ThreatConnect

Microsoft® Defender for Endpoint Integration

User Guide

Software Version 1.0

January 13, 2022

30077-01 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

TABLE OF CONTENTS

OVERVIEW

The Microsoft Defender for Endpoint integration allows you to ingest alerts into ThreatConnect® and then automate triage and investigative actions across your security stack.

There is a Playbook App and a Service App for this integration, each of which can be found in the ThreatConnect App Catalog under the names **Microsoft Defender for Endpoint** and **Microsoft Defender for Endpoint Service**, respectively. The Playbook App provides a powerful set of actions that can be leveraged within a larger security workflow orchestration or even simple automation. Immediate actions can be taken to investigate, stop, and remediate potential threats at the endpoint, based on external threat intelligence.

This guide covers how to install the **Microsoft Defender for Endpoint Service** App, configure and activate a corresponding Service, and create a Playbook that uses the custom Trigger Service.

DEPENDENCIES

ThreatConnect Dependencies

- Playbooks enabled by a System Administrator
- System role of Administrator to install Service Apps and create, view, and activate Services
- Organization role of Standard User to build a Playbook that uses a Trigger Service

Microsoft Defender for Endpoint Dependencies

- Microsoft Azure® AD Tenant with administrator rights to create an App registration and manage permissions
- Azure App registration with application-level permissions to **SecurityAlert.ReadWrite.All** in the Microsoft Graph API and **Alert.ReadWrite.All** in the WindowsDefenderATP API

MICROSOFT AZURE APP REGISTRATION AND CONFIGURATION

This integration requires an App registration in the Azure portal. The App must also have the required permissions. Follow the steps in this section to create a new App registration and assign the appropriate permissions.

1. Create a new App registration with the Microsoft identity platform. Note the **Client ID** and **Tenant ID** on the App's **Overview** screen, as these values will be entered as configuration parameters into the ThreatConnect integration.

   NOTE: In most cases, a type of** Single Tenant **should be selected, and the optional** Redirect URI **field should be left blank.

2. On the App page, under **Manage**, select **API Permissions**. The **Request API permissions** screen will be displayed.
3. Click **+ Add a permission**. The **Request API permissions** drawer will be displayed.
4. On the **Microsoft APIs** tab, select the **Microsoft Graph** API (Figure 1).

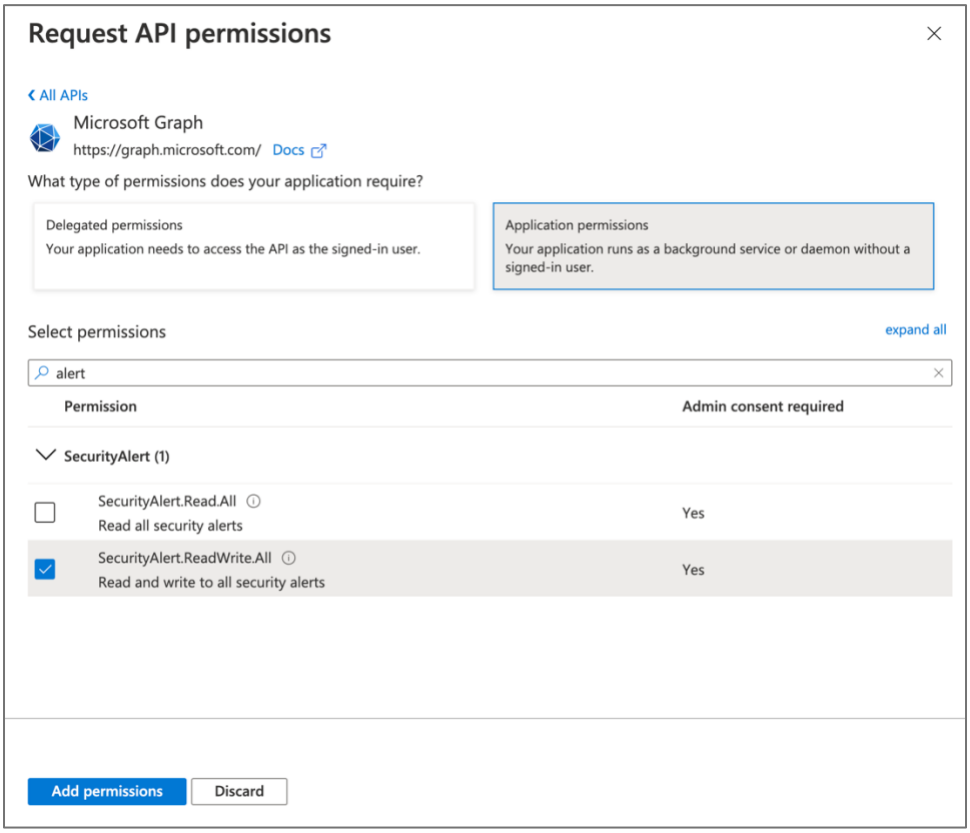

Figure 1

- **What type of permissions does your application require?**: Select **Application permissions**.

- **Select permissions**: Select **SecurityAlert.ReadWrite.All**.
- Click the **Add permissions** button. The added permissions will now be listed under the **Configured permissions** section of the **API permissions** screen.

5. On the **API permissions** screen, click **+ Add a permission**. The **Request API permissions** drawer will be displayed again.
6. Select the **APIs my organization uses** tab, and then select the **WindowsDefenderATP** API (Figure 2).

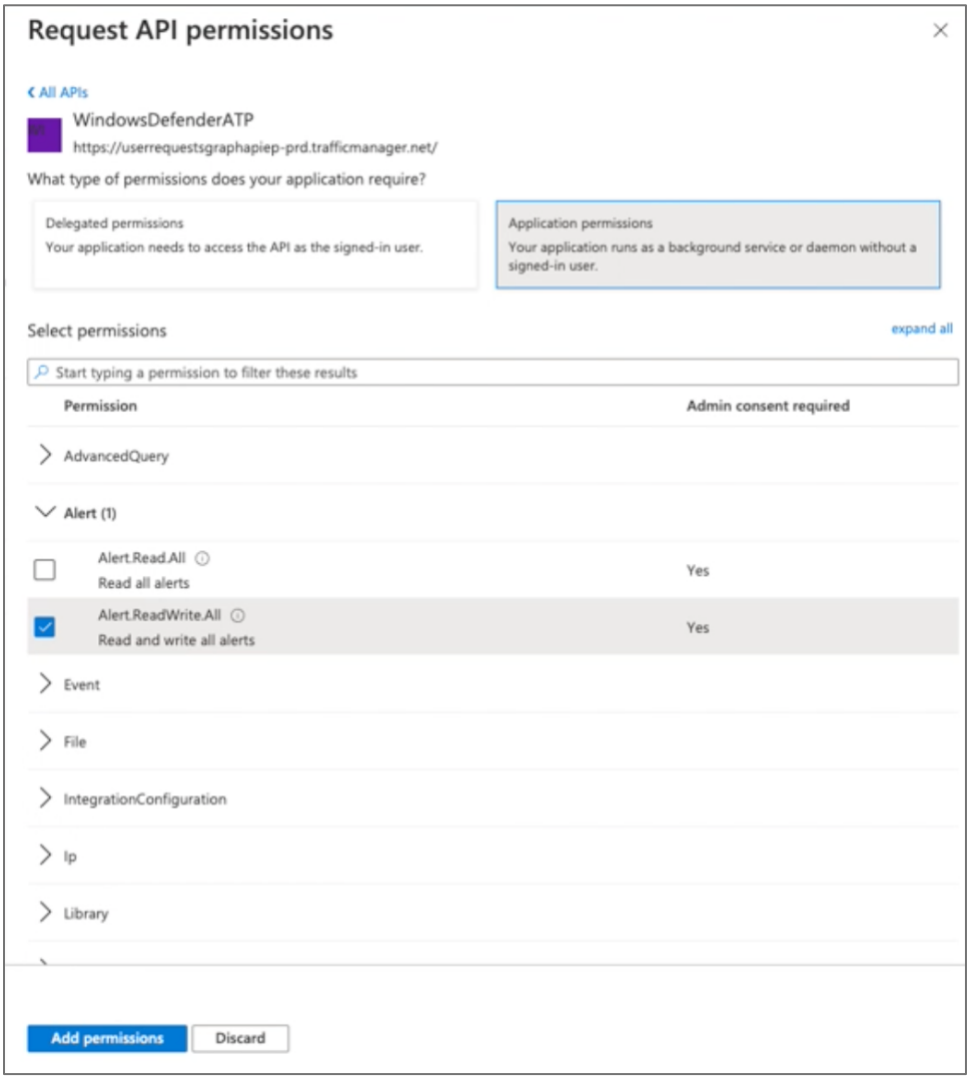

Figure 2

- **What type of permissions does your application require?**: Select **Application permissions**.
- **Select permissions**: Select **Alert.ReadWrite.All**.
- Click the **Add permissions** button. The added permissions will now be listed under the **Configured permissions** section of the **API permissions** screen.

7. In the **Configured permissions** section of the **API permission** screen, click ✓ **Grant admin consent for <*Organization Name*>** (Figure 3**Error! Reference source not found.**).

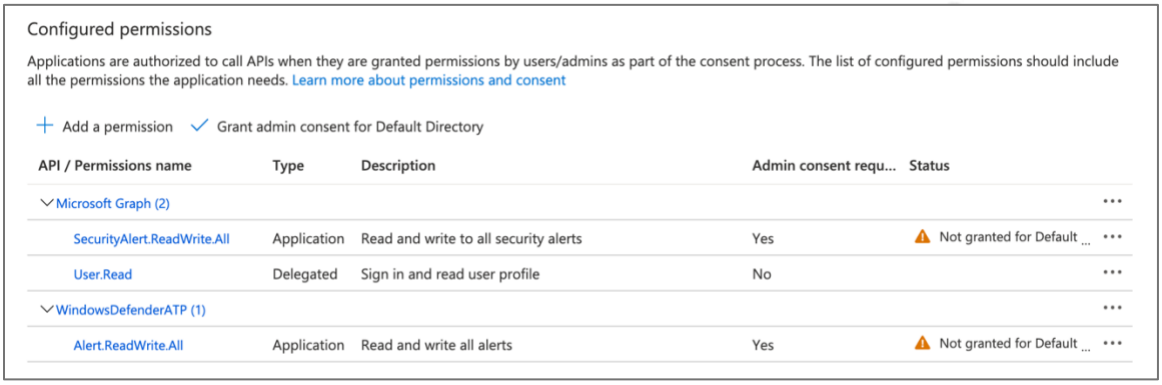

Figure 3

8. The **Grand admin consent confirmation** window will be displayed. Click the **Yes** button. The following entry will be displayed in the **Status** column for each permission: ✅ **Granted for <*Organization Name*>** (Figure 4**Error! Reference source not found.**).

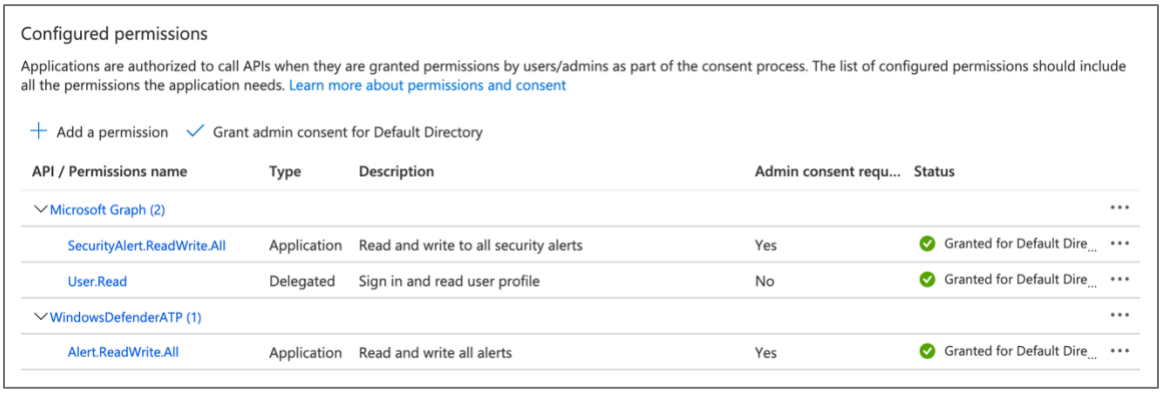

Figure 4

9. On the App page, under **Manage**, select **Certificates & secrets**. The **Certificates & secrets** screen will be displayed.
10. Select the **Client secrets** tab, and then click **+ New Client Secret**. The **Add a client** secret drawer will be displayed (Figure 5).

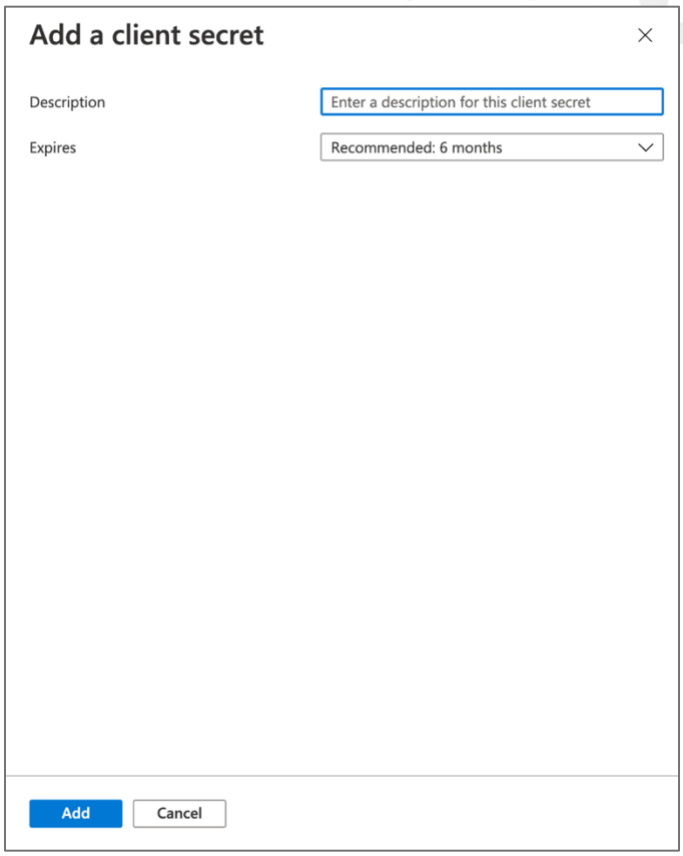

Figure 5

- **Description**: Enter a description for the client secret.
- **Expires**: Select the amount of time after which the client secret will expire.
- Click the **Add** button.

11. The client secret will be displayed on the **Client secrets** tab of the **Clients & secrets** screen (Figure 6). Save the client secret's **Value**. This value will be entered as a configuration parameter into the ThreatConnect integration, along with the **Client ID** and **Tenant ID** from Step 1.

Figure 6

WARNING: Make sure to save the client secret's **Value**, as you will not be able to retrieve it again after leaving this screen.

THREATCONNECT CONFIGURATION

Installing the Microsoft Defender for Endpoint Service App

A System Administrator should follow these steps to use TC Exchange™ to install the **Microsoft Defender for Endpoint Service** App.

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Settings** and select **TC Exchange Settings**. The **Installed** tab of the **TC Exchange Settings** screen will be displayed.
3. Select the **Catalog** tab. The **Catalog** screen will be displayed.
4. Enter "microsoft defender" (without quotation marks) in the search bar to filter the results to show the **Microsoft Defender for Endpoint** Playbook App and **Microsoft Defender for Endpoint Service** App (Figure 7).

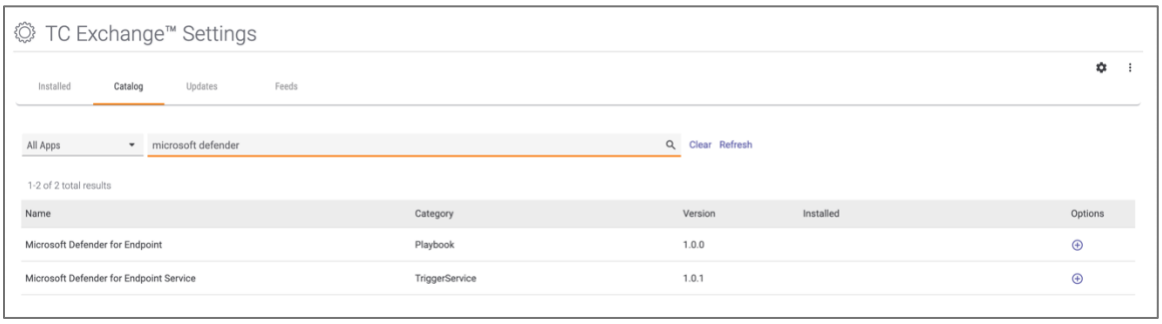

Figure 7

NOTE: This guide covers the installation and configuration of the** Microsoft Defender for Endpoint Service **App only.

5. Click **Install** ⊕ in the **Options** column for the **Microsoft Defender for Endpoint Service** App. The **Release Notes** window for the **Microsoft Defender for Endpoint Service** App will be displayed (Figure 8).

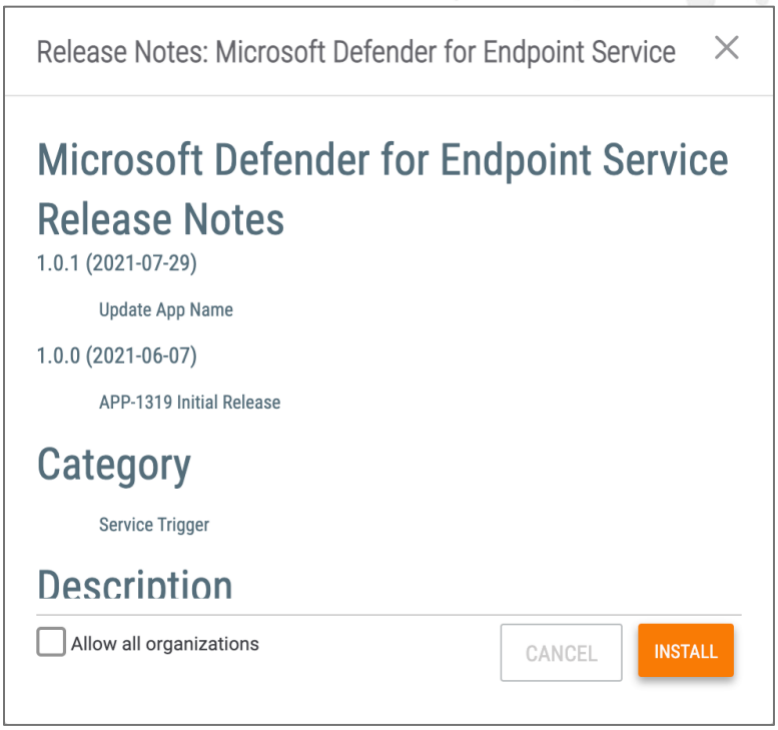

Figure 8

- **Allow all organizations**: When installing a Service App, it does not matter whether this checkbox is selected. The Service itself, rather than the Service App, sets the permissions and access to the App, as detailed in the "Creating and Configuring a Playbook Trigger Service" section.
- Click the **INSTALL** button.

Creating and Configuring a Playbook Trigger Service

This section provides instructions on creating a Playbook Trigger Service for the **Microsoft Defender for Endpoint Service** App. For instructions on creating general Playbook Services, see *Playbook Services*.

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover the cursor over **Playbooks** and select **Services**. The **Services** screen will be displayed.
3. Click the **+ NEW** button at the upper-left corner of the screen. The **Select** screen of the **Create Service** drawer will be displayed (Figure 9).

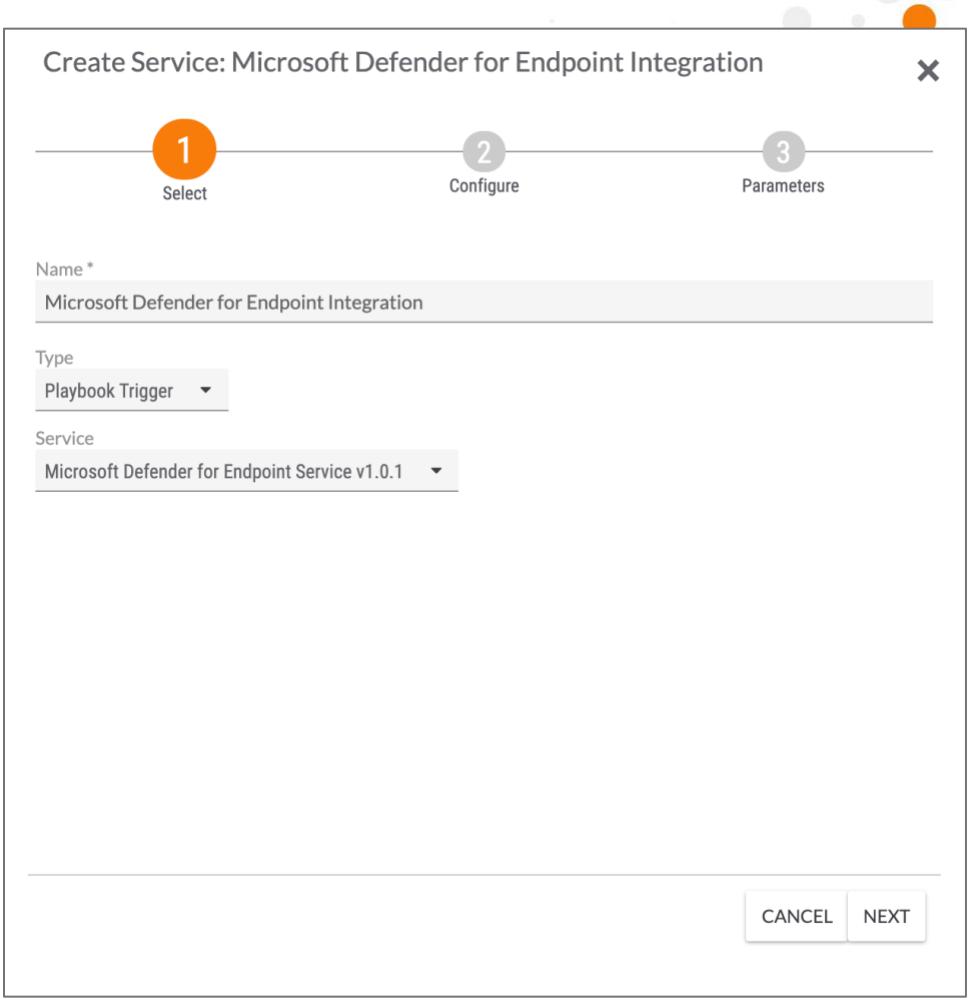

Figure 9

- **Name**: Enter a unique name for the Service.

  NOTE: When naming the Service, consider the fact that one Service can be created multiple times for different customers by using different credentials.

- **Type**: Select **Playbook Trigger**.
- **Service**: Select **Microsoft Defender for Endpoint Service v1.0.1**.
- Click the **NEXT** button.

4. The **Configure** screen of the **Create Service** drawer will be displayed (Figure 10).

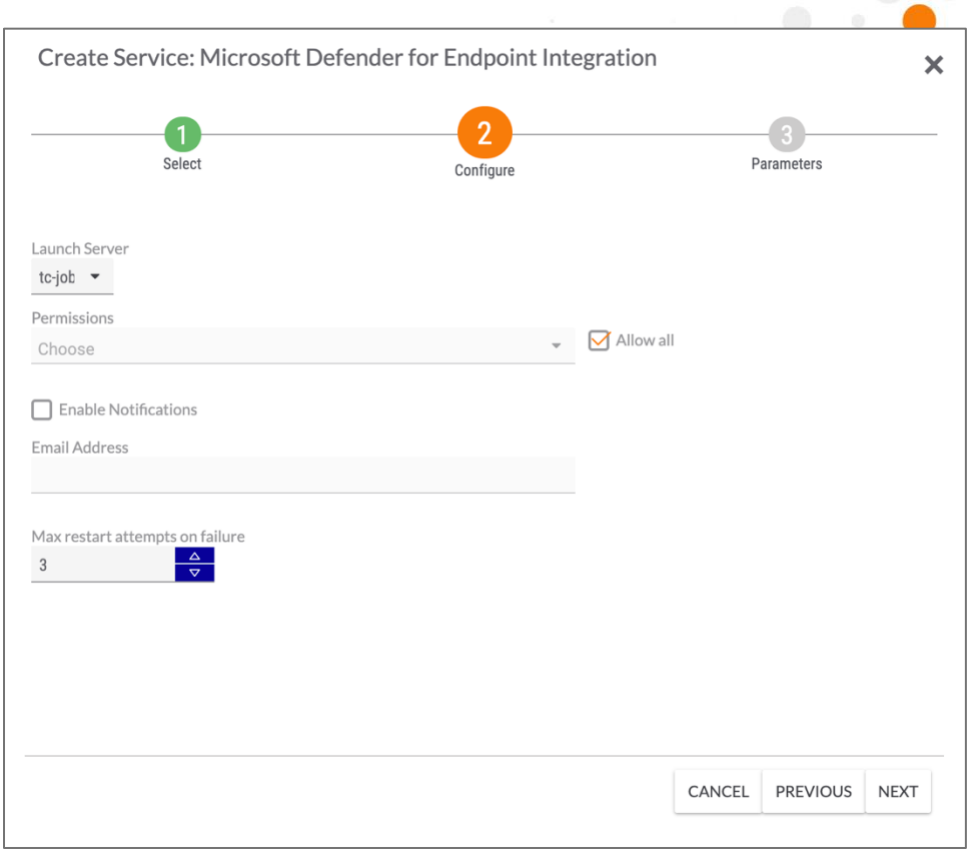

Figure 10

- **Launch Server**: Select the server on which the Service will launch. Typically, on multi-server environments, the Service is launched on the **tc-job** server.
- **Permissions**: Select the Organizations that will have access to the Service.
- **Allow all**: Select this checkbox if you want to give all Organizations on the ThreatConnect instance access to the Service.
- **Enable Notifications**: Select this checkbox to send an email when the Service fails to start. It is recommended to enable this setting.
- **Email Address**: If the **Enable Notifications** checkbox is selected, enter the email address to which notifications should be sent. It is recommended to enter an email address for a ThreatConnect user with a System role of Administrator.
- **Max restart attempts on failure**: Enter the number of times ThreatConnect should try to restart the Service if it fails. It is recommended to set this value to **3**.
- Click the **NEXT** button.

5. The **Parameters** screen of the **Create Service** drawer will be displayed (Figure 11).

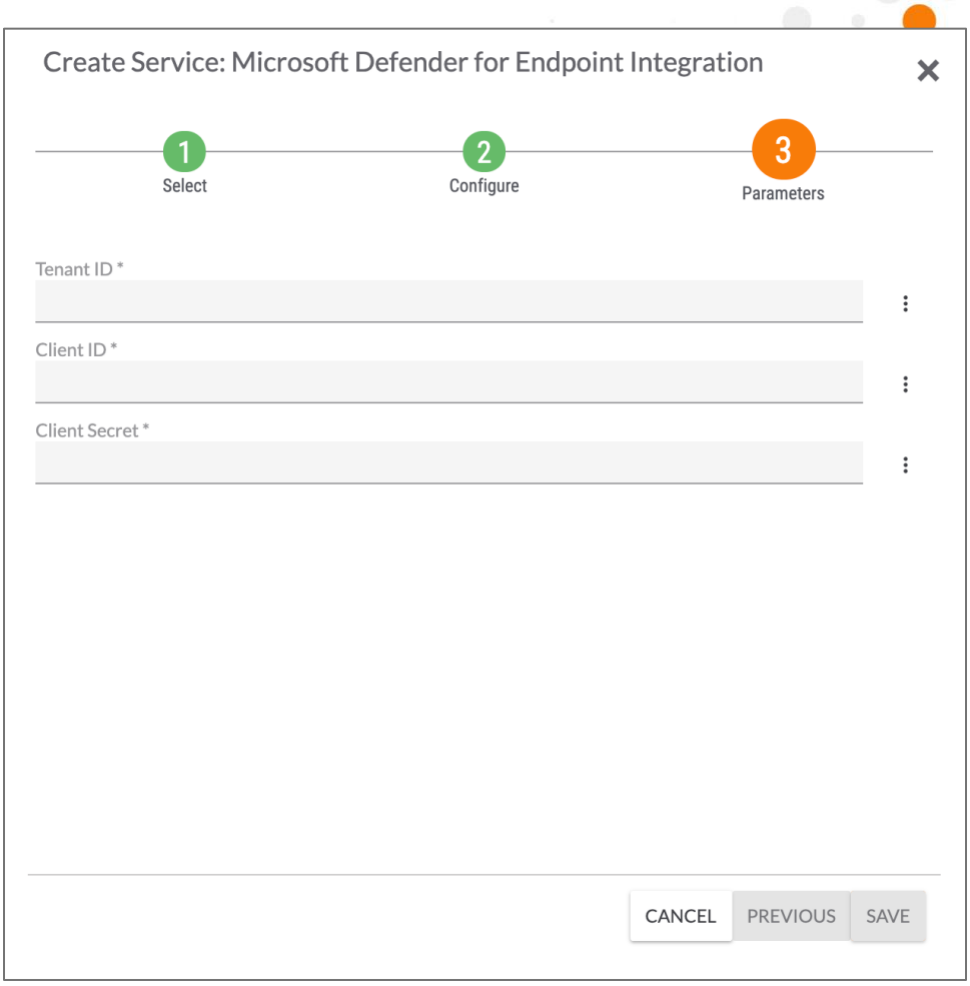

Figure 11

- **Tenant ID**: Enter the **Tenant ID** of the App registered in Microsoft Azure during Step 1 of the "Microsoft Azure App Registration and Configuration" section.
- **Client ID**: Enter the **Client ID** of the App registered in Microsoft Azure during Step 1 of the "Microsoft Azure App Registration and Configuration" section.
- **Client Secret**: Enter the **Value** of the client secret saved during Step 11 of the "Microsoft Azure App Registration and Configuration" section.
- Click the **SAVE** button.

6. The Service will now be displayed on the **Services** screen (Figure 12). Toggle its slider on (orange) to activate the Service. If the Service is not activated, Playbooks that use its corresponding Service Trigger will produce a validation error.

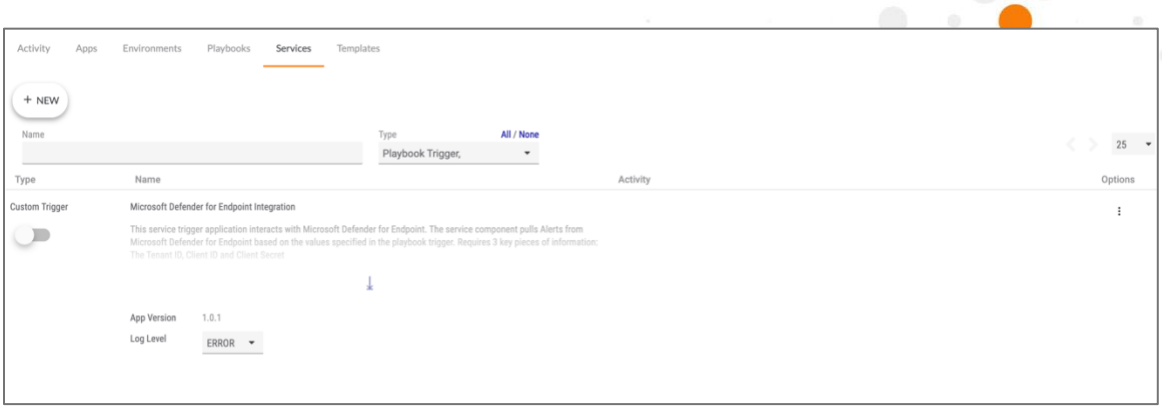

Figure 12

Building a Playbook

This section provides instructions on building a Playbook that will execute whenever an alert is generated in Microsoft Defender for Endpoint. This Playbook is built using a Service Trigger that corresponds to the Service created in the "Creating and Configuring a Playbook Trigger Service" section and a **JMESPath** App.

1. On the top navigation bar, click **Playbooks** to display the **Playbooks** screen. Alternatively, click the **Playbooks** tab to the left of the **Services** tab when on the **Services** screen.
2. Hover over the **NEW** button at the upper-left corner of the screen and select **Create Playbook**. The **Create Playbook** window will be displayed (Figure 13).

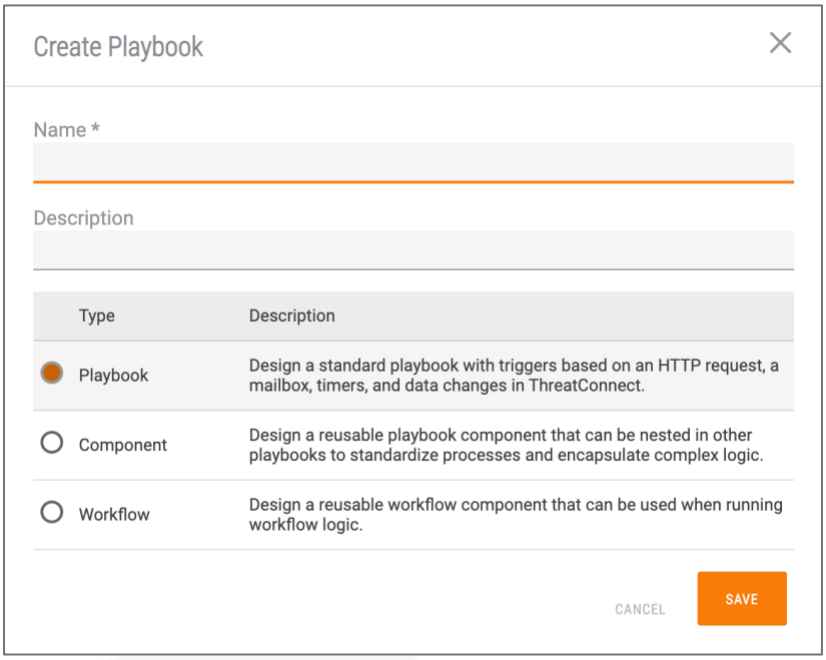

Figure 13

- **Name**: Enter a name for the Playbook.
- **Description**: Enter a description for the Playbook.
- **Type**: Keep the selection of **Playbook**.
- Click the **SAVE** button.

3. The **Playbook Designer** will be displayed. Select the Service Trigger corresponding to the Service created in the "Creating and Configuring a Playbook Trigger Service" section from the **Service Trigger** section of the **Triggers** pane on the left side of the **Playbook Designer** screen to add it to the design pane (Figure 14).

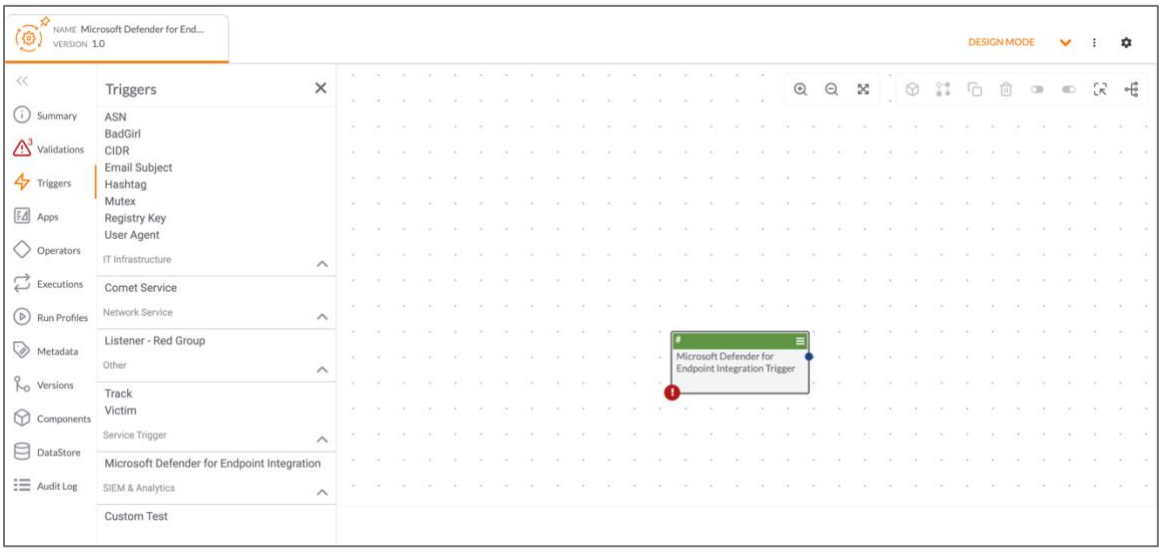

Figure 14

4. Double-click the Service Trigger to edit it. The **Configure** section of the **Edit Trigger** pane will be displayed on the left side of the **Playbook Designer** screen (Figure 15).

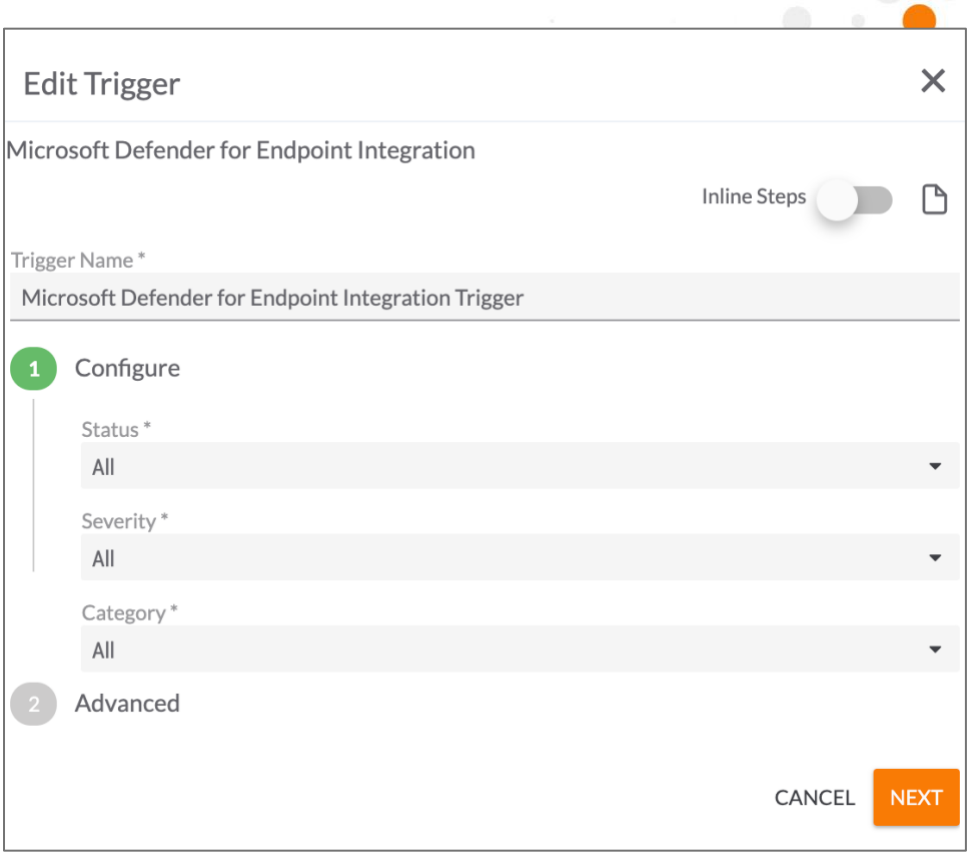

Figure 15

- **Trigger Name**: By default, the Trigger's name is set to the name of the Service created in the "Creating and Configuring a Playbook Trigger Service" section, followed by the word "Trigger." Edit the Trigger's name, if desired.
- **Status**: Select the alert status (**All**, **Unknown**, **New**, **In Progress**, or **Resolved**) that will trigger the execution of the Playbook.
- **Severity**: Select the alert severity (**All**, **UnSpecified**, **Informational**, **Low**, **Medium**, or **High**) that will trigger the execution of the Playbook.
- **Category**: Select the alert category that will trigger the execution of the Playbook.

  NOTE: Alerts generated in Microsoft Defender for Endpoint must meet all three criteria specified for** Status, Severity, **and** Category. **For example, if you set** Status **to** New, Severity **to** Medium, **and** Category **to** Defense Evasion, **only alerts with that status, severity, and category will trigger the Playbook.

- Click the **NEXT** button.

5. The **Advanced** section of the **Edit Trigger** pane will be displayed (Figure 16).

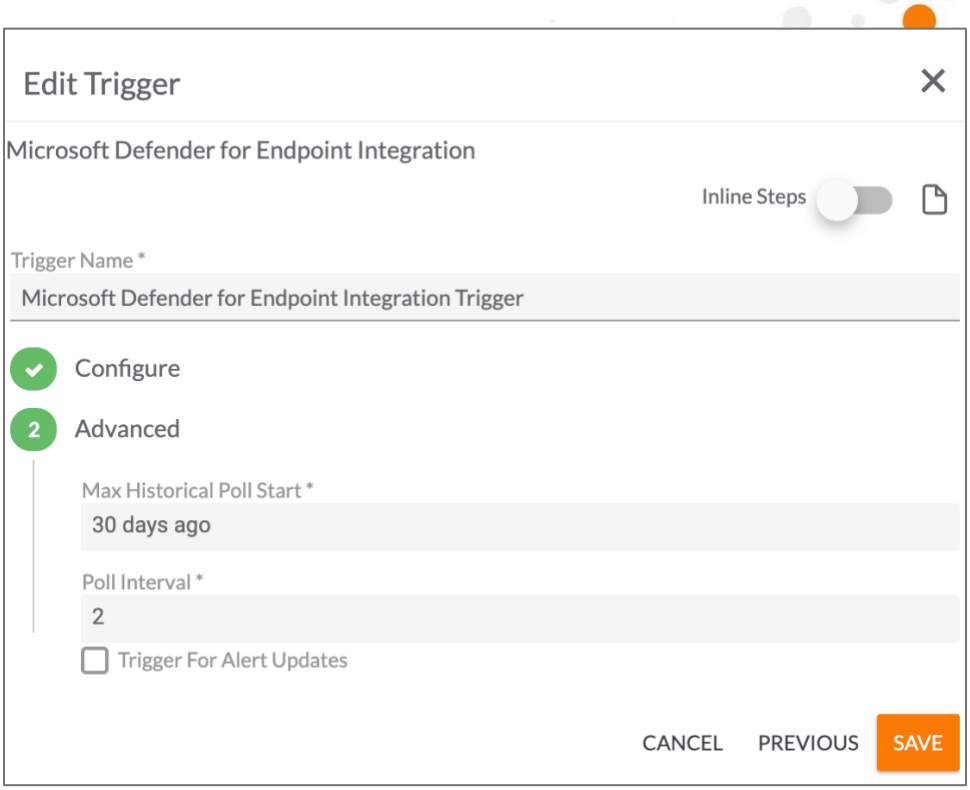

Figure 16

- **Max Historical Poll Start**: Upon activation, the first poll will be conducted after the completion of the first **Poll Interval** period. On future runs, if the time of the last run is greater than the **Poll Interval**, the App will only retrieve data as far back as the input value for this field. This value must be parseable as a datetime (e.g., 30 days ago).
- **Poll Interval**: Enter the polling interval in minutes.
- **Trigger For Alert Updates**: Select this checkbox to trigger the Playbook for new alerts *and* updates to existing alerts.
- Click the **SAVE** button.

6. Click **Apps** on the side navigation bar of the **Playbook Designer** screen and select the **JMESPath** App to add it to the design pane.
7. Connect the Service Trigger to the **JMESPath** App (Figure 17).

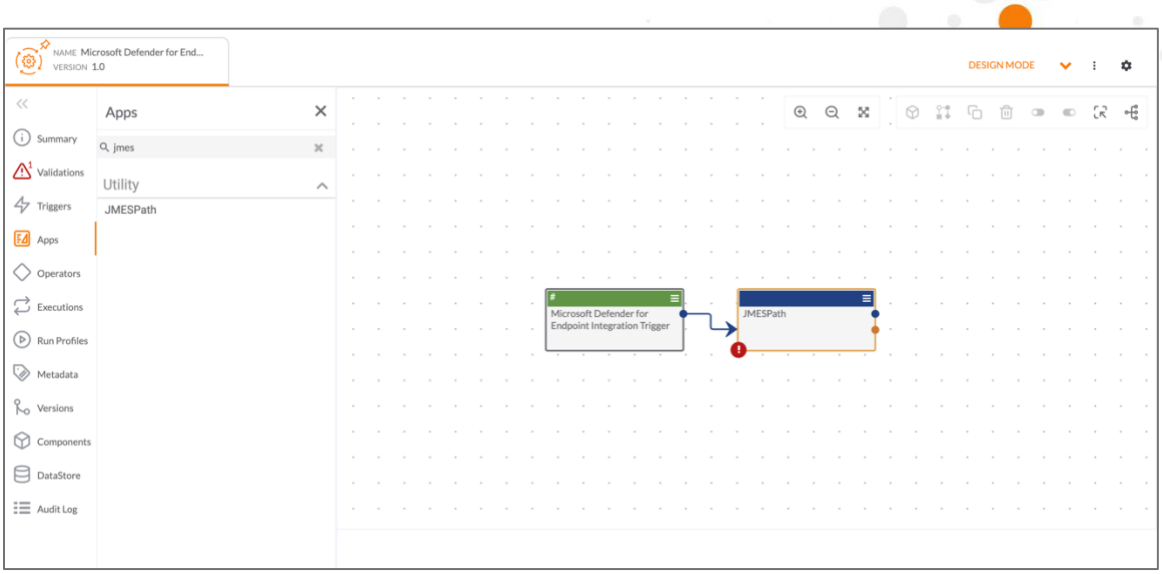

Figure 17

8. Double-click the **JMESPath** App to edit it. The **Edit App** pane will be displayed on the left side of the **Playbook Designer** screen (Figure 18).

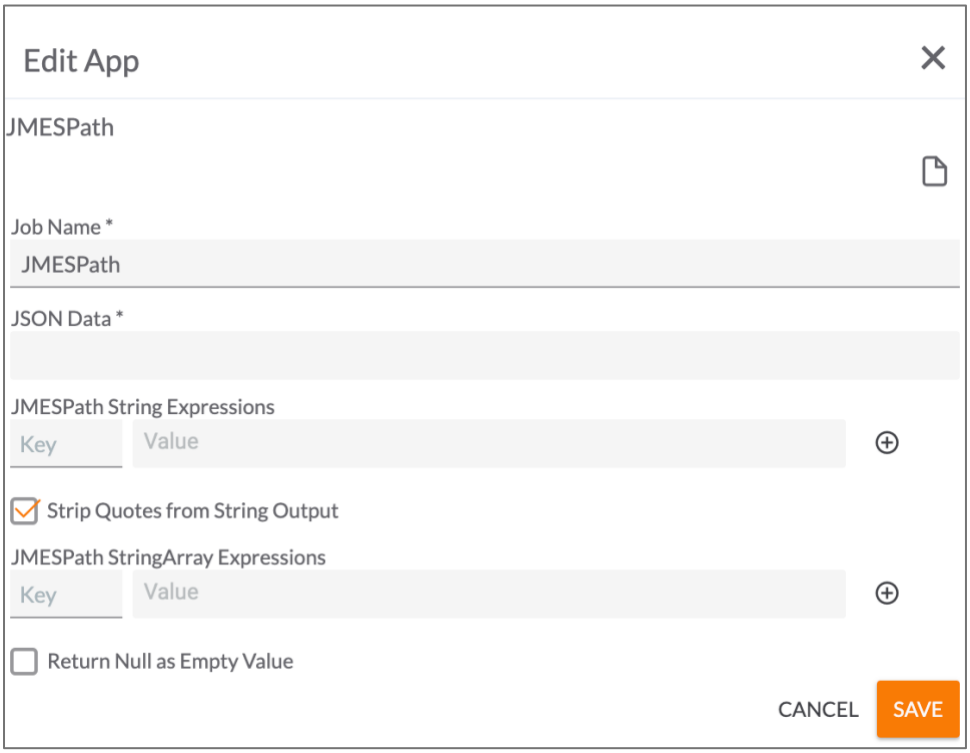

Figure 18

- **Job Name**: Edit the name of the **JMESPath** App, if desired.
- **JSON Data**: Type **#** and select **msft.defender.response.json.raw** from the list that is displayed.

- Leave all remaining fields unchanged, and then click the **SAVE** button.

9. Click **Settings** at the upper-right corner of the **Playbook Designer** screen and set the Playbook's **Log Level** to **TRACE**.

10. Click the **MODE** dropdown at the upper-right corner of the **Playbook Designer** screen and switch the Playbook from **Design Mode** to **Active** (Figure 19).

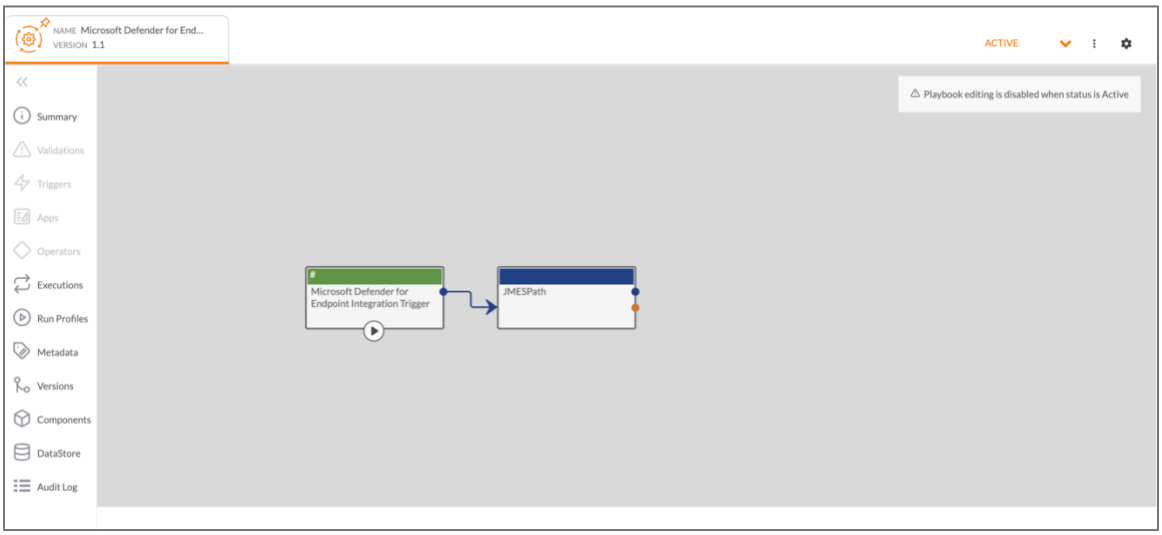

Figure 19

The Playbook is now configured and will execute whenever an alert that meets the criteria defined in the **Configure** section of the **Edit Trigger** pane (Figure 15) is generated in Microsoft Defender for Endpoint. After the Playbook executes, the results of its execution can be viewed by opening the Playbook and clicking **Executions** on the side navigation bar of the **Playbook Designer** screen.

ADDITIONAL RESOURCES

- Alerts Queue in Microsoft 365 Defender documentation
- Microsoft Defender for Endpoint documentation
- View and Organize the Microsoft Defender for Endpoint Alerts Queue documentation