This page explains how to use user-managed service accounts and their private keys to authenticate an application to the Cloud IoT Core API.

You can use applications to administer registries and devices. See Registry Management Samples (/iot/docs/samples/registry-management-samples) and Device Management Samples (/iot/docs/samples/device-manager-samples) for examples of how to do so.

A user-managed service account (/iam/docs/service-accounts#user-%0Amanaged_service_accounts) is a type of Google account that represents an application. User-managed service accounts are primarily used for server-to-API authentication.

This page does not describe service accounts that are created and owned by Google in order to manage roles and ssions for different services. For example, when you first enable the Cloud IoT Core API for a project, a new service ac /docs/service-accounts#google-managed_service_accounts) for the project is automatically assigned a role to enab ning to Pub/Sub topics. For details, see Creating a Device Registry docs/how-tos/devices#iam_role_for_pubsub_publishing).

Cloud IoT Core uses two types of authentication. When authenticating devices to Cloud IoT Core, you use private/public key pairs (/iot/docs/how-tos/credentials/keys) and JSON Web Tokens (/iot/docs/how-tos/credentials/jwts). When authenticating an application to the Cloud IoT Core API, however, you must use GCP authentication (/docs/authentication) in the form of user-managed service accounts.

User-managed service accounts have their own private keys, which come in various formats. By providing a user-managed service account's private key to an application, you can create credentials and authenticate the application.

The recommended way to authenticate applications is to use user-managed service accounts and private JSON keys, as they are the most widely supported and flexible methods. You can create a user-managed service account and download a private JSON key by completing the steps in Getting Started with Authentication (/docs/authentication/getting-started).

The following samples show how to use a user-managed service account's private JSON key to authenticate an application to the Cloud IoT Core API: