Mandiant

SCALE GOOGLE CLOUD INTEGRATION

The Mandiant Advantage Attack Surface Management (MA-ASM) Google Cloud Integration leverages Google Cloud's Service Account Impersonation. By creating a service account and delegating account access, MA-ASM can assume control of the service account and fetch the respective resources. This technique is easy and prevents both applications from having to persist credentials.

This document provides steps on how to create the Google Cloud integration at scale to allow MA-ASM access to all projects in your organization.

Scaling information for Google Cloud integration configurations

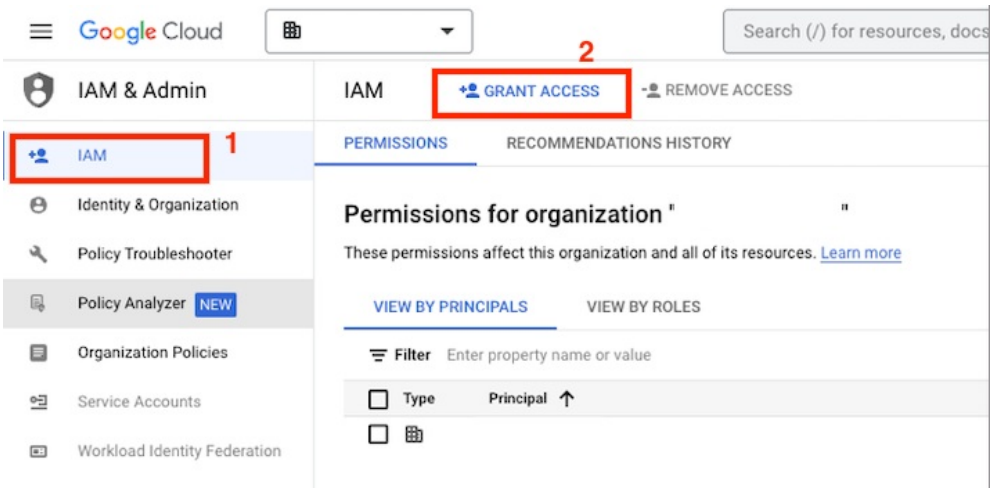
Follow either Method A or Method B as outlined in the **ASM Google Cloud Integration (https://docs.mandiant.com/home/asm-gcp-integration)** documentation and incorporate the following steps, as directed:

- **Additional steps to scale using Method A: Creating a Service Account through Google Cloud Console**
- **Alternative steps to scale using Method B: Creating a Service Account through gcloud CLI**

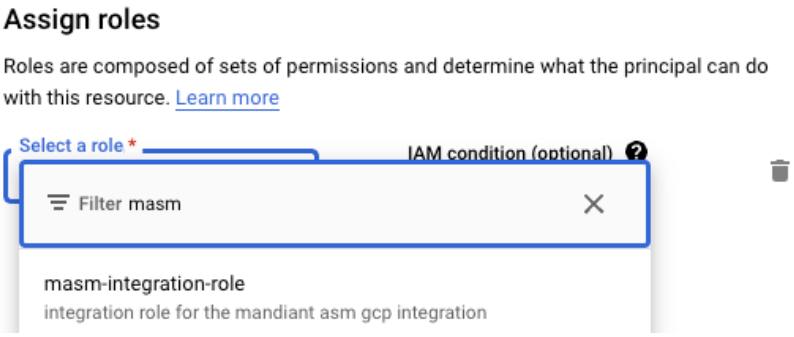
Additional steps to scale for **Method A:** Creating a Service Account through Google Cloud Console

Follow steps 1 through 12 as outlined in **Creating a Service Account through Google Cloud Console (https://docs.mandiant.com/home/asm-gcp-integration#method-a)**. Then:

1. Browse to the **IAM settings (https://console.cloud.google.com/iam-admin/iam)** for your organization and click **GRANT ACCESS**.

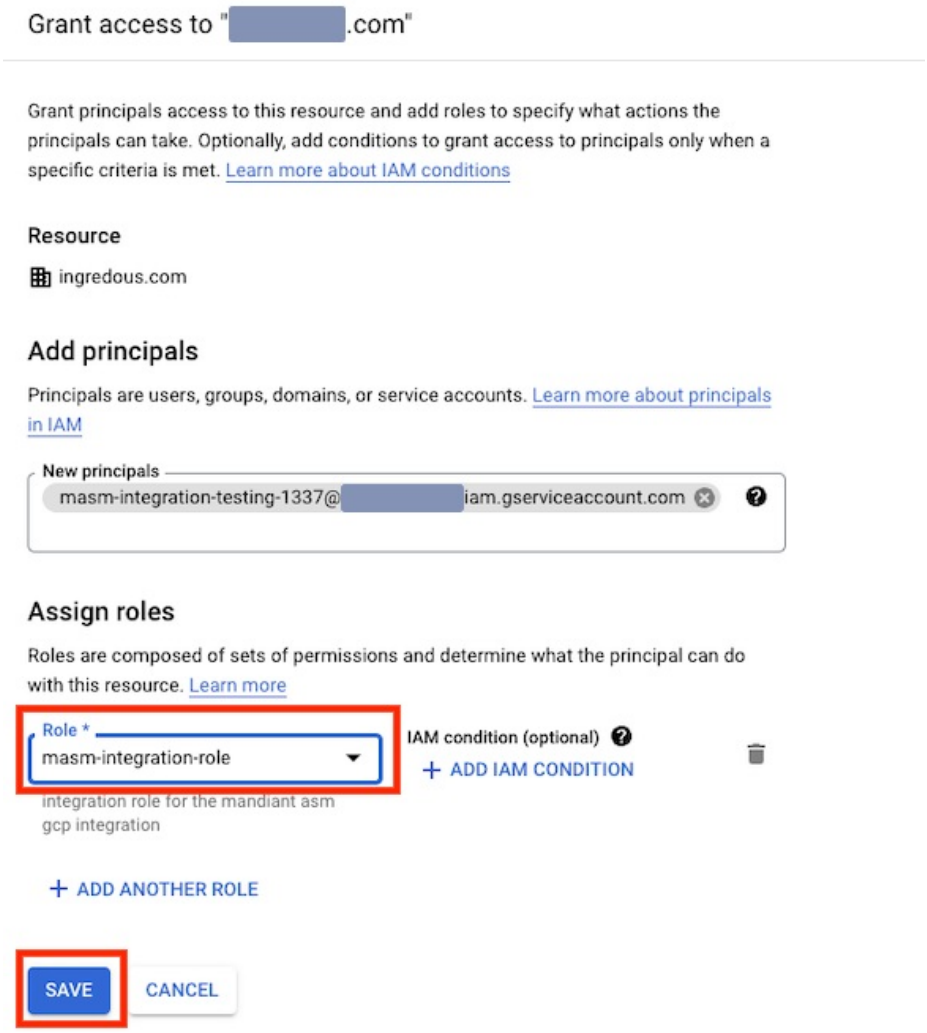


2. In the **Grant Access** interface, in the **New principal** field, enter the email belonging to the service account that was created for the **ASM Google Cloud Integration (https://docs.mandiant.com/home/asm-gcp-integration)**.
3. In the **Select a role** field, search for and select the role that was created in **step two of Creating a Service Account through Google Cloud Console (https://docs.mandiant.com/home/asm-gcp-integration#role)**.



If the role does not populate, ensure that the role was created at the organizational level.

4. Click **Save.**



5. Return to and complete **step 13 of Creating a Service Account through Google Cloud Console (https://docs.mandiant.com/home/asm-gcp-integration#enable-apis)**.

Alternative steps to scale using **Method B:** Creating a Service Account through gcloud CLI

Mandiant

Google Cloud only allows service accounts to be created at the project level, not the organizational level. Roles, however, are created at the organizational level and then assigned to the service account to provide organization-wide access. Therefore, the steps outlined here look similar to the steps outlined in **Method B: Creating a Service Account through gcloud CLI (https://docs.mandiant.com/home/asm-gcp-integration#method-b)**.

PROJECT_ID and *ORGANIZATION_ID* are variables. Therefore, where relevant in the following commands:

- Replace *PROJECT_ID* with the ID of your Google Cloud Project.
- Replace *ORGANIZATION_ID* with the Organization ID belonging to your organization.

To see a list of all the projects in your organization and their respective Project IDs, run the following command:

```
gcloud projects list
```

To access your Organization ID, run the following command:

```
gcloud organizations list
```

1. Make sure you're authenticated with Google Cloud through the gcloud CLI by running the following command:

   ```
   gcloud auth list
   ```

   The following output should be returned:

   ```
   Credentialed Accounts
   ACTIVE  ACCOUNT
   *       user.account@org.tld

   To set the active account, run:
     $ gcloud config set account 'ACCOUNT'
   ```

2. Set the project for which you would like the integration to fetch resources by running the following command:

   ```
   gcloud config set project PROJECT_ID
   ```

3. Create a custom role within Google Cloud that follows the principle of least privileges.
   Save the contents of the following YAML configuration:

   ```
   title: masm-integration-role
   description: integration role for the mandiant asm gcp integration
   stage: GA
   includedPermissions:
   - cloudasset.assets.listResource
   - dns.managedZones.list
   - dns.resourceRecordSets.list
   - resourcemanager.projects.get
   - apigateway.apiconfigs.get
   ```

   Using the gcloud CLI, run the following command:

```
gcloud iam roles create masm_integration_role
--organization ORGANIZATION_ID
--file=role.yaml
```

4. Create a service account.
   Using the gcloud CLI, run the following command:

```
gcloud iam service-accounts create masm-integration-svc-account
--description="Service Account for MASM GCP Integration"
--display-name="MASM GCP Integration Service Account"
```

5. Bind the role created in **step 3** to the newly created service account.
   Using the gcloud CLI, run the following command:

```
gcloud organizations  add-iam-policy-binding org_id
--member="serviceAccount:masm-integration-svc-account@PROJECT_ID.iam.gserviceaccount.com"
--role="organizations/ORGANIZATION_ID/roles/masm_integration_role"
```

6. Allow MA-ASM to impersonate your service account.
   Using the gcloud CLI, run the following command:

```
gcloud iam service-accounts add-iam-policy-binding masm-integration-svc-account@PROJECT_ID.iam.gserviceaccount.com
--member="serviceAccount:gcp-inbound-integration@asm-mcp-prod-01-f8ec.iam.gserviceaccount.com"
--role="roles/iam.serviceAccountTokenCreator"
```

7. Enable the `Cloud Asset API`, `Cloud Resource Manager API`, `Cloud DNS API`, and `API Gateway API` services. Using the gcloud CLI, run the following commands:

```
gcloud services enable cloudresourcemanager.googleapis.com
gcloud services enable cloudasset.googleapis.com
gcloud services enable dns.googleapis.com
gcloud services enable apigateway.googleapis.com
```

   If successful, each command should return output similar to:

```
Operation "operations/acat.p2-11111111111-88a9d5b4-c262-40fa-aeee-be6029ebfef3" finished successfully.
```

   If no response is returned, it is most likely because the service was already enabled.

> The `Cloud Asset API` and `Cloud Resource Manager API` must be enabled for all Google Cloud projects in-scope for MA-ASM.