Dropbox Dash

Dropbox Dash for Business

Introduction

Dropbox Dash for Business combines universal content access control with artificial intelligence (AI) universal search and organization. It connects with everyday work applications to create a central hub for your company's information, while providing administrators with the ability to audit access permissions. Admins can easily, quickly manage access to company content, thanks to robust access permission controls. With universal search, AI-powered insights, and content collections, Dash makes it easy to secure content and help teams find, organize, and share work. Dash helps teams work more securely and faster than ever before, bringing advanced data access governance and search capabilities to businesses of any size.

Under the hood

Dropbox Dash is backed by an infrastructure designed to ensure fast, reliable search and secure protection of company content. To make this happen, we continually improve our product and architecture to increase response speed, 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) and Dropbox infrastructure.

Dash starts with the admin console, where IT professionals configure connectors to cloud-based applications and enable single-sign on (SSO) if applicable, and assign licenses. Employees with an assigned license will be invited to login to Dash and enable connectors that are specific to their role or job function. Employees can use the Dash desktop client, Chrome or Edge browser extension, or Dash.ai website to search for content across all connected or applications, organize similar content into stacks, and ask questions about their current work. Each of these functions is enhanced by Large Language Models (LLM).

Security

Dropbox Dash is secure by design. Millions of customers trust Dropbox with their most important information. Dash is designed with the same focus on security. Our security foundations hold us accountable to meeting our commitment to maintain customer trust today and in the future. For more information, see the **Security** section below.

Configuration and management

The Dash admin console gives admins several tools for managing the Dash deployment. In addition to license assignment and general Dash settings, the admin console allows admins to configure connectors. Connectors are Dropbox services that index your business content from popular cloud services like Dropbox, Google Workspace, Microsoft SharePoint and OneDrive, and others. More information about the types of available connectors can be found in the **Connectors** section.

OAuth and API tokens that are used by connectors to cloud services are securely stored using best-in-class encryption techniques.

The Dash admin console provides operational status and insights into how employees are using Dash. If a connector is disconnected by an admin, Dash will purge all content associated to that connector. The status of indexing and purging is provided in the admin console for monitoring by the deployment's administrators.

Content indexing

Once a connector has been added, Dash's connector infrastructure indexes all content for that service and performs incremental refreshes. This ensures that the latest versions of content are searchable and that search results, based upon permissions, is accurate.

Content is stored and indexed to support Retrieval Augmented Search (RAG) for Answers and Stacks. Engagement signals like comments and views can be collected from some content types or the Dash browser extension and are used to improve the Search and Answers experience by providing the most active and relevant content to employees.

Product overview

Dash provides end users and administrators with four core product benefits, which are covered in more detail below.

Core benefits

AI universal search

Dash provides advanced AI universal search capabilities across all a company's connected applications and associated content. With connections to major platforms like Dropbox, Google Workspace, Microsoft OneDrive and SharePoint, Confluence, and more, employees can find everything in one place and let Dash search across countless documents to find answers in seconds. Employees can quickly and easily find what they need across their workspace applications. Dash transforms the information discovery process by streamlining search across multiple platforms with AI-powered precision, ensuring that employees only access authorized, relevant content in real-time.

All information in Dash respects the permissions from the source applications, so employees will only see what they have access to.

Data access governance

Through the protect and control panel in the Dash admin console, administrators have full visibility into who has access to company content. Administrators are able to quickly uncover and remediate security risks across company content and applications. This visibility and controls exist in one place, so administrators don't need to run manual scripts or jump between admin consoles.

AI work assistant

Employees can use Dash's AI work assistant capabilities to simplify getting work done. Dash enables employees to get summaries of content, ask questions and get answers about work, plus generate insights based on company content. Employees can also organize, find, and easily share content from multiple applications using the Stacks feature.

Knowledge management tool

Dash optimizes the access and flow of information within an organization. It can function as an intranet or wiki and allows companies to create a centralized repository of information.

Core services

Search and metadata databases

Once a connector has been added, metadata and the data itself will be indexed to these databases, which are logically separated, sharded, and replicated as needed to meet performance and high availability requirements.

AI and ML

We partner with companies whose privacy policies and commitment to our customers' rights and safety align with our own. When we partner with companies to provide ML, they do not train on your company's data and do not store it for longer than 30 days.

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.

Query service

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

Users and 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.

Natural language services

Dash is capable of processing and responding to queries posed in everyday language form, from within the standard 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.

Dash user interfaces

Dash can be utilized and accessed through the dash.ai web site, a browser extension, and a desktop application.

Web application

Dash is supported in any browser at dash.ai. It allows users to easily 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.

Web browser extension

The Dash browser extension is currently supported by Chrome and Edge. It makes it easy to re-retrieve content, intelligently groups related content together through smart stacks, and it also makes suggestions so users always have the right content, at the right time. The extension enables searching within stacks, surfaces related stacks, provides a view into all stacks, and gives users the ability to both create and add items to stacks. It also allows browsing history to be intelligently surfaced along with other relevant content on a browser start page.

Desktop application

The Dash desktop application is a powerful universal search client enabling users to seamlessly search through their data across multiple platforms. It uses the local file system search APIs on Windows and macOS, so that files on the device can be used in search results.

Dash enables users to connect a variety of data sources and use a highly customizable interface to locate content. As the connector platform acquires content from both integrated SaaS and local resources, de-duplication, enrichment, and content protections are applied to it as it is added to the Search Index and Metadata Graph databases.

Security

Dropbox Dash is secure by design. Millions of customers trust Dropbox with their most important information. Dash is designed with the same focus on security. Our security foundations hold us accountable to meeting our commitment to maintain customer trust today and in the future.

At Dropbox, 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 Dash 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.

Account security and authentication

Dash supports authentication through your company's enterprise identity provider, enabling the use of your existing SSO setup and ensuring secure account access with two-factor authentication and industry standard integrations to third-party identity providers.

ACL service and strict permissions enforcement

We know how important it is to keep information secure. With Dash, end-users only have access to the content they have permissions for across any given company or individual connector. 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.

Admin controls

Data access governance

For some company connectors, Dropbox Dash admins have full control and visibility over who has access to content within source connectors at the individual document level, and can batch update permissions for any amount of assets. This enables protection of sensitive company information while also supporting seamless collaboration.

Dash provides the following advanced data access governance capabilities across select platforms.

Granular content access controls:

- Set permissions at the document and folder level for more precise security.
- Ensure sensitive information is accessible only to authorized users.
- Access settings can be easily adjusted as roles and needs evolve.

Full visibility into content access settings:

- Get a complete view of every type of permissions risk and how much exposure exists.
- Have instant visibility into every document with a public or company link.
- Identify any internal and external account and domain that has access to documents.

User-friendly content permission management:

- Easily bulk update and manage permissions for any amount of assets in seconds across multiple platforms.
- Simplify the process of controlling access, even in complex environments.
- Enable seamless cross-functional collaboration without compromising security.

Audit and activity logging

Full visibility into how Dash is being used in your company's environment with the ability to export logs for quick analysis or integrate with SIEM solutions for centralized monitoring and alerting. Numerous logging events include information about connector creation and removal; stack creation, deletion, and various usage types; member and setting management; and more.

Managed deployments

Setup is easy with simple standard deployment solutions in your environment for Windows, macOS clients, and browser extensions.

Data protection and encryption

Content stored from the Dash client or integrated applications is encrypted using FIPS 140-2, Level 3 cryptographic services via AWS Key Management Service (KMS), with key management processes handled by Dropbox.

Dash encrypts all data both in transit and at rest, and this is verified as part of our annual SOC 2 Type 2 audit. All Requests between Dash backend services and the public internet (including calls from Dash clients and calls to Cloud Service providers for Data Acquisition) are mediated by HTTPS. Requests between internal components of the Dash backend are encrypted using mutual TLS. Encryption at rest is handled transparently at the disk level for all Dropbox database technologies, while AWS S3 storage services are encrypted using Dropbox-managed keys on a per-customer basis.

Dash's infrastructure is currently multi-tenant, meaning that all customer data is stored in the same data stores. These data stores share the same mature security tooling used by Dropbox File Sync and Share, which includes extensive security auditing, monitoring and alerting as well as strict production access controls.

A multi-layered approach is taken to controls, including infrastructure-as-code controls, which require security peer review for modification.

Dash plans to introduce varying levels of optional data isolation in the coming months to provide customers even more confidence and flexibility for their most critical data.

Connectors

To allow search across company applications, Dash has pre-built integrations for productivity and business applications, such as Google Workspace, Salesforce, Microsoft Outlook, etc.

Dropbox Dash provides two types of connectors:

- **User connectors** allow individual team members to connect applications that are relevant to their work.
- **Company connectors** create a centralized connection to applications that are used organization-wide, like Google Drive, Microsoft OneDrive/SharePoint, Dropbox, and Confluence. Company connectors can be set up by administrators to shared applications at the organizational level, so that employees don't need to set them up individually. Select Company connectors allow administrators to govern data within these applications, and users to view content they're authorized to see.

These connectors are 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.

As Dash integrates with company services, we minimize access only to critical data elements to provide an optimal experience.

Dropbox Dash has created and partnered with solution providers to create a library of connectors that allow users 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.

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.

Company connector service accounts

Company connectors enable admins to create a centralized connection to apps that are used organization-wide, like Google Drive, Microsoft OneDrive, and Dropbox. Select company connectors also allow admins to manage file access permissions and secure sensitive cloud data from unauthorized sharing.

These are enabled through the use of service accounts. To understand more about service accounts and naming convention recommendations, see the links below. Each company connector setup guide provides instructions on how to create service accounts and how to connect each service to Dropbox Dash.

Learn more about admin implementation, and specific company connectors:

- **Admin Implementation Guide**
- **Company Connectors: One Drive**
- **Company Connectors: Google Drive**
- **Company Connectors: Dropbox**
- **Company Connectors: Confluence**

Once an admin has their service account ready, they can return to the Dash admin console and set up the respective company connector.

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 nines of durability.

Dropbox has extensive history with AWS and S3, and implements multiple levels of redundant controls over our infrastructure as code (IaC) deployments.

Source sync, index and ingestion controls

Built-in syncing ensures company content stays aligned with source connectors while allowing administrators to stay informed with status notifications and controls over what Dash indexes and ingests. Syncing speeds may vary between different third party services.

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. Users can make these requests through their admins, who can work with their account managers or contact **privacy@** for help with the request.

Dropbox systematically applies retention policies that govern the period of time personal data is retained. We also apply the principles of data minimization and purpose limitation to only keep data for as long as we have use for it.

Sub-processors

To enable provision of our Dash Services, Dropbox may engage sub-processors with access to customer personal data. Before we engage with sub-processors, Dropbox performs due diligence on sub-processor privacy, security, and confidentiality practices and executes appropriate contractual measures regarding protection of personal data. You can find a list of our sub-processors **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.

For more information about Dropbox's privacy practices and processes, visit the **Privacy and Data Protection Whitepaper**.

Compliance

Certifications, attestations, and regulatory compliance

Customers all over the world trust Dropbox with their most sensitive data. Dash was built with the same priority on security to meet the highest industry standards. 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 are now actively working towards achieving ISO 27001 certification in Q4 2024, further strengthening our security framework. View earned regulator certifications and information on security, compliance, and privacy so you can see how Dash's security stacks up to competitors. Access the latest security policies in real time and stay up to date about how we keep your company data and information secure.

Dash currently is certified by or complies with:

- **SOC 2 Type II:** Dash meets the Trust Services Criteria for Security, underscoring our commitment to industry standards and the protection of our clients' data.
- **CCPA:** Dash is committed to safeguarding the security and privacy of our users' data and is in compliance with CCPA.
- **EU - US DPF:** 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.

Reports for Dropbox Dash are available upon request. For more information, see **Dropbox Trust Center**.

Share security findings

Help Dash stay secure. If you believe you have found a security vulnerability in Dash's product offering, please email your findings to **dash-security@dropbox.com**.

We also have a bug bounty program that provides an incentive for researchers to identify and responsibly disclose software bugs. Issues can be reported by submitting a report to **Bugcrowd**.