View Assurance Audit Logs

View Audit Logs for Assurance

Audit logs are created to capture critical activities, such as when configuration changes were requested, when the configuration changes were executed, and if errors occurred during the configuration. For Assurance, audit logs are provided when configuration changes are made to Intelligent Capture, Issue Thresholds, Sensors, and AI Network Analytics.

To access the audit logs, choose **Activities** > **Audit Logs**. For a detailed procedure, see the "View Audit Logs" topic in the *Cisco DNA Center Administrator Guide*.

For Assurance, the following data is captured in the audit logs:

Table 1: Audit Logs

Item	Description
Date and Time	Date and time the log was received or executed.
Description	A brief description explaining the audit log.
User	The user that requested or executed the change.

Intelligent Capture Audit Logs

For Intelligent Capture, audit logs are provided to capture the following configuration changes:

- Enable or disable AP Statistics, globally.
- Enable or disable AP Statistics for a set of individual APs.
- Enable or disable Anomaly Capture, globally.
- Enable and disable Anomaly Capture for a set of individual APs.
- Enable or disable Spectrum Analysis.
- Enable or disable Scheduled Capture.
- Enable or disable Live Capture.

• Enable or disable Data Packet Capture.

If any errors occurred during the configuration, that information is also provided in the audit logs.

Issue Threshold Audit Logs

For issue threshold, audit logs are provided to capture the following updates:

• Updates on site health.

• Updates on the health score.

• Updates on the issue settings.

Sensor Audit Logs

For sensors, audit logs are provided to capture the following configuration requests:

• Received request to add test suite.

• Received request to update test suite.

• Received request to delete test suite.

• Received request to update tests for certificate bundle.

• Received request to add test status.

AI Analytics Audit Logs

For AI Analytics, audit logs are provided to capture the following AI agent configuration changes:

• Agent onboarded.

• Agent restored.

• Agent reconfigured.