

CCP Adding New Telemetry Data Source 2.0.1

Management User Interface

Date of publish: 2017-11-06

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with the letter "E" stylized as three horizontal bars.

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Getting Started with the Management User Interface.....	4
--	----------

Getting Started with the Management User Interface

The Management user interface provides mechanisms for adding parsers, enriching telemetry events, configuring and prioritizing threat intelligence, and tuning parser Storm parameters.

You can use the Management user interface main window to view existing parsers, start, stop, pause, and delete parsers, and start the process to add a new parser.

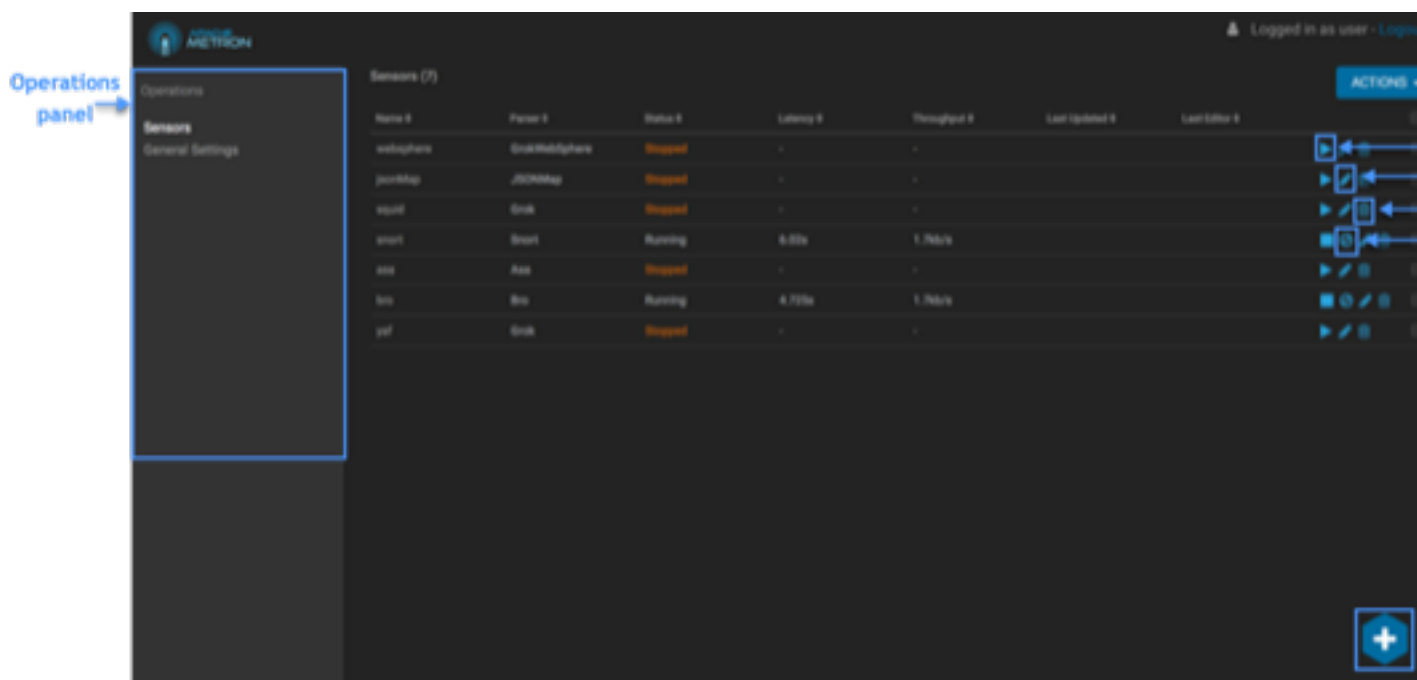


Table 1: Management UI Main Window

Tools	Description
Operations panel	You can use the functions in the Operations panel to view existing sensors or view general settings.
Management icons	You can use the management icons to start, stop or pause a sensor, edit a sensor, or delete a sensor.
Add new sensor	You can change the status of or dismiss an alert.
Meta Alerts	The meta alert feature enables you to create a system entity that contains a collection of filtered alerts.

You can use the sensor panel in the Management user interface to create new sensors.

The screenshot shows a configuration panel for a new sensor. On the left, there are blue labels with arrows pointing to specific fields in the panel:

- New parser type** points to the **NAME *** field.
- Kafka topic name** points to the **KAFKA TOPIC** field.
- Parser type** points to the **PARSER TYPE *** dropdown menu, which currently shows "Grok".
- New parser Grok statement** points to the **GROK STATEMENT** field, which contains "[object Object]".
- Transformations, enrichments, threat intelligence** points to the **SCHEMA** section, which includes sub-sections for TRANSFORMATIONS, ENRICHMENTS, and THREAT INTEL, each with a count of 0.
- Threat triage** points to the **THREAT TRIAGE** section, which includes a **RULES** count of 0.
- Storm settings** points to the **STORM SETTINGS** section, which has a "Select" button.

At the bottom of the panel are three buttons: **SAVE**, **CANCEL**, and **Advanced**.

Table 2: New Sensor Panel

Tools	Description
New parser name	The name of the new parser. This name typically matches the name of the telemetry.
Kafka topic name	The name of the Kafka topic. This name typically matches the name of the telemetry.
New parser type	The type of parser you are creating.
New parser Grok statement	The Grok statement for the new parser.
Transformations, enrichments, threat intelligence	Displays the panels for transforming the telemetry data or adding enrichments and threat intelligence information.

Tools	Description
Threat triage	Displays the panel to prioritize for the telemetry threat intelligence information.
Storm settings	Displays the panel to configure Storm settings.

Advanced

Raw JSON settings →

RAW JSON

Select

HDFS settings →

HDFS INDEX NAME

bro

HDFS BATCH SIZE

5

HDFS ENABLED

☒

Elasticsearch settings →

ELASTICSEARCH INDEX NAME

bro

ELASTICSEARCH BATCH SIZE

5

ELASTICSEARCH ENABLED

☒

Solr settings →

SOLR INDEX NAME

bro

SOLR BATCH SIZE

5

SOLR ENABLED

☒

New parser configurations →

PARSER CONFIG

enter field

enter value

+

SAVE CANCEL

Table 3: Advanced Sensor Panel

Tools	Description
Raw JSON settings	Displays the panel to add or modify the sensor parser configuration, enrichment configuration, and indexing configuration.
HDFS settings	Enables the HDFS index, and specifies the HDFS name and batch size.
Elasticsearch settings	Enables the Elasticsearch index, and specifies the HDFS name and batch size.
Solr settings	Enables the Solr index, and specifies the HDFS name and batch size.
New parser configurations	The name and value for a new parser configuration.