Cloudera Runtime 7.1.1

# Securing Cruise Control

**Date published: 2020-05-04**
**Date modified:**

**https://docs.cloudera.com/**

# Legal Notice

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.

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

# Enable security for Cruise Control

You can use SSL/TLS security protocols for securing Cruise Control. The security protocol should be the same as it is for Kafka. You can also choose between Spengo and Trusted Proxy as authentication method, and can assign admin, user and viewer roles to users to achieve further authorization over Cruise Control tasks.

You can find the security settings for Cruise Control at Cloudera Manager > Configuration > Security .

You must to set the SSL/TLS security protocol in Cruise Control just as it is set for Kafka. You can set the following security protocols:

- PLAINTEXT
- SSL
- SASL_PLAINTEXT
- SASL_SSL

Keytabs are generated when using Kerberos. You need to provide the trust store file location and the trust store password.

You can enable TLS/SSL for the Cruise Control web server using the webserver.ssl.enable property. You must provide the TLS/SSL configuration settings of the Kafka broker to the keystore. For more information about the security settings for Kafka, see the Kafka documentation.

There are two authentication methods for Cruise Control Spengo and Trusted Proxy. Spengo uses Kerberos over HTTP. Trusted Proxy uses Knox through a gateway mechanism where Knox authenticates with Cruise Control over Spengo and forwards the real user ID.

You can specify users in the following user groups:

- Admin role: has access to all endpoints
- User role: has access to all the GET endpoints except bootstrap and train
- Viewer role: has access to the most lightweight kafka_cluster_state, user_tasks and review_board endpoints