LOGZILLA DOCUMENTATION

Iotops

LogZilla App Store application: Iotops

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/iotops

Overview

IoTOps provides unified IoT monitoring across all log sources. Events from IoT gateways, sensors, smart devices, and edge controllers are aggregated into a single dashboard with consistent severity levels.

App Function

- Aggregate IoT events from installed vendor apps
- Provide unified dashboard for cross-vendor IoT visibility
- Assign severity levels based on Event Type
- Alert on security threats and firmware updates

Vendor Documentation

This is a LogZilla aggregate app. No external vendor documentation applies.

Device Configuration

No device configuration is required. IoTOps automatically processes events from any app that sets `Event Class` containing `IoT`.

Incoming Log Format

IoTOps processes events tagged by vendor apps. It does not parse raw log formats directly. Vendor apps set:

- `Event Type`: Sensor, Telemetry, Firmware, Provisioning, Threat

Parsed Metadata Fields

Tag Name	Example	Description
`IoTOps Event`	`1`	Rollup tag for IoT events
`IoTOps Severity Level`	`High`	Aggregated severity based on Event Type

Severity Level Assignment

Severity	Condition
Critical	Threat, Policy Violation
High	Firmware updates, Provisioning
Medium	Sensor alerts, Telemetry anomalies

Log Examples

Sensor Alert

```
sensor-agent: Temperature threshold exceeded on device sensor-001
```

Firmware Update

```
ota-updater: Firmware update initiated for device gateway-01 v2.1.0
```

Unauthorized Device

```
iot-security: Unauthorized device MAC 00:11:22:33:44:55 detected
```

Dashboard

The IoTOps dashboard provides:

- Key metrics: Total events, threats, firmware, sensor events
- Unique devices and gateways
- EPS gauge and time chart for rate monitoring
- Event Type distribution over time
- Top devices, gateways, and vendors
- Severity distribution

- Live event stream with IoT context

Triggers

Trigger	Description
`IoTOps: Security Threat`	Unauthorized device or attack
`IoTOps: Policy Violation`	IoT policy breach
`IoTOps: Firmware Event`	Firmware update activity
`IoTOps: Provisioning Event`	Device provisioning
`IoTOps: Sensor Alert`	Sensor threshold exceeded