Mandiant

ASM AWS INTEGRATION

> This integration is not currently supported for AWS GovCloud (US) users.

To provide a more thorough view of your inventory, Mandiant Advantage Attack Surface Management (MA-ASM) can integrate with Amazon Web Services (AWS) to retrieve the following:

- Public EC2 instances
- S3 buckets

  > MA-ASM confirms whether S3 buckets are publicly accessible and creates relevant Issues.

- Route 53 zones
- Amazon Relational Database Service (RDS DB) instances

  > MA-ASM uses Mandiant Security Integrations-as-a-Service (MSI) to collect RDS DB data.

Adding the AWS integration requires three steps:

1. **Create the policy in AWS**
2. **Create an access method for MA-ASM**
3. **Provide AWS credentials to MA-ASM**

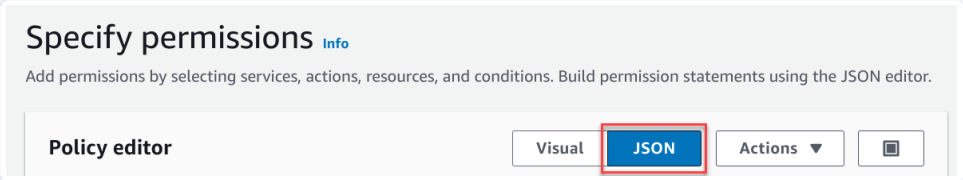
Create the policy in AWS

You first need to create the policy in AWS for MA-ASM to use.

1. Authenticate to AWS and browse to **Identity and Access Management (IAM)** in the AWS console.
2. Go to **Access Management > Policies**. Alternatively, access **https://us-east-1.console.aws.amazon.com/iam/home#/policies**.
3. Click **Create policy**.

   > You must have permissions to create roles and policies within AWS.

4. Select **JSON**.



5. Copy and paste the following JSON snippet into the text field and click **Next**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

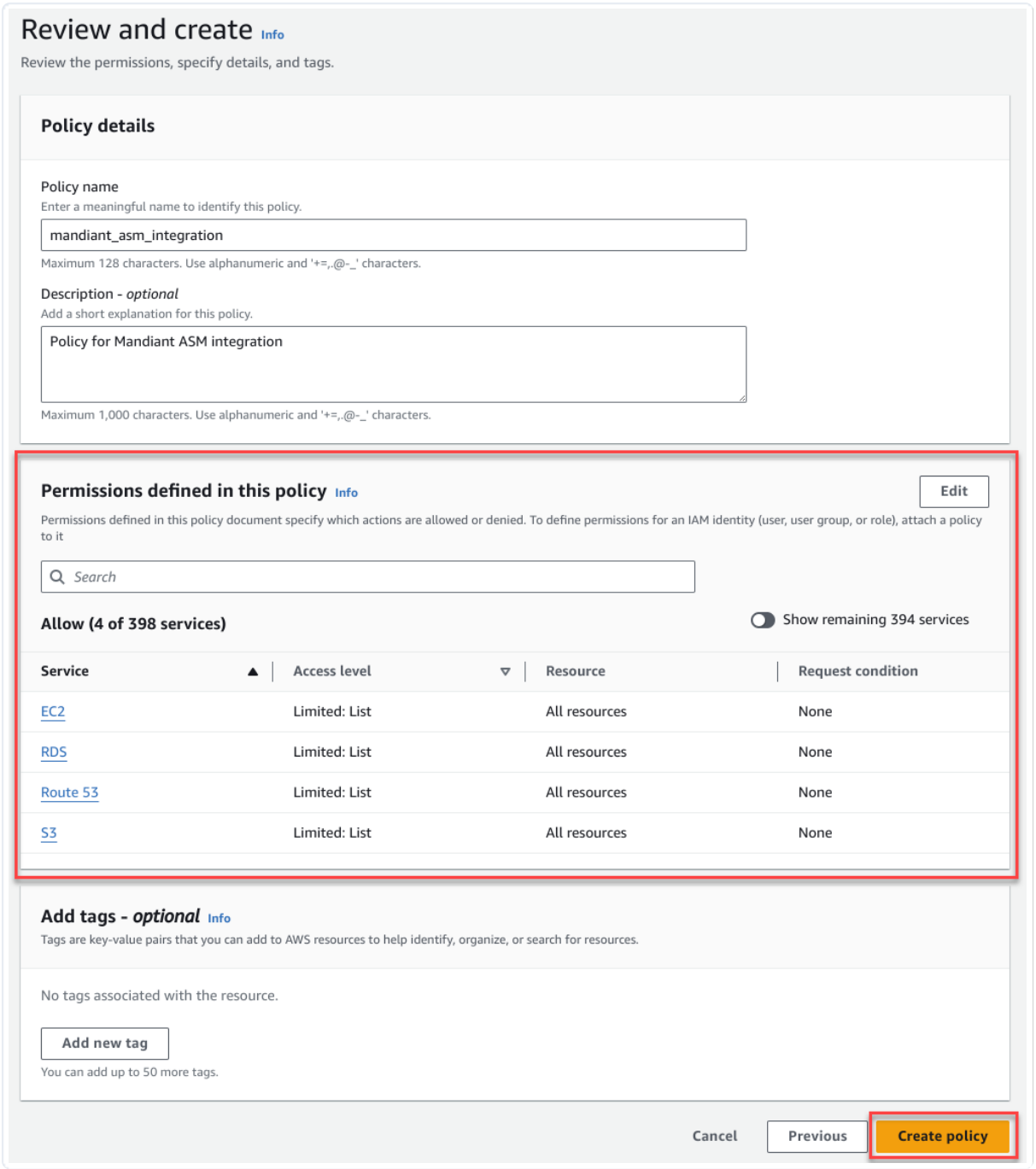
```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":"s3:ListAllMyBuckets",
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":"ec2:DescribeInstances",
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":"rds:DescribeDBInstances",
      "Resource":"*"
    }
  ]
}
```

6. On the **Review and create** page, populate the following **Policy details** fields:
   - **Policy name**: Name for the policy.

     Make a note of the name that you use as it is needed in the next section.

   - **Description - *optional***: Description of the policy.
7. Review the **Permissions defined in this policy** section and click **Create policy**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



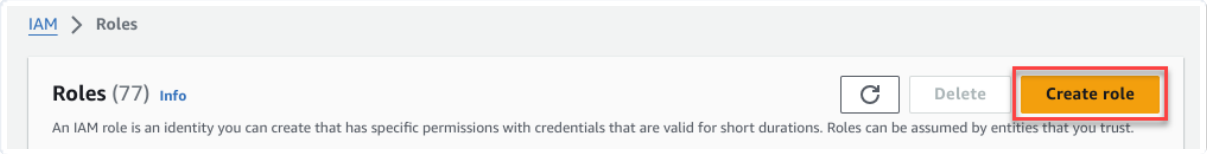
Authenticate using cross-account access

Once the AWS Policy is created, you must provide a method for MA-ASM to authenticate with your AWS Accounts. MA-ASM uses the cross-account access from the preceding section to automatically generate temporary, short-lived tokens whenever it needs to integrate with your AWS account. This access method eliminates the need for any additional access keys.

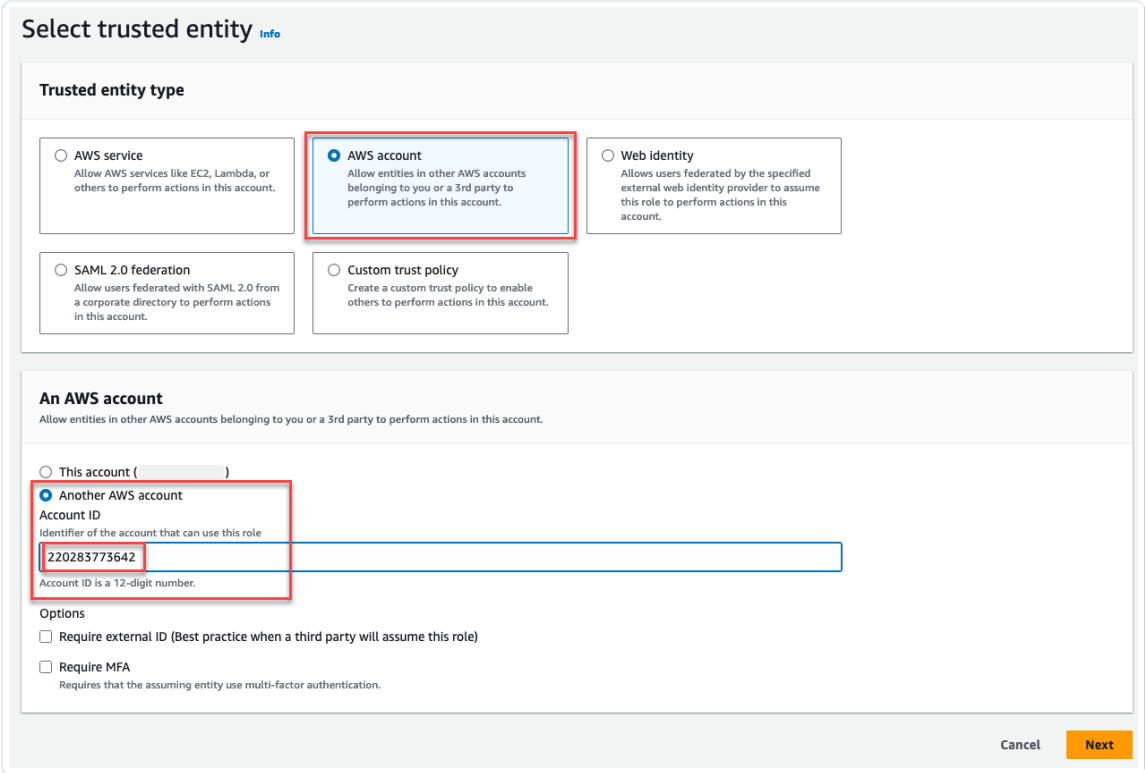
1. In the AWS console, browse to **Identity and Access Management (IAM)**.
2. Go to **Access Management > Roles**. Alternatively, access **https://us-east-1.console.aws.amazon.com/iam/home#/roles**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

3. Click **Create role**.



4. On the **Select trusted entity** page:
   a. Select the **AWS Account** tile.
   b. Select the **Another AWS account** radio button.
   c. In the **Account ID** field, enter `220283773642`.



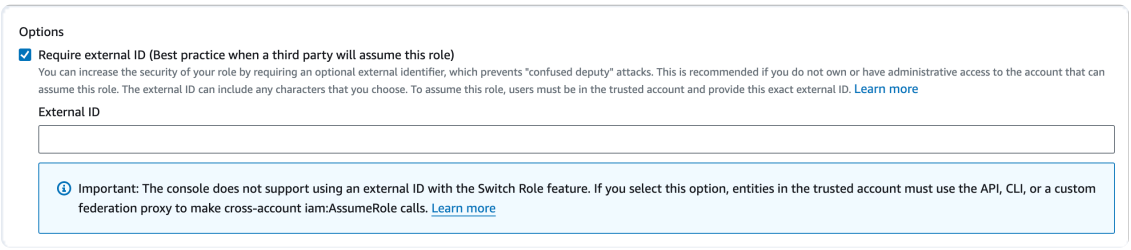
5. Under **Options**, select the checkbox requiring use of an external ID. Copy the **External ID** from MA-ASM and paste it here.

> Requiring an External ID is an AWS best practice when a third party (MA-ASM, in this case) assumes the role.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

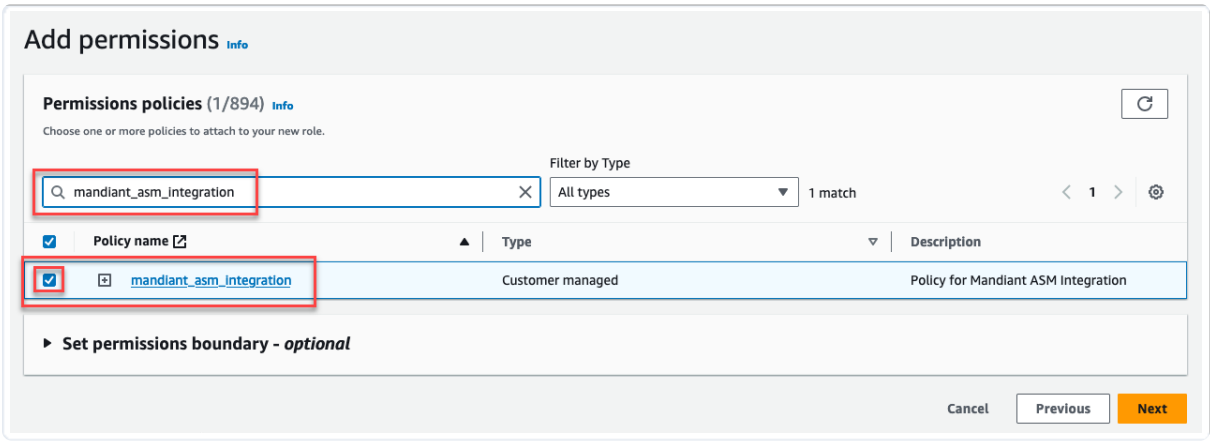
- There is one External ID per MA-ASM project.
- To access the **AWS External ID** from MA-ASM:
  1. From the **Projects and Settings** menu in MA-ASM, select the appropriate Project then click Account Settings.
  2. Click **Integrations**.
  3. Click **Add New** for **AWS (Roles)**.
  4. Click **Copy Key**.

AWS External ID in MA-ASM with **Copy Key** option



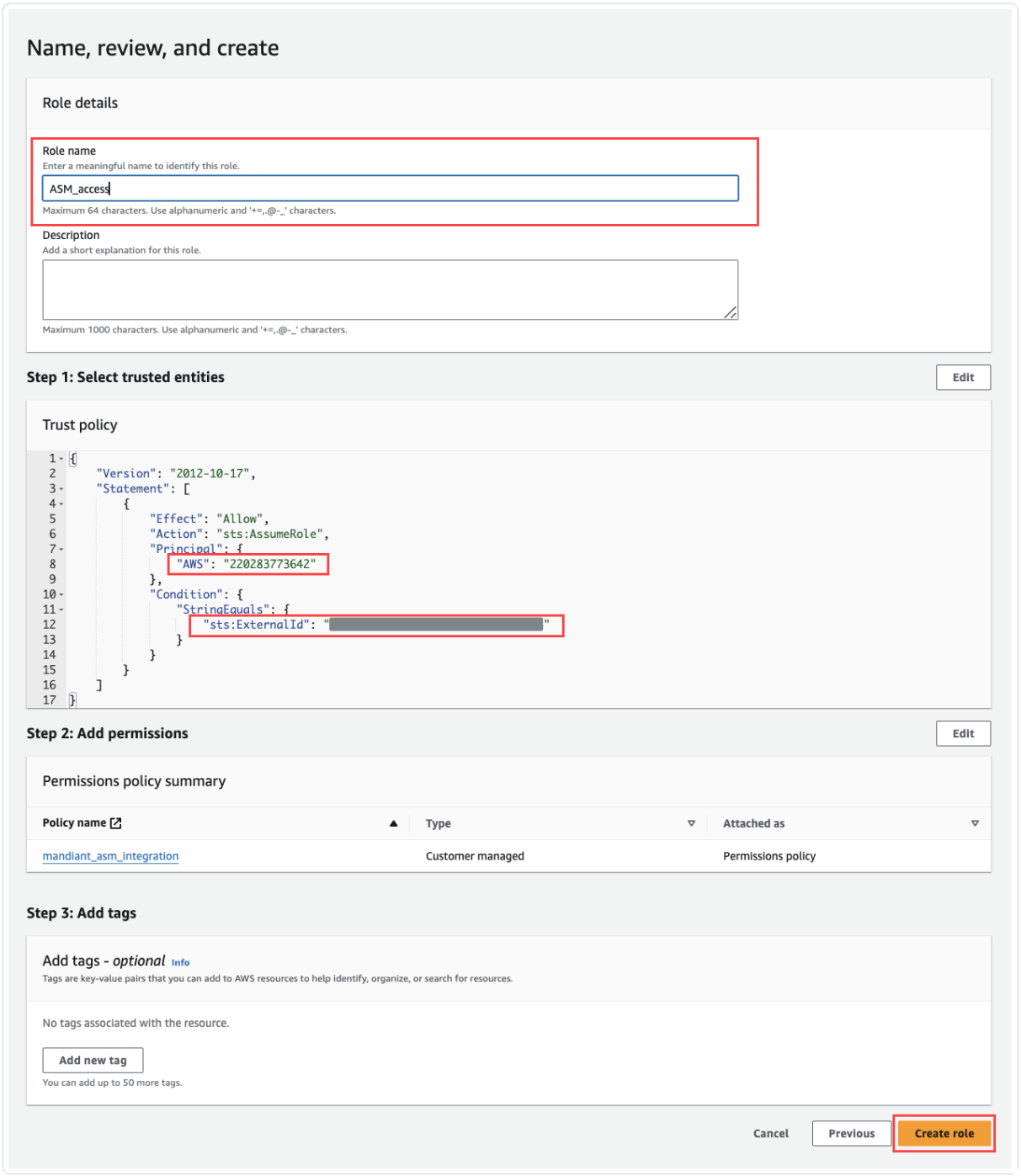
AWS view with option selected to require an external ID

6. Click **Next**.
7. On the **Add permissions** page, search for the name of the policy that you created in the preceding section. Once the search populates, select the checkbox associated with the policy.



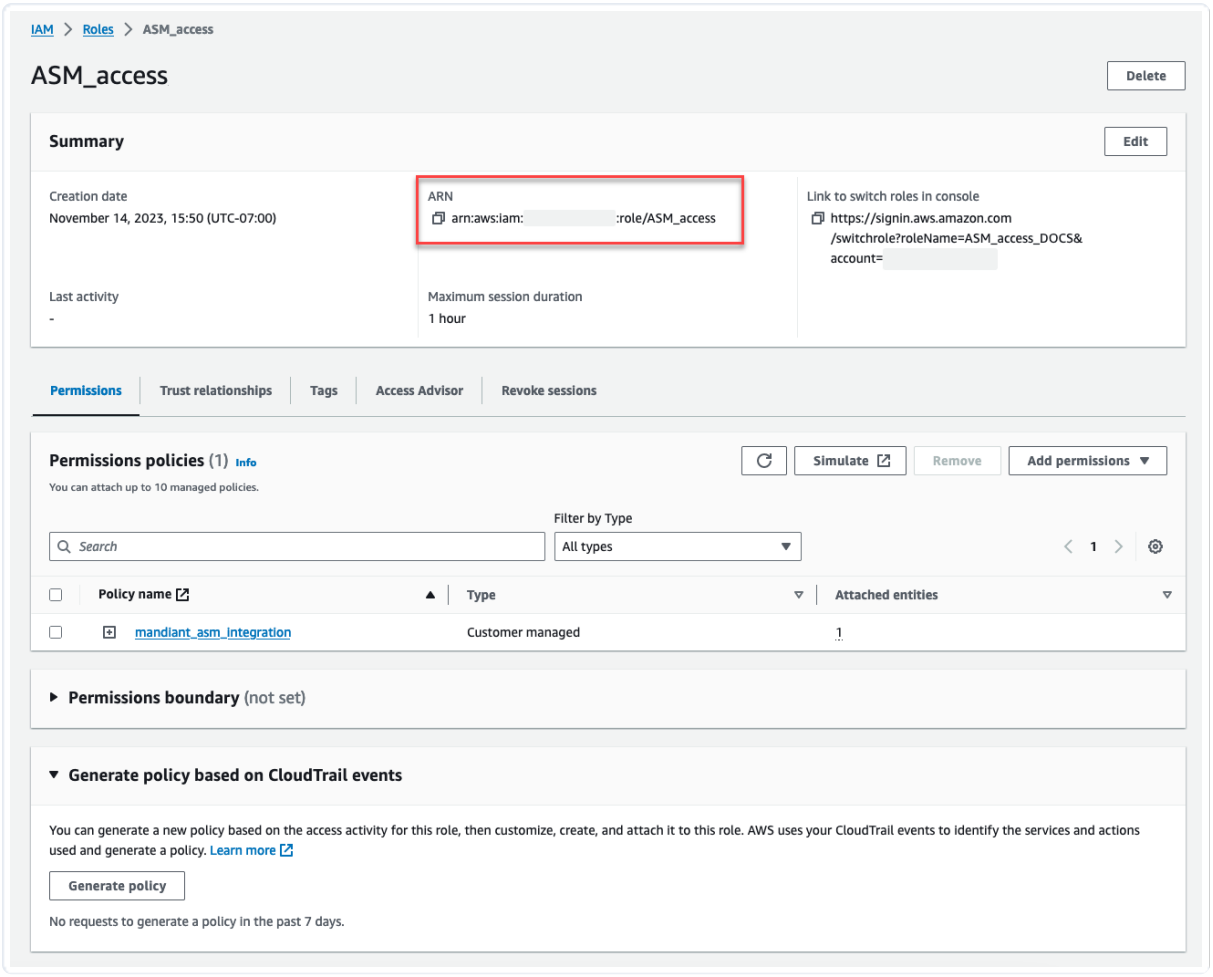
8. Click **Next**.
9. On the **Name, review and create** page:
   a. In the **Role name** field, enter a meaningful name.
   b. Confirm that the **Step 1: Select trusted entities** section shows `"AWS": "220283773642"` and `"sts:ExternalID": "AWS External ID"`.
   c. Click **Create role**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



10. Select the newly created role and make a note of the **Role ARN** to be used when **providing AWS Credentials to MA-ASM**.

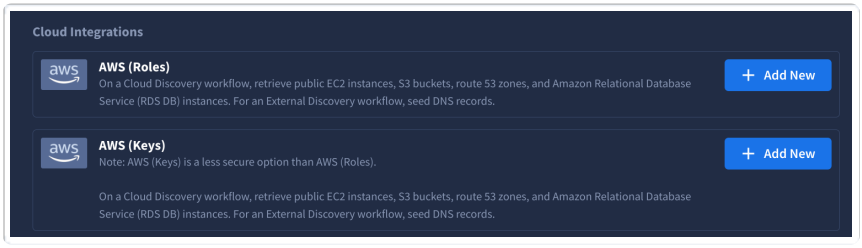
MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



Provide AWS Credentials to MA-ASM

Now that you have AWS ready to accept connection requests from MA-ASM, it's time to add the appropriate AWS credentials into your Project.

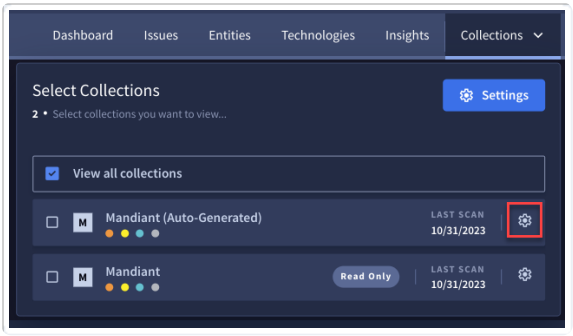
1. From the **Projects and Settings** menu in MA-ASM, select the appropriate Project then click **Account Settings**.
2. Click **Integrations**.
3. Click **Add New** for the appropriate connection method:
    - Recommended: **AWS (Roles)**
    - **AWS (Keys)**



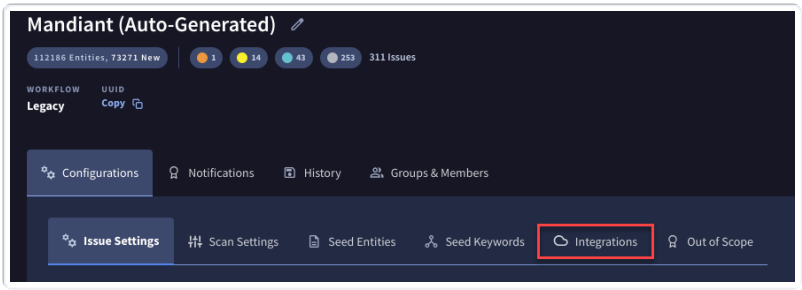
4. Depending on what you select in the preceding step:
    - Enter the **Role ARN** value from your AWS account into the appropriate field.
    - Enter the AWS **Access Key ID** and AWS **Secret Access Key** into the appropriate fields.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

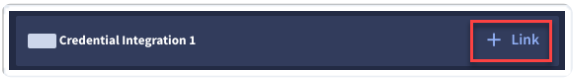
5. Click **Connect**.
6. Connect the integration to the appropriate Collection.
    a. Click **Collections** and click **Collection Settings** for the Collection that you want to connect the integration to.



    b. Select the **Integrations** tab.

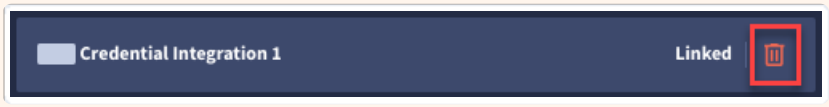


    c. Select **Connect Integration** and **Link** the integration.



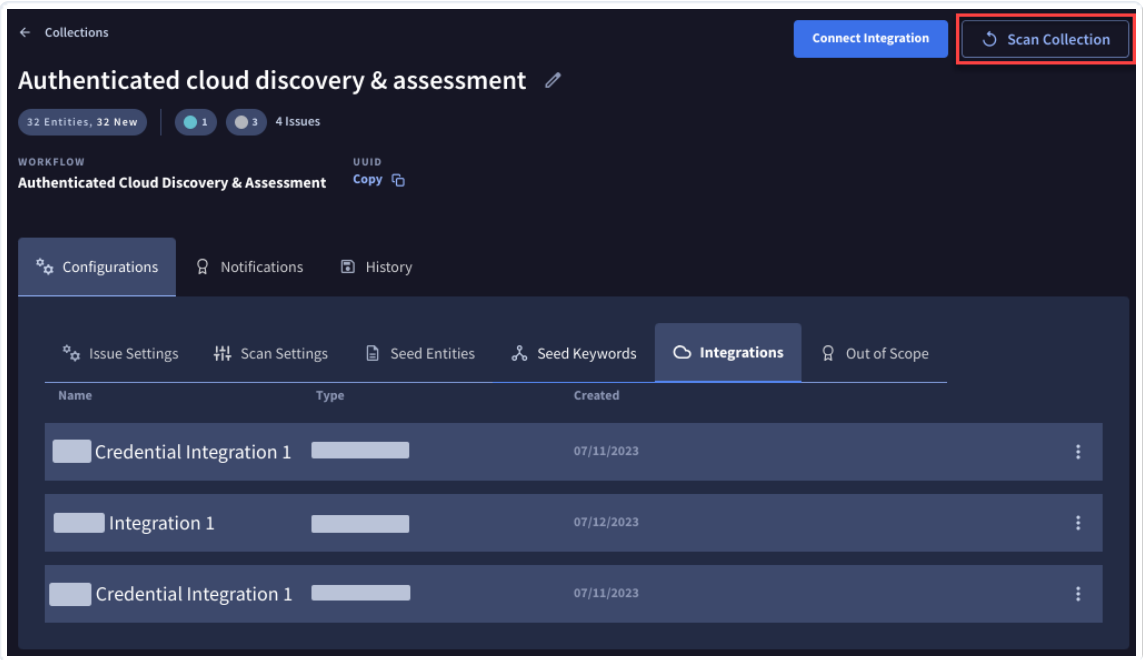
    The integration is immediately added to the Collection.

    Click to remove the integration from this 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.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.