

Securing Streams Messaging Manager

Date published: 2020-08-10

Date modified: 2020-11-30



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.....	6
Enabling TLS Encryption for SMM on CDP Private Cloud.....	9
TLS/SSL settings for Streams Messaging Manager.....	10

Securing Streams Messaging Manager

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

About this task

If you deploy SMM without security, the login page is not enabled on the SMM UI by default. When you enable Kerberos authentication, SMM 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 SMM, anyone within the organization can login to SMM. 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 SMM.

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 SMM

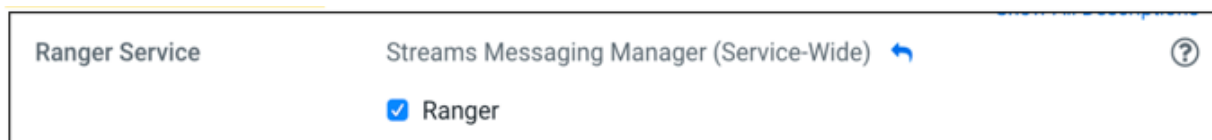
For more information, see *CDP Data Center Installation Guide*.



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

Procedure

1. Go to Cloudera Manager > SMM, and click Configuration.
2. Enable Ranger for SMM.



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.

Ranger

Access Manager

Audit

Security Zone

Settings

admin

Service Managercm_kafka Policies

List of Policies : cm_kafka

Search for your policy...

Add New Policy

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
22	all - consumer group	--	Enabled	Enabled	--	--	<div>crusecontrolstreamsmgmrkafka</div> <div>streamsmgmr+ More...</div>	<div></div> <div></div> <div></div>
23	all - topic	--	Enabled	Enabled	--	--	<div>crusecontrolstreamsmgmrkafka</div> <div>streamsmgmr+ More...</div>	<div></div> <div></div> <div></div>
24	all - transactional id	--	Enabled	Enabled	--	--	<div>crusecontrolstreamsmgmrkafka</div> <div>streamsmgmr+ More...</div>	<div></div> <div></div> <div></div>
25	all - cluster	--	Enabled	Enabled	--	--	<div>crusecontrolstreamsmgmrkafka</div> <div>streamsmgmr+ More...</div>	<div></div> <div></div> <div></div>
26	all - delegation token	--	Enabled	Enabled	--	--	<div>crusecontrolstreamsmgmrkafka</div> <div>streamsmgmr+ More...</div>	<div></div> <div></div> <div></div>
27	ATLAS_HOOK	--	Enabled	Enabled	--	--	<div>hbasehiveimpalmigov+ More...</div>	<div></div> <div></div> <div></div>
28	ATLAS_ENTITIES	--	Enabled	Enabled	--	--	<div>atlasrangertagsynccloudera-scm</div>	<div></div> <div></div> <div></div>
29	ATLAS_SPARK_HOOK	--	Enabled	Enabled	--	public	<div>atlascloudera-scm</div>	<div></div> <div></div> <div></div>
30	atlas consumer group	--	Enabled	Enabled	--	--	<div>atlas</div>	<div></div> <div></div> <div></div>
31	ranger_entities_consumer consumer group	--	Enabled	Enabled	--	--	<div>rangertagsync</div>	<div></div> <div></div> <div></div>
42	enable-create	--	Enabled	Enabled	--	--	<div>cloudera-scm</div>	<div></div> <div></div> <div></div>

The Policy Details page appears.

Policy Details :

Policy Type

Access

Policy Name *

enable-create

Policy Label

Policy Label

cluster

*

x *

Description

Audit Logging

YES

enabled

normal

include

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"/>
<div> <div>+</div> <div>Exclude from Allow Conditions :</div> </div>					
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="Select Users"/>	Add Conditions +	Add Permissions +	<input type="checkbox"/>

add/edit permissions

☐ Configure
☒ Describe
☐ Kafka Admin
☒ Create
☐ Idempotent Write
☐ Describe Configs
☐ Alter Configs
☐ Cluster Action
☐ Alter
☐ Select/Deselect All

✓ ✕

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

Related Information

[How to Configure Browsers for Kerberos Authentication](#)

[Configure a resource-based service: Kafka](#)

[Enable Kerberos Authentication](#)

[CDP Private Cloud Base Installation Guide](#)

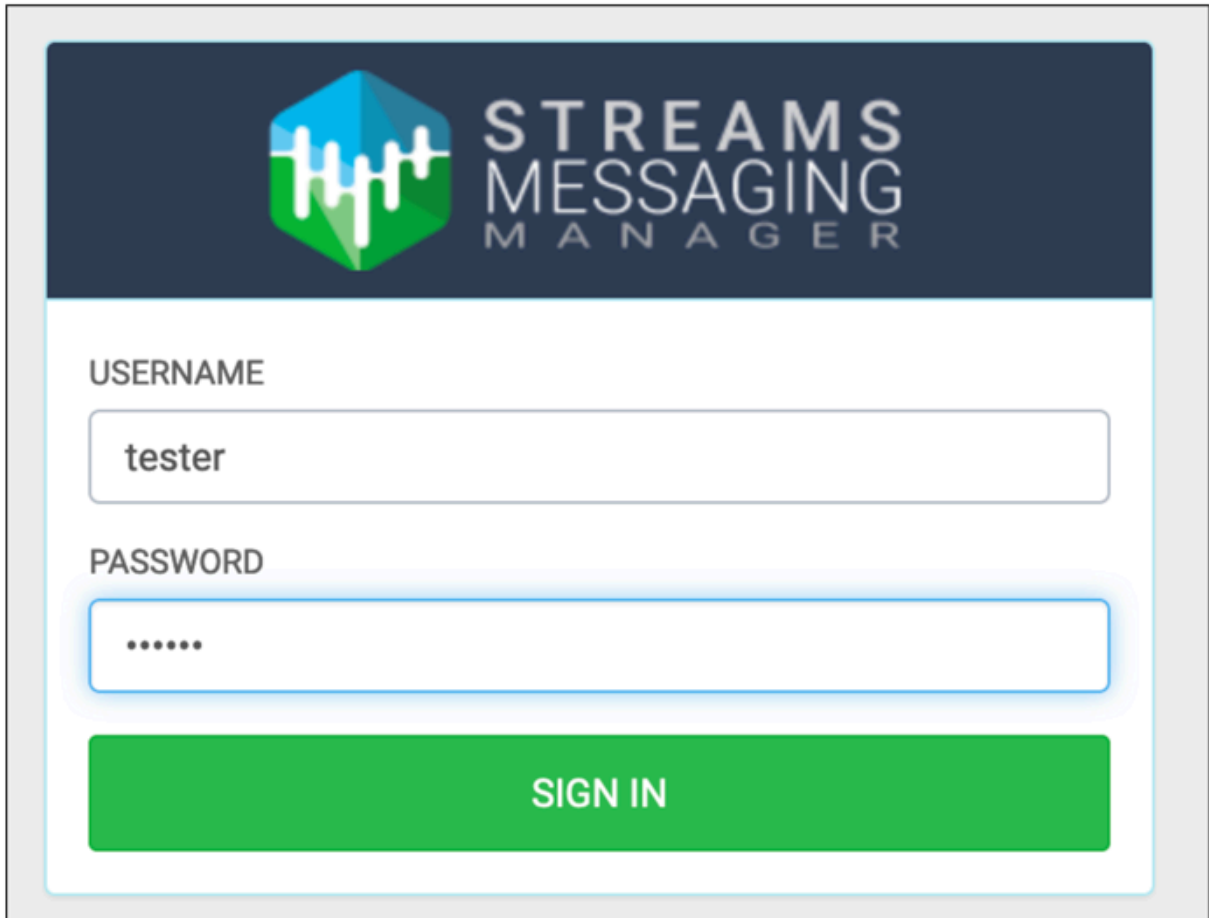
Verifying the setup

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

Procedure

1. Go to Cloudera Manager > SMM .

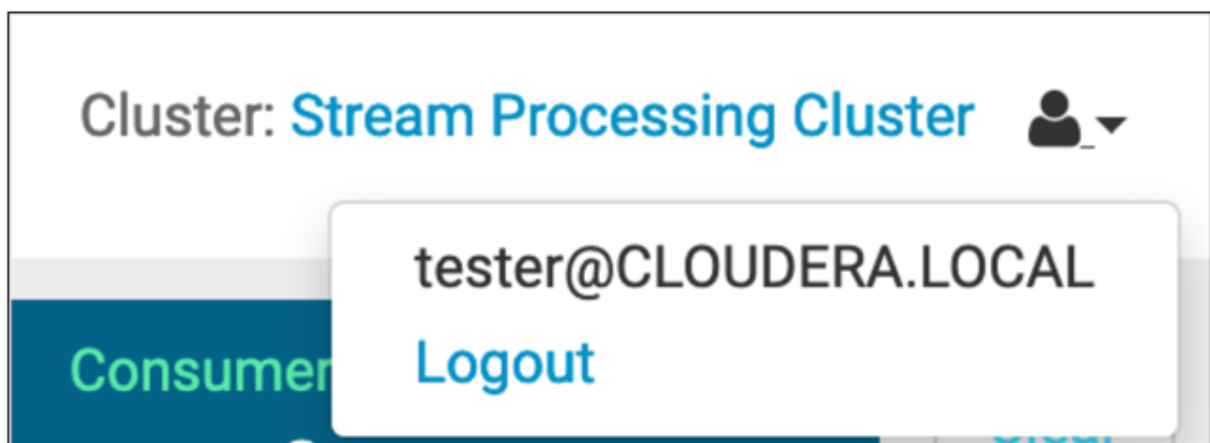
The login page for SMM appears.



The screenshot shows the login interface for Streams Messaging Manager. At the top, there is a dark blue header with the SMM logo (a green and blue hexagon with a white waveform) and the text "STREAMS MESSAGING MANAGER". Below the header, the form has two input fields: "USERNAME" with the value "tester" and "PASSWORD" with masked characters ".....". A large green "SIGN IN" button is positioned below the password field.

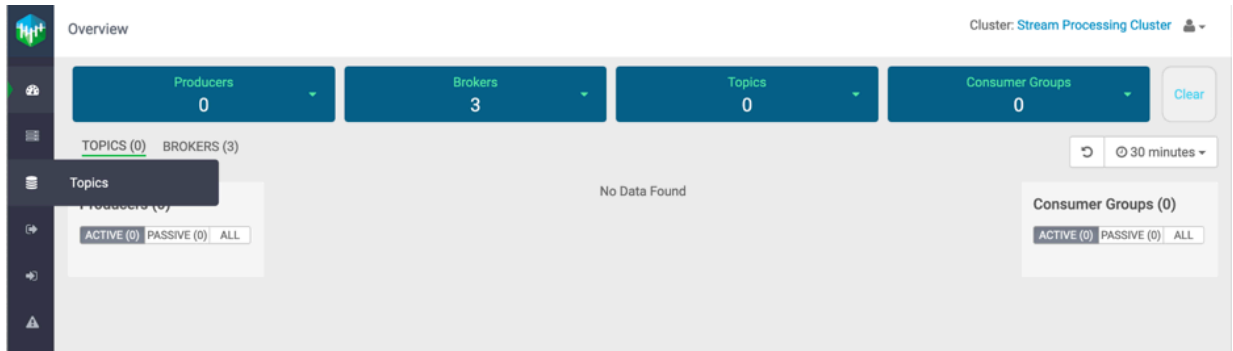
2. Login to the SMM UI using your regular credentials.

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.

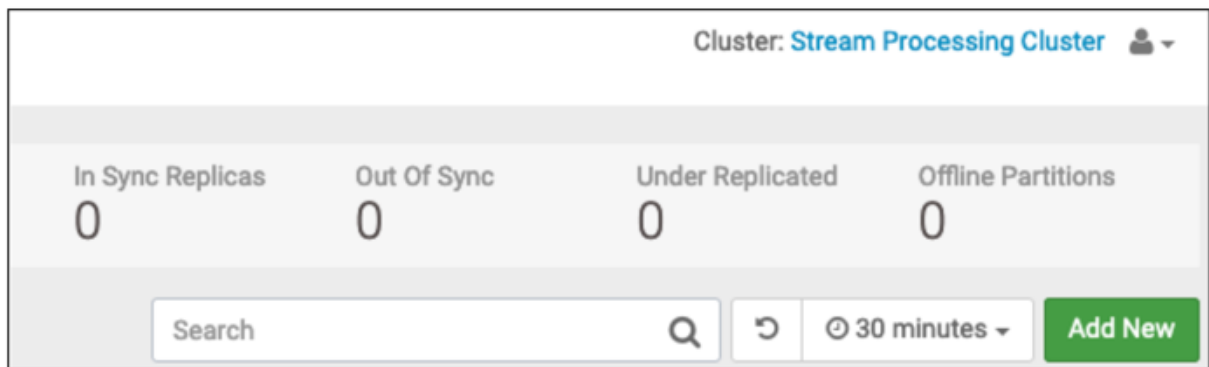


3. Click Streams Messaging Manager Web UI.

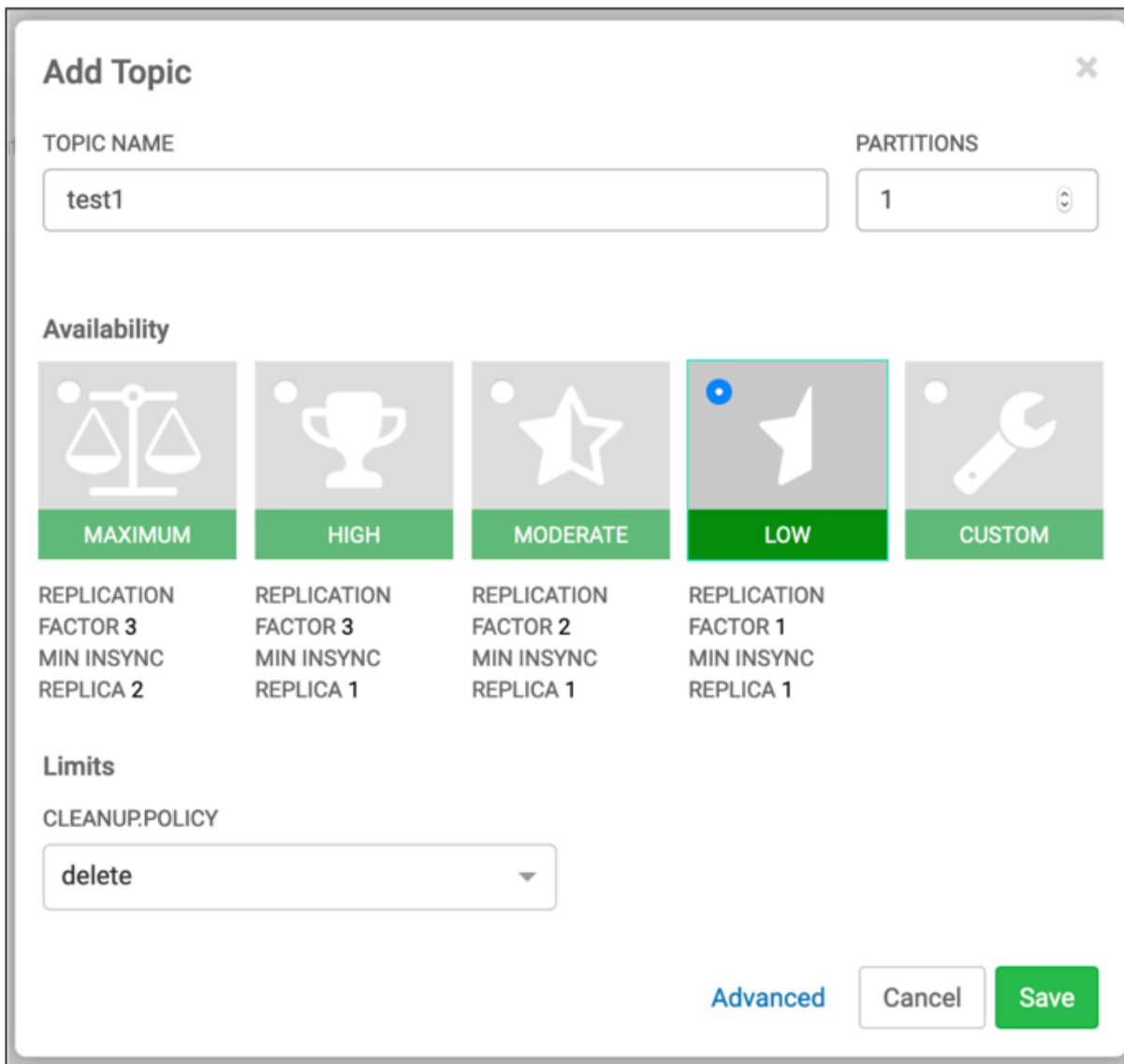
4. To add a topic, go to Topics.



5. Click Add New.



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

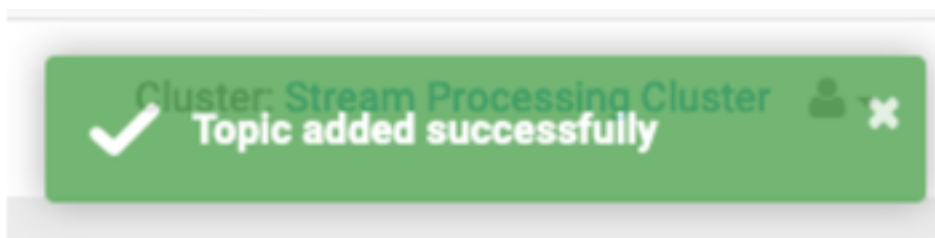


The 'Add Topic' dialog box contains the following fields and options:

- TOPIC NAME:** A text input field containing 'test1'.
- PARTITIONS:** A dropdown menu set to '1'.
- Availability:** Five radio button options with icons:
 - MAXIMUM:** Scales icon. REPLICATION FACTOR 3, MIN INSYNC REPLICA 2.
 - HIGH:** Trophy icon. REPLICATION FACTOR 3, MIN INSYNC REPLICA 1.
 - MODERATE:** Star icon. REPLICATION FACTOR 2, MIN INSYNC REPLICA 1.
 - LOW:** Star with dot icon (selected). REPLICATION FACTOR 1, MIN INSYNC REPLICA 1.
 - CUSTOM:** Wrench icon.
- Limits:** A dropdown menu for 'CLEANUP.POLICY' set to 'delete'.
- Buttons:** 'Advanced' (blue text), 'Cancel' (white button), and 'Save' (green button).

7. Click Save.

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



Enabling TLS Encryption for SMM on CDP Private Cloud

Learn how to enable TLS/SSL encryption for Streams Messaging Manager (SMM) on CDP Private Cloud to secure the communication of sensitive information. You can enable the settings in Cloudera Manager according to the cluster configuration.

About this task

If Kerberos is enabled, then you must enable SSL for Streams Messaging Manager (SMM). SMM UI fails to load if Kerberos is enabled and SSL is not enabled.

Also, if Kafka has Kerberos/SSL enabled, the same should be enabled for SMM.

Procedure

1. Log in to Cloudera Manager.
2. Select the Streams Messaging Manager cluster.
3. Click Configuration from the menu bar.
4. In the Search field, type TLS/SSL to show the SMM TLS/SSL properties.

The security related properties appear.

5. Edit the security properties according to the cluster configuration.
6. Click Save Changes.

TLS/SSL settings for Streams Messaging Manager

To enable TLS/SSL settings for Streams Messaging Manager (SMM), you need to configure SMM server properties, SMM UI properties, and SMM Server's Oracle TLS connection properties. You can configure the TLS/SSL properties in Cloudera Manager according to the cluster configuration.

Table 1: TLS/SSL Settings for SMM

Properties	Description
SMM Server properties	
Enable TLS/SSL for Streams Messaging Manager Rest Admin Server ssl.enable	Encrypts communication between clients and Streams Messaging Manager Rest Admin Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Streams Messaging Manager port (SSL) streams.messaging.manager.ssl.port	The HTTPS port that Streams Messaging Manager REST server runs on when SSL is enabled.
Streams Messaging Manager Admin Port (SSL) streams.messaging.manager.ssl.adminPort	The HTTPS admin port that Streams Messaging Manager REST server runs on when SSL is enabled.
SSL Keystore Type streams.messaging.manager.ssl.keyStoreType	The keystore type. Required if Streams Messaging Manager REST server's SSL is enabled. For example, PKCS12 or JKS. If a value is not specified for this property, then the keystore type is inherited from Cloudera Manager settings.
SSL TrustStore Type streams.messaging.manager.ssl.trustStoreType	The truststore type. Required if SMM's SSL is enabled. For example, PKCS12 or JKS. If a value is not specified for this property, then the keystore type is inherited from Cloudera Manager settings.
Streams Messaging Manager Rest Admin Server TLS/SSL Server JKS Keystore File Location streams.messaging.manager.ssl.keyStorePath	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Streams Messaging Manager Rest Admin Server functions as a TLS/SSL server.
Streams Messaging Manager Rest Admin Server TLS/SSL Server JKS Keystore File Password	The password for the Streams Messaging Manager Rest Admin Server keystore file.
Streams Messaging Manager Rest Admin Server TLS/SSL Server JKS Keystore Key Password	The password that protects the private key contained in the keystore. Used when Streams Messaging Manager Rest Admin Server functions as a TLS/SSL server.

Properties	Description
Streams Messaging Manager Rest Admin Server TLS/SSL Client Trust Store File streams.messaging.manager.ssl.trustStorePath	The location on disk of the truststore used to confirm the authenticity of TLS/SSL servers to which the Streams Messaging Manager Rest Admin Server might connect. This is used when Streams Messaging Manager Rest Admin Server is the client in a TLS/SSL connection. This truststore must contain the certificate(s) used to sign the service(s) connected to. If a value is not specified for this property, the default list of known certificate authorities is used instead.
Streams Messaging Manager Rest Admin Server TLS/SSL Client Trust Store Password	The password for the Streams Messaging Manager Rest Admin Server TLS/SSL Certificate Trust Store File. This password is not mandatory to access the truststore; this field is optional. This password provides optional integrity checking of the file. The contents of truststores are certificates, and certificates are public information.
Cloudera Manager Metrics TrustStore Type cm.metrics.truststore.type	Cloudera Manager's truststore type. If a value is not specified for this property, then the keystore type is inherited from Cloudera Manager settings.
SSL ValidateCerts streams.messaging.manager.ssl.validateCerts	Whether or not to validate TLS certificates before starting SMM. If enabled, SMM does not start when certificates are expired or invalid.
SSL validatePeers streams.messaging.manager.ssl.validatePeers	Whether or not to validate TLS peer certificates.
SMM UI properties	
Enable TLS/SSL for Streams Messaging Manager UI Server streams.messaging.manager.ui.ssl.enable	Encrypt communication between clients and Streams Messaging Manager UI Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format) streams.messaging.manager.ui.ssl.private.key.location	The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Streams Messaging Manager UI Server functions as a TLS/SSL server. The certificate file must be in Privacy Enhanced Mail (PEM) format.
Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format) streams.messaging.manager.ui.ssl.cert.location	The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Streams Messaging Manager UI Server functions as a TLS/SSL server. The certificate file must be in PEM format.
Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format) streams.messaging.manager.ui.ssl.ca.cert.location	The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Streams Messaging Manager UI Server functions as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.
Streams Messaging Manager UI Server TLS/SSL Private Key Password	The password for the private key in the Streams Messaging Manager UI Server TLS/SSL Server Certificate and Private Key file. If a value is not specified for this property, the private key is not protected by a password.
Streams Messaging Manager UI Server TLS/SSL Certificate Trust Store File streams.messaging.manager.ui.ssl.trust.store.location	The location on disk of the truststore, in .pem format, used to confirm the authenticity of the TLS/SSL servers that Streams Messaging Manager UI Server might connect to. This is used when Streams Messaging Manager UI Server is the client in a TLS/SSL connection. This truststore must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not specified, the default list of known certificate authorities is used instead.
SMM Server's Oracle TLS connection properties	
Enable TLS with Oracle DB streams.messaging.manager.enable.TLS.Oracle	Enable TLS with Oracle as a database for Schema Registry.
Oracle.net.ssl_version streams.messaging.manager.oracle.net.ssl_version	Oracle net ssl version.

Properties	Description
Oracle TLS javax.net.ssl.keyStore streams.messaging.manager.javax.net.ssl.keyStore	Path to keystore file if enabling TLS using Oracle database.
Oracle TLS javax.net.ssl.keyStoreType streams.messaging.manager.javax.net.ssl.keyStoreType	KeyStoreType type if enabling TLS using Oracle database.
Oracle TLS javax.net.ssl.keyStorePassword streams.messaging.manager.javax.net.ssl.keyStorePassword	KeyStorePassword if enabling TLS using Oracle database.
Oracle TLS javax.net.ssl.trustStore streams.messaging.manager.javax.net.ssl.trustStore	Required Path to truststore file if enabling TLS using Oracle database.
Oracle TLS javax.net.ssl.trustStoreType streams.messaging.manager.javax.net.ssl.trustStoreType	Required truststore type if enabling TLS using Oracle database.
Oracle TLS javax.net.ssl.trustStorePassword streams.messaging.manager.javax.net.ssl.trustStorePassword	TrustStorePassword type if enabling TLS using Oracle database.
Oracle TLS oracle.net.ssl_cipher_suites streams.messaging.manager.oracle.net.ssl_cipher_suites	Net SSL Cipher Suites if enabling TLS using Oracle database. For example, SSL_DH_DSS_WITH_DES_CBC_SHA.
Oracle TLS oracle.net.ssl_server_dn_match streams.messaging.manager.oracle.net.ssl_server_dn_match	SSL server domain name match if enabling TLS using Oracle database.
Oracle TLS oracle.net.authentication_services streams.messaging.manager.oracle.net.authentication_services	Oracle net authentication service if enabling TLS using Oracle database.