AppSheet

Google Cloud

AppSheet Security and Compliance FAQ

What is AppSheet?

AppSheet is a no-code, web-based mobile app design platform. Using a web browser, you can connect to your data, design an app and publish to your audience in minutes. You can learn more here.

Is AppSheet GDPR/CCPA compliant?

Appsheet is a part of the Google Cloud family of products. Just like with the many other Google products available - G Suite, Cloud SQL, and other services - we are committed to these ongoing compliance initiatives. You can learn more about these topics here.

Is AppSheet SOC compliant?

Yes. Appsheet is SOC2 Type 2 audited. Our SOC Report is available to customers under NDA and upon request.

Where can I see AppSheet's privacy policy?

Appsheet is part of the Google Cloud product suite and the privacy policy is located here. AppSheet is also a member of the Privacy Shield Framework.

Does Appsheet have a data processing and security terms sheet?

Yes. Details for that are available here.

Does Appsheet capture IP addresses or Geolocation of my audience?

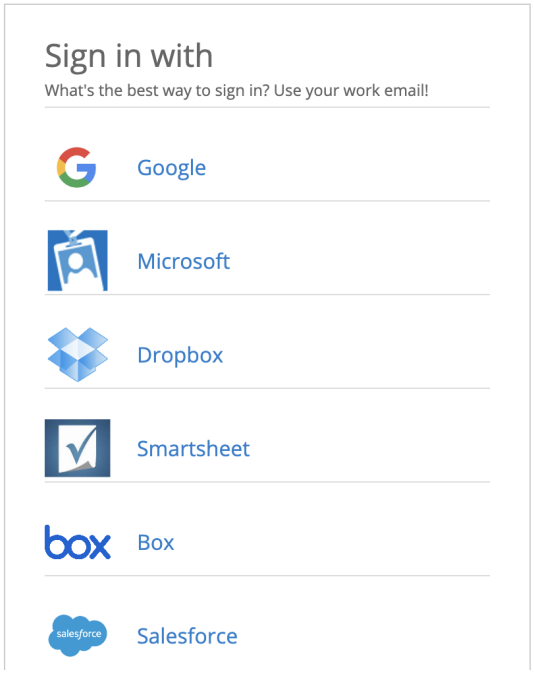
Not by default. The platform itself does not capture this information in any server-side logs. Inside of an individual application, you can design a column to capture the current latitude and longitude for a record. In this case, the end user will be warned that the application will request access to their current location.

What are the details of the Appsheet architecture?

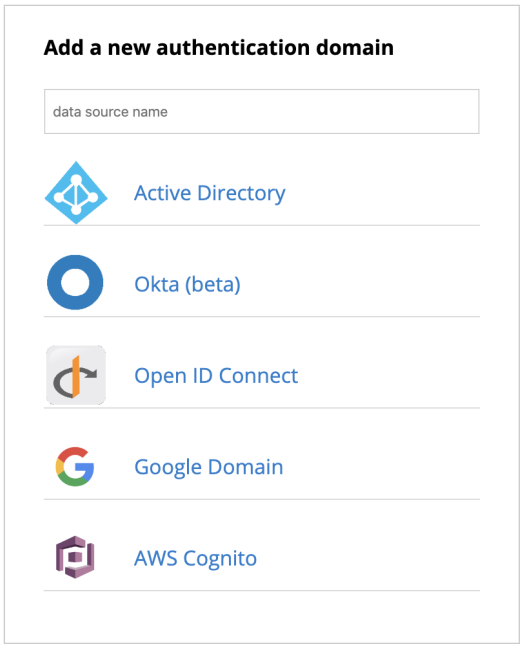
Appsheet is a 100% SaaS platform. Appsheet runs on Google Cloud Computing services and provides high availability across the globe using several availability zones. A list of specific services, logical entity maps, and topologies are available to customers under NDA by request.

How do I authenticate against AppSheet?

AppSheet not only supports but ***requires*** SSO using one of the following providers:



We also have robust *domain authentication* support using one of the following providers:



We never store your authentication credentials in our cloud. Instead, during the single sign on (SSO) process, an oAuth token is issued to the device (either browser on laptop, or token on device), after which you are identified as a valid user in our platform.

What types of compliance information do end users see during authentication?

There are different permissions requested of app creators (people who build apps) versus app users (people who use those apps on browsers or devices). We strive to only ask for the minimum permissions needed to perform either of these two roles. You can learn more about the process here.

Does AppSheet support Azure Active Directory groups for authentication?

Yes, you can authenticate against AD group(s) in AppSheet if they are cloud-based Azure AD groups. More information is available here.

Does AppSheet support Google Auth for authentication?

Yes, if they are google domain groups. Google smtp/email groups are not supported. You can get started with domain authentication here.

Does AppSheet support Domain Groups for authentication?

In some cases we can integrate with domain groups, e.g. via Google Groups, AD Groups, and Okta. Custom groups defined in your IDP can then be leveraged for roles-based access inside of individual applications. You can read more about this here.

Is there granular control over which users can see which applications?

Yes. Each app in your organization can have its own security. You can either A) explicitly list users, B) enable domain auth support for this one application, or C) Enable domain group support if your provider supports that feature. You can learn more here.

Do you store our data in your cloud?

We do not! AppSheet is a “pass-through” platform. Your data starts and ends at your location, and passes through the appsheet platform for usage, processing, workflows and so forth. We never store your data in our cloud.

Is my data encrypted during transit?

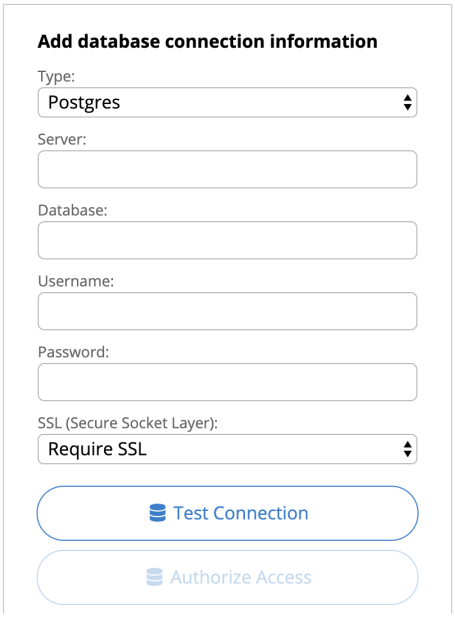
Yes, via HTTPS using TLS at all times.

Is my data encrypted at rest?

Since your data is never stored in the AppSheet cloud, this is a factor of your existing data stores and not a question for the AppSheet platform.

If AppSheet connects to my (e.g.) Postgres database in the cloud, how are credentials managed?

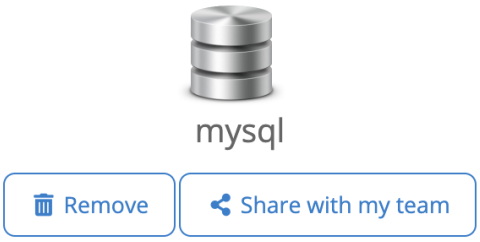
When connecting to your cloud database for the first time, we need the hostname, port, username and password to connect:



After this has happened, we store the database credentials in our platform using AES256 encryption.

After I connect to a database, can any AppSheet user in my org connect to that database?

Not necessarily. This is controlled by you, the original designer of the app and the person who originally connected to the database store. Once you build a database connection, you can optionally share it with your Appsheet team. AppSheet also includes team governance features to allow you to control who can access which shared database resources.



Does AppSheet have row and column - level security (e.g. authorization)?

We 100% support this at very granular levels. Here are some examples (not inclusive!):

- Rows can be secured using data-driven concepts e.g. “this team can only see their team’s data”
- Columns can be secured e.g. “if the current user is a member of a [piece of data-driven] role called ‘admin’ then show this column”
- Entire views in your app can be shown or displayed.
- AppSheet Actions, Workflows and Reports can be secured.
- Generally: show-if logic can be applied to almost any element inside of an Appsheet application.

Where are the AppSheet services offered? What cloud zones are you available in?

Currently USA, EU, AU, and SP zones. However, we support access from the entire globe and currently have 170+ countries using our platform. Additionally, note that the US is considered a valid data processor for EU and GDPR purposes per existing adequacy rules. More information on infrastructure is available upon request and under NDA with Google Inc.

What support does AppSheet have for Pii or other sensitive information?

Appsheet has logs which can be turned down to the minimum retention of one day. Inside each application, AppSheet also allows you to designate information (columns) as “Pii sensitive”. This designation will strip this information from our platform’s logging and audit trail entirely. To learn more about this feature go here.

Does AppSheet have a Rest API for inbound requests?

Yes. You can invoke add, delete, edit, find, and {run action} (a previously built AppSheet Action inside of your app). We have several help articles to get you started. To learn more start here.

Does AppSheet have a webhook mechanism for outbound API requests?

Yes. You can add webhooks to AppSheet workflows. These can perform post, put, patch and delete requests. You cannot, however, receive back a response or a result set from invoking a webhook. To learn more, go here.

Can AppSheet connect to my on-premise database

As a SaaS platform, Appsheet expects your SQL databases to be network-available to our cloud. You can use IP firewall whitelisting which is documented here to enable access from our cloud platform to your SQL instance. Optionally, you can expose your SQL instance via API Management or another web front end, and then connect to that front end using Appsheet's Rest API support.

How is AppSheet secured on individual devices?

After initial authentication, AppSheet inherits the security protections of the device on which it is installed - we do not require login for each session of the app. We recommend two-factor or MFA on your devices as well as ensuring that the device has a locking mechanism in place. All device and browser security is pass-through from Appsheet's point of view, and all requirements for 2FA or MFA are part of the single sign-on process, after which your Appsheet session will be allowed or denied accordingly.

What types of governance features does Appsheet include

Appsheet Enterprise version includes account-level policies and governance features which then control all behaviors across the entire account. These can include restricting which Appsheet designers are allowed to publish apps, which types of data sources can be connected to, which types of end users are allowed to access apps, and many more examples. You can get started with policy management here.