

NG SIEM - Azure CSPM Integration

This manual explains how to get started monitoring the security posture of your Azure CSP using the Cloud Security Posture Management (CSPM) feature.

Requirements

- The user who gives the CSPM integration permissions in Azure must be an Azure subscription **admin**.

Setup

Service principal with client secret

Before using this method, you must have set up a **Microsoft Entra application** and **service principal that can access resources**. Please go [here](#) before following the steps below.

1. The following information is required.
 1. Directory (**tenant**) ID and **Application (client) ID**
 - To get these values:
 - Go to the **Registered apps** section of Microsoft Entra ID.
 - Click on **New Registration**, name your app and click **Register**.
 - Copy your new app's **Directory (tenant) ID** and **Application (client) ID**.
 2. **Client Secret**
 - In Azure portal, select **Certificates & secrets**, then go to the **Client secrets** tab. Click **New client secret**.
 - Copy the new secret.
2. Return to Azure. Go to your Azure subscription list and select the subscription or management group you want to monitor with CSPM.
3. Go to **Access control (IAM)** and select **Add Role Assignment**.
4. Select the **Reader** function role, assign access to **User, group, or service principal**, and select your new app.

Please save and provide these values to AQUILA Support Team.

1. **Directory (tenant) ID**
2. **Application (client) ID**
3. **Client Secret Value:**

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

Revision #5

Created 23 September 2025 08:07:27 by Richmond Abella

Updated 3 October 2025 12:39:13 by Richmond Abella