GCP IAM Handover document

TABLE OF CONTENTS

1. Document overview

- This document includes details about deployment of GCP IAM for quest diagnostics.
- It also includes all the infrastructure details configured for this setup. (Took recommendation from google team)
- Includes details like
  - Authentication overview
  - Single Sign-on
  - Provisioning Users/Groups
  - Role assignment
  - Service Accounts

2. Authentication Overview

For GCP, user authentication is implemented via SAML federation to the Quest's Microsoft Entra ID (Azure AD) system. This setup delegates authentication to Entra ID, enforcing all configured policies, including Multi-Factor Authentication (MFA) once enabled.

2.1 Single sign-on: Whenever a user needs to authenticate, Google Cloud delegates the authentication to Microsoft Entra ID by using the Security Assertion Markup Language (SAML) protocol.

Having Cloud Identity delegate authentication to Microsoft Entra ID not only avoids having to synchronize passwords to Google Cloud, it also ensures that any applicable policies or multi-factor authentication (MFA) mechanisms configured in Microsoft Entra ID are enforced.

Single sign-on has been configured with an administrator account to the Google Admin Console (https://admin.google.com/).

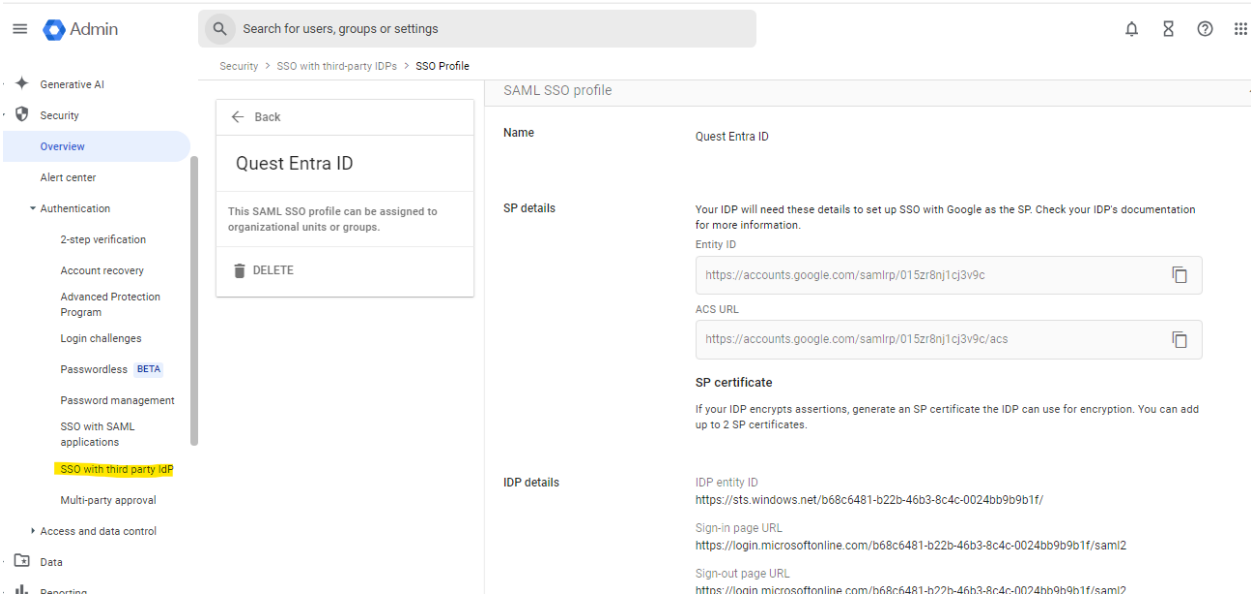
2.1.1 SAML SSO profile: SAML SSO Profile named "Quest Entra ID" has been configured and enforced for implementing SSO.

SP details: Below details have been configured in Entra ID to setup SSO with Google as the SP.

Entity ID	https://accounts.google.com/samlrp/015zr8nj1cj3v9c
ACS URL	https://accounts.google.com/samlrp/015zr8nj1cj3v9c/acs

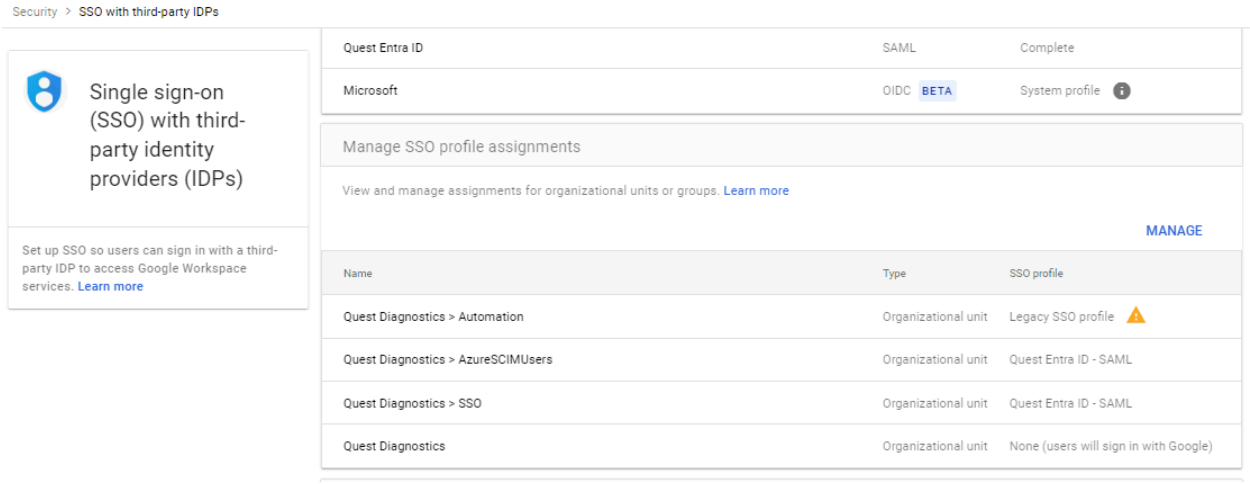
IDP details: Details received from Entra ID as part of SAML enablement as listed below.

IDP entity ID	https://sts.windows.net/b68c6481-b22b-46b3-8c4c-0024bb9b9b1f/
Sign-in page URL	https://login.microsoftonline.com/b68c6481-b22b-46b3-8c4c-0024bb9b9b1f/saml2
Sign-out page URL	https://login.microsoftonline.com/b68c6481-b22b-46b3-8c4c-0024bb9b9b1f/saml2
Change password URL	https://account.activedirectory.windowsazure.com/changepassword.aspx
Verification certificate	Expires Nov 20, 2027



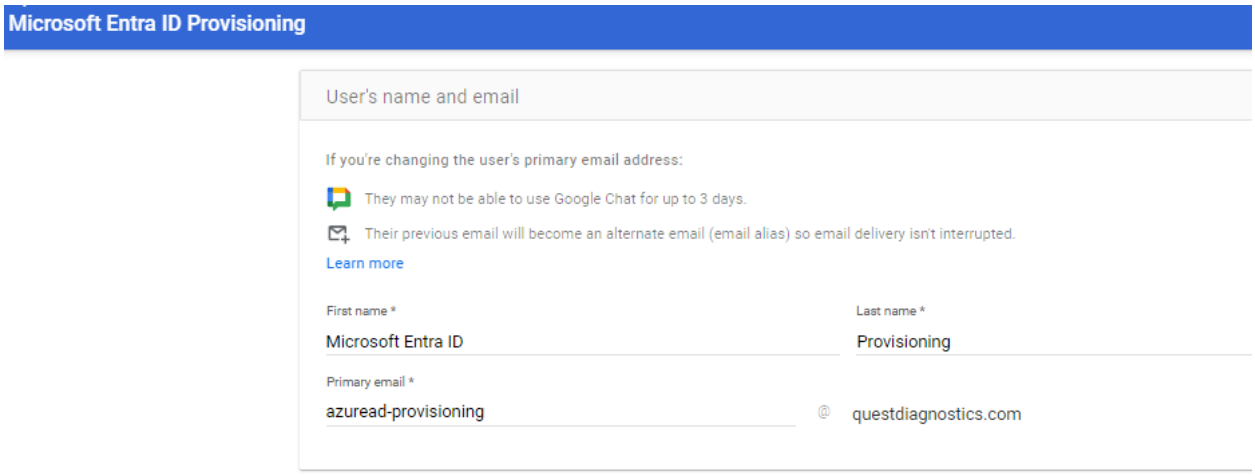
2.2.2 SSO Profile Assignment: Decide which users should use SSO

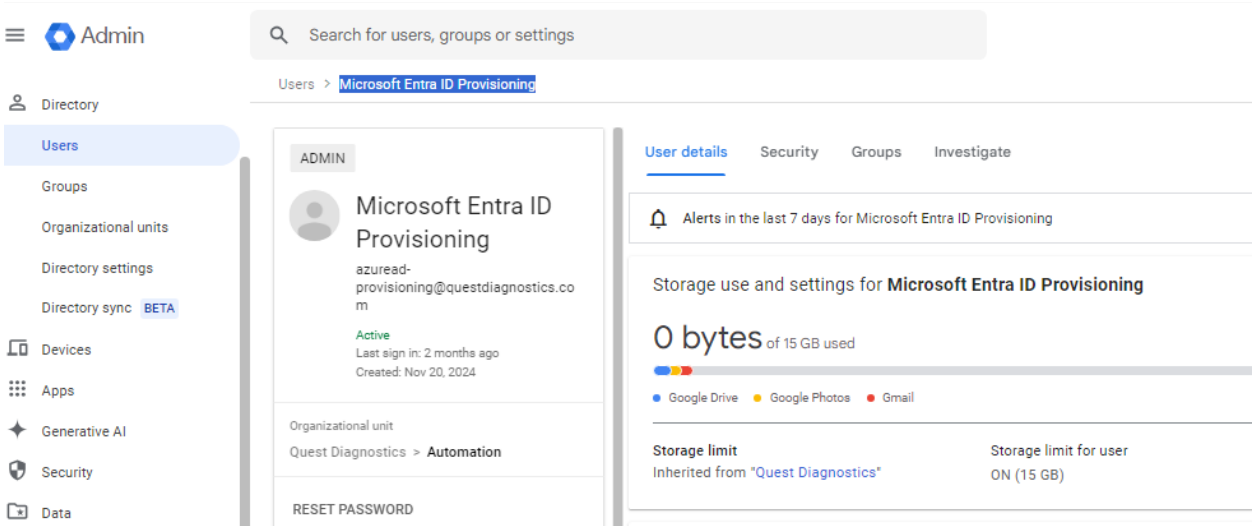
Turn SSO on for an organizational unit or group by assigning an SSO profile and its associated IdP. Or turn SSO off by assigning 'None' for the SSO profile. Above mentioned SAML SSO profile has been assigned to designated OU for enforcing SAML Authentication.



3. **Provisioning Users/Groups**
   Relevant users and groups are synchronized periodically from Microsoft Entra ID to Cloud Identity via GCDS Enablement. This process ensures that when we create a new user in Microsoft Entra ID or synchronize a new user from Microsoft Entra ID it's made available in Google Cloud so that it can be referenced in Google Cloud even before the associated user has logged in for the first time. This process also ensures that user deletions are being propagated.

To let Microsoft Entra ID access Cloud Identity a Microsoft Entra ID user (azuread-provisioning) is created which is only intended for automated provisioning. Newly created user is placed in the "Automation" OU.





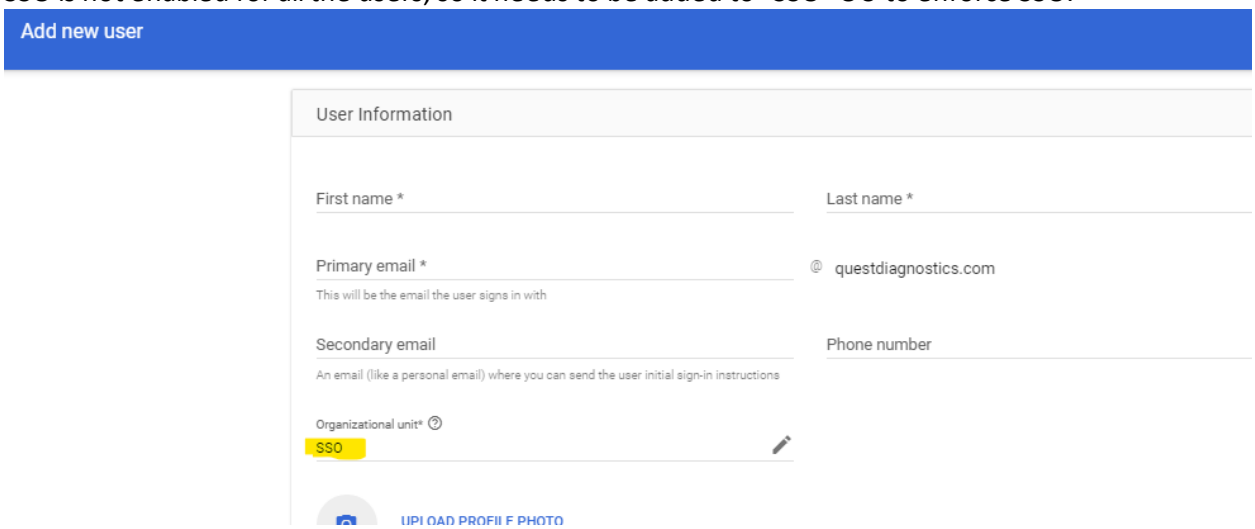
To allow Microsoft Entra ID to manage all users, including delegated administrators and super-admin users, "azuread-provisioning" user has been assigned super-admin role in google admin console.
To Configure Microsoft Entra ID provisioning to Google Cloud Identity an enterprise application has been created in Entra ID by setting up the *Google Cloud/G Suite Connector by Microsoft* gallery app from the Microsoft Azure marketplace.

<Until cleanup of existing unmanaged users is completed, SCIM cannot be turned on. While those items are being worked and closed any groups manually created in GCP must also be created and populated in AD via SNOW ticket. Currently, Users and groups are created manually in admin

console for enabling access and role assignment>.

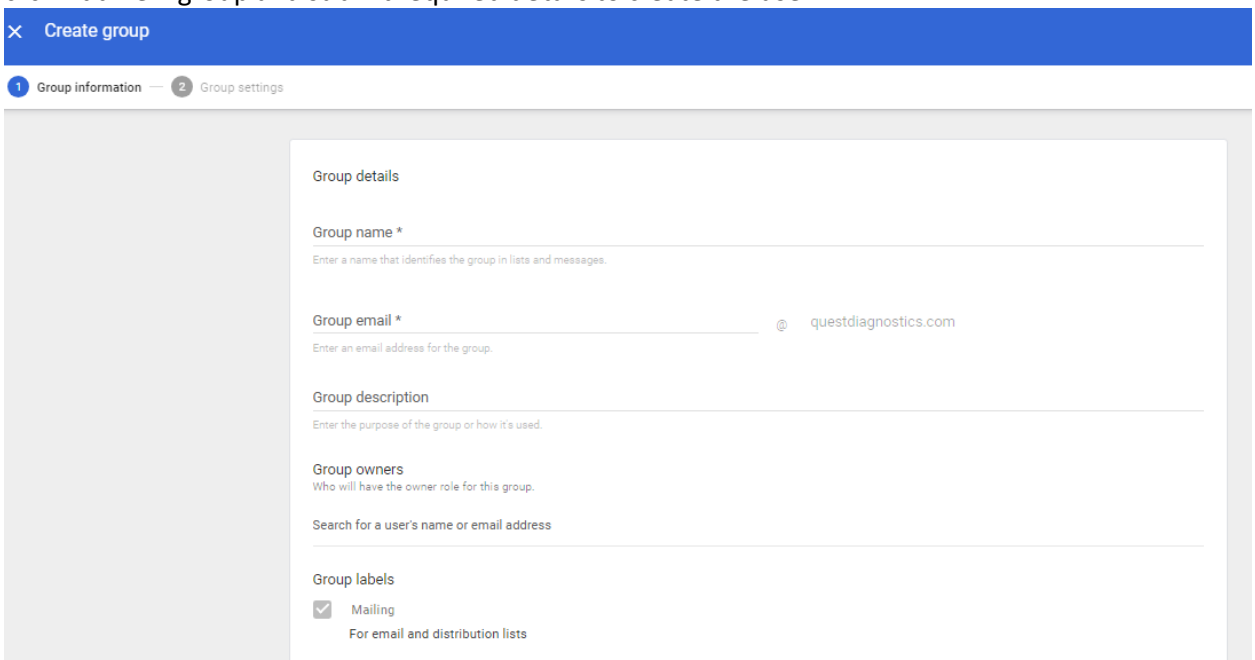
4. User creation in google admin console

Sign in with an administrator account to the Google Admin console and navigate to Menu>Directory>Users, click Add new user and submit required details to create the user. Currently SSO is not enabled for all the users, so it needs to be added to “SSO” OU to enforce SSO.



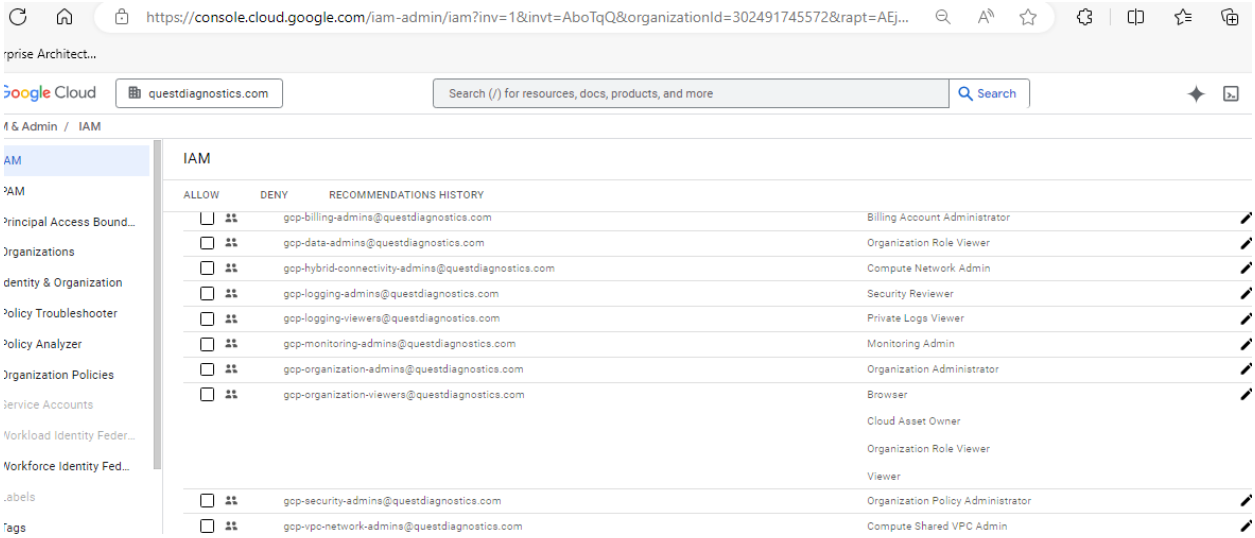
5. Group creation in google admin console

Groups can be created as per naming convention suggested in TIDD. Sign in with an administrator account to the Google Admin console and navigate to Menu>Directory>Groups, click Add new group and submit required details to create the user.



6. Role provisioning

Groups can be assigned permissions via roles at different levels in the hierarchy from organization wide to folders or individual projects. This is known as 'binding' and is managed within GCP, typically through an infrastructure-as-code tool such as terraform.
After SCIM enablement AD groups would be synchronized to GCP, allowing us to leverage existing AD group memberships for cloud access control. By assigning GCP IAM roles (like admin, editor, or viewer) to these synced groups, you can grant broad permissions while using deny rules and custom roles within GCP to achieve fine-grained restrictions.



7. Service Account

Service accounts are utilized by applications and virtual machines to authenticate their access to Google Cloud APIs. This specialized account has its own identity, and applications leverage its credentials to authorize their interactions with a designated set of APIs. The actions that these applications can perform are governed by the permissions that have been specifically assigned to the service account.
Below mentioned service accounts were identified as part of Infrastructure deployment which are to be used by applications directly that need the service account's privileges.

Service Accounts for creation during landing zone deployment

GCP Project	SeviceAccount	Roles
prj-boot-iac-us-4000	sa-boot-iac-us-4000	roles/storage.admin
prj-shrd-ntwk-3	sa-fortigate-iac-us-4001	roles/config.agent roles/compute.networkAdmin roles/compute.admin roles/iam.serviceAccountUse roles/storage.objectViewer
prj-ospacker-useast-dev-23295	sa-ospacker-us-4002	roles/compute.instanceAdmin.v1 roles/iam.serviceAccountUser roles/iap.tunnelResourceAccessor
prj-shrd-dev-67236	sa-composer-us-4001	roles/storage.objectAdmin
prj-eda-qadp-raw-dev-48699	sa-dataflow-us-4001	roles/storage.objectAdmin
prj-ghrunner-useast-dev-63055	sa-gkeghrunner-dev	roles/artifactregistry.admin roles/container.admin roles/container.nodeServiceAgent roles/iam.serviceAccountAdmin
prj-ghrunner-useast-prd-	sa-gkeghrunner-prd	roles/artifactregistry.admin roles/container.admin roles/container.nodeServiceAgent roles/iam.serviceAccountAdmin

Service Accounts for Data Foundation build

GCP Project	Service	SeviceAccount	Roles
prj-shrd-dev-67236	Cloud Composer	sa-use4-shrd-composer-dev	roles/storage.admin
			roles/composer.user
			roles/composer.worker
			roles/iam.serviceAccountUser
prj-shrd-ntwk-3	Cloud Composer	service-1046068350740@cloudcomposer-accounts.iam.gserviceaccount.com	roles/composer.sharedVpcAgent
	Dataflow		roles/storage.admin

prj-eda-qadp-raw-dev-48699		sa-use4-qadp-raw-dataflow-dev	roles/pubsub.publisher
			roles/pubsub.subscriber
			roles/iam.serviceAccountUser
			roles/dataflow.worker
			roles/dataflow.admin
			roles/artifactregistry.writer
prj-eda-qadp-raw-dev-48699	Snowflake	sa-use4-qadp-raw-snowflake-dev	roles/storage.objectAdmin
prj-cus-qaw-dev-66576	QuickSight	sa-use4-cus-qaw-quicksight-dev	roles/bigquery.metadataViewer
			roles/bigquery.jobUser
prj-shrd-ntwk-3	Dataflow	service-<476093664680@dataflow-service-producer-prod.iam.gserviceaccount.com	roles/compute.networkUser
prj-eda-qadp-raw-dev-48699	Dataflow	service-476093664680@dataflow-service-producer-prod.iam.gserviceaccount.com	roles/dataflow.admin
			roles/dataflow.worker
			roles/dataflow.serviceAgent
			roles/compute.networkUser
			roles/storage.objectAdmin
			roles/iam.serviceAccountUser
prj-eda-qadp-raw-dev-48699	Compute	476093664680-compute@developer.gserviceaccount.com	roles/dataflow.worker
			roles/storage.objectAdmin
prj-eda-qadp-int-dev-33915	Compute	476093664680-compute@developer.gserviceaccount.com	roles/bigquery.dataEditor
			roles/bigquery.jobUser
			roles/bigquery.user
prj-cus-qaw-dev-66576		zz_gcp_qadp_qs_dev	roles/bigquery.jobUser
prj-cus-qaw-dev-66576		zz_gcp_qadp_qs_dev	roles/bigquery.metadataViewer
prj-eda-qadp-raw-dev-48699		zz_gcp_qadp_ms_dev	roles/storage.objectAdmin
prj-cus-qaw-dev-66576		zz_gcp_qaw_db_dev	roles/cloudsql.admin
prj-cus-qaw-dev-66576		zz_gcp_qadp_qs_dev	roles/bigquery.jobUser
prj-eda-qadp-bus-dev-68801		zz_gcp_qadp_qs_dev	roles/bigquery.jobUser

8. Github Repositories

Below is the link for Github repositories and workflows used for IAM related deployments.

https://github.com/QDXEnterpriseOrg/dso-gcpfoundation-iac-iam

Link is accessible only to Dev Leads group. To obtain DevLeads access, it can be requested with "dgx-github-platform-admin" <dgx-github-platform-admin@questdiagnostics.com> to get added to the AD group - "azrgh-team-dso-gcpfoundation-iac-devlead-1"