Microsoft Entra Permissions Management

Onboarding

<Name>

<Job role>

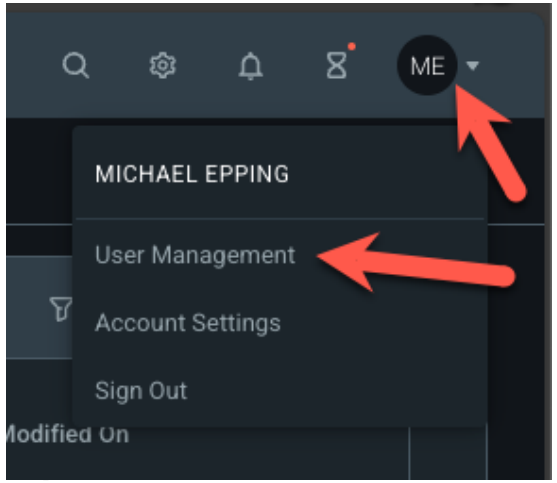
Agenda

- Microsoft Entra Permissions Management RBAC Configuration
- Azure
- AWS
- GCP

MEPM RBAC Configuration

MEPM Roles

Roles → Manage from User Management menu



Recommendations

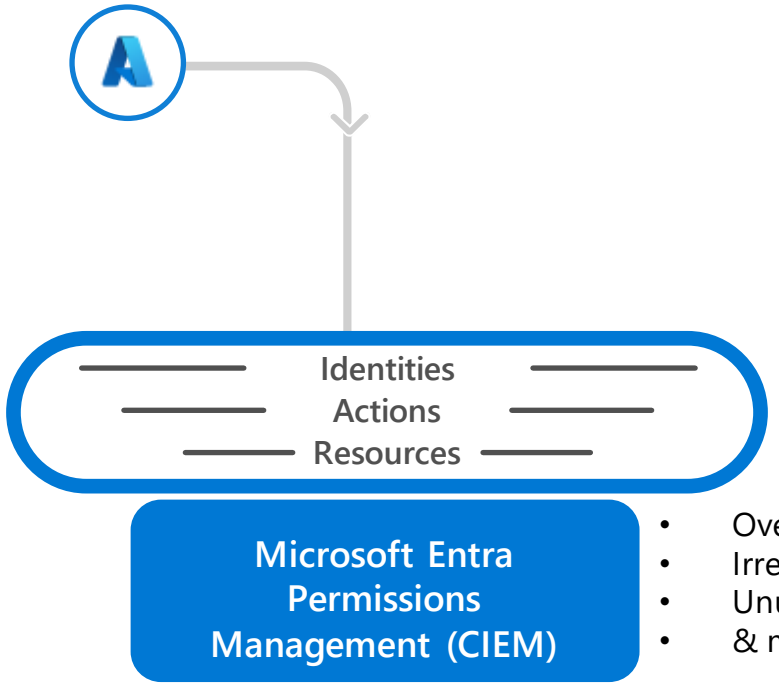
Azure AD Role: Global Administrator	Use only for initial setup of Entra Permissions Management
Azure AD Role: Permissions Management Administrator	Manage role through PIM and/or PIM Groups. Use for most “root user” tasks in MEPM rather than Global Administrator.
Custom MEPM Roles: Used to limit admins to specific Auth system types	Map to PIM-managed Azure AD Security Groups

Onboarding at a Glance

RBAC configuration

Azure	AWS	GCP
1. Add Azure Subscription 2. Authorization setting	1. Register Application to Entra ID 2. Run AWS template 3. Authorization setting 4. AWS Identity provider setting (Optional)	1. Register Application to Entra ID 2. Setup GCP OIDC project 3. Run script in Google cloud shell 4. Authorization setting

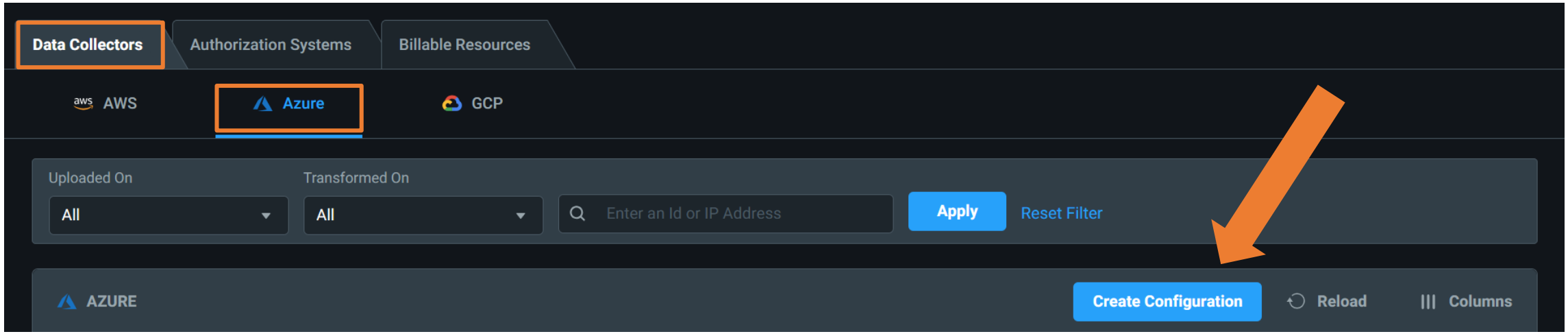
Azure Onboarding



- Over privileged identities
- Irregular permission pattens
- Unused permissions
- & more

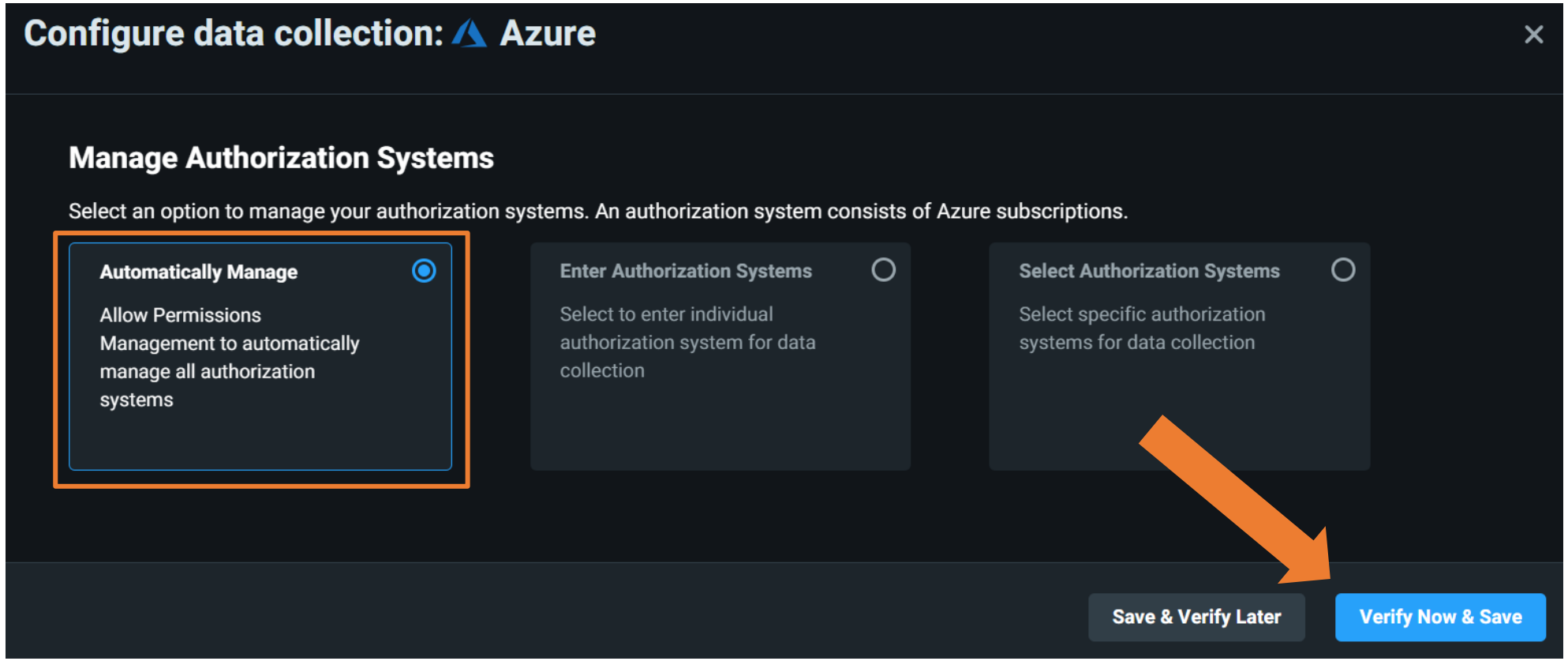
Azure Setup

1. Add Azure subscription details
   - In the EPM portal, navigate to the "Data Collectors" tab, select Azure, and click Create Configuration



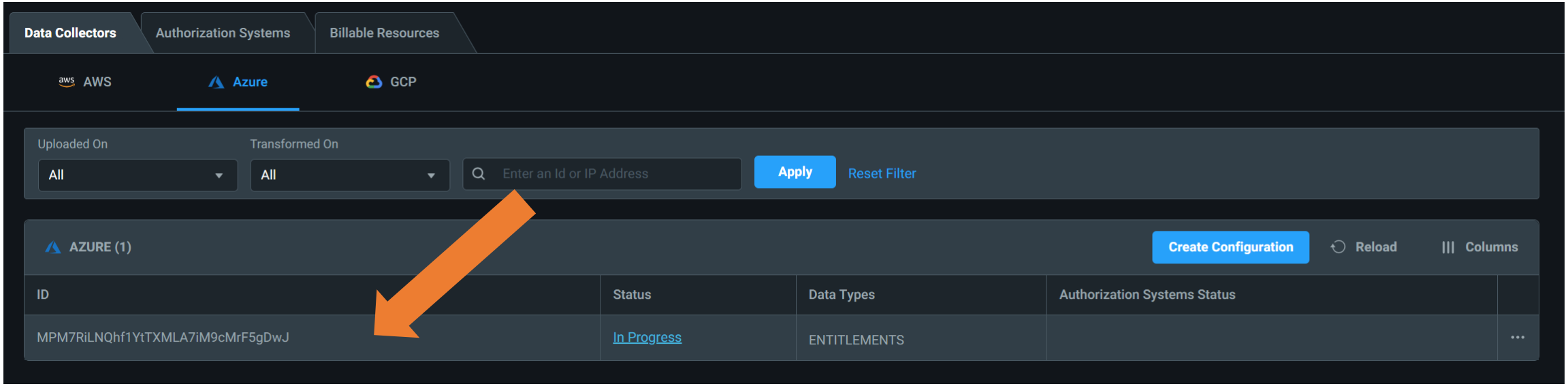
Azure Setup

2. Ensure Automatically Manage is selected. Click Verify Now & Save

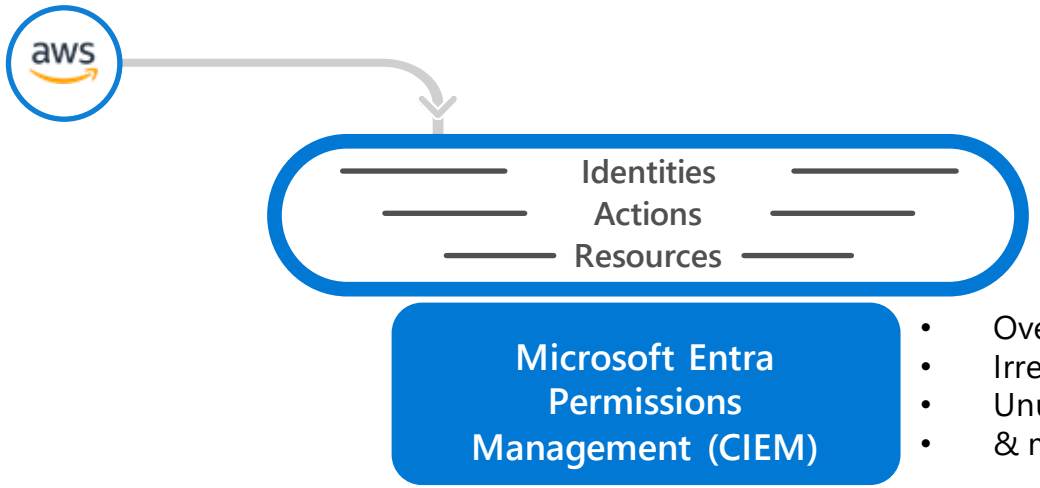


Azure Setup

3. You will now see the Azure Data Collector



AWS Onboarding



- Over privileged identities
- Irregular permission pattens
- Unused permissions
- & more

AWS Setup

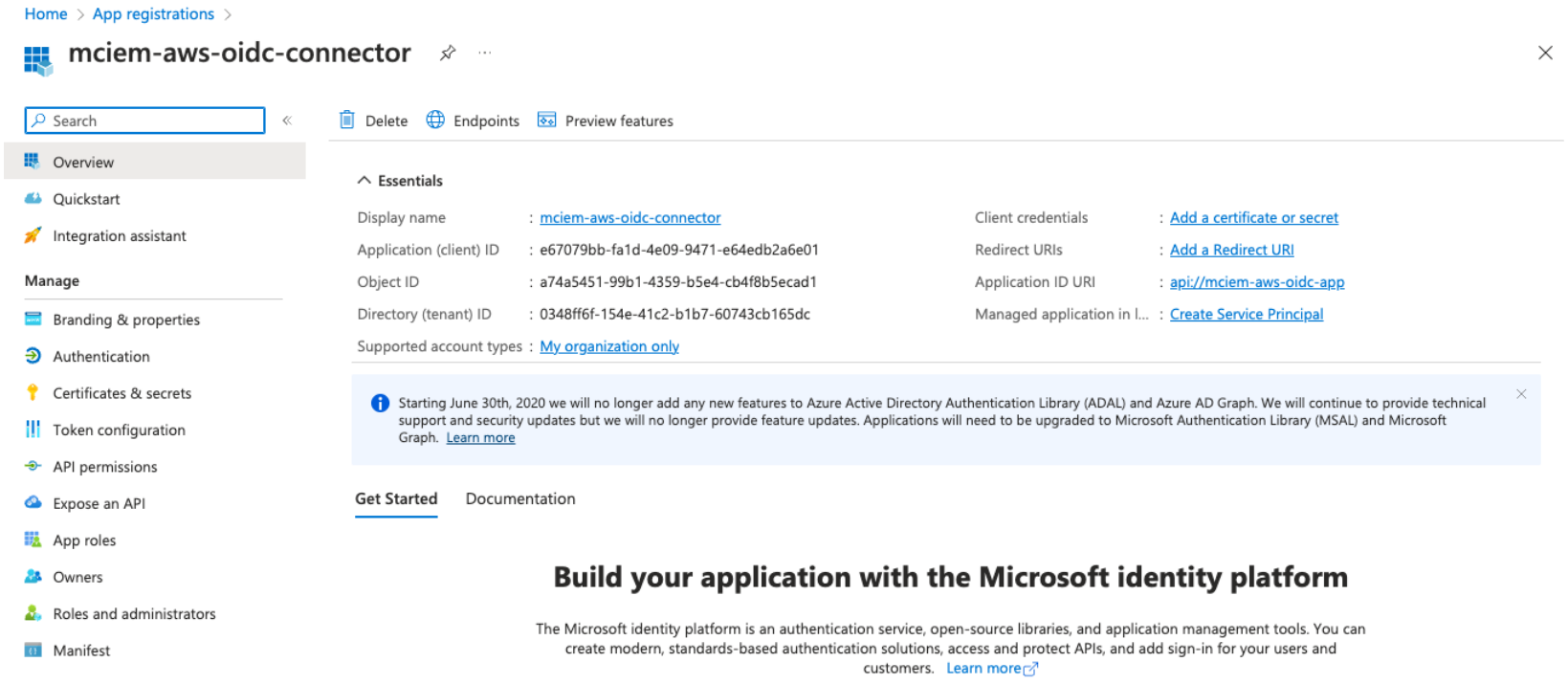
1. Azure AD OpenID Connect Application (App Registration)
   - Can be run by any role that can create app registrations
   - Recommend using Azure Cloud Shell for simplicity
   - App name and API can be customized if desired

```
#use this script for Azure version >3.7
az ad app create --display-name "mciem-aws-oidc-connector" --identifier-uris "api://mciem-aws-oidc-app" --sign-in-audience AzureADMyOrg

#PowerShell Script
New-AzureADApplication -DisplayName  "mciem-aws-oidc-connector" -IdentifierUris "api://mciem-aws-oidc-app"
```

```
michael [ ~ ]$ az ad app create --display-name "mciem-aws-oidc-connector" --identifier-ur
is "api://mciem-aws-oidc-app" --sign-in-audience AzureADMyOrg
```

AWS Setup

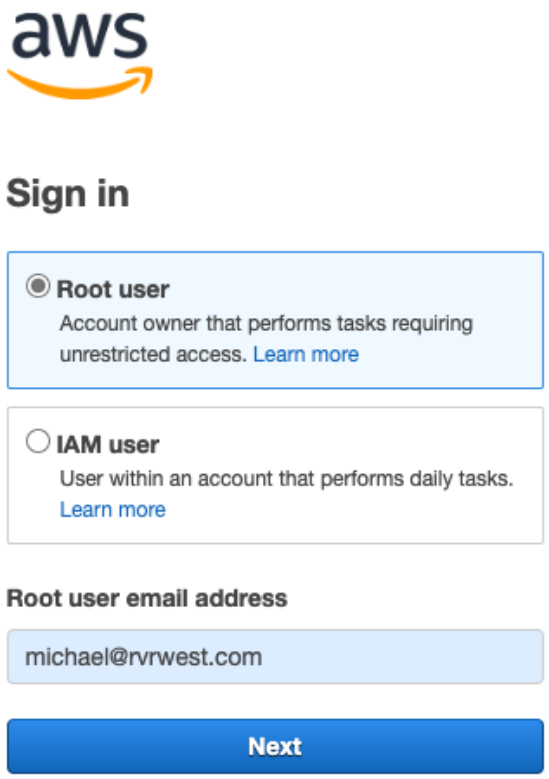
1. Azure AD OpenID Connect Application (App Registration)
   - Can be run by any role that can create app registrations
   - Recommend using Azure Cloud Shell for simplicity
   - App name and API can be customized if desired



AWS Setup

2. AWS Account OIDC Account ID

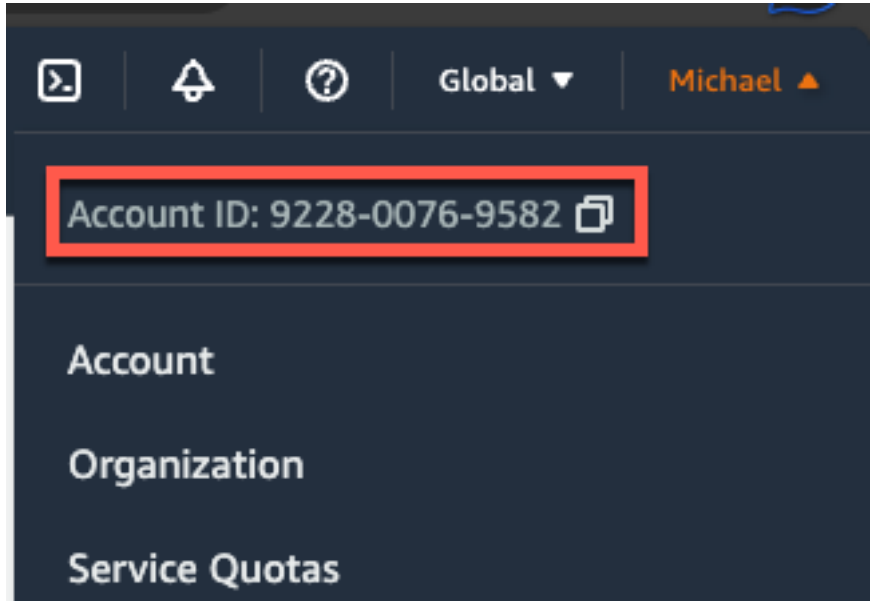
- If you aren't sure what this is, go to https://console.aws.amazon.com and login with your AWS Root user account:



AWS Setup

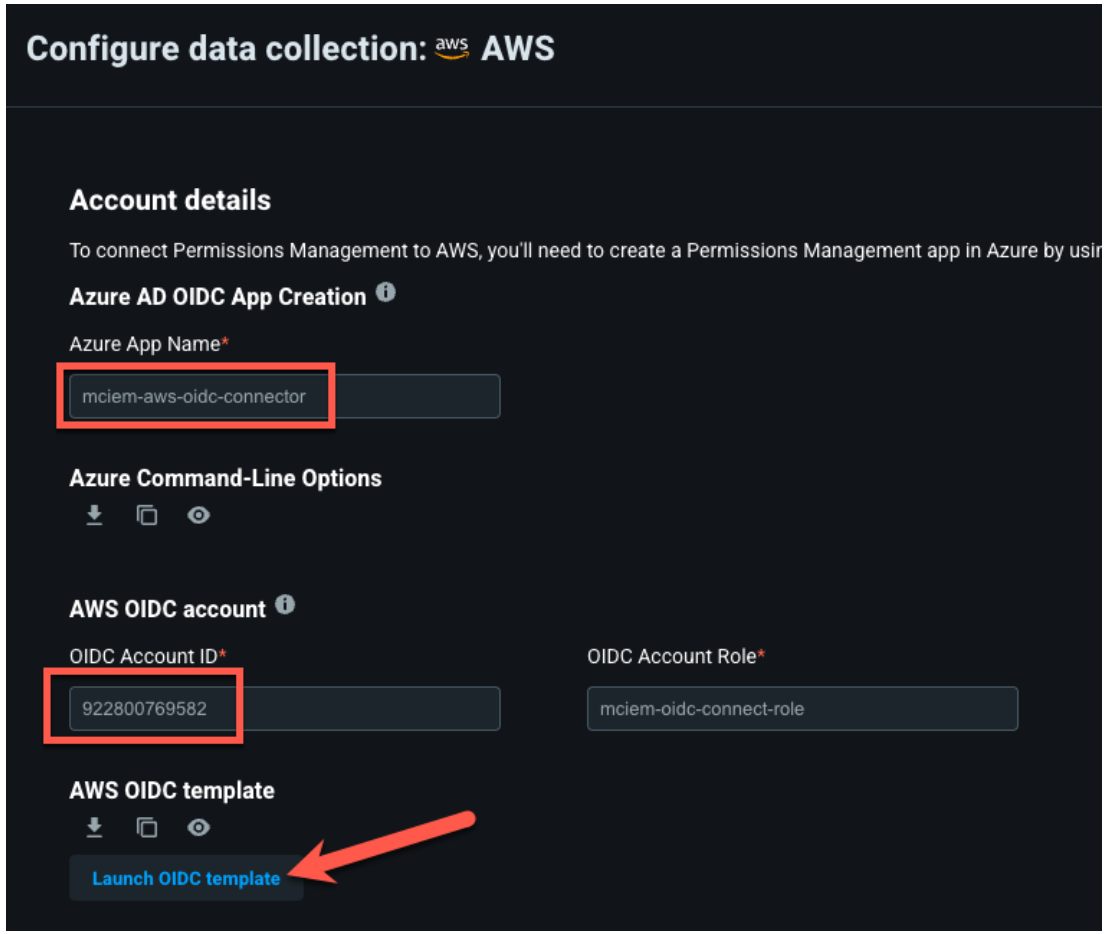
2. AWS Account OIDC Account ID

- Get the Account ID from the menu in the upper right corner of the portal:



AWS Setup

3. Run AWS Template
   - Provide the Azure App Name and OIDC Account ID identified in previous steps
   - Click the Launch OIDC template button



AWS Setup

3. Run AWS Template
   - An AWS CloudFormation template will open with the parameters already filled in
   - This is an infrastructure as code template, similar to Azure ARM templates
   - This particular template creates an OIDC provider on the AWS side

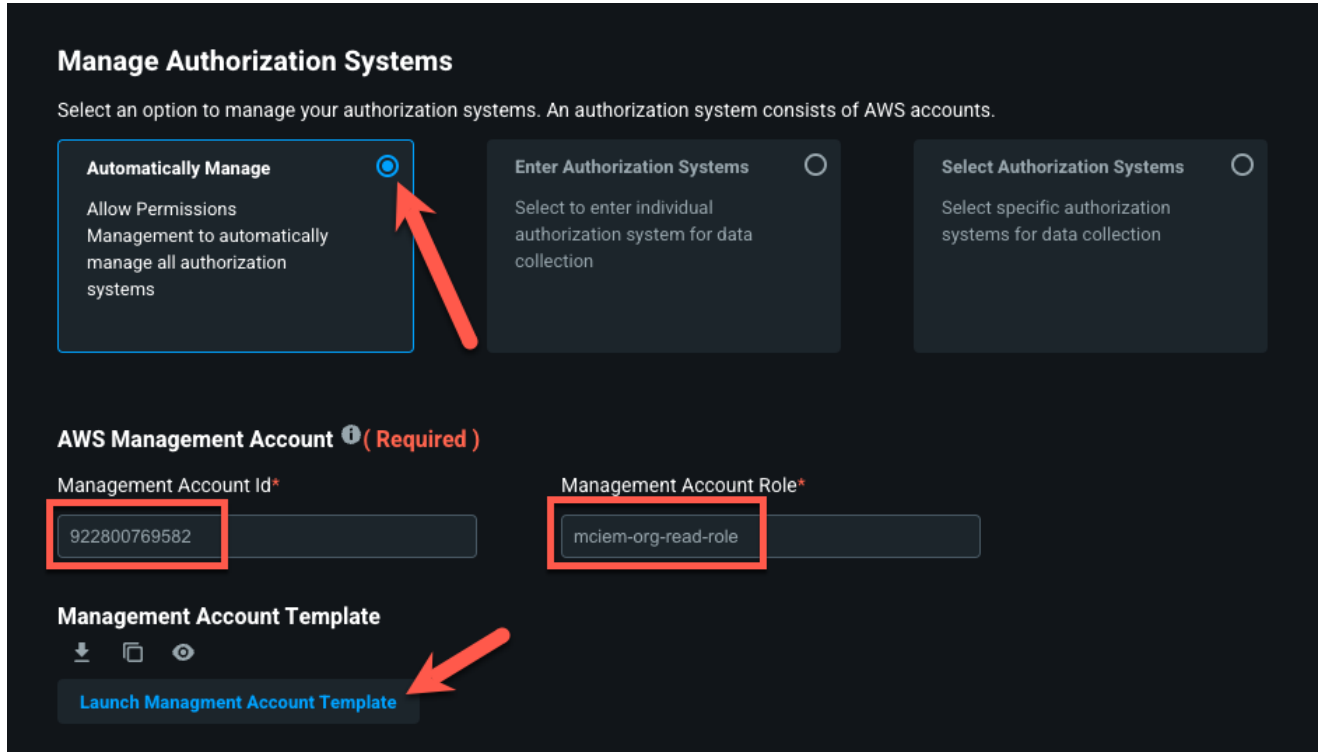
Events (11)

Search events

Timestamp	Logical ID	Status	Status reason
2023-06-15 15:10:35 UTC-0700	mciem-oidc-0348ff6f-154e-41c2-b1b7-60743cb165dc	CREATE_COMPLETE	-
2023-06-15 15:10:34 UTC-0700	CIEMOidcRole	CREATE_COMPLETE	-
2023-06-15 15:10:22 UTC-0700	CIEMOidcRole	CREATE_IN_PROGRESS	Resource creation Initiated
2023-06-15 15:10:21 UTC-0700	CIEMOidcRole	CREATE_IN_PROGRESS	-
2023-06-15 15:10:20 UTC-0700	AssumeRolePolicy	CREATE_COMPLETE	-
2023-06-15 15:10:10 UTC-0700	CIEMOidcIdP	CREATE_COMPLETE	-
2023-06-15 15:10:09 UTC-0700	CIEMOidcIdP	CREATE_IN_PROGRESS	Resource creation Initiated
2023-06-15 15:10:09 UTC-0700	AssumeRolePolicy	CREATE_IN_PROGRESS	Resource creation Initiated
2023-06-15 15:10:08 UTC-0700	AssumeRolePolicy	CREATE_IN_PROGRESS	-
2023-06-15 15:10:08 UTC-0700	CIEMOidcIdP	CREATE_IN_PROGRESS	-
2023-06-15 15:10:05 UTC-0700	mciem-oidc-0348ff6f-154e-41c2-b1b7-60743cb165dc	CREATE_IN_PROGRESS	User Initiated

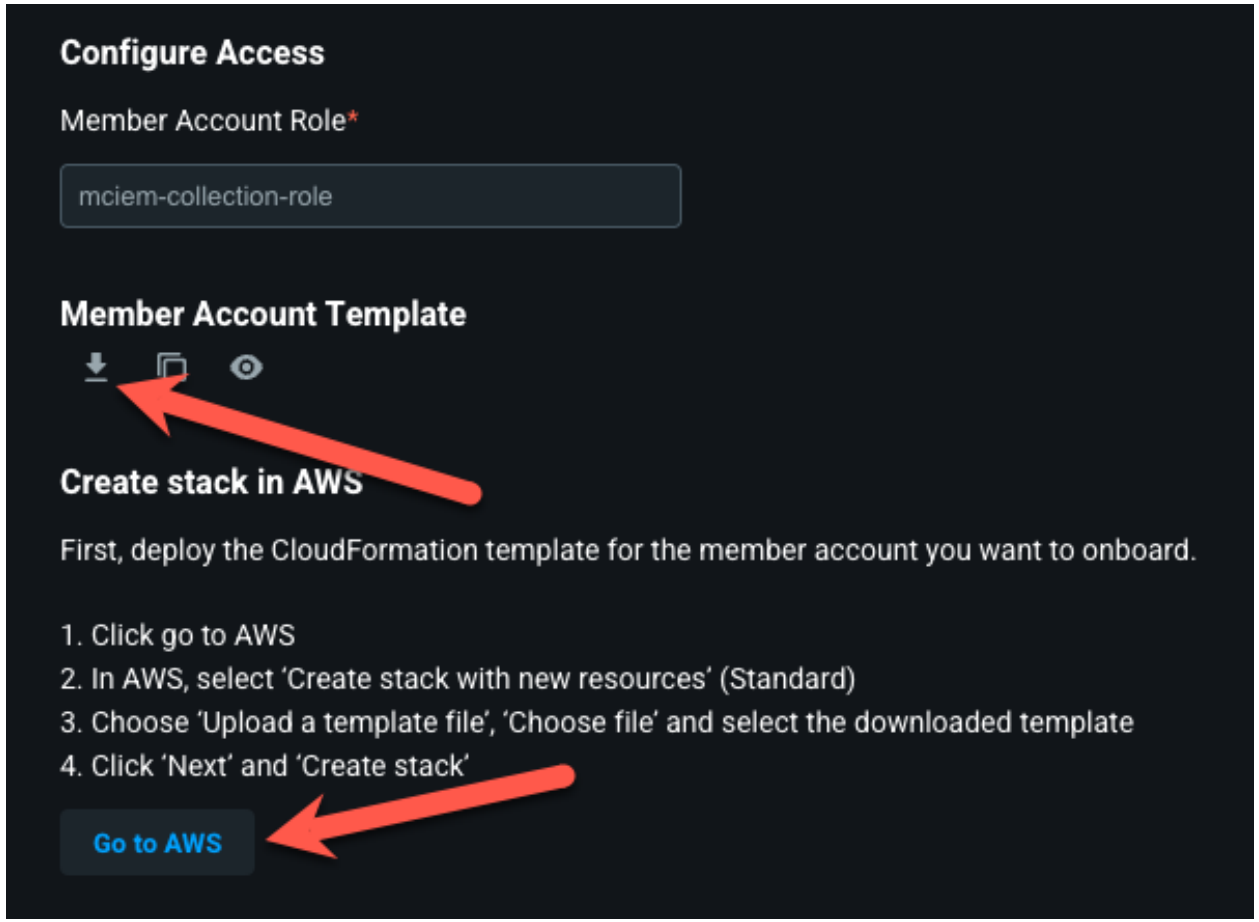
AWS Setup

4. Manage Authorization Systems
   - We recommend choose Automatically manage for the POC
   - Must provide the Management Account ID, which may be the same ID as the last step
   - Launch Management Account Template and then click Create Stack in AWS



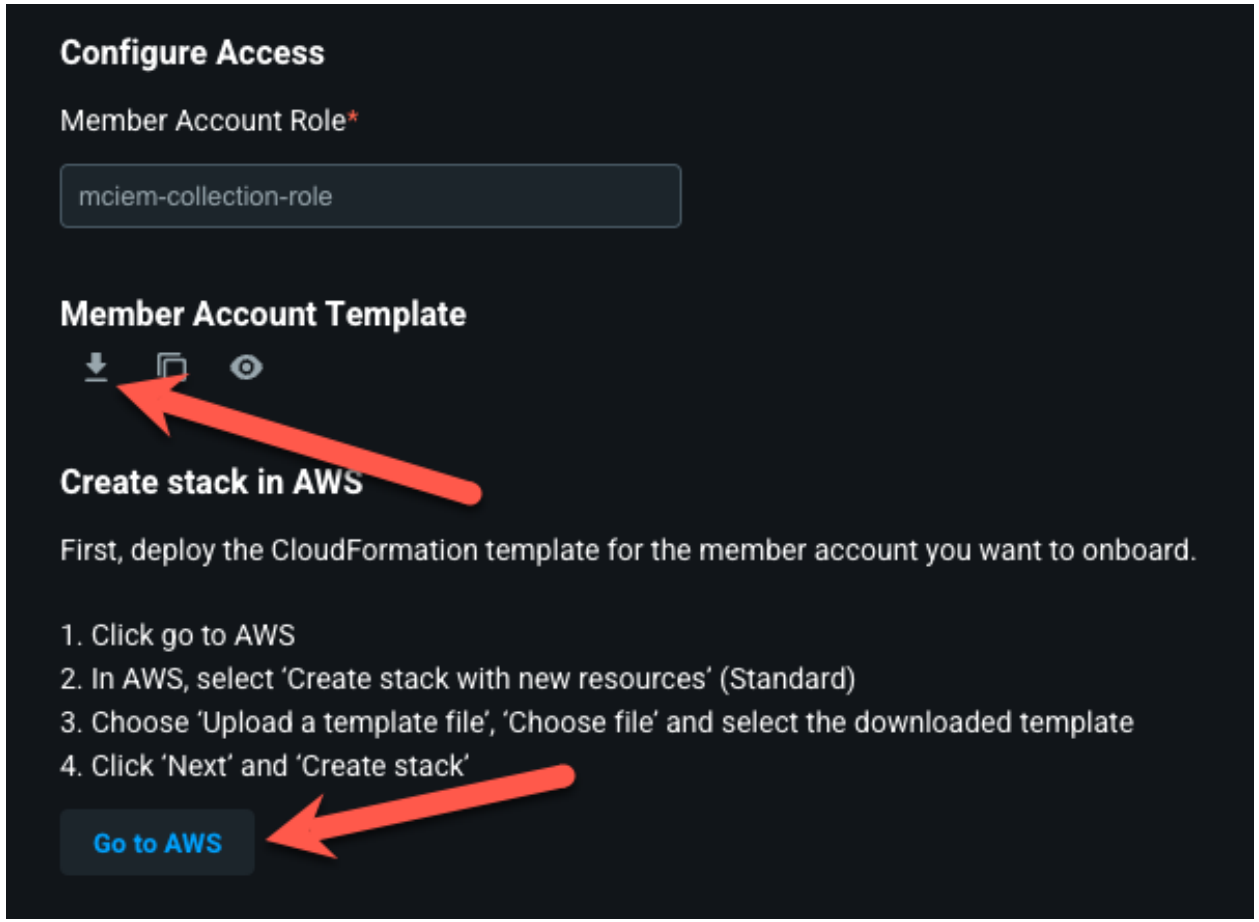
AWS Setup

4. Manage Authorization Systems – Member Account Role
   - Next, download the Member Account Template
   - Click Go to AWS



AWS Setup

4. Manage Authorization Systems – Member Account Role
   - A 3rd CloudFormation template needs to be run to configure the member account
   - Click Go to AWS



AWS Setup

4. Manage Authorization Systems – Member Account Role
   - Review the template – if you'd like to enable read/write features in Entra Permissions Management then change the Enable Controller setting to true:

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

CloudKnox Permissions Management Configuration Parameters

CloudTrail Bucket Name

S3 Bucket name where cloudtrail logs are stored

Enter String

Enable Controller

Enabling your controller gives CloudKnox Permissions Management the privileges to provide the Privilege-On-Demand feature

false

Member Account Role Name

Name of the IAM Role

mciem-collection-role

OIDC Provider Role Name

Name of the IAM Role OIDC Provider can assume role into

mciem-oidc-connect-role

OIDC Provider Account ID

Account Id where OIDC Provider is created

922800769582

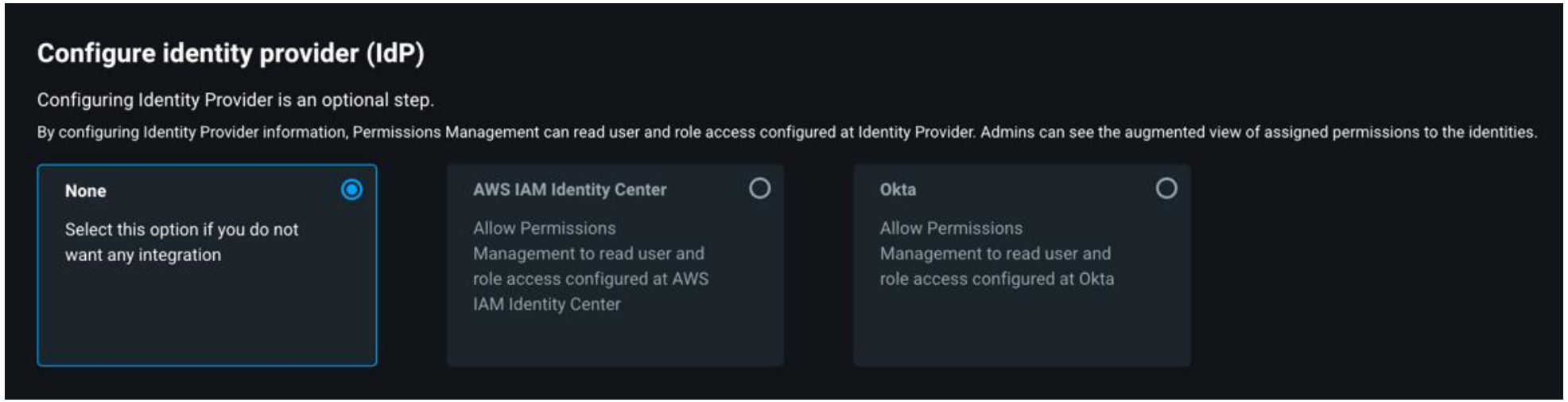
Tenant ID

Id of the tenant where the application is created

0348ff6f-154e-41c2-b1b7-60743cb165dc

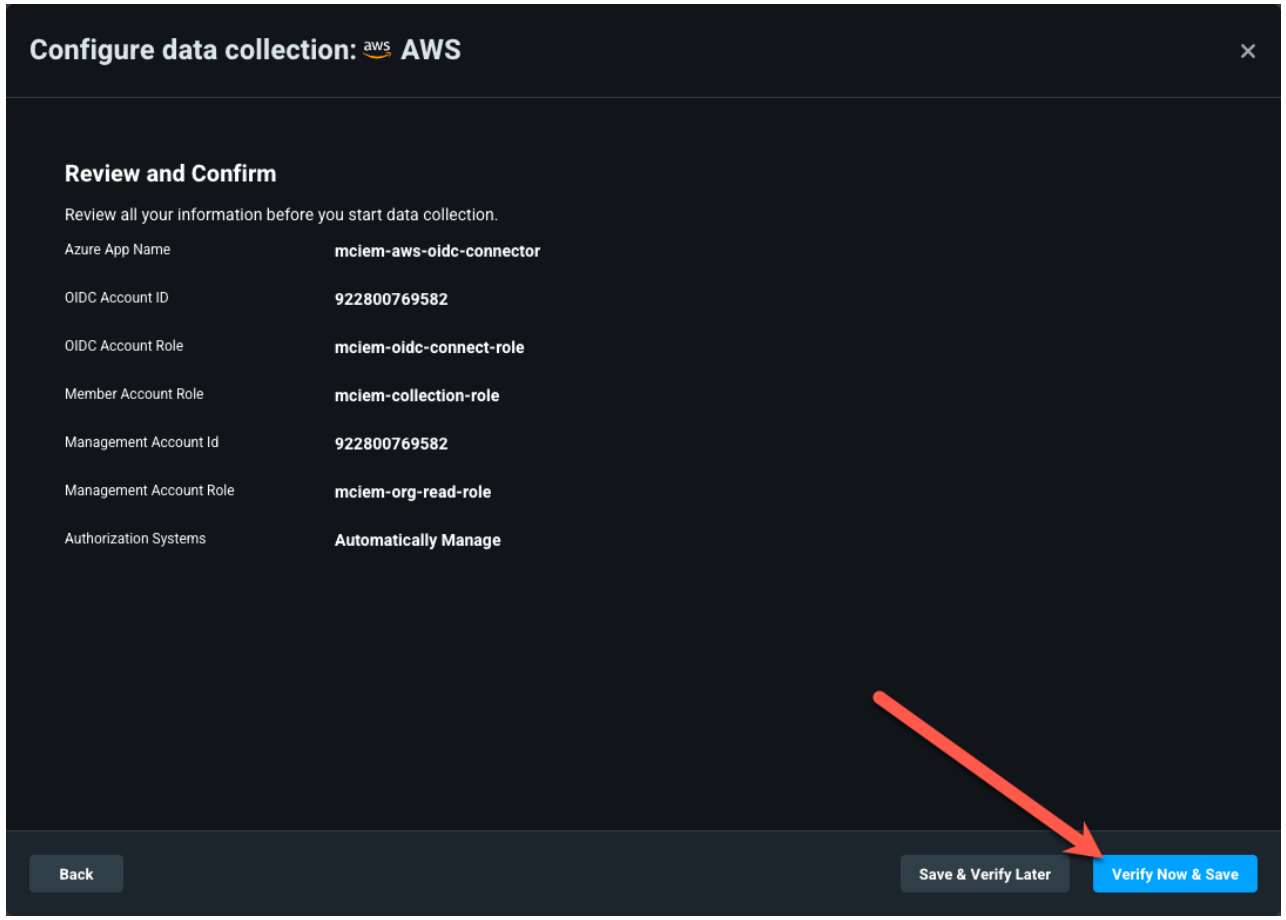
AWS Setup

5. If you use AWS Identity Provider, then follow additional steps to integrate



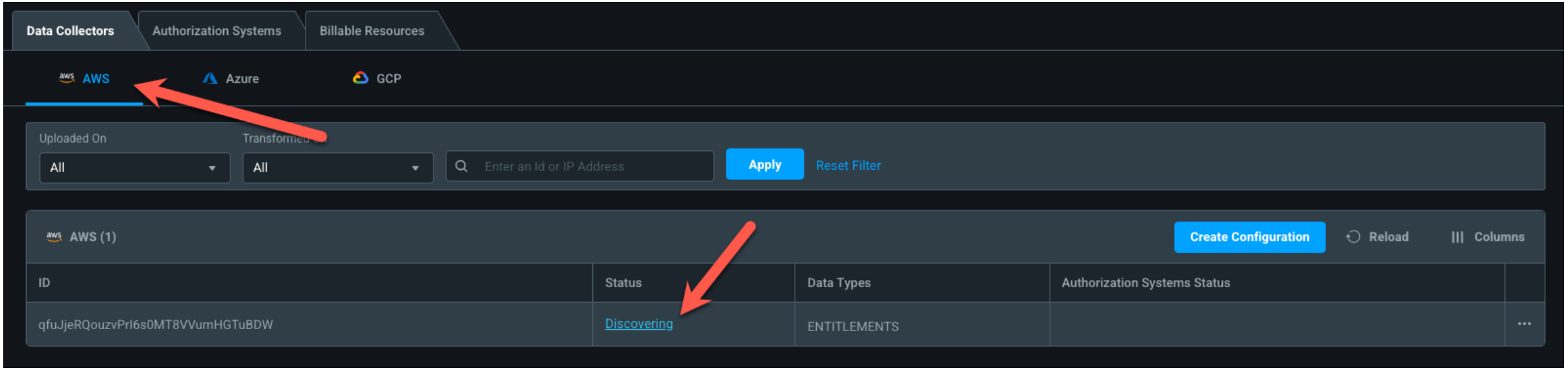
AWS Setup

6. Finally, review your configuration and click Verify Now & Save:

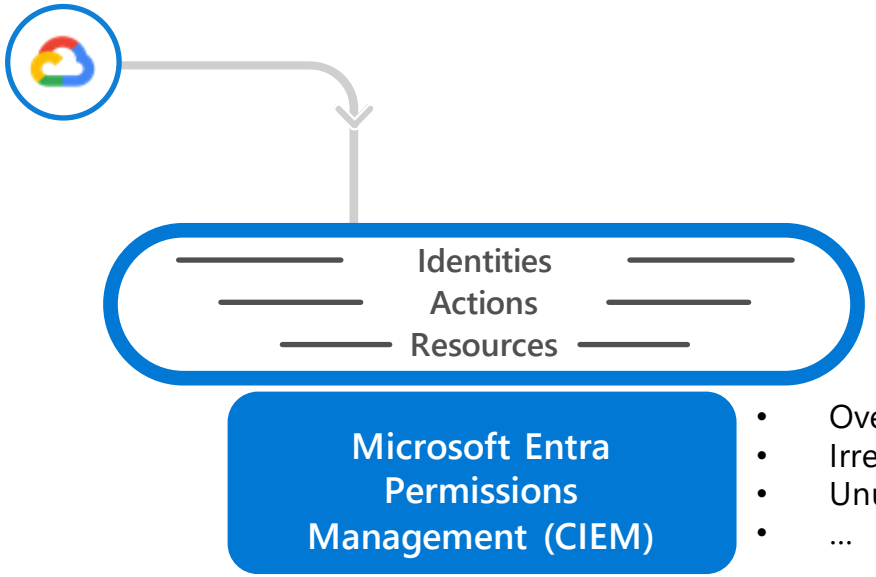


AWS Setup

7. You should now see an AWS Data Collector with a Discovering Status. Discovery may take some time.



GCP Onboarding



- Over privileged identities
- Irregular permission pattens
- Unused permissions
- …

GCP Setup

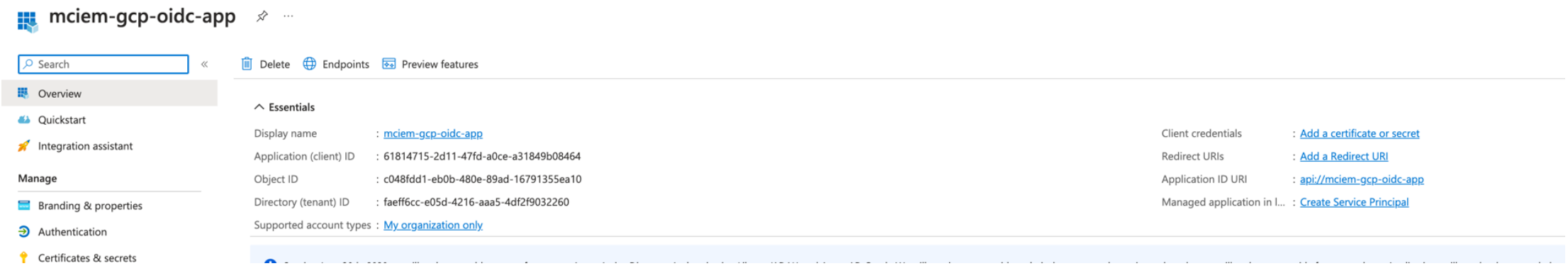
1. Azure AD OpenID Connect Application (App Registration)
   - Can be run by any role that can create app registrations
   - Recommend using Azure Cloud Shell for simplicity
   - App name and API can be customized if desired

```
#use this script for Azure version >3.7 az ad app create --display-name "mciem-gcp-oidc-app" --identifier-uris "api://mciem-gcp-oidc-app" --sign-in-audience AzureADMyOrg

#PowerShell Script New-AzureADApplication -DisplayName "mciem-gcp-oidc-app" -IdentifierUris "api://mciem-gcp-oidc-app"
```

```
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

mark [ ~ ]$ az ad app create --display-name "mciem-gcp-oidc-app" --identifier-uris "api://mciem-gcp-oidc-app" --sign-in-audience AzureADMyOrg
```

GCP Setup

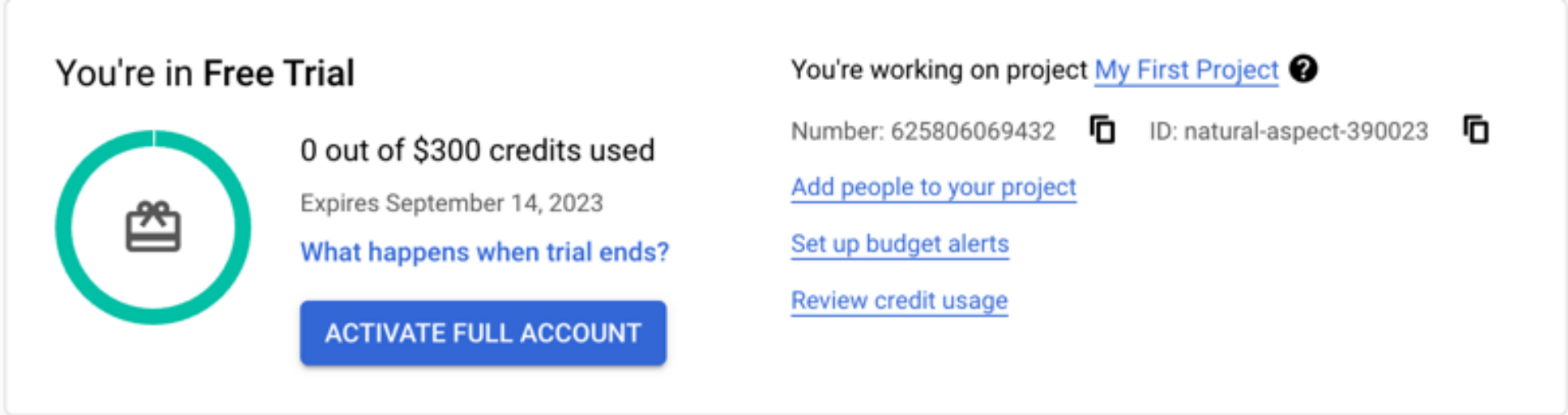
1. Azure AD OpenID Connect Application (App Registration)
   - Can be run by any role that can create app registrations
   - Recommend using Azure Cloud Shell for simplicity
   - App name and API can be customized if desired



GCP Setup

2. Setup a GCP OIDC Project

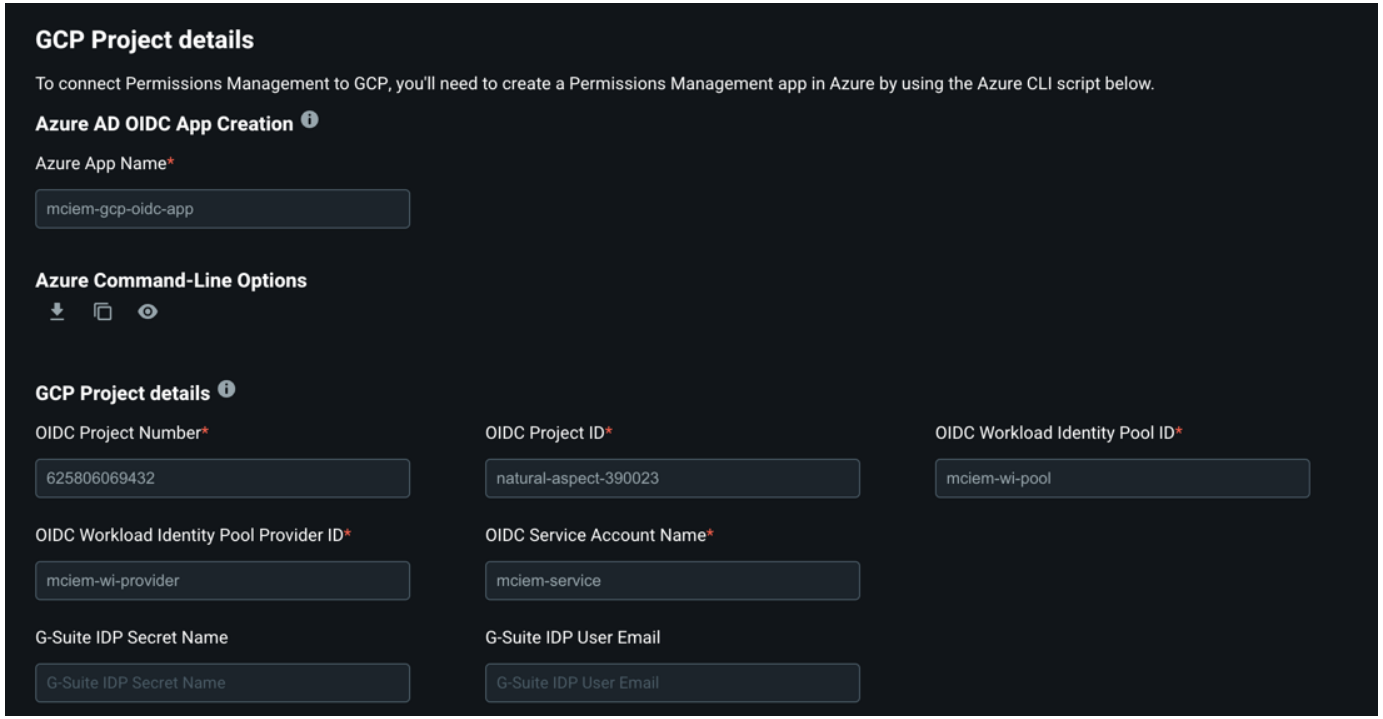
- You'll need to go to the GCP console and get the project ID and project number. This is on the home page of the project



GCP Setup

2. Setup a GCP OIDC Project

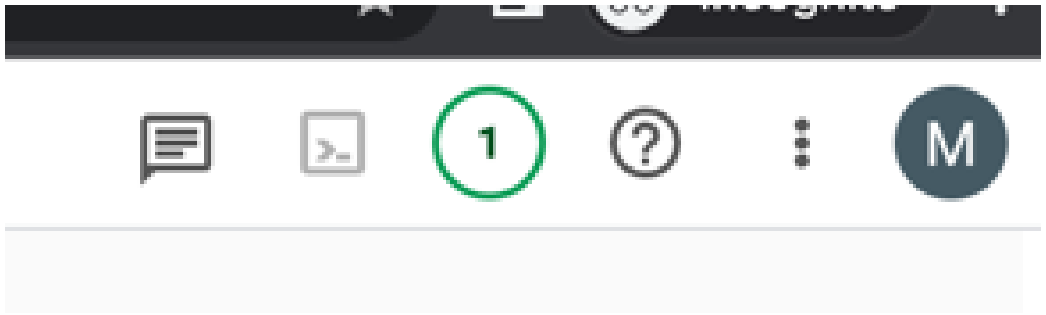
- You can update the Workload Identity PoolID, ProviderID or ServiceAccount name if you wish or accept the defaults. You will now need to go to the GCP console



GCP Setup

3. Run Setup script in Google Cloud Shell. It’s in the upper right corner that looks like a shell prompt.

- A console will open in the lower pane similar to the Azure Cloud Shell
- Copy and paste the setup script. Authorize permissions to your logged in creds if needed



GCP Setup

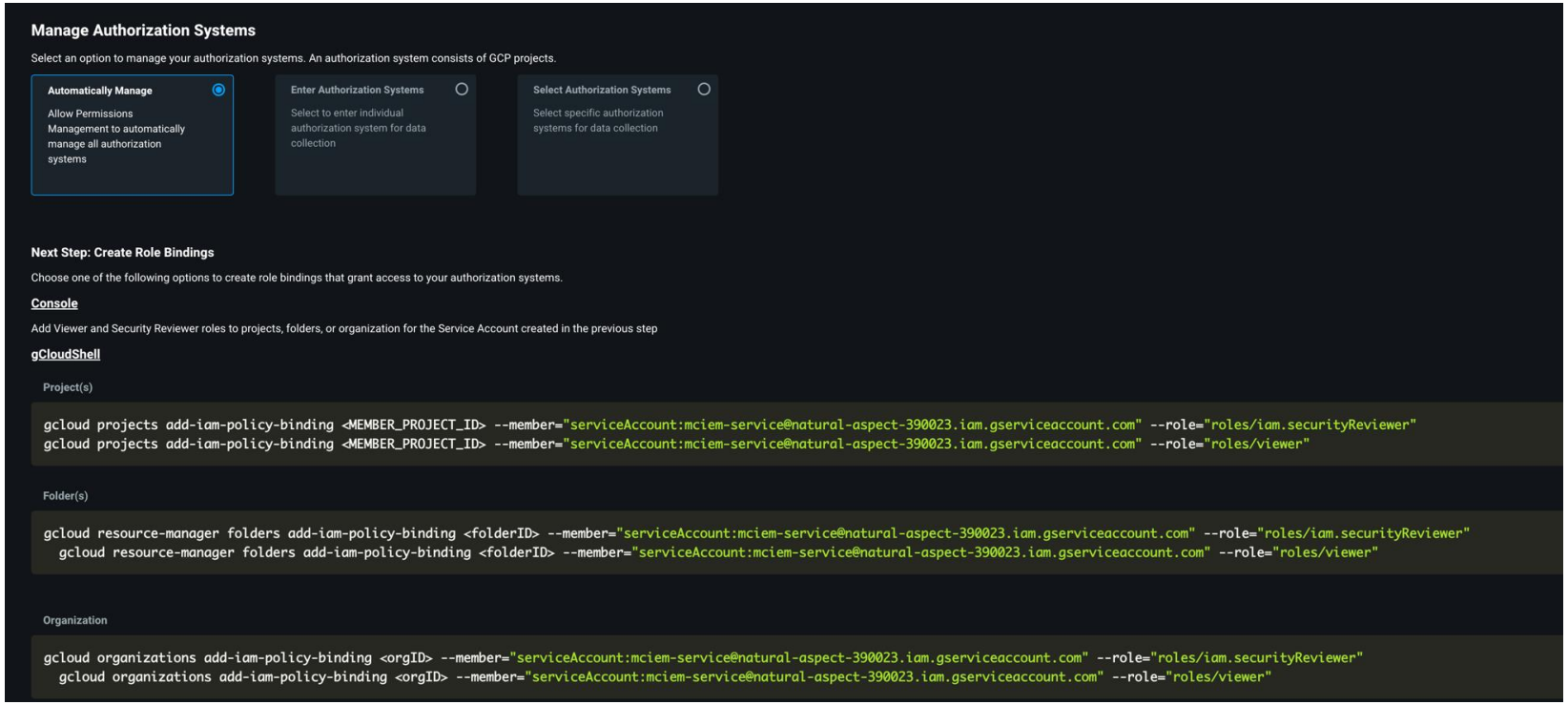
4. Confirm setup is complete in the output. Click next in EPM portal

```
If you have already logged in with a different account, run:

  $ gcloud config set account ACCOUNT

to select an already authenticated account to use.
Updated property [core/project].
In project name: number:625806069432 id:natural-aspect-390023
Enabling IAM API in project natural-aspect-390023
Operation "operations/acat.p2-625806069432-a5cad535-deb5-412d-9244-4f71af3c956a" finished successfully.
Enabling IAM Credential API in project natural-aspect-390023
Enabling IAM Credential API in project natural-aspect-390023
Operation "operations/acat.p2-625806069432-11f53af4-730d-4d0b-b87e-27e77955e6e6" finished successfully.
Create workload identity pool mciem-wi-pool
Created workload identity pool [mciem-wi-pool].
Create workload identity pool provider mciem-wi-provider
Created workload identity pool provider [mciem-wi-provider].
Create IAM service account mciem-service
Created service account [mciem-service].
Add IAM policy binding for iam.workloadIdentityUser to mciem-service@natural-aspect-390023.iam.gserviceaccount.com
Updated IAM policy for serviceAccount [mciem-service@natural-aspect-390023.iam.gserviceaccount.com].
bindings:
- members:
  - principalSet://iam.googleapis.com/projects/625806069432/locations/global/workloadIdentityPools/mciem-wi-pool/*
  role: roles/iam.workloadIdentityUser
etag: BwX-QZt6Jwg=
version: 1
markmorowepm@cloudshell:~ (natural-aspect-390023)$
```

GCP Setup

5. Manage Authorization Systems

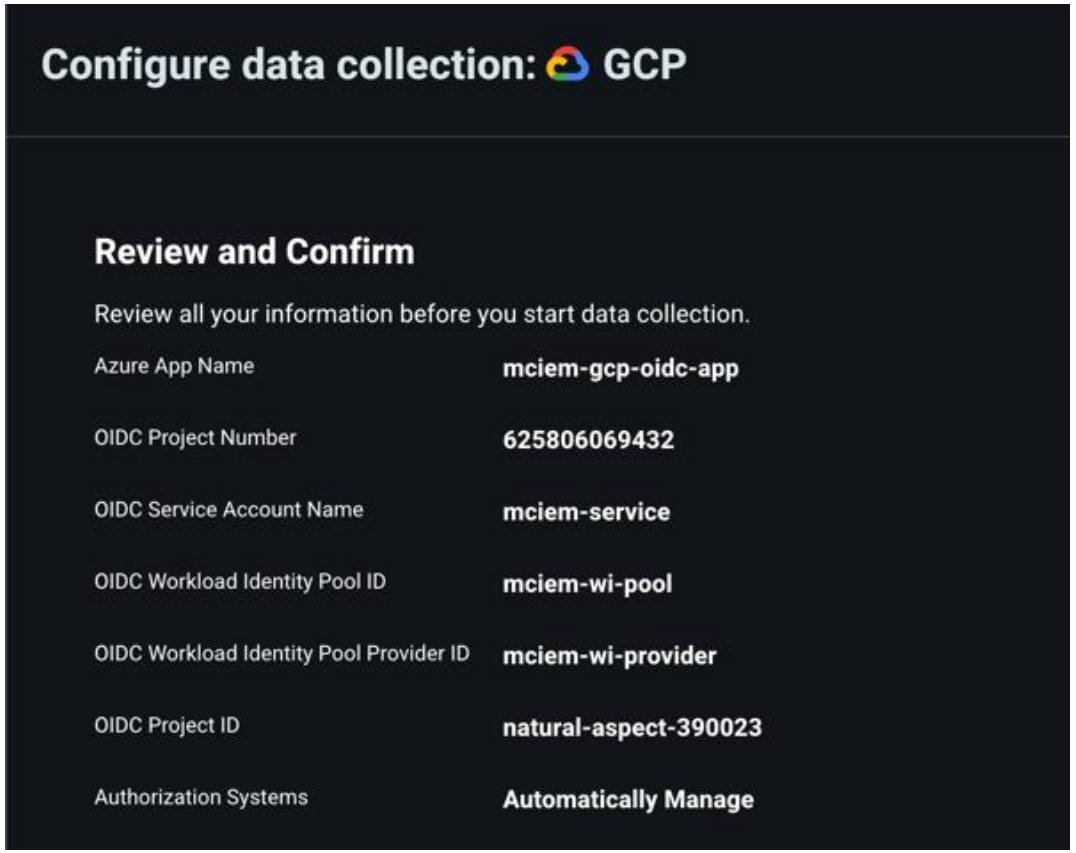
- We recommend choose Automatically manage for the POC, click Next.



GCP Setup

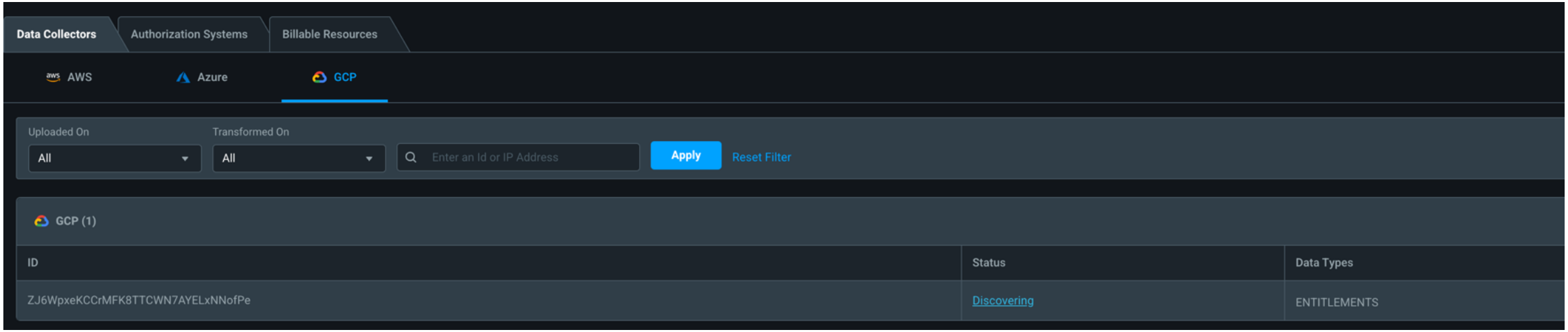
6. Review and Confirm

- You'll see the setting screen. Click Verify Now & Save



GCP Setup

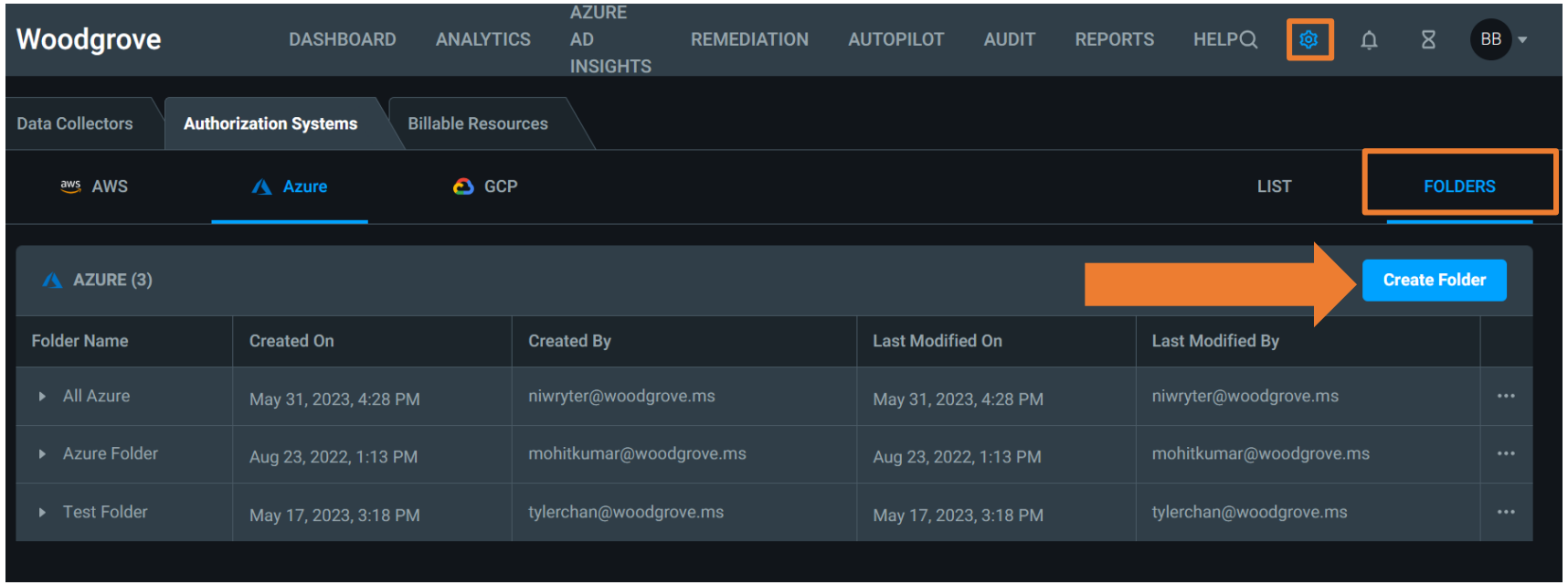
7. You should now see an GCP Data Collector with a Discovering Status. Discovery may take some time.



Next Steps

Recommendation: Create Folders

- Folders ease administrative burden in the Entra Permissions Management console by organizing accounts and subscriptions
- To create a folder, go to Settings (gear) > Folders > Create Folder



Where do we go from here?

- Brilliant at the Basics
- About the Performance Creep Index and Remediation
- Automation and Alerting
- Go-Do's

Known Issues

- Add Known Issues (if any) here

Resources

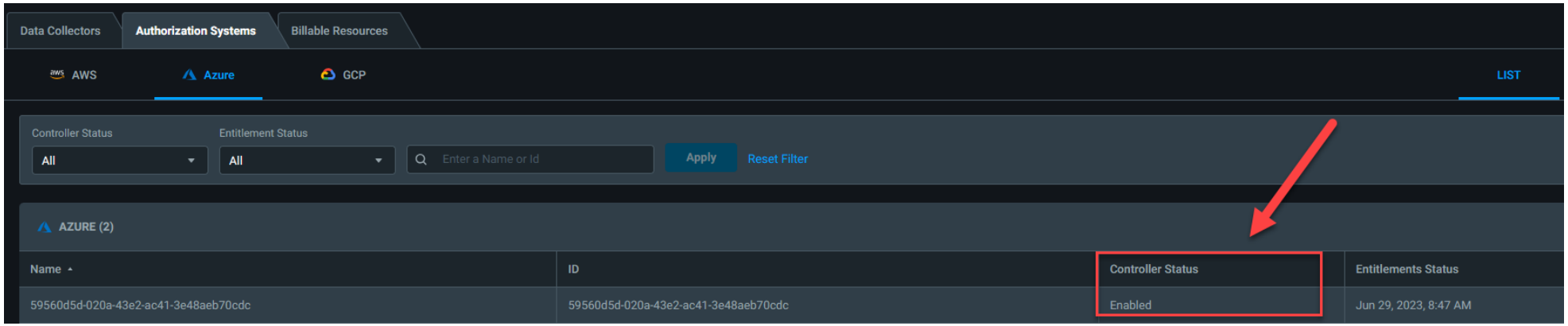
- Onboard an Amazon Web Services (AWS) account
- Onboard a Microsoft Azure subscription
- Onboard a Google Cloud Platform (GCP) project
- Configure AWS IAM Identity Center as an identity provider
- Enable or disable the controller in Permissions Management after onboarding is complete
- Add an account /subscription/ project to Permissions Management after onboarding is complete

Thank you!

Azure Setup: Enable Controller

For controller functionality, the app **Cloud Infrastructure Entitlement Management** requires **'User Access Administrator**' role to create and implement right-size roles.

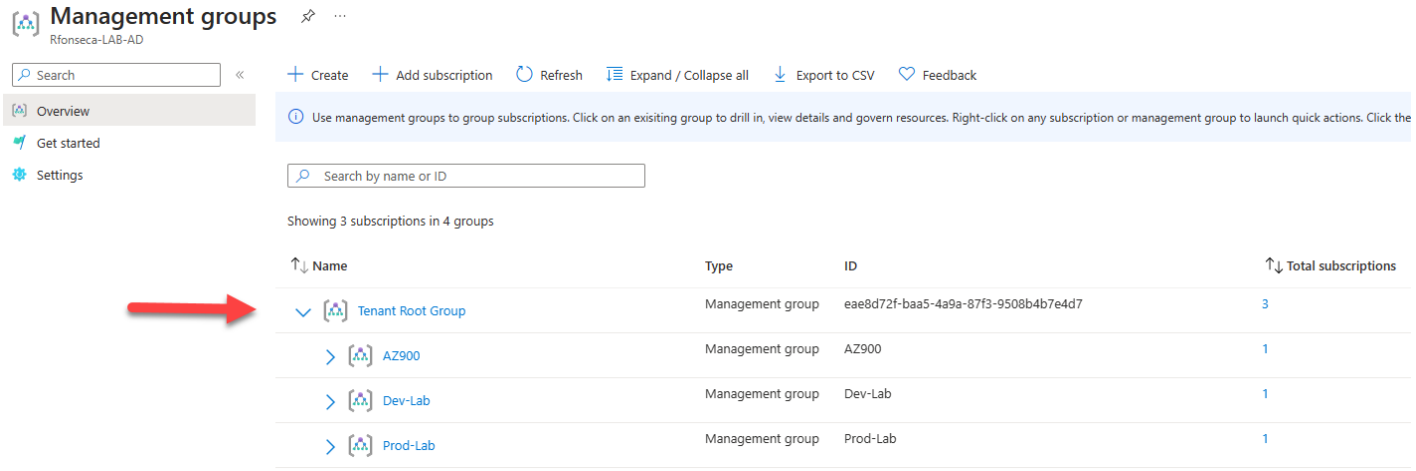
Before onboarding, you can make sure the app has **User Access Administrator** role in all desired Subscriptions or Management Groups.



Azure Setup: Enable Controller

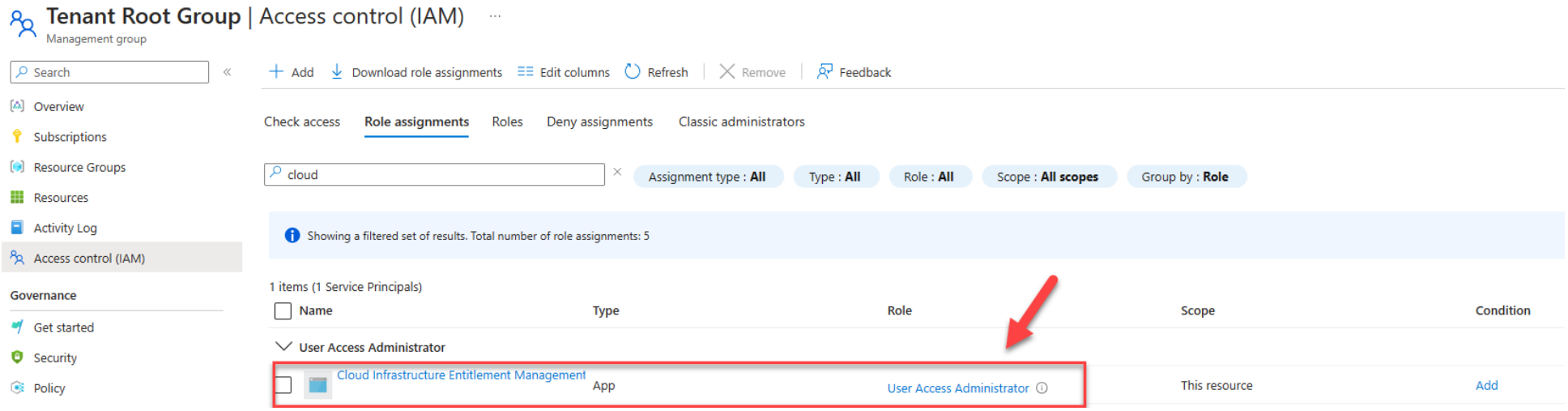
You can enable or disable the controller in Azure at the Subscription or Management Group(s) level.

1. From the Azure **Home** page, select **Management groups**.
2. Locate the group for which you want to enable or disable the controller



Azure Setup: Enable Controller

3. To add the administrative role assignment, go to the **Access control (IAM)** page, and then select **Add role assignment**.
4. Add "**User Access Administrator**" role assignment for **Cloud Infrastructure Entitlement Management** to enable controller



Azure Setup: Enable Controller

5. Go to the Permissions Management home page, select Settings (the gear icon), and then select the Data Collectors subtab.
6. On the Data Collectors dashboard, select Azure, and then select Create Configuration.
7. On the Permissions Management Onboarding - Azure Subscription Details page, enter the Subscription ID, and then select Next.
8. On Permissions Management Onboarding – Summary page, review the controller permissions, and then select Verify Now & Save.
9. The following message appears: Successfully Created Configuration.

GCP Setup: Enable Controller

During Step 5 - Manage Authorization Systems – Users can choose to enable controller mode **'On'** for any projects, add following roles to service account for the specific projects:

- Role Administrators
- Security Admin

```
gcloud projects add-iam-policy-binding <MEMBER_PROJECT_ID> --
member="serviceAccount:mciem-service@123.iam.gserviceaccount.com" --
role="roles/iam.securityAdmin"
```

```
gcloud projects add-iam-policy-binding <MEMBER_PROJECT_ID> --
member="serviceAccount:mciem-service@123.iam.gserviceaccount.com" --
role="roles/iam.roleAdmin"
```

GCP Setup: Enable Controller

To enable or disable the controller in Google Cloud Platform (GCP) after onboarding is complete:

1. Execute the *gcloud auth login*.

2. Follow the instructions displayed on the screen to authorize access to your Google account.

3. Execute the *sh mciem-workload-identity-pool.sh* to create the workload identity pool, provider, and service account.

4. Execute the *sh mciem-member-projects.sh* to give Permissions Management permissions to access each of the member projects.

   - If you want to manage permissions through Permissions Management, select **Y** to **Enable controller**.
   - If you want to onboard your projects in **read-only mode**, select **N** to **Disable controller**.

5. Optionally, execute *mciem-enable-gcp-api.sh* to enable all recommended GCP APIs.

6. Go to the Permissions Management home page, select Settings (the gear icon), and then select the Data Collectors subtab.

GCP Setup: Enable Controller

7. On the Data Collectors dashboard, select GCP, and then select **Create Configuration**.

8. On the Permissions Management Onboarding - Azure AD OIDC App Creation page, select **Next**.

9. On the Permissions Management Onboarding - GCP OIDC Account Details & IDP Access page, enter the OIDC Project Number and OIDC Project ID, and then select **Next**.

10. On the Permissions Management Onboarding - GCP Project IDs page, enter the Project IDs, and then select **Next**.

11. On the Permissions Management Onboarding – Summary page, review the information you've added, and then select **Verify Now & Save**.

12. The following message appears: **Successfully Created Configuration.**

Microsoft Security