



---

# Anomaly Detection

SL1 version 12.3.0

---

# Table of Contents

<b>Introduction to Anomaly Detection</b> .....	<b>3</b>
What is Anomaly Detection? .....	4
Viewing Graphs and Data for Anomaly Detection .....	4
Using Anomaly Detection to Trigger Events .....	5
Using Anomaly Detection to Trigger Run Book Actions .....	6
<b>Enabling Anomaly Detection</b> .....	<b>7</b>
Configuring Anomaly Detection in SL1 .....	8
Running the Skylar SL1 Management Script .....	8
Enabling Anomaly Detection for an Organization .....	8
Viewing the List of Devices that Have Anomaly Detection Enabled .....	9
Enabling Anomaly Detection Events for Specific Metrics .....	9
Enabling Anomaly Detection Events for a Metric on the Device Investigator Page .....	9
Enabling Anomaly Detection Events for a Metric on the Service Investigator Page .....	10
Viewing Graphs and Data for Anomaly Detection .....	11
<b>Using Anomaly Detection to Trigger Events and Automations</b> .....	<b>13</b>
Creating an Event Policy for Anomalies .....	14
Using Anomaly-related Events to Trigger Automated Run Book Actions .....	15

## Introduction to Anomaly Detection

---



### Overview

The Anomaly Detection component of **Skylar Analytics** uses Skylar AI to identify unusual patterns that do not conform to expected behavior. Anomaly Detection provides always-on, unsupervised, machine-learning-based monitoring that automatically identifies unusual patterns in the real-time performance metrics and resource data that it observes.

You can view a list of all devices that have metrics being monitored for anomalies on the corresponding **Device Investigator** or **Service Investigator** pages.

**NOTE:** Unlike the Data Visualization and Exploration and Predictive Alerting components of Skylar Analytics, this release of Anomaly Detection with Skylar Analytics works on all Dynamic Applications in SL1. Data Visualization and Exploration as well as Predictive Alerting currently monitor server and network metrics, with more metrics planned for future SL1 releases.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter covers the following topics:

<a href="#">What is Anomaly Detection?</a> .....	4
<a href="#">Viewing Graphs and Data for Anomaly Detection</a> .....	4

---

## What is Anomaly Detection?

**Anomaly detection** is a technique that uses machine learning to identify unusual patterns that do not conform to expected behavior. Anomaly detection provides always-on, unsupervised machine learning-based monitoring that automatically identifies unusual patterns in the real-time performance metrics and resource data that it observes.

Anomalies do not necessarily represent problems or events to be concerned about; rather, they represent unexpected behavior that might require further investigation.

**NOTE:** Unlike the Data Visualization and Exploration and Predictive Alerting components of Skylar Analytics, this release of Anomaly Detection with Skylar Analytics works on *all* types of time-series performance metrics gathered by Dynamic Applications in SL1, with the exception of "Internal Collection" data types such as network interfaces. Data Visualization and Exploration and Predictive Alerting currently monitor server and network interface metrics, with more metrics planned for future SL1 releases.

Anomaly detection is calculated and displayed in the SL1 user interface for all Performance Dynamic Applications. This detection is enabled by default and cannot be disabled. You can control which device data gets sent to Skylar for analysis based on the organization aligned with the device or devices. All devices in the selected organization will get anomaly detection analysis.

For more information, see [Enabling Skylar Analytics for One or More SL1 Organizations](#).

---

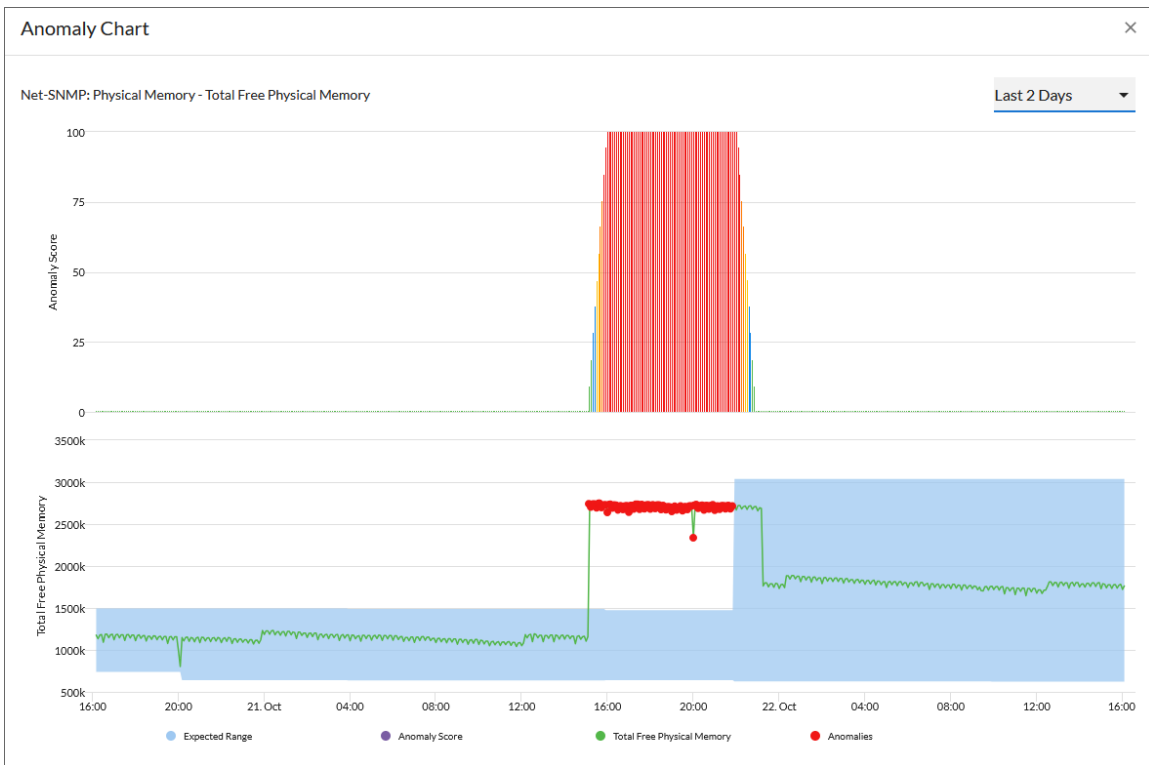
## Viewing Graphs and Data for Anomaly Detection

After SL1 begins performing anomaly detection for a device, you can view graphs and data about each anomaly. Graphs for anomalies appear on the following pages in SL1:

- The **Anomaly Detection** page, available from the Skylar AI (🔍) page.
- The **[Anomaly Detection]** tab in the **Device Investigator**.
- The **Anomalies** widget in the **Service Investigator** for a business, IT, or device service.

You can view the anomaly detection graphs for the metrics by clicking the **Open** icon (↗) next to the metric for the device. The **Anomaly Chart** modal appears, displaying the "Anomaly Score" chart above the chart for the specified metric you are monitoring.

The "Anomaly Score" chart displays a graph of values from 0 to 100 that represent how far the real data for a metric diverges from its normal patterns. The lines in the chart are color-coded by the severity level of the event that gets triggered as the data diverges further. The anomaly score is basically a running sum over a small window of time, so after anomalies stop, the score will drop to zero over that time.



The second graph displays the following data:

- A blue band representing the range of probable values that SL1 expected for the device metric.
- A green line representing the actual value for the device metric.
- A red dot indicating anomalies where the actual value appears outside of the expected value range.

You can hover over a value in one of the charts to see a pop-up box with the **Expected Range** and the metric value. The **Anomaly Score** value also displays in the pop-up box, with the severity in parentheses: Normal, Low, Medium, High, or Very High.

You can zoom in on a shorter time frame by clicking and dragging your mouse over the part of the chart representing that time frame, and you can return to the original time span by clicking the **[Reset zoom]** button.

## Using Anomaly Detection to Trigger Events

You can use anomaly detection to trigger an event or to add extra criteria to an event policy. For example, you could specify that if an anomaly occurs five times within 10 minutes, SL1 should trigger an event. For more information, see [Creating an Event Policy for Anomalies](#).

**TIP:** Because anomalies do not always correspond to problems, ScienceLogic recommends creating an event policy only for scenarios where anomalies appear to be correlated with some other behavior that you cannot otherwise track using an event or alert.

## Using Anomaly Detection to Trigger Run Book Actions

You can also use events based on anomaly detection to trigger run book automation actions that perform further diagnostics or send notifications. For more information, see [Using Anomaly-related Events to Trigger Automated Run Book Actions](#).



## Enabling Anomaly Detection

---

### Overview

This chapter describes how to enable anomaly detection events in SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter covers the following topics:

<a href="#">Configuring Anomaly Detection in SL1</a> .....	8
<a href="#">Viewing the List of Devices that Have Anomaly Detection Enabled</a> .....	9
<a href="#">Enabling Anomaly Detection Events for Specific Metrics</a> .....	9
<a href="#">Viewing Graphs and Data for Anomaly Detection</a> .....	11

---

## Configuring Anomaly Detection in SL1

Before you can start using Anomaly Detection, you will need to perform the following configurations in SL1:

- [Run the Skylar SL1 Management Script](#)
- [Enable Anomaly Detection for one or more organizations](#)

After you perform these configurations, you can access Anomaly Detection, Skylar Analytics, and other key Skylar AI components from the **Skylar AI** page (🔗) in SL1.

### Running the Skylar SL1 Management Script

The Skylar SL1 Management Script lets you set up your SL1 connectors and SL1 services for exporting data to Skylar. The script is named `sl-otelcol-mgmt.py`, and it is included with Skylar Analytics in the `sl-otelcol` package.

To run the Skylar SL1 Management Script:

1. Run the Skylar SL1 Management Script on the Database Server (an SL1 Central Database or an SL1 Data Engine):

```
sudo sl-otelcol-mgmt.py -vv skylar --skylar-metrics --skylar-config -  
-skylar-endpoint "https://skylar.com" --skylar-api-key "<Skylar-API-  
Key>" --ap2-feature-flags
```

where `<Skylar-API-Key>` is the API key for Skylar AI. Ask your ScienceLogic contact for this value.

After successfully running the script, on the **System Log** page (System > Monitor > System Logs), you will see "Info" messages for each configuration change. You will also see "Major" system log messages whenever connectivity fails for the Skylar endpoint or the OpenTelemetry Collector.

2. Continue to the next step to specify the organizations you want to use for exporting data to Skylar.

### Enabling Anomaly Detection for an Organization

In SL1, if you want to use Anomaly Detection and Predictive Alerting, you will need to select one or more organizations that will share data with Skylar AI. This data will come from all of the devices in a selected organization. By default, the Skylar AI features are disabled.

You can see which organizations are currently sending data to Skylar AI by going to the **Organizations** page (Registry > Accounts > Organizations) and looking at the **Skylar AI Status** column for the organizations.

To enable Anomaly Detection and Predictive Alerting:


1. In SL1, go to the **Organizations** page (Registry > Accounts > Organizations) and click the check box for one or more organizations.
2. In the **Select Action** drop-down, select *Send Data from Selected Orgs to Skylar AI* and click **[Go]** to start sending data about the selected organizations to Skylar AI. The **Skylar AI Status** column for the selected organizations changes to *Enabled*.



---

## Viewing the List of Devices that Have Anomaly Detection Enabled

The **Anomaly Detection** page displays a list of devices that are currently using anomaly detection, as well as devices for which you can enable anomaly detection if it is not enabled already.

To navigate to the **Anomaly Detection** page, click the **Skylar AI** icon (  ) and click the button for *Anomaly Detection*.

**TIP:** You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the *Introduction to SL1* manual.

**TIP:** You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the *Introduction to SL1* manual.

For each device in the list, the **Anomaly Detection** page displays the following information:

- **Device Name.** Displays the name of the device. Click the hyperlink to go to the **[Anomaly Detection]** tab of the **Device Investigator** page for that device. Each row on the **Anomaly Detection** page represents a specific device and metric for that device. As a result, a device might appear in the list multiple times if anomaly detection is enabled for multiple metrics on that device.
- **Metric Type.** Indicates the metric that SL1 is evaluating for anomalies on the device.
- **ML Enabled By User.** Indicates the username of the user that enabled anomaly detection for the device and metric.
- **Class.** Displays the Device Class for the device.
- **Category.** Displays the device's Device Category.
- **Anomaly Count.** Displays the number of anomalies detected by SL1.

---

## Enabling Anomaly Detection Events for Specific Metrics

You can set up anomaly detection events for specific metrics for devices and business services so that event policies are triggered when an anomaly is detected for that metric.

### Enabling Anomaly Detection Events for a Metric on the Device Investigator Page

To enable anomaly detection events for a metric on the **Device Investigator** page:

1. On the **Devices** page (📱), click the **Device Name** for the device on which you want to enable anomaly detection events. The **[Anomaly Detection]** tab for **Device Investigator** displays.

**TIP:** If the **[Anomaly Detection]** tab does not already appear on the **Device Investigator**, click the **More** drop-down menu and select it from the list of tab options.

2. On the **[Anomaly Detection]** tab, click the **Actions** icon (⚙️) for any of the listed metrics and select **Enable**. The **Select Available Metrics** modal appears.
3. In the **Select Metric** drop-down, use the **Search** field to search for a specific metric or click one of the category names, such as "Dynamic Apps" or "Collection Labels", to view a list of available metrics for that metric category.
4. Click the name of the metric on which you want to enable anomaly detection events for the device.
5. For some metrics, a second drop-down field might display that enables you to specify the device directory. If this field appears, click the name of the directory on which you want to enable anomaly detection.
6. Click **[Enable]**. That metric is enabled for events for that device.

**TIP:** To disable anomaly detection events for a metric, click the **Actions** icon (⚙️) for that metric and select **Disable**.

## Enabling Anomaly Detection Events for a Metric on the Service Investigator Page

On the **[Anomaly Detection]** tab on a **Service Investigator** page, you can enable anomaly detection events for additional metrics or disable anomaly detection metric events on which it is currently enabled.

**NOTE:** The **[Anomaly Detection]** tab appears only if you have at least one device in the selected service that has anomaly detection enabled.

To enable anomaly detection events for a metric on the **Service Investigator** page:

1. On the **Business Services** page (📁), select a service from the list of business, IT, and device services by clicking its name. The **Service Investigator** displays.
2. On the **Service Investigator** page, click the **[Anomaly Detection]** tab.
3. Click the **Actions** icon (⚙️) for any of the listed metrics and select **Enable**. The **Select Available Metrics** modal appears.
4. In the **Select Metric** drop-down, use the **Search** field to search for a specific metric or click one of the category names, such as "Dynamic Apps" or "Collection Labels", to view a list of available metrics for that metric category.
5. Click the name of the metric on which you want to enable anomaly detection events for the device.

6. For some metrics, a second drop-down field might display that enables you to specify the device directory. If this field appears, click the name of the directory on which you want to enable anomaly detection .
7. Click Enable.

**TIP:** To disable anomaly detection for a metric, click the **Actions** icon (⚙️) for that metric and select *Disable*. The metric is removed from the **[Anomaly Detection]** tab.

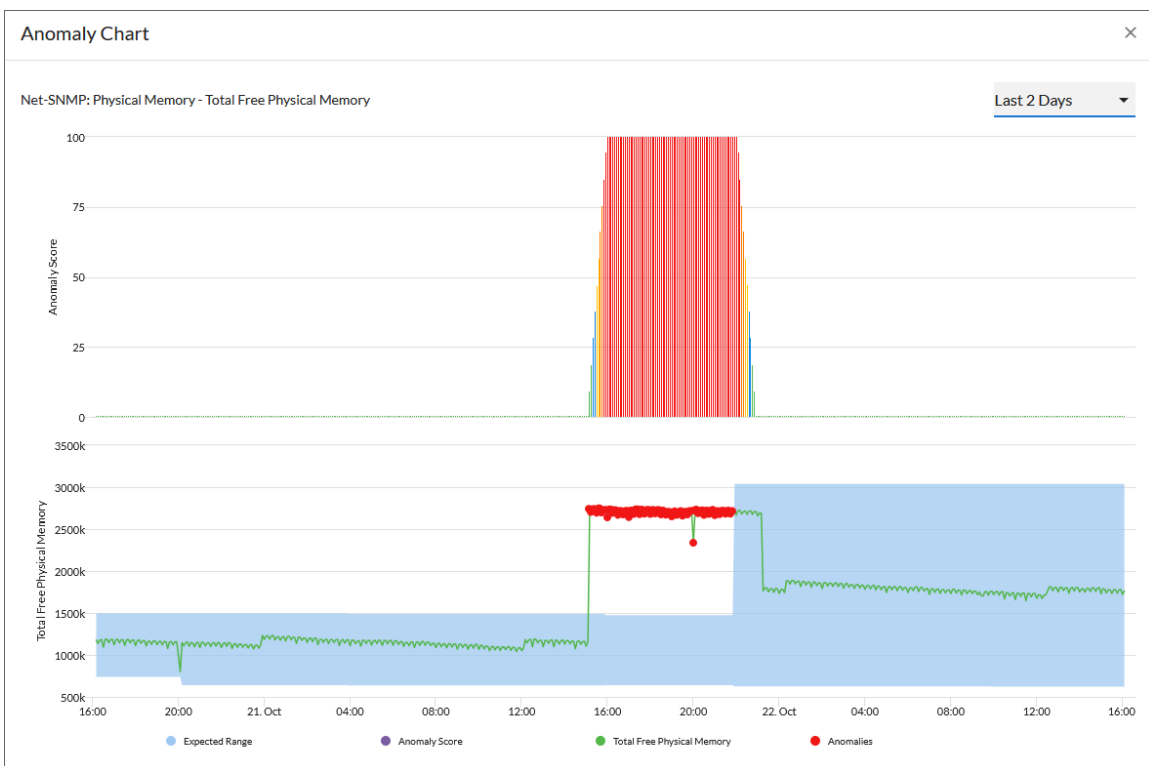
## Viewing Graphs and Data for Anomaly Detection

After SL1 begins performing anomaly detection for a device, you can view graphs and data about each anomaly. Graphs for anomalies appear on the following pages in SL1 :

- The **[Anomaly Detection]** tab in the **Device Investigator**.
- The **Anomalies** tab in the **Service Investigator** for a business, IT, or device service.

You can view the anomaly detection graphs for the metrics by clicking the **Open** icon (↗️) next to the metric for the device. The **Anomaly Chart** modal appears, displaying the "Anomaly Score" chart above the chart for the specified metric you are monitoring.

The "Anomaly Score" chart displays a graph of values from 0 to 100 that represent how far the real data for a metric diverges from its normal patterns. The lines in the chart are color-coded by the severity level of the event that gets triggered as the data diverges further. The anomaly score is basically a running sum over a small window of time, so after anomalies stop, the score will drop to zero over that time.



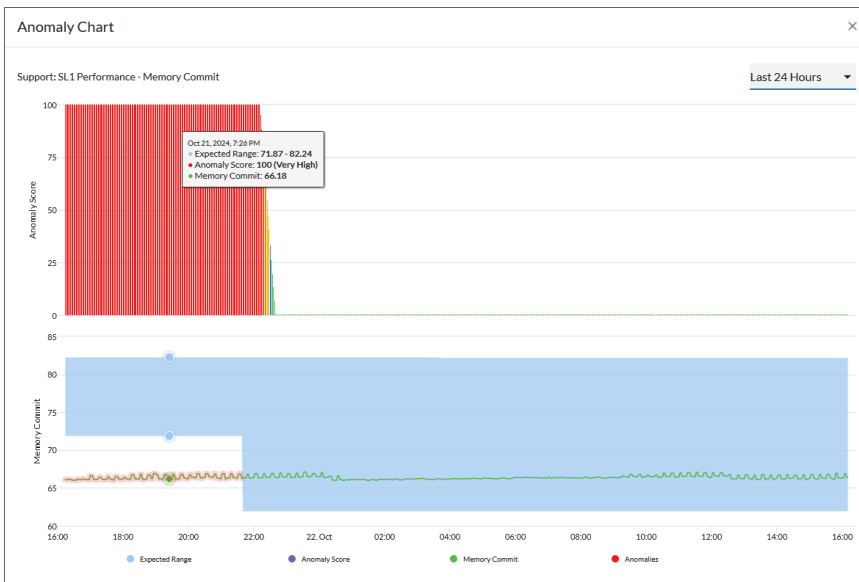
The second graph displays the following data:

- A blue band representing the range of probable values that SL1 expected for the device metric.
- A green line representing the actual value for the device metric.
- A red dot indicating anomalies where the actual value appears outside of the expected value range.

You can hover over a value in one of the charts to see a pop-up box with the **Expected Range** and the metric value. The **Anomaly Score** value also displays in the pop-up box, with the severity in parentheses: Normal, Low, Medium, High, or Very High.

You can zoom in on a shorter time frame by clicking and dragging your mouse over the part of the chart representing that time frame, and you can return to the original time span by clicking the **[Reset zoom]** button.

You can view the alert levels when you hover over a value in one of the charts on the **Anomaly Chart** modal. The Anomaly Score severity level displays after the index value, in parentheses: Normal, Low, Medium, High, or Very High:



**NOTE:** An Anomaly Score severity level of Normal is assigned to a value in the chart that is *lower* than the lowest enabled alert level. For example, if the threshold for the Low severity is enabled and set to 20 or higher, an Anomaly Score of 16 would have a severity level of Normal.



## Using Anomaly Detection to Trigger Events and Automations

---

### Overview

This chapter describes how to use anomaly detection to trigger events and automations in SL1 .

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (  ).

This chapter covers the following topics:

<a href="#">Creating an Event Policy for Anomalies</a> .....	14
<a href="#">Using Anomaly-related Events to Trigger Automated Run Book Actions</a> .....	15

## Creating an Event Policy for Anomalies

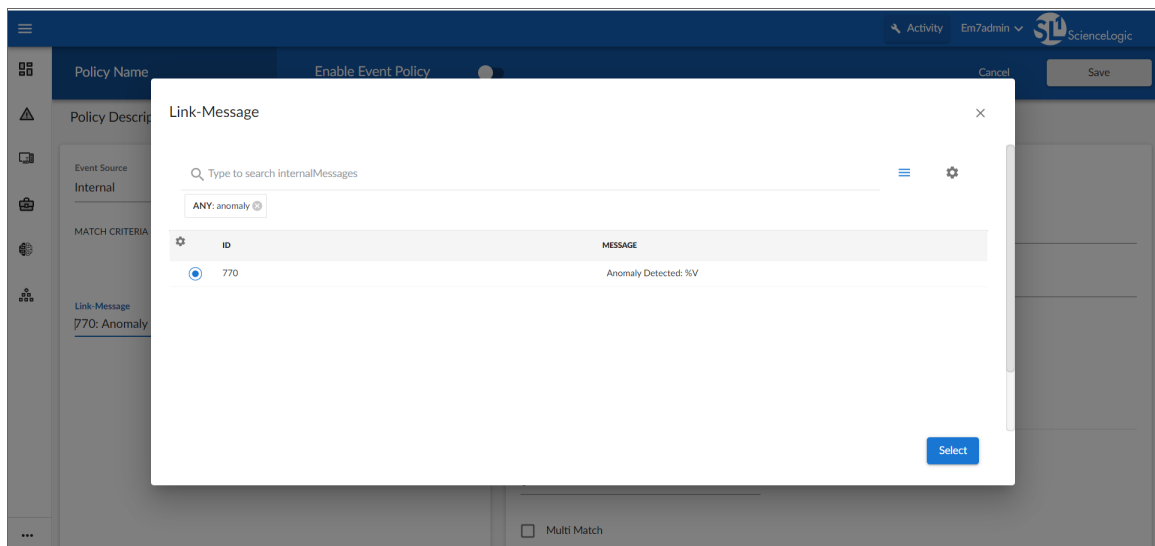
After you have enabled anomaly detection for devices, you can create additional event policies that will trigger events in SL1 when anomalies are detected for those devices.

**TIP:** Because anomalies do not always correspond to problems, ScienceLogic recommends creating an event policy only for scenarios where anomalies appear to be correlated with some other behavior that you cannot otherwise track using an event or alert.

**NOTE:** Because the anomaly detection model is constantly being refined as SL1 collects more data, you might experience a larger number of anomaly-related events if you create an event policy for anomalies soon after enabling anomaly detection compared to if you were to do so after SL1 has had an opportunity to learn more about the device metric's data patterns.

To create an event policy for anomalies:

1. Go to the **Event Policies** page (Events > Event Policies).
2. On the **Event Policies** page, click the **[Create Event Policy]** button. The **Event Policy Editor** page appears.
3. In the **Policy Name** field, type a name for the new event policy.
4. Click the **[Match Logic]** tab.
5. In the **Event Source** field, select *Internal*.
6. In the **Match Criteria** field, click the **[Select Link-Message]** button.
7. In the **Link-Message** modal page, search for "Anomaly" to locate the message "Anomaly Detected: %V":



8. Click the radio button for the message "Anomaly Detected: %V", and then click **[Select]**.
9. Complete the remaining fields and tabs in the **Event Policy Editor** based on the specific parameters that you want to establish for the event. For more information about the fields and tabs in the **Event Policy Editor**, see [Defining an Event Policy](#).
10. To enable the event policy, click the **Enable Event Policy** toggle so that it is in the "on" position.
11. When you are finished entering all of the necessary information into the event policy, click **[Save]**.

## Using Anomaly-related Events to Trigger Automated Run Book Actions

SL1 includes automation features that allow you to define specific event conditions and the actions you want SL1 to execute when those event conditions are met. You can use these features to trigger automated run book actions whenever an anomaly-related event is generated in SL1.

To use anomaly-related events to trigger automated run book actions:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the **[Create]** button. The **Automation Policy Editor** page appears:

The screenshot shows the 'Automation Policy Editor' interface for creating a new policy. The browser address bar shows the URL: https://10.128.88.92/em7/index.em7?exec=registry\_policies\_automation\_editor&height=700&wid=... The page title is 'Automation Policy Editor | Creating New Automation Policy'. A 'Reset' button is in the top right corner.

The form contains the following sections:

- Policy Name:** Anomaly High
- Policy Type:** Active Events
- Policy State:** Enabled (highlighted with a red box)
- Policy Priority:** Default
- Organization:** Sample
- Criteria Logic:**
  - Severity >= [Minor]
  - and 5 minutes has elapsed
  - since the first occurrence
  - and event is NOT cleared
  - and all times are valid
- Match Logic:** Text search
- Match Syntax:** (empty)
- Repeat Time:** Only once
- Align With:** Devices
- Include events for entities other than devices (organizations, assets, etc.)
- Trigger on Child Rollup
- Available Devices:** Sample, AWS: Service: test, ScienceLogic, Inc.: EM7 Data Collector: mrktng-dc1, ScienceLogic, Inc.: EM7 Data Collector: mrktng-dc2, System
- Aligned Devices:** All devices
- Available Events:** anom, [1768] Critical: Anomaly Score Critical - new york, [18] Minor: Anomaly Score Minor, [17] Notice: Anomaly Score Notice (this section is highlighted with a red box)
- Aligned Events:** [20] Critical: Anomaly Score Critical, [19] Major: Anomaly Score Major
- Available Actions:** SNMP Trap [1]: SL1 Event Trap, Snippet [5]: Automation Utilities: Calculate Memory Size for Ea, Snippet [5]: AWS: Account Creation, Snippet [5]: AWS: Account Write Back, Snippet [5]: AWS: Disable Instance By Tag
- Aligned Actions:** (empty)

A 'Save' button is located at the bottom center of the form.

3. In the **Policy State** field, select *Enabled*.
4. In the **Available Events** field, search for and select an anomaly-related event policy, and then click the right-arrow icon to move it to the **Aligned Events** field. For more information about anomaly-related events, see [Creating an Event Policy for Anomalies](#).
5. Complete the remaining fields on the **Automation Policy Editor** page based on the specific parameters that you want to establish for the automation policy. For more information about the fields on the **Automation Policy Editor** page, see [Automation Policies](#).
6. When you are finished, click **[Save]**.



© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

#### Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

#### Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: [legal@sciencelogic.com](mailto:legal@sciencelogic.com). For more information, see <https://sciencelogic.com/company/legal>.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010