



Microsoft Entra Permissions Management

Onboarding

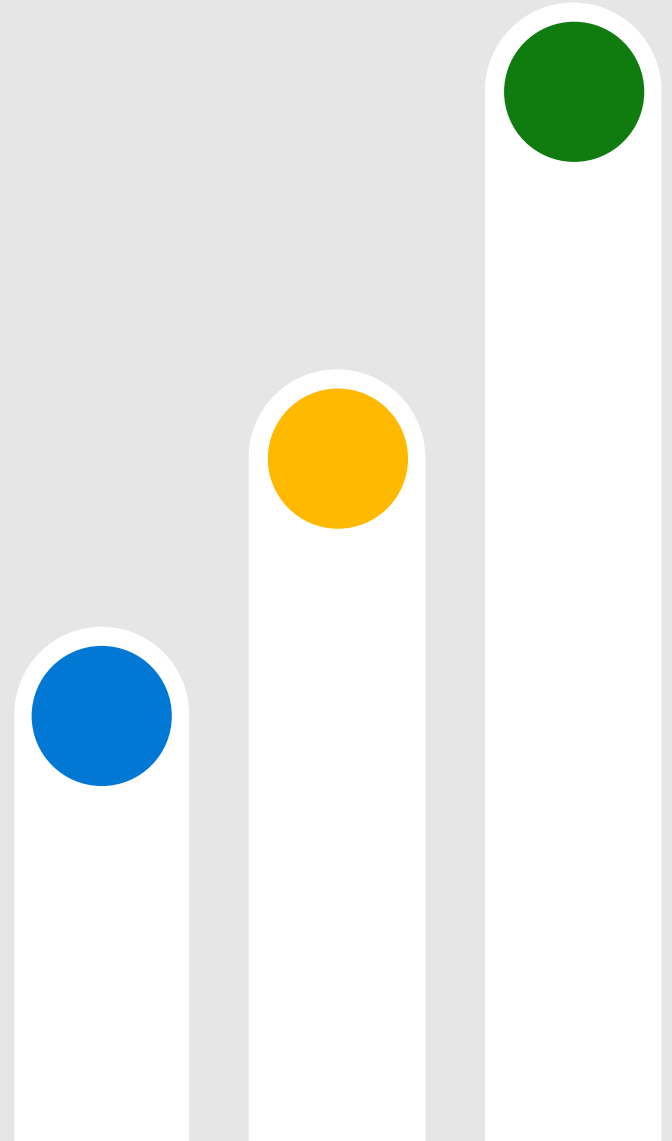
<Name>

<Job role>

Agenda

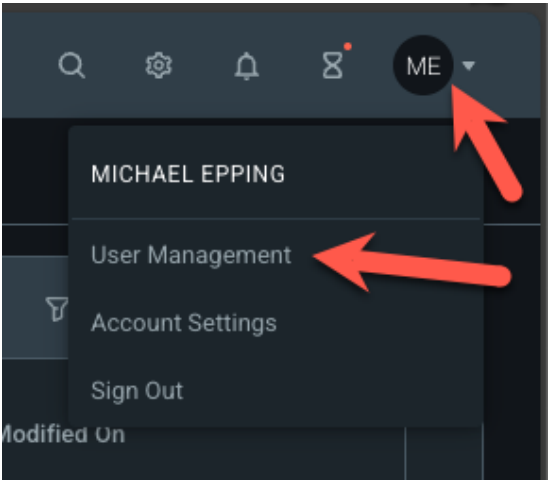
- Microsoft Entra Permissions Management RBAC Configuration
- Azure
- AWS
- GCP

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

1. Add Azure Subscription
2. Authorization setting

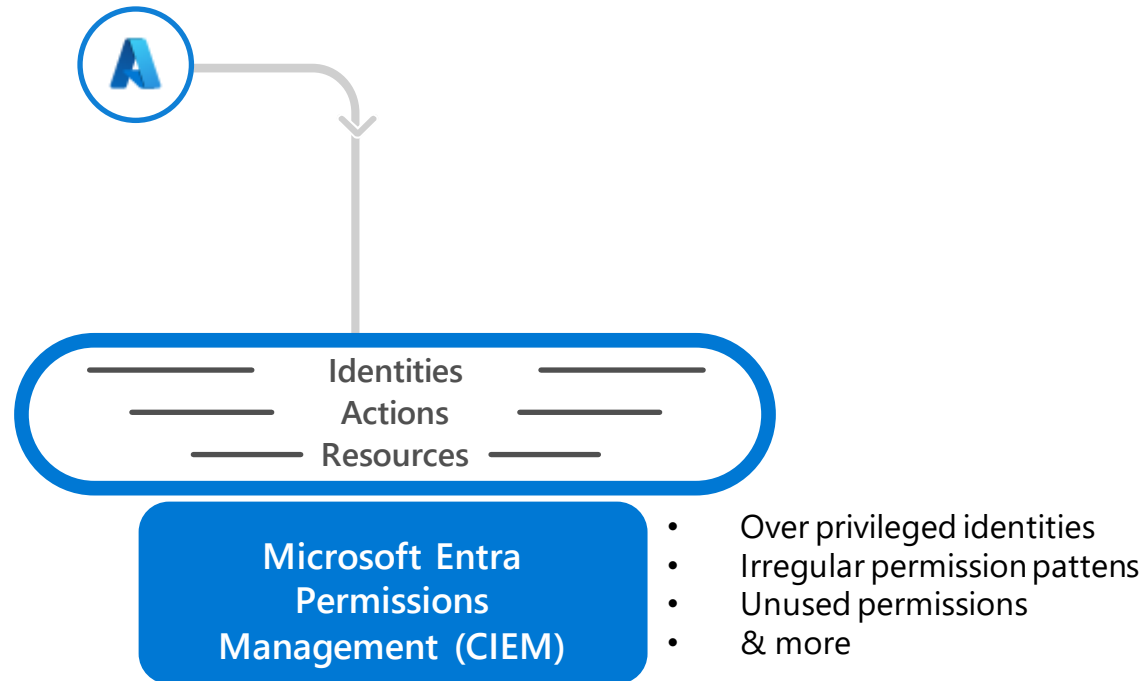
AWS

1. Register Application to Entra ID
2. Run AWS template
3. Authorization setting
4. AWS Identity provider setting (Optional)

GCP

1. Register Application to Entra ID
2. Setup GCP OIDC project
3. Run script in Google cloud shell
4. Authorization setting

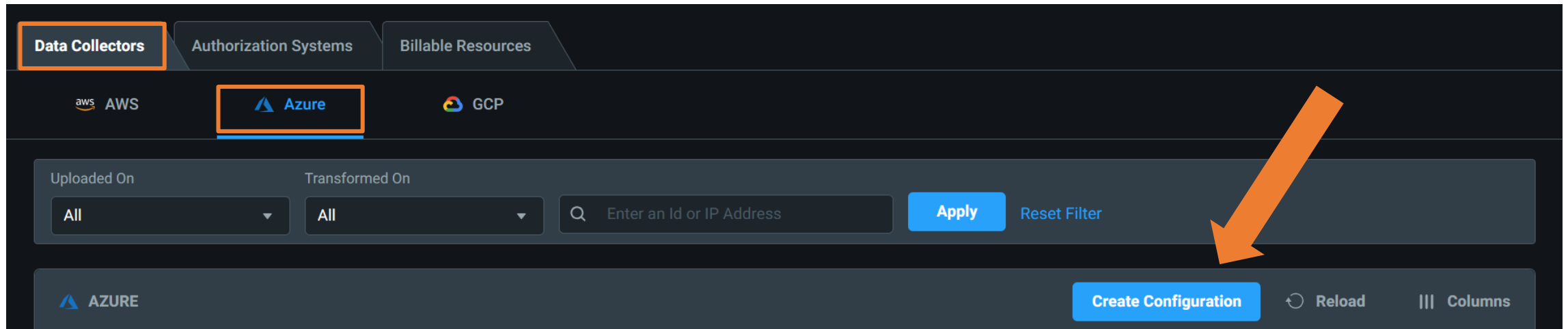
Azure Onboarding



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

Configure data collection: Azure

Manage Authorization Systems

Select an option to manage your authorization systems. An authorization system consists of Azure subscriptions.


Automatically Manage ☒
Allow Permissions Management to automatically manage all authorization systems

Enter Authorization Systems ☐
Select to enter individual authorization system for data collection

Select Authorization Systems ☐
Select specific authorization systems for data collection

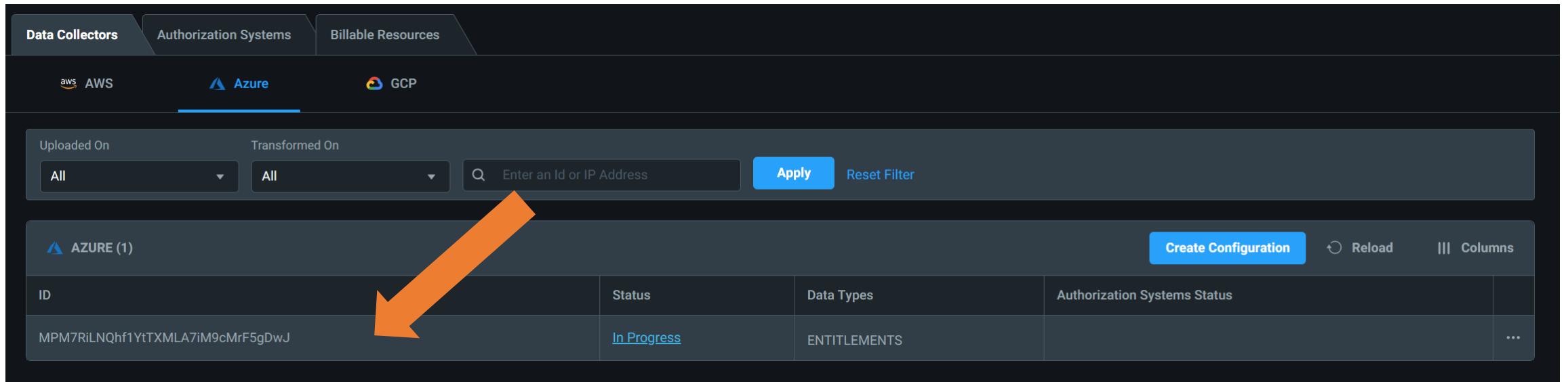
Save & Verify Later

Verify Now & Save



Azure Setup

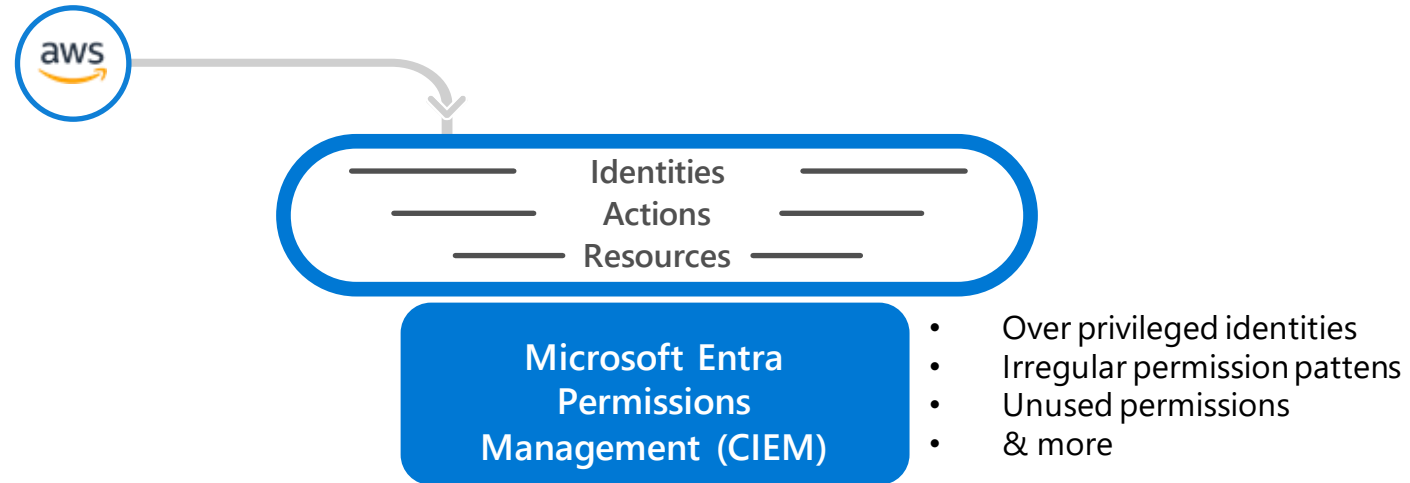
3. You will now see the Azure Data Collector



The screenshot displays the Azure Data Collector interface. At the top, there are tabs for 'Data Collectors', 'Authorization Systems', and 'Billable Resources'. Below these, there are logos for AWS, Azure (selected), and GCP. A filter bar includes 'Uploaded On' and 'Transformed On' dropdowns (both set to 'All'), a search input 'Enter an Id or IP Address', and buttons for 'Apply' and 'Reset Filter'. Below the filter bar, a section titled 'AZURE (1)' contains a table with one data row. An orange arrow points to the ID of this row. The table has columns for ID, Status, Data Types, and Authorization Systems Status. The 'Status' column for the row shows 'In Progress' with a link. The 'Data Types' column shows 'ENTITLEMENTS'. The 'Authorization Systems Status' column is empty. A 'Create Configuration' button, a 'Reload' button, and a 'Columns' menu are located to the right of the table header.

ID	Status	Data Types	Authorization Systems Status
MPM7RiLNQhf1YtTXMLA7iM9cMrF5gDwJ	In Progress	ENTITLEMENTS	

AWS Onboarding



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-uris "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

The screenshot shows the Azure AD App Registration page for an application named 'mciem-aws-oidc-connector'. The left sidebar contains navigation links: Overview (selected), Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area displays the 'Essentials' section with the following details:

Display name	: mciem-aws-oidc-connector	Client credentials	: Add a certificate or secret
Application (client) ID	: e67079bb-fa1d-4e09-9471-e64edb2a6e01	Redirect URIs	: Add a Redirect URI
Object ID	: a74a5451-99b1-4359-b5e4-cb4f8b5ecad1	Application ID URI	: api//mciem-aws-oidc-app
Directory (tenant) ID	: 0348ff6f-154e-41c2-b1b7-60743cb165dc	Managed application in I...	: Create Service Principal
Supported account types	: My organization only		

Below the essentials section, there is a 'Get Started' link and a 'Documentation' link. A blue banner at the bottom of the page reads: 'Build your application with the Microsoft identity platform'. Below this banner, a paragraph states: 'The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)'.

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:



Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

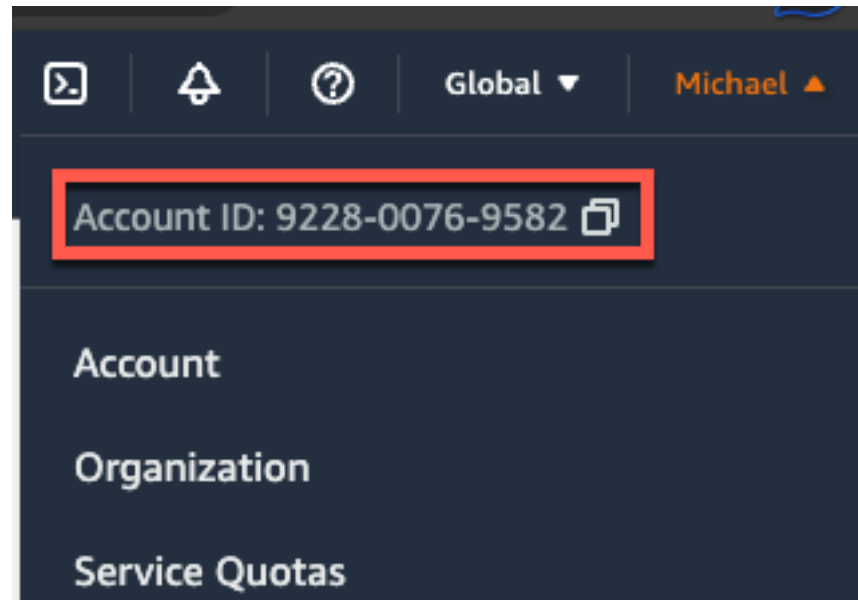
michael@rvrwest.com

Next

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

Configure data collection:  **AWS**

Account details

To connect Permissions Management to AWS, you'll need to create a Permissions Management app in Azure by using the Azure AD OIDC App Creation tool.

Azure AD OIDC App Creation ⓘ

Azure App Name*

Azure Command-Line Options

⬇️ 📄 👁️

AWS OIDC account ⓘ


OIDC Account ID*

OIDC Account Role*

AWS OIDC template

⬇️ 📄 👁️

[Launch OIDC template](#)



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)			
<input type="text" value="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

Manage Authorization Systems

Select an option to manage your authorization systems. An authorization system consists of AWS accounts.

Automatically Manage ☒

Allow Permissions Management to automatically manage all authorization systems

Enter Authorization Systems ☐

Select to enter individual authorization system for data collection

Select Authorization Systems ☐

Select specific authorization systems for data collection

AWS Management Account ⓘ (Required)

Management Account Id*

Management Account Role*

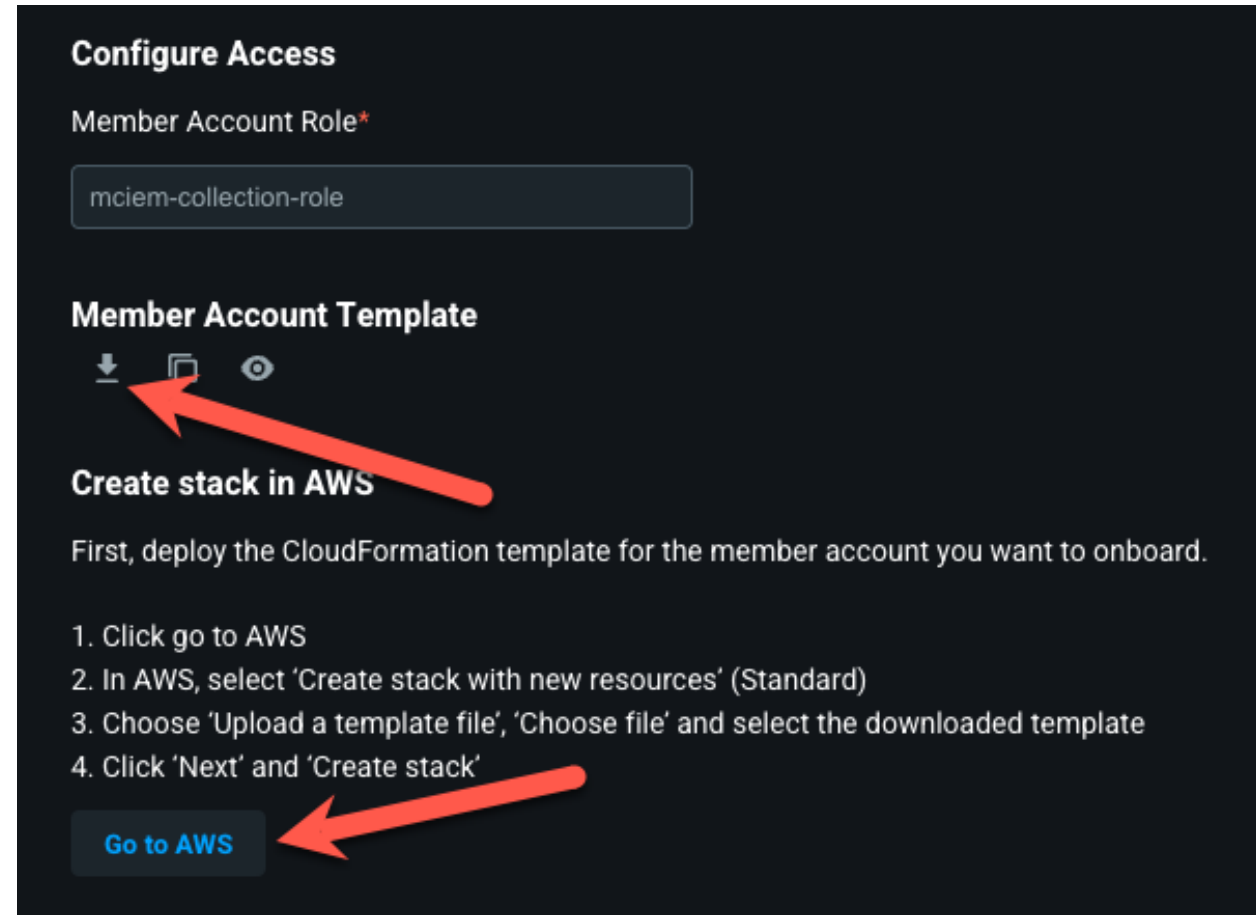
Management Account Template

⬇ ⬅ 🔍

[Launch Management Account Template](#)

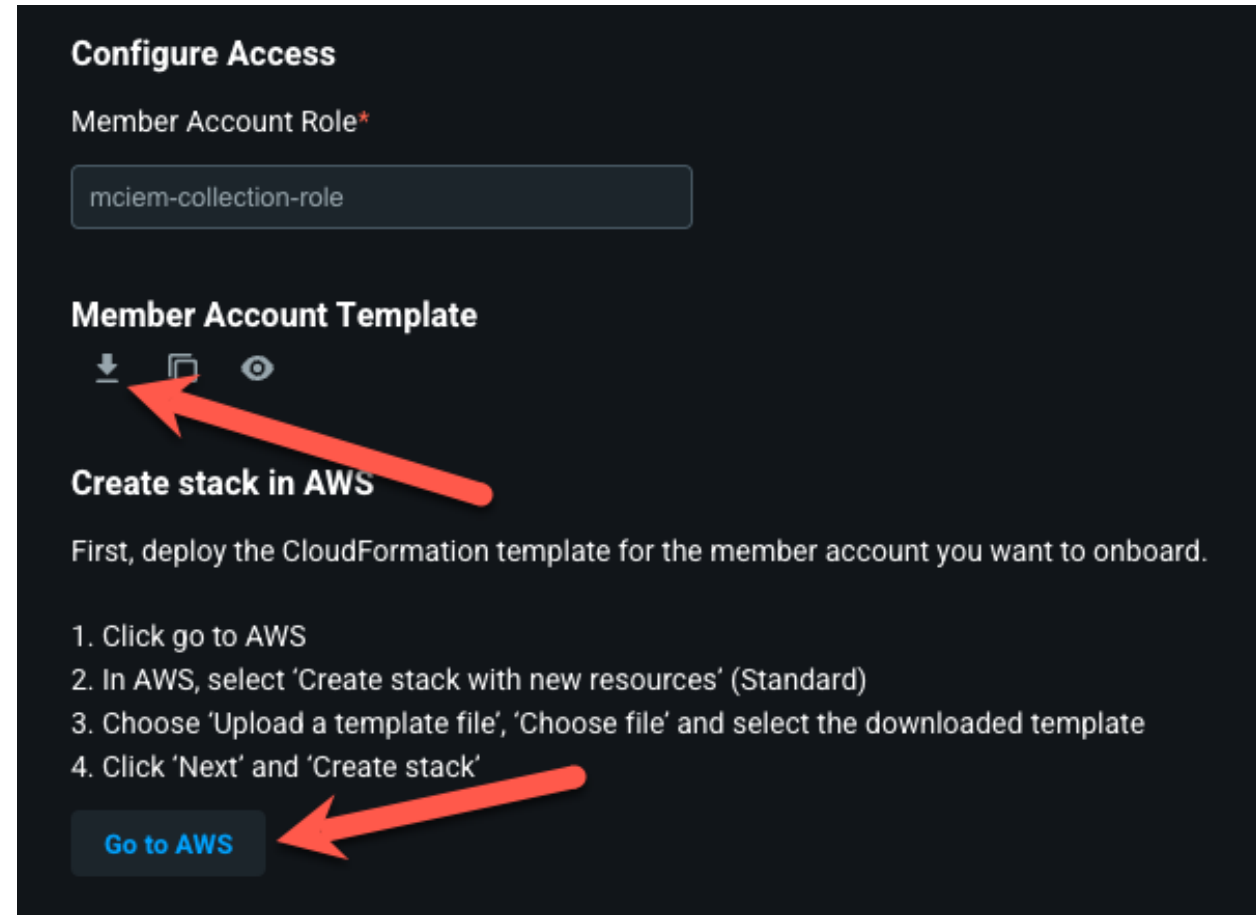
AWS Setup

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



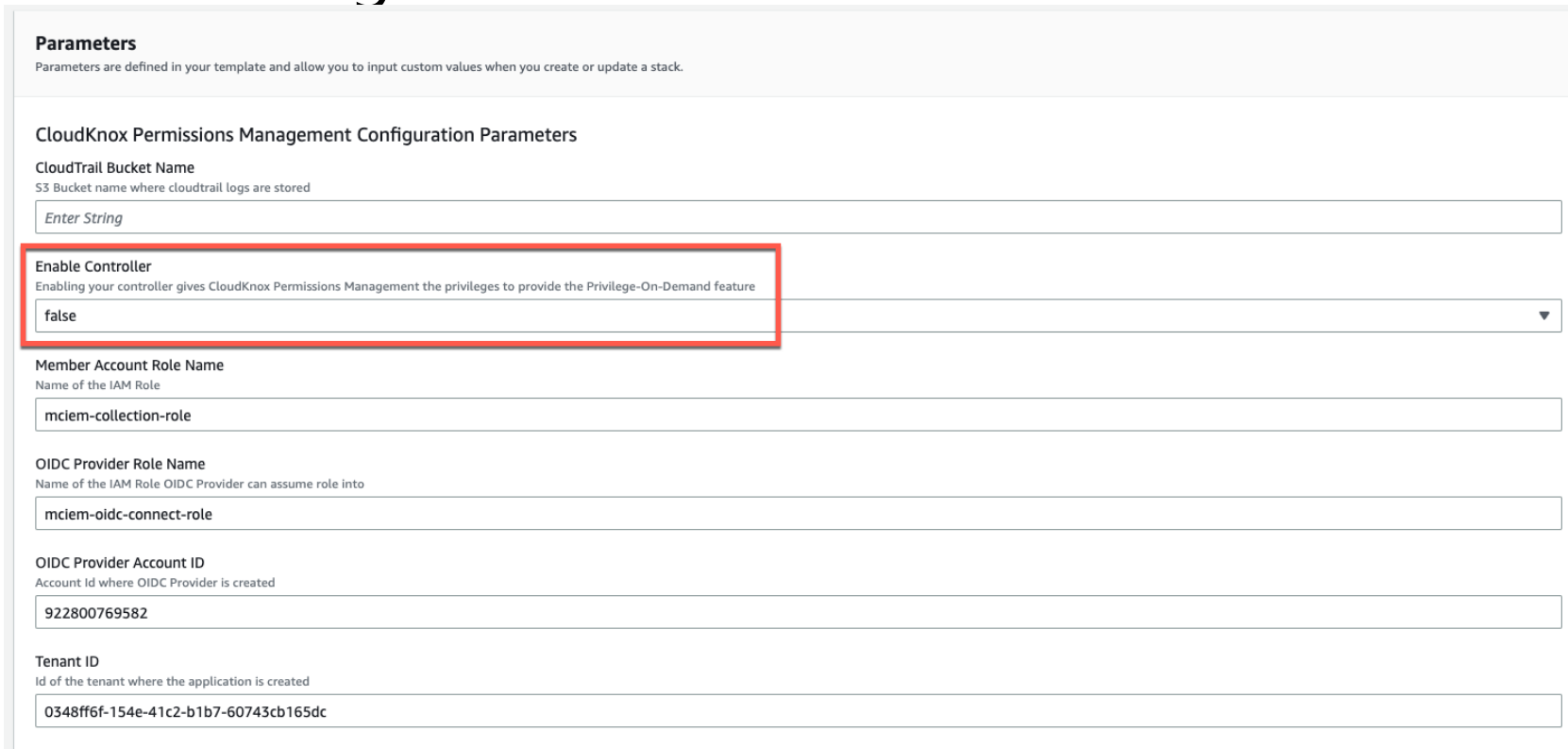
AWS Setup

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

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

Member Account Role Name
Name of the IAM Role

OIDC Provider Role Name
Name of the IAM Role OIDC Provider can assume role into

OIDC Provider Account ID
Account Id where OIDC Provider is created

Tenant ID
Id of the tenant where the application is created

AWS Setup

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

Configure identity provider (IdP)

Configuring Identity Provider is an optional step.

By configuring Identity Provider information, Permissions Management can read user and role access configured at Identity Provider. Admins can see the augmented view of assigned permissions to the identities.

None☒

Select this option if you do not want any integration

AWS IAM Identity Center☐


Allow Permissions Management to read user and role access configured at AWS IAM Identity Center

Okta☐

Allow Permissions Management to read user and role access configured at Okta

AWS Setup

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

Configure data collection:  AWS

Review and Confirm


Review all your information before you start data collection.

Azure App Name	mciem-aws-oidc-connector
OIDC Account ID	922800769582
OIDC Account Role	mciem-oidc-connect-role
Member Account Role	mciem-collection-role
Management Account Id	922800769582
Management Account Role	mciem-org-read-role
Authorization Systems	Automatically Manage

Back

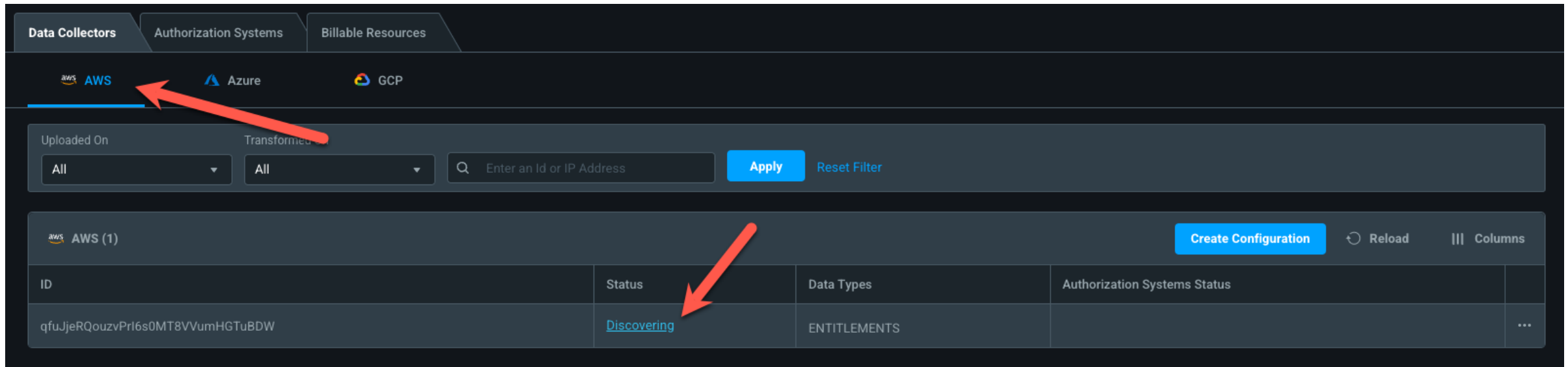
Save & Verify Later

Verify Now & Save



AWS Setup

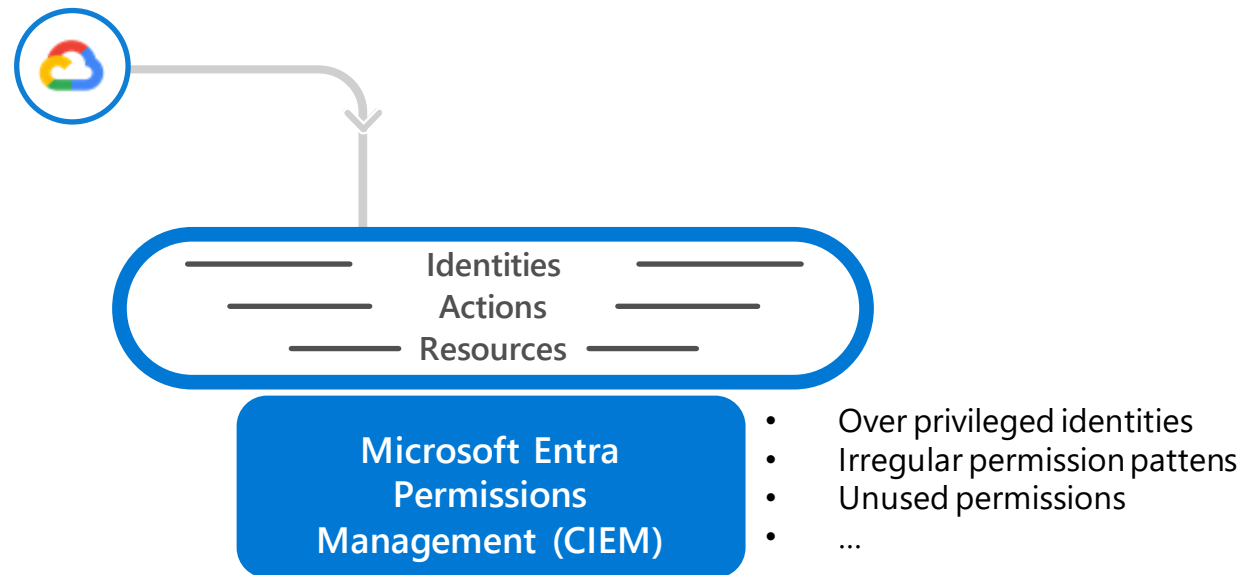
7. You should now see an AWS Data Collector with a Discovering Status. Discovery may take some time.



The screenshot displays the AWS Data Collector management interface. At the top, there are tabs for 'Data Collectors', 'Authorization Systems', and 'Billable Resources'. Below these, there are buttons for 'AWS', 'Azure', and 'GCP'. The 'AWS' button is highlighted with a red arrow. Below the buttons, there are filters for 'Uploaded On' and 'Transformed', both set to 'All'. A search bar with the placeholder 'Enter an Id or IP Address' and an 'Apply' button are also present. The main table shows one AWS Data Collector with the ID 'qfuJJeRQouzvPrI6s0MT8VVumHGTuBDW'. The 'Status' column for this collector is 'Discovering', which is highlighted with a red arrow. The 'Data Types' column shows 'ENTITLEMENTS'. The 'Authorization Systems Status' column is empty. At the bottom right, there are buttons for 'Create Configuration', 'Reload', and 'Columns'.

ID	Status	Data Types	Authorization Systems Status
qfuJJeRQouzvPrI6s0MT8VVumHGTuBDW	Discovering	ENTITLEMENTS	

GCP Onboarding



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" -IdentifierUri "api://mciem-gcp-oidc-app"`

```
Welcome to Azure Cloud Shell
```

```
Type "az" to use Azure CLI
```

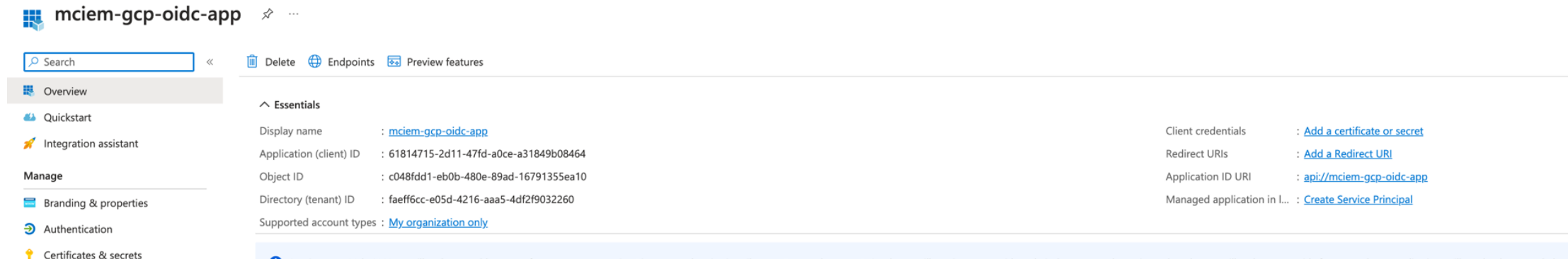
```
Type "help" to learn about Cloud Shell
```

```
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



The screenshot shows the Azure AD application registration page for an application named 'mciem-gcp-oidc-app'. The interface includes a left-hand navigation pane with options like Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, and Certificates & secrets. The main content area displays the 'Essentials' tab, which lists various application properties and their values, along with links to manage client credentials, redirect URIs, and service principals.


Property	Value	Action
Display name	mciem-gcp-oidc-app	
Application (client) ID	61814715-2d11-47fd-a0ce-a31849b08464	
Object ID	c048fdd1-eb0b-480e-89ad-16791355ea10	
Directory (tenant) ID	faeff6cc-e05d-4216-aaa5-4df2f9032260	
Supported account types	My organization only	
Client credentials		Add a certificate or secret
Redirect URIs		Add a Redirect URI
Application ID URI	api//mciem-gcp-oidc-app	
Managed application in I...		Create Service Principal

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

You're in Free Trial





0 out of \$300 credits used

Expires September 14, 2023

[What happens when trial ends?](#)

[ACTIVATE FULL ACCOUNT](#)

You're working on project [My First Project](#) ?

Number: 625806069432  ID: natural-aspect-390023 

[Add people to your project](#)

[Set up budget alerts](#)

[Review credit usage](#)

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 Project details

To connect Permissions Management to GCP, you'll need to create a Permissions Management app in Azure by using the Azure CLI script below.

Azure AD OIDC App Creation ⓘ

Azure App Name*

Azure Command-Line Options

[↓](#) [📄](#) [👁](#)

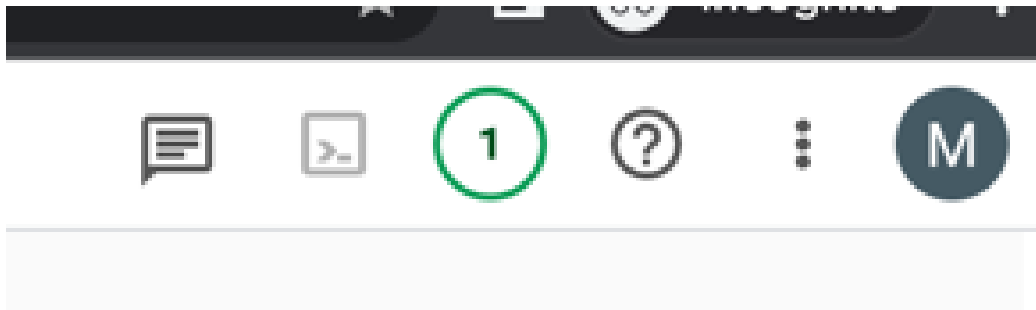
GCP Project details ⓘ

OIDC Project Number*	OIDC Project ID*	OIDC Workload Identity Pool ID*
<input type="text" value="625806069432"/>	<input type="text" value="natural-aspect-390023"/>	<input type="text" value="mciem-wi-pool"/>
OIDC Workload Identity Pool Provider ID*	OIDC Service Account Name*	
<input type="text" value="mciem-wi-provider"/>	<input type="text" value="mciem-service"/>	
G-Suite IDP Secret Name	G-Suite IDP User Email	
<input type="text" value="G-Suite IDP Secret Name"/>	<input type="text" value="G-Suite IDP User Email"/>	

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/acet.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/acet.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.

Manage Authorization Systems

Select an option to manage your authorization systems. An authorization system consists of GCP projects.

Automatically Manage
Allow Permissions Management to automatically manage all authorization systems

Enter Authorization Systems
Select to enter individual authorization system for data collection

Select Authorization Systems
Select specific authorization systems for data collection

Next Step: Create Role Bindings

Choose one of the following options to create role bindings that grant access to your authorization systems.

Console

Add Viewer and Security Reviewer roles to projects, folders, or organization for the Service Account created in the previous step

gCloudShell

Project(s)

```
gcloud projects add-iam-policy-binding <MEMBER_PROJECT_ID> --member="serviceAccount:mciem-service@natural-aspect-390023.iam.gserviceaccount.com" --role="roles/iam.securityReviewer"
gcloud projects add-iam-policy-binding <MEMBER_PROJECT_ID> --member="serviceAccount:mciem-service@natural-aspect-390023.iam.gserviceaccount.com" --role="roles/viewer"
```

Folder(s)

```
gcloud resource-manager folders add-iam-policy-binding <folderID> --member="serviceAccount:mciem-service@natural-aspect-390023.iam.gserviceaccount.com" --role="roles/iam.securityReviewer"
gcloud resource-manager folders add-iam-policy-binding <folderID> --member="serviceAccount:mciem-service@natural-aspect-390023.iam.gserviceaccount.com" --role="roles/viewer"
```


Organization

```
gcloud organizations add-iam-policy-binding <orgID> --member="serviceAccount:mciem-service@natural-aspect-390023.iam.gserviceaccount.com" --role="roles/iam.securityReviewer"
gcloud organizations add-iam-policy-binding <orgID> --member="serviceAccount:mciem-service@natural-aspect-390023.iam.gserviceaccount.com" --role="roles/viewer"
```

GCP Setup

6. Review and Confirm

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

Configure data collection:  **GCP**

Review and Confirm

Review all your information before you start data collection.

Azure App Name	mciem-gcp-oidc-app
OIDC Project Number	625806069432
OIDC Service Account Name	mciem-service
OIDC Workload Identity Pool ID	mciem-wi-pool
OIDC Workload Identity Pool Provider ID	mciem-wi-provider
OIDC Project ID	natural-aspect-390023
Authorization Systems	Automatically Manage

GCP Setup

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

Data Collectors

Authorization Systems

Billable Resources

AWS

Azure

GCP

Uploaded On

Transformed On

Q Enter an Id or IP Address

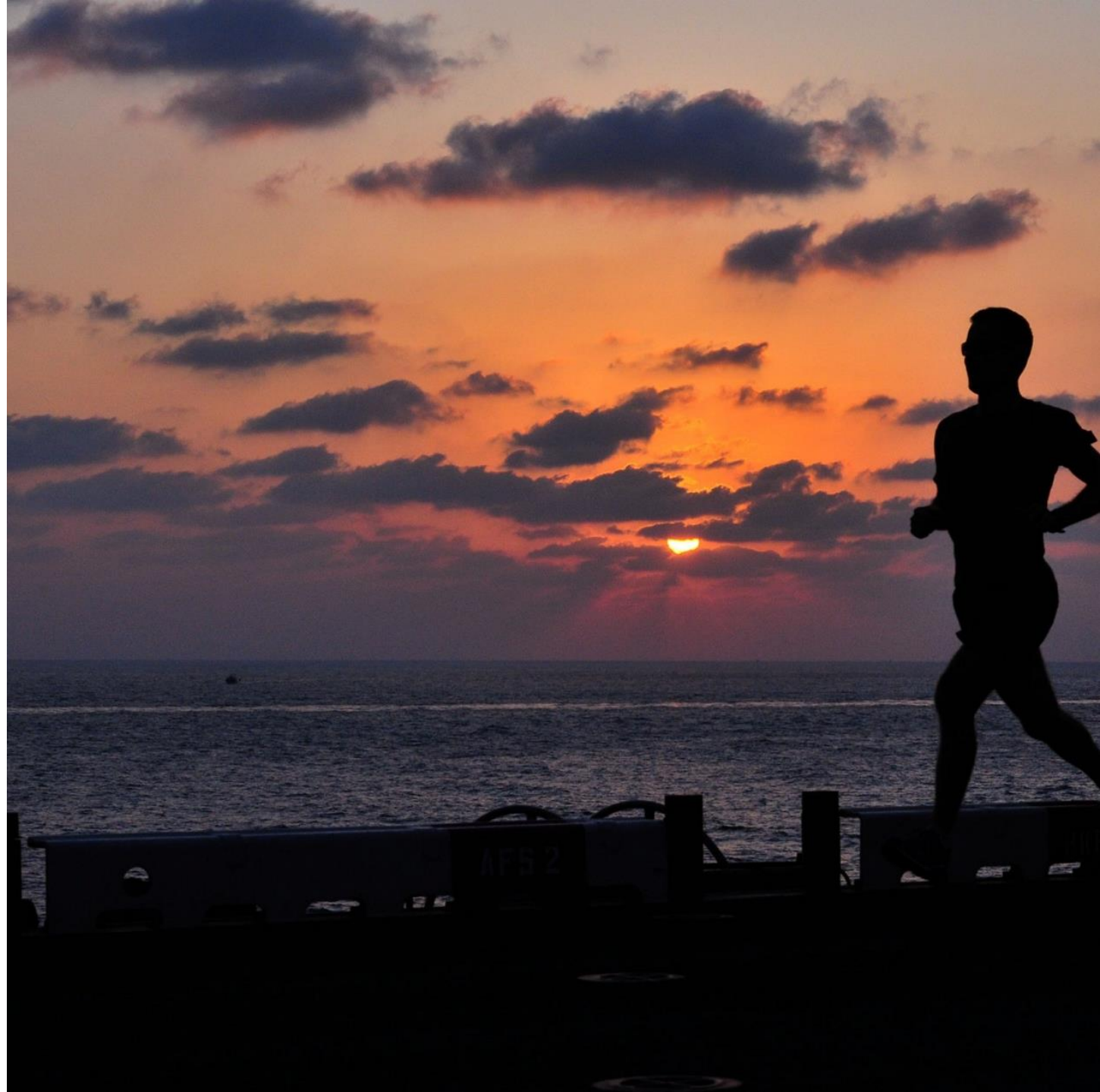
Apply

Reset Filter

GCP (1)

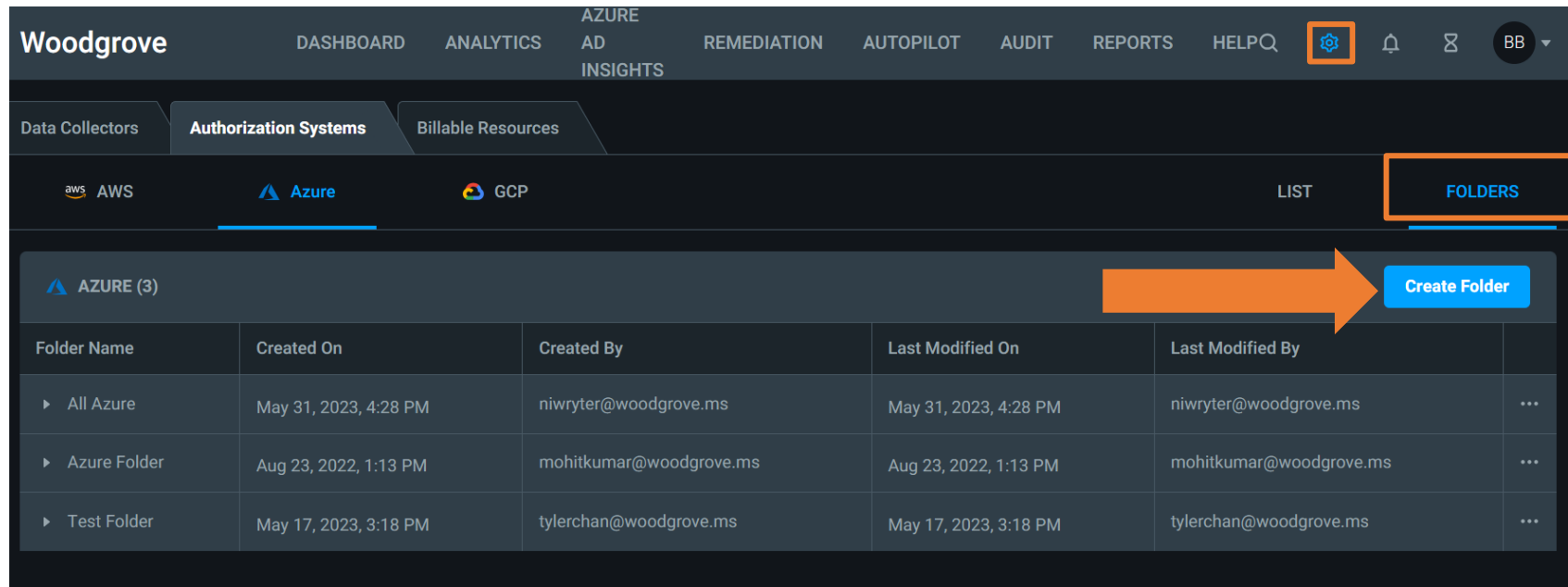
ID	Status	Data Types
ZJ6WpxeKCCrMFK8TTCWN7AYELxNNofPe	Discovering	ENTITLEMENTS

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



The screenshot shows the Woodgrove Azure AD console interface. The top navigation bar includes links for DASHBOARD, ANALYTICS, AZURE AD INSIGHTS, REMEDIATION, AUTOPILOT, AUDIT, REPORTS, and HELP. A settings gear icon is highlighted with an orange box. Below this, the 'Authorization Systems' tab is active, showing options for AWS, Azure, and GCP. The 'FOLDERS' button is also highlighted with an orange box. A table lists existing folders under the 'AZURE (3)' section. An orange arrow points from the 'Create Folder' button to the table.

Folder Name	Created On	Created By	Last Modified On	Last Modified By	
▶ All Azure	May 31, 2023, 4:28 PM	niwryter@woodgrove.ms	May 31, 2023, 4:28 PM	niwryter@woodgrove.ms	...
▶ Azure Folder	Aug 23, 2022, 1:13 PM	mohitkumar@woodgrove.ms	Aug 23, 2022, 1:13 PM	mohitkumar@woodgrove.ms	...
▶ Test Folder	May 17, 2023, 3:18 PM	tylerchan@woodgrove.ms	May 17, 2023, 3:18 PM	tylerchan@woodgrove.ms	...

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](#)

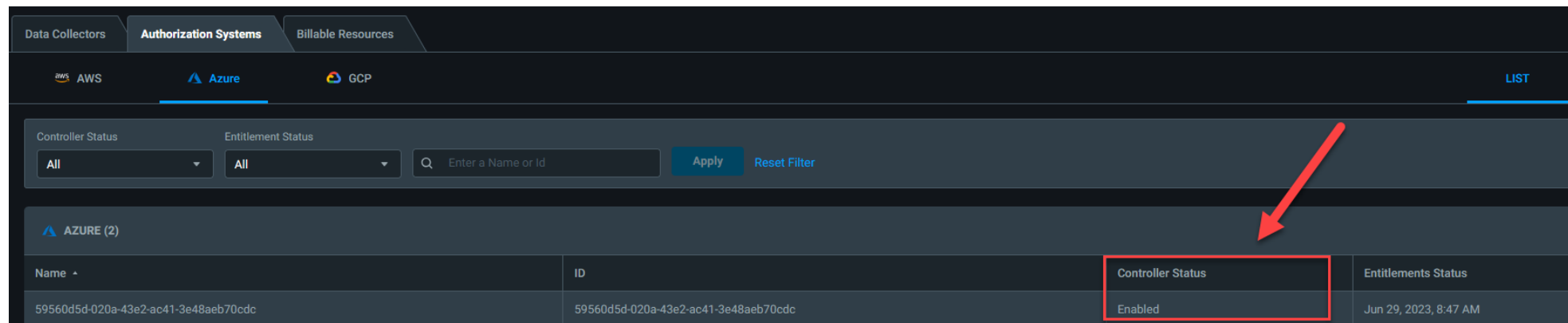
Thank you!



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.

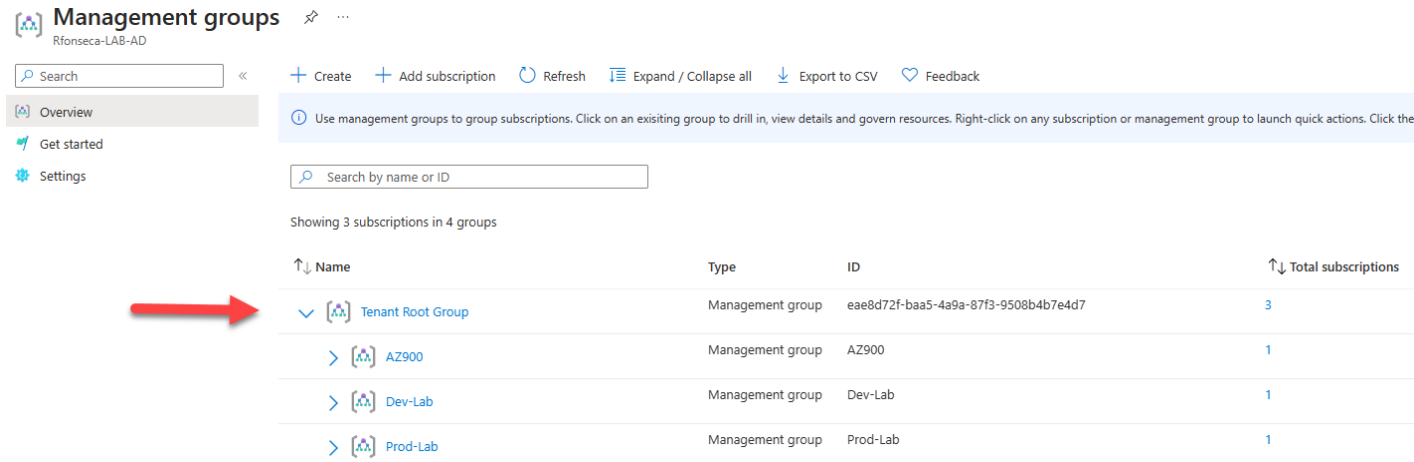


Data Collectors Authorization Systems Billable Resources			
AWS Azure GCP LIST			
Controller Status: All Entitlement Status: All Search: Enter a Name or Id Apply Reset Filter			
AZURE (2)			
Name	ID	Controller Status	Entitlements Status
59560d5d-020a-43e2-ac41-3e48aeb70cdc	59560d5d-020a-43e2-ac41-3e48aeb70cdc	Enabled	Jun 29, 2023, 8:47 AM

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



The screenshot shows the Azure portal interface for 'Management groups' under the 'Rfonseca-LAB-AD' subscription. The left sidebar contains navigation links: 'Overview' (selected), 'Get started', and 'Settings'. The main content area displays a table of management groups. A red arrow points to the 'Tenant Root Group' row.

↑↓ Name	Type	ID	↑↓ Total subscriptions
✓ [Azure Icon] Tenant Root Group	Management group	ee8d72f-baa5-4a9a-87f3-9508b4b7e4d7	3
> [Azure Icon] AZ900	Management group	AZ900	1
> [Azure Icon] Dev-Lab	Management group	Dev-Lab	1
> [Azure Icon] Prod-Lab	Management group	Prod-Lab	1

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

The screenshot shows the Azure portal's 'Access control (IAM)' page for a 'Tenant Root Group'. The left sidebar contains navigation links: Overview, Subscriptions, Resource Groups, Resources, Activity Log, Access control (IAM), Governance, Get started, Security, and Policy. The main area is titled 'Access control (IAM)' and includes a search bar and filters. The 'Role assignments' tab is selected, showing a filtered set of results (5 total). A table lists the assignments, with one item highlighted: 'User Access Administrator' role assigned to 'Cloud Infrastructure Entitlement Management' (App) with the scope 'This resource'. A red arrow points to the 'User Access Administrator' role name, and a red box highlights the entire row.

Name	Type	Role	Scope	Condition
Cloud Infrastructure Entitlement Management	App	User Access Administrator	This resource	Add

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 *mciam-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**.

