**Integrating AlertOps with ScienceLogic SL1**

**Introduction**

This document describes how to integrate AlertOps with ScienceLogic SL1 to automatically forward events and streamline incident management. By following the steps in this guide, you can configure SL1 to send detailed alert payloads to AlertOps, enabling centralized alert handling and response.

This section covers the following topics:

- What is AlertOps?
- What Does the AlertOps Integration Do?
- Installing and Configuring the AlertOps Integration
- **Experience: Using the Integration**

---

**What is AlertOps?**

AlertOps is an incident management and alerting platform designed to help organizations streamline their response to IT incidents and improve communication among teams. It centralizes alerts from various monitoring systems, automates workflows, and reduces alert fatigue, ultimately decreasing the mean time to resolution (MTTR) for critical issues.

---

**What Does the AlertOps Integration Do?**

The AlertOps integration for ScienceLogic SL1 uses a PowerPack to enable seamless communication between the two platforms.

**Features include:**

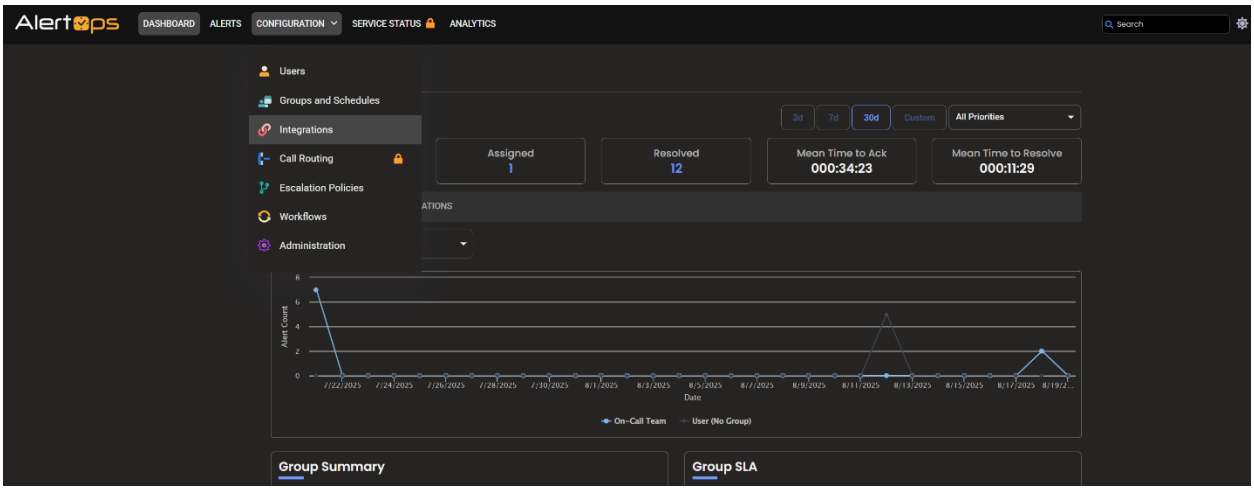
- **Runbook Actions**: Two Python-based snippets that post alert payloads to the AlertOps API.
- **Runbook Policies**: Two pre-configured policies to trigger the Runbook Actions for both critical events and event clearances.
- **Custom API Integration**: A dedicated inbound integration in AlertOps to receive and process alerts from SL1.

---

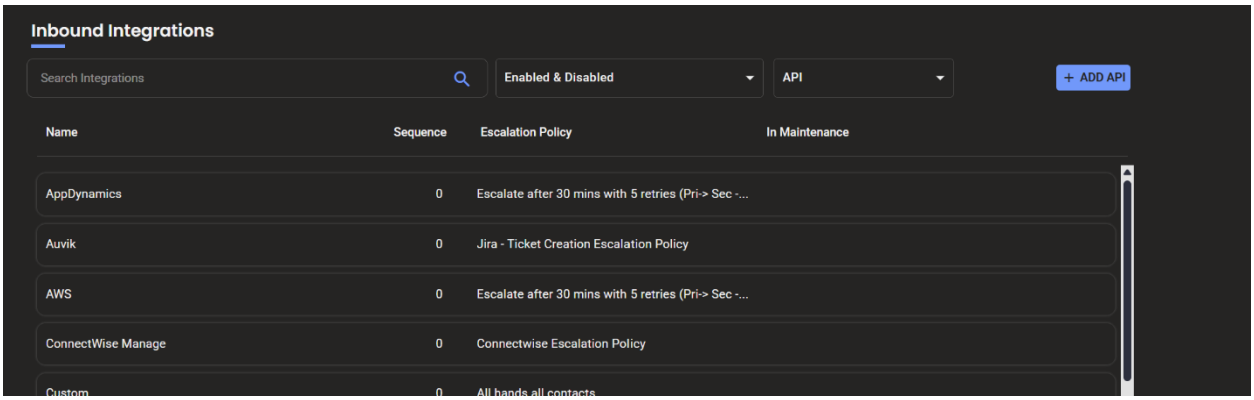
## Installing and Configuring the AlertOps Integration

### 1. Configure the Custom API Integration in AlertOps

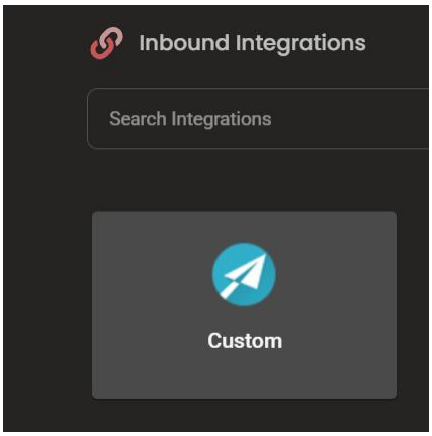
1. In AlertOps, navigate to **Configuration > Integrations**.



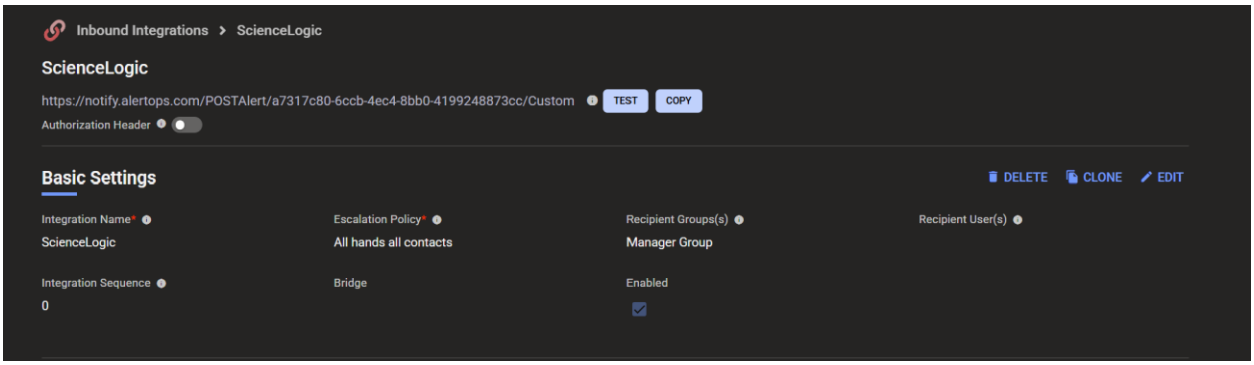

2. Select **Inbound Integrations**, then click **API** and choose **Add API**.




3. Create a **Custom API Integration** for SL1.



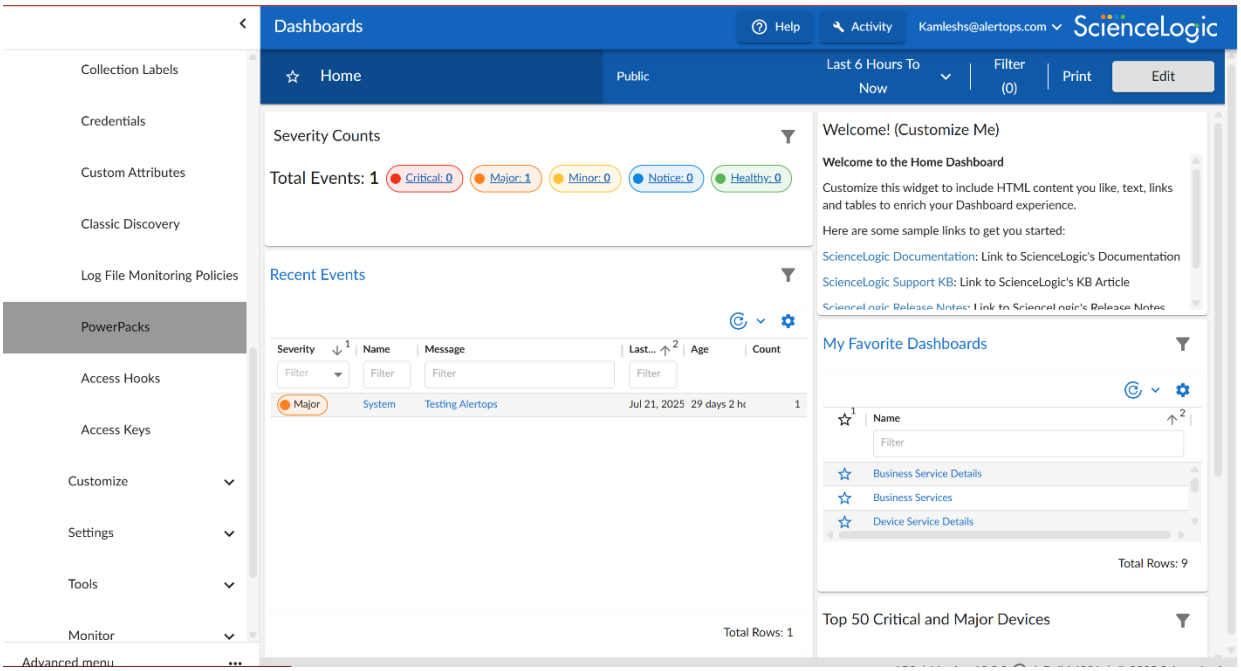
4. Assign an **Escalation Policy** and a **Recipient Group**.
5. Save the integration to generate a unique **API endpoint URL**. Copy this URL for use in the SL1 configuration.




---

## 2. Import the AlertOps PowerPack into ScienceLogic SL1

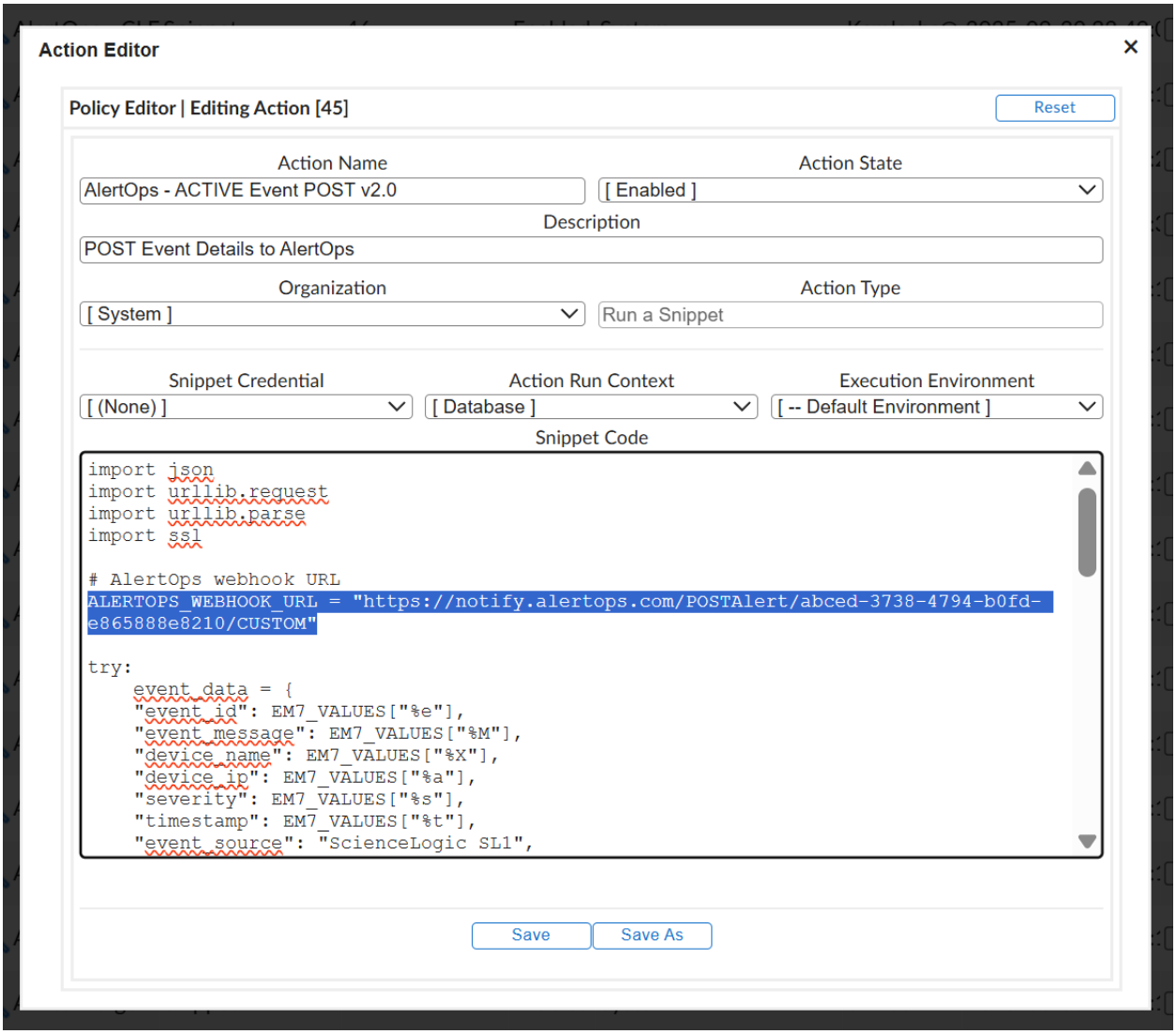
1. Log into SL1.
2. Navigate to **System > Manage > PowerPacks**.




3. Choose **Import PowerPack**.
4. Select the AlertOps PowerPack file and click **Import**.
5. Click **Install** in the PowerPack Installer modal.

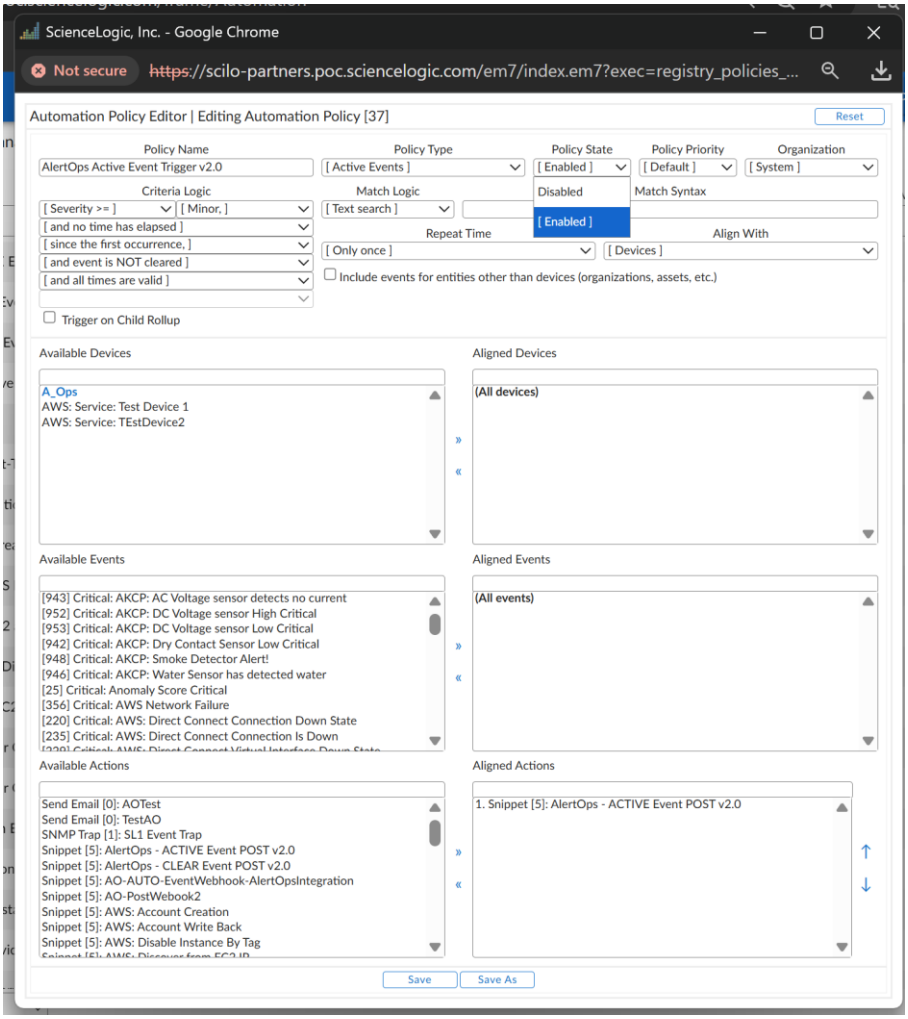
### 3. Configure the AlertOps Runbook Actions in SL1

1. In SL1, go to **Automation > Runbook Actions**.
2. Locate the two AlertOps snippets.
3. For each snippet, set the **ALERTOPS_WEBHOOK_URL** to the AlertOps API endpoint URL:
    1. **AlertOps – ACTIVE Event POST 2.0**
    2. **AlertOps – CLEAR Event POST 2.0**



## 4. Configure the AlertOps Runbook Policies

1. Navigate to **Registry > Runbook > Automations**.
2. Enable the following:
    - **AlertOps Active Event Trigger v2.0**
    - **AlertOps Clear Event Trigger v2.0**
3. Review and adjust devices and events to fit your alerting strategy.

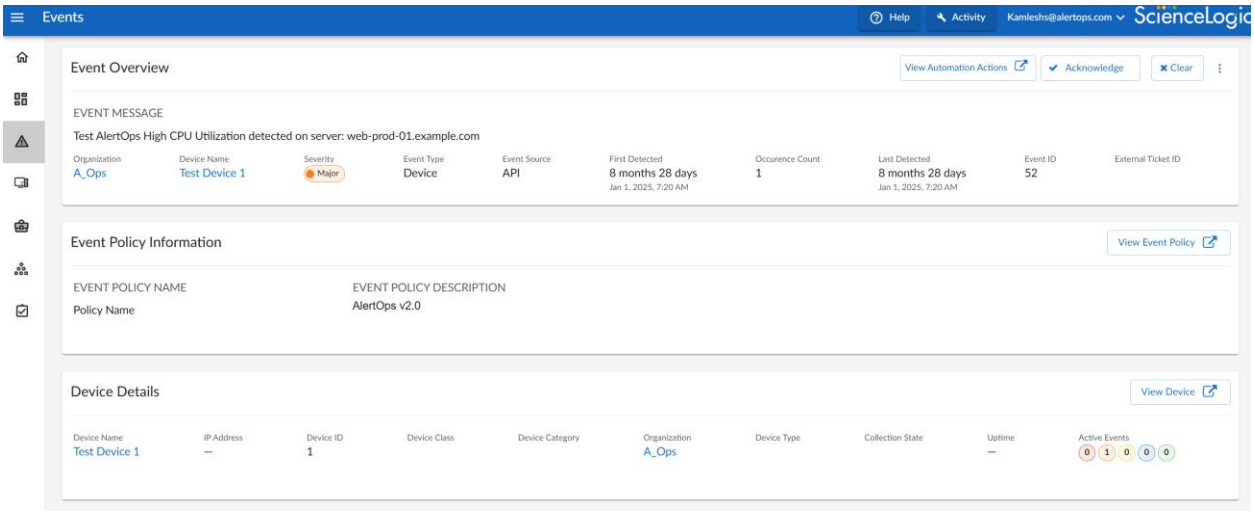


**Experience: Using the Integration**

Once configured, customers experience a **seamless event-to-resolution pipeline**.

**1. Event Triggered in SL1**

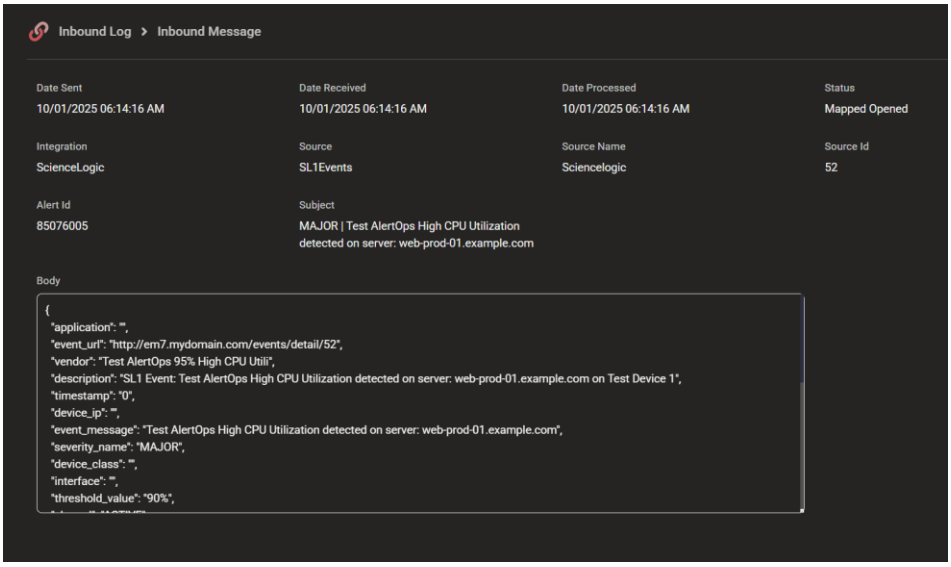
- A critical issue (e.g., CPU overload, service failure) is detected.
- The RBA Policy executes, sending event details to AlertOps.



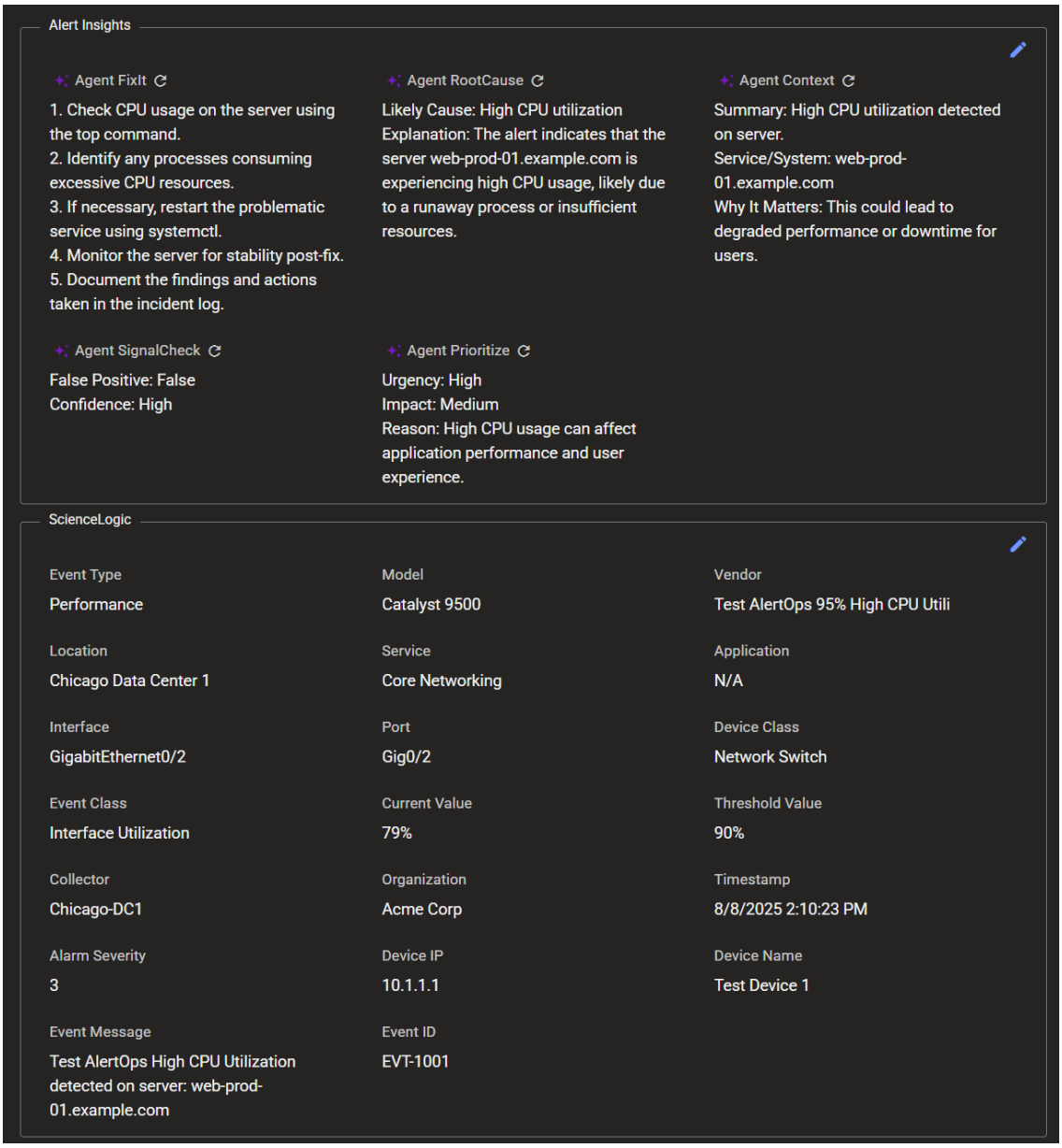

---

**2. Alert Created in AlertOps**

- AlertOps parses the payload, applies templates, and creates a grouped alert (if relevant).

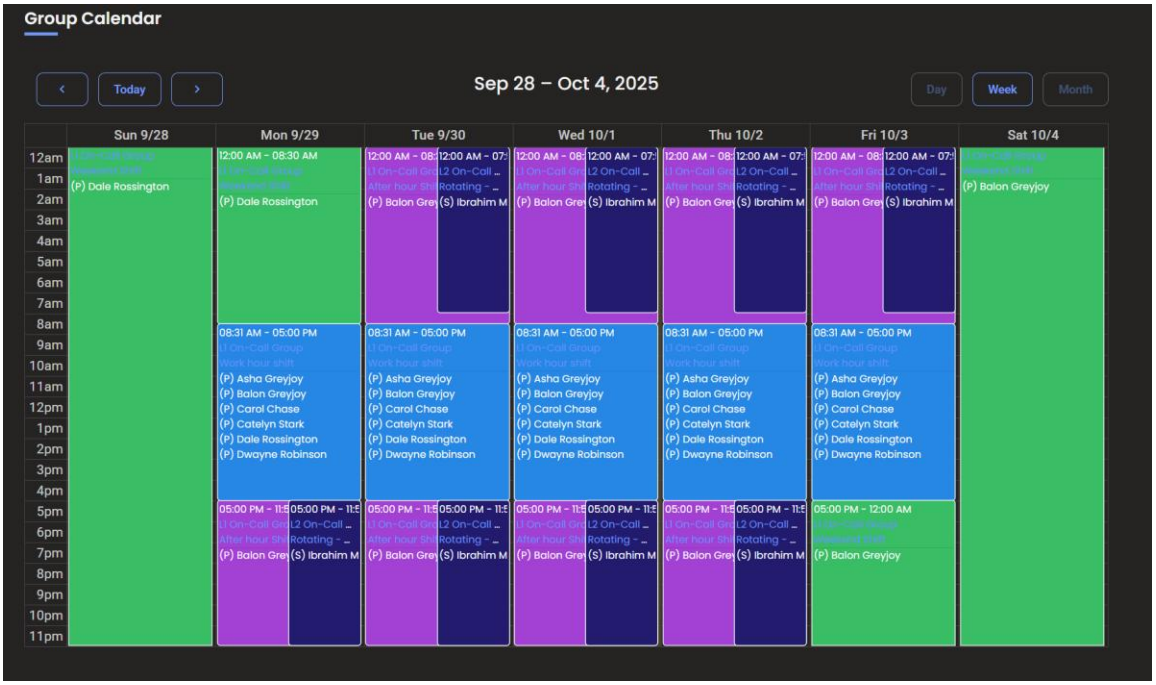



- The alert is enriched with metadata (time, source, severity, device).

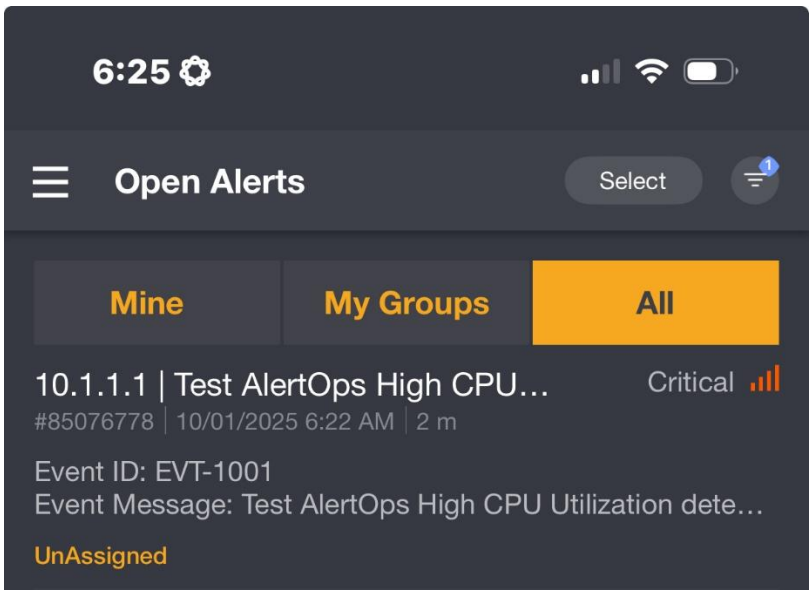

Alert Insights
Agent FixIt
1. Check CPU usage on the server using the top command.
2. Identify any processes consuming excessive CPU resources.
3. If necessary, restart the problematic service using systemctl.
4. Monitor the server for stability post-fix.
5. Document the findings and actions taken in the incident log.
Agent RootCause
Likely Cause: High CPU utilization
Explanation: The alert indicates that the server web-prod-01.example.com is experiencing high CPU usage, likely due to a runaway process or insufficient resources.
Agent Context
Summary: High CPU utilization detected on server.
Service/System: web-prod-01.example.com
Why It Matters: This could lead to degraded performance or downtime for users.
Agent SignalCheck
False Positive: False
Confidence: High
Agent Prioritize
Urgency: High
Impact: Medium
Reason: High CPU usage can affect application performance and user experience.
ScienceLogic
Event Type
Performance
Model
Catalyst 9500
Vendor
Test AlertOps 95% High CPU Utili
Location
Chicago Data Center 1
Service
Core Networking
Application
N/A
Interface
GigabitEthernet0/2
Port
Gig0/2
Device Class
Network Switch
Event Class
Interface Utilization
Current Value
79%
Threshold Value
90%
Collector
Chicago-DC1
Organization
Acme Corp
Timestamp
8/8/2025 2:10:23 PM
Alarm Severity
3
Device IP
10.1.1.1
Device Name
Test Device 1
Event Message
Test AlertOps High CPU Utilization detected on server: web-prod-01.example.com
Event ID
EVT-1001

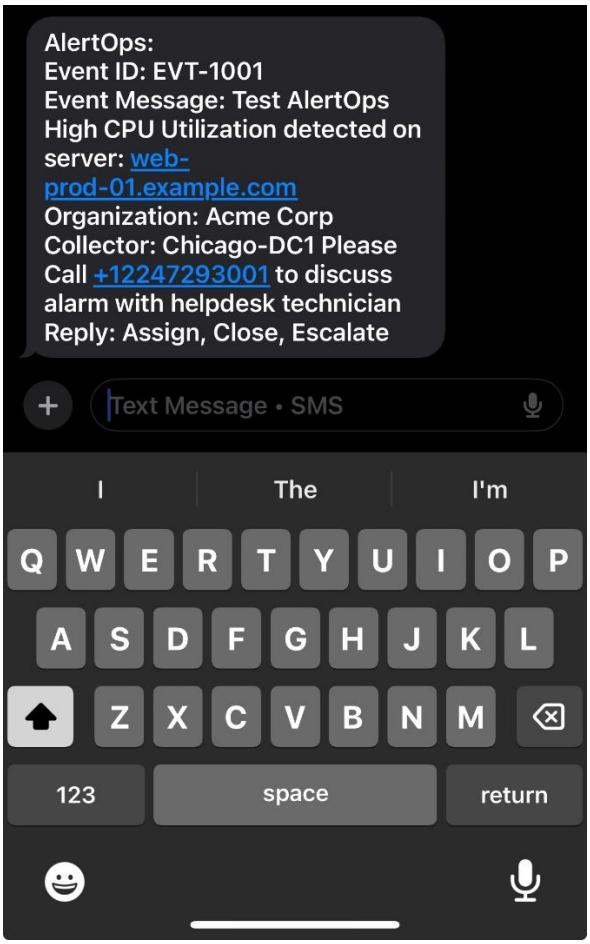
### 3. Multi-Channel Notifications

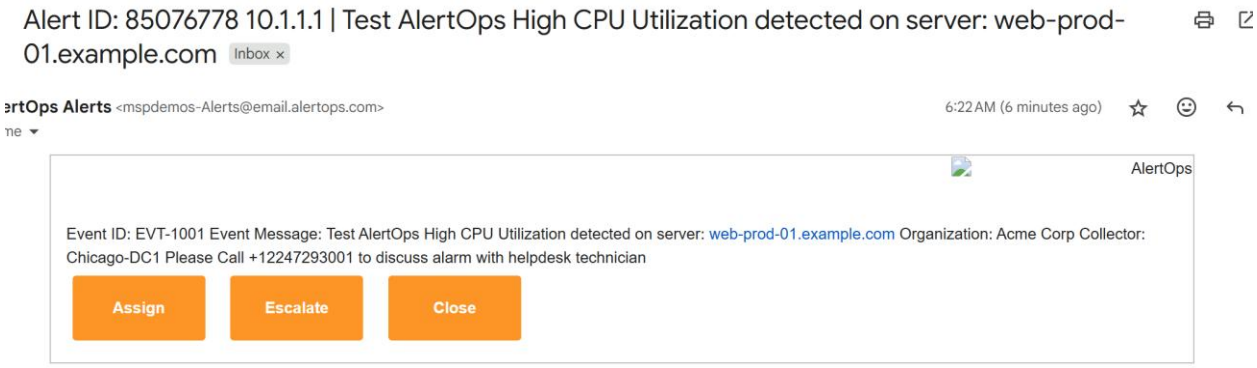
- AlertOps determines who the appropriate On-Call Member would be from the shifts.




- Primary on-call receives a notification through their preferred contacts such as **SMS , E-mail, Push Notification, and voice call**





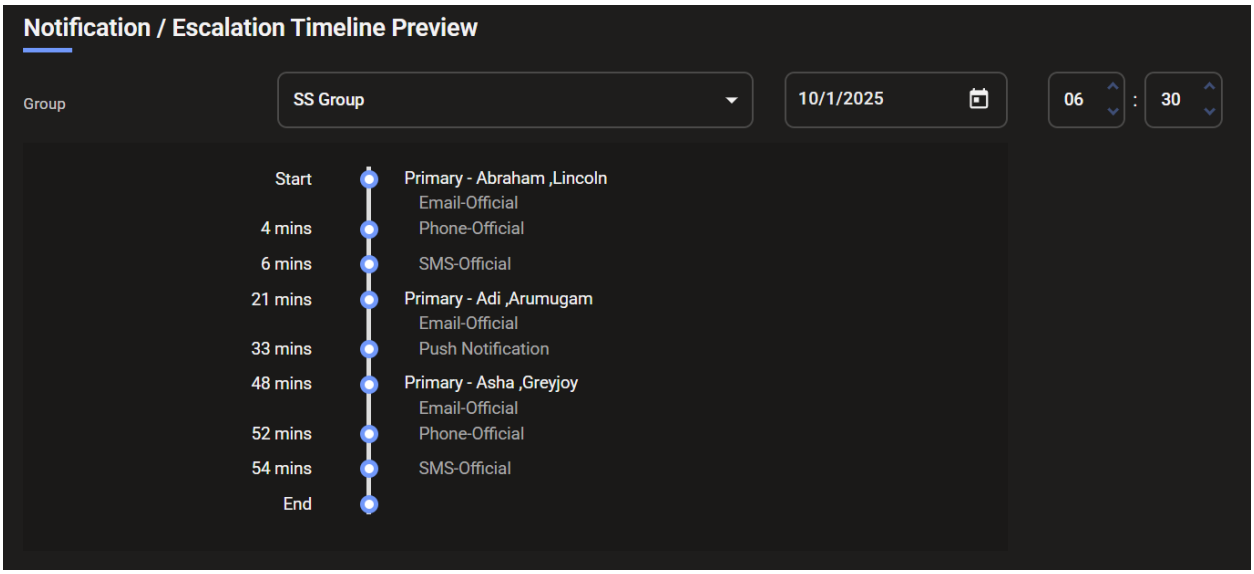




---

### 4. Escalation in Action

- If Primary does not acknowledge in X minutes, escalation automatically triggers.
- Secondary receives a **phone call + email**.

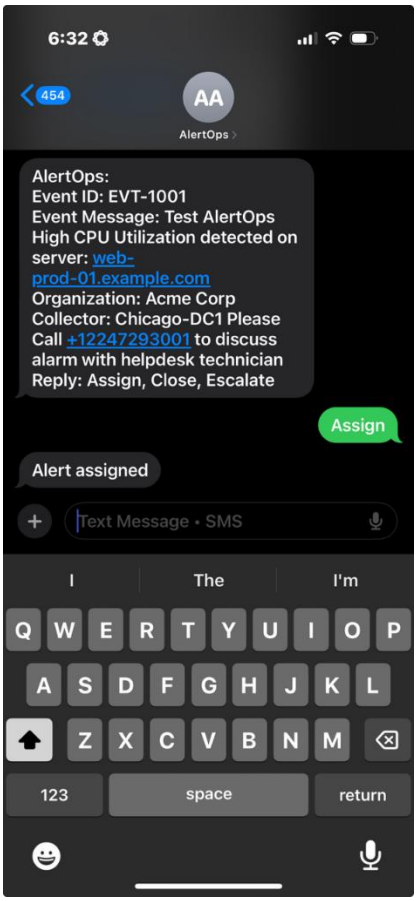
- Manager is notified if escalation reaches final stage.




---

### 5. Acknowledgement & Closure

- On-call acknowledges via **mobile app swipe**, **reply to SMS**, or **click in Slack/Teams** to prevent further escalation
- Once resolved in SL1 the AlertOps Alert will be Auto-Closed




---

**Customer Benefits in Daily Use**

- **Confidence**: Teams know every SL1 event reaches the right person.
- **Speed**: Escalations cut MTTA dramatically.
- **Clarity**: Centralized alert feed in AlertOps eliminates noise.
- **Mobility**: On-call can acknowledge directly from mobile or chat apps.
- **Accountability**: Audit trails show exactly who responded and when.