



MURAL Anomaly Analysis User Guide

Version 3.9

Published: 2016-09-30

Copyright © 2016, Cisco Systems, Inc.

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706 USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

MURAL Anomaly Analysis User Guide

Copyright © 2016, Cisco Systems, Inc. All rights reserved.

Table of Contents

| | |
|---|----------|
| Introducing Anomaly Analysis | 1 |
| Viewing the Anomaly Tab | 1 |
| Managing Anomaly Rules | 5 |
| Viewing Rules | 5 |
| Configuring Rules | 6 |
| Understanding Thresholds | 6 |
| Setting Threshold Granularity | 7 |
| Deleting Rules | 7 |
| Monitoring Anomalies | 9 |
| Sorting Notifications | 9 |

Introducing Anomaly Analysis

Anomalies are events which exceed the expected value of a measure (baseline). The primary goal of this feature is to identify anomalies under a specified scope of interest to improve system health according to Key Performance Indicators (KPIs).

A detection algorithm runs across designated network attributes and compares data over a specified time interval. These values are compared against a baseline to find deviations (anomalies) in the data. Detected anomalies are assigned a severity rating according to the severity assigned to the rule.

Viewing the Anomaly Tab

The **Anomaly** tab has two views:

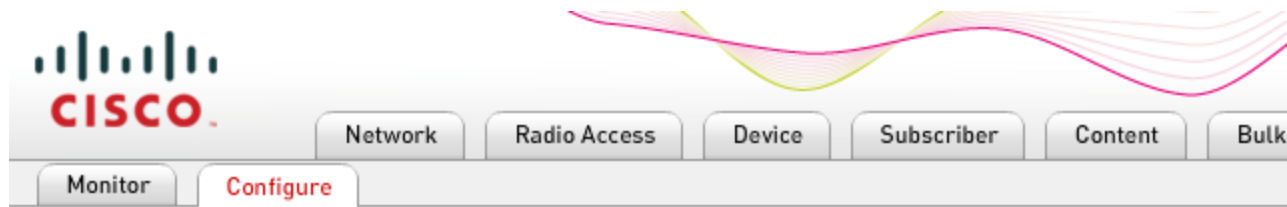
- The **Monitor** view displays all instances in which an anomaly was found, according to the defined rules. Anomalies are displayed in a table which can be sorted by column, individual items deleted, or the page refreshed.



| Severity | Time Stamp ▼ | Rule Name | Granularity | |
|----------|-------------------|---------------------------|-------------|--------------------|
| ● | 31 Jan 2015 23:00 | DC_Susbc | Hourly | Gateway: GMPLAB |
| ● | 30 Jan 2015 03:00 | hourly_static_lessThan | Hourly | App Category: Pro |
| ● | 30 Jan 2015 03:00 | hourly_static_lessThan | Hourly | App Category: Pro |
| ● | 30 Jan 2015 03:00 | hourly_static_lessThan | Hourly | App Category: Pro |
| ● | 30 Jan 2015 03:00 | hourly_static_lessThan | Hourly | App Category: Pro |
| ● | 30 Jan 2015 03:00 | hourly_static_lessThan | Hourly | App Category: Pro |
| ● | 30 Jan 2015 03:00 | hourly_static_lessThan | Hourly | App Category: Pro |
| ● | 30 Jan 2015 02:00 | mmtestrule | Hourly | Protocol: Jabber, |
| ● | 30 Jan 2015 02:00 | 4dims | Hourly | Traffic Type Categ |
| ● | 30 Jan 2015 02:00 | filesharing_hourly | Hourly | Traffic Type Categ |
| ● | 30 Jan 2015 02:00 | GERAN_Subscr | Hourly | Radio Access Type |
| ● | 30 Jan 2015 02:00 | hourly_static_greaterThan | Hourly | Protocol: Jabber, |
| ● | 30 Jan 2015 02:00 | filesharing_hourly | Hourly | Traffic Type Categ |
| ● | 30 Jan 2015 02:00 | mmtestrule | Hourly | Protocol: Jabber, |
| ● | 30 Jan 2015 02:00 | 4dims | Hourly | Traffic Type Categ |
| ● | 30 Jan 2015 02:00 | GERAN_Subscr | Hourly | Radio Access Type |
| ● | 30 Jan 2015 02:00 | mmtestrule | Hourly | Protocol: Jabber, |
| ● | 30 Jan 2015 02:00 | filesharing_hourly | Hourly | Traffic Type Categ |
| ● | 30 Jan 2015 02:00 | GERAN_Subscr | Hourly | Radio Access Type |
| ● | 30 Jan 2015 02:00 | 4dims | Hourly | Traffic Type Categ |

- The **Configure** view lists the rules with the measured value and defined

thresholds. Rules are displayed in a table which can be sorted by column, created, edited, deleted, or the page refreshed.



| Severity | Rule Name ▲ | Range | Granularity | 5 |
|----------|-------------------------------|---------------------------------------|-------------|------|
| ● | 4dms | 29 Jan 2015 10:00 - 02 Apr 2015 10:00 | Hourly | Expi |
| ● | DC_Susbcr | 27 Jan 2015 00:00 - 28 Feb 2015 00:00 | Hourly | Expi |
| ● | GERAN_Subscr | 27 Jan 2015 00:00 - 28 Feb 2015 00:00 | Hourly | Expi |
| ● | Prashant | 01 Feb 2015 21:00 - 03 Feb 2015 21:00 | Hourly | Expi |
| ● | daily_movingAvg_equals | 28 Jan 2015 00:00 - 07 Jun 2015 00:00 | Daily | Acti |
| ● | daily_movingAvg_greaterThan | 28 Jan 2015 00:00 - 07 Jun 2015 00:00 | Daily | Acti |
| ● | daily_movingAvg_lessThan | 28 Jan 2015 00:00 - 07 Jun 2015 00:00 | Daily | Acti |
| ● | daily_static_equal | 31 Jan 2015 00:00 - 10 May 2015 00:00 | Daily | Acti |
| ● | daily_static_greaterThan | 28 Jan 2015 00:00 - 07 Jun 2015 00:00 | Daily | Acti |
| ● | daily_static_greaterThan_4... | 03 Feb 2015 00:00 - 07 Jul 2015 00:00 | Daily | Acti |
| ● | daily_static_lessThan | 31 Jan 2015 00:00 - 11 May 2015 00:00 | Daily | Acti |
| ● | filesharing_hourly | 27 Jan 2015 00:00 - 28 Feb 2015 00:00 | Hourly | Expi |
| ● | hourly_MovingAvg_equal | 28 Jan 2015 03:00 - 31 May 2015 03:00 | Hourly | Acti |
| ● | hourly_decMovingAvg | 31 Jan 2015 23:00 - 09 May 2015 22:00 | Hourly | Acti |
| ● | hourly_incMovingAvg | 28 Jan 2015 03:00 - 31 May 2015 03:00 | Hourly | Acti |
| ● | hourly_static_equal | 31 Jan 2015 23:00 - 06 Jun 2015 22:00 | Hourly | Expi |
| ● | hourly_static_greaterThan | 28 Jan 2015 03:00 - 30 Apr 2015 03:00 | Hourly | Expi |
| ● | hourly_static_lessThan | 28 Jan 2015 03:00 - 30 Apr 2015 03:00 | Hourly | Expi |
| ● | hourly_static_lessThan2 | 31 Jan 2015 23:00 - 09 May 2015 22:00 | Hourly | Expi |
| ● | mmtestrule | 29 Jan 2015 23:00 - 31 Mar 2015 23:00 | Hourly | Expi |
| ● | monthly_movingAvg_equals | 01 Jan 2015 00:00 - 01 Jan 2015 00:00 | Monthl | Acti |

Note: Not all users are allowed to configure rules. If you do not have an administrator account, the Configure tab displays a message stating that "Only administrators are authorized to configure alerts."

Managing Anomaly Rules

Anomaly detection is based on finding variances between a measured value and an expected value (baseline). This section explains the rules and values which define the baseline.

Note: The maximum number of active rules that can be in the system at any given time is 25.



Viewing Rules

1. Click on the **Configure** tab. The screen refreshes with a new table.
2. The table lists all active Rules and their values, such as:
 - **Severity**—A method of ranking the rules and their results according to the user's perception of the impact to system health when the measure crosses the set threshold.
 - **Rule Name**—Designated name for the anomaly rule.
 - **Range**—Time range which is checked for crossing the threshold.
 - **Granularity**—Size of the data sets being evaluated by this rule.
 - **Status**—Determines if the rule is being run.

Note: The maximum number of anomalous events that can be detected by the system for a rule is 10. After identifying 10 events, the rule becomes inactive.

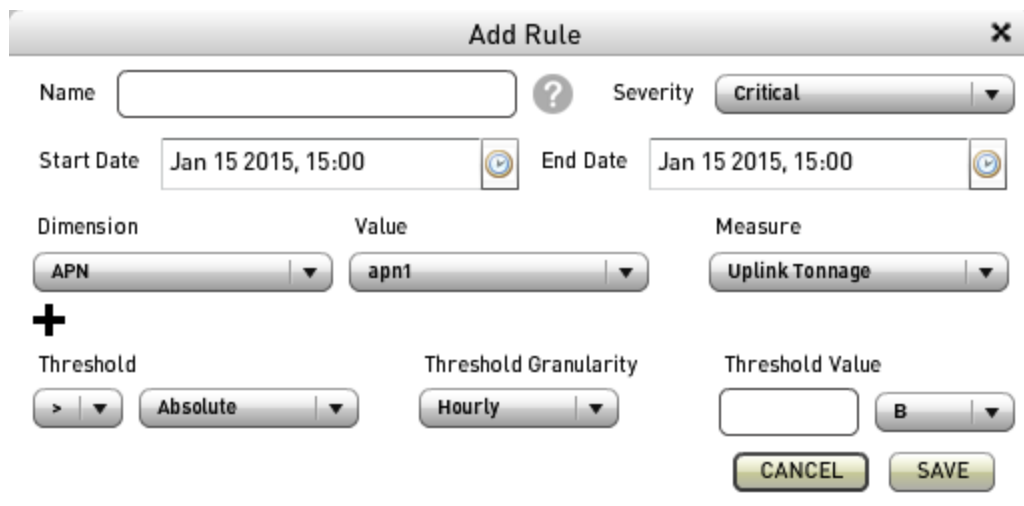
- **Dimension**—Parameters defining parts of the network which should be checked against this rule.
- **Measure**—The type of data which should be checked against this alert rule.
- **Condition**—How the threshold is compared to the data set. Determining if the data is less than, equal to, or greater than the threshold.
- **Threshold**—Specific number or a rolling average which represents

the baseline, or normal value, of the specified measure.

- **Edit/Delete**—Two icons for actions that can be performed on this alert rule: edit  and delete .

Configuring Rules

To add a rule, click the **Add Rule** button in the top-right corner of the **Configure** view. The main window is greyed out and the window below appears.



The screenshot shows the 'Add Rule' configuration window. It includes the following fields and controls:

- Name:** An empty text input field.
- Severity:** A dropdown menu set to 'critical'.
- Start Date:** A date and time picker set to 'Jan 15 2015, 15:00'.
- End Date:** A date and time picker set to 'Jan 15 2015, 15:00'.
- Dimension:** A dropdown menu set to 'APN'.
- Value:** A dropdown menu set to 'apn1'.
- Measure:** A dropdown menu set to 'Uplink Tonnage'.
- Threshold:** A dropdown menu set to '>'.
- Threshold Granularity:** A dropdown menu set to 'Absolute'.
- Threshold Value:** An empty text input field.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom right.

Note: Before setting the Threshold, Threshold Granularity, or Threshold Value, review the next two sections:

- "Understanding Thresholds" below
- "Setting Threshold Granularity" on the facing page

Understanding Thresholds

The baseline is a threshold defined by the user for each rule. There are two methods of defining the baseline:

- **Static value**—A non-variant number.
- **Temporal Moving Average**—A variant number, determined by averaging the last N (three) values for the specified interval being analyzed.

Setting Threshold Granularity

The time series is broken into hourly intervals, making it the smallest increment that can be used to analyze anomalies. The granularity for thresholds within rules are Hourly, Daily, and Monthly.

If using the Temporal Moving Average as the rule threshold, the formula to determine the baseline will be a rolling average of:

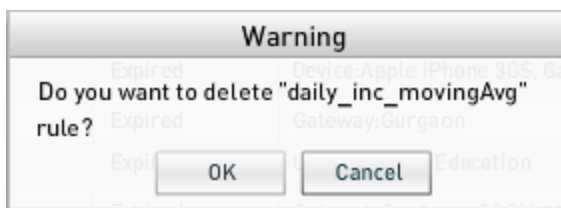
- **Hourly**—Hourly data-points from the same time and day of the last three weeks
- **Daily**—Daily data-points from the same day of the previous three weeks
- **Monthly**—Monthly data-points from the last three months

Note: If using a Temporal Moving Average threshold value, the amount of time defined in these formulas is also the amount of time the system requires to "learn" the rule after it is created. So if you create a rule that averages the last three months for the baseline, the rule will not identify anomalies until three months after it was created.


Deleting Rules

Delete an rule by clicking on the delete icon (🗑️) in the **Edit/Delete** column.

Before it deletes the rule, a pop-up appears warning you what the system is about to do.



Modifying Anomaly Rules

1. Click the edit  button for the rule you want to change. The **Edit Rule** pop-up window appears showing the current settings.

Edit Rule [X]

Name: ? Severity:

Start Date: End Date:

| Dimension | Value | Measure |
|--|---|--|
| <input type="text" value="App Type"/> | <input type="text" value="Browser"/> | <input type="text" value="Total Tonnage"/> |
| <input type="text" value="URL Category"/> | <input type="text" value="Health and Fitness"/> | |
| <input type="text" value="Service Provider"/> | <input type="text" value="crossfit.com"/> | |
| <input type="text" value="Gateway"/> | <input type="text" value="Gurgaon"/> | |
| <input type="text" value="Radio Access Type"/> | <input type="text" value="UTRAN"/> | |

Threshold: Absolute

Threshold Granularity:

Threshold Value: GB

Note: Fields which are greyed out cannot be changed. This is because changing these fields would result in the three hours, days, or months learning cycle starting over. Only the Threshold Value can be modified without causing this reset.

2. Apply necessary changes.
3. Select **Save** to apply your changes or **Cancel** to discard them. You can also cancel your changes by clicking the **X** in the top-right corner to close the pop-up.

Monitoring Anomalies

The Monitoring view displays the instances where a notification was generated because of an active rule. To view them, click on the **Monitoring** tab. The screen refreshes with a new table which matches the Configure view with the following exceptions:

- **Time Stamp**—Indicates the day and time that the threshold of the rule was crossed.
- **Value**—Actual value of the measured data.
- **Baseline Value**—Expected value for the data.
- The Condition is included in the Threshold column.
- There is no Status column, or an Edit option because they do not apply to notifications.

Sorting Notifications

If you want to filter the notifications, click on the colored portions header row of the column you want to sort by.

