

Create Rule to Set Alert Levels on the Cisco FindIT Kaseya Plugin

Introduction

The Cisco FindIT Kaseya Plugin is a module that installs on the Kaseya Virtual System Administrator (VSA). It tightly integrates the Cisco FindIT Network Manager with the Kaseya VSA, allowing for centralized management of the network. The plugin allows access to the powerful management features of FindIT including action management, dashboards, device discovery, network topology, remote device management, actionable alerts, and event history.

The Alerts page in the Cisco FindIT Kaseya Plugin web-based utility allows you to create rules that use FindIT events as a trigger to generate standard Kaseya alerts.

Create Rule ✕

Name ⓘ **Description** ⓘ
Required

For Events: **Event Type** **Event Severity** Include higher

Matching nodes: **Node** **Network** **Node Type**

Raise action: Ticket Alarm

Script **Agent Procedure** **Agent**

Email **Email Address**

[Create Rule](#)

In this scenario, a rule will be created to send out a Warning message for any events that would occur in all FindIT sites and devices to inform the user and take actions as necessary.

Objective

This article aims to show how to create a rule to set Alert levels on the Cisco FindIT Kaseya Plugin.

Applicable Devices

- FindIT Network Manager

- FindIT Network Probe

Software Version

- 1.1

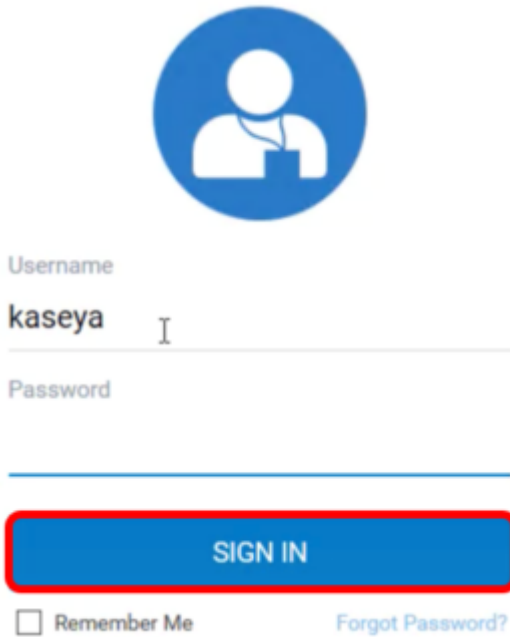
Create Rule to Set Alert Levels

Step 1. Launch a web browser and enter the IP address of your Kaseya VSA server on the address bar and then click **Enter**.



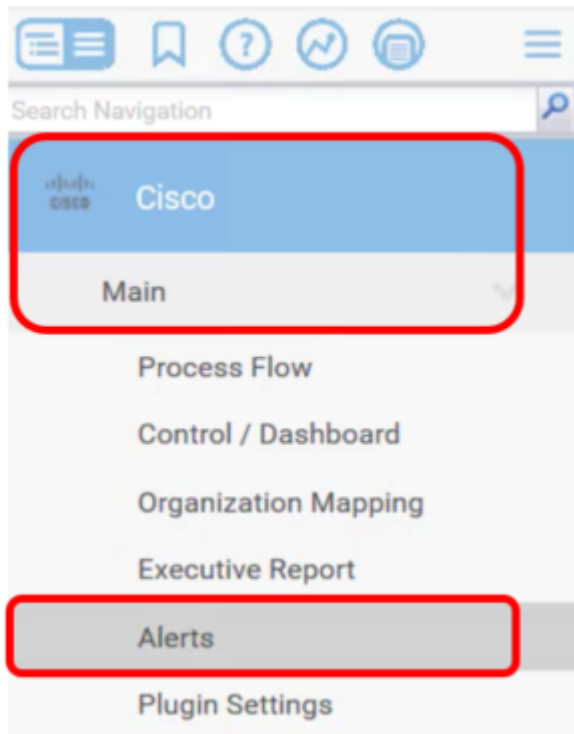
Note: In this example, the IP address used is 10.10.0.1

Step 2. Enter your Kaseya account login credentials in the *Username* and *Password* fields provided, and then click **SIGN IN**.

A screenshot of the Kaseya login page. At the top center is a blue circular icon containing a white silhouette of a person. Below the icon are two input fields: "Username" and "Password". The "Username" field contains the text "kaseya" and has a cursor at the end. Below the "Password" field is a blue horizontal line. At the bottom of the form is a blue button with the text "SIGN IN" in white, which is highlighted with a red rectangular border. Below the button are two links: "Remember Me" with an unchecked checkbox, and "Forgot Password?".

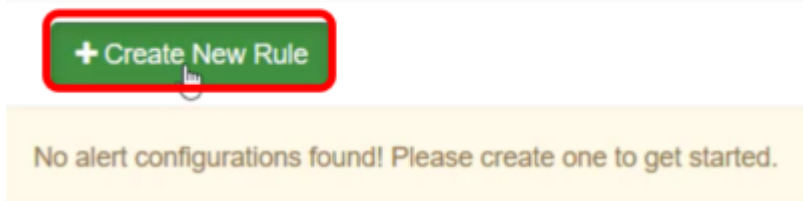
Note: In this example, *kaseya* is used as the Username.

Step 3. Choose **Cisco > Main > Alerts** in the Navigation Panel.



Step 4. Under FindIT Alerts, click on the **Create New Rule** button.

FindIT Alerts



The Create Rule page will then appear.

Step 5. In the *Name* field, enter the name that you want for the rule.

Name ⓘ

Note: In this example, *Warning Level* is entered.

Step 6. In the *Description* field, enter a description for the rule.

Description ⓘ

Note: In this example, *Warning or higher* is entered.

Step 7. Click on the Event Type drop-down menu in the For Events area to choose the type of event for the rule to apply.

For Events: **Event Type**

All

All

/action/reboot/accept

/action/reboot/fail

/action/reboot/progress

/action/reboot/complete

/action/backup/accept

Matching devices:

Raise action:

Note: In this example, *All* is chosen. This means that the Warning alert will be sent out whenever an event occurs, regardless of its type.

Step 8. Click the Event Severity drop-down menu to choose the severity.

Event Severity

All

All

Critical

Warning

Info

Note: In this example, *Warning* is chosen.

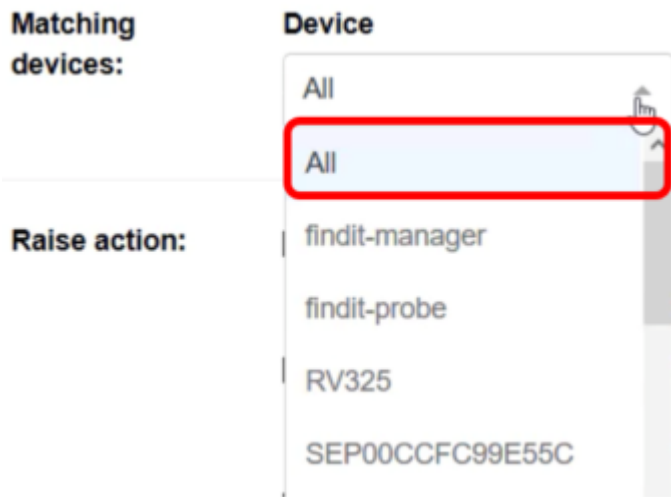
Step 9. (Optional) Check the **Include higher** check box if you want the rule to also apply when events occur that have higher severity than the one you have set.

Event Severity

Warning

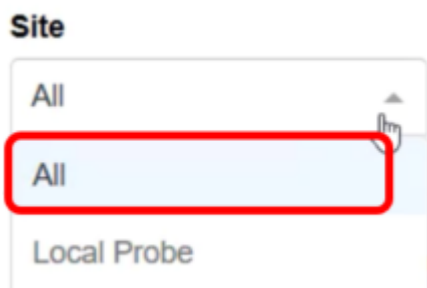
Include higher

Step 10. Click on the Device drop-down menu in the Matching devices area to choose the FindIT devices where the rule shall apply.



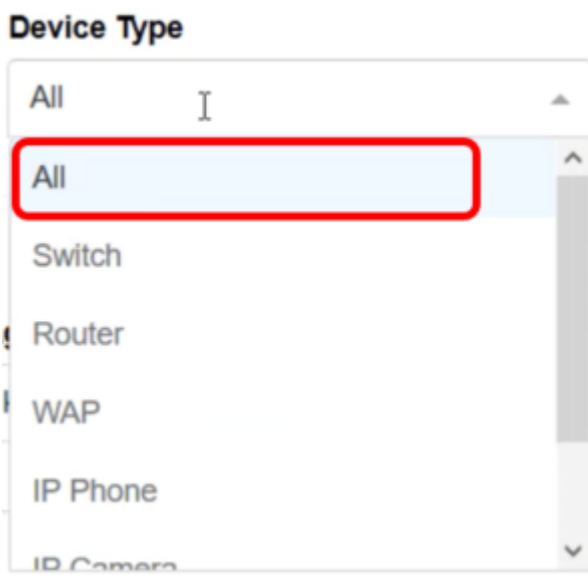
Note: In this example, *All* is chosen.

Step 11. Click on the Site drop-down menu to choose the FindIT site where you wish the rule to apply.



Note: In this example, *All* is chosen.

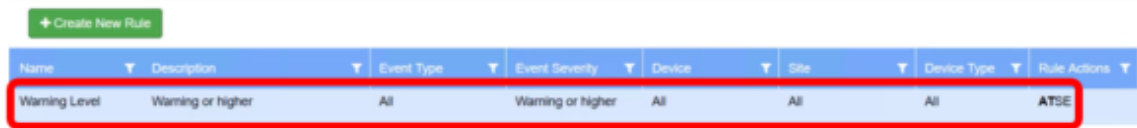
Step 12. Click on the Device Type drop-down menu to filter the FindIT devices where you wish the rule to apply depending on their type. In this example, *All* is chosen.



Note: The Raise action section is outside of the scope boundary as items correlate to functions outside of the plugin, thus, in Kaseya VSA itself.

Create Rule

Step 13. Click on the **Create Rule** button. When settings have been saved, the table showing the newly configured rule will now be visible in the FindIT Alerts page.



The screenshot shows a user interface for managing alerts. At the top left, there is a green button labeled '+ Create New Rule'. Below it is a table with a blue header and one data row. The data row is highlighted with a red border. The table columns are: Name, Description, Event Type, Event Severity, Device, Site, Device Type, and Rule Actions. The data row contains: Warning Level, Warning or higher, All, Warning or higher, All, All, All, and ATSE.

Name	Description	Event Type	Event Severity	Device	Site	Device Type	Rule Actions
Warning Level	Warning or higher	All	Warning or higher	All	All	All	ATSE

You now have successfully created a rule to set the Alert levels on the Cisco FindIT Kaseya Plugin.