

## Encryption reference

Date published: 2020-07-28

Date modified: 2021-12-13



# 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>Rotate Auto-TLS Certificate Authority and Host Certificates.....</b> | <b>5</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 CDP services support auto-TLS:

- Atlas
- Cloudera Manager Host Monitor Debug Interface
- Cloudera Manager Service Monitor Debug Interface
- Cruise Control
- HBase
- HDFS Client Configuration
- HDFS NameNode Web UI
- Hive-on-Tez
- HiveServer2
- HttpFS
- Hue Client
- Hue Load Balancer
- Hue Server
- Impala Catalog Server
- Impala Server
- Impala StateStore
- Java Keystore Key Management Server (KMS)
- Kafka Broker Server
- Kafka Mirrormaker
- Knox
- Kudu
- Livy
- Oozie
- Ozone
- Phoenix
- Ranger
- Safenet Luna Hardware Security Modules (HSM) KMS
- Schema Registry
- Solr
- Spark History Server
- Streams Messaging Manager
- Streams Replication Manager
- Thales HSM KMS
- YARN Web UI

- Zeppelin
- ZooKeeper

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

### Limitations

- It is not possible to rename hostnames of cluster nodes in an Auto-TLS setup.

### Related Information

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

## Rotate Auto-TLS Certificate Authority and Host Certificates

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

### Using an internal CA (Use case 1)

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

### Using a custom CA (Use case 3)

1. Use the `/cm/commands/addCustomCerts` API command to replace the old certificates with new certificates in CMCA directory for each host. You must run this command for each host separately. An example of a curl command to upload the certificates to Cloudera Manager :

```
curl -u admin:admin -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{
    "location": "/opt/cloudera/AutoTLS",
    "interpretAsFileNames": true,
    "hostCerts": [ {
        "hostname": "ccycloud-10.vcdp71.root.hwx.site",
        "certificate":
            "/tmp/auto-tls/certs/ccycloud-10.vcdp71.root.hwx.site.pem",
        "key":
            "/tmp/auto-tls/certs/ccycloud-10.vcdp71.root.hwx.site.pem"
    } ]
}' 'https://ccycloud-7.vcdp71.root.hwx.site:7183/api/v41/cm/commands/addCustomCerts'
```

In the example above, the "location" should be omitted if Auto-TLS was enabled or rotated after 7.1, and the file paths should point to files on the CM server host.

2. Use CM API `/hosts/{hostId}/commands/generateHostCerts` to deploy the new certificates to each host. You must run this command for each host separately. An example curl command :

```
curl -u admin:admin -X POST --header 'Content-Type: application/json' --header
    'Accept: application/json' -d '{ "sshPort" :
    22, "userName" : "root", "password" : "cloudera" }'
```

```
'https://ccycloud-7.vcdp71.root.hwx.site:7183/
api/v41/hosts/250e1bb7-8987-419c-a53f-c852c275d299/commands/generateHost
Certs'
```

where '250e1bb7-8987-419c-a53f-c852c275d299' in the command above is the hostID.

## 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                        |