



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:

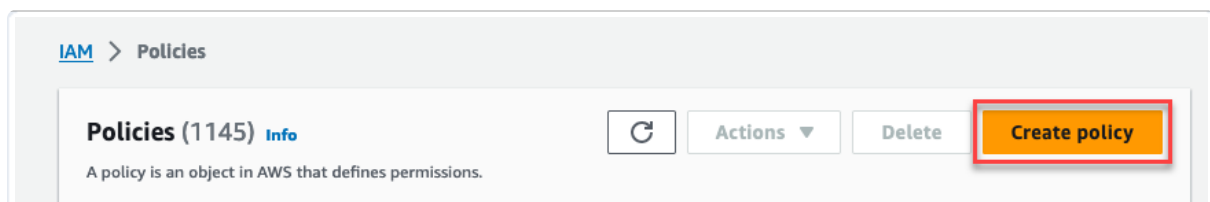
1. **Create the policy in AWS**
2. **Create an access method for MA-ASM**
3. **Provide AWS credentials to MA-ASM**

Create the policy in AWS

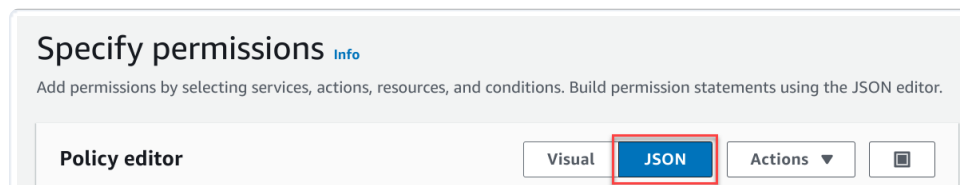
You first need to create the policy in AWS for MA-ASM to use.

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**.

```
{
  "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**.

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=, @, _' characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=, @, _' characters.

Permissions defined in this policy [Info](#) Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (4 of 398 services) Show remaining 394 services

Service	Access level	Resource	Request condition
EC2	Limited: List	All resources	None
RDS	Limited: List	All resources	None
Route 53	Limited: List	All resources	None
S3	Limited: List	All resources	None

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

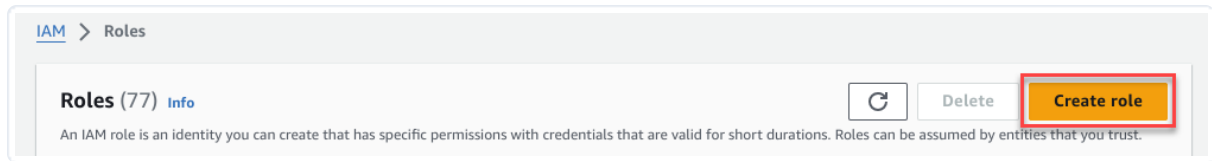
You can add up to 50 more tags.

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.

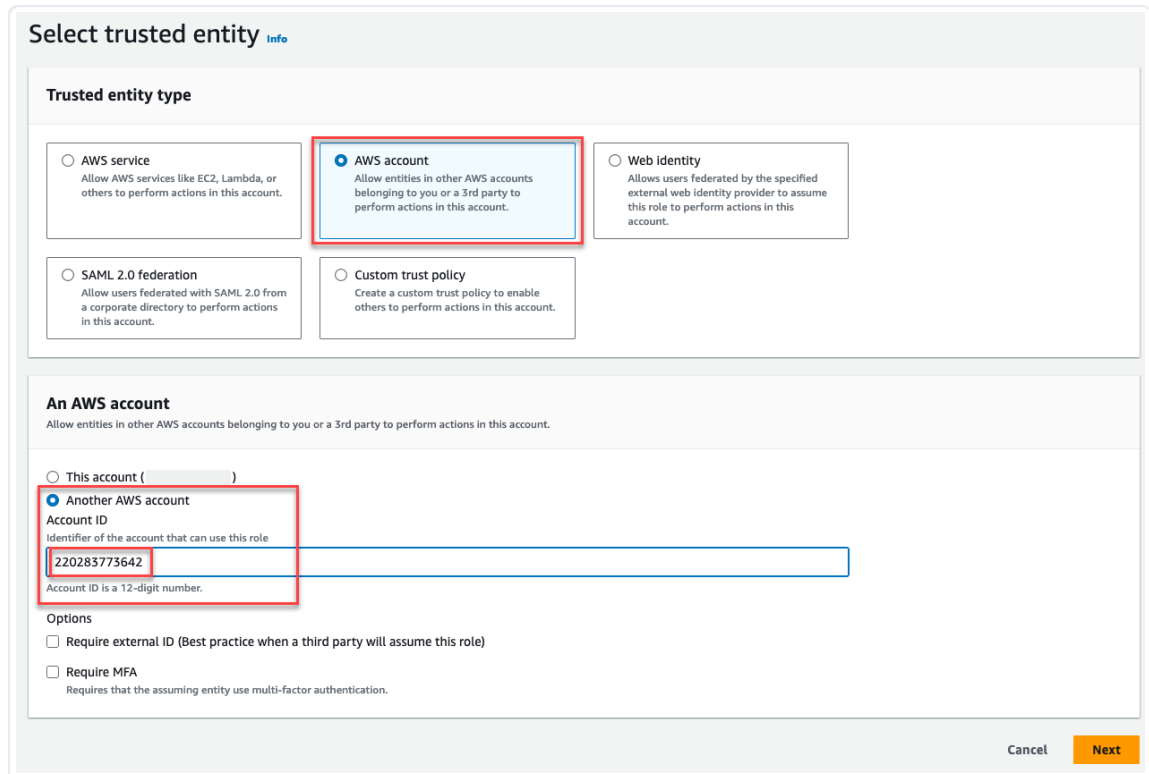
1. In the AWS console, browse to **Identity and Access Management (IAM)**.
2. Go to **Access Management > Roles**. Alternatively, access <https://us-east-1.console.aws.amazon.com/iam/home#/roles>.

3. Click **Create role**.



The screenshot shows the IAM Roles page. At the top, it says "IAM > Roles". Below that, there's a header "Roles (77) Info". On the right side, there are three buttons: "Refresh", "Delete", and "Create role". The "Create role" button is highlighted with a red box. Below the buttons, there's a note: "An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust."

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`.



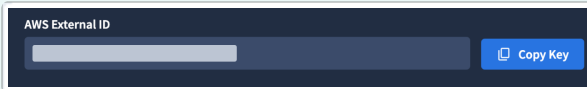
The screenshot shows the "Select trusted entity" page. Under "Trusted entity type", the "AWS account" option is selected and highlighted with a red box. Below that, under "An AWS account", the "Another AWS account" radio button is selected and highlighted with a red box. The "Account ID" field is also highlighted with a red box and contains the value "220283773642". Below the field, there are two options: "Require external ID (Best practice when a third party will assume this role)" and "Require MFA". The "Require external ID" checkbox is checked. At the bottom right, there are "Cancel" and "Next" buttons.

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.

- 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

Options

Require external ID (Best practice when a third party will assume this role)
 You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

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.

Add permissions Info

Permissions policies (1/894) Info

Choose one or more policies to attach to your new role.

Search: Filter by Type: 1 match

<input checked="" type="checkbox"/>	Policy name <small>↗</small>	Type	Description
<input checked="" type="checkbox"/>	mandiant_asm_integration	Customer managed	Policy for Mandiant ASM Integration

▶ **Set permissions boundary - optional**

Cancel Previous **Next**

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**.

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=, @, _' characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+=, @, _' characters.

Step 1: Select trusted entities Edit

Trust policy

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": "sts:AssumeRole",
7-       "Principal": {
8-         "AWS": "220283773642"
9-       },
10-      "Condition": {
11-        "StringEquals": {
12-          "sts:ExternalId": " "
13-        }
14-      }
15-    }
16-  ]
17- }
```

Step 2: Add permissions Edit

Permissions policy summary

Policy name ?	Type	Attached as
mandiant_asm_integration	Customer managed	Permissions policy

Step 3: Add tags

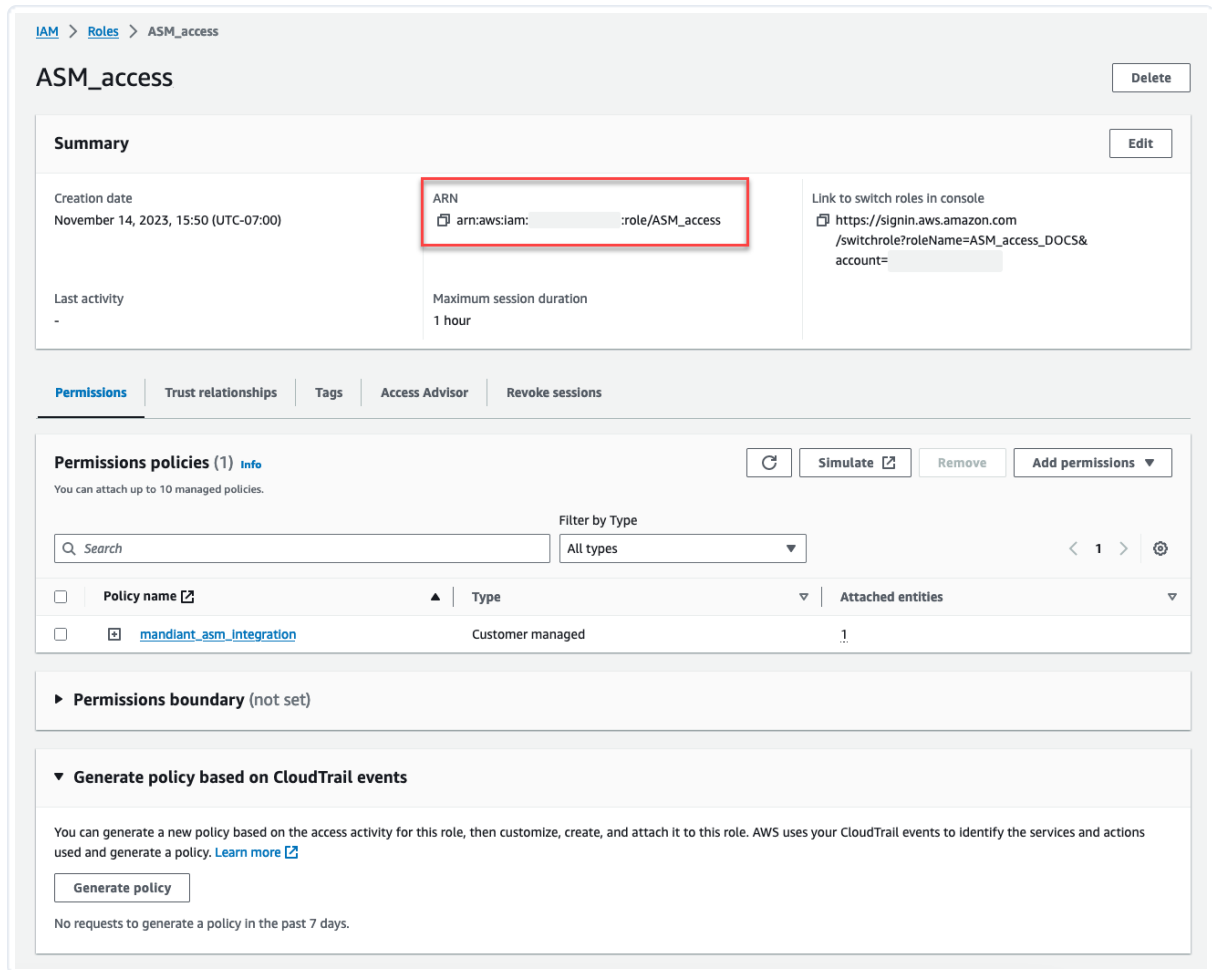
Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

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



IAM > Roles > ASM_access

ASM_access Delete

Summary Edit

Creation date
November 14, 2023, 15:50 (UTC-07:00)

ARN
`arn:aws:iam:::role/ASM_access`

Link to switch roles in console
`https://signin.aws.amazon.com/switchrole?roleName=ASM_access_DOCS&account=`

Last activity
-

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type
All types

Policy name	Type	Attached entities
mandiant_asm_integration	Customer managed	1

► **Permissions boundary** (not set)

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

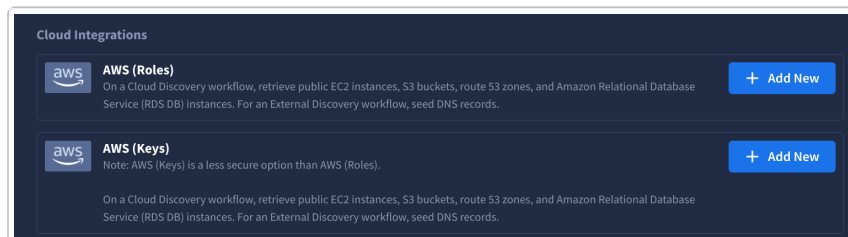
Generate policy

No requests to generate a policy in the past 7 days.

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)**




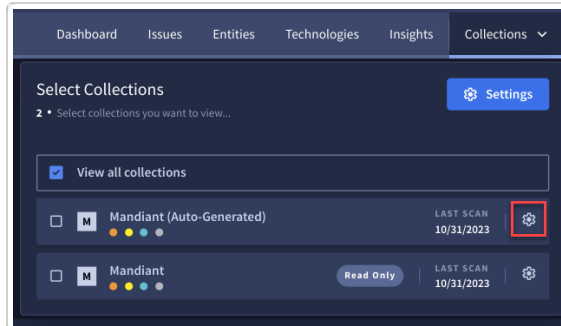
Cloud Integrations

AWS (Roles) + Add New
On a Cloud Discovery workflow, retrieve public EC2 instances, S3 buckets, route 53 zones, and Amazon Relational Database Service (RDS DB) instances. For an External Discovery workflow, seed DNS records.

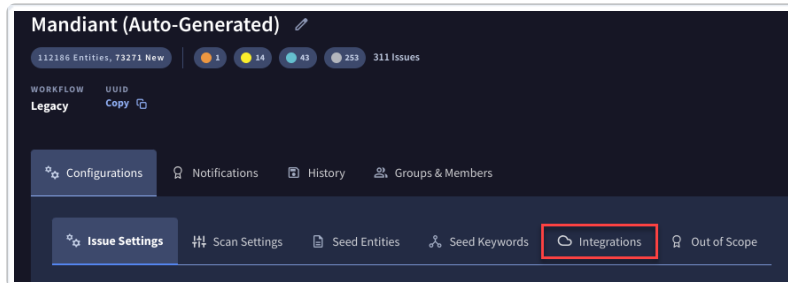
AWS (Keys) + Add New
Note: AWS (Keys) is a less secure option than AWS (Roles).
On a Cloud Discovery workflow, retrieve public EC2 instances, S3 buckets, route 53 zones, and Amazon Relational Database Service (RDS DB) instances. For an External Discovery workflow, seed DNS records.

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.

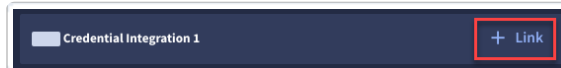
5. Click **Connect**.
6. Connect the integration to the appropriate Collection.
 - a. Click **Collections** and click  **Collection Settings** for the Collection that you want to connect the integration to.



- 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.

The screenshot displays the Mandiant interface for a workflow titled "Authenticated cloud discovery & assessment". At the top right, there are two buttons: "Connect Integration" and "Scan Collection", with the latter highlighted by a red rectangular border. Below the title, there are statistics: "32 Entities, 32 New" and "4 Issues". The workflow name is repeated below, with a "Copy" icon. A navigation bar includes "Configurations", "Notifications", and "History". A secondary navigation bar includes "Issue Settings", "Scan Settings", "Seed Entities", "Seed Keywords", "Integrations" (which is selected), and "Out of Scope". Below this is a table with columns for "Name", "Type", and "Created".

Name	Type	Created
Credential Integration 1		07/11/2023
Integration 1		07/12/2023
Credential Integration 1		07/11/2023