



Web



Overview



WEB > GUIDES > PSPDFKIT SERVER > OVERVIEW

PSPDFKit Server security



PSPDFKit Server has been deprecated and replaced by [Document Engine](#). To migrate to Document Engine and unlock advanced document processing capabilities, refer to our [migration guide](#). Learn more about these enhancements on our [blog](#).

We deliver PSPDFKit for Web as a Docker container deployed on-premises or in the cloud (AWS, Azure, Google Cloud, and others) by you.

We have no access to a deployed instance, including documents or annotation data. PSPDFKit Server does perform regular license checks. If you have specific requirements that don't offer internet access, ask our [sales team](#) about alternative license verification methods.

Data access

There are three ways PSPDFKit Server can be accessed:

- 1 Your backend uses the [server API](#) to get full access to all documents, annotations, and other data stored on the server. This API is protected by a [configurable API access token](#).
- 2 Your backend signs [JSON Web Tokens \(JWTs\)](#) asserting that the holder of such a token is allowed to access a given document. It then passes them to your client apps using PSPDFKit for Android, iOS, and Web. Your apps then pass it to PSPDFKit Server to prove they have access to the claimed document.



ASK AI

- 3 Your team uses the optional [dashboard](#), which gives access to all documents uploaded to PSPDFKit Server. The optional dashboard is protected with a configurable username and password.

To limit the possible attack surface area, you can disable the optional dashboard completely by setting the username and password configuration options to empty strings, or by not setting them at all.

Network

We strongly recommend following these practices to improve security and privacy from a network perspective:

- 1 Enable HTTPS. Since PSPDFKit Server doesn't support serving traffic over HTTPS, run a load balancer or reverse proxy with HTTPS support in front of Server. If you deploy to the cloud, you can rely on your cloud provider's HTTPS termination (e.g. [AWS Application Load Balancer](#)). When running on-premises, you can set up HTTPS using [nginx](#) or [Caddy](#).
- 2 Disable dashboard and server API access from the internet. PSPDFKit Server serves its internal API used by PSPDFKit for Web, the [server API](#), the [client API](#), and the [dashboard](#) on the same port. However, only the internal API needs to be exposed to the internet so that your application using PSPDFKit for Web can access it. To achieve this, configure your load balancer or reverse proxy so that only HTTP requests that target paths starting with `/i` are allowed. In addition, if you also use the client API in your application, make sure to allow paths that start with `/documents`.
- 3 Unless your application specifically requires it, disable [document creation from a URL](#) by setting `ALLOW-REMOTE-DOCUMENTS` to `false`. If your application uses this feature, exercise the principle of least privilege by configuring your network firewall or container service to prevent URL resolution from untrusted sources.

Data encryption

PSPDFKit Server fully supports encryption in transit and at rest, depending on your underlying platform.

Encryption in transit is achieved by enabling HTTPS. You can read more about it in the previous section.

PSPDFKit Server delegates encryption at rest to the underlying platform: If you implement encryption at rest for your Docker and PostgreSQL hosts, PSPDFKit Server's data will be encrypted at rest as well.

Was this helpful?

 YES

 NO

Questions? [Contact us](#)

