This topic describes authentication information for Security Command Center.

Security Command Center supports the following authentication methods.

Service accounts are recommended for almost all use cases, whether you are developing locally or in a production application. For an example of how to set up authentication with a service account, see Accessing Security Command Center programmatically (/security-command-center/docs/how-to-programmatic-access).

For more information about setting up authentication with a production application, see setting up authentication for server to server production applications (/docs/authentication/production).

You can authenticate users directly to your application, when the application needs to access resources on behalf of an end user. For most use cases, we recommend using a service account instead (#service-accounts).

Examples of why to use user accounts with Security Command Center include:

If your application uses end user authentication, you need to specify OAuth scopes when making a method call. See Security Command Center reference (/security-command-center/docs/reference/rest) for per-method OAuth scopes.

For more information about setting up authentication with user accounts, see authenticating as an end user (/docs/authentication/end-user).

Roles limit an authenticated identity's ability to access resources. When building a production application, only grant an identity the permissions it needs in order to interact with applicable GCP APIs, features, or resources.

For more information about these roles, see Security Command Center access control (/security-command-center/docs/access-control).

- To learn more about GCP authentication, see the authentication guide (/docs/authentication/).