

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:

- **AWS Access Key (Required) ***
 - AWS Access Key required to authenticate with the AWS API
 - **NOTE: This is not required if you are setting this up with Role ARN and External ID**
- **AWS Secret Access Key (Secret) (Required) ***
 - AWS Secret Access Key required to authenticate with the AWS API
 - **NOTE: This is not required if you are setting this up with Role ARN and External ID**
- **Athena Query Results S3 (String | S3 URL) (Required)**
 - S3 URL where Athena query results will be stored.
- **Database (String) (Required)**
 - Database automatically generated by Security Lake
- **Catalog (String) (Required)**
 - AWS Glue Data Catalog Name. This can be found under Athena > Administrations > Data sources catalogs. Default is AWSDataCatalog.
- **Region (String) (Required)**
 - AWS Security Rollup region or desired region where Security Lake Athena tables exist.
- **ReliaQuest Threat Intel S3 Bucket (String | S3 URL) (Optional)**
 - S3 URL to bucket which can store ReliaQuest curated IOCs.
 - **NOTE: This is used by the intel push feature. If you do not want to enable this feature, please enter N/A into the text box and ensure the Intel Push toggle remains unchecked.**
- **Role ARN (Optional) ***
 - AWS ARN of the Role created to be assumed with the GreyMatter AWS Account.

Amazon Security Lake Integration Guide

- **External ID (Optional) ***
 - An External ID set in the trust policy and to be used by the GreyMatter AWS Service Account to ensure a successful and secure authentication.
 - **NOTE: Please generate a UUID here: [CyberChef](#)** to be used as an External ID.

Note: Role ARN and External ID are the preferred method of authentication as it follows AWS best practices. An AWS GM Service Account will assume the predefined role and interact with the resources defined in the role permissions.

Obtain Authentication Variables

AWS Permission Policy Setup

Additional Variables	Steps to Retrieve ARN
Catalog	arn:aws:glue:{rollup_region}:{account-id}:catalog For example: arn:aws:glue:us-east-1:123456789012:catalog
Database	Ensure you are in the proper rollup region <ol style="list-style-type: none"> 1. Navigate to AWS Glue 2. Under Data Catalog select Databases 3. Select the table name with the format: amazon_security_lake_glue_db_{region} arn:aws:glue:{rollup_region}:{account-id}:database/{database_name from Step 3 above} For example: arn:aws:glue:us-east-1:123456789012:database/amazon_security_lake_glue_db_us_east_1
Table	arn:aws:glue:{rollup_region}:{account-id}:table/{database_name from above}/* For example: arn:aws:glue:us-east-1:123456789012:table/default/*

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" "athena:ListTableMetadata"	https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Amazon Security Lake Integration Guide

		"athena:GetTableMetadata" "athena:GetDataCatalog" "athena:GetWorkGroup" "s3:GetObject" "s3:ListBucket" "s3:GetBucketLocation" "s3:PutObject" "glue:GetTable" "glue:GetPartition" "glue:GetPartitions" "glue:GetDatabase" "glue:GetDatabases"	
Detection	All Actions	"athena:StartQueryExecution" "athena:GetQueryExecution" "athena:GetQueryResults" "athena:StopQueryExecution" "athena:ListTableMetadata" "athena:GetTableMetadata" "athena:GetDataCatalog" "athena:GetWorkGroup" "s3:GetObject" "s3:ListBucket" "s3:GetBucketLocation" "s3:PutObject" "glue:GetTable" "glue:GetPartition" "glue:GetPartitions" "glue:GetDatabase" "glue:GetDatabases"	https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
Intel Push	All Actions	"athena:StartQueryExecution" "athena:GetQueryExecution" "athena:GetQueryResults" "athena:StopQueryExecution" "athena:ListTableMetadata" "athena:GetTableMetadata" "athena:GetDataCatalog" "athena:GetWorkGroup" "s3:GetObject" "s3:ListBucket" "s3:GetBucketLocation" "s3:PutObject" "glue:GetTable" "glue:CreateTable" "glue:GetPartition" "glue:GetPartitions" "glue:GetDatabase" "glue:GetDatabases"	https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
Test Connection	Test Connection	"athena:StartQueryExecution" "athena:GetQueryExecution" "athena:GetQueryResults" "athena:StopQueryExecution" "athena:ListTableMetadata" "athena:GetTableMetadata" "athena:GetDataCatalog"	https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Amazon Security Lake Integration Guide

	"athena:GetWorkGroup" "s3:GetObject" "s3:ListBucket" "s3:GetBucketLocation" "s3:PutObject" "glue:GetTable" "glue:GetPartition" "glue:GetPartitions" "glue:GetDatabase" "glue:GetDatabases"	
--	---	--

Create a Policy

1. **Navigate** to the AWS console.
2. In the **Search Bar** type **IAM** to navigate to the IAM section.
3. Navigate to the IAM Menu by **Clicking** on the ☰ icon.
4. Under **Access Management** select **Policies**.
5. In the top left **click** the **Create policy** button.
6. For **Policy editor** select **JSON** to open the json editor.

Amazon Security Lake Integration Guide

7. Replace the starter json with this template:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AthenaPermissions",
      "Action": [
        "athena:StartQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StopQueryExecution",
        "athena:ListTableMetadata",
        "athena:GetTableMetadata",
        "athena:GetDataCatalog",
        "athena:GetWorkGroup"
      ],
      "Resource": [
        "{Workgroup ARN from Configuration Dependencies > Athena Config Step 6 of this document}",
        "arn:aws:athena:{rollup region}:{customer AWS Account ID}:datacatalog/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "S3Permissions",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "{Athena Query Result S3 ARN from Configuration Dependencies > Athena Config Step 7}",
        "{Athena Query Result S3 ARN from Configuration Dependencies > Athena Config Step 7}/*",
        "{OPTIONAL: ReliaQuest Threat Intel S3 ARN}",
        "{OPTIONAL: ReliaQuest Threat Intel S3 ARN}/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "GluePermissions",
      "Action": [
        "glue:CreateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource": [
        "{Catlog ARN from the start of this section}",
        "{Database ARN from the start of this section}",
        "{Table ARN from the start of this section}"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "LakeformationPermissions",
      "Effect": "Allow",
      "Action": [
        "lakeformation:ListResources",
        "lakeformation:GetDataAccess"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

8. Click **Next** at the bottom of the page.
9. Under Policy details set a meaningful **Policy name**. For example, **GreyMatter-SecurityLake-AccessPolicy**.
10. Click **Create policy** to create the policy.

Note: "glue:CreateTable" Is specifically for the Intel Push Feature. If you do not wish to use this feature you may remove the permission from the IAM Policy Statement.

Amazon Security Lake Integration Guide

AWS Access Key + Secret Key Authentication

Ensure you are on the AWS Security Lake Delegated Account

1. **Navigate** to the AWS console.
2. In the **Search Bar** type **IAM** to navigate to the IAM section.
3. Navigate to the IAM Menu by **Clicking** on ☰ icon.
4. Under **Access Management** select **Users**.
5. Click into the User created in the **IAM User Config** section.
6. Navigate to the **Security credentials** tab.
7. Scroll down to the **Access keys** section.
8. Click on the **Create access key** button.
9. Under Use case select **Third-party service**.
10. **Ensure** the Confirmation is checked .
11. Click **Next**
12. Click the **Create Access Key** button.
13. **Copy** and **Note** the **Access Key** and **Secret access key**.

AWS Assume Role

Ensure you are on the AWS Security Lake Delegated Account

AWS Role Setup

1. **Navigate** to the AWS console.
2. In the **Search Bar** type **IAM** to navigate to the IAM section.
3. Navigate to the IAM Menu by **Clicking** on ☰ icon.
4. Under **Access Management** select **Roles**.
5. Click **Create Role**.
6. For Trusted entity type select **AWS account**.
7. Under the AWS Account Section ensure “**Another AWS account**” is selected.
8. Enter the GM Service Account ID
 - a. Please request the GM Service Account ID from the ReliaQuest team.
9. Under the subsection **Options** ensure the **Require external ID (Best practice when a third party will assume this role)** is checked.
10. Enter an External ID.
 - a. **Please generate a UUID here: [CyberChef](#)** to be used as an External ID.
11. Click **Next**.
12. Select the Permission Policy created above in the **AWS Permission Policy Setup** section to attach to this role by checking the box.
13. Click **Next**.
14. Enter a meaningful name for the Role.
15. Review and Click **Create role**.

Amazon Security Lake Integration Guide

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.