This page describes authentication information for calling Web Security Scanner APIs.

The Web Security Scanner API supports the following authentication methods. To make calls against the API, use the techniques described below.

Service accounts are recommended for almost all use cases, whether you are developing locally or in a production application.

To use a service account to authenticate to the Web Security Scanner, follow the instructions to create a service account (/iam/docs/creating-managing-service-accounts#creating_a_service_account). Select **JSON** as your key type.

After you create a service account, your service account key is downloaded to your browser's default downloads location.

If you call the Web Security Scanner API directly, such as by making an HTTP request with cURL, you'll pass your authentication as a bearer token in an `Authorization` header. To get a bearer token using your service account, follow the steps below:

1. Install the `gcloud` command line tool (/sdk/downloads#interactive).
2. Authenticate to your service account, where ***key-file*** is the path to your service account key file:

3. Get an authorization token using your service account:

The command returns an access token value.

4. When you call the API, pass the token value as a `bearer` token in an `Authorization` header:

Roles limit an authenticated identity's ability to access resources. When you build a production application, only grant an identity the permissions it needs to interact with applicable Google Cloud APIs, features or resources.

For more information about these roles, see Web Security Scanner access control (/security-scanner/docs/access-control).