

# AWS Cloud Integration Guide

The connection between GreyMatter and AWS cloud allows you to get visibility into your AWS ecosystem by interacting with individual AWS services to ensure an up-to-date inventory is kept for all accounts across all regions.

## Deployment Type

This integration supports **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please check your organization's compatibility before continuing.

## Required Information and Setup

To integrate GreyMatter with AWS Cloud, collect the following details:

- Root AWS Role ARN
  - The ARN of the root or delegated account that has permission to all child accounts in an organization.
  - If the AWS environment is not set up in your organization structure, you need to create an integration for each account you're tracking.
- External ID
  - Used for all roles.
- Org Wid AWS Role Name (optional)
  - Role name all child accounts have access to.

See instructions below to gather the required information.

### Create Role with External ID

1. Search for and select **IAM** in the AWS console.
2. Click the IAM **Menu** icon.
3. Select **Roles** under Access Management.
4. Click **Create Role**.
5. Select **AWS Account** for Trusted entity type.
6. Make sure **Another AWS account** is selected under the AWS Account section
7. Enter the GreyMatter Service Account ID.
  - Request the ID from the ReliaQuest team.
8. Make sure **Require external ID (Best practice when a third party will assume this role is checked** under the Options subsection.
9. Generate a **UUID** on **CyberChef**.
10. Enter the generated UUID as the **External ID**.
11. Click **Next**.
12. Check the box for the Permission Policy created for the GreyMatter connection.
13. Click **Next**.

# AWS Cloud Integration Guide

14. Enter a meaningful name for the role.
15. Review and click **Create Role**.

## Permissions and Functionality

### Permissions

GreyMatter Capability	Required Permission
Asset Inventory	<p><b>EC2</b></p> <ul style="list-style-type: none"> <li>ec2:Describe*</li> <li>ec2:GetSecurityGroupsForVpc</li> <li>ec2:GetLaunchTemplateData</li> <li>elasticloadbalancing:Describe*</li> <li>cloudwatch:ListMetrics</li> <li>cloudwatch:GetMetricStatistics</li> <li>cloudwatch:Describe*</li> <li>autoscaling:Describe*</li> </ul> <p><b>S3 Buckets</b></p> <ul style="list-style-type: none"> <li>s3:Get*</li> <li>s3:List*</li> <li>s3:Describe*</li> <li>s3-object-lambda:Get*</li> <li>s3-object-lambda:List*</li> </ul> <p><b>IAM</b></p> <ul style="list-style-type: none"> <li>iam:GenerateCredentialReport</li> <li>iam:GenerateServiceLastAccessedDetails</li> <li>iam:Get</li> <li>iam:List*</li> <li>iam:SimulateCustomPolicy</li> <li>iam:SimulatePrincipalPolicy</li> </ul>

### Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with AWS Cloud, providing real-time insights into what assets you own, their status, and potential risks.

**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.