AQUILA - Microsoft Defender for Endpoint

Overview

This guide walks through the full process of integrating Microsoft Defender for Endpoint (MDE) to centralize security telemetry, enrich alerts, and enable unified threat hunting across your environment.

This integration is for Microsoft Defender for Endpoint logs.

Microsoft Defender for Endpoint integration collects data for Alert, Machine, Machine Action, and Vulnerability logs using REST API.

This integration collects the following logs:

- Alert - Retrieves alerts generated by Microsoft Defender for Endpoint.
- Machine - Retrieves machines that have communicated with Microsoft Defender for Endpoint.
- Machine Action - Retrieves logs of actions carried out on machines.
- Vulnerability - Retrieves logs of Vulnerability.

Prerequisites

Before you begin, ensure the following are in place:

- An active Microsoft Defender for Endpoint license (Plan 1 or Plan 2, or Microsoft 365 Defender)
- Access to the Microsoft Entra ID (formerly Azure AD) portal to register an application
- Permissions to grant API permissions within your tenant (typically a Global Administrator or Security Administrator role)

Azure App Registration

This integration authenticates to the MDE API using OAuth 2.0 client credentials. You need to register an application in Microsoft Entra ID and grant it the appropriate API permissions.

Step 1: Register a New Application

- Navigate to **portal.azure.com** and sign in with an account that has sufficient privileges.
- Go to **Microsoft Entra ID** > **App registrations** > **New registration**.
- Provide a descriptive name.
- Under Supported account types, select Accounts in this organizational directory only (Single tenant).
- Leave the Redirect URI blank. Click Register.
- Copy and save the **Application (client) ID** and **Directory (tenant) ID** from the overview page. You will need these later.

Step 2: Create a Client Secret

- In your newly created app registration, navigate to **Certificates & secrets** > **Client secrets** > **New client secret**.
- Add a description and choose an expiry period appropriate for your organization.
- Click Add, then immediately copy the **secret Value**. This is the only time it is shown in full.

Step 3:

- In the app registration, go to **API permissions** > **Add a permission**.
- Select APIs my organization uses, then search for and select WindowsDefenderATP.
- Choose Application permissions and grant the following minimum required scopes:

Permission	Purpose
Alert.Read.All	Read all MDE alerts and incidents
Machine.Read.All	Read device inventory and health state
Vulnerability.Read.All	Read vulnerability and software inventory
AdvancedQuery.Read.All	Execute advanced hunting queries (optional)

Step 4:

- Click Add permissions, then click Grant admin consent for [Your Tenant]. Confirm when prompted.
- Verify the Status column shows Granted for [tenant] for all added permissions.

> Please saved and provide this values:

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

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

Revision #3
Created 5 March 2026 07:22:27
Updated 13 May 2026 18:46:47 by Richmond Abella