# Google Cloud Service Account Key Rotation Plug-in

The Google Cloud Service Account Key Rotation plugin allows Secrets Broker to rotate the service account keys in Google Cloud. By default, service account keys in Google Cloud never expire and there is no auto rotation. If a key was accidentally leaked, it could be used for authentication. However, with this plugin, the service account key can be rotated and the previous key will be deleted, making any new authentication attempts with it fail.

The plugin only supports running in reverse flow mode. The rotation interval can be configured in days, from 1 to 1,000. Unfortunately, Secrets Broker will cal the plugin every 60 seconds. The plugin will ignore those calls, but it causes Secrets Broker to write an error message in the log file. Those errors can safely be ignored. You will see the following:

2024-11-30 10:59:01.415 -07:00 [INF] Getting Password for account managedbysafeguard@devtest-oid-rnd-amer-safeguard.iam.gserviceaccount.com to GoogleCloudServiceAccountKey.

2024-11-30 10:59:01.415 -07:00 [ERR] Unable to get the Password for managedbysafeguard@devtest-oid-rnd-amer-safeguard.iam.gserviceaccount.com to GoogleCloudServiceAccountKey.

That is normal.

## Google Cloud Service Account Key Rotation plugin specific configuration

### Plug-in Details

* **Supported Credential Types** - Password
* **Supports Reverse Flow** - Yes, it only supports reverse flow. Running in normal mode will throw an error.
* **Project Id** - The Google Cloud Project ID that contains your service account.

### Google Cloud

See images at end of document for some visual guidance on enabling the IAM API.

1. Log into your Google Cloud project at <https://console.cloud.google.com/>.
2. If your Google Cloud was created after May 3, 2024, you will need to remove the iam.disableServiceAccountKeyCreation constraint.
   1. See <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#disable_service_account_key_creation> for more details.
   2. If iam.disableServiceAccountKeyCreation is enforced, creating a service account will fail with the error:  
      *FAILED\_PRECONDITION: Key creation is not allowed on this service account*.
   3. You can also consider an expiry time for all newly created keys in your project.  
      <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#limit_key_expiry>
3. Enable the IAM API:  
   <https://cloud.google.com/iam/docs/keys-disable-enable#before-you-begin>  
   or  
   <https://console.cloud.google.com/apis/dashboard?project=><your project>  
   then click the ***Enable APIs and Services*** link at the top.
4. Create a new service account that will be added to Safeguard for Privileged Passwords and used as the "service account key admin", responsible for rotating all other service account keys.
   1. Navigate to IAM & Admin → Service Accounts. Or just search for *Service Accounts*.
   2. Choose to create a new service account.
   3. Assign the roles/iam.serviceAccountKeyAdmin role.
      1. Note, the account you are currently logged in with must have the necessary permissions to grant this role. If you don't see or have this option, then you will need to have someone else create the service account.
   4. The service account should then have permissions to list, add, and delete keys on all other service accounts. If you want to restrict access to specific service accounts, then you will have to adjust permissions accordingly.
   5. After the service account is created, go to the **Keys** tab and click the **Add Key** to create a new key pair.
   6. Choose **JSON** for the key type.
   7. The private key will be downloaded and saved to your local computer as a file. The contents of the file will be used in the next step.
5. Create a new asset and account in Safeguard for Privileged Passwords to hold this Google Cloud service account credentials.
   1. Manually set the password on this Safeguard service account to the file contents of the JSON file that was downloaded from Google.
      1. Change the Password text box to *multi-line*. Then just copy and paste the JSON contents.
6. Configure the Secrets Broker plugin, specifying the key admin service account as the plugin's service account from Safeguard.
7. Add the key admin service account as a managed account of the plugin too, such that it's key will also be rotated.
8. Add any other Google Cloud service account to Safeguard and then to Secrets Broker to have the keys rotated.
   1. The account name must match that in Google Cloud, the fully qualified, email address like name. For example, managedbysafeguard@devtest-oid-rnd-amer-safeguard.iam.gserviceaccount.com.
9. The plugin stores new service account keys as the same JSON string that you get when creating a new key from the Google Cloud console web site.
   1. Your application must be able to parse the JSON and extract and use the private key accordingly.
   2. Note that any OAuth token created with the private key will be valid for the duration of its own lifetime (1 hour). After the OAuth token is created, it is not subject to the private key being rotated/deleted.  
      See <https://cloud.google.com/iam/docs/keys-create-delete#deleting>
10. Service account keys are rotated according to the KeyRotationInDays configuration property, or whenever the Secrets Broker service is restarted. Keys are not rotated just because you stop and start the monitoring of Secrets Broker. The plug-in stores its own *"last updated"* in-memory cache that is only cleared when the plug-in is completely unloaded.

