# Lab 2 -- Enable Data Connectors in Microsoft Sentinel

## Objectives

In this Lab you will learn how to enable Data Connectors in Microsoft Sentinel to bring alerts and/or telemetry from different sources.

Prerequisites

This lab assumes that you have completed Lab 1, as you will need an Microsoft Sentinel workspace provisioned.

Some of the data connectors that will be used in this lab, require some specific permissions on the workspace or your azure subscription. If you don't have the appropriate permissions, you can still continue doing the rest of the labs.

## Exercise 1 -- Enabling Data Connectors in Microsoft Sentinel

### Task 1 - Enabling Azure Activity data connector

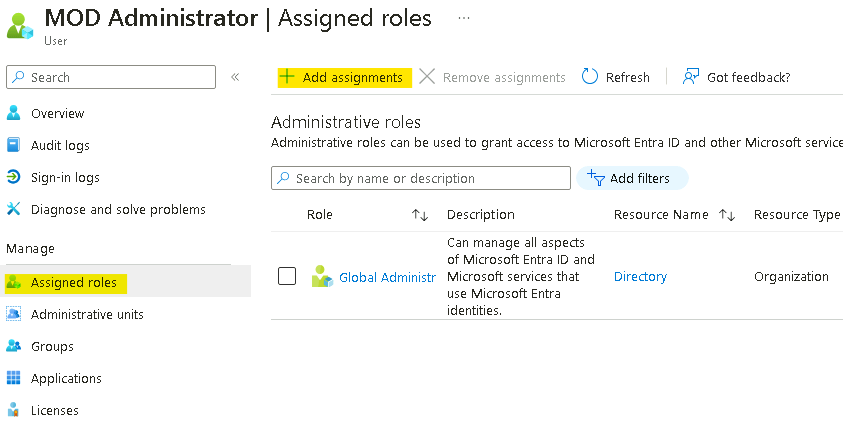
This exercise shows you how to enable Data connectors.

1. In the browser tab navigate to <https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/AllUsers> and select the Tenant Administrator account

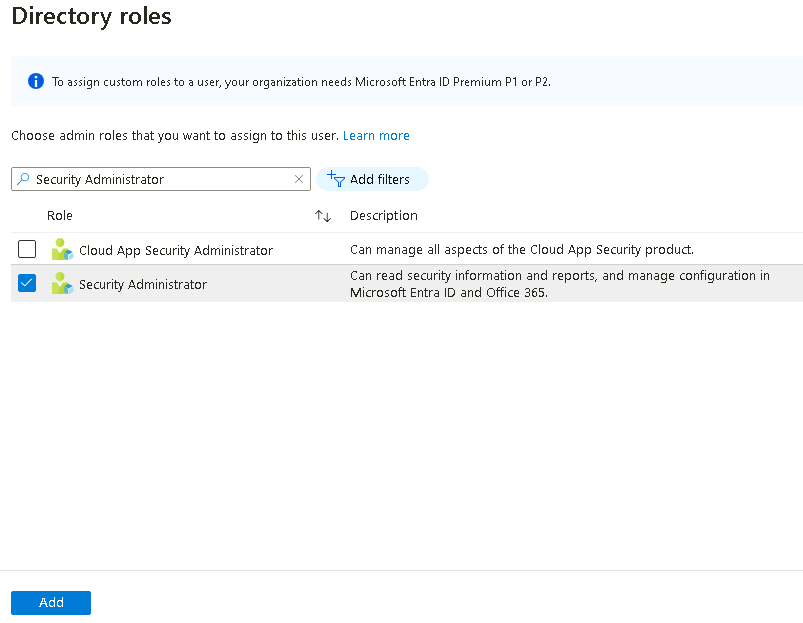
A screenshot of a computer

Description automatically generated

1. Select the **Assigned roles** under Manage and then click on **+ Add assignments.**



1. Search and select **Security Administrator**, then click on the **Add** button.





1. On the **Azure Portal** [**http://portal.azure.com**](urn:gd:lg:a:send-vm-keys), search for **Microsoft Sentinel** and click on **Microsoft Sentinel**.

A screenshot of a computer

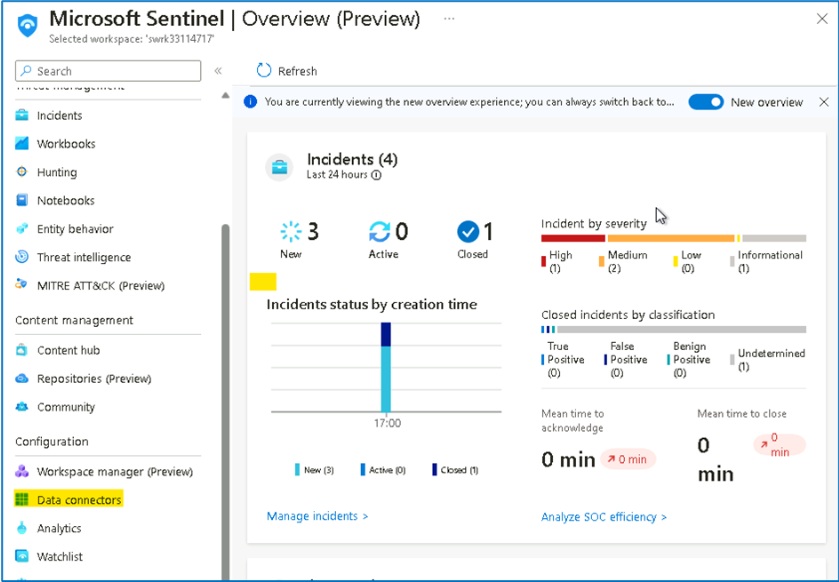
Description automatically generated

1. Select **SwrkXXXXXXX**.

A screenshot of a computer

Description automatically generated

1. Now select **Data Connectors** under **Configuration** section.



1. You should be able to see the **Data connectors** already available based on the selection made during the deployment.

A screenshot of a computer

Description automatically generated

1. On the data connectors screen, select the **Azure Activity** connector and click on **Open connector page**.

A screenshot of a computer

Description automatically generated

1. On the **Azure Activity connector** page, go to option number **2. Connect your subscriptions through diagnostic settings new pipeline**. This method leverages Azure Policy and it brings many improvements compared to the old method (more details about these improvements can be found here). Click on the **Launch Azure Policy Assignment** wizard, this will redirect you to the policy creation page.

A screenshot of a computer

Description automatically generated

1. On the **Scope** selection select **Azure Pass -- Sponsorship** and under **Resource Group** select **RG4Sentinel**. Click **Select**.

A screenshot of a computer

Description automatically generated

1. Go to the **Parameters** tab. On the **Primary Log Analytics workspace** select the **SwrkXXXXXXX**.

A screenshot of a computer

Description automatically generated

1. Under **Remediation** tab, select the check box besides **Create a remediation task** and then click on **Review + create** button

A screenshot of a computer

Description automatically generated

1. On the **Review + create** tab, click on the **Create** button.

A screenshot of a computer

Description automatically generated

1. In the **Notification** pane you will be able to see the '**Role Assignments creation succeeded**', '**Remediation task creation succeeded**' and '**Creating policy assignment succeeded**' notifications.

A screenshot of a computer

Description automatically generated

1. On the **Azure Activity connector** page you will be able to see the connection status.

**Note**: It is normal if you don't immediately see the connector showing as connected and in green, it takes around 30 minutes for the process to complete. Also, each subscription has a maximum of 5 destinations for its activity logs. If this limit is already reached, the policy created as part of this exercise won't be able to add an additional destination to your Microsoft Sentinel workspace.

A screenshot of a computer

Description automatically generated

1. Continue to the next task then you can check back after 30 minutes.
2. Close the **Azure Activity** connector blade to go back to the **Data Connectors** page.

### Task 2 - Enabling Tenant-based Microsoft Defender for Cloud data connector

This task shows you how to enable the Microsoft Defender for Cloud data connector. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

1. On the **Data connectors** screen, type **tenant** in the search bar, select the **Tenant-based Microsoft Defender for Cloud** **(Preview)** connector and click on **Open connector page**.

A screenshot of a computer

Description automatically generated

1. On the **Tenant-based Microsoft Defender for Cloud** **(Preview)** connector page, under **Configuration** section click on the **Connect** button.

A screenshot of a computer

Description automatically generated

1. You should receive the notification as Connected successfully. **[If may be possible that the notification may not appear.]{.underline}**

A screenshot of a computer

Description automatically generated

1. Wait for 3-5 minutes and then refresh the page, the Status of the connector should also be updated to **Connected.**

A screenshot of a computer

Description automatically generated

### Task 3 - Enabling Microsoft Defender Threat Intelligence connector

The **Microsoft Defender Threat Intelligence** (MDTI) connector to your Sentinel workspace, which ingests Microsoft Threat Intelligence indicators automatically into the ThreatIntelligenceIndicator table. MDTI provides a set of indicators and access to the https://ti.defender.microsoft.com portal at no additional cost, with the premium features of the MDTI portal and API requiring licensing.

The *Threat Intelligence* content solution includes the data connectors for all supported forms of Threat Intelligence.

**NOTE:** Sentinel also supports importing Threat Intelligence indicators via the TAXII protocol using the **Threat Intelligence - TAXII** data connector, so if you have your own preferred TI source, you can add that to your workspace instead.

1. On the **Azure Portal** [**http://portal.azure.com**](urn:gd:lg:a:send-vm-keys), search for **Microsoft Sentinel** and click on **Microsoft Sentinel**.

A screenshot of a computer service

Description automatically generated

1. Select **SwrkXXXXXXX**.

A screenshot of a computer

Description automatically generated

1. From the left menu choose the ***Microsoft Defender Threat Intelligence (preview)*** connector and click **Open Connector Page** at the bottom right.

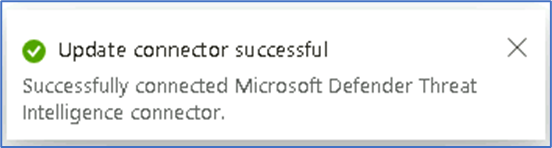
A screenshot of a computer

Description automatically generated

1. On the Connector page, from the **Import indicators** list, leave the default "**All available**" selected, and click **Connect**.

A screenshot of a computer

Description automatically generated



1. The Status of the Connector should be updated to **Connected.**

A screenshot of a computer

Description automatically generated

1. Threat Intelligence indicators will start being ingested into the **ThreatIntelligenceIndicator** table.