

RingCentral Alerts User Guide

[Home](#) » [RingCentral](#) » RingCentral Alerts User Guide 

Contents

- 1 RingCentral Alerts User Guide
- 2 Alerts
- 3 Access & Recommended Users
- 4 Alert Management Page
- 5 Alerts List
- 6 Search filter and Create New button
- 7 Create New Alert Page
- 8 General information
- 9 Alert Trigger
- 10 Target
- 11 Trigger
- 12 Threshold and Condition
- 13 Condition is used to monitor status or health of one or more devices and rooms.
- 14 Time Frame and Alert Frequency
- 15 Advanced Options
- 16 Endpoints
- 17 Monitoring Hours
- 18 Call Volume
- 19 Call Results
- 20 Streams For Monitoring
- 21 Monitor Each Stream Separately
- 22 Delivery Channel
- 23 RingCentral App
- 24 Editing Settings
- 25 Saving Incomplete Alert Rules
- 26 Alert Notifications
- 27 Alert Log
- 28 Search & Filter
- 29 Events Trend Graph
 - 29.1 Example:
- 30 Triggered Alerts Log
- 31 Download
- 32 Read More About This Manual & Download PDF:
- 33 Documents / Resources
 - 33.1 References
- 34 Related Posts

RingCentral Alerts User Guide



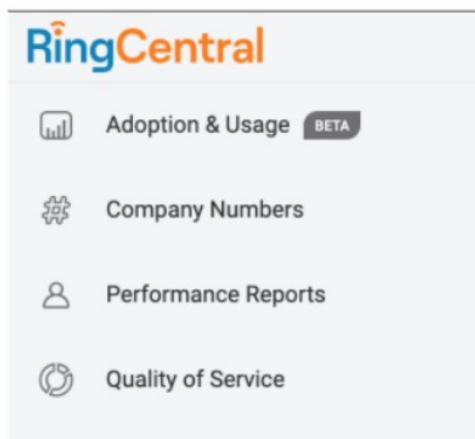
Alerts

The RingCentral Analytics Portal – Alerts enables admins to automate,

- Quality of service monitoring
 - Rooms and Device status monitoring (device status monitoring is only available to Ultimate Tier) by setting customized alerts on a variety of quality metrics, targets and monitoring frequency.
- Alerts monitors near real time data, sends immediate notifications whenever a problem occurs via email or RC App Message with a summary of the problem and a link to the report that narrows down the problem area for IT admins.
- Alerts enable admins to proactively identify and address an issue before end users report them.
- The Alerts product is specifically helpful when:
- There is a need to monitor the company-wide status of RingCentral services
 - There are specific problematic locations that are known to have issues and need monitoring on a regular basis
 - The cost of any location being down is too high and issues in any of them have to be either prevented or resolved immediately;
 - Call quality for specific users such as Execs needs to be guaranteed
 - The overall system complexity is such that even after identifying a problem, it's hard to determine a specific area where the problem originated
 - Issues occur frequently, but there is not enough data to pinpoint a root cause, or to aggregate unconnected incidents into a holistic vision of the system's state.

Access & Recommended Users

By default, all super admins will have access to this analytics and any admins can be granted access on RingCentral's admin portal.



Once access is granted, admins can access Alerts by going to:

- <https://analytics.ringcentral.com/alerts/list>
- OR
- Accessing “Analytics” tab from within RingCentral’s online admin portal
- Clicking Alerts on the left navigation bar
- Clicking on More -> Admin Tools -> Analytics on your mobile Ringcentral application

Alert Management Page

The Alert Management page contains two tabs,

- Alerts List -> List of all existing Alerts within your Account
- Alerts Log -> Log of all the triggers from your active alerts

Alerts List

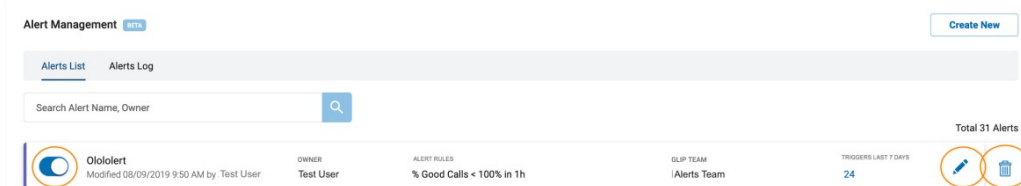
The Alerts List tab lists the record of all alerts created by all the users in the account (a crosscompany list). Every alert rule is presented in the form of a tile that shows basic information about an alert:

- Name – A customizable alert name. Give alerts a descriptive and meaningful title so that it is possible to search and find a particular alert when you need.
 - Last modified date & username – The date and time the alert was last changed and the name of the user that made the changes. When no changes have been made, this value is the date and time when the rule was created. Pausing an alert doesn't affect the last modified date.
- Severity – Severity level set on each alert at the time of Alert creation (Only visible in HD resolution screens)
- Owner – The name of the user that created the alert.
- Alert Rules – Alert monitoring rules setup during creation of alerts.
- Recipients – The first recipient (email or RC App team) and the number of recipients.
- Triggers Last 7 Days- Number of times an alert triggered in the last 7 days period.

The count links to Alerts Log page where details of the triggers can be viewed. On each Alert record, there are options to perform three actions:

- Pause – The toggle button on the left side of Alert allows to pause or reactivate an Alert. It may be necessary to pause alert when it is not relevant for a period of time. For instance, an admin might not want to get alerts during the Christmas holidays, so the rule

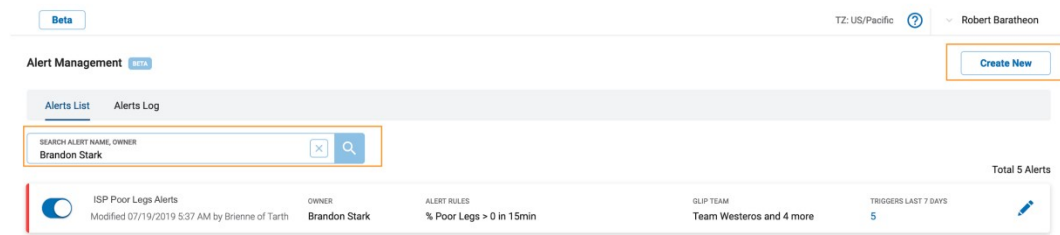
can be paused. Both pausing and reactivating are manual actions, and it is not possible to schedule such events. The blue toggle indicates that the alert is enabled, grey indicates paused.



- Edit/View – Alert creators can restrict access to an Alert as view only or editable at the time of alert creation. All alerts are editable by Alert owner.
 - Locked Alert (View Only) – If the owner has set up the alert as editable only by the owner, the alert record will show up with a lock sign in Alert Management page with a “View” sign on the right side of the Alert tile. These alerts can be edited by owners and only viewed by other users.
 - In the event the owner of an alert who created a locked alert is no longer part of the account, all their alerts will be moved to unlocked state so that other users have access to it.
 - Unlocked/Editable Alert – If owner has not restricted an alert as editable only by owner at the time of creation, the alert tile will show an edit icon option at the right end of the tile.
- Delete – You can delete an alert. Deleted alerts cannot be restored.

Search filter and Create New button

The search filter looks for the specified alert name and owner. The Create New alert button opens the “Create Alert” page where you can set up and customize an alert rule (alert name, severity, trigger, trigger value, alert target, etc.) . See the “Create New Alert Page” for details



Create New Alert Page

The Create New Alert page is comprised of six distinct sections:

A screenshot of the 'Create New Alert' form. It is divided into six sections: 1. 'General Information' with fields for 'ALERT NAME' and 'ALERT SEVERITY'. 2. 'Alert Trigger' with fields for 'TARGET', 'TARGET VALUE', 'TRIGGER', 'CONDITION', 'THRESHOLD', 'MONITORING TIMEFRAME', and 'ALERT FREQUENCY'. 3. 'Advanced Options' with a toggle switch, 'ENDPOINTS FOR MONITORING' (22 of 22 Endpoints), 'MONITORING HOURS' (Days 12:00 AM - 11:59 PM), and 'MINIMUM LEG VOLUME' (0). 4. 'Delivery Channel' with a 'DELIVERY CHANNEL' dropdown and a 'RECIPIENTS' field. 5. 'Editing Settings' with a toggle switch and the text 'Only Owner can edit this alert'. 6. A 'Create' button at the bottom right.

- General Information
 - Alert Severity
- Alert Trigger
- Advanced Options
- Delivery Channel
- Editing Settings

General information

Alert name is the field that clearly identifies the alert. The name can include all kinds of characters, including special characters, and can be up to 64 digits.

Alert severity is a subjective indicator of how important the alert is. The severity sign is shown in Glip alert messages, and as an email importance flag for high priority alerts.

Alert Trigger

Setting up the right rule is the most important part of an alert. The alert target, target value, trigger and threshold are closely interrelated. Depending on what is selected for monitoring, specified values and triggers are proposed.

General Information

ALERT NAME

ALERT SEVERITY

Alert Trigger

TARGET

- Entire Company
- Locations
- Users
- ISPs
- Devices
- Rooms

TARGET VALUE

THRESHOLD

ENDPOINTS FOR MONITORING
22 of 22 Endpoints

MONITORING HOURS
Days 12:00 AM – 11:59 PM

MINIMUM LEG VOLUME
0

Target

Target comes with a key-value pair fields where you can specify the type of the target you want to monitor and specify any subset granularity of those targets you want to monitor:

- Entire Company – Monitors entire company, no further granularity
- Locations – Select 1 or more IP addresses to be monitored from the pre-populated list of all IP addresses within your account. Every address will be monitored separately, the system does not aggregate the selected IP addresses into a single location.
- Users – Select 1 or more users from the pre populated list to be monitored for quality issues
- ISPs – Select 1 or more ISPs from the pre populated list to be monitored for quality issues
- Devices – Select 1 or more devices from the pre populated list to be monitored when devices go offline.
- Rooms – Select 1 or more rooms from the pre populated list to be monitored for quality issues
- Sites – For premium/ultimate accounts, you can also select 1 or more sites from the pre populated list to be monitored for quality issues.

If users set Target as Locations, Users, ISPs, Devices, Rooms and Sites, users have the option to include future items as long as all items in the list are selected.

Trigger

Trigger is a specific method of monitoring, and also depends on the selected target.

- Entire Company
 - Calls
 - Percentage of Good calls (MOS >= 3.5)
 - Meetings
 - Percentage of Good Streams
 - Percentage of Poor Streams
 - Devices
 - Number of Offline Devices
 - Percentage of Offline Devices
 - Rooms
 - Number of Offline Rooms
 - Percentage of Offline Rooms
 - Number of Online Rooms
 - Percentage of Online Rooms
 - Number of Rooms in Critical Condition
 - Percentage of Rooms in Critical Condition
 - Number of Rooms in Warning or Critical Condition
 - Percentage of Rooms in Warning or Critical Condition
 - Location(s)
 - Call
 - Number of Poor Legs (MOS <= 00)
 - Percentage of Good Legs (MOS >= 5)
 - Percentage of Poor and Moderate Legs (MOS <= 49)
 - Percentage of Poor Legs (MOS <= 3.00)

- Meetings
- Percentage of Good Streams
- Percentage of Poor Streams
- Devices
- Number of Offline Devices
- Rooms
- Number of Offline Rooms
- Number of Online Rooms
- Number of Rooms in Critical Condition
- Number of Rooms in Warning or Critical Condition
- User(s)
- Number of Poor and Moderate Calls (MOS <= 49) Calls
- Number of Poor Calls (MOS <= 00)
- Meetings
- Percentage of Good Streams
- Percentage of Poor Streams
- ISP(s)
- Calls
- Percentage of Poor and Moderate Legs (MOS <= 49)
- Percentage of Poor Legs (MOS <= 3.00)
- Meetings
- Percentage of Good Streams
- Percentage of Poor Streams
- Device(s)
- is Offline
- Room(s)
- Room Status
- Room Health

Threshold and Condition

Threshold is a concrete numeric value that defines when exactly the problem begins and it is time to send an alert message.

- Trigger with Percentage
 - Example, for the alert trigger and condition ‘% of good legs less than’ the threshold could be 92.5. The ‘%’ sign is not needed. The alert will be fired when the percentage of good calls is less than 92.5%.
- Trigger with Number
 - Example, for the alert trigger ‘# of poor calls in Belmont is more than’, value of the threshold is a whole number, such as 10. The alert will be triggered when the number of poor calls is more than 10.

Alert Trigger

TARGET: Locations

LOCATIONS: 51 of 10473 IPs

TRIGGER: Percent of Poor Legs

CONDITION: Greater than

THRESHOLD: 20

MONITORING TIMEFRAME

ALERT FREQUENCY

Condition is used to monitor status or health of one or more devices and rooms.

- Trigger as Device Status
 - There is only one condition for Device Status, which is offline, an alert will be sent when the monitored device goes offline.
- Rooms
 - Trigger as Room Status
- There is only one condition for Rooms Status, which is offline, this means the controller or/and host are offline or logged out. An alert will be sent when the monitored room goes offline
- Trigger as Room Health
- Room health is determined by device status within a RC room set up. Condition for room health could be
- Warning or Critical Condition: this means an alert will be sent when a room is in either warning or critical condition.
 - Warning: Calendar is not connected OR One or more preferred peripherals are offline
 - Critical: Host or/and controller are offline or logged out
- Critical Condition: this means an alert will be sent when a room is in critical condition, when host or/and controller are offline or logged out.
- You can edit your criteria for room health in Advanced Options

Alert Trigger

TARGET: Rooms

ROOMS: No Selected Rooms

TRIGGER: Room Health

CONDITION: is in Critical or Warning Condition

is in Critical Condition

Advanced Options

Time Frame and Alert Frequency

Both the alert examples above lack a clearly-defined monitoring time frame. Ten poor calls may happen in 15 minutes, or in four hours.

The Time Frame and Alert Frequency control the timing of an alert. There are two important notions: Time Frame is the period of time that a trigger is monitored to determine if an alert threshold is exceeded. Ten poor calls in 15 minutes (a critical situation) is a much larger problem than in 4 hours (normal, not critical). Available time frames are *15 minutes, 30 minutes, 1 hour and 2 hours*.

The Alert Frequency becomes important in case the alert threshold is exceeded and a notification about the problem is sent. You can instruct the system when the next notification should be sent out in case the problem persists. The alert can be muted (after being triggered) for 15 minutes, 30 minutes, 1 hour, 2 hours or 4 hours.

For example, the alert rule 'Inform me if # of poor calls in Belmont more than 10 in 15 minutes' triggers at 11 am. If the Alert Frequency is set at 2 hours, then in the next two hours the alert monitoring continues but notifications won't be sent. The second notification will be sent earliest at 1 pm. The alert frequency allows for muting the alert for a certain period of time to avoid irrelevant notifications about a problem for which everyone was previously informed.

Alert Trigger

TARGET Rooms

ROOMS No Selected Rooms

TRIGGER Room Health

CONDITION

- is in Critical or Warning Condition
- is in Critical Condition

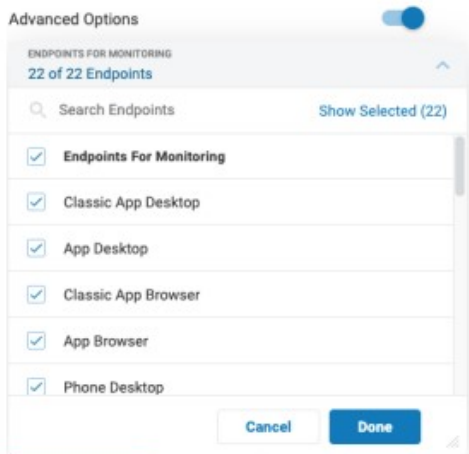
Advanced Options

Advanced Options

Advanced options allow users to set additional conditions for monitoring the set Alert rules. You can turn on Advanced Options to modify the selections in each setting. There are three advanced options:

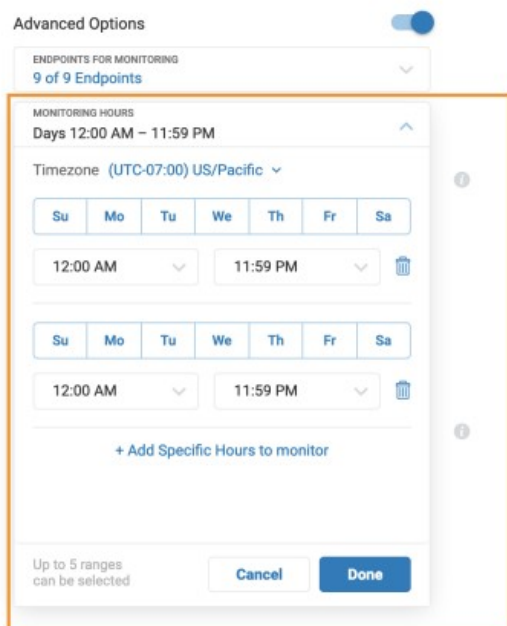
Endpoints

It is possible to include specific types of endpoints to monitor in case it is already known that one or several endpoints generate low quality calls or certain endpoints are not in use. For example, you may monitor calls made from the desktop only. By default all endpoints are checked to be monitored.




Monitoring Hours

Users may want to monitor for issues only on specific days of the week and times of the day. For example, excluding weekends and non office hours. Also, users may want to define the hours in a specific timezone because users may be monitoring remote locations. This is facilitated by Monitoring Hours advanced options. Here, you can define the timezone these time ranges are applied to and select the time ranges and days when the alert should be on.



Call Volume

This option is relevant for those triggers that calculate the percentage of poor or problematic (poor/moderate) calls or legs. For example, when one of two calls is poor, the percentage is 50% and an alert notification is fired unproductively. Set the minimum meaningful call volume so that the trigger captures actual problems.

Advanced Options 

ENDPOINTS FOR MONITORING


App Desktop

MONITORING HOURS

Days 12:00 AM – 11:59 PM

MINIMUM LEG VOLUME

6500




Call Results

This option is relevant to those triggers that monitor call quality. Users can choose to include some or all call results. Users can choose to only monitor connected call quality.

MINIMUM LEG VOLUME

6500



INCLUDE CALLS WITH CALL RESULTS

3 of 3 Call Results

☒ Include Calls with Call Results

☒ Connected

☒ Missed


☒ Voicemail

Streams For Monitoring

This option is relevant to those triggers that monitor meeting stream quality. Users can choose to monitor one or more streams with this option. For example, if users want to set up different thresholds for quality for each stream type, they can use this option to monitor one stream type per alert.

MINIMUM LEG VOLUME

6500



INCLUDE CALLS WITH CALL RESULTS

3 of 3 Call Results

☒ Include Calls with Call Results

☒ Connected

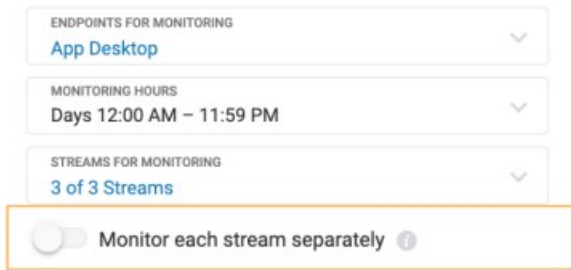
☒ Missed

☒ Voicemail

Monitor Each Stream Separately

This option is relevant to those triggers that monitor meeting stream quality. If users want to monitor each stream

type separately with the same threshold, they can turn this option on.



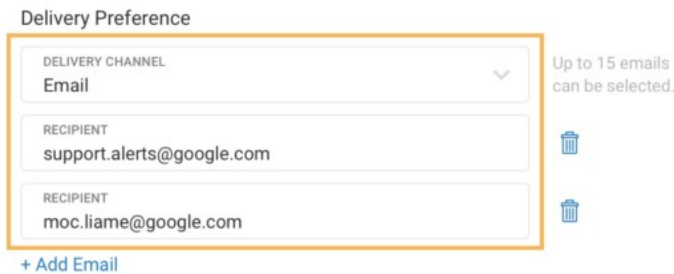
The image shows a configuration interface with three dropdown menus and a toggle switch. The first dropdown is labeled 'ENDPOINTS FOR MONITORING' and has 'App Desktop' selected. The second dropdown is labeled 'MONITORING HOURS' and has 'Days 12:00 AM - 11:59 PM' selected. The third dropdown is labeled 'STREAMS FOR MONITORING' and has '3 of 3 Streams' selected. Below these is a toggle switch labeled 'Monitor each stream separately' which is currently turned off.

Delivery Channel

Delivery Channel is the way how alerts messages can be delivered to alerts recipients. Analytics portal provides two channels: Email and Glip.

Email

Enter up to 15 distinct email addresses.



The image shows a 'Delivery Preference' form. It has a dropdown menu for 'DELIVERY CHANNEL' with 'Email' selected. Below this are two input fields for 'RECIPIENT' with the email addresses 'support.alerts@google.com' and 'moc.liame@google.com'. To the right of the form, there is a note 'Up to 15 emails can be selected.' and two trash icons. At the bottom left, there is a '+ Add Email' link.

RingCentral App

Alert creators can set up alerts to send notification to RC App groups by picking Glip as Delivery option. Users are able to see and select one or more RC App teams that they are part of to deliver the alert.

Delivery Channel

DELIVERY CHANNEL
RingCentral App

GROUPS
No RingCentral App teams selected

Search Teams Show Selected (0)

☐ My Teams

☐ Analytics

☐ Analytics

☐ Analytics

☐ Analytics

☐ Analytics

Cancel Done

Note: If the alert owner leaves a Glip group, alerts will stop being delivered.

Editing Settings

Since every created alert is visible to everyone, it's important to have the ability to "lock" an alert from being edited by others. To do this, enable the "Only owner can edit the alert" toggle (blue color). Locked alerts can be viewed by others, but changes can be applied only by the alert owner.

Delivery Channel

DELIVERY CHANNEL

RECIPIENTS

Editing Settings


Only Owner can edit this alert ☒ 

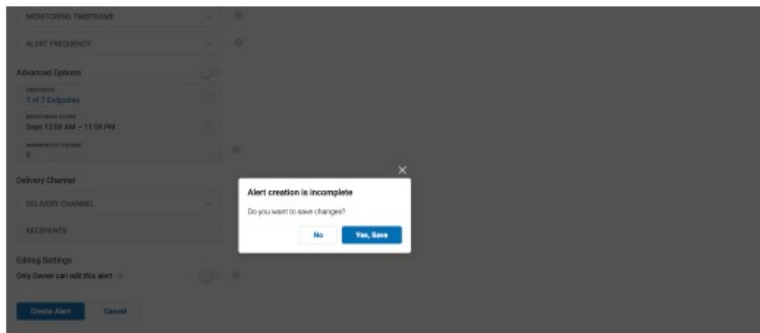
Figure 16 Create Alert – Editing settings

Unlocked alerts can be edited by anyone with access to the Alerts functionality. It is the privilege of the owner to change editing settings. These actions cannot be done by non-owners regardless of the editing settings.

Saving Incomplete Alert Rules

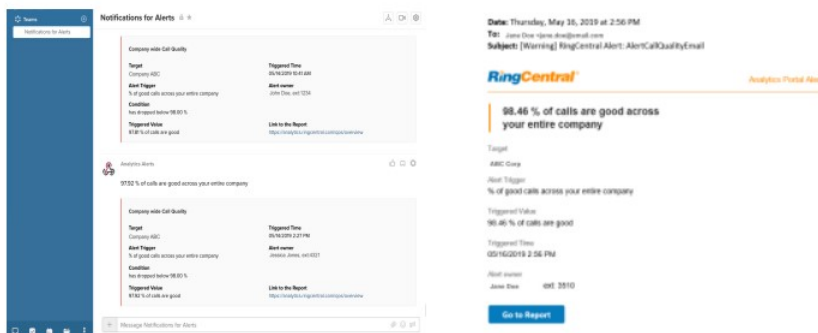
During Alert creation, before submitting the alerts if you move away from the page, you will be offered with an option to save the settings made thus far. You have an option to save or cancel.

If you opt to save, the settings you made will persist and will be available to you next time when you open the Alert creation page



Alert Notifications

Once Alerts are created in your account with your desired delivery method, our system will monitor for the trigger conditions at the monitoring time frame you have set for the alert. When an alert condition is met system will send a notification as per the desired channel as follows:



Clicking on the link provided under the “Link to the Report” or “Go to Report” button, will take you to the QoS report “Calls” page filtered out to specific calls that resulted in Alerts to be triggered.

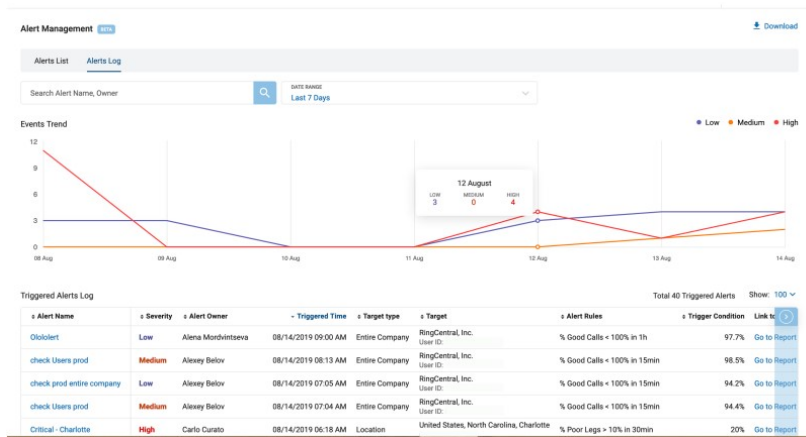
Alert Log

Alert Log page helps you keep track of all the alert notifications from the Alerts in your account over the last 6 months period. Alert Log page is the second tab on Alert Management page and features three main sections:

- Search & Filter
- Events Trend Graph
- Triggered Alerts Log

Search & Filter

On the Alerts Log page, you can search Alerts by Alert Name or Alert Owner. Search of a specific alert or alerts by a specific user updates the graph and the log with data on those alerts. You can narrow down using “DATE RANGE” Filter to alert notifications that occurred during a specific date range. By default Alert Log page filters alert logs of last 7 days.



Events Trend Graph

Events trend graph displays the Alert triggers that resulted in notifications for the selected date range and/or Alerts in the search field. Each of the three lines displayed on the graph represents alerts belonging to a specific severity level.

Example:

Purple line represents all alerts of severity level low that resulted in notification.

Orange line represents all alerts of severity level medium that resulted in notification.

Red line represents all alerts of severity level high that resulted in notification.

Hovering on the graph displays the number of alert triggers for each category of severity during a specific time duration. The duration is hourly when shorter date range filters are applied such as today, yesterday and daily if a larger date range filter is applied such as last week or custom date range of multiple days.

Clicking on a specific point on the graph will filter the “Triggered Alerts Log” to show the specific alerts contained in that specific point in time.

Triggered Alerts Log

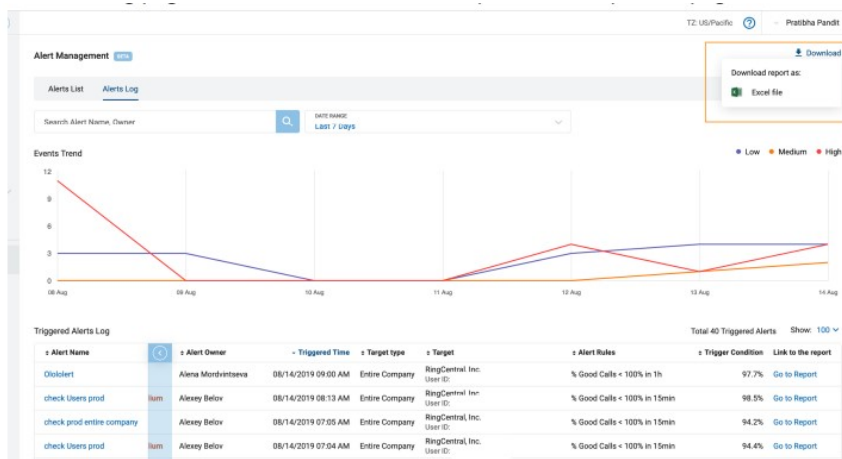
Triggered Alerts Log is a list of all the alert triggers that resulted in notification being sent out.

These alert logs contain all the same information you receive in an Alert notification while offering an ability to assess the behavior of your alerts in one place.

The Alerts log can be filtered to find a specific Alerts of your choice or click on the “Go To Report” link to go to the QoS “Calls” page with call records specific to the alert trigger or access the Alert settings by clicking the “Alert Name” link to make any modifications. Alerts Log page provides a one stop space for you to conveniently monitor and manage all of your alerts.

Download

The Alert Log page also features a “Download” option at the top of the page.



All the information displayed in the “Triggered Alerts Log” table can be downloaded into an Excel file for further analysis. Excel file will be downloaded as: “RC_ALERTS_Alerts_Log_Date_Time.xls”
 The Excel file will have two tabs;
 Filters: List of all the filters applied to the downloaded log file
 Details: Triggered Alerts Log table

The screenshot shows an Excel spreadsheet with the following data:

Alert Name	Severity	Alert owner	Triggered Time	Target Type	Target	Alert Trigger	Triggered Value	Link to the Report
Ololiolert	Low	Alena Mordvintseva	08/14/2019 09:00:00 AM	Entire Company	RingCentral, Inc., User ID:	% Good Calls < 100.00% in 1 h	97.66 %	Go to Report
check Users prod	Medium	Alexey Belov	08/14/2019 08:13:41 AM	Entire Company	RingCentral, Inc., User ID:	% Good Calls < 100.00% in 15 m	98.49 %	Go to Report
check prod entire com	Low	Alexey Belov	08/14/2019 07:05:52 AM	Entire Company	RingCentral, Inc., User ID:	% Good Calls < 100.00% in 15 m	94.15 %	Go to Report
check Users prod	Medium	Alexey Belov	08/14/2019 07:04:32 AM	Entire Company	RingCentral, Inc., User ID:	% Good Calls < 100.00% in 15 m	94.44 %	Go to Report
Critical - Charlotte	High	Carlo Curato	08/14/2019 06:18:13 AM	Location	United States, North Carolina, Charlotte,	% Poor Legs > 10.00% in 30 min	20.00 %	Go to Report
Critical - Denver	High	Carlo Curato	08/14/2019 06:13:53 AM	Location	United States, Colorado, Denver,	% Poor Legs > 10.00% in 30 min	20.00 %	Go to Report
Critical - Charlotte	High	Carlo Curato	08/14/2019 06:00:48 AM	Location	United States, North Carolina, Charlotte,	% Poor Legs > 10.00% in 30 min	20.00 %	Go to Report
Critical - Denver	High	Carlo Curato	08/14/2019 05:55:01 AM	Location	United States, Colorado, Denver, 50.205	% Poor Legs > 10.00% in 30 min	20.00 %	Go to Report
Ololiolert	Low	Alena Mordvintseva	08/14/2019 05:00:00 AM	Entire Company	RingCentral, Inc., User ID: 37439510	% Good Calls < 100.00% in 1 h	98.57 %	Go to Report

The Column "Link to the Report" includes a clickable link to the actual report associated with the alert trigger.

Read More About This Manual & Download PDF:

Documents / Resources

	RingCentral Alerts [pdf] User Guide Alerts
--	--

References

- [Analytics and Reporting](#)