

Cloudera Runtime 7.3.1

Securing Streams Messaging Manager

Date published: 2019-08-22

Date modified: 2024-07-10

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with the letter 'E' in the middle of "CLouDERA" having a unique design where the top bar is a horizontal line and the bottom part is a vertical line, creating a stylized 'E'.

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

Legal Notice

© Cloudera Inc. 2025. 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.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

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

Securing Streams Messaging Manager.....	4
Verifying the setup.....	7

Securing Streams Messaging Manager

As a cluster administrator, you can combine Kerberos authentication and Ranger authorization to secure the Streams Messaging Manager web user interface (UI). After you secure the Streams Messaging Manager web UI, the login page appears, which does not appear by default.

About this task

If you deploy Streams Messaging Manager without security, the login page is not enabled on the Streams Messaging Manager UI by default. When you enable Kerberos authentication, Streams Messaging Manager uses SPNEGO to authenticate users and allows them to view or create topics within Kafka by administering Ranger Kafka Policies. For information on enabling browsers to use SPNEGO, see [How to Configure Browsers for Kerberos Authentication](#).

After you secure Streams Messaging Manager, anyone within the organization can login to Streams Messaging Manager. However, if they do not have the correct policy configuration in Ranger, then they may not have the necessary privileges to perform their required tasks through Streams Messaging Manager.

Before you begin

- Configure Kafka in Ranger

For more information, see *Configure a resource-based service: Kafka*.

- Enable Kerberos authentication for Kafka

For more information, see *Enable Kerberos authentication*.

- Add and configure Streams Messaging Manager

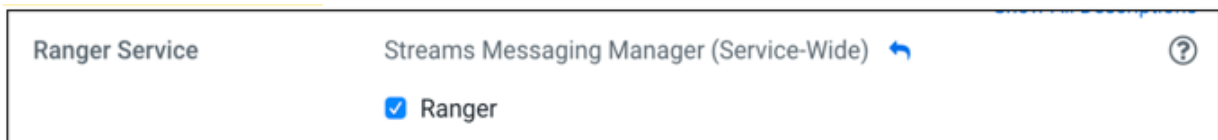
For more information, see *Creating your first Streams Messaging cluster*.



Note: For the Kafka Client security protocol, it is possible to use INFERRED, SASL_PLAINTEXT, and SASL_SSL for securing Streams Messaging Manager. However, Cloudera recommends using SASL_SSL.

Procedure

1. Go to Cloudera Manager Streams Messaging Manager , and click Configuration.
2. Enable Ranger for Streams Messaging Manager.



3. Go to the Ranger service UI and configure the Kafka policies.



Note: Review your Ranger Kafka Policies. Remember to log in to Ranger with a user that has the Ranger Admin role.

4. Click cm_kafka in the Ranger service UI.



The List of Policies page appears.

5. Click Add New Policy.

The screenshot shows the Ranger Access Manager interface. At the top, there are navigation tabs for 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user is logged in as 'admin'. Below the navigation, there is a breadcrumb trail: 'Service Manager > cm_kafka Policies'. The main heading is 'List of Policies : cm_kafka'. There is a search bar with the placeholder text 'Search for your policy...' and an 'Add New Policy' button. Below the search bar is a table with the following columns: Policy ID, Policy Name, Policy Labels, Status, Audit Logging, Roles, Groups, Users, and Action. The table contains 12 rows of policy information.

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
22	all - consumergroup	--	Enabled	Enabled	--	--	crusecontrol, streamsmgmr, kafka, streamsmgmr, + More...	[Eye] [Edit] [Delete]
23	all - topic	--	Enabled	Enabled	--	--	crusecontrol, streamsmgmr, kafka, streamsmgmr, + More...	[Eye] [Edit] [Delete]
24	all - transactionalid	--	Enabled	Enabled	--	--	crusecontrol, streamsmgmr, kafka, streamsmgmr, + More...	[Eye] [Edit] [Delete]
25	all - cluster	--	Enabled	Enabled	--	--	crusecontrol, streamsmgmr, kafka, streamsmgmr, + More...	[Eye] [Edit] [Delete]
26	all - delegationtoken	--	Enabled	Enabled	--	--	crusecontrol, streamsmgmr, kafka, streamsmgmr, + More...	[Eye] [Edit] [Delete]
27	ATLAS_HOOK	--	Enabled	Enabled	--	--	hbase, hive, impala, mgov, + More...	[Eye] [Edit] [Delete]
28	ATLAS_ENTITIES	--	Enabled	Enabled	--	--	atlas, rangertagsync, cloudera-scm	[Eye] [Edit] [Delete]
29	ATLAS_SPARK_HOOK	--	Enabled	Enabled	--	public	atlas, cloudera-scm	[Eye] [Edit] [Delete]
30	atlas consumergroup	--	Enabled	Enabled	--	--	atlas	[Eye] [Edit] [Delete]
31	ranger_entities_consumer consumergroup	--	Enabled	Enabled	--	--	rangertagsync	[Eye] [Edit] [Delete]
42	enable-create	--	Enabled	Enabled	--	--	cloudera-scm	[Eye] [Edit] [Delete]

The Policy Details page appears.

The screenshot shows the 'Policy Details' page for the 'enable-create' policy. The page has a title 'Policy Details :'. Below the title, there are several fields and controls:

- Policy Type:** A dropdown menu set to 'Access'.
- Policy Name *:** A text input field containing 'enable-create'. To its right is an 'enabled' toggle switch (checked) and a 'normal' toggle switch (unchecked).
- Policy Label:** A text input field containing 'Policy Label'.
- cluster *:** A dropdown menu set to 'cluster' and a text input field containing 'x *'. To its right is an 'include' toggle switch (checked).
- Description:** A large text area for entering a description.
- Audit Logging:** A toggle switch set to 'YES'.

6. Add a policy name and select cluster from the dropdown.

Policy Details :

Policy Type **Access**

Policy Name * enabled normal

Policy Label include

- topic
- transactionalid
- cluster
- delegationtoken
- consumergroup

Description

Audit Logging **YES**

7. Type * in the field beside cluster, and select the * from the values that appear.
8. Go to the Allow Condition section and select the user.
9. Add permissions by clicking the + under Add Permissions.

Allow Conditions :

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="x streamsmgmr"/>	Add Conditions +	Add Permissions +	<input type="checkbox"/> hide
<div style="border: 1px solid #ccc; padding: 5px;"> <p>⚠ Exclude from Allow Conditions :</p> </div>					
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="Select Users"/>	Add Conditions +	<div style="border: 1px solid #ccc; padding: 5px;"> <p>add/edit permissions</p> <ul style="list-style-type: none"> <input type="checkbox"/> Configure <input checked="" type="checkbox"/> Describe <input type="checkbox"/> Kafka Admin <input checked="" type="checkbox"/> Create <input type="checkbox"/> Idempotent Write <input type="checkbox"/> Describe Configs <input type="checkbox"/> Alter Configs <input type="checkbox"/> Cluster Action <input type="checkbox"/> Alter <input type="checkbox"/> Select/Deselect All </div>	<input type="checkbox"/> hide

10. Select Create and Describe permissions.
11. Click Add.

Related Information

- [Configure a resource-based service: Kafka](#)
- [Configure a resource-based service: Kafka](#)
- [Enable Kerberos Authentication](#)
- [Enable Kerberos Authentication](#)
- [Setting up your Streams Messaging cluster](#)

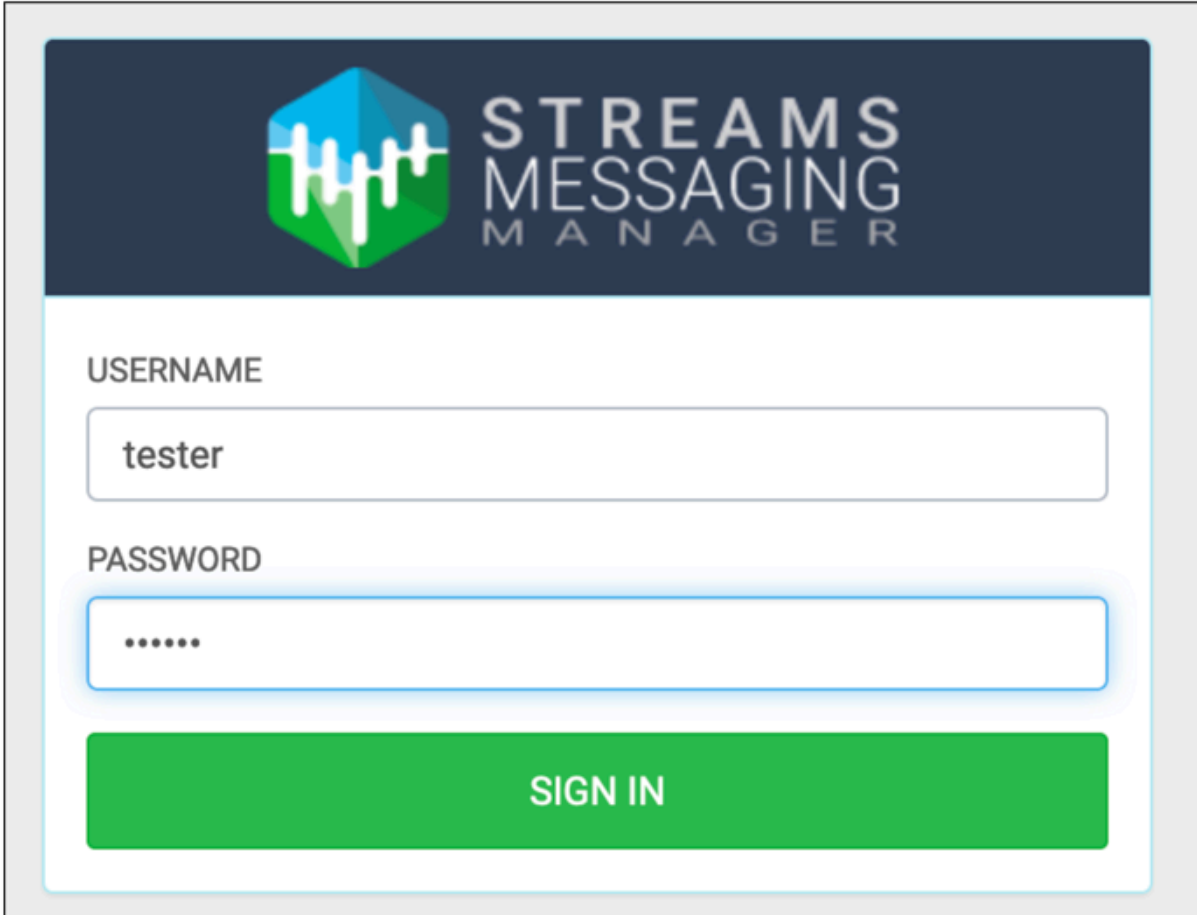
Verifying the setup

After you secure Streams Messaging Manager, you can verify the security setup. You can login to the Streams Messaging Manager web UI and create Kafka topics.

Procedure

1. Go to Cloudera Manager Streams Messaging Manager .

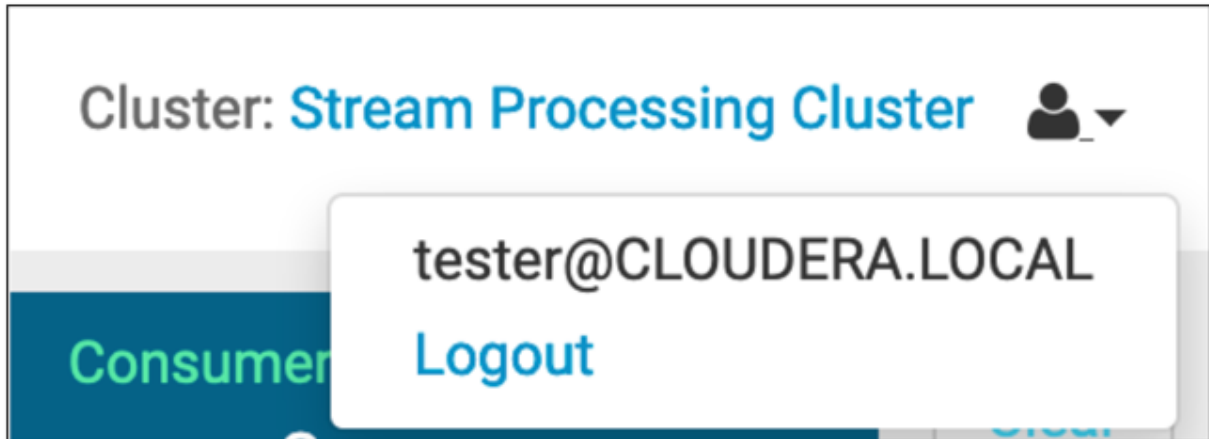
The login page for Streams Messaging Manager appears.



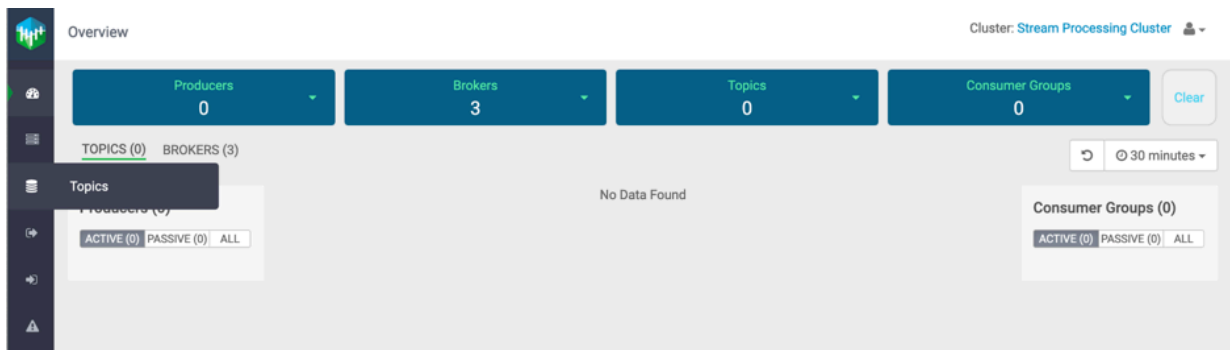
The screenshot shows the login interface for Streams Messaging Manager. At the top, there is a dark blue banner containing the Cloudera logo (a green and blue hexagon) and the text "STREAMS MESSAGING MANAGER". Below the banner, the form is white with a light blue border. It includes a "USERNAME" label above a text input field containing "tester". Below that is a "PASSWORD" label above a password input field with seven dots. At the bottom of the form is a prominent green button with the text "SIGN IN" in white capital letters.

2. Login to the Streams Messaging Manager UI using your regular credentials.

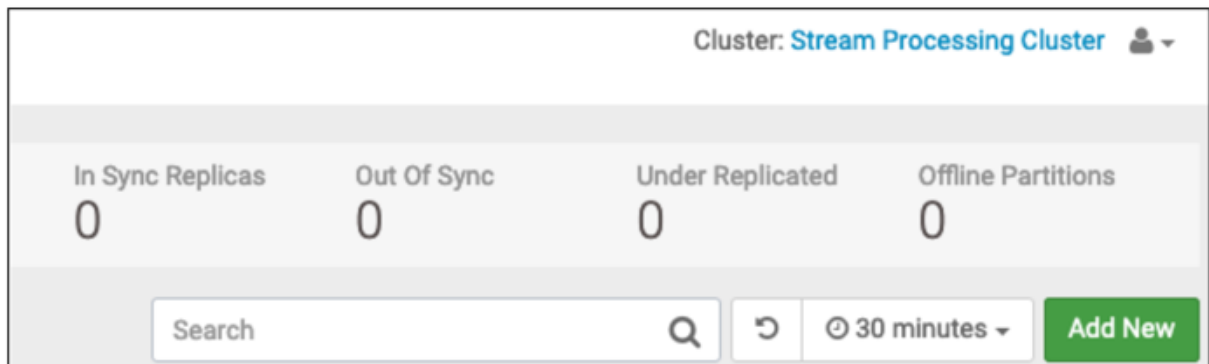
After you log in, you see the user logout dropdown at the top right corner of your screen. It shows the domain associated with the user.



3. Click Streams Messaging Manager Web UI.
4. To add a topic, go to Topics.



5. Click Add New.








6. Add a topic name, select partitions, and cleanup policy.

Add Topic

TOPIC NAME

PARTITIONS

Availability

 MAXIMUM	 HIGH	 MODERATE	 LOW	 CUSTOM
REPLICATION FACTOR 3 MIN INSYNC REPLICA 2	REPLICATION FACTOR 3 MIN INSYNC REPLICA 1	REPLICATION FACTOR 2 MIN INSYNC REPLICA 1	REPLICATION FACTOR 1 MIN INSYNC REPLICA 1	

Limits

CLEANUP.POLICY

[Advanced](#)

7. Click Save.

You see the following message in the top right corner of the webpage.

