

Mismatched Files

- Mismatched Files, on page 1

Mismatched Files

This alarm monitors the integrity of the software artifacts and files running on the device by verifying their hashes against the Known Good Values (KGVs) for the version of software running on the device. You can configure the number of mismatches that would trigger an alarm. To address mismatched files, you can investigate the device and look at which Cisco IOS XR version is running, who last deployed the file, where the file came from, and so on. To configure this alarm, do the following:

Procedure

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Mismatched Files**.

Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate the number of mismatched files that will trigger this alarm. Crosswork Cloud will send a notification if the number of mismatched files is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.

Mismatched Files