Dokkio Security & Privacy Practices

Updated: November 2020

Summary

Dokkio is a cloud software service that helps your team find, organize, understand and collaborate on the cloud files that you use every day, or on archives of files you have used in the past. To accomplish that mission, with your specific permission, Dokkio connects to the various cloud accounts where your files "live", such as:

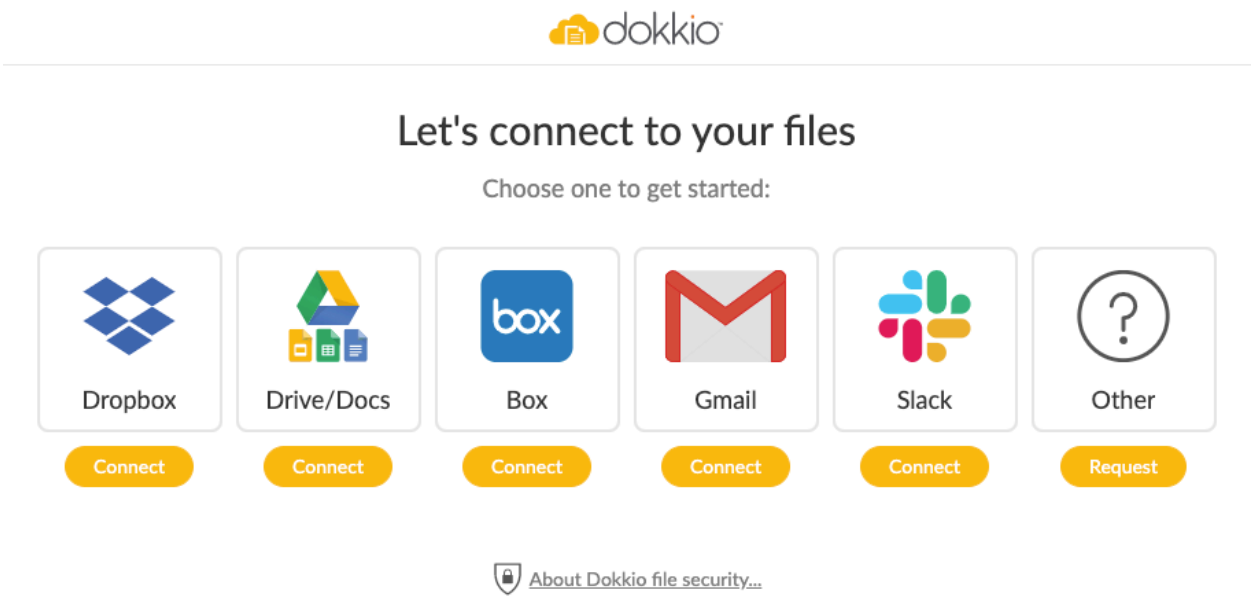
- Dropbox or Google Drive accounts where files are stored & shared
- Email accounts where files are attached to email messages
- Team communication tools, such as Slack, where files are shared

Dokkio aims to provide a "one-stop shop" for searching and organizing files "wherever they live". We are steadily adding to the list of cloud file sources that Dokkio supports. The principles and concepts described in this document apply to the file sources that we currently support, and the ones we plan to support in the future.

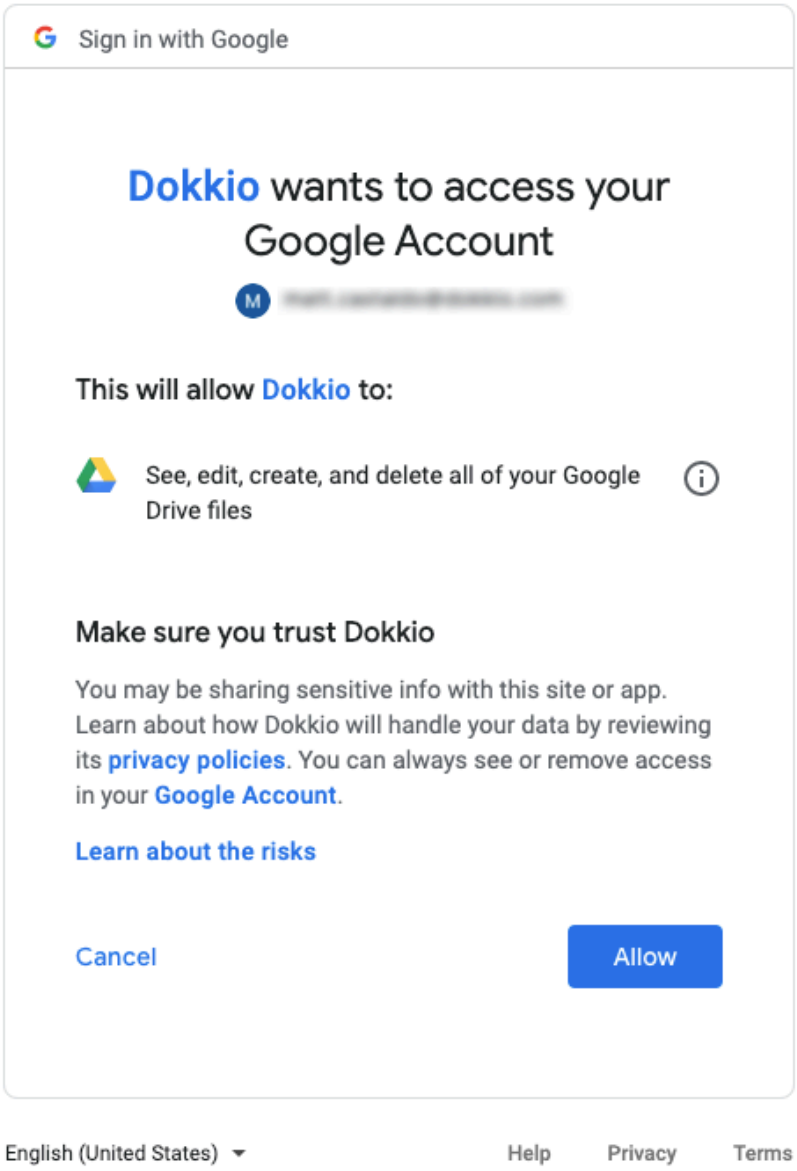
Dokkio takes the security and privacy of your files very seriously. We believe that the Dokkio product must earn your continued use, by delivering clear, compelling value. Further, the Dokkio product must earn your trust if you connect it to files that contain sensitive or confidential information. This document describes how the Dokkio product, and Dokkio as a company, safeguard the security and privacy of your files.

Dokkio Accesses Only What You Authorize

Each Dokkio user connects Dokkio to one or more file sources which contain the files they want Dokkio to understand and work with. As a user, you specifically ask Dokkio to connect to the sources that you choose during the setup process. Here is a typical account setup screen that illustrates this choice:



When you choose one of the cloud providers (such as Google Drive/Docs, for example), Dokkio tells you what will happen during the setup process, as shown here:



The cloud service that manages the files (the “provider” of those files - Google Drive, in this case) specifically asks for your permission to allow Dokkio to access your files. You explicitly give Dokkio permission using a secure web page that is managed by the provider. The provider

will typically ask for your username and password, or it may use 2-factor authentication or other methods to verify your identity when you give access permission.

Because that interaction is directly between you and the provider, Dokkio does not observe your password or other means of identification.

If you explicitly tell the provider that you give permission, Dokkio receives an access token that it subsequently uses to access the files managed by that provider. This access token is securely stored by Dokkio, as described in a later section. If you deny permission, Dokkio has no access.

Dokkio connects only to the specific cloud accounts that you choose. Many people have two or three (or more) Google accounts, for example, or they may have a Personal Dropbox and a Business Dropbox. You can choose to connect specific accounts, and may choose to not connect others. This gives you, the user, control over which of your files and accounts Dokkio can access.

Dokkio Adheres to & Enforces Provider Access Controls

When you connect Dokkio to one of your cloud accounts, Dokkio accesses the files that it manages using your own, personal credentials. For example, if you connect Dokkio to a shared business Dropbox as mary.jones@acme.com, Dokkio will have access only to the files that you can access directly in Dropbox, logged in as Mary Jones. Dokkio will not have access to any of the files that your colleagues have stored in that same business Dropbox, unless they have specifically granted access permission to "Mary Jones", just as you would not have any access to their files if you are directly logged into Dropbox.

Similarly, if you connect Dokkio to your Google Mail account (using the account mary.jones@acme.com, for example), you will see only files attached to emails that you have sent or received. The files attached to emails that your colleague, robert.smith@acme.com, has sent or received are not visible to you, just as those emails and files are not visible to you when you are logged directly into gmail.

The access restrictions are simply stated – when you connect to a provider (Google Drive, Dropbox, Slack, etc.) using Dokkio, you have access only to the files that you would have access to if you were logged in to the provider directly. In this way, Dokkio abides by and enforces the access restrictions that are already set up in Dropbox or Drive, for example, to whom you have already entrusted your files.

The access restrictions already set up in the provider also govern the types of access that you have via Dokkio. If you have the ability to only view certain files or folders within a shared Dropbox, for example, but not to edit or move or delete them, then you will have exactly those capabilities, and no more, when accessing those files or folders via Dokkio. Again – Dokkio enforces and maintains the access restrictions already set up in the underlying trusted provider.

Dokkio Gives You Granular Control Over What's Connected

It's often convenient to connect an entire cloud storage account to Dokkio – for example, connect an entire Dropbox, or an entire Google Drive. When you do this, Dokkio can use the comprehensive view of your files to help it understand and present them in an organized way.

You can also connect Dokkio to only some of the files in your cloud storage. Perhaps you want to use Dokkio only with the folders that contain Marketing and Sales files, but not with the folders that contain Engineering or Finance files, for example.

Dokkio lets you select exactly which folders and files are connected, down to the level of an individual folder or folders. You can choose to connect only specific folders when you first set up your Dokkio account, and each time you connect a new cloud account to Dokkio. And you can expand or contract the scope of files connected to Dokkio at any time. This capability puts you, the user, firmly in control of exactly which folders are connected to, and visible through, your Dokkio account.

Finally, you can change the selection of which files and which folders are connected to Dokkio at any time. Using the Settings Menu, you can disconnect an entire cloud account from your Dokkio account at any time. You can also revoke Dokkio's access from your Dropbox, Google Drive, Slack, Gmail, or other cloud account. And you can add or restore access to a cloud account at any time, using the same Settings Menu. Dokkio analyzes and displays only the files in the folders and accounts you have connected, putting you in complete control.

Dokkio's Use of File Information Is Limited

Dokkio uses information about the files that you connect – file names, file metadata (such as size and revision date), and file contents (images & text) solely to support its mission of helping you find, organize, understand and collaborate on your files. Complete information about how Dokkio does and does not use files and any personally identifiable information, and your privacy rights when using Dokkio, is contained in the Dokkio Privacy Policy, at www.dokkio.com/privacy, and linked from the Dokkio website.

Dokkio's business model is subscription-based. Dokkio does not sell information about you or your files to any third parties. Dokkio does not use its information about you or your files to target advertising or promotion. We offer the Dokkio as a free service to new users, and we begin to charge a monthly subscription fee for the service if and when your usage exceeds certain thresholds (sometimes called a "freemium" model). Our revenue and growth depends on the quality and value delivered by the Dokkio software, not on selling advertising, nor on selling insights about you or your files to third parties.

Dokkio software uses its access to your files in order to:

- Build and maintain a search index to let you search connected files by name and contents
- Analyze text file contents to suggest metadata, such as file categories or tags, or the names of customers or projects, to characterize and present an organized view of your files.

- Analyze image file contents to suggest metadata, such as file categories or tags, to characterize and present an organized view of your files
- Create and maintain preview images of connected files, so that you can view file previews and contents as you use Dokkio to find, organize, and collaborate on files.

Dokkio uses aggregated data about user interactions – such as whether users accept or reject Dokkio's suggestions – to improve the quality of its analysis and suggestions. Similarly, Dokkio uses data about the sequence of user interactions to improve the quality of the Dokkio user experience. This data about user interactions is controlled by the same confidentiality and privacy standards and obligations that govern access to your file contents.

The Dokkio Service Is Secure

Dokkio is accessed using a web browser, using the same techniques used by the web clients of Dropbox, Google Drive, Slack, Gmail, OneDrive and other popular cloud services. Dokkio's interaction with the user is managed by Javascript software running in the user's web browser. Dokkio's interaction with the user's files is managed by Dokkio server software running in a highly secure environment under Amazon Web Services (AWS). All communication between the Dokkio server software and the user's web browser uses secure (HTTPS) encrypted communication, with the same level of encryption used by cloud services from Google, Dropbox, Slack, Box and Microsoft.

A user can only login to and use the Dokkio service after they have proved their right to access a particular Dokkio account which they created or two which they have been invited. Access to a Dokkio account can be protected by an email address and a Dokkio password. Or the user can authenticate to Dokkio using their Google or Microsoft or Facebook identity. For security-conscious accounts, Dokkio recommends using Google/Microsoft/Facebook authentication, which supports additional security restrictions such as single sign-on or two-factor authentication. There is no requirement that the user establish their own Dokkio password; Dokkio accounts offer complete functionality when a user operates with Google-based authentication, for example.

Dokkio's client-side software is secured by the interaction with the user's web browser (such as Google Chrome or Safari or Firefox or Microsoft Edge), using the same techniques used by the web interfaces of Google Drive, Dropbox, Slack or Gmail. Only temporary files and data (relevant to the current browser session) is stored by the browser. Dokkio uses a standard cookie structure to identify a specific user across sessions.

Dokkio's server-side software runs in a secure Amazon Web Services (AWS) environment. Permanent information about a user's files is encrypted and stored in a secure Postgres database and/or a secure Elastic Search service and AWS-managed caches. All data is encrypted at rest, and all communication with Dokkio's client-side software and among components of Dokkio's server-side software is encrypted. Encryption keys are managed by AWS key management services for security.

Dokkio Enforces Security with Employees & Contractors

Dokkio personnel (whether employees or contractors) are individually bound by confidentiality agreements to protect the privacy and confidentiality of your files and information. Dokkio personnel have access to information about your files (such as the information stored in Dokkio databases) on a "need to know" basis. Dokkio uses industry best practices to isolate access to user data from functions that do not require such access, such as software development. All Dokkio software is peer-reviewed prior to being deployed in our test environment, and tested before production deployment, both to ensure code quality and to protect against introduced security vulnerabilities.

All Dokkio personnel with any potential access to user files or information undergo a full third party reference check prior to starting work. Personnel access to your files is strictly controlled by our privacy policy. Employees and contractors will only view the contents of your files with your explicit permission, and if you grant that permission, our use of your files is restricted to resolving reported issues and supporting your use of the Dokkio service.

Dokkio Complies with Google's Security Standards

Beginning in 2019, Google established security standards for any software (such as Dokkio) that uses Google APIs to access information stored and maintained by Google services (such as Google Drive and Gmail). The standards are designed to ensure that services like Dokkio "do exactly what they say they do" when accessing user files and data. In order to continue using the Google APIs, Dokkio must pass an annual audit which includes:

- Review by Google Engineering, which conducts an evaluation of the Dokkio product, functionality and policies for conformance to Google standards
- Review by a Third Party Security Auditor, which conducts an evaluation of the Dokkio product, security policies and practices, and validation of Dokkio security against intrusion

Dokkio fully adheres to and complies with the security standards required by Google.

Dokkio Welcomes Your Security and Privacy Questions

We want you, as a Dokkio user, to be confident that you can trust the Dokkio service and Dokkio organization. If you have any questions or concerns about security and privacy, simply email us at security@dokkio.com, and we will respond promptly.