# Lab 6 - UEBA with Microsoft Sentinel

## Exercise 1: Explore UEBA with Microsoft Sentinel

A screenshot of a computer program

Description automatically generated

You are a Security Operations Analyst working at a company that implemented Microsoft Sentinel. Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards.

Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

### Task 1: Explore Entity Behavior

In this task, you will explore Entity behavior analytics in Microsoft Sentinel.

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

A screenshot of a computer

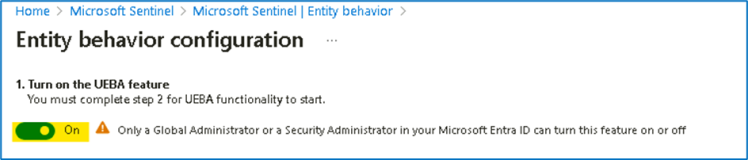
Description automatically generated

1. On the popup from **Entity behavior settings**, select **Set UEBA**.

A screenshot of a computer

Description automatically generated

1. On the next page, you should notice that **UEBA** is already enabled as a part of the Deployment done in Lab 1.



**Note**: If UEBA is not On by default, turn it on from entity behavior settings.

A screenshot of a computer

Description automatically generated

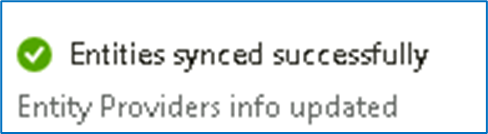
A screenshot of a computer

Description automatically generated

1. For the section **2. Sync Microsoft Sentinel with at least one of the following directory services**, notice the Microsoft Entra ID is already selected, click on the **Apply** button.

A screenshot of a computer

Description automatically generated



1. You should receive the Notification as shown in below image. The page will automatically be redirected to the Entity behaviour page.



1. The confirms that the Entity behaviour is configured successfully.

A screenshot of a computer

Description automatically generated

### Task 2: Confirm and review Anomalies rules

In this task, we will confirm if Anomalies analytics rules are enabled.

1. While on the Microsoft Sentinel page click on **Analytics** under configuration, then select the **Anomalies** tab.

A screenshot of a computer

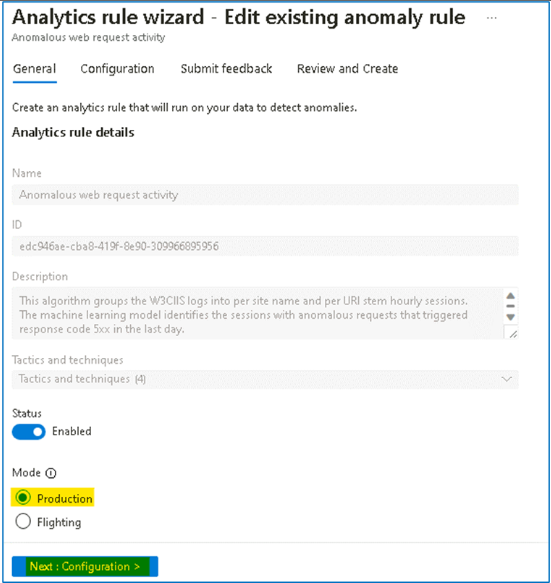
Description automatically generated

1. Select any rule and then select **Edit** on the rule blade.

A screenshot of a computer

Description automatically generated

1. Review the **General** tab information. Notice the **Mode** is **Production** and then select **Next: Configuration**.



1. Review the ***Configuration*** tab information. Notice that you cannot change the **Anomaly score threshold**.

A screenshot of a computer

Description automatically generated

1. Then select **X** in the top right corner to exit the Analytics rule wizard.
2. Scroll right to the analytics rule you selected until see and select the ellipsis **(...)** icon. Select **Duplicate**

A screenshot of a computer

Description automatically generated

1. Scroll left to review the new rule with the **FLGT** tab at the beginning of the name. Select **FLGT** rule and then select **Edit** on the rule blade.

A screenshot of a computer

Description automatically generated

1. Review the **General** tab information. Set the status to **Enabled**, you will notice the **Mode** is **Flighting** and then select **Next: Configuration**.

A screenshot of a computer

Description automatically generated

1. Review the **Configuration** tab information. Notice that you can now change the **Anomaly score threshold**.

A screenshot of a video

Description automatically generated

1. Set the value to **1** and then select **Next: Submit Feedback**.

A screenshot of a computer

Description automatically generated

1. Provide the feedback and then click on **Next: Review + create**.

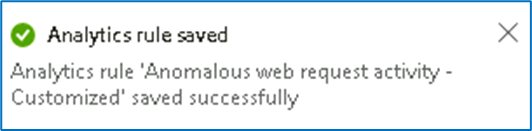
A screenshot of a computer

Description automatically generated

1. After the Validation is completed, click on Save button to update the rule

A screenshot of a computer

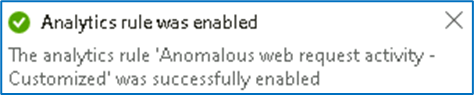
Description automatically generated



1. If the **FLGT Analytic rule** still shows **Disabled**, then right-click on it and select **Enable** option.

A screenshot of a computer

Description automatically generated



1. Now it should be enabled.

A screenshot of a computer

Description automatically generated