

# Amazon Security Lake Integration Guide

Amazon Security Lake lets users centralize security data to streamline threat detection and accelerate response by analyzing comprehensive data sets.

Because the GreyMatter platform is designed to be vendor neutral, you can connect GreyMatter with over 170 different sources, including Amazon Security Lake, to reduce the time it takes to investigate threats and perform hunts.

**Note: Note:** GreyMatter uses Amazon Athena to query Amazon Security Lake data for Investigate and Hunt actions in GreyMatter.

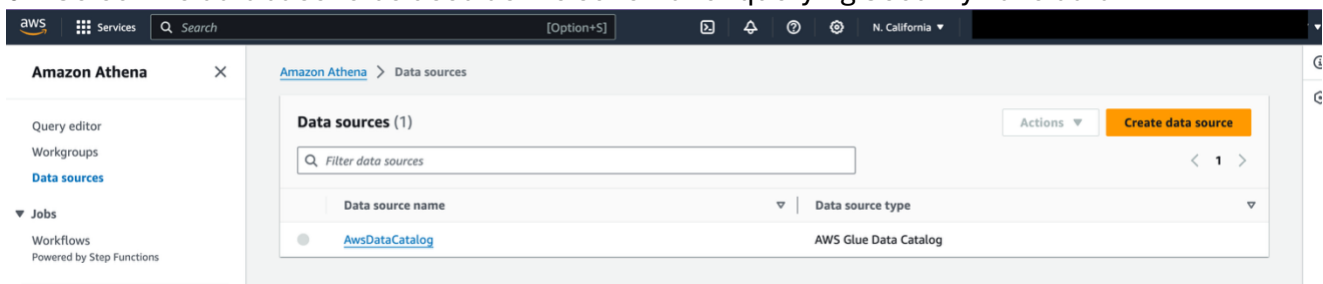
## Deployment Type

GreyMatter supports cloud deployments of Amazon Security Lake through **port 443**. If you already know your deployment method, continue to the next step. If you do not know what your Amazon Security Lake deployment method is, contact your internal Network or IT Infrastructure team to confirm.

## Required Information and Setup

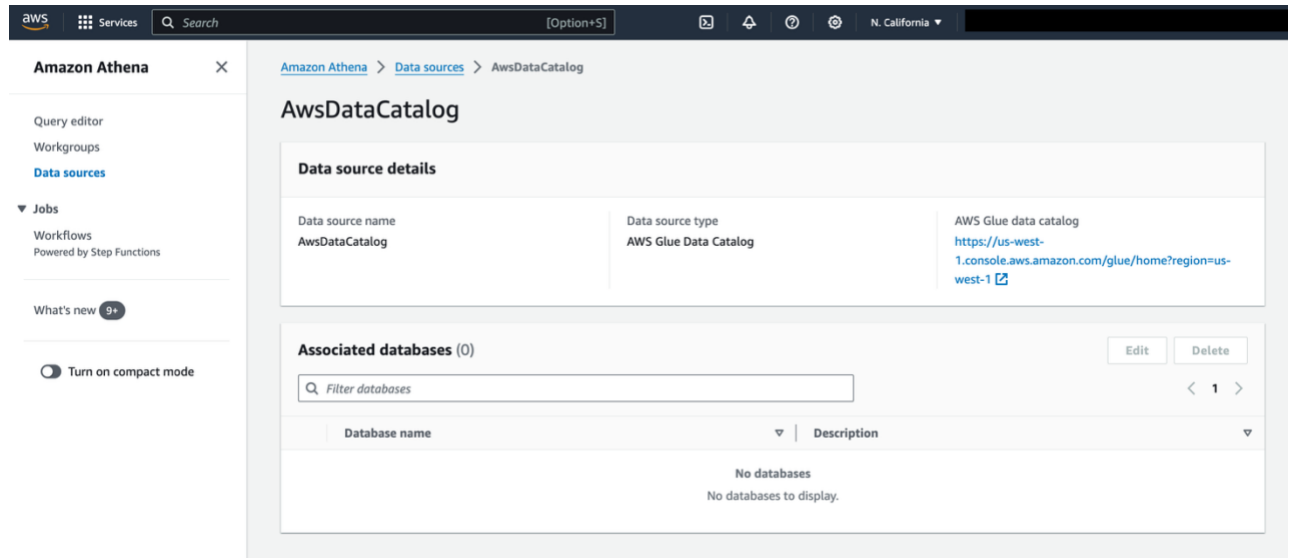
Follow the steps in this guide to collect the required details:

- **Region** (where your Security Lake is hosted)
- **Access Key ID**
- **Secret Access Key**
- **S3 Bucket**
  - Formated as S3://<bucket>
  - The S3 bucket for storing Security Lake data.
- **Database Name**
  - Group of tables
  - Navigate to Amazon Athena Data Sources in AWS
  - This data is the Data Source that holds the database containing Security Lake tables.
  - Select the database to be used as the schema for querying Security Lake data.



- **Catalog Name**
  - AWS Glue Data Catalog.
  - Navigate to Amazon Athena Data Sources in AWS.
  - This value is the Data Source that holds the database containing Security Lake tables.

# Amazon Security Lake Integration Guide



## Configure the required permission(s)

The following permissions are required for this integration. Using the instructions in the Create Policy section below, create a policy in AWS.

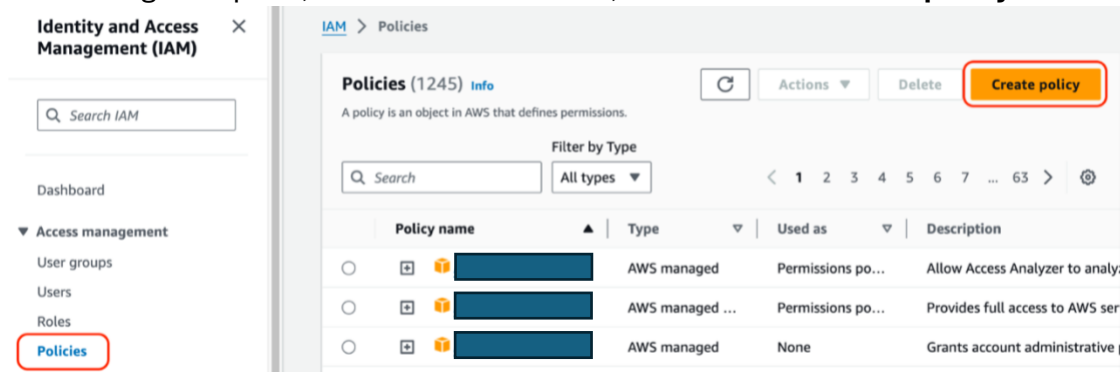
GreyMatter Capability	Action	API Authentication Permission(s)	Vendor Documentation
Investigate & Hunt	All actions	athena:StartQueryExecution athena:GetQueryExecution athena:GetQueryResults athena:StopQueryExecution s3:GetObject s3:ListBucket s3:GetBucketLocation s3:PutObject glue:GetTable glue:GetPartitions glue:GetDatabase	<a href="https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html">https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html</a>
Detection	All Actions	athena:StartQueryExecution athena:GetQueryExecution athena:GetQueryResults athena:StopQueryExecution s3:GetObject s3:ListBucket s3:GetBucketLocation s3:PutObject glue:GetTable glue:GetPartitions glue:GetDatabase	<a href="https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html">https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html</a>
Intel Push	All Actions	athena:StartQueryExecution athena:GetQueryResults athena:GetQueryExecution athena:GetWorkGroup	<a href="https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html">https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html</a>

# Amazon Security Lake Integration Guide

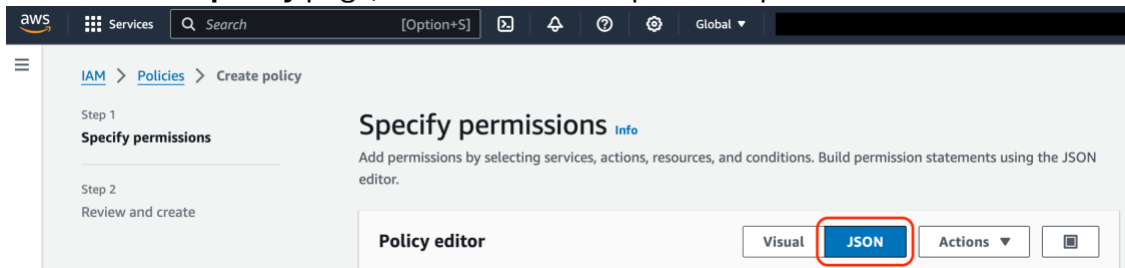
		athena:GetDataCatalog athena:GetTableMetadata athena:ListTableMetadata s3:ListBucket s3:GetBucketLocation s3:GetObject s3:PutObject glue:GetDatabase glue:CreateTable	
--	--	---	--

## Create a Policy

1. Navigate to the **Identity and Access Management (IAM)** console.
2. In the navigation pane, click the **Policies** link, then click the **Create policy** button.



3. On the **Create policy** page, select the **JSON** option to open the JSON editor.



4. Paste the following code snippet into the JSON editor **and fill in <resources> with values specific to your organization**:

```

1. {
2.   "Version": "2012-10-17",
3.   "Statement": [
4.     {
5.       "Sid": "VisualEditor0",
6.       "Effect": "Allow",
7.       "Action": [
8.         "s3:GetObject",
9.         "s3:PutObject"
10.      ],
11.      "Resource": [
12.        "<s3 arn>"
13.      ]
14.    },
15.    {
16.      "Sid": "Statement1",
17.      "Effect": "Allow",
18.      "Action": [
19.        "athena:StartQueryExecution",

```

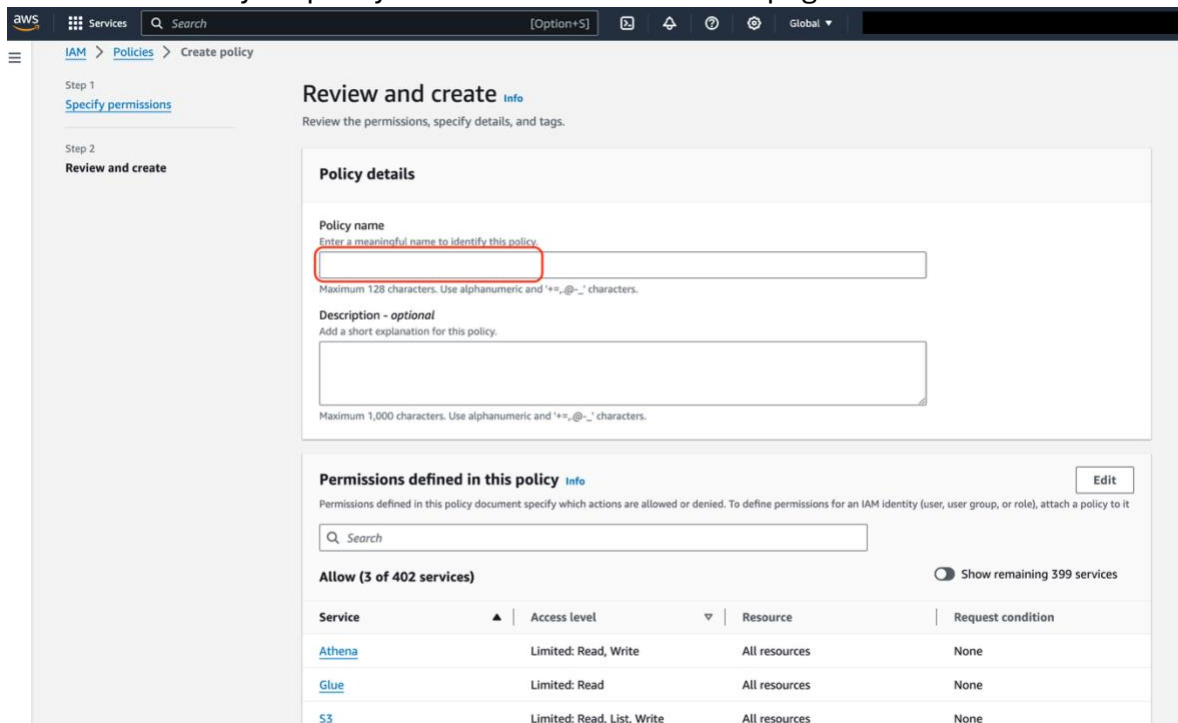
# Amazon Security Lake Integration Guide

```

20.         "athena:GetQueryResults",
21.         "athena:GetQueryExecution",
22.         "athena:StopQueryExecution",
23.         "athena:GetWorkGroup",
24.         "athena:GetDataCatalog",
25.         "athena:GetTableMetadata",
26.         "athena:ListTableMetadata"
27.     ],
28.     "Resource": [
29.         "*"
30.     ]
31. },
32. {
33.     "Sid": "GluePermissions",
34.     "Effect": "Allow",
35.     "Action": [
36.         "glue:GetTable",
37.         "glue:GetPartitions",
38.         "glue:CreateTable",
39.         "glue:GetDatabase"
40.     ],
41.     "Resource": [
42.         "*"
43.     ]
44. },
45. {
46.     "Sid": "Statement3",
47.     "Effect": "Allow",
48.     "Action": [
49.         "s3:ListBucket",
50.         "s3:GetObject",
51.         "s3:PutObject",
52.         "s3:GetObject",
53.         "s3:GetBucketLocation"
54.     ],
55.     "Resource": [
56.         "*"
57.     ]
58. }
59. ]
60. }

```

- Once you have modified the policy document using resources specific to your organization, click the **Review policy** button.
- Enter a name for your policy on the **Review and Create** page.



**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 (3 of 402 services)** [Show remaining 399 services](#)

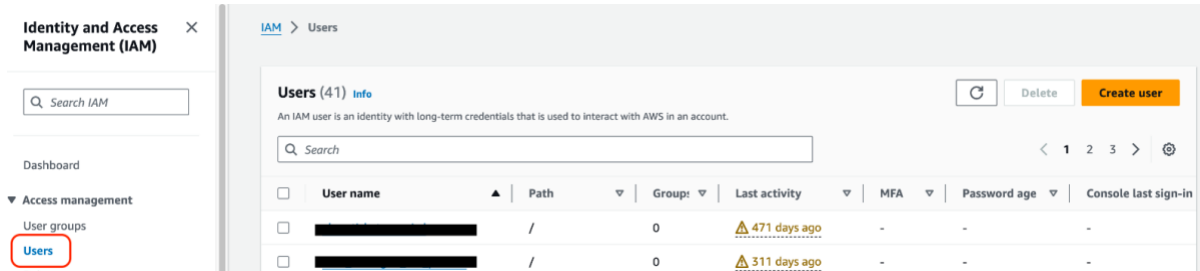
Service	Access level	Resource	Request condition
<a href="#">Athena</a>	Limited: Read, Write	All resources	None
<a href="#">Glue</a>	Limited: Read	All resources	None
<a href="#">S3</a>	Limited: Read, List, Write	All resources	None

# Amazon Security Lake Integration Guide

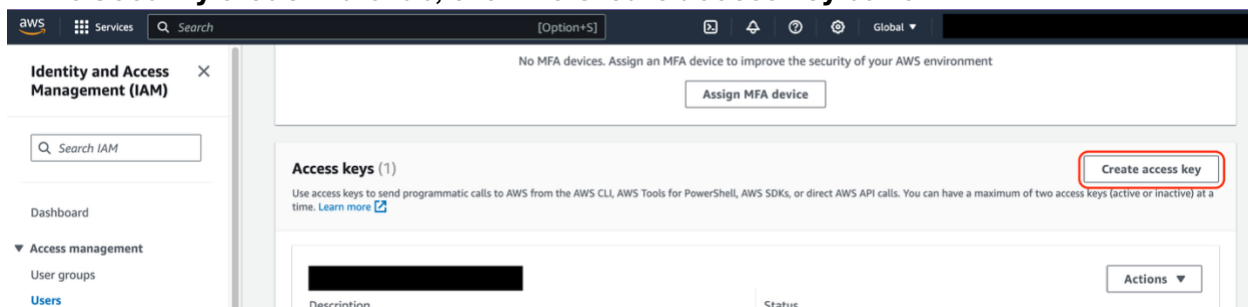
- Click the **Create Policy** button.

## Apply an Access Key to the New Policy

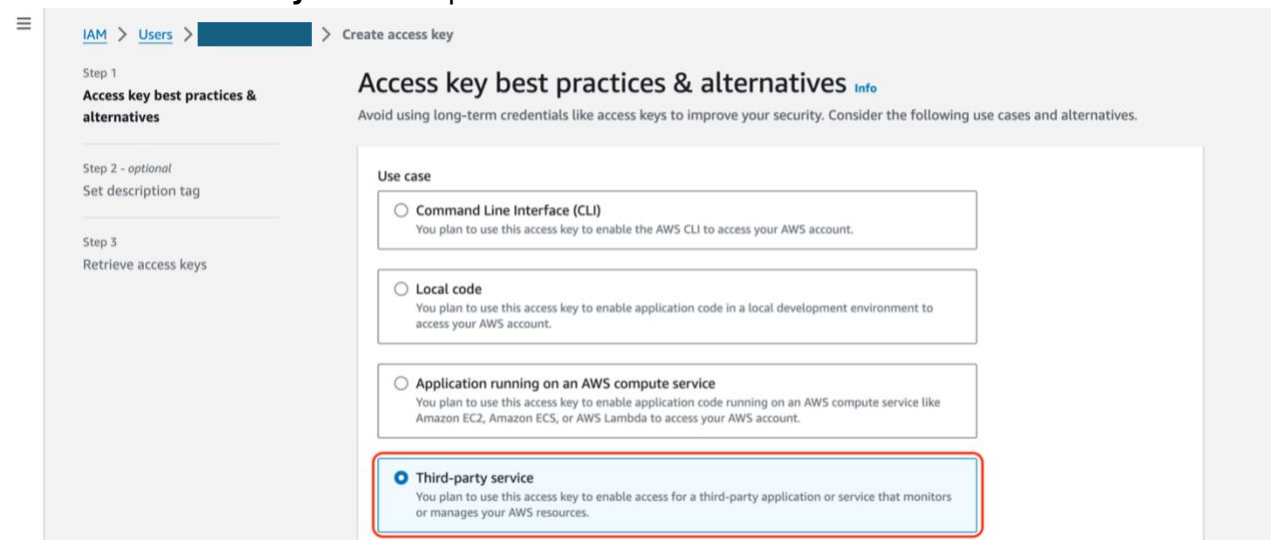
- In the Identity and Access Management (IAM) console, click the **Users** link in the navigation pane.



- Select the user or user group to whom you want to attach the policy.
  - Create a new user or user group if you don't have a GreyMatter specific user or group already.
- In the **Security credentials** tab, click the **Create access key** button.

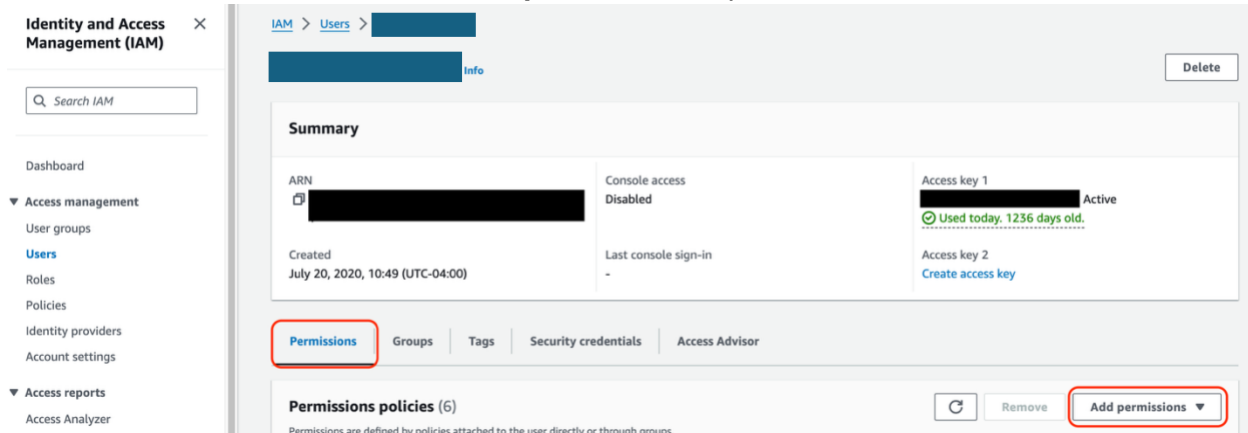


- A pop-up window will appear displaying the new access key. Copy and store the Access Key ID and Secret Access Key in a secure place. You will need to provide these values to your Implementation Specialist or Customer Success Manager (CSM) later during the setup process.
- Select the **Third Party Service** option.

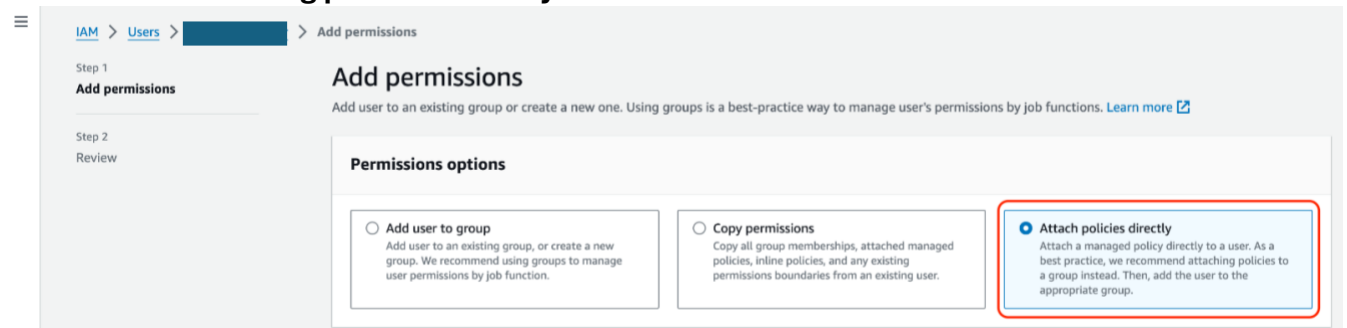


# Amazon Security Lake Integration Guide

6. In the **Permissions** tab, click the **Add permissions** option.

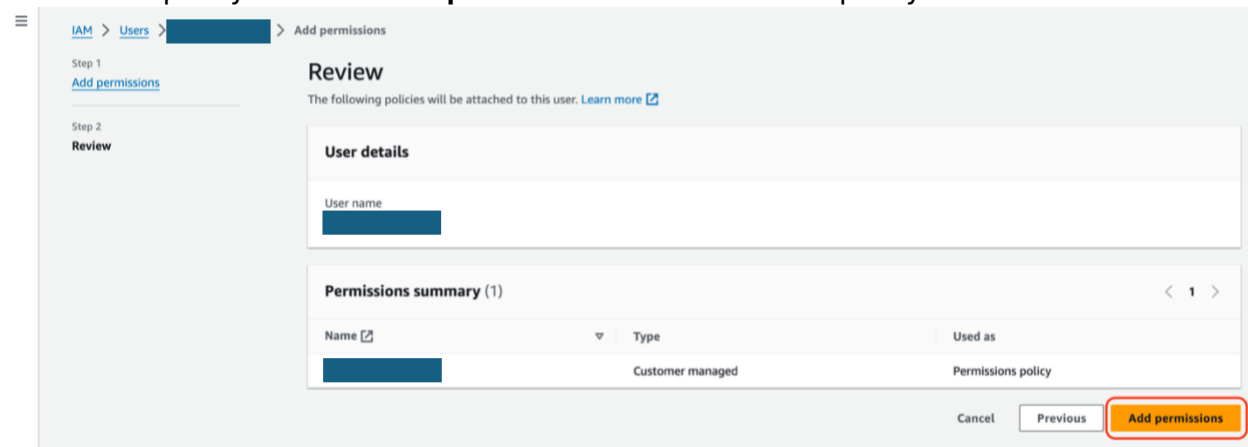


7. Select **Attach existing policies directly**.



8. Select the policy named **GreyMatter - Security Lake Integration**.

9. Review the policy and click **Add permissions** and attach the policy to the user.



Your Implementation Specialist or CSM will provide a secure method for sharing these pieces of information with ReliaQuest. Once you've sent the details, our team will complete the setup tasks. You will be notified if ReliaQuest requires any additional information or needs to perform additional validation steps.

**Disclaimer:** All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.