

Encryption Reference 1.0.0

## Encryption reference

Date published: 2017-11-06

Date modified: 2018-07-15

# CLOUDERA

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

# Legal Notice

© Cloudera Inc. 2024. 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

|   |          |
|---|----------|
| <b>Auto-TLS Requirements and Limitations.....</b>                       | <b>4</b> |
| <b>The certmanager utility.....</b>                                     | <b>4</b> |
| <b>Rotate Auto-TLS Certificate Authority and Host Certificates.....</b> | <b>6</b> |
| <b>Auto-TLS Agent File Locations.....</b>                               | <b>6</b> |

# Auto-TLS Requirements and Limitations

Reference information for Auto-TLS requirements, limitations, and component support.

## Requirements

- You must install the Cloudera Manager Agent software on the Cloudera Manager Server host.
- You can enable auto-TLS using certificates created and managed by a Cloudera Manager certificate authority (CA), or certificates signed by a trusted public CA or your own internal CA. If you want to use a trusted public CA or your own internal CA, you must obtain all of the host certificates before enabling auto-TLS. For instructions on obtaining certificates from a CA, see “Manually Configuring TLS Encryption for Cloudera Manager”>“On Each Cluster Host”.

## Component support for Auto-TLS

The following Cloudera Enterprise services support auto-TLS:

- Cloudera Navigator Audit Server
- Cloudera Navigator Metadata Server
- HBase
- HDFS Client Configuration
- HDFS NameNode Web UI
- HiveServer2
- HttpFS
- Hue Client
- Hue Load Balancer
- Hue Server
- Impala Catalog Server
- Impala Server
- Impala StateStore
- Kafka Broker Server
- Oozie
- Phoenix
- Spark History Server
- YARN Web UI

For unlisted Cloudera Enterprise services, you must enable TLS manually. See the applicable component guide for more information.

## Related Information

[Manually Configuring TLS Encryption for Cloudera Manager](#)

## The certmanager utility

Auto-TLS is managed using the certmanager utility, which is included in the Cloudera Manager Agent software, and not the Cloudera Manager Server software. You must install the Cloudera Manager Agent software on the Cloudera Manager Server host to be able to use the utility. You can use certmanager to manage auto-TLS on a new installation.

### certmanager syntax

```
/opt/cloudera/cm-agent/bin/certmanager [OPTIONS] COMMAND [ARGS]...
```

## Options

- `--location <certmanager-dir-root>`

The directory where certmanager stores all of its files on the Cloudera Manager Server host. If omitted, defaults to `/var/lib/cloudera-scm-server/certmanager`. This directory is created automatically, and must not exist before running the command. If it does exist, you can use the `--rotate` argument (documented below) to back up the existing directory and create a new one in its place.

The agent host certificates and other files are stored elsewhere on each agent .

- `--help`

Displays the help message.

## Commands

- `add_custom_cert`

Adds a custom certificate and key for a host. Use this command only if you have configured a custom certificate directory (using the `setup_custom_certdir` command). You must run this command before adding a host in Cloudera Manager.

- `export_ca_cert`

Displays the Cloudera Manager internal CA certificate. You can export the certificate to a file using a redirect operator (`>` or `>>>`).

- `setup`

Initializes the certificate manager and the internal CA, and configures Cloudera Manager Server to enable auto-TLS.

- `--configure-services`

Configures Cloudera Manager Server to enable automatic configuration of TLS for supported components, such as HDFS, YARN, and so on. If you omit this option, auto-TLS will only be configured for Cloudera Manager agent/server communication.

- `--rotate`

Backs up the certmanager root directory (`/var/lib/cloudera-scm-server/certmanager` by default, or specified by the `--location` option) if it exists, and creates a new one in its place. If the directory does not exist, it is created. If the directory exists, and you do not use the `--rotate` argument, the command fails.

- `--override ca_dn="<CA_DN>"`

Overrides the default CA distinguished name (DN) with the provided DN. Use this if your environment requires that the common name (CN) matches the hostname. For example:

```
--override ca_dn="CN=cm01,DC=example,DC=com"
```

- `--stop-at-csr`

Stops the setup process after generating the private key and certificate signing request (CSR) for an intermediate CA certificate, and outputs the CSR file location to the screen. Submit the provided CSR to your

internal root CA for signing. After receiving the signed intermediate CA certificate, continue the setup using the `--signed-ca-cert` parameter.

When using the `--stop-at-csr` and `--signed-ca-cert` arguments, make sure that the remaining command options and arguments are the same.

- `--signed-ca-cert=<intermediate_CA_cert>`

Resumes the setup process using the provided signed intermediate CA certificate.

When using the `--stop-at-csr` and `--signed-ca-cert` arguments, make sure that the remaining command options and arguments are the same.

- `setup_custom_certdir`

Initializes the certificate manager using a custom certificate directory. Use this command if you are using existing certificates signed by a trusted public CA or your own internal CA.

- `--configure-services`

Configures Cloudera Manager Server to enable automatic configuration of TLS for supported components, such as HDFS, YARN, and so on. If you omit this option, auto-TLS will only be configured for Cloudera Manager agent/server communication.

- `--rotate`

Backs up the certmanager root directory (`/var/lib/cloudera-scm-server/certmanager` by default, or specified by the `--location` option) if it exists, and creates a new one in its place. If the directory does not exist, it is created. If the directory exists, and you do not use the `--rotate` argument, the command fails.

## Rotate Auto-TLS Certificate Authority and Host Certificates

Your cluster security requirements may require that you rotate the auto-TLS CA and certificates.

### About this task



**Note:** When using a custom CA, you must first use the `/cm/commands/addCustomCerts` API command to replace the old certificates with new certificates before using the following procedure.

### Procedure

1. Navigate to Administration Security . Click the Rotate Auto-TLS Certificates button to launch the wizard.
2. Complete the wizard.

## Auto-TLS Agent File Locations

The certificates, keystores, and password files generated by auto-TLS are stored in `/var/lib/cloudera-scm-agent/agent-cert` on each Cloudera Manager Agent.

## Filenames

**Table 1: Auto-TLS Agent Files**

| Filename                          | Description   |
|-----------------------------------|---|
| cm-auto-global_cacerts.pem        | CA certificate and other trusted certificates in PEM format |
| cm-auto-global_truststore.jks     | CA certificate and other trusted certificates in JKS format |
| cm-auto-in_cluster_ca_cert.pem    | CA certificate in PEM format                                |
| cm-auto-in_cluster_truststore.jks | CA certificate in JKS format                                |
| cm-auto-host_key_cert_chain.pem   | Agent host certificate and private key in PEM format        |
| cm-auto-host_cert_chain.pem       | Agent host certificate in PEM format                        |
| cm-auto-host_key.pem              | Agent host private key in PEM format                        |
| cm-auto-host_keystore.jks         | Agent host private key in JKS format                        |
| cm-auto-host_key.pw               | Agent host private key password file                        |