cutting edge capabilities from partners, such as Microsoft and Google, to make Dropbox a safe place for our customers.

Bug bounties

While we work with professional firms for penetration testing engagements and conduct our own testing in-house, bug bounties (or vulnerability rewards programs) tap into the expertise of the broader security community. Our bug bounty program provides an incentive for researchers to identify and responsibly disclose software bugs. This involvement of the external community provides our security team with independent scrutiny of our applications to help keep users safe. We strive to be among the industry leaders in bounty rewards, as well as response and remediation times.

We've established a scope for eligible submissions and Dropbox applications, as well as a responsible disclosure policy that promotes the discovery and reporting of security vulnerabilities to increase user safety. This policy sets forth the following guidelines:

- Share the security issue with us in detail.
- Please be respectful of our existing applications. Spamming forms through automated vulnerability scanners will not result in any bounty or award since those are explicitly out of scope.
- Give us reasonable time to respond before making any information about the security issue public.
- Do not access or modify user data without permission of the account owner.
- Do not view, alter, save, store, transfer, or otherwise access the data, and immediately purge any local information upon reporting the vulnerability to Dropbox.
- Act in good faith to avoid privacy violations, destruction of data, and interruption or degradation of our services (including denial of service).

Issues can be reported by submitting a report to Bugcrowd at: bugcrowd.com/dropbox.

Data protection and encryption

Data in transit / Data transfers

To protect data in transit between Dropbox apps and our servers, Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a Dropbox for Teams client (currently desktop, mobile, API, or web) and the hosted service is encrypted via SSL/TLS. For the Dash client and modern browsers, we use strong ciphers and on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security

(HSTS) with include SubDomains enabled. Similarly, Paper doc data in transit between a Paper client (currently mobile, API, or web) and the hosted services is encrypted via SSL/TLS.

For Dropbox Sign and DocSend, documents are stored behind a firewall and authenticated against the sender's session every time a request for that document is made. In addition, each document is encrypted with a unique key. As an additional safeguard, each key is encrypted with a regularly-rotated master key. This means that even if someone were able to bypass physical security and remove a hard drive, they wouldn't be able to decrypt your data.

For endpoints we control (desktop and mobile) and modern browsers, we use strong ciphers and support perfect forward secrecy and certificate pinning. Additionally, on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS) with includeSubDomains enabled.

Note: Dropbox uses TLS exclusively and has deprecated the use of SSLv3 due to known vulnerabilities. However, TLS is frequently referred to as "SSL/TLS," so we use that designation here.

To prevent attacker-in-the-middle attacks, authentication of Dropbox front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the transfer of any files or Paper docs to help ensure secure delivery to Dropbox front-end servers.

Data at rest

Dropbox files uploaded by users are encrypted at rest using 256-bit Advanced Encryption Standard (AES). Files are stored in multiple data centers in discrete file blocks. Each block is fragmented and encrypted using a strong cipher. Only blocks that have been modified between revisions are synchronized. Paper docs at rest are also encrypted using 256-bit Advanced Encryption Standard (AES). Paper docs are stored across multiple availability zones using third-party systems.

Key management

The Dropbox key management infrastructure is designed with operational, technical, and procedural security controls with very limited direct access to keys. Encryption key generation, exchange, and storage is distributed for decentralized processing. Key management services are designed with operational, technical, and procedural security controls.

- ***File encryption keys***

  By design, Dropbox manages file encryption keys on behalf of users to remove complexity, and enable advanced product features and strong cryptographic control. File encryption keys are created, stored, and protected by production system infrastructure security controls and security policies.

- ***Internal SSH keys***

  Access to production systems is restricted with unique SSH key pairs. Security policies and procedures require protection of SSH keys. An internal system manages the secure public key exchange process, and private keys are stored securely. Internal SSH keys cannot be used to access production systems without a separate second factor for authentication.

- ***Key distribution***

  Dropbox automates the management and distribution of sensitive keys to systems that are required for operations.

Certificate pinning

Dropbox uses certificate pinning on our desktop and mobile clients. Certificate pinning is an extra check to ensure that our clients will only connect to servers with digital certificates from an authorized list of certificate authorities. We use it to guard against nation-state attackers in control of a rogue certificate authority, as well as to protect you from local malware that may be hijacking your connections.

Protecting authentication data

Dropbox goes beyond regular hashing to protect the login credentials of users. In keeping with industry best practices, each password is salted with a randomly generated, unique per-user salt, and we use iterative hashing to slow computation. These practices help protect against brute force, dictionary, and rainbow attacks. As an added precaution, we encrypt the hashes with a key stored separately from the database, which helps to keep passwords secure in the event of a database-only compromise.

Malware scanning

We've developed an automated system that scans for malware at the point that any content is shared outside of the origin user's account. The system leverages both proprietary technology and industry-standard detection engines and is designed to stop malware from being spread.

Product Security

Design reviews

The security team at Dropbox integrates security review into the product roadmap, so every major release has undergone threat models and design reviews in order to deliver a secure experience for our users.

Secure deployment

As part of our software development lifecycle, whenever new Dropbox application features are added to our codebase, the code is first analyzed and scanned for code quality and security flaws. Features must pass this review process, including peer evaluation, before it is deemed ready for release.

Change management

All development, issue remediation, and patch processes follow our formal Change Management Policy, which is defined by the Dropbox Engineering team to ensure that system changes have been tested and authorized prior to implementation in the production environments. Source code changes are initiated by developers who want to make an improvement to the Dropbox application or service. Changes are stored in a version control system and are required to go through automated Quality Assurance (QA) testing procedures to verify that security requirements are met. Successful completion of QA procedures leads to implementation of the change. QA-approved changes are automatically implemented in the production environment. Our software development lifecycle (SDLC) requires adherence to secure coding guidelines, as well as screening of code changes for potential security issues via our QA and manual review processes. Changes released into production are logged and archived, and alerts are automatically sent to Dropbox Engineering team management.

Changes to Dropbox infrastructure are restricted to only authorized personnel. The Dropbox Security team is responsible for maintaining infrastructure security and ensuring that the servers, firewalls, and other security-related configurations are kept up-to-date and compliant with industry standards. Firewall rule sets, and individuals with access to production servers, are reviewed regularly.

Data privacy

Individuals and organizations trust Dropbox with their most important work every day, and it is our responsibility to protect this information. At Dropbox we believe that you own your data, and we're committed to keeping it private. Our Privacy Policy clearly describes how we handle and protect your information. On an annual basis, our independent third-party auditors test our privacy-related controls and provide their reports and opinions which we can provide to you upon request. For more information about our privacy practices and principles, please see the Privacy and Data Protection Whitepaper.

To report a privacy-related issue, please contact: privacy@dropbox.com.

Dropbox for Teams

Digital transformations continue to take hold across multiple industries and it's vital that data, teams, and devices are protected wherever they are. Organizations that rely on cloud solutions like Dropbox for Teams to enable remote and distributed workflows need to streamline collaboration, proactively manage cloud risks, and implement effective controls that ensure confidentiality of intellectual property (IP), integrity of stored and shared data, and availability of data through managed and resilient cloud services.

Over 575,000 businesses and organizations rely on Dropbox for Teams as the solution for remote and distributed teams to collaborate securely. The core Dropbox for Teams solution includes the smart workspace for collaboration, and file sync and share capabilities. Our solutions are backed by industry-leading infrastructure as well as features for advanced enterprise security, team & content security, electronic signature, secure transfer, and data governance. Except where noted, the information in this whitepaper applies to all Dropbox for Teams products. Paper is a feature of Dropbox for Teams.

At the core of Dropbox for Teams is our comprehensive security program—the Dropbox Trust Program—that takes a multilayered approach to security, which is essential as global approaches to remote work evolve.

This whitepaper details Dropbox for Teams product security capabilities, Dropbox's operational security measures, our privacy and transparency commitment as well as back-end policies, and independent certifications and regulatory compliance measures that make Dropbox the secure solution for your organization.

Except where noted, the information in this whitepaper applies to all Dropbox for Teams. Paper is a feature of Dropbox for Teams.

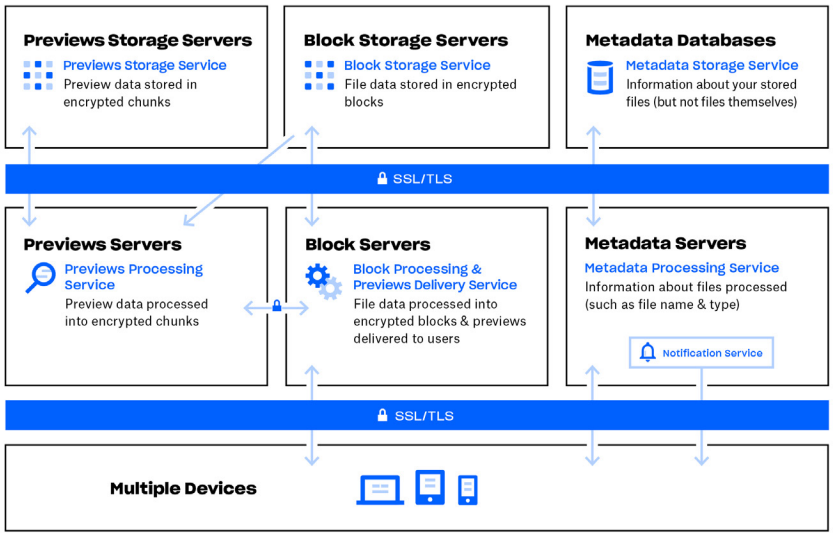
Under the hood

Our easy-to-use interfaces are backed by an infrastructure working behind the scenes to ensure fast, reliable syncing, sharing, and collaboration. To make this happen, we continually improve our product and architecture to speed data transfer, improve reliability, and adjust to changes in the environment. In this section, we'll explain how data is transferred, stored, and processed securely.

File infrastructure

Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

Dropbox's file infrastructure is comprised of the following components:



- ***Metadata servers***

  Certain basic information about user data, called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, which helps support features like version history, recovery, and sync.

- ***Metadata databases***

  File metadata is stored in a transactional key value store with multi-version concurrency control and is sharded and replicated as needed to meet performance and high availability requirements.

- ***Block servers***

  By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. Block Servers process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the Block Servers of the change, and new or modified file blocks are processed and transferred to the Block Storage Servers. In addition, Block Servers are used to deliver files and previews to users. For detailed information on the encryption used by these services both in transit and at rest, please see Data protection and encryption.

- ***Block storage servers***

  The actual contents of user files are stored in encrypted blocks with the Block Storage Servers. Prior to transmission, the Dropbox client splits files into file blocks in preparation for storage. The Block Storage Servers act as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.

- ***Previews servers***

  The Previews Servers produce previews of files. Previews are a rendering of a user's file in a different file format that is more suited for fast display on an end user's device. Previews Servers retrieve file blocks from the Block Storage Servers to generate previews. When a file preview is requested, the Previews Servers retrieve the cached preview from the Previews Storage Servers and transfer it to the Block Servers. Previews are ultimately provided to users by Block Servers.

- ***Previews storage servers***

  Cached previews are stored in an encrypted format in the Previews Storage Servers.

- ***Notification service***

  This separate service monitors whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the Metadata Servers securely to synchronize any changes.

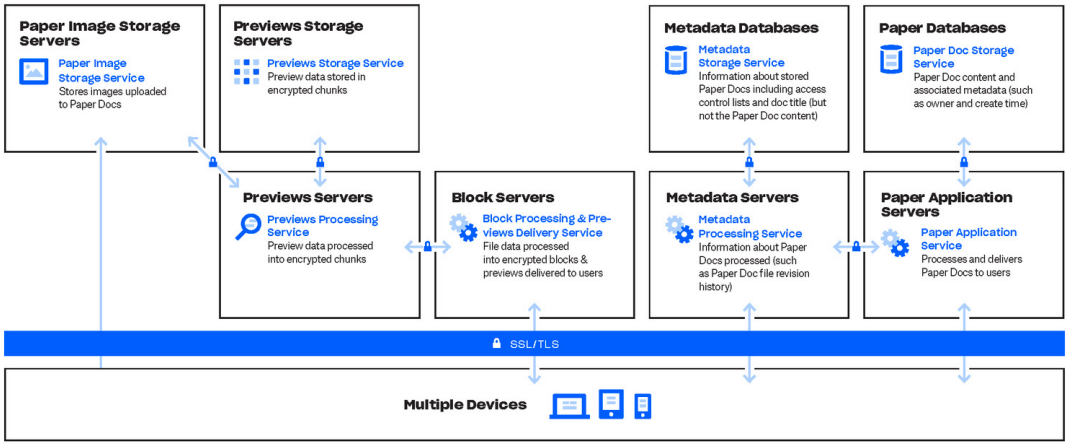
File data storage

Dropbox primarily stores two kinds of file data: metadata about files (such as the date and time a file was last changed) and the actual contents of files (file blocks). File metadata is stored on Dropbox servers. File blocks are stored in one of two systems: Amazon Web Services (AWS) or Magic Pocket, Dropbox's in-house storage system. Magic Pocket consists of both proprietary software and hardware and has been designed from the ground up to be reliable and secure. In both Magic Pocket and AWS, file blocks are encrypted at rest, and both systems meet high standards for reliability. For more details, please see Reliability.

Paper infrastructure

Dropbox users can access Paper docs at any time from the web and mobile clients, or through third-party applications connected to the Dropbox Paper application. All of these clients connect to secure servers to provide access to Paper docs, allow doc sharing with others, and update linked devices when docs are added, changed, or deleted.

Dropbox Paper's infrastructure is comprised of the following components:



- ***Paper application servers***

  The Paper Application Servers process user requests, render the output of edited Paper docs back to the user, and perform notification services. Paper Application Servers write inbound user edits to the Paper Databases, where they are placed in persistent storage. Communication sessions between the Paper Application Servers and Paper Databases are secured with Secure Hypertext Transfer Protocol (HTTPS).

- ***Paper databases***

  The actual contents of users' Paper docs, as well as certain metadata about these Paper docs, are encrypted in persistent storage on the Paper Databases. This includes information about a Paper doc (such as the title, owner, create time, and other information) as well as content within the Paper doc itself, including comments and tasks. The Paper Databases are sharded and replicated as needed to meet performance and high availability requirements.

- ***Metadata servers***

  Paper uses the same Metadata Servers described in the Dropbox infrastructure diagram to process information about Paper docs, such as Paper doc file revision history and shared folder membership. Dropbox directly manages the Metadata Servers, which are located in third-party, co-located data centers.

- ***Metadata databases***

  Paper uses the same Metadata Databases described in the Dropbox infrastructure diagram to store information related to Paper docs, such as sharing, permissions, and folder associations. Paper doc metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements.

- ***Paper image storage servers***

  Images uploaded to Paper docs are stored and encrypted at rest on the Paper Image Storage Servers. Transmission of image data between the Paper Application and Paper Image Storage Servers occurs over an encrypted session.

- ***Previews servers***

  The Previews Servers produce previews both for images uploaded to Paper docs, as well as hyperlinks embedded within Paper docs. For images uploaded to Paper docs, the Previews Servers fetch image data stored in the Paper Image Storage Servers via an encrypted channel. For hyperlinks embedded within Paper docs, Previews Servers fetch the image data and render a preview of the image using encryption as specified by the source link. Previews are ultimately served to users by Block Servers.

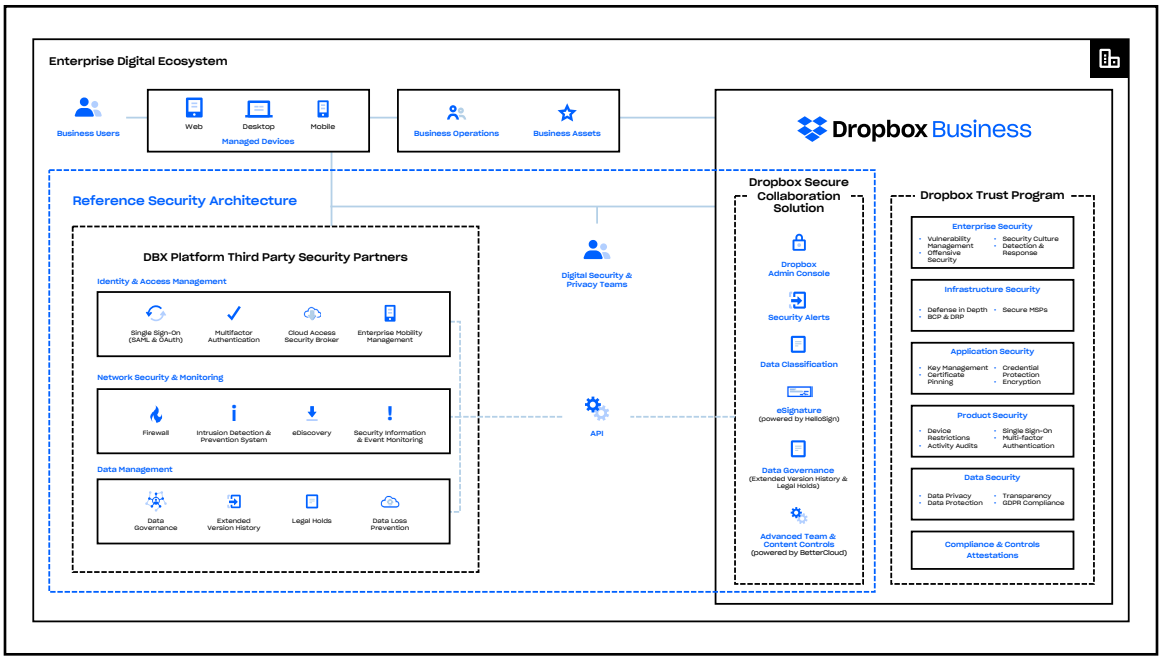
- ***Previews storage servers***

  Paper uses the same Preview Storage Servers described in the Dropbox infrastructure diagram to store cached image previews. Cached preview chunks are stored in an encrypted format in the Previews Storage Servers.

Paper doc storage

Dropbox primarily stores the following kinds of data in Paper docs: metadata about Paper docs (such as a doc's shared permissions) and the actual contents of Paper docs uploaded by the user. These are collectively referred to as Paper doc data, and images uploaded to Paper docs are referred to as Paper image data. Each of these kinds of data is stored in Amazon Web Services (AWS). Paper docs are encrypted at rest in AWS, and AWS meets high standards for reliability. For more details, please see Reliability.

We follow a multilayered approach to secure the enterprise, infrastructure, applications, and products that impact your organization.



Reliability

A storage system is only as good as it is reliable and, to that end, we've developed Dropbox with multiple layers of redundancy to guard against data loss and ensure availability.

File metadata

Redundant copies of metadata are distributed across independent devices within a data center in at least an N+2 availability model. Incremental backups are performed at least hourly, and full backups are performed every 36 hours. Metadata is stored on servers hosted and managed by Dropbox in the United States.

File blocks

Redundant copies of file blocks are stored independently in at least two separate geographic regions and replicated reliably within each region. (Note: For customers who choose to have their files stored in our German, Australian, Japanese or United Kingdom infrastructure, file blocks are replicated within their respective regions only. For more information, see Data centers and managed service providers.) Both Magic Pocket and AWS are designed to provide annual data durability of at least 99.999999999%.

Dropbox's architecture, applications, and sync mechanisms work together to protect user data and make it highly available. In the rare event of a service availability outage, Dropbox users still have access to the latest copies of files that have been synced to the local Dropbox folder on linked computers. Copies of files synced in the Dropbox desktop client / local folder are accessible from a user's hard drive during downtime, outages, or when offline. Changes to files and folders are synced to Dropbox once service or connectivity is restored.

Paper docs

Redundant copies of Paper doc data are distributed across independent devices within a data center in an N+1 availability model. Full backups of Paper doc data are also performed daily. For Paper doc storage, Dropbox uses AWS infrastructure in the United States, which is designed to provide annual data durability of at least 99.999999999%. In the rare event of a service availability outage, users still have access to the latest synced copies of their Paper docs in "offline" mode within the mobile application.

File sync

Dropbox offers industry-recognized, best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox sync is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for end users.

Delta sync

Using this sync method, only modified portions of files are downloaded / uploaded. Dropbox stores each uploaded file in discrete, encrypted blocks and only updates the blocks that have changed.

Streaming sync

Instead of waiting for a file upload to complete, streaming sync will begin downloading synced blocks to a second device before all of the blocks have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.

Saving hard drive space

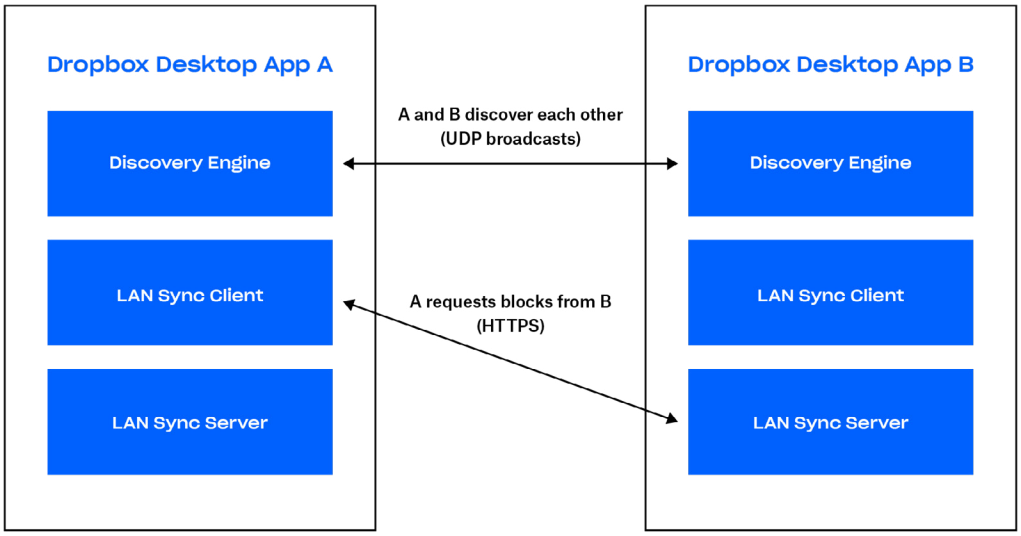
Users can free up storage space on their computers by making only the files they want on their hard drive available offline. This frees up computer space by keeping everything else online-only at dropbox.com.

LAN sync

When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

Architecture

There are three main components of the LAN sync system that run on the desktop app: the discovery engine, the server, and the client. The discovery engine finds machines on the network to sync with. This is limited to machines that have authorized access to the same personal or shared Dropbox folder(s). The server handles requests from other machines on the network, serving the requested file blocks. The client requests file blocks from the network.



Discovery engine

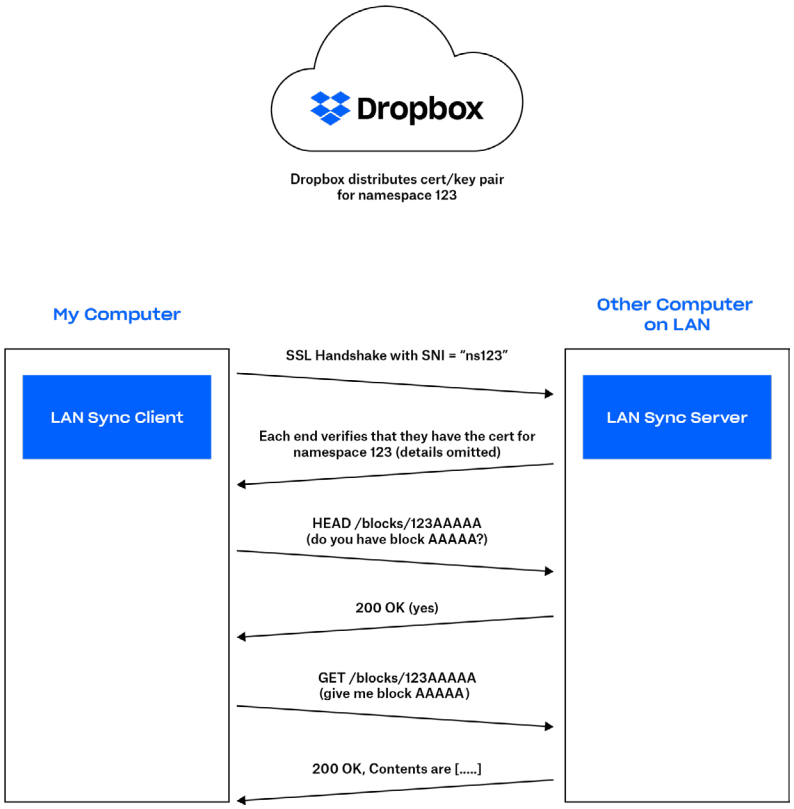
Each machine on the LAN periodically sends and listens for UDP broadcast packets over port 17500 (which is reserved by IANA for LAN sync). These packets contain the version of the protocol used by that computer; the personal and shared Dropbox folders supported; the TCP port that's being used to run the server (which might be different from 17500 if that port is unavailable); and a random identifier for the machine. When a packet is seen, the IP address of the machine is added to a list for each personal or shared folder, indicating a potential target.

Protocol

The actual file block transfer is done over HTTPS. Each computer runs an HTTPS server with endpoints. A client will poll multiple peers to see if they have the blocks, but only download blocks from one server.

To keep all of your data safe, we make sure that only clients authenticated for a given folder can request file blocks. We also make sure that computers cannot pretend to be servers for folders that they do not control. To solve for this, we generate SSL key/certificate pairs for every personal Dropbox or shared folder. These are distributed from Dropbox servers to the user's computers that are authenticated for the folder. The key/certificate pairs are rotated any time membership changes (for example, when someone is removed from a shared folder). We require both ends of the HTTPS connection to authenticate with the same certificate (the certificate for the Dropbox or shared folder). This proves that both ends of the connection are authenticated.

When making a connection, we tell the server which personal Dropbox or folder we are trying to connect to by using Server Name Indication (SNI) so that the server uses the correct certificate.



Server/client

With the protocol described above, the server needs only know which blocks are present and where to find them.

Based on the results of the discovery engine, the client maintains a list of peers for each personal Dropbox folder and shared folder. When the LAN sync system gets a request to download a file block, it sends a request to a random sample of the peers that it has discovered for the personal Dropbox or shared folder, and then requests the block from the first one responding that it has the block.

To avoid latencies, we use connection pools to allow us to reuse already-started connections. We don't open a connection until it is needed and, once it is open, we keep it active in case we need it again. We also limit the number of connections to any single peer.

If a file block is not found or downloaded successfully, or if the connection turns out to be too slow, the system falls back to getting the block from Dropbox servers.

Dropbox user interfaces

The Dropbox service can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect user data while ensuring ease of access.

- ***Web***

  This interface can be accessed through any modern web browser. It allows users to upload, download, view, and share their files. The web interface also allows users to open existing local versions of files through their computer's default application.

- ***Desktop***

  The Dropbox desktop application is a powerful sync client that stores files locally for offline access. It gives users full access to their Dropbox accounts, and runs on Windows and Mac operating systems. Files are viewed and can be shared directly within operating system file browsers.

- ***Mobile***

  The Dropbox app is available for iOS and Android devices, allowing users to access all of their files on the go. The mobile app also enables users to make files available for offline access.

- ***API***

  Dropbox APIs provide a flexible way to read and write to Dropbox user accounts as well as access advanced functionality like search, revisions, and restoring files. The APIs can be used to manage the user lifecycle for a Dropbox for Teams account, perform actions on all members of a team, and enable access to Dropbox for Teams admin functionality.

Paper user interfaces

The Paper service can be utilized and accessed through a number of interfaces. Each has security settings and features that process and protect user data while ensuring ease of access.

- ***Web***

  This interface can be accessed through any modern web browser. It allows users to create, view, edit, download, and share their Paper docs.

- ***Mobile***

  The Paper mobile application is available for iOS and Android mobile devices and tablets, allowing users to access all their Paper docs on the go. The mobile application is built as a hybrid application consisting of native code (iOS or Android) wrapped around an internal webview browser.

- ***API***

  The Dropbox API described above contains endpoints and data types for managing documents and folders in Dropbox Paper, including support for functionality such as permissions management, archive, and permanent deletion.

Apps for Dropbox

The DBX Platform is composed of a robust ecosystem of developers who build on top of our flexible Application Programming Interfaces (APIs). More than 750,000 developers have built applications and services on the platform for productivity, collaboration, security, administration, and more.

Pre-built components

The Chooser, Saver, and Embedder are pre-built web and mobile components that allow easy access to Dropbox in third-party apps/sites in just a few lines of code.

- The Chooser enables selection of files from Dropbox.
- The Saver allows users to save files directly to Dropbox.
- The Embedder allows users to view files and folders from Dropbox.

The authorization to these components is entirely through Dropbox. Apps are granted access to files selected by the choose through Dropbox shared links or short lived download links. These pre-built components may be used independently, or in conjunction with the API, described below.

Dropbox for Teams API integrations

The public Dropbox API allows third-party developers the ability to access and interact with Dropbox within their applications. This includes file and metadata interaction, sharing, and team functionality.

Authorization

Dropbox uses OAuth, an industry-standard protocol for authorization, to allow users to grant apps account access without exposing their account credentials. We support OAuth 2.0 for authenticating API requests; requests are authenticated through the Dropbox website or mobile app. Dropbox supports OAuth best practices, including short-lived access tokens and PKCE for distributed apps.

User permissions

Apps using the Dropbox API can be built with the following level of content access to an end user's Dropbox:

- ***App folder***

  A dedicated folder named after the app is created within the Apps folder of a user's Dropbox. The app receives read and write access to this folder only and users can provide content to the app by moving files into this folder. In addition, the app may request file / folder access via the Chooser or Saver.

- ***Full Dropbox***

  The app receives full access to all the files and folders in a user's Dropbox, and may also request file / folder access via the Chooser or Saver.

Applications may also request specific scopes, restricting their behaviors by access to subsets of API endpoints. For example, applications may be limited to read-only access of files—or the ability to upload content, but not to create shares.

Team permissions

Administrators of Dropbox for Teams may authorize applications to administration functionality found in the team's admin console. The actions team linked apps are able to perform are limited through scopes, specifying what team settings the app may read or manage.

Common combinations of scopes combinations include:

- ***Team information***

  Read-only information about the team and high-level usage.

- ***Team auditing***

  Read-only access to team info and the detailed event log.

- ***Team member file access***

  The ability to perform actions on behalf of users on the team, such as managing their files and folders.

- ***Team member management***

  Adding and removing members to and from the team.

Webhooks

Webhooks are a way for web apps to get real-time notifications about changes in a user's Dropbox. Once a URI is registered to receive webhooks, an HTTP request will be sent to that URI every time there's a change for any of the app's registered users. Using the Dropbox for Teams API, webhooks can also be used to generate notifications about changes to team membership. Many security apps use webhooks to help admins track and manage team activities.

Extensions

Apps may register extension URIs, enabling actions to appear in the 'Share' and 'Open' menus in the Dropbox UI. Extensions allow users to kick off custom third-party workflows directly from a file in a Dropbox surface. When an action is triggered, Dropbox will redirect users to the URI specified, passing a file identifier that can be used with the API to perform any file operation. An app needs to be authorized before a registered extension is visible to the user. We may promote a select set of extension integrations in the 'Share' and 'Open' menus, though these apps won't have access to content until the user authorizes it.

Dropbox developer guidelines

We provide a number of guidelines and practices to help developers create API apps that respect and protect user privacy while enhancing users' Dropbox experience.

- ***App keys***

  For each distinct app a developer writes, a unique Dropbox app key must be used. In addition, if an app provides services or software that wrap the DBX Platform for other developers to use, each developer must also sign up for their own Dropbox app key.

- ***App permissions***

  Developers are instructed that an app should use the least privileged permission it can. When a developer submits an app for production status approval, we review to ensure that the app doesn't request an unnecessarily broad permission based on the functionality provided by the app.

- ***App review process***

  - **Development status**
    When a Dropbox API app is first created, it is given development status. The app functions the same as any production status app, except that it can only be linked with up to 500 total Dropbox users. Once an app links 50 Dropbox users, the developer has two weeks to apply for and receive production status approval before the app's ability to link additional Dropbox users will be frozen.

  - **Production status and approval**
    In order to receive production status approval, all API apps must adhere to our developer branding guidelines and Terms & Conditions, which include prohibited uses of the DBX Platform. These uses include: promoting IP or copyright infringement, creating file sharing networks, and downloading content illegally. Developers are first prompted for additional information regarding their app's functionality, and how it uses the Dropbox API before submitting for review. Once the app is approved for production status, any number of Dropbox users can link to the app.

Team app administration

Inside the team administration console, administrators of Dropbox for Teams may manage linked apps and integrations for their team.

API partnerships

Dropbox has worked closely with its technology partners to enable them to develop integrations with their popular software packages. These partners build applications using Dropbox APIs, working closely with Dropbox architects to follow best security and UX practices. These include a variety of end user productivity apps, as well as security and management tools such as:

- ***Security information and event management (SIEM) and analytics***

  Connect your Dropbox for Teams account to SIEM and analytics tools to monitor and evaluate user sharing, sign-in attempts, admin actions, and more. Access and manage employee activity logs and security-relevant data through your central log management tool.

- ***Data loss prevention (DLP)***

  Automatically scan file metadata and content to trigger alerts, reporting, and actions when important changes are made in your Dropbox for Teams account. Apply company policies to your Dropbox for Teams deployment and help meet regulatory compliance requirements.

- ***eDiscovery and legal hold***

  Respond to litigation, arbitration, and regulatory investigations with data from your Dropbox for Teams account. Search for and collect relevant electronically stored information, and preserve your data through the eDiscovery process, saving your business time and money.

- ***Digital rights management (DRM)***

  Add third-party content protection for sensitive or copyrighted data stored in employee accounts. Gain access to powerful DRM features including client-side encryption, watermarking, audit trails, access revocation, and user / device blocking.

- ***Data migration and on-premises backup***

  Migrate data to Dropbox from existing servers or other cloud-based solutions, saving time, money, and effort. Automate backups from your Dropbox for Teams account to on-premise servers.

- ***Identity management and single sign-on (SSO)***

  Automate the provisioning and de-provisioning process and speed up onboarding for new employees. Streamline management and bolster security by integrating Dropbox for Teams with an existing identity system.

- ***Custom workflows***

  Build in-house apps that integrate Dropbox into existing business processes to enhance their internal workflows.

See the Dropbox App Integrations page for a list of these technology partners. End users may discover select 1st and third-party apps & integrations in the App Center.

Dropbox integrations

We have also worked with some of our top technology partners to build integrations featured in Dropbox surfaces. These deeper integrations are co-developed by Dropbox & the partner. These include:

Dropbox extensions

These integrations let you use various types of app extensions to seamlessly perform actions, like publishing a video, adding files to emails and chats, sending a file for eSignature, and more, right from Dropbox. These applications are built by the partner, while Dropbox facilitates discovery of select Extension partners through 'Open with' and 'Share with' menus.

Slack

This integration is built 1st party by Dropbox, enabling users to start Slack conversations from within Dropbox. End users authenticate to Slack via OAuth.

Microsoft Office for mobile and web

Our Microsoft Office integrations allow users to open Word, Excel, and PowerPoint files stored in their Dropbox; make changes in the Office mobile or web apps; and save those changes directly back to Dropbox. Users are prompted to grant access on the first attempt to open a Dropbox file in each Office mobile app or any Office web app. Subsequent launches will retain these links.

Adobe Acrobat and Acrobat Reader

Our integrations with the desktop and mobile (Android and iOS) versions of these apps enable users to view, edit, and share PDFs stored in their Dropbox. Users are prompted to grant access on the first attempt to open a Dropbox file in each app. Changes to PDFs are saved back to Dropbox automatically.

Product security

Dropbox provides administrative control and visibility features that empower both IT and end users to effectively manage and secure data. With Dropbox, you get everything you need for work—your tools, content, and collaborators—all in one place. Dropbox is more than secure storage—it's a smart, seamless way to optimize your existing workflow.

Below are highlights of features available to admins and users, as well as third-party integrations for managing core IT processes.

Note: Availability of features varies by subscription plan. See dropbox.com/business/plans for details.

Content controls

Protecting sensitive business assets—such as intellectual property (IP) and personally identifiable information (PII)—is crucial to IT and data security teams. From granular content permissions to data retention policies and legal holds, Dropbox provides industry-leading solutions to manage, monitor, and protect your content. Below are the key Dropbox products and features that support content control.

Granular content permissions and shared file and folder permissions

- ***Permissions for shared files***

  A team member who owns a shared file can remove access for specific users and disable commenting for the file.

- ***Permissions for shared files***

  A team member who owns a shared folder can remove folder access for specific users, change view/edit permissions for specific users, and transfer folder ownership. Depending on the team's global sharing permissions, each shared folder's owner might also be able to control whether it can be shared with people outside the team, whether others with edit permissions can manage membership, and whether links can be shared with people outside of the folder.

- ***Passwords for shared links***

  Any shared link can be protected with an owner-defined password. Before any file or folder data is transmitted, an access control layer verifies that the correct password has been submitted and all other requirements (such as team, group, or folder ACL) have been met. If so, a secure cookie is stored in the user's browser to remember that the password was verified previously. With sharing controls, admins can also set default passwords, instead of having them as optional, to better safeguard their team's content.

- ***Expirations for shared links***

  Users can set an expiration for any shared link to provide temporary access to files or folders. With sharing controls, admins can also set default expirations, instead of having them as optional, to better safeguard their team's content.

Paper doc and shared Paper folder permissions

- ***Permissions for Paper docs and shared Paper folders***

  A team member who owns a Paper doc or shared Paper folder can remove access for specific users and disable editing for the Paper doc.

- ***Permissions for Paper docs***

  A team member who owns a Paper doc can remove access for specific users who are explicitly listed in the share panel. Both the owner and editors of a Paper doc can change view / edit permissions for specific users as well as change the link policy of the doc. The link policy governs which users can open the doc and the permissions granted to them. The team admin can set team-wide policies for links and doc sharing.

- ***Permissions for Paper folders***

  A team member who is a member of the folder can change the sharing policy of the folder and remove access for specific users that had been explicitly added to the folder.

File and folder actions

- ***Team folders for files***

  Admins can create team folders that automatically give groups and other collaborators the correct access level (view or edit) to the content they need.

- ***Granular access and sharing controls***

  Sharing controls let admins manage membership and permissions at the top level or subfolder level so that people and groups inside and outside the company have access to specific folders only.

- ***Team folder manager***

  Admins can view all their team folders and customize sharing policies from a central place to help prevent mis-sharing of confidential materials.

- ***Shared folders for Paper docs***

  Admins can create shared Paper folders that automatically give other collaborators the correct access level—comment or edit—to the content they need.

- ***Remote wipe***

  When employees leave the team or in the event of device loss, admins can remotely delete Dropbox data and local copies of files. Files will be removed from both computers and mobile devices when they come online and the Dropbox application is running.

- ***Account transfer***

  After deprovisioning a user (either manually or via directory services), admins can transfer files and ownership of Paper docs created by the former team member from that user's account to another user on the team. The account transfer feature can be used while removing a user or at any time after deleting a user's account.

The following capabilities are available as add-on features (contact Sales for more information).

- ***Scan content***

  With the Advanced Team and Content Controls add-on, Dropbox for Teams Advanced and Enterprise customers can scan for new and existing content in Dropbox to locate and avoid data vulnerabilities.

- ***Set up and trigger customized workflows***

  With the Advanced Team and Content Controls add-on, admins can take customizable actions against files that violate company policies.

- ***Set up alerts***

  Admins can monitor security concerns in real-time and avoid data vulnerabilities. Get alerts on files being shared externally and sensitive data scanned.

Content visibility

Security alerts and notifications

Administrators on Dropbox Enterprise can receive real-time notifications when abusive activities, risky activity, or potential data leaks are detected on their accounts. The following events can be monitored:

- Mass deletions
- Mass data moves
- Sensitive content shared externally
- Malware shared from outside your team
- Malware shared within your team
- Too many failed sign-in attempts
- Sign-in from a high-risk country
- Ransomware detection

Dropbox also provides the ability to configure alert thresholds, adjust notification recipients, and trigger alerts when folders with sensitive files are shared externally. Admins can also mark alerts as reviewing, resolved, or dismissed. Additionally, a dashboard widget shows overall team alert insights and trends for the past week.

External sharing report and page

Dropbox is providing additional visibility with external sharing report and page. Admins can create a report from either the insights page or the external sharing page. The report will list all of the team's files and folders that are shared outside their team and all shared links. The external sharing page is an additional page in the Admin Console that allows admins to see and filter (file type, who shared, link settings, and many more) through the files and folders shared directly out of team and shared links.

Sharing controls

Sharing settings give team admins more control over the sharing and access to their team's content. Admins can set team-level default expirations, password restrictions, or both. These restrictions reduce risk of data loss by removing the responsibility from the users to set restrictions.

Data classification

Teams on Dropbox Enterprise can have personal and sensitive data automatically labeled to better protect it from being exposed. Admins will receive data loss prevention (DLP) alerts via email and in the Admin Console when files or folders saved within team folders containing sensitive information are shared outside their team. Admins have the ability to automatically identify and classify sensitive data stored in shared folders and personal team member folders. Dropbox Enterprise admins can activate automatic data classification from the Admin Console.

Data governance add-on

Data Governance is the overall set of processes, technologies, and teams that come together to manage and protect an organization's data assets. This includes the ability to store, identify, discover, and retrieve corporate data, as needed.

The Dropbox Data Governance Add-on bundles a set of features that allows organizations to better control and secure their data, while reducing risks and costs associated with meeting regulatory and compliance needs. Currently, this add-on includes four key features for team admins and compliance admins.

- ***Extended version history***

  Your default file version history depends on the type of Dropbox account you have. However, with Dropbox for Teams, you can purchase an Extended Version History (EVH) add-on separately or as part of the Data Governance Add-On bundle that allows recovery of any file deleted or changed in the last 10 years.

- ***Legal holds***

  Placing a legal hold on a team member allows team and compliance admins to view and export content that's been created or modified by that member. Members affected by a legal hold will not be notified of the hold and will still maintain their permissions to create, edit, and delete files.

- ***Data retention***

  Data retention enables teams and compliance admins to prevent accidental deletion of content that is required by regulations to be held for a certain amount of time. This feature will allow customers retain data past 10 years from latest "revision" date.

- ***Data disposition***

  Data disposition enables team and compliance admins to permanently delete data at a specified date to comply with data retention and disposition requirements. Admins can monitor activity by receiving reports alerting them of upcoming file deletions.

Recovery and version control

Dropbox for Teams customers have the ability to restore deleted files and Paper docs, as well as recover previous versions of files and Paper docs, ensuring changes to important data can be tracked and retrieved.

Data security on mobile devices

- ***Erase data***

  For additional security, a user can enable the option to erase all Dropbox data from the device after 10 failed passcode attempts.

- ***Internal storage and offline files***

  By default, files are not stored on the internal storage of mobile devices. Dropbox mobile clients feature the ability to save individual files and folders to the device for offline viewing. When a device is unlinked from a Dropbox account, via either the mobile or web interface, those files and folders are automatically deleted from the device's internal storage.

- ***Offline Paper docs***

  When a device is unlinked from Paper, via the Dropbox account security page, the user is logged out, and offline Paper docs are automatically deleted from the device's internal storage.

Team controls

No two organizations are exactly alike, so we've developed a number of tools that empower admins to customize Dropbox for Teams to their teams' particular needs. Dropbox for Teams includes tools for end users to further protect their accounts and data. The authentication, recovery, logging, and other security features below are available through the various Dropbox user interfaces.

Below are several control and visibility features available via the Dropbox for Teams Admin Console.

Granular content permissions

- ***Tiered admin roles***

  Dropbox offers tiered admin roles to enable more effective team management. Account admins can be assigned one of three access levels. There is no limit to the number of admins a team can have, and any team member can be assigned an admin role.

- ***Team admin***

  Can set team-wide security and sharing permissions, create admins, and manage members. The team admin has all available admin permissions. Only team admins can assign or change admin roles, and there must always be at least one team admin on a Dropbox for Teams account.

- ***User management admin***

  Can address most team management tasks, including adding and removing team members, managing groups, and viewing a team's activity feed.

- ***Support admin***

  Can address common service requests from team members, like restoring deleted files or helping team members locked out of two-step verification. Support admins can also reset non-admin passwords and export an activity log for a specified team member.

- ***Billing admin***

  Can access billing pages in the admin console.

- ***Content admin***

  Can create & manage team folders within the Content Manager.

- ***Report admin***

  Can create reports within the Admin Console and has access to the Activity page.

- ***Security admin***

  Can manage security alerts, external sharing, and security risks.

- ***Compliance admin (only available for teams with the Data Governance add-on)***

  Can manage Data Governance pages (legal holds, data retention, and data disposition) and also access Content Manager.

- ***Groups***

  Teams can create and manage lists of members within Dropbox and easily give them access to specific folders. Dropbox can also sync Active Directory groups using the Active Directory Connector.

- ***Company-managed groups***

  Only admins can create, delete, and manage the membership for this type of group. Users cannot request to join or leave a company-managed group.

- ***User-managed groups***

  Admins can choose whether users can create and manage their own groups. Admins can also change a user-managed group to a company-managed group at any time to take control of it.

- ***Restricting multiple accounts on computers***

  Admins can block team members from linking a second Dropbox account to computers that are linked to their work Dropbox account.

- ***Suspended user state***

  Admins have the ability to disable a user's access to their account while preserving their data and sharing relationships to keep company information safe. Admins can later reactivate or delete the account.

- ***Sign in as user***

  Team admins can sign in as members of their teams. This gives admins direct access to the files, folders, and Paper docs in team member accounts so that they can make changes, share on behalf of team members, or conduct audits of file-level events. "Sign in as user" events are recorded in the team's activity log, and admins can determine whether members are notified of these events.

- ***Sharing permissions***

  Team admins have comprehensive control of their team's sharing abilities using Dropbox, including whether:

  - Team members can share files and folders with people outside the team.
  - Team members can edit folders owned by people outside the team.
  - Shared links created by team members will work for people outside the team.
  - Team members can create file requests and collect files from team members and / or people outside the team.
  - People can view and make comments on files owned by the team.
  - Team members can share paper docs and paper folders outside of the team.
  - Permanent delete permissions are granted.

The team admin of a Dropbox for Teams account can limit the ability to permanently delete files and Paper docs to team admins only.

Onboarding and user provisioning

User provisioning and identity management methods

- ***Email invitation***

  A tool in the Dropbox for Teams Admin Console allows administrators to manually generate an email invitation.

- ***Active Directory***

  Dropbox for Teams administrators can automate the creation and removal of accounts from an existing Active Directory system via our Active Directory connector or a third-party identity provider. Once integrated, Active Directory can be used to manage membership.

- ***Single sign-on (SSO)***

  Dropbox for Teams can be configured to allow team members access by signing into a central identity provider. Our SSO implementation, which uses the industry-standard Security Assertion Markup Language 2.0 (SAML 2.0), makes provisioning easier and more secure by placing a trusted identity provider in charge of authentication and giving team members access to Dropbox without an additional password to manage. Dropbox has also partnered with leading identity management providers so that users can be provisioned and de-provisioned automatically. Please see Dropbox for Teams API integrations.

- ***API***

  The Dropbox for Teams API can be used by customers to build custom user provisioning and identity management solutions. Please see Dropbox for Teams API integrations.

Two-step verification

This highly recommended security feature adds an extra layer of protection to a user's Dropbox account. Once two-step verification is enabled, Dropbox will require a six-digit security code in addition to a password upon sign-in or when linking a new computer, phone, or tablet.

- Admins can choose to require two-step verification for all team members or just specific ones.
- Account administrators can track which team members have two-step verification enabled.
- Dropbox two-step authentication codes can be received via text message or apps which conform to the Time-Based One-Time Password (TOTP) algorithm standard.
- In the event a user cannot receive security codes via these methods, they may opt to use a 16-digit, one-time-use emergency backup code. Alternately, they may use a secondary phone number to receive a backup code via text message.
- Dropbox also supports the open standard FIDO Universal 2nd Factor (U2F), which enables users to authenticate with a USB security key they've set up instead of a six-digit code.

Enterprise installer

Admins requiring scaled provisioning can use our enterprise installer for Windows to install the Dropbox desktop client silently and remotely via managed-software solutions and deployment mechanisms.

Managed devices and log-in

- ***Enterprise mobility management (EMM)***

  Dropbox integrates with third-party EMM providers to give admins of Dropbox for Teams on an Enterprise plan more control over how team members use Dropbox on mobile devices. Admins can restrict mobile app usage for Dropbox Enterprise accounts to just managed devices (whether company-provided or personal), gain visibility into app usage (including available storage and access locations), and remote wipe a lost or stolen device. Please note that the Paper mobile app is not manageable by EMM.

- ***Device approvals***

  Dropbox enables admins of Dropbox for Teams on the Advanced and Enterprise plans to set limits on the number of devices that a user can sync with Dropbox, and to choose whether approvals are user-managed or admin-managed. Admins can also create an exception list of users that are not restricted to a certain number of devices. Please note that the Paper mobile app is not included in device approvals.

- ***Two-step verification requirement***

  Admins can choose to require two-step verification for all team members or just specific members. Other multi-factor authentication requirements can be enforced through the team's SSO implementation.

- ***Password control***

  Admins of Education, Advanced, and Enterprise teams can require members to set and maintain strong, complex passwords for their accounts. When this feature is enabled, team members will be signed out of any web sessions and required to create new passwords when they sign in. A built-in tool analyzes the strength of passwords by comparing them against a database of commonly used words, names, patterns, and numbers. A user entering a common password is prompted to come up with something more unique and difficult to guess. Admins can also reset passwords for the entire team or on a per-user basis.

- ***Domain management***

  Dropbox provides a set of tools for companies to simplify and speed up the process of onboarding users and controlling Dropbox usage.

  - **Domain verification**
    Companies can claim ownership of their domains and unlock the other domain management tools.

  - **Invite enforcement**
    Admins can require individual Dropbox users who have been invited to the company's Dropbox team to migrate to the team or change the email address on their personal account.

- **Domain insights**
  Admins are able to see key information, such as how many individual Dropbox accounts are using company email addresses.

- **Account capture**
  Admins can force all Dropbox users using a company email address to join the company's team or change the email address on their personal account.

- ***Web session control***

  Admins can control how long team members can stay signed in to dropbox.com. Admins can limit the duration of all web sessions and / or sessions that are idle. Sessions reaching these limits will be signed out automatically. Admins can also track and terminate the web sessions of individual users.

- ***App access***

  Admins have the ability to view and revoke third-party app access to user accounts.

- ***Unlink devices***

  Computers and mobile devices connected to user accounts can be unlinked by the admin through the Admin Console or the user through individual account security settings. On computers, unlinking removes authentication data and provides the option to delete local copies of files the next time the computer comes online (see Remote wipe). On mobile devices, unlinking removes files marked as favorites, cached data, and sign-in information. Unlinking also removes offline Paper docs from the Paper mobile application. If two-step verification is enabled, users must re-authenticate any device upon relinking. Additionally, users' account settings provide the option to send a notification email automatically when any devices are linked.

- ***Network control***

  Admins of Dropbox for Teams on an Enterprise plan can restrict Dropbox usage on the company network to only the Enterprise team account. This feature integrates with the company's network security provider to block any traffic that exists outside of the sanctioned account on computers. Please note that Paper is not currently managed through network control.

Mobile security

- ***Fingerprint scanning***

  Users can enable Touch ID or Face ID on iOS devices and Fingerprint unlock (where supported) on Android devices as a method to unlock the Dropbox mobile app.

Access visibility

- ***Technical support identity verification***

  Before any troubleshooting or account information is provided by Dropbox Support, the account admin must provide a one-time use, randomly-generated security code to validate his or her identity. This PIN is only available through the admin console.

User account activity

Each user can view the following pages from their account settings to obtain up-to-date information regarding their own account activity.

- ***Sharing page***

  This page shows the shared folders that are currently in the user's Dropbox, as well as shared folders the user can add. A user can unshare folders and files and set sharing permissions.

- ***Files page***

  This page shows the files that have been shared with the user and the date each file was shared. The user has the option to remove their access to these files. To see Paper docs that have been shared with the user by others, the user can navigate to the "Shared with me" page within the Paper doc navigation interface.

- ***Links page***

  This page shows all active shared links that the user has created and the creation date for each. It also shows all links shared with the user by others. The user can disable links or change permissions.

- ***Email notifications***

  A user can opt in to receive an email notification immediately when a new device or app is linked to their Dropbox account.

User account permissions

- ***Linked devices***

  The Devices section of a user's account security settings displays all computers and mobile devices linked to the user's account. For each computer, the IP address, country, and approximate time of most recent activity is displayed. A user can unlink any device, with the option to have files on linked computers deleted the next time it comes online.

- ***Active web sessions***

  The Sessions section shows all web browsers currently logged into a user's account. For each, the IP address, country, and login time of the most recent session, as well as the approximate time of most recent activity, is displayed. A user can terminate any session remotely from the user's account security settings.

- ***Linked apps***

  The Apps linked section provides a list of all third-party apps with access to a user's account, and the type of access each app holds. A user can revoke any app's permission to access the user's Dropbox.

Activity feed

Dropbox for Teams records file actions in the team's activity feed, which can be accessed from the Admin Console. The activity feed offers flexible filtering options that enable admins to conduct targeted investigations of account, file, or Paper doc activity. For example, they can view the full history of a file or Paper doc and how users have interacted with it, or view all activity for the team over a specified time period. The activity feed can be exported as a downloadable report in CSV format and also integrated directly into a SIEM (security information and event management) product or other analysis tool through third-party partner solutions. The following content events are recorded in the activity feed:

- ***Sharing for files, folders, and links***

  Where applicable, reports specify whether actions involved people outside the team.

  Shared files

  - Added or removed a team member or non-team member.
  - Changed the permissions for a team member or non-team member.
  - Added or removed a group.
  - Added a shared file to the user's Dropbox.
  - Viewed the content of a file that was shared via a file or folder invitation.
  - Copied shared content to the user's Dropbox.
  - Downloaded shared content.
  - Commented on a file.
  - Resolved or unresolved a comment.
  - Deleted a comment.
  - Subscribed or unsubscribed to comment notifications.
  - Claimed an invitation to a file owned by the team.
  - Requested access to a file owned by the team.
  - Unshared a file.

  Shared folders

  - Created a new shared folder.
  - Added or remove a team member, non-team member, or group.
  - Added a shared folder to the user's Dropbox, or user removed their own access to a shared folder.
  - Added a shared folder from a link.
  - Changed the permissions of a team member or non-team member.
  - Transferred folder ownership to another user.
  - Unshared a folder.
  - Claimed membership to a shared folder.
  - Requested access to a shared folder.
  - Added requesting user to a shared folder.
  - Blocked or unblocked non-team members from being added to a folder.
  - Allowed any team member to add people to a folder or only the owner.
  - Changed group access to a shared folder.

Shared links

- Created or removed a link.
- Made the contents of a link visible to anyone with the link or team members only.
- Made the contents of a link password protected.
- Set or removed an expiration for a link.
- Viewed a link.
- Downloaded the contents of a link.
- Copied the contents of a link to the user's Dropbox.
- Created a link to a file via an API app.
- Shared a link with a team member, non-team member, or group.
- Blocked or unblocked non-team members from viewing links to files in a shared folder.
- Shared an album.

File requests

- Created, changed, closed, or deleted a file request.
- Added users to a file request.
- Added or removed a file request deadline.
- Changed a file request folder.
- Received files via a file request.
- Received files via email to Dropbox.

Individual file and folder events

- Added a file to Dropbox.
- Created a folder.
- Viewed a file.
- Edited a file.
- Downloaded a file.
- Copied a file or folder.
- Moved a file or folder.
- Renamed a file or folder.
- Reverted a file to a previous version.
- Rolled back changes in files.
- Restored a deleted file.

- Deleted a file or folder.
- Permanently deleted a file or folder.

Successful and failed logins

- Successful or failed login attempt.
- Failed login attempt or error via single sign-on (SSO).
- Failed login attempt or error via EMM.
- Logged out.
- Change of IP address for web session.

Passwords

Changes to password or two-step verification settings. Admins do not have visibility into users' actual passwords.

- Changed or reset password.
- Enabled, reset, or disabled two-step verification.
- Set up or changed two-step verification to use SMS or a mobile app.
- Added, edited, or removed a backup phone for two-step verification.
- Added or removed a security key for two-step verification.

Membership

Additions to and removals from the team.

- Invited a team member.
- Joined the team.
- Removed a team member.
- Suspended or unsuspended a team member.
- Recovered a removed team member.
- Requested to join the team based on account domain.
- Approved or declined a request to join the team based on account domain.
- Sent domain invites to existing domain accounts.
- User joined the team in response to account capture.
- User left domain in response to account capture.
- Blocked or unblocked team members from suggesting new team members.
- Suggested a new team member.

Apps

Linking of third-party apps to Dropbox accounts.

- Authorized or removed an application.
- Authorized or removed a team application.

Devices

Linking computers or mobile devices to Dropbox accounts.

- Linked or unlinked a device.
- Used remote wipe and successfully deleted all files or failed to delete some files.
- Change of IP address for desktop computer or mobile device.

Admin actions

Changes to settings in the admin console, such as shared folder permissions.

- ***Authentication and single sign-on (SSO)***
  - Reset team member's password.
  - Reset all team members' passwords.
  - Blocked or unblocked team members from disabling two-step verification.
  - Enabled or disabled SSO.
  - Made sign-in via SSO required.
  - Changed or removed the SSO URL.
  - Updated the SSO certificate.
  - Changed the SSO identity mode.
- ***Membership***
  - Blocked or unblocked users from requesting to join the team based on account domain.
  - Set team membership requests to be automatically approved or require manual admin approval.
- ***Member account management***
  - Changed a team member's name.
  - Changed a team member's email address.
  - Gave or removed admin status, or changed the admin role.
  - Signed in or signed out as a team member.
  - Transferred or deleted the contents of a removed member's account.
  - Permanently deleted the contents of a removed member's account.

- ***Global sharing settings***
  - Blocked or unblocked team members from adding shared folders owned by non-team members.
  - Blocked or unblocked team members from sharing folders with non-team members.
  - Turned on warnings that are shown to users before they share folders with non-team members.
  - Blocked or unblocked non-team members from viewing shared links.
  - Set shared links to be team-only by default.
  - Blocked or unblocked people from making comments on files.
  - Blocked or unblocked team members from creating file requests.
  - Added, changed, or removed a logo for shared link pages.
  - Blocked or unblocked team members from sharing Paper docs and Paper folders with non-team members.
- ***Team folder management for files***
  - Created a team folder.
  - Renamed a team folder.
  - Archived or unarchived a team folder.
  - Permanently deleted a team folder.
  - Downgraded a team folder to a shared folder.
- ***Domain management***
  - Attempted to verify or successfully verified a domain, or removed a domain.
  - Dropbox Support verified or removed a domain.
  - Enabled or disabled sending domain invites.
  - Turned on or off “Automatically invite new users”.
  - Changed account capture mode.
  - Dropbox Support granted or revoked account capture.
- ***Enterprise mobility management (EMM)***
  - Enabled EMM for test (optional) mode or deploy (required) mode.
  - Refreshed EMM token.
  - Added or removed team members from EMM excluded users list.
  - Disabled EMM.
  - Created an EMM exception list report.
  - Created an EMM mobile app usage report.
- ***Changes to other team settings***
  - Merged teams.

- Upgraded the team to Dropbox for Teams or downgraded to a free team.
- Changed the team name.
- Created a team activity report.
- Blocked or unblocked team members from having more than one account linked to a computer.
- Allowed all team members or only admins to create groups.
- Blocked or unblocked team members from permanently deleting files.
- Started or ended a Dropbox Support session for a reseller.

Groups

Creation, deletion, and membership information for groups.

- Created, renamed, moved, or deleted a group.
- Added or removed a member.
- Changed a group member's access type.
- Changed group to team-managed or admin-managed.
- Changed the external ID of a group.

Paper activity log

Admins can select a type of Paper activity on the Activity feed or download a full activity report. Paper events are recorded for:

- Paper enabled or disabled.
- Paper doc creation, editing, exporting, archiving, permanent deletion, and restoration.
- Paper doc commenting and resolution of comments.
- Paper doc shared and unshared with team members and non-team members.
- Paper doc access requests from team members and non-team members.
- Paper doc mentions for team members and non-team members.
- Paper doc viewed by team members and non-team members.
- Paper doc followed.
- Paper doc member permission changes (edit, comment, or view only).
- Paper doc external sharing policy changes.
- Paper folder creation, archiving, and permanent deletion.
- Paper doc added to or removed from a folder.
- Paper folder renamed.
- Paper doc and folder transfers.

Key storage

Browser extensions

On web browsers, the user key is stored in the browser extension's local storage area. Browser extension local storage values are only accessible from the extension. Any code running in websites that the user visits cannot read from the browser extension's local storage area. Furthermore, browser extensions disallow execution of any code that is not included in the signed extension package, eliminating the risk of a XSS vulnerability that would access local storage values.

An attacker with unrestricted access to the user's device may access the user key by reading the local storage file on disk. Examples of such threats include: an attacker with physical access to the device or an attacker running malicious malware on the device. To protect against these scenarios, the user is able to configure a local device passphrase.

When a passphrase is configured, the user key is encrypted at rest in the browser extension's local storage. The encryption key is derived from the passphrase through Argon2 password hashing, and the encryption method used is XChaCha20-Poly1305. Each time the browser extension restarts, the user must supply their passphrase to decrypt the user key and unlock their data. Consequently, an attacker without the passphrase cannot decrypt the user key stored in the local storage file on disk.

iOS

On iOS, the user key is stored in the iOS Keychain, which is an encrypted database file on disk. This file is encrypted with a secret key that is stored in the Secure Enclave hardware module, using AES256-GCM as the encryption method. Only the signed Dropbox Passwords iOS app can access the items that it has stored in the keychain. This prevents other code running on the user's device from accessing the user key.

Android

On Android, the user key is stored in an EncryptedSharedPreferences object, which is an encrypted preference file on disk. This file is encrypted with a master key that is stored in the Android Keystore secure hardware, using AES256-GCM as the encryption method. Only the signed Dropbox Passwords Android app can access the master key used to decrypt the preference file.

Local authentication

Dropbox Passwords provides optional local authentication measures to further restrict access to a user's Passwords data on their physical device. For mobile applications, the local OS authentication gesture can be reused (i.e.: a passcode with supplemental biometric authentication). For browser extensions, an optional passphrase can be configured. These mechanisms provide an additional layer of application security when the user's device OS is unlocked. This allows the user to secure their Passwords data when another user may be accessing their device, such as a family member or coworker.

Password strength suggestion

Dropbox built the open-source zxcvbn tool that is used by several password managers to estimate password strength. The tool compares passwords against a database of 30k common passwords, common names and surnames according to US census data, popular English words from Wikipedia and US television and movies, and other common patterns like dates, repeats (aaa), sequences (abcd), keyboard patterns (qwertyuiop), and Leet (1337) Speak. If the password that a user tries to enter is common, the tool prompts them to enter something more unique and difficult to guess. Using the Very strong setting helps ensure the highest level of account security for users.

Dropbox Passwords

Dropbox Passwords is a secure, simple way to store, sync and autofill usernames, passwords, and credit and debit cards across devices so you can protect your online credentials. Dropbox Passwords protects your sensitive online account usernames, passwords, and credit and debit cards with zero-knowledge encryption in the cloud and on your devices. Our products are built for daily use and secure by design.

Zero-knowledge encryption

Dropbox Passwords stores your encrypted data in the cloud but the keys to decrypt that data are only stored on your devices. **Dropbox never has access to them**. These keys are long, random and generated on your device. They never leave your device except when you decide to pair or enroll a new device. This transfer uses public key cryptography to both cryptographically sign and protect the keys during transfer so that you can be confident nobody else can decrypt them while also verifying that they are authentic. This property is frequently called zero-knowledge encryption because the encrypted data is useless to anyone who doesn't have the keys, including Dropbox. This means only you can look at your information and in the unlikely event that Dropbox were hacked, your information would still be safe. The encrypted data is segregated from visible Dropbox folders and cannot be traversed using Dropbox clients or APIs.

Encryption details

Dropbox encrypts your data using XChaCha20-Poly1305 in combined mode for implicit authentication. Our browser extensions and mobile applications all use encryption implementations backed by libsodium, which is an audited and widely-distributed fork of NaCl.

Each encrypt operation generates a random 192-bit nonce, which is stored with the encrypted payload for later decryption. Unlike AES-GCM, XChaCha20-Poly1305 supports random nonces. When decrypting, the 192-bit nonce is read from the payload and used to decrypt the encrypted payload. Any subsequent encryption generates a random 192-bit nonce independent of the previous nonce. Dropbox Passwords generates random numbers using libsodium, which defaults to a cryptographically secure random number generator on each of the platforms that we support.

Keys and recovery words

We generate a 256-bit symmetric key (the encryption key) from 128 bits of entropy (the user key) via Blake2 hashing. This encryption key only stays on its owner's devices, and whenever possible, stays in the most secure storage to which we have access on those devices. For example, on iPhones we store the encryption key in the iOS Keychain.

We use 128 bits of entropy as our source because it offers sufficient security while only requiring 12 recovery words using the BIP-39 standard for backup. BIP-39 provides a human-friendly way of representing large random keys by transforming those keys into a list of 12 words. Any 128-bit key has a corresponding list of words and each list of 12 words uniquely identifies 128 bits. The only caveat is that the 12 words actually correspond to 132 bits so the extra four bits are used as a checksum to identify errors. The recovery words provide a way for you to recover your encryption key in case your device is lost or stolen. We recommend printing them out and storing them in a safe spot. You may also consider giving them to a trusted friend or family member or storing them on a thumb drive.

Device enrollment

When a user signs into Dropbox Passwords on a new device, that device must complete a secure enrollment procedure to access the user's Passwords data. This procedure helps ensure that a user's secret key and Passwords data are accessible only among the user's enrolled devices. It also helps ensure that a user can only enroll additional devices if they have access to an existing enrolled device or their recovery words. The device enrollment procedure occurs as follows.

A new enrolling device randomly generates a 256-bit public/private device key pair, and uploads the public key to the Dropbox server. Then, either scenario **A, B,** or **C** occurs.

A: If the user has not previously enrolled a device, then the enrolling device randomly generates a 128-bit secret user key. Both the user key and device key pair are stored in a secure OS-specific location as described in the following Key Storage section. The device initializes the user's Passwords data, encrypts it, and uploads the encrypted payload to the Dropbox server.

B: If the user has any previously enrolled device(s), then an enrollment approval request is sent to each of those devices. The enrolling device's public key is attached to the request. The user must then approve the request on one of their enrolled devices. If approved, the enrolled device encrypts the user key using its private key and the enrolling device's public key via X25519 ECDH with XSalsa20-Poly1305. The enrolled device uploads the encrypted user key to the Dropbox server to send to the enrolling device. The enrolling device downloads and decrypts the user key using its private key and the enrolled device's public key. The enrolling device then downloads the encrypted Passwords payload data, and decrypts it with the user key.

C: If the user has previously enrolled a device, but can no longer access them, they can enter

their 12 recovery words to locally reconstruct the user key. The enrolling device then downloads the encrypted Passwords payload data, and decrypts it with the user key.

Privacy certifications, attestations, and regulatory compliance

Every day, people and organizations trust Dropbox with their most important work files. Because of this, it's our responsibility to protect those files and keep them private. Our commitment to your privacy is at the heart of every decision we make.

ISO/IEC 27018 (Code of Practice for Protecting Personal Data in the Cloud) and ISO/ IEC 27701 (Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management)

Dropbox for Teams was one of the first major cloud service providers to achieve certification with ISO/IEC 27018 and ISO/IEC 27701.

ISO/IEC 27018 is a global standard for privacy and data protection in the cloud and was published in August 2014 to specifically address user privacy and data protection.

ISO/IEC 27701 is the first certifiable global standard for privacy information management and was published in 2019 to provide a framework for extending the information security management system (ISMS) from ISO/IEC 27001 to a privacy information management system (PIMS) by including data privacy considerations.

The standards lay out many requirements regarding how Dropbox will and will not use your organization's information:

- ***Your organization is in control of your data***

  We only use the personal information you give us to provide you the services you signed up for. You can add, modify, or delete files and Paper docs from Dropbox when you need to.

- ***We'll be transparent about your data***

  We'll be transparent about where your data resides on our servers. We'll also let you know who our trusted partners are. We'll tell you what happens when you close an account or delete a file or Paper doc. Lastly, we'll tell you if any of these things change.

- ***Your data is safe and secure***

  ISO/IEC 27018 and ISO/IEC 27701 were designed as enhancements and extensions to ISO/IEC 27001, one of the most accepted information security standards in the world. We received ISO/IEC 27001 certification renewal in October 2021.

- ***Our practices are reviewed regularly***

  As part of our adherence to ISO/IEC 27018, ISO/IEC 27701, and ISO/IEC 27001, we will undergo annual audits by an independent third party to maintain these certifications. You can view all of our ISO certifications here.

Data transfers

When transferring data from the European Union, the European Economic Area, the United Kingdom, and Switzerland, Dropbox relies upon a variety of legal mechanisms, such as contracts with our customers and affiliates, Standard Contractual Clauses, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the European Commission's adequacy decisions about certain countries, as applicable.

Dropbox complies with the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, as well as the UK Extension to the EU-U.S. Data Privacy Framework, as set forth by the U.S. Department of Commerce regarding the processing of personal data transferred from the European Union, the European Economic Area, the United Kingdom, and Switzerland to the United States. Dropbox has certified to the U.S. Department of Commerce that it adheres to the Principles of these Data Privacy Frameworks with respect to such data, but this does not include the DocSend or FormSwift portions of the Services. If there is any conflict between this Privacy Policy and the Data Privacy Framework Principles, the Principles shall govern. In accordance with the Principles, Dropbox shall remain liable for onward transfers if a processor processes personal data in a manner inconsistent with the Principles. To learn more about the Data Privacy Framework, and to view our certification, visit www.dataprivacyframework.gov.

Complaints and disputes related to our Data Privacy Framework compliance are investigated and resolved through JAMS, an independent third party. To learn more, please see our Privacy Policy (dropbox.com/privacy).

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a 2018 European Union regulation that establishes a comprehensive framework for handling and protecting personal data.

Dropbox is committed to the security and protection of our users' data in line with legal requirements and best practices at all times. In line with our commitment to our users, we have worked hard to ensure that Dropbox is GDPR compliant, including appointing a Data Protection Officer; re-architecting our privacy program to ensure that users can exercise their data subject rights; documenting our data processing activities; and bolstering our internal processes in the event of a security breach. We continue to make adjustments to ensure that, as further guidance continues to emerge from data protection authorities, our process and practices meet or exceed specific elements of the new rules.

EU Cloud Code of Conduct

The EU Cloud Code of Conduct is a voluntary instrument that enables a cloud service provider, such as Dropbox, to demonstrate our commitment to GDPR compliance. Dropbox for Teams, which is comprised of the Standard, Advanced, Enterprise, and Education plans for teams, has been declared adherent to the EU Cloud Code of Conduct and received a Compliance Mark of "Level 2," which means that these services have implemented technical, organizational, and contractual measures in line with the requirements of the Code. For more information about the EU Cloud Code of Conduct and Dropbox's compliance with the code, please visit the Code's official website.

For more information about our privacy practices and policies, please see the Dropbox Privacy and Data Protection Whitepaper.

Compliance

There are various regulatory and industry-specific requirements for security and privacy that your organization may be required to comply with. Our approach is to combine the most accepted standards with compliance measures geared to the specific needs of our customers' businesses or industries.

ISO

The International Organization for Standardization (ISO) has developed a series of world-class standards for information and societal security to help organizations develop reliable and innovative products and services. Dropbox has certified its data centers, systems, applications, people, and processes through a series of audits by an independent third-party, EY CertifyPoint, Netherlands. EY CertifyPoint maintains its ISO accreditations from the Raad voor Accreditatie (Dutch Accreditation Council).

ISO/IEC 27001 (Information Security)

ISO/IEC 27001 is recognized as the premier information security management system (ISMS) standard around the world. The standard also leverages the security best practices detailed in ISO/ IEC 27002. To be worthy of your trust, we're continually and comprehensively managing our physical, technical, and legal controls at Dropbox.

View the Dropbox for Teams ISO/IEC 27001 certificate

ISO/IEC 27017 (Cloud Security)

ISO/IEC 27017 is an international standard for cloud security that provides guidelines for security controls applicable to the provision and use of cloud services. Our Shared Responsibility Guide explains several of the security, privacy, and compliance requirements that Dropbox and its customers can solve together.

View the Dropbox for Teams ISO/IEC 27017 certificate

ISO/IEC 27018 (Cloud Privacy and Data Protection)

ISO/IEC 27018 is an international standard for privacy and data protection that applies to cloud service providers like Dropbox who process personal information on behalf of their customers and provides a basis for which customers can address common regulatory and contractual requirements or questions.

View the Dropbox for Teams ISO/IEC 27018 certificate

ISO/IEC 22301 (Business Continuity)

ISO/IEC 22301 is an international standard for business continuity that guides organizations on how to decrease the probability of disruptive events and respond to them appropriately if they occur by minimizing potential damage. The Dropbox Business Continuity Management System (BCMS) is part of our overall risk management strategy to protect people and operations during times of crises.

View the Dropbox for Teams ISO/IEC 22301 certificate

ISO/IEC 27701 (Privacy Information Management)

ISO 27701 is an international standard for privacy information management. The standard provides a framework to enhance and extend the information security management system under ISO 27001 to a privacy information management system (PIMS). Dropbox for Teams have received this certification as a PII Processor.

View the Dropbox for Teams ISO 27701 certificate

SOC

Service Organization Controls (SOC) Reports, known as SOC 1, SOC 2, or SOC 3, are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox has validated its systems, applications, people, and processes through a series of audits by an independent third-party auditor, Ernst & Young LLP.

SOC 3 for Security, Confidentiality, Integrity, Availability, and Privacy

The SOC 3 assurance report covers all five Trust Services Criteria for Security, Confidentiality, Integrity, Availability, and Privacy (TSP Section 100). The Dropbox general-use report is an executive summary of the SOC 2 report and includes the independent third-party auditor's opinion on the effective design and operation of our controls.

View the Dropbox for Teams SOC 3 examination

SOC 2 for Security, Confidentiality, Integrity, Availability, and Privacy

The SOC 2 report provides customers with a detailed level of controls-based assurance, covering all five Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP Section 100). The SOC 2 report includes a detailed description of Dropbox's processes and more than 100 controls in place to protect your stuff. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control. Our SOC 2 report (sometimes referred to as a SOC 2+ report) also includes an audited mapping of our controls to the ISO standards mentioned above, providing additional transparency to our customers. The SOC 2 examination for Dropbox for Teams is available upon request.

SOC 1 / SSAE 18 / ISAE 3402 (formerly SSAE 16 or SAS 70)

The SOC 1 report provides specific assurances for customers who determine that Dropbox for Teams is a key element of their internal controls over financial reporting (ICFR) program. These specific assurances are primarily used for our customers' Sarbanes-Oxley (SOX) compliance. The independent third-party audit is conducted in accordance with the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). These standards have replaced the deprecated Statement on Standards for Attestation Engagement No. 16 (SSAE16) and Statement on Auditing Standards No. 70 (SAS 70). The SOC 1 examination for Dropbox for Teams is available upon request.

CSA

Cloud Security Alliance: Security, Trust, and Assurance Registry (CSA STAR)

The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly-accessible registry that offers a security assurance program for cloud services, thereby helping users assess the security posture of cloud providers they currently use or are considering contracting with.

Dropbox for Teams have received both the CSA STAR Level 2 Certification and Level 2 Attestation. CSA STAR Level 2 requires a third-party independent assessment of our security controls by EY CertifyPoint (for Certification) and Ernst & Young LLP (for Attestation), based on the requirements of ISO/IEC 27001, SOC 2 Trust Service Criteria, and the CSA Cloud Controls Matrix (CCM) v4.0.2.

View our CSA STAR Level 2 Certification and Attestation on the CSA website

HIPAA/HITECH

Dropbox will sign Business Associate Agreements (BAAs) with Dropbox for Teams customers who require them in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). See Dropbox and HIPAA/HITECH for more information.

Dropbox makes available a third-party assurance report evaluating our controls for the HIPAA/HITECH Security, Privacy, and Breach Notification rules, as well as a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA/HITECH Security and Privacy Rule requirements with Dropbox for Teams.

Customers interested in requesting these documents or learning more about purchasing Dropbox for Teams can reach out to our sales team. If you're currently a Dropbox for Teams team admin, you can sign a BAA electronically from the Account page in the Admin Console.

Please note that the ability to sign an electronic BAA via the Admin Console is available only to US-based customers.

NIST 800-171

The U.S. National Institute of Standards and Technology (NIST) promotes and maintains standards and guidelines to help protect information systems. The NIST Special Publication (SP) 800171 Revision 2 (R2) provides guidelines on protecting Controlled Unclassified Information (CUI) in nonfederal information systems and organizations. Any entity that processes or stores U.S. government CUI, such as research institutions and the education sector, should comply with NIST SP 800-171 R2. Dropbox's CUI systems, processes, and controls were validated by an independent third-party auditor, Ernst & Young LLP.

The NIST SP 800-171 R2 report for Dropbox for Teams is integrated into our SOC 2 report, which is available upon request through our sales team or (for existing Dropbox for Teams customers) support.

Please note that Dropbox Paper is not included in the scope of the NIST SP 800-171 R2 report.

FERPA and COPPA (Students and Children)

Dropbox for Teams allows customers to use the services in compliance with the vendor obligations imposed by the Family Education Rights and Privacy Act (FERPA). Educational institutions with students under the age of 13 can also use Dropbox for Teams consistent with the Children's Online Privacy Protection Act (COPPA), provided that they agree to specific contractual provisions requiring the institution to obtain parental consent regarding the use of our services.

FDA 21 CFR Part 11

Title 21 of the Code of Federal Regulations (CFR) governs food and drugs within the United States for the Food and Drug Administration (FDA), the Drug Enforcement Administration, and the Office of National Drug Control Policy. Part 11 of Title 21 sets forth the criteria under which FDA considers electronic records and signatures to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

Please see our Dropbox and FDA 21 CFR Part 11 Whitepaper and help center article for more information on how Dropbox can help aid in your compliance efforts with 21 CFR Part 11.

PCI DSS

Dropbox is a Payment Card Industry Data Security Standard (PCI DSS) compliant merchant. However, Dropbox for Teams and Dropbox Paper are not meant to process or store credit card transactions. The PCI Attestation of Compliance (AoC) for our merchant status is available upon request.

More information about Dropbox for Teams compliance, visit dropbox.com/business/trust/compliance.

Summary

Dropbox for Teams offers easy-to-use tools to help teams collaborate effectively, while providing the security measures and compliance certifications organizations require. With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses with a powerful solution that can be tailored to their unique needs. To learn more about Dropbox for Teams, contact us at: sales@dropbox.com.

Dropbox Dash

This section describes the version of Dropbox Dash for individual users. For information about Dropbox for teams and businesses, see Dash for Business Security.

Dropbox Dash is AI-powered universal search that helps speed up the way you work across all your applications. Dash learns and evolves with you, getting better the more you use it.

Dash's intelligent connection to your applications allows you to find, organize, and take action on content and information. Finding content is easy via the web browser extension installed on your Windows or MacOS device. Flexible organization of your content from any connected applications allows you to group items into Stacks, matching how you work versus the rigid file structures and data silos of the past. Dash will provide smart recommendations based on topic and usage to help with Stack creation and curation.

As content is found via Dash or organized with Stacks, both solutions become an easy platform to launch right to that referenced content or solution. Natural language queries will provide rich answers based upon the aggregate context of your information.

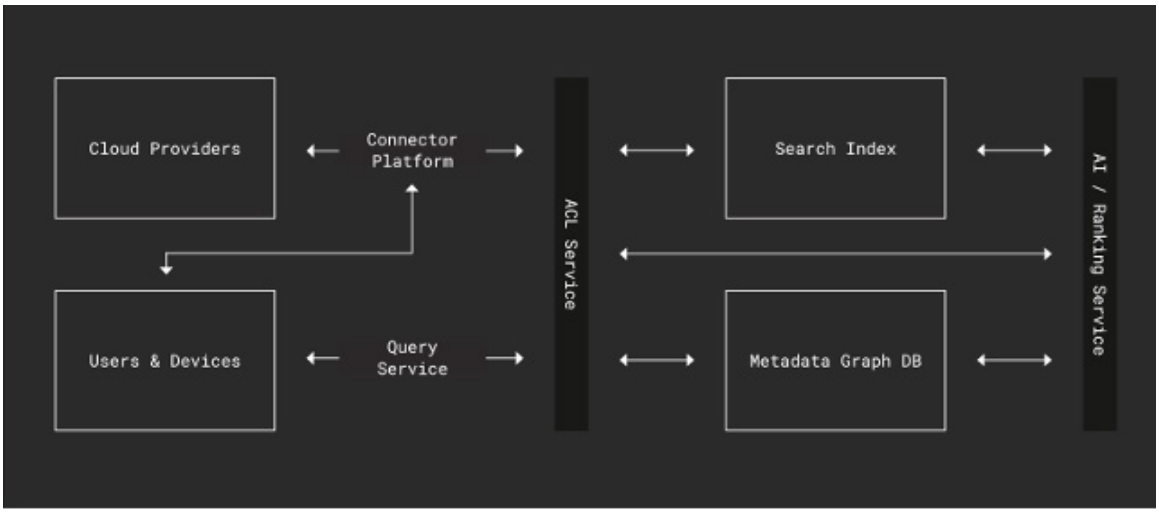
Encryption

Databases that store content from the Dash client or integrated applications are encrypted using FIPS 140-2, Level 3 cryptographic services provided by AWS Key Management Service (KMS) and key management processes built and managed by Dropbox.

Under the hood

Dropbox Dash is backed by an infrastructure designed to ensure fast, reliable search and secure protection of your content. To make this happen, we continually improve our product and architecture to speed responses, improve reliability, and adjust to changes in the environment. Dash uses a modern stack comprised of off-the-shelf and custom services hosted on Amazon Web Services (AWS) infrastructure.

Dropbox Dash's infrastructure is comprised of the following major components:



Connector platform

To allow search across all your applications, Dash has pre-built integrations for modern productivity and business applications, such as Google Workspace, Salesforce, Microsoft Outlook, etc. These integrations are HTTP/REST-based, encrypted API connections and are authorized either via API keys or an OAuth 2.0 authorization flow that grants Dash access to acquire and index data associated to the application. The connector platform optimizes content retrieval from multiple sources through efficient connection pooling. It intelligently prioritizes the connectors based on their significance or specific criteria, ensuring efficient content access.

Search and metadata databases

Once an integration has been established to an application, metadata and the data itself, will be ingested to these databases, which are logically separated, sharded, and replicated as needed to meet performance and high availability requirements.

AI / Ranking service

In order to provide relevant returns for queries from the user, Dash will utilize AI to rank metadata and content on multiple categories and dimensions. Dash constructs a knowledge graph based on the content the user has access to and their interactions, enabling it to construct valuable insights and patterns. The Dash AI models leverage the user's knowledge graph and personalized engagement to rank and score the results. The ranking will be based on recency, relationship between content, and usage patterns of the users and team members. Our AI Principles guide our teams as we develop AI products and features responsibly.

ACL service

To ensure partitioning and to maintain tenancy of the data/indices, permission and access are acquired when data is acquired from connected services. The ACL service contains data permission metadata that is matched and validated prior to returning a response, which ensures that only authorized results are returned to the user.

Query service

This service brokers requests from the user or supporting applications to initiate the search.

Users & devices

Dash provides support for modern operating systems and browsers allowing the end user to initiate searches for data that has been indexed from the device or integrated applications. A browser extension, which is installed with the Dash client, allows browsing history to be intelligently surfaced along with other relevant content on a browser start page.

Connector data storage

Data is stored on AWS infrastructure and leverages redundancies built into AWS. Our connector infrastructure leverages RDS, with multi-AZ redundancy and failover within a region and full data snapshots are created daily. Additional, non-critical data is stored in AWS S3, which has 11 9's of durability.

Natural Language services

Dash is capable of processing and responding queries posed in everyday language form, from within the standard Dash user interface. Dash uses aggregated information relevant to each individual user to be able to provide a curated response to queries that come up in the normal course of business, reducing time spent in looking for the correct content.

Application security

Dash user interfaces

Dash can be utilized and accessed through a Web browser extension or the dash.ai web site. Each has security settings and features that process and protect user data while ensuring ease of access.

Web browser extension

The Dash browser extension is currently supported by Chrome and Edge browsers. It allows users to easily re-retrieve content and has smart stacks which intelligently groups related content together and makes suggestions so users always have the right content, at the right time.

Desktop

The Dash desktop application is a powerful universal search client enabling users to seamlessly search through their data across multiple platforms. It runs on Windows and Mac operating systems, and allows users to connect a variety of data sources and use a highly customizable interface to locate content.

Integrations

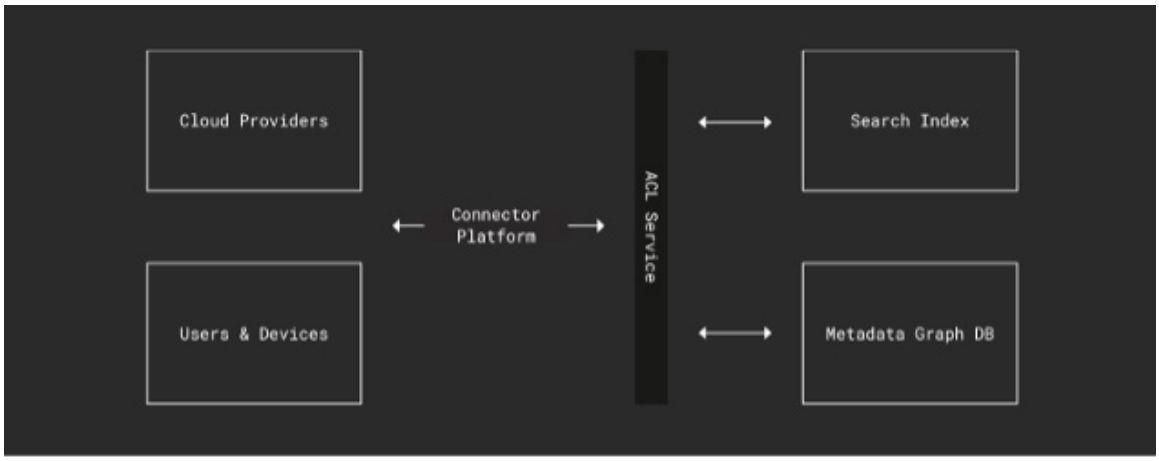
Dropbox Dash has created and partnered with solution providers to create a library of connectors that allow you to integrate modern SaaS applications and other information resources. Generally, each connector uses public APIs of those applications and authorization to the APIs is granted by an administrator or a user via oAuth 2.0. Certain applications will allow an administrator for Dash to create the integration from a future version of the Dropbox Dash Admin Console. Applications like Gmail and Outlook require that individual users create the integration, which can be done during initial Dash setup or from the Dropbox Dash client on Windows or MacOS.

Once this integration is complete, the Dropbox Dash connector platform connects to the integrated SaaS application to acquire content based on a known data schema for the service. Permissions and access controls for that content are acquired and this metadata is stored in our ACL service. A periodic refresh of both content and permissions is performed to ensure freshness of the index and secure control of query results related to the content.

When the Dropbox Dash client is installed on Windows or MacOS, a browser extension is also installed and can be enabled for Chrome and Edge browsers. This extension works in conjunction with the Dropbox Dash connector platform to provide recent browser activity to Dash.

The Dropbox Dash client also contains a component that utilizes the local file system search APIs on Windows and MacOS, so that files on your device can be used in search results.

As the Dash connector platform acquires content from the integrated SaaS and local information resources; de-duplication, enrichment, and content protections are applied to content as it is committed to the Search Index and Metadata Graph databases.



Privacy

Every day, people and organizations trust Dropbox with their most important data. Because of this, it's our responsibility to protect this data and keep it private. Our commitment to your privacy is at the heart of every decision we make.

We support users' right to request access or deletion of their personal data via automated processes. Users can also correct their personal data via their account settings, or by engaging with our account and CX teams. Lastly, we systematically apply retention policies that govern the period of time personal data is retained. We apply the principles of data minimization and purpose limitation to only keep data for as long as we have use for it.

Use of artificial intelligence (AI)

Dropbox Dash contains and uses AI components, which helps get the information that you need and provides more context about that information. The privacy and protection of that information is paramount to Dropbox's commitment to "Be Worthy of Trust". Our AI Principles guide our teams as we develop AI products and features responsibly.

Dash uses AI, which is supported by the third-party service, OpenAI. Individual users have the ability to control both which apps they integrate with Dash and what data is shared with Dash. Data sent to OpenAI is never used to train OpenAI models, and is deleted after 30 days.

Data transfers

When transferring data from the European Union, the European Economic Area, the United Kingdom, and Switzerland, Dropbox relies upon a variety of legal mechanisms, such as contracts with our customers and affiliates, Standard Contractual Clauses, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the European Commission's adequacy decisions about certain countries, as applicable.

Compliance

Compliance certifications, attestations, and regulatory compliance

At Dropbox, we prioritize the security of our customer data. We are proud to have successfully achieved SOC 2 Type II compliance, meeting the Trust Services Criteria for Security, underscoring our commitment to industry standards and the protection of our clients' data. The SOC 2 report provides a thorough description of Dropbox's processes and the controls in place to protect your data, including the independent third-party auditor's opinion on the operational effectiveness of these controls over a specified period. Building on this foundational accomplishment, we're now advancing towards obtaining additional compliance certifications. Reports for Dropbox Dash are available upon request.

Dropbox Sign

The documents, contracts, and agreements you sign as a business are some of the most important documents you have. Many of these types of transactions involve a legally-binding signature and are critical in a company's operations. Examples include new employee hiring documents, sales contracts, building leases, partner relationships, vendor agreements, and so much more. These documents often contain sensitive information, so security is a primary concern. With Dropbox Sign Services, which includes Dropbox Sign, Dropbox Forms, and Dropbox Fax, protection of your documents and related transactions are the highest priority. We are committed to ensuring the privacy, security, and protection of every document that is signed using Dropbox Sign Services.

Security covers a very broad range of topics, and this whitepaper provides a fairly thorough overview of all of them. For customers purchasing a certain minimum contract value, Dropbox can work with you on customized security reviews, questionnaires, and assessments.

Documents are stored behind a firewall and authenticated against the sender's session every time a request for that document is made. Dropbox Sign enforces the use of industry best practices for the transmission of data to our platform (Transport Layer Security TLS) and data is stored in SOC 1 Type II, SOC 2 Type I, and ISO 27001 certified data centers. Customer documents are stored and encrypted at rest using AES 256-bit encryption.

More information can be found on our security page.

Audit trail

Dropbox Sign Product

Each signature on a contract is imposed and affixed to the document. When you request a signature, Dropbox Sign affixes an audit trail page to the document itself. The audit trail contains a globally unique identifier (GUID) that can be used to look up a record in our database, showing who signed a document and when. Read our statement of legality for more details.

The tamper-evident audit trail ensures that every action on your documents is thoroughly tracked and time-stamped, to provide defensible proof of access, review, and signature.

There are a number of different audit-tracked events in Dropbox Sign, including:

- Document Sent
- Document Viewed
- Document Signed
- Decline to Sign
- Signer Name/Email Address Updated
- Attachment Uploaded
- In-person Signing Activated
- Signer Access Code Authenticated
- Electronic Record and Signature Disclosure Accepted
- Signature Request Delegated
- Signature Request Completed
- Completed Request Continued

A current list of all audit-tracked events can be found on our security page.

Authenticity

Dropbox Sign is designed to keep your documents secure and prevent tampering during and after the signing process. Utilizing hashing technology, Dropbox Sign creates a unique record of the underlying document before either party signs it and then creates a separate unique record of the underlying document that contains all of the signatures. If you ever need to prove there was no tampering between the pre and post-signed documents, Dropbox Sign can provide you with the two unique document records. Dropbox Sign utilizes the same technology to help protect your eSignatures.

Authentication

We offer several capabilities that ensure strong authentication of individuals so you can verify a user is who they say they are before being allowed to either issue a document for signature or execute a signature.

2-Factor Authentication

Users are able to set up 2-Factor Authentication, which requires the entry of a unique code generated via Google Authenticator or sent to the individual via SMS.

This code must be used in addition to their username and password. Team admins can mandate which method is used for 2-Factor Authentication.

- Single Sign-On is available using a Dropbox or Google account.
- API key-based authentication for the API.
- All passwords are securely hashed and salted.

Sessions expire after a certain time

1 hour by default, which can be extended to 30 days if the user selects **Remember Me** during login.

Dropbox Sign product specific authentication features

- **Access Code protected signature requests.** For the Dropbox Sign product, users can enable a Signer Access Code (a 4 through 12 character alpha numeric string) that signers must enter in order to view a document.
- **OAuth.** The Dropbox Sign API supports OAuth as a means of authenticating API calls on behalf of a user.
- **SAML.** Dropbox Sign supports SAML 2.0 for enterprise single sign-on.

Permissions

It's imperative that you can control who can do what within the system.

Dropbox Sign Product

Different roles carry different access rights, both in the Dropbox Sign API and in the end user product. For example, Administrators control team-wide settings, billing information, and roles.

- **Role-based security.** Enables different levels of permissions for different members of a team, ranging from administrative rights to members who have only permissions to view templates and issue signature requests.
- **Signer-specific access codes.** As an extra layer of security, each signer can be assigned a Signer Access Code for additional assurance of who is signing.

Dropbox Forms Product

- **Role-based security.** Enables different levels of permissions for different members of a team, ranging from administrative rights to members with limited access to functionality.

Compliance certifications, attestations, and regulatory compliance

Dropbox Sign adheres to the following frameworks, standards, and regulations:

SOC

Service Organization Controls (SOC) Reports, known as SOC 1, SOC 2, or SOC 3, are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox Sign has validated its systems, applications, people, and processes through a series of audits by an independent third-party auditor, Ernst & Young LLP.

SOC 3 for Security, Confidentiality, Integrity, Availability, and Privacy

The SOC 3 assurance report covers all five Trust Services Criteria for Security, Confidentiality, Integrity, Availability, and Privacy (TSP Section 100). The Dropbox Sign general-use report is an executive summary of the SOC 2 report and includes the independent third-party auditor's opinion on the effective design and operation of our controls.

View the Dropbox Sign SOC 3 examination

SOC 2 Type II

The SOC 2 report provides customers with a detailed level of controls-based assurance, covering the Trust Service Criteria for Security, Availability, and Confidentiality (TSP Section 100). The SOC 2 report includes a detailed description of Dropbox Sign's processes and the more than 100 controls in place to protect your customer data. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control. The SOC 2 examination is available upon request.

ISO 27001 (Information Security Management)

ISO 27001 is recognized as the premier information security management system (ISMS) standard around the world. The standards also leverage the security best practices detailed in ISO 27002. To be worthy of your trust, we're continually and comprehensively managing and improving our physical, technical, and legal controls at Dropbox Sign. Our auditor, Ernst & Young LLP, maintains its ISO 27001 accreditation from the ANSI-ASQ National Accreditation Board (ANAB). View the Dropbox Sign, Dropbox Fax, and Dropbox Forms ISO 27001 Certificate.

ISO 27018 (Cloud Privacy and Data Protection)

ISO 27018 is an international standard for privacy and data protection that applies to cloud service providers, like Dropbox Sign, who process personal information on behalf of their customers and provides a basis for which customers can address common regulatory and contractual requirements or questions. Our adherence to ISO 27018 is validated as part of our ISO 27001 certification. View the Dropbox Sign, Dropbox Fax, and Dropbox Forms ISO 27018 Certificate.

HIPAA Compliance

Dropbox Sign supports Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) compliance.

These laws aim to encourage the proliferation of technology in the health care industry, while building protections for the security and privacy of health information. Organizations like hospitals, doctors' offices, and dental practices, as well as individuals who interact with protected health information (PHI) may be subject to HIPAA/HITECH. This may also extend to companies that work with these businesses and come into contact with PHI on their behalf.

Dropbox Sign makes available a report related to HIPAA Security Rule and HITECH Breach Notification Requirements. These documents are available to customer upon request.

The U.S. ESIGN Act of 2000

The Electronic Signatures in Global and National Commerce Act is a federal law that provides a general rule of validity for electronic records and signatures for transactions. Among other things, The U.S. ESIGN Act requires demonstration of an intent to sign, certain consumer disclosures, and record retention.

The Uniform Electronic Transactions Act (UETA) of 1999

Passed in 1999 by the National Conference of Commissioners on Uniform State Laws, the Uniform Electronic Transaction Act allows the use of electronic communication transactions by giving electronic signatures the same legal weight as handwritten pen to paper signatures. The UETA has been adopted by every state except New York.

eIDAS Regulation (eIDAS regulation for the EU of 2016 (EU Regulation 910/2014), which replaced the former European EC/1999/93 Directive)

The eIDAS regulation defines three types of electronic signature (SES, AES, QES) and is a regulation on electronic identification and trust services for electronic transactions in the European Single Market. It establishes a legal framework for people, companies (in particular small to mid-size

enterprises) and public administrations to safely access services and execute transactions digitally across all the EU member states. Dropbox Sign supports SES and QES electronic signatures. Find more information about eIDAS on our compliance page.

Data Privacy Framework

Dropbox Sign complies with the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, as well as the UK Extension to the EU-U.S. Data Privacy Framework, as set forth by the U.S. Department of Commerce regarding the processing of personal data transferred from the European Union, the European Economic Area, the United Kingdom, and Switzerland to the United States. To learn more about the Data Privacy Framework, and to view our certification, visit www.dataprivacyframework.gov.

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a 2018 European Union regulation that marked a significant change to the previous framework for processing personal data of EU data subjects. The GDPR introduced a series of new or enhanced requirements that applies to companies like Dropbox, which handle personal data. Dropbox Sign adheres to GDPR so that customers can use Dropbox Sign to facilitate their GDPR compliance. Get the full details on GDPR compliance on our compliance page.

Subservice Providers

Dropbox Sign utilizes Amazon Web Services as its IaaS provider, which continually manages risk and undergoes recurring assessments to ensure compliance with industry standards (e.g. SOC 1, SOC 2, ISO 27001).

Further detail on the AWS Compliance Program can be found here.

Audits and reports for Dropbox Sign are available upon request.

Links to important resources

- Dropbox Sign Privacy Policy
- Dropbox Sign Trust Center
- Dropbox Sign Security
- Dropbox Sign Compliance

Dropbox DocSend

Dropbox DocSend is the secure document sharing platform everyone can use. We make managing, sharing, and tracking your important files as easy as sharing a link. From email authentication to an embedded NDA, DocSend's advanced document security features have you and your sensitive information covered. In addition to DocSend's document-level analytics, which gives you insight into who's viewed your document and where specifically they've spent time, DocSend's advanced security features include allowlisting (limiting access to your content by domain or email address), watermarking, document viewer email verification, and one-click NDAs that make signing an NDA mandatory before viewing a confidential document. Control every aspect of your shared files—even after you hit send—with DocSend.

DocSend services are designed with a secure, distributed infrastructure with multiple layers of protection. We work to ensure your data is protected, and empower our customers with tools that provide control and visibility.

You can learn more about DocSend product features at www.docsend.com.

Dropbox DocSend provides a wide range of features, which vary by plan. For more information, see Dropbox DocSend Pricing. Depending on plan type, features that our users have access to include:

Secure file sharing

Control every aspect of shared files, enable secure file sharing with DocSend links and passcodes, and set expiration dates for downloads.

Dynamic watermarking

Helps prevent unwanted sharing, displays viewer info, and more.

Virtual data rooms

Virtual data rooms (VDRs) enable sharing multiple documents with a single link and provides viewers with content and ability to upload files with or without a DocSend account. They can support specified email addresses and domains, as well as passcodes and NDA signatures.

eSignature

Convert files to signable documents, or create them directly from DocSend. Complies with E-Sign and UETA regulations and supports multiple users and the analytics associated with their document interactions. Once signed, receive an audit trail of the signing process or export a list of signatures for a document.

NDAs

Set up NDAs or other agreements for sensitive content, requiring viewers to provide a signature before accessing a document even if it was forwarded to someone new.

User roles

Use multiple levels of user access, including role-based security permissions. Users range from members who upload and update content to the admins who manage them and their accounts. All plans also include an account owner, who can access the Billing page and transfer account ownership.

User management

Keep documents secure and billing current. DocSend Owners and Admins can add, deactivate, suspend, and reactivate users.

Transfer user data

DocSend Owners and Admins can use Transfer User Data to move all of a suspended or deactivated user's data to another active user, ensuring that the inactive user's links and documents remain accessible.

Single Sign-On (SSO)

Teams can log in securely through Okta or OneLogin via SAML 2.0, with which DocSend also supports SCIM for user provisioning.

Sub-teams

Use Sub-teams to organize and grant access to specific content that's relevant to each team within an organization. This helps keep content secure and ensure that only authorized users can access it. Folder access can be managed by sub-teams as well.

Encryption

DocSend protects data in transit between our apps and our servers, and at rest. Documents are stored behind a firewall and authenticated against the sender's session every time a request for that document is made. We enforce the use of industry best practice for the transmission of data to our platform, Transport Layer Security (TLS), and data is stored in SOC 1 Type II, SOC 2 Type II, and ISO 27001 certified data centers. Your documents are stored and encrypted at rest using AES 256-bit encryption.

Audit trail

In connection with DocSend's e-signature services, an audit trail ensures that every action is thoroughly tracked and time-stamped, to provide defensible proof of access, review and signature. These records include a hash of the PDF document which we can compare to the hash of a questionable PDF document to determine whether or not it has been modified or tampered with.

Authentication

We offer several capabilities that ensure strong authentication of individuals so you can verify a user is who they say they are before accessing your content, being allowed to issue a document for signature, or execute a signature.

All passwords are securely hashed and salted

Single Sign-On

DocSend can be configured to allow team members access by signing into a central identity provider. Our SSO implementation, which uses the industry-standard Security Assertion Markup Language 2.0 (SAML 2.0), makes provisioning easier and more secure by placing a trusted identity provider in charge of authentication and giving team members access to Dropbox without an additional password to manage.

DocSend product specific authentication features

- **Password-protected file sharing:** users can set a passcode, verify via email, and restrict access to ensure only the right people can view their files. Users can also set expiration dates and turn on or off the ability to download the files.
- **Gate access with agreements:** users can gate access to content with an agreement, such as an NDA.

Permissions

It's imperative that you can control who can do what within the system.

DocSend product

Different roles carry different access rights. For example, Administrators control team-wide settings, billing information, and roles.

- **Role-based security:** enables different levels of permissions for different members of a team, ranging from administrative rights to members.
- **Sub-teams:** DocSend sub-teams allow users to grant access to specific content that is relevant to each team within an organization. Sub-teams keep sensitive content secure and ensure that only authorized users have access to it.

Our subservice providers

At least annually, Dropbox DocSend performs a review of our subservice providers. In the event these reviews have material findings which we determine present risks to DocSend or our customers, we will work with the service provider to understand any potential impact to customer data and track their remediation efforts until the issue is resolved.

Our Privacy Policy explains the limited circumstances under which your data may be shared with third parties.

Compliance certifications, attestations, and regulatory compliance

At Dropbox DocSend we believe that compliance is an effective way to validate a service's trustworthiness. On an annual basis our independent third-party auditors test our controls and provide their reports and opinions, which we can provide to you upon request.

SOC 2 Type II

Service Organization Controls (SOC) Reports are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox DocSend has validated its systems, applications, people, and processes through an audit by an independent third-party, Ernst & Young LLP.

The SOC 2 report provides customers with a detailed level of controls-based assurance, covering the Trust Service Criteria for Security, Availability, and Confidentiality (TSP Section 100). The SOC 2 report includes a detailed description of Dropbox DocSend's processes and the more than 80 controls in place to protect your customer data. In addition to our independent third-party auditor's opinion on the effective design and operation of our controls, the report includes the auditor's test procedures and results for each control. The SOC 2 examination is available upon request through our sales team by emailing support@docsend.com.

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a 2018 European Union regulation that marked a significant change to the previous framework for processing personal data of EU data subjects. The GDPR introduced a series of new or enhanced requirements that applies to companies like Dropbox, which handle personal data. Dropbox DocSend adheres to GDPR so that customers can use Dropbox DocSend to facilitate their GDPR compliance.

Subservice Providers

Dropbox DocSend services utilize Amazon Web Services for SaaS and IaaS, which continually manages risk and undergoes recurring assessments to ensure compliance with industry standards (e.g., SOC 1, SOC 2, ISO 27001). Additionally, PaaS through Heroku, is also independently evaluated by third-party assurance assessments (e.g., SOC 1, SOC 2, ISO 27001).

Further detail on the AWS Compliance Program can be found here.

In addition, DocSend has completed the rigorous security review process put in place by Salesforce as part of being listed on the Salesforce AppExchange.

Links to important resources

- Dropbox DocSend Terms of Service
- Dropbox DocSend Privacy Policy
- Dropbox DocSend Copyright and IP Policy
- Dropbox DocSend Cookie Policy

End-to-End Encryption

With End-to-End Encryption (E2EE) for selected Team Folders, customers can comply with regulations, safeguard intellectual property, and foster reliance on the security of devices. End-to-end encryption provides a secure environment for sharing and collaborating on sensitive data, preventing unauthorized interception and breaches by external parties and even Dropbox itself. With E2EE, the encryption and decryption keys are generated on the user's device. This means that the data is encrypted on the user's device itself before it is sent to Dropbox's servers. By incorporating end-to-end encryption, businesses can confidently leverage Dropbox while mitigating the risks of unauthorized access and data compromise.

Protocol Roles

Dropbox Servers (PKI, data storage, protocol coordination)

We assume that each server is a singular entity. Its purpose is to store and distribute public keys and encrypted private or symmetric keys. It is a core component in our PKI (the Encrypted Key Management System or EKMS). It stores the folders, files, and their metadata, and is responsible for regular, non cryptographic authorization and authentication.

Teams (File owner)

A team is a collection of users, cryptographically represented by a shared, cryptographic team key. The team owns its files, and the protocol ensures that members can only access the files their team owns.

Users

Users contribute to the file collection of their team. They are authenticated to the Dropbox server and participate in the protocol through their devices. The protocol ensures that they are only able to access files their team owns.

Admins

Admins are a subset of users. They are authorized through regular authorization (e.g. ACLs) to manage the parameters and users for their team. From a cryptographic point of view, they have access to a recovery key, which allows them to perform cryptographic operations, such as enrolling new users or devices, even if they themselves don't have any enrolled devices.

Devices

Devices offer an interface for the user to participate in the protocol. Devices are "trusted" in that they are deemed acceptable to store and protect secret information, like cryptographic keys.

Dropbox Employees

Dropbox employees are not participating directly in the protocol, but do have elevated access to the Dropbox server. We distinguish between employees with read access, employees with write access to a user's data, and employees with the ability to change the behavior of the server / protocol.

Third Parties

Third parties do not participate directly in the protocol. In other words, these are entities that are not authorized to access a user's files. The protocol ensures that they cannot decrypt the user's files. In this way, it protects users from a threat actor of any kind.

Employee policy and access

Upon hire, each Dropbox employee is required to complete a background check, sign a security policy acknowledgment and non-disclosure agreement, and receive security training. Based on each individuals' job role and responsibilities, they may be granted physical and/or logical access to the corporate and production environments. Employee access is promptly removed when an employee leaves the company. In addition, all employees are required to complete annual security training, and they receive regular security awareness training via informational emails, talks and presentations, and resources available on our intranet and training portal.

Employee access to the Dropbox environment is maintained and authenticated using a combination of strong passwords, passphrase-protected SSH keys, and two-factor authentication. Remote access requires the use of VPN protected with two-factor authentication, and any special access is reviewed and vetted by the Security team. Access to corporate and production networks is strictly limited based on defined policies. For example, production network access is SSH key-based and restricted to engineering teams requiring access as part of their duties. Firewall configuration is tightly controlled and limited to a small number of administrators.

In addition, our internal policies require employees accessing production and corporate environments to adhere to best practices for the creation and storage of SSH private keys. Access to other resources, including data centers, server configuration utilities, production servers, and source code development utilities is granted through explicit approval by appropriate management. A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals.

Dropbox employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about End-to-End Encryption. In order to protect end user privacy and security, only a small number of engineers responsible for developing core Dropbox End-to-End Encryption services have access to its production environment.

As Dropbox becomes an extension of our customers' infrastructure, they can rest assured that we are responsible custodians of their data.

Goals and Threat Model

Goals

End-to-End Encryption protects users from a defined set of scenarios, enhancing user trust in Dropbox. The scenarios are outlined in our threat model, below.

Important note: This document covers cryptographic protection only. Regular access control mechanisms will complement the protocol, for example, by allowing a more fine grained access control among individual team members. All protocol roles use a secure communication channel (e.g. TLS 1.2) to communicate with the server.

Threat Model

The End-to-End Encryption protocol must ensure:

- Confidentiality in terms of the Dropbox Server.
- Confidentiality in terms of Dropbox employees.
- Confidentiality in terms of other teams, their users, and third parties.
- Integrity of encrypted files for modifications.
- Availability of encrypted files outside of the server environment

Reduced Threat Model through Disabling Key Verification

Key verification requires out-of-band verifications, which might be impractical in some usage scenarios. To account for these scenarios, key verification is optional. If key verification is disabled, the threat model is reduced as follows:

- **Integrity and Confidentiality** is no longer guaranteed against an actively malicious Dropbox server, or against Dropbox employees with write access to user data (i.e. against active attacks).

Coming Soon:

- Confidentiality for new files or modifications after a key rotation (a former team member becoming untrusted is a common scenario in which existing files could be regarded as compromised, and confidentiality should be cryptographically ensured through key rotation from that point on).
    - Devices do not have to be online for a key rotation to take effect, making the rotation process a fairly rapid one.

Rationales

End-to-End Encryption is designed to balance the information security needs of data confidentiality, integrity, and also availability, extended with usability so that team productivity would not be hampered.

The Team Centric Approach

If the cryptographic security boundary is drawn around the individual user, then this places the responsibility for the key on that user. Data loss through key loss is a risk in end-to-end encrypted systems and individual users being able to lose their keys results in a risk for the availability of the data of the company. Solutions for that risk exist, but they increase the complexity of the product and decrease its usability, especially considering that the feature is operating in an async and teams-only environment.

With the security boundary drawn around the team, we have a layer of protection: As long as one user still has access to the team key, all data can be recovered, even if one or more users loses access to the key. In addition, the team centric approach improves the user experience and simplifies the complexity of the protocol, reducing the risk of security issues.

Automatic Device Enrollment

Manually setting up end-to-end encryption on a new device can be a significant challenge for non-technical users, resulting in low adoption rates. By leveraging device-to-device enrollments authenticated by Dropbox's standard authentication and access control mechanisms, users are relieved of this burden through defined threat and trust models.

Limitations

- Clients are considered trustworthy, which is a common assumption for End-to-End Encryption. This is due to the less dynamic nature of the client, which is considered manually approved through the installation process. Security guarantees offered by the web client are weaker than those offered by native applications because they are delivered more dynamically.
- The freshness of individual files cannot be guaranteed because it is not possible to cryptographically prove that a file is its latest revision.

Trust Model

- Users inside a team are trusted and access restrictions between them are not enforced cryptographically, but by ACLs.
- The user is responsible to keep their device secure.
- The End-to-End Encryption feature protects cryptographically against anyone else, including Dropbox.

Important: When Key Verification is disabled, trust is extended to the Dropbox server and employees with write access. By adhering to the protocol, the server delivers the correct keys for each file operation and any potential attacker with access to a Dropbox database is not able to learn anything about the team file contents. Likewise, Dropbox is not able to decrypt any data at rest.

Relationship with Regular Access Control

The End-to-End Encryption feature is a security improvement, complementing already existing access control mechanisms. This section describe how standard Dropbox security features work with the addition of End-to-End Encryption.

Team-internal access control

The End-to-End Encryption feature protects against threats outside of a team. As such, no cryptographic protection between members of the same team is required or implemented. Access control among members of the same team is implemented outside of the protocol, through regular ACLs.

Protection status of les when a member leaves the team

Up to the point that a member leaves a team, that team member has had, in terms of the protocol, access to all team files. New content is encrypted with a new key. Regular access control blocks access to files the former team member had access to without delay.

Cryptographic Primitives, Types, and Definitions

Keys and Key Material

All keys and key material are created on the device.

Entity Key Pair

An Entity Key Pair represents an asymmetric cryptographic key pair, consisting of a Public Entity Key and a Private Entity Key. The key pairs are always created on the device, and the Private Entity Key must be encrypted before it leaves the device. Entity Key Pairs are either stored on the Dropbox servers (encrypted), remain on the device, or are exportable for backup purposes.

Data Key

An Entity encrypts any kind of data with symmetric Data Keys. Each data unit (for example, a file) is encrypted with a new, unique Data Key. Symmetric keys are never stored on the Dropbox servers unencrypted. They are always encrypted by another key.

The algorithm used is Blockwise AES-GCM.

Algorithms for Keys

Symmetric Keys

For all symmetric encryption, AES-256-GCM with a 128-bit auth tag and a 96-bit nonce is used. The nonce is randomly generated on device side.

Asymmetric Keys

- For all asymmetric encryption, HPKE, single shot, base mode with kem (Kem.DhkemP256HkdfSha256, kdf: Kdf.HkdfSha256, aead: Aead.Aes256Gcm) is used.
- When Key Verification is enabled, aad: utf8(algorithmID) is added, and HPKE **auth mode** is used to encrypt namespace and file keys.
    - Key verification for the team key is done implicitly out-of-band.
    - The sender for the namespace key encryption is the team private key.
    - The sender for the file key encryption is the namespace private key.

Encrypted Key Management System (EKMS)

The Encrypted Key Management System (EKMS) is a cryptographic key management solution designed for both security and efficiency. EKMS preserves data confidentiality through client-side encryption, strictly adhering to the Zero Knowledge principle. This ensures that all cryptographic keys are securely encrypted on the device, making them unusable on the server-side. Consequently, EKMS establishes robust end-to-end encryption.

EKMS adopts a "team-centric key management" approach, where each user within a team is granted cryptographic access to other keys within that specific team. This approach ensures efficient key management while maintaining security.

EKMS ensures that every team member with cryptographic access to Team Keys also possesses access to all File Keys. However, access to encrypted binary data (encrypted files) remains governed by strict access controls. If a team member lacks access rights, they will be unable to download the encrypted binary data.

Types of Keys within EKMS

- ***File Key***

  File Keys are symmetric keys. Devices have the flexibility to specify the cryptographic algorithm for their use. Generated on the device, these keys are encrypted before transmission to the server. This ensures that the keys and the data they protect remain confidential.

- ***Encrypted Team Folder Keys***

  Encrypted Team Folder Keys are asymmetric keys, assigned to folders protected with End-to-End Encryption. Devices can define the cryptographic algorithms used for these keys. These Keys are generated on the device and the private key is encrypted with the active Team Key before being securely transmitted to the server.

- ***Team Key***

  Team Keys are also asymmetric and are specifically assigned to teams. These keys are generated on the device and further protected by encrypting the private key with Recovery and Device Keys before being sent to the server.

- ***Device Key***

  Device Keys are asymmetric keys, uniquely assigned to individual devices and owned by a user. Only the public key is registered on the server, while the private key remains exclusively on the device. These keys are used to encrypt Team Keys within a user's team.

- ***Recovery Key***

  Recovery Keys are asymmetric keys allocated to a particular team and generated by an administrator. Administrators have the capability to delete Recovery Keys, but at least one Recovery Key must be retained at all times. As with Device Keys, only the public key is registered on the server, and the private key is securely stored by the administrator.

Decrypting Private Keys

Whenever a private key is decrypted and its public key is provided separately, the private key will be verified against the public key, and usage of the decrypted key will be rejected on a mismatch.

Team Enrollment

In order to enhance the security and efficiency of our team enrollment process, we have implemented a design that ensures the safeguarding of critical cryptographic keys.

The process begins with the generation of a recovery key pair on the device. The private key is then securely presented to the administrator for safekeeping.

The recovery public key is registered on the server, while a new team key pair is generated on the device and the private team key is encrypted using the recovery key.

When key verification is enabled, a fingerprint of the public team key is displayed to the administrator and must be broadcasted out-of-band to all yet-to-be-enrolled members of the team.

To complete the team enrollment, the plaintext team public key and encrypted team private key are registered on the server. These steps result in a fully enrolled team.

Device Enrollment

The Device Enrollment process consists of two parts:

1. A device requesting access to an encrypted team folder. This step consists of locally generating and registering unique device keys.
2. An already enrolled device or an admin granting the device access by re-encrypting the private team key for the previously registered device keys.

The device is requesting access as follows (this corresponds to step 1):

1. A device enrolls by generating a unique key pair, consisting of a public key and a private key, on the local device.

2. The device safeguards the private key securely on the device, as it is the key to decrypting sensitive information.

3. The device's public key is registered on the server.

Note: When Key Verification is enabled, the user is required by the admin to send the device's public key fingerprint out-of-band. The device recognizes the fact that key verification is enabled and displays the team key and device fingerprints to the user. The necessity to verify the team key fingerprint and forward the device fingerprint needs to be communicated to the user by the administrator. The device remembers the team key fingerprint once it is approved by its user.

An already enrolled device is granting access as follows (this corresponds to step 2):

Note: An authorized entity is able to enroll new devices. Such an authorized entity can be an already enrolled device, or the administrator, leveraging recovery keys in the admin console. If the key verification feature is enabled, only the latter approach is supported.

1. The authorized entity retrieves the public key of the new device from the server. When Key Verification is enabled, only the administrator is able to enroll the new device. In that case, the administrator verifies the fingerprint of the received public key out-of-band with the one displayed on the enrolling device.

2. The authorized entity also loads the encrypted private team key from the server, or retrieves it from its cache.

3. Using their own private key or recovery key, the authorized entity decrypts the private team key. When Key Verification is enabled, it verifies that the decrypted private team key fits the locally stored team key fingerprint.

4. The authorized entity takes the decrypted private team key and re-encrypts it using the new device's public key. This step ensures that only the new device with the corresponding private key can access the team key.

5. The re-encrypted private team key is registered on the server.

   Note: When Key Verification is enabled, should the server at any point deliver an encrypted team key with a different fingerprint, then the device alerts the user about this and requires a confirmation of the validity of this new team key. This can happen during a key rotation. In this case, the new team key's fingerprint would have been distributed out-of-band during the rotation process.

6. In cases where an enrolled device may not be available during the enrollment process, administrators can leverage the concept of Recovery Keys. This method enables the secure enrollment of new devices even when existing devices are offline or unavailable. Currently, enrolling devices with key verification enabled is only possible in the admin console, leveraging the Recovery Keys.

7. When Key Verification is disabled and enrolled devices are online, they automatically download the public keys of the devices to be enrolled and seamlessly initiate the enrollment process in the background. This streamlined approach ensures that device enrollment can occur efficiently and securely.

Adding Recovery Keys

An administrator can add multiple recovery keys.

Follow these steps to create a new recovery key:

1. To start, the admin must have access to an existing recovery key. This existing key is a prerequisite for adding a new one.
2. In the browser, a new recovery key pair is generated. This key pair includes a public key and a private key. The private key will be used in later steps.
3. The newly generated recovery public key is registered on the server. This step ensures that the system recognizes and associates the new key with the team.
4. The admin must enter the existing recovery private key.
5. After the existing recovery private key is provided, get the encrypted private team key. This key is encrypted with the entered recovery key.
6. Decrypt the private team key using the provided existing recovery private key. This allows access to the private team key.
7. Next, encrypt the private team key with the newly generated recovery public key. This step ensures that the private team key is now associated with the new recovery key.
8. Finally, register the encrypted private team key on the server. This action completes the process of creating a new recovery key and ensures that the new key is securely stored and recognized by the server for future recovery purposes.

Key Management and Rotation

Note: Currently, key rotation and key verification are mutually exclusive, that is, you can't have both activated.

Access Revocation

Currently, Access Revocation is not implemented. Team members can be removed but are, from a cryptographic point of view, only prevented from continuing access to the files through regular ACLs. What follows is the concept for access revocation that will be implemented in the future.

Access Revocation is a crucial security feature that ensures the controlled deletion of both Device and Recovery Keys. It ensures that former team members will be unable to compromise the security of the team's data through encryption. This process plays a fundamental role in maintaining the integrity and confidentiality of the data. Access Revocation includes the following aspects:

Revocation of Recovery Keys: Authorized administrators have the capability to revoke recovery keys. When a team key rotation is initiated, the new team key is not being re-encrypted with the affected recovery public key. This guarantees security for newly created or modified files.

Revocation of Device Keys: When a user leaves the team, a team key rotation can be initiated and the new team key is not being re-encrypted with the affected device public key.

Key Rotation: Key Rotation is an essential process in maintaining the security and confidentiality of our data. It provides a mechanism for updating encryption keys.

Prerequisite — Access Revocation: Key Rotation depends on Access Revocation. Before keys can be rotated, any user or recovery keys that need revocation must be either deleted or marked as deactivated.

Admin-Controlled Key Rotation: Administrators have the ability to initiate key rotation through the admin console.

Following steps are required to rotate the keys:

1. **Rotate Team Key:**
    - A new team key is created locally.
    - The new team key fingerprint is displayed to the administrator for out-of-band distribution (**Key Verification enabled only**)
    - All available and active recovery keys and device keys are retrieved from the server. If key verification is enabled, the device public key fingerprints are validated out-of-band by the administrator
    - The new team private key is re-encrypted with **all active recovery and device keys** to maintain data access.
2. **Rotate Namespace Keys**: A new namespace key is introduced for each existing namespace. This new key is encrypted with the new team's public key.
3. **Activate Team Key**: When the new team key is encrypted with all active recovery and device keys, and encrypts all new namespace keys, it will be marked as active. That means it will be used for encryption operations.
4. **Expiry and Usage**: The existing team keys, namespace keys and file keys expire. Expired keys will no longer be permitted for encryption operations. They are only usable for decryption operations.
5. **Prohibit File Commits with Existing File Keys**: In situations where file keys are expired, file commits will be rejected. Devices are required to generate new file keys and re-encrypt the content before uploading again. This ensures that no sensitive data is compromised through the use of outdated encryption keys.
6. **When Key Verification is enabled**, users verify and confirm that their device is using the new team key through the out-of-band distributed team key fingerprint and the capability of their device to display the currently used team key.

External Sharing

External sharing, which will provide cryptographic protection when collaborating with another team, is coming soon.

Sharing with external teams

External teams will need to be enrolled in End-to-End Encryption, which means that they have a valid team key pair. Sharing is then done on a team folder level by encrypting the team's private key with the external team public key. This provides the external team with cryptographic access to the team folder and its content.

Key Rotation for External Shares

Key rotation is performed as described above, starting with the team key of the team doing the rotation. For example, if Team A has a shared folder with Team B, and Team B rotates its keys, then the shared folder keys would also be rotated. The new shared folder key is automatically shared with Team A again to allow access for both teams. This provides cryptographic protection when someone leaves a team.

Important Note: External sharing is only available when Key Validation is disabled.

Team Key Fingerprints

With key rotation, several team keys may be in use at any time. Key team fingerprints mitigate a scenario where key rotation could reduce security. For example, a security issue would occur if the server was able to create a rogue team key, encrypt it with a customer's device key, and present it as an expired team key. Devices would reject writes with this team key because it has already expired, but the server could still inject arbitrary content as read-only, presenting it as older team data. This would break integrity.

The team key fingerprint prevents this by authenticating not only the current team key, but also all expired ones. This process is done through Sparse Merkle Trees.

Initial Creation

The team key fingerprint consists of a Merkle Tree hash consisting of one leaf. This means that the initial team public key hash is already the team key fingerprint.

The team public key hash is calculated by concatenating the algorithm name, a separation character and the public key, and hashing the result with Sha256.

Re-Calculation After Key Rotation

A key rotation introduces a new team key. The administrator executing the key rotation has the previous team key fingerprint via the root of the Merkle Tree. The server provides the administrator with the information required to extend the Merkle Tree with the new team key's hash and to calculate **the new Merkle Tree root (i.e.: the new team key fingerprint)**. During this process, the server cannot inject invalid values, because the administrator is aware of the previous Merkle Tree root hash and would easily detect such an attempt.

The new team key hash replaces the first **null** value from the left in the sparse tree. The newest team key hash can be determined by looking at the first non-null value in the tree's leaves from the right.

Verification of Any Team Key

With the delivery of any team key, whether expired or active, the server will provide a membership proof of the key. The device, having previously verified and locally stored the team key fingerprint (i.e. the Merkle root hash), can successfully verify the proof and then accept the team key.

File Encryption

The algorithm used to encrypt the file content is designed to be replaceable. Each encrypted key on the server includes the identifier of the algorithm with which it is meant to be used. Currently, only one algorithm is used: Blockwise AES-GCM.

Raw File Algorithm

File content is encrypted with a symmetric encryption algorithm named Blockwise AES-GCM.

Encryption

1. Specify |authTag| = 128 bit and |blocksize| = 4 MB
2. Create a new hmac_key := random(256 bit) and nonce_hmac_key := random(96 bit)
3. Calculate (encrypted_hmac_key, hmac_auth_tag) := AES-GCM-encrypt(revision_key, nonce_hmac_key, hmac_key).
4. Expect plaintext := f_0 || f_1 || ... || f_n with |f_i| = blocksize. The last block may be smaller than the blocksize.
5. For each f_i
   - Chose nonce_i := random(96 bit)
   - Calculate (encrypted_f_i, auth_tag_i) := AES-GCM-encrypt(revision_key, nonce_i, f_i)
6. Calculate authSetHmac := HMAC_SHA256(hmac_key, auth_tag_0 || auth_tag_1 || ... || auth_tag_n)
7. Return encrypted_hmac_key, nonce_hmac_key, hmac_auth_tag, all nonce_i, all auth_tag_i, all encrypted_f_i and authSetHmac.

Decryption

1. Decrypt the hmac_key.
2. Verify the authSetHmac by re-calculating it and comparing it with the stored value.

Calculate f_i := AES-GCM-decrypt(revision_key, nonce_i, auth_tag_i, encrypted_f_i)

AES-GCM

AES-GCM is used as an underlying primitive due to its wide availability in cryptographic libraries.

Encrypting a File

A hash value of each plaintext block is stored on the Dropbox Server. This hash value does not have to be decryptable by the server, but it needs to be decryptable by the device. To account for that, and to remove the revision limitation of Blockwise-AES-256-GCM, we're introducing a Revision Key, which is inserted between the File Key and the Raw File Algorithm.

The steps to encrypt a file with a given file_key are as follows:

1. Create a new, random AES-256 key (the revision_key).
2. Encrypt the revision_key with the file_key
3. Encrypt the file with the revision_key.
4. Hash each plaintext block, and encrypt each plaintext block with the revision_key.
5. Send the encrypted file, its metadata, the encrypted revision key, and the encrypted plaintext block hashes to the Dropbox Server.

Steps to decrypt a file:

1. Reverse the steps of the file encryption
2. For each decrypted block of the file, calculate the decrypted block's hash and make sure it matches the expected hash (the encrypted plaintext block hashes are provided to the decryption routine).

Each encryption, and each modification of an existing file, is done using a newly created revision_key. This reduces the revision limit of Blockwise-AES-256-GCM from *block count of a file and its revisions* to *block count of a file*.

Note: Files can currently not be moved between different encrypted team folders, but only within them. For example, if you're working within a team folder, you can move files freely — into and out of subfolders. However, if you have a second encrypted team folder, it is not possible to move files between the two team folders.

Advanced Key Management

Businesses need sophisticated security solutions that meet compliance requirements. Security teams need visibility into and control over the way in which company data is protected to safeguard sensitive content. This can be accomplished within Dropbox, without third-party data protection solutions. We make it easy to adopt this new enhanced data encryption model that leverages an industry-standard key management infrastructure. Securely manage your encryption keys on Dropbox and benefit from the following features.

Automation and Control

- Automatic scheduled rotation of team encryption keys every year for assured protection.
- Manually revoke your team encryption key at any time to permanently remove access to your team's data whenever a threat is detected.

Increased Data Protection

- Multilayered encryption model with a unique top-level, team associated encryption key.
- Team Encryption Key (TEK) is generated and stored using industry standard Hardware Security Modules (HSM).

Auditability

- View activity related to your encryption key, including rotations and revocations, with audit logs.

Multi-Level Encryption

While all data stored on Dropbox is encrypted, for extra layers of control and security, you can choose to have Dropbox generate a unique team encryption key for your team.

As a part of Dropbox's multi-level encryption process, data at rest for teams that enable Dropbox managed encryption keys will be encrypted using Dropbox's multi-level encryption process, where data at rest stored on Dropbox will be encrypted at three layers using different keys — at the block level, the namespace level, and the team level. The Dropbox managed encryption keys (DMEK) feature provides customers with a unique team-level encryption key (TEK), which allows for greater flexibility for data security and regulatory compliance. Dropbox will manage the storage, organization, and rotation of TEKs using the industry-standard AWS KMS (Key Management Service).

Keys are unique for every customer. Each team is assigned a unique team-level key. TEKs are generated, stored, and audited utilizing FIPS 140-2-compliant features of AWS Key Management Service (KMS). Once you activate DMEK in the Admin Console, no setup is required.

Note: Activating DMEK will not impact any Dropbox functionality. Collaboration features such as Previews, Sharing, and Search, will continue to work as expected.

Dropbox managed encryption keys (DMEK) Activation

You can activate DMEK through Advanced Key Management in the Dropbox Admin Console.