

Hardware Integrity Validation

• Hardware Integrity Validation, on page 1

Hardware Integrity Validation

This alarm monitors the number of Cisco Secure Unique Device Identifier (SUDI) certificate failures. The SUDI can be used as an unchangeable device identity for configuration, security, auditing, and management. It enables accurate, consistent, and electronic identification of Cisco products for asset management, provisioning, version visibility, service entitlement, quality feedback, and inventory management.

You specify the number of SUDI failures that will trigger an alarm. 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 **Hardware Integrity Validation**.

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 SUDI failures that will trigger this alarm.

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**.

Hardware Integrity Validation