


ASM AZURE INTEGRATION

 This integration is not currently supported for Azure Government users.


With Azure, Mandiant Advantage Attack Surface Management (MA-ASM) retrieves public virtual machine (VM) instances, public DNS zones, and Blob Storage resources. For Blobs, MA-ASM checks to see if they are publicly accessible and creates relevant issues. This gives a more thorough view of your inventory.

 Only one Azure integration is allowed per Project in MA-ASM.

Adding this integration requires three steps:

1. Give MA-ASM access to Azure

For this step, you are required to authenticate using an Azure account that has privileges to add an application to the Azure account. This should be one of the following account types:

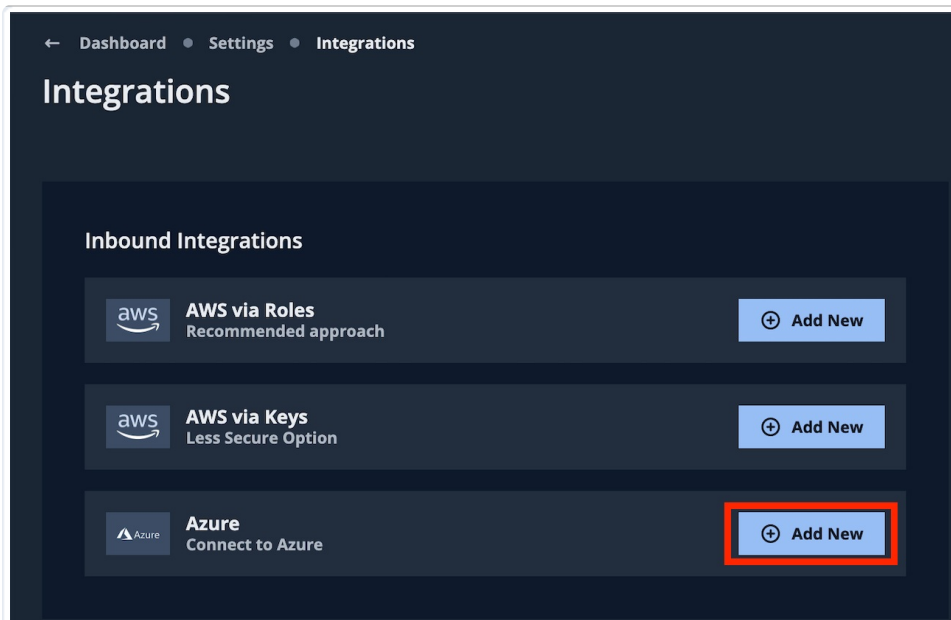
- 
 - Global Administrator
 - Privileged Role Administrator
 - Cloud Application Administrator
 - Application Administrator

2. Add role assignment for MA-ASM in Azure

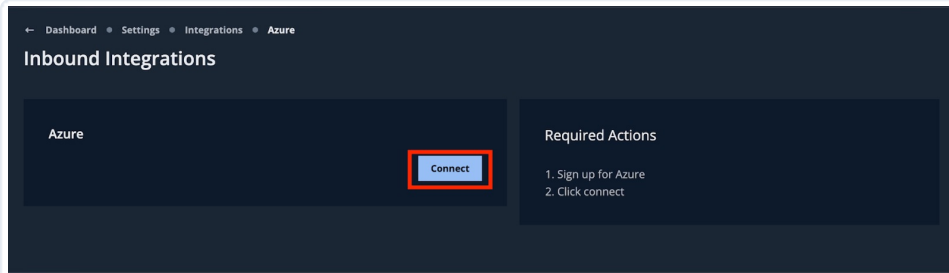
3. Connect the integration to the appropriate Collection

Give MA-ASM access to Azure

- From the **Projects and Settings** menu in MA-ASM, select the appropriate Project then click **Account Settings**.
- Click **Integrations**.
- Next to Azure, click **Add New**.

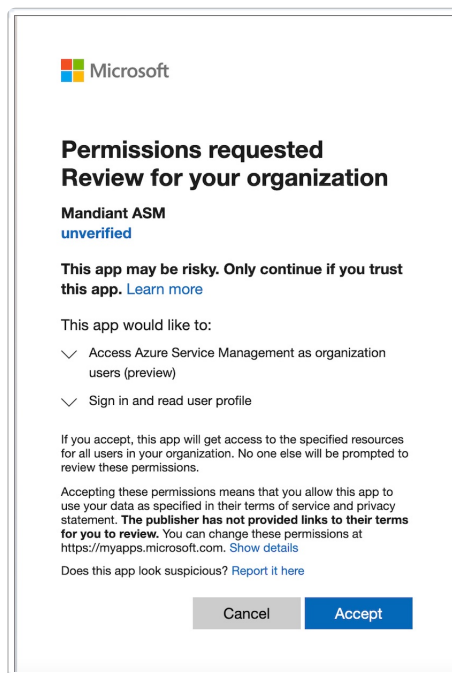


4. Click **Connect**.



The system redirects you to the Microsoft sign-in page.


5. Authenticate using an account that has privileges to add an application to the Azure account.
6. When authentication is complete, you see a Microsoft screen requesting permission for **Mandiant ASM** to access your Azure instance.



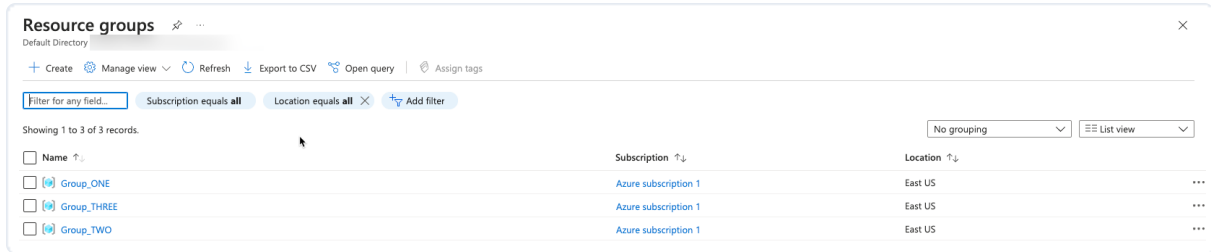
7. Click **Accept** and the system redirects you back to MA-ASM.

Add role assignment for MA-ASM in Azure

Role assignment can be performed for specific resource groups, or all resource groups in a subscription. This includes any future resource groups that may be added to a subscription. For role assignment, sign in to the Azure Portal and perform the following actions:

 The following screenshots depict the role assignment workflow for resource groups but the process is the same for subscriptions.

1. Browse to **Resource groups** (<https://portal.azure.com/#blade/HubsExtension/BrowseResourceGroups>) (or **Subscriptions** (https://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade)) within Microsoft Azure.



Resource groups

Default Directory

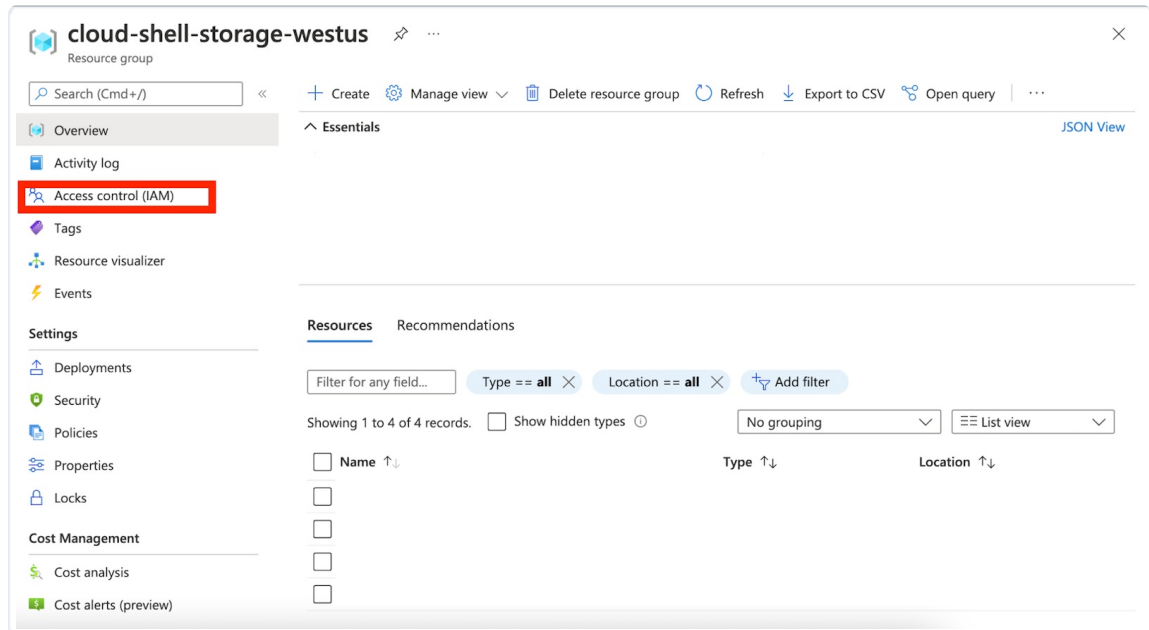
+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

Showing 1 to 3 of 3 records. No grouping List view

| Name | Subscription | Location |
|-------------|----------------------|----------|
| Group_ONE | Azure subscription 1 | East US |
| Group_THREE | Azure subscription 1 | East US |
| Group_TWO | Azure subscription 1 | East US |

2. For each resource group (or subscription) that you would like to allow MA-ASM to pull data in from, perform the following actions:
 - a. Click the respective resource group (or subscription).
 - b. Click **Access control (IAM)**.



cloud-shell-storage-westus

Resource group

Search (Cmd+/) Create Manage view Delete resource group Refresh Export to CSV Open query

Overview Activity log **Access control (IAM)** Tags Resource visualizer Events

Settings Deployments Security Policies Properties Locks Cost Management Cost analysis Cost alerts (preview)

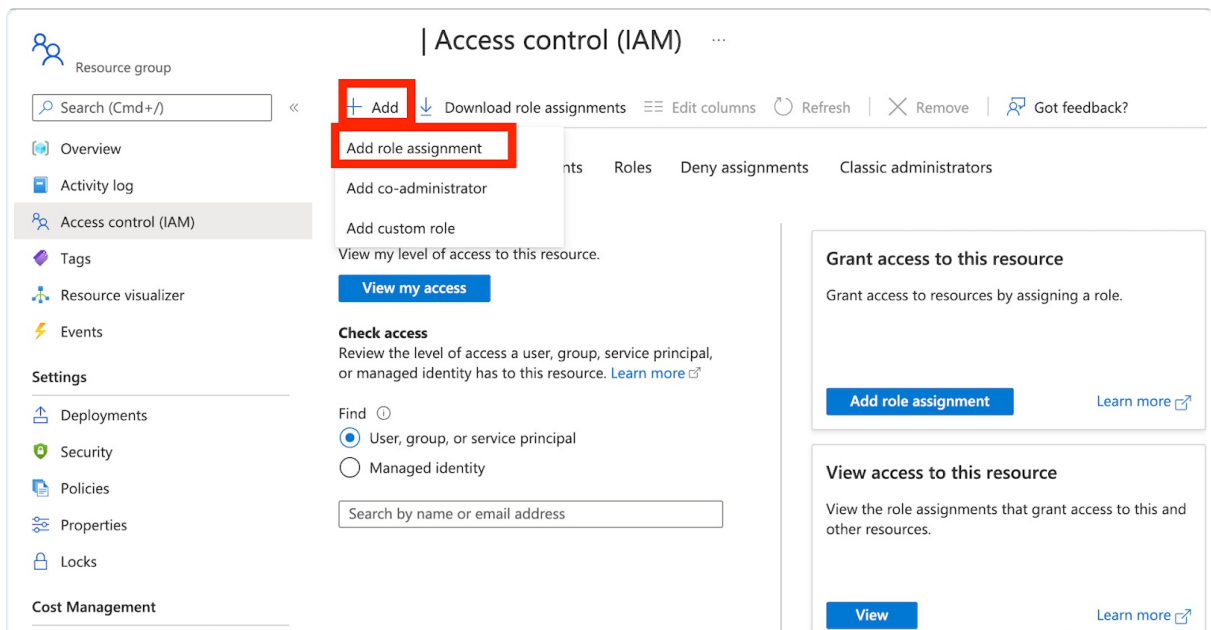
Resources Recommendations

Filter for any field... Type == all Location == all Add filter

Showing 1 to 4 of 4 records. Show hidden types No grouping List view

| Name | Type | Location |
|------|------|----------|
| | | |
| | | |
| | | |
| | | |

3. Within the **Access Control (IAM)** menu, click **Add** and select **Add role assignment**.



Resource group | Access control (IAM)

Search (Cmd+/) Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log **Access control (IAM)** Tags Resource visualizer Events

Settings Deployments Security Policies Properties Locks Cost Management

Roles Deny assignments Classic administrators

Add co-administrator

Add custom role

View my level of access to this resource.

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find

User, group, or service principal

Managed identity

Search by name or email address

Grant access to this resource

Grant access to resources by assigning a role.

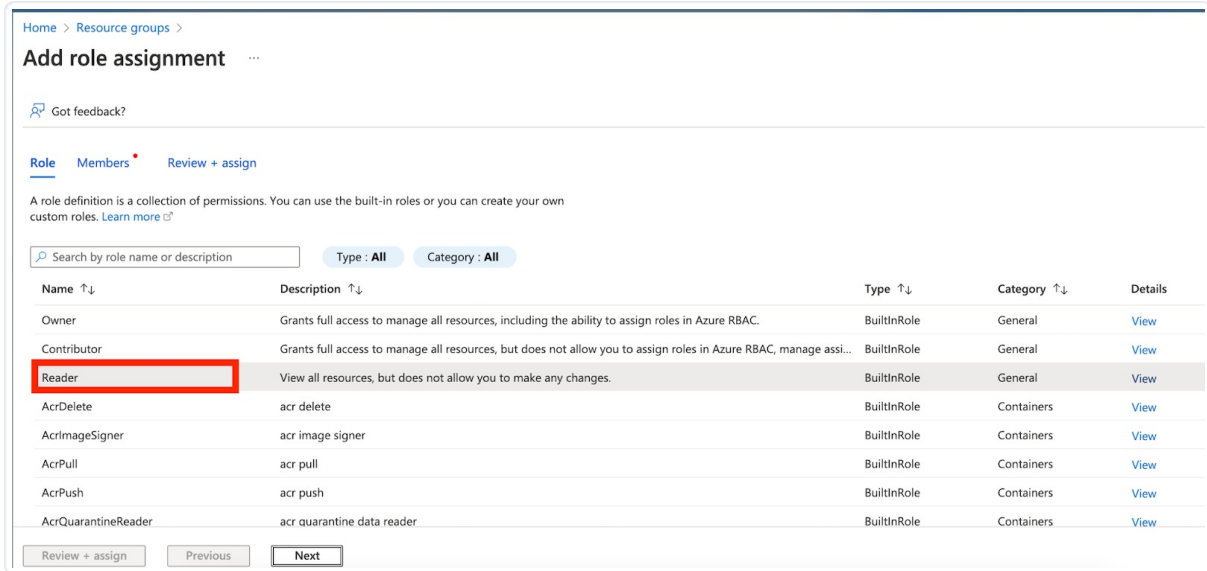
Add role assignment [Learn more](#)

View access to this resource

View the role assignments that grant access to this and other resources.

View [Learn more](#)

4. Select **Role** and choose the **Reader** role for view-only access. Click **Next**.



Home > Resource groups >

Add role assignment

Got feedback?

Role Members Review + assign

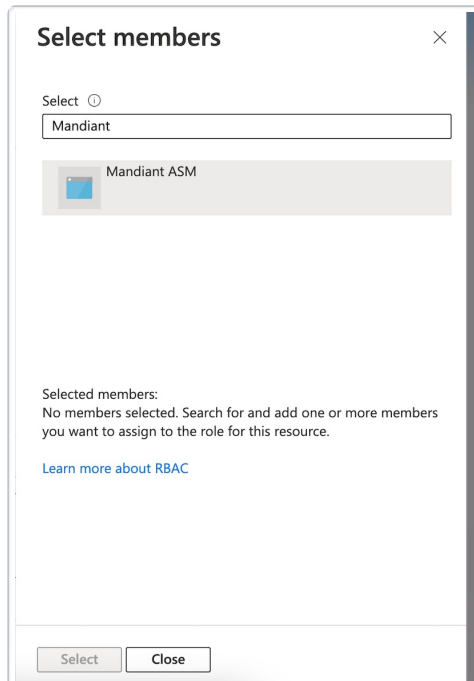
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Search by role name or description Type: All Category: All

| Name ↑↓ | Description ↑↓ | Type ↑↓ | Category ↑↓ | Details |
|---------------------|------------------------------------------------------------------------------------------------------------------|-------------|-------------|----------------------|
| Owner | Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. | BuiltInRole | General | View |
| Contributor | Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assi... | BuiltInRole | General | View |
| Reader | View all resources, but does not allow you to make any changes. | BuiltInRole | General | View |
| AcrDelete | acr delete | BuiltInRole | Containers | View |
| AcrImageSigner | acr image signer | BuiltInRole | Containers | View |
| AcrPull | acr pull | BuiltInRole | Containers | View |
| AcrPush | acr push | BuiltInRole | Containers | View |
| AcrQuarantineReader | acr quarantine data reader | BuiltInRole | Containers | View |

Review + assign Previous **Next**

5. On the **Members** screen, choose the following options:
 - a. **Assign access to: User, group, or service principal**
 - b. Click + **Select members**. When the **Select members** menu opens, search for and select **Mandiant ASM**.
 - c. Click **Select**.



Select members

Select

Mandiant

Mandiant ASM

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

[Learn more about RBAC](#)

Select Close

6. Click **Review + assign**.

Home > Resource groups >

Add role assignment


Got feedback?

Role **Members** Review + assign

Selected role Reader

Assign access to User, group, or service principal
 Managed identity

Members + Select members

| Name | Object ID | Type |
|--------------|--------------------------------------|-----------------------------------------------------------------------------------------|
| Mandiant ASM | ff540617-cdcd-4f64-ac6f-6ba7f7db10ee | App  |

Description Optional

Review + assign Previous Next

7. Ensure that all the information in the **Review + assign** section is correct and click **Review + assign**.

Home > Resource groups >

Add role assignment

Got feedback?

Role Members **Review + assign**

Role Reader

Scope /subscriptions/

Members


| Name | Object ID | Type |
|--------------|--------------------------------------|------|
| Mandiant ASM | ff540617-cdcd-4f64-ac6f-6ba7f7db10ee | App |

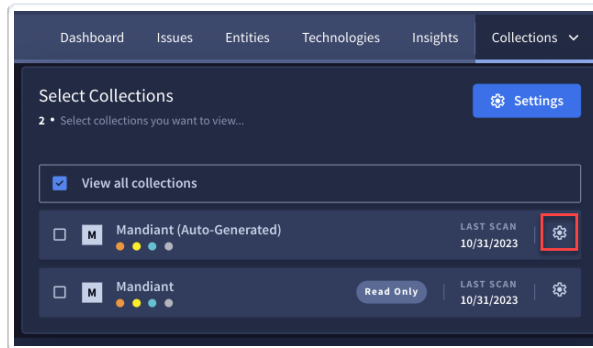
Description No description

Review + assign Previous

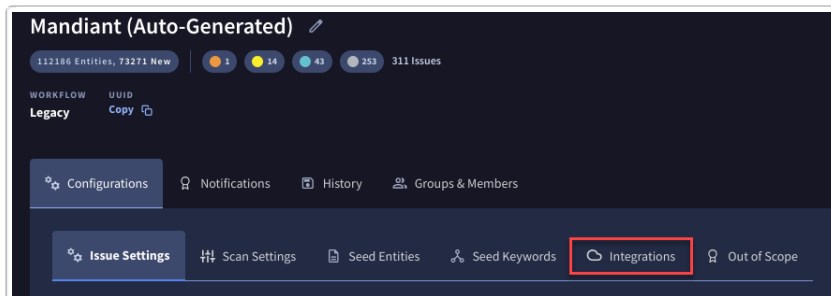
Connect the integration to the appropriate Collection

Connect the integration to the appropriate Collection.

- a. Click **Collections** and click  **Collection Settings** for the Collection that you want to connect the integration to.



b. Select the **Integrations** tab.




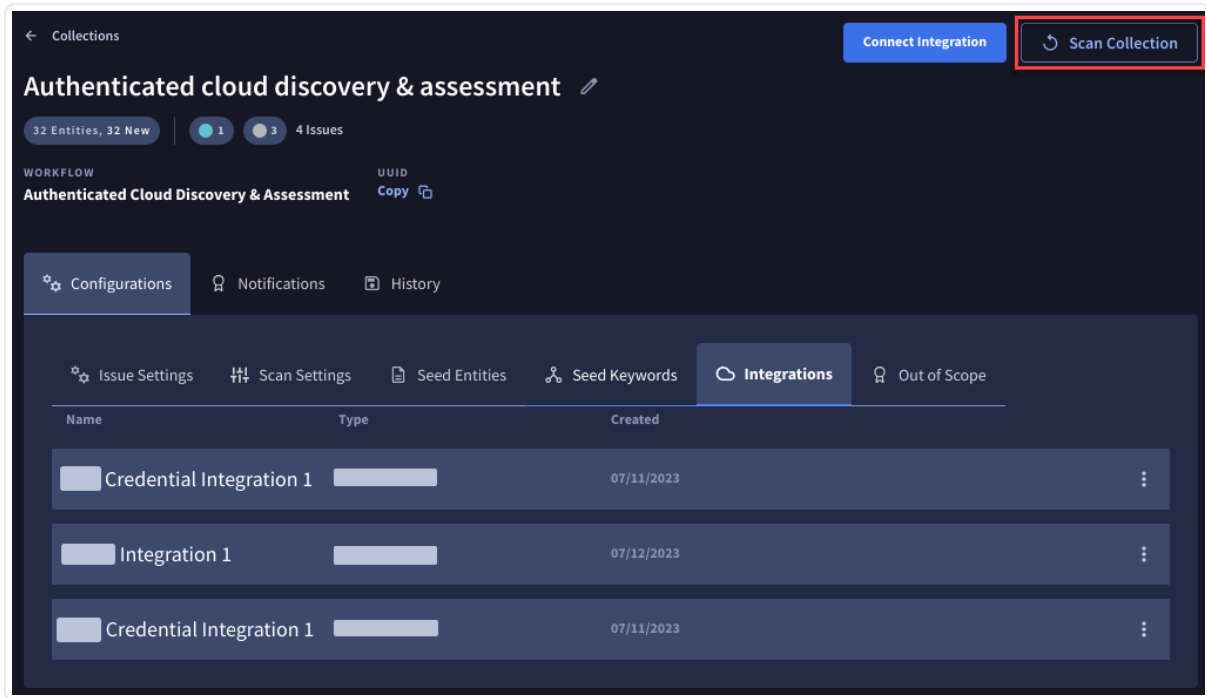
c. Select **Connect Integration** and **Link** the integration.



The integration is immediately added to the Collection.



d. Click  to close the **Connect Integration** pane. Click **Scan Collection** to update your Collection with the current settings and integrations. Otherwise, your newly configured integration is incorporated at your regularly scheduled scan interval.



Repeat the same steps for each resource group or subscription you would like MA-ASM to access.