Mandiant

WORKING WITH EVENT FILTER RULES

> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

There are four places you can view and create Event Filter Rules in the platform, three of which prepopulate the first condition for you if you're creating a new rule. In addition, two of those areas allow you to edit and delete the event Filter Rules.

Location	Prepopulated Condition
Integration Event Filter Rules Table on Integration Page	N/A
An Integration in the Integrations Table on the Integrations page	Automatically adds the Integration
Action Preview / Action Details	Automatically adds the VID
Event section for a Job Action	Automatically adds the Event Description

This topic covers:

- Configuring the Event Filter Type, used as the default for all Event Filter Rules
- Creating Event Filter Rules
- Updating and Deleting Event Filter Rules

To Configure the Event Filter Type

To allow you to quickly update the behavior of your event filter rules, there is a global event filter type. When creating and editing rules, you can override this setting.

1. Go to **Settings** > **Integrations** and click **Change Event Filter Type** in the Integration Event Filter Rules table.
2. Choose your option, Suppress Events or Drop Events, and click **Save**. This will be what happens to Events that match an Event Filter rule in jobs moving forward, unless you override the setting.

To add an event filter rule

> New Event Filter Rules only apply to new Jobs, they do not change Jobs that ran before the rule was created.

1. Locate the Event Filter Rules section of the page and click Add Event Filter Rule.
   - Go to **Settings** > **Integrations** and click **Add Event Filter Rule**.
   - Go to **Settings** > **Integrations**, select an Integration's action menu and click **Add Event Filter Rule**.
   - Scroll to the Event Filter Rule section of an Action and click **Add Event Filter Rule**.
   - Open the Events section for a Job Action, select an Event's action menu, and click **Add Event Filter Rule**.
2. (Optional) If you don't want to use the system setting for what happens with the event, click Override system settings and select the setting you want instead. In addition to Suppress Events & Drop Events, you also have the

option to Keep Events that match your rule.

3. In the Event Filter Rule tab, add your Conditions.
    - The first condition will be added automatically if you start from an Action or an Event
    - When you add multiple conditions, the event must match all conditions for the rule to be applied
    - Conditions can be defined for Actions, Integrations, and Events

4. In the Event JSON tab, add your filter rules using the various drop down fields and their conditions. When you have added all your conditions for each JSON drop-down option, click **Add to Rule**.
    - "description": This is the description of the Event. Conditions include:
        - In
        - Not In
        - Contains
        - Doesn't Contain
        - Starts With
        - Ends With
    - "dest_ip": This is the destination IP address for the Event. Conditions include:
        - In
        - Not In
    - "host": This is the host for the Event. Conditions include:
        - In
        - Not In
    - "src_ip": This is the source IP address for the Event. Conditions include:
        - In
        - Not In

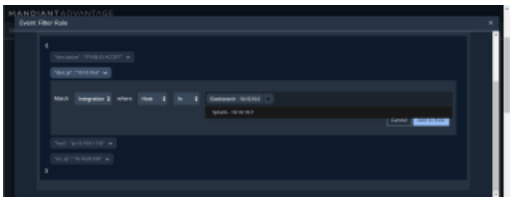
5. Select the Priority tab and order the Event Filter Rules based on how you want them to run.
6. Click **Save**.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880ba6445d5e3e714b3bec/n/json-event-filter-ex1.png)

Example of Event JSON tab

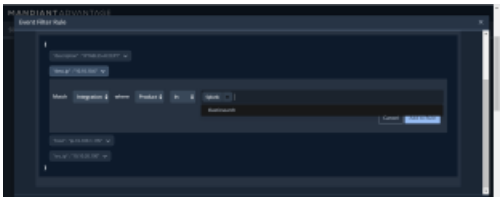
(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880ba6445d5e3e714b3bee/n/json-event-filter-ex2.png)

Example of Event Condition Options



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880ba6445d5e3e714b3bf0/n/json-event-filter-int-host-ex.png)

Example of Integration and Host Options



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62880ba7445d5e3e714b3bf2/n/json-event-filter-int-product-ex.png)

Example of Integration and Product Options

To edit an event filter rule

Changes to Event Filter Rules only apply to new Jobs, they do not change Jobs that ran before the rule was updated.

1. Locate the Event Filter Rules you want to change and click the edit Event Filter Rule option.
   - Go to **Settings** > **Integrations**. Select the filter's action menu and click **Edit Event Filter Rule**.
   - Scroll to the Event Filter Rule section of an Action. Select the filter's action menu and click **Edit Event Filter Rule**.
2. Modify any of the settings you want to change.
   - Override the System Setting (Action on Match)
   - Add / remove Conditions
   - Change the priority (change when the filter rule runs compared to other filter rules)
3. Click **Save**.

To Delete an event filter rule

Deleting Event Filter Rules do not change Jobs results.

1. Locate the Event Filter Rules you want to change and click **Delete**.
   - Go to **Settings** > **Integrations**. Select the filter's action menu and click **Delete**.
   - Scroll to the Event Filter Rule section of an Action. Select the filter's action menu and click **Delete**.
2. Confirm you want to delete by clicking **OK**.