AQUILA CSPM - AWS Integration

Overview

This page explains how to get started monitoring the security posture of your cloud assets using the Cloud Security Posture Management (CSPM) feature.

Set up cloud account access

The CSPM integration requires access to AWS's built-in `SecurityAudit` IAM policy in order to discover and evaluate resources in your cloud account. To provide access we need:

- **IAM Role**
- **Direct access keys**

Create IAM User

Follow AWS's IAM roles for Amazon EC2 documentation to create an IAM role using the IAM console, which automatically generates an instance profile.

1. Create an IAM role:
    1. In AWS, go to your IAM dashboard. Click **Roles**, then **Create role**.
    2. On the **Select trusted entity** page, under **Trusted entity type**, select **AWS service**.
    3. Under **Use case**, select **EC2**. Click **Next**.
    The Select trusted entity screen in AWS
    4. On the **Add permissions** page, search for and select `SecurityAudit`. Click **Next**.
    The Add permissions screen in AWS
    5. On the **Name, review, and create** page, name your role, then click **Create role**.

2. Attach your new IAM role to an EC2 instance:
    1. In AWS, select an EC2 instance.
    2. Select **Actions > Security > Modify IAM role**.
    The EC2 page in AWS
    3. On the **Modify IAM role** page, search for and select your new IAM role.

4. Click **Update IAM role**.

Create Direct access keys

Access keys are long-term credentials for an IAM user or AWS account root user. To use access keys as credentials, you must provide the `Access key ID` and the `Secret Access Key`. After you provide credentials, finish manual setup.

For more details, refer to Access Keys and Secret Access Keys.

- `Access key ID`: The first part of the access key.
- `Secret Access Key`: The second part of the access key.

source: https://www.elastic.co/guide/en/security/current/cspm-get-started.html

> **Please provide the following information to CyTech Support:**

- **Access key ID**
- **Secret Access Key**

How to integrate to AQUILA CSPM Module

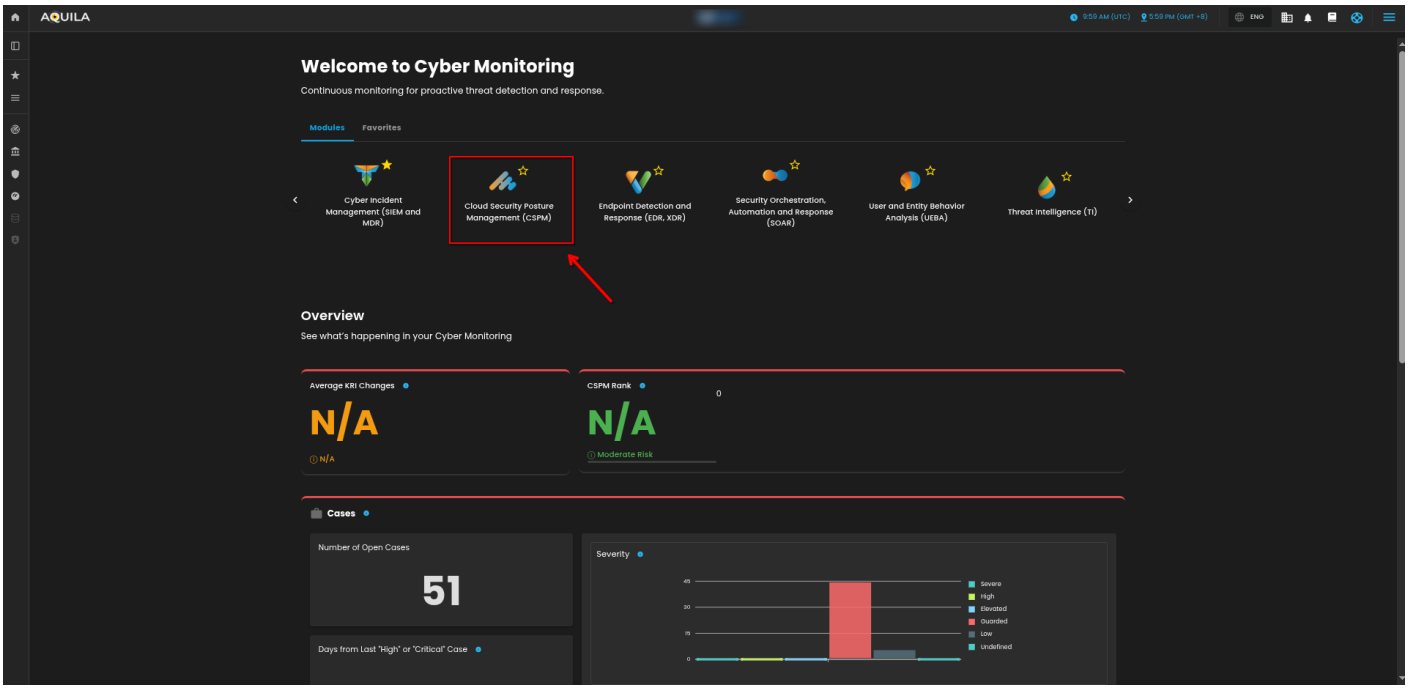
Pre-requisites

1. **Access to CyTech - AQUILA**
   - Only users assigned the **"Owner"** or **"Admin"** role can access the Log Collector installation resources within the platform.

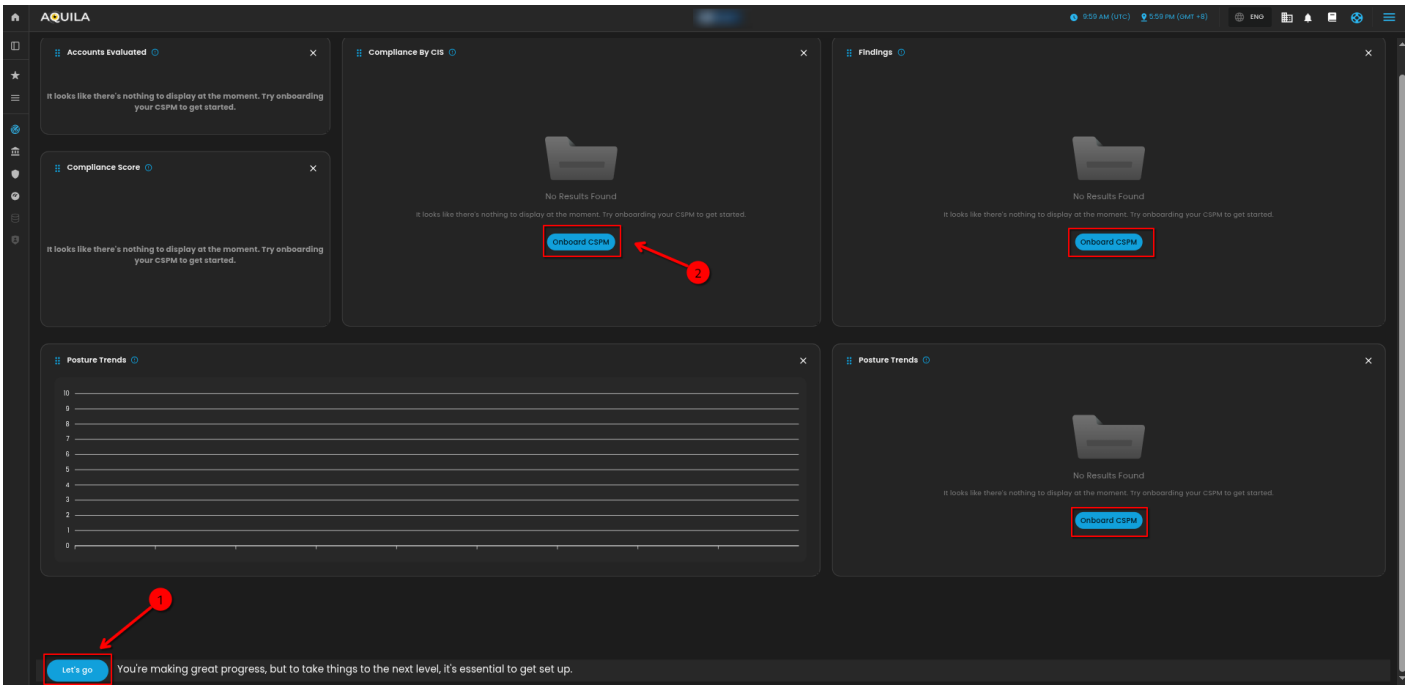
> **To navigate to CSPM Module please follow the instructions below:**

Step 1: Log in to CyTech - AQUILA. Click here --> AQUILACYBER.ai
Step 2: Click on Cyber Monitoring.

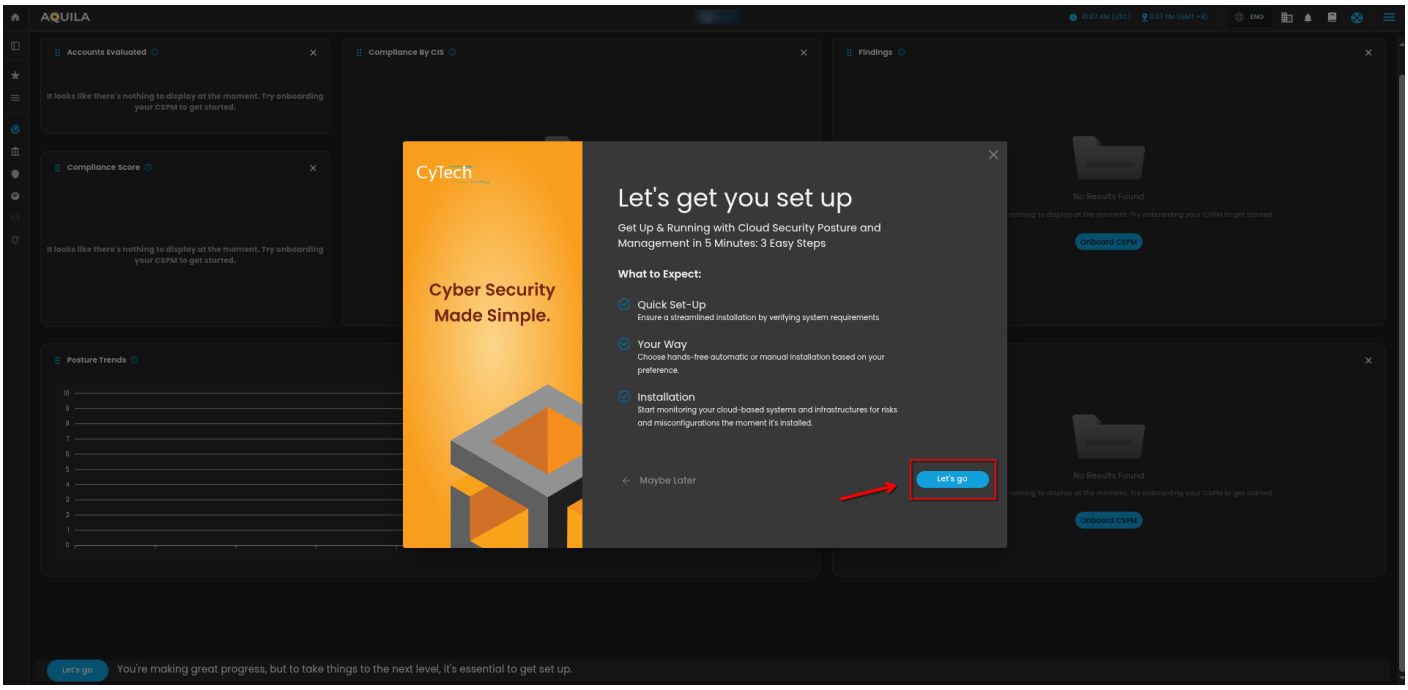
Step 3: Choose Cloud Security Posture Management (CSPM).



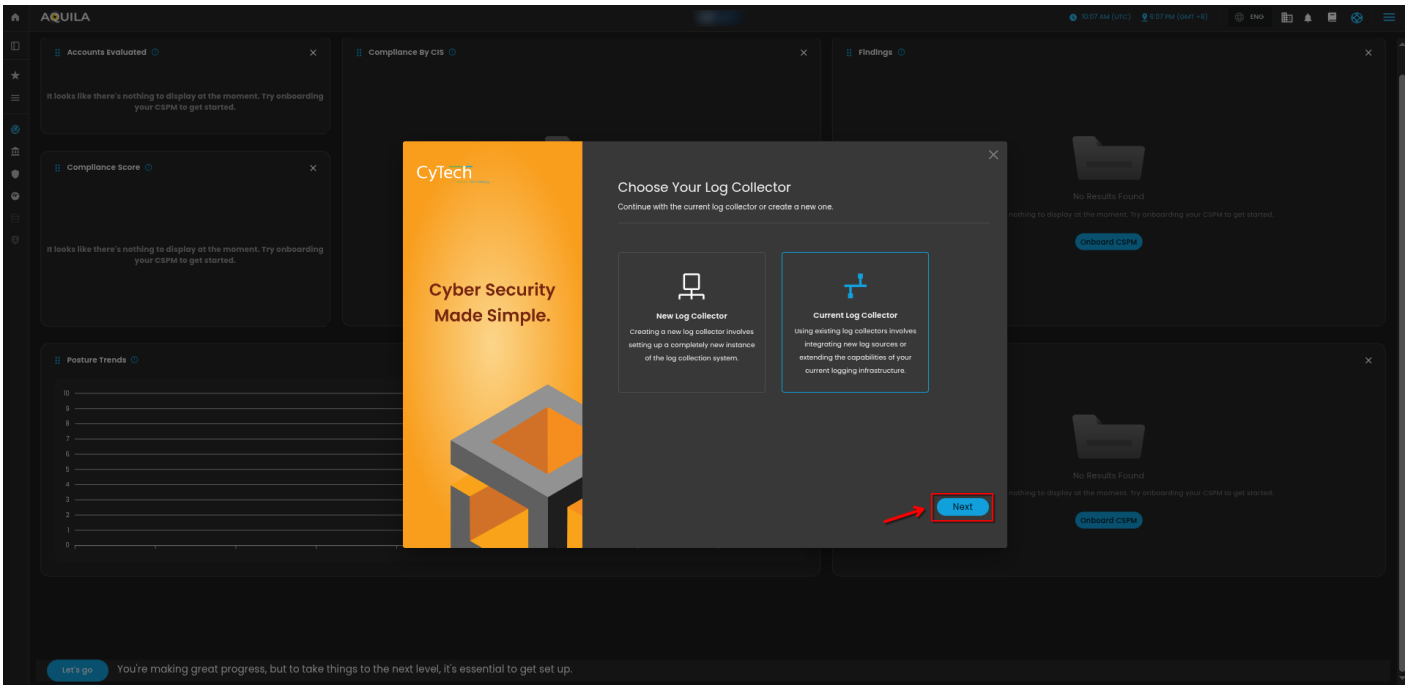
Step 4: Click the "Let's Go" or "Onboard CSPM" icon to launch installation window.



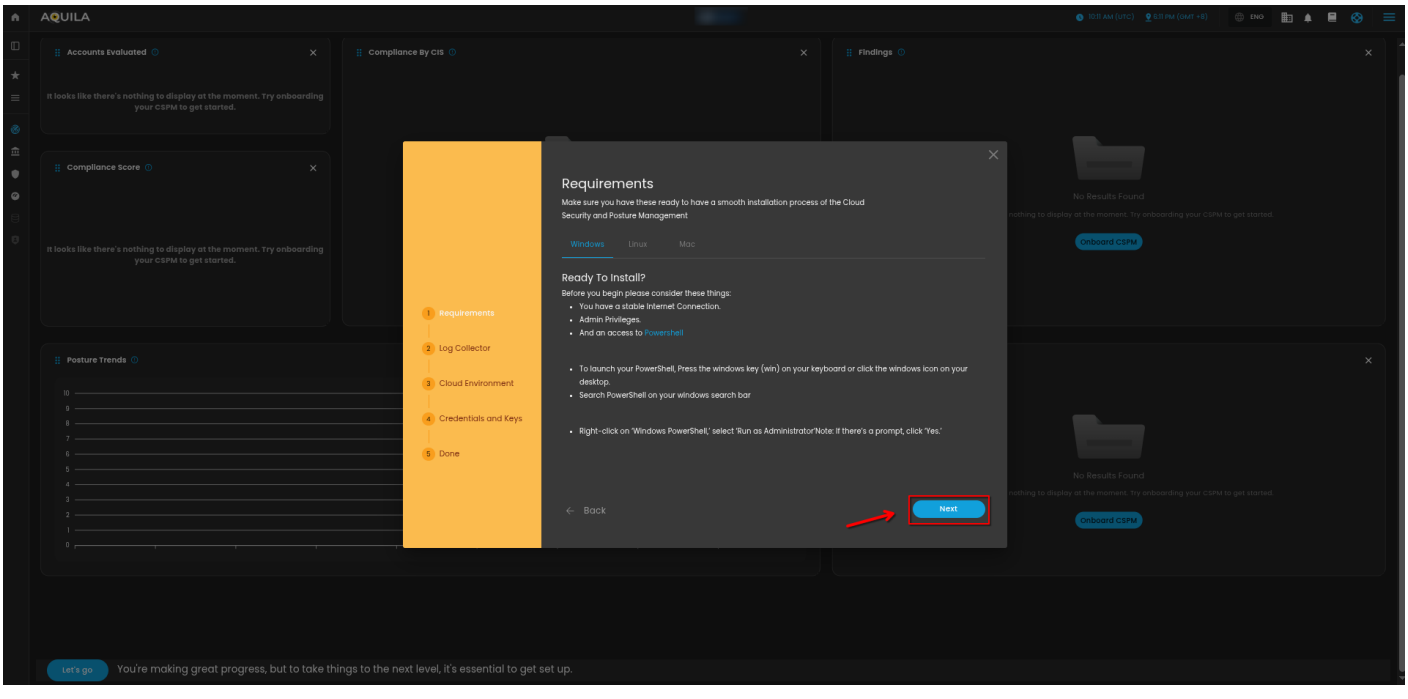
Step 5: Click "Let's go" to start the integration process.



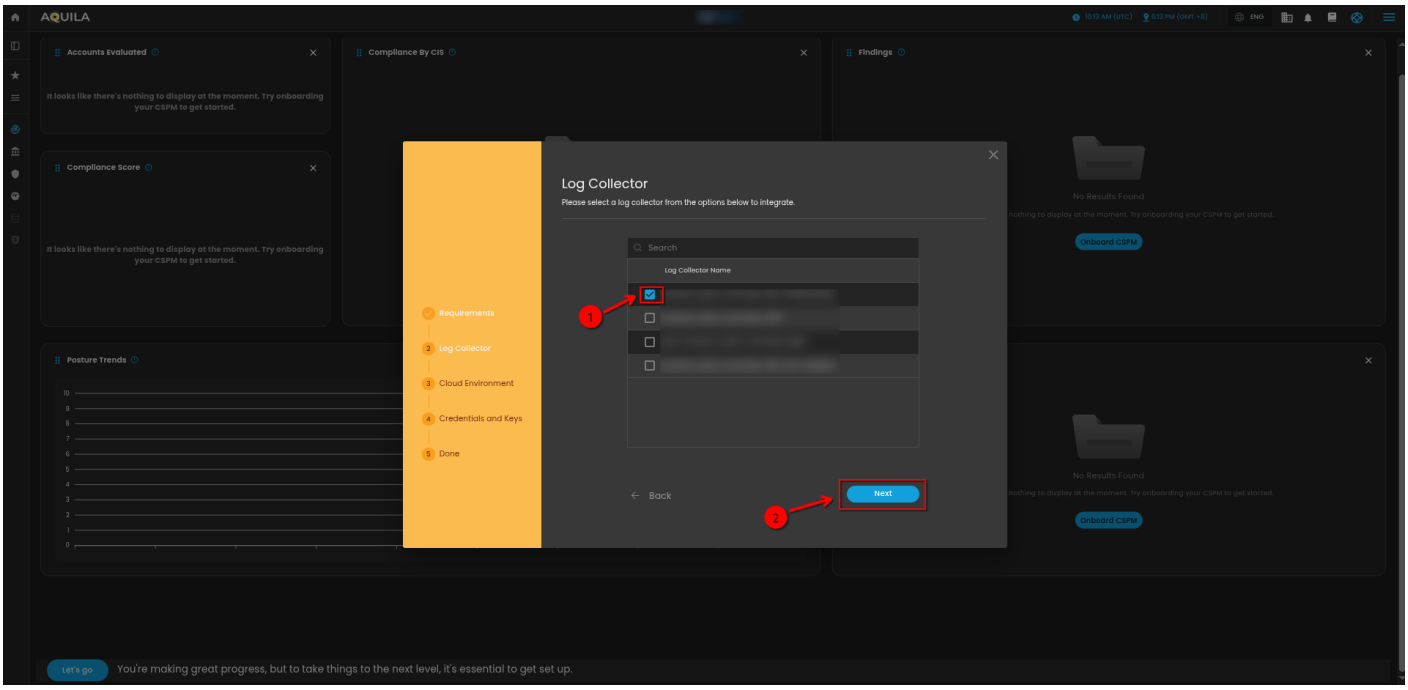
Step 6: Choose your log collector. If you haven't installed a log collector yet choose "New Log Collector" click here --> Log Collector Installation. If you have already have an existing log collector choose "Current Log Collector" and click "Next".



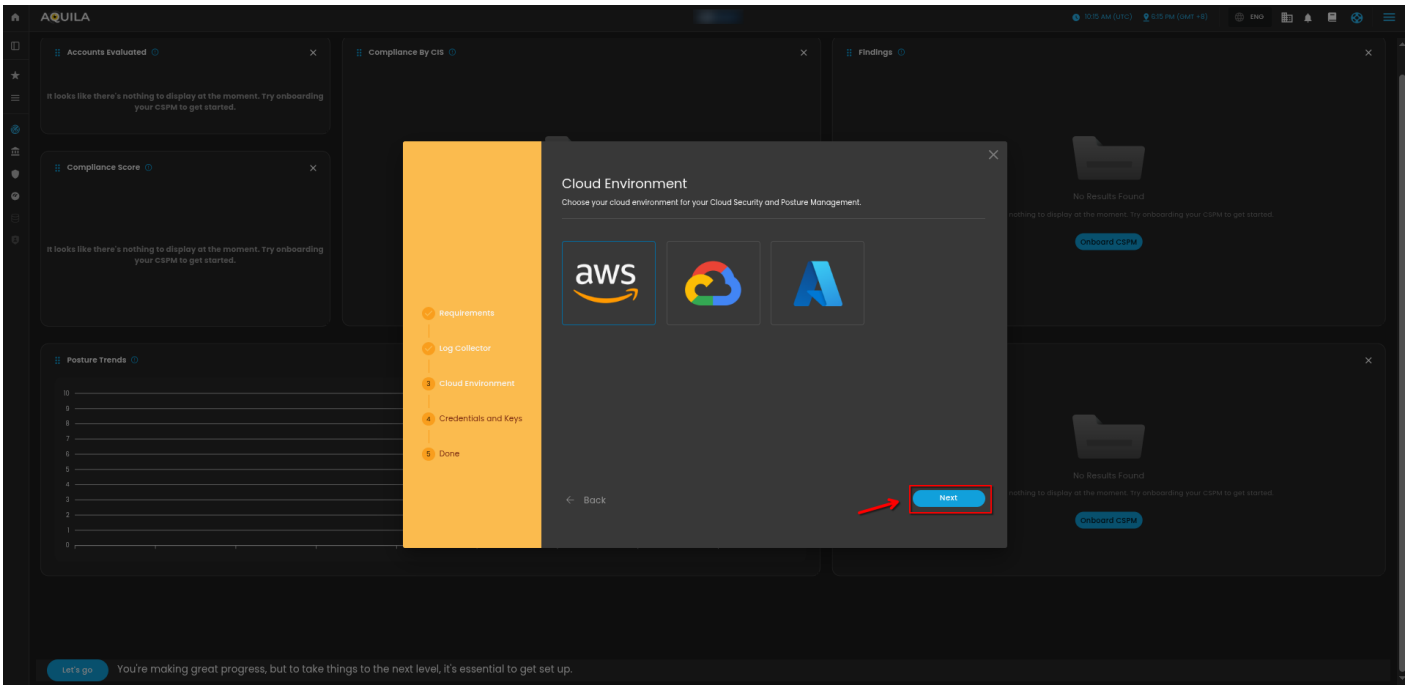
Step 7: Click "Next" if the requirements are met.



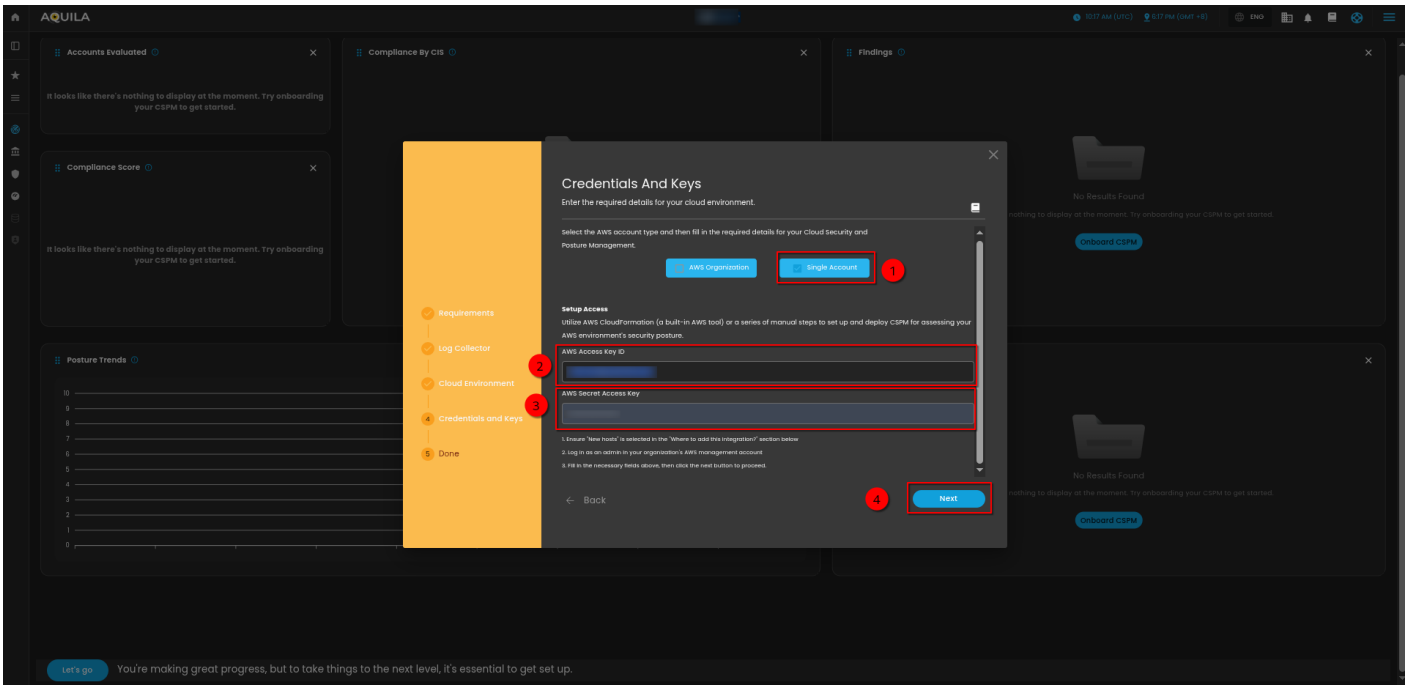
Step 8: Choose your current log collector. This will collect the logs coming from your log sources.



Step 9: Choose Amazon Web Services and click "Next" to proceed.



Step 10: Input all the required credentials from the previous AWS configurations and click "Next" to initiate the integration process. Wait for couple of minutes until a success window shows up.



Please refer to this manual for the full guidelines of our CSPM Module. *click here--> CyTech - AQUILA CSPM Manual*

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #2
Created 14 April 2025 05:45:06 by Richmond Abella
Updated 26 June 2025 11:51:02 by Richmond Abella