Data source parameters

The following data source parameters are used for integration with and connection to Cassandra.

Parameter	Description	Default value
cassandra.contactPoints	Cassandra hosts or IP addresses, separated by commas.	localhost
cassandra.port	Cassandra port for CQL clients.	9042
cassandra.keyspace.replication.factor	Cassandra replication factor for “auth” keyspace which is used by the authentication server. The replication factor should be set the same as in the TWCloud **application.conf** file.	1
cassandra.connection.max.attempts	Maximum number of attempts to connect to Cassandra on server startup.	10
cassandra.connection.sleep.before.attempt	Time interval before connection attempts in milliseconds.	30000
cassandra.username	The user name used for connecting to Cassandra.	cassandra
cassandra.password	The password used for connecting to Cassandra.	cassandra
cassandra.ssl.enabled	Enable SSL authentication for Cassandra.	false

Secure connection between Authentication server and Cassandra

You can establish secure connection between the Authentication server and Cassandra. You need to configure Authentication server Trust Store and Cassandra, for more details how to configure Cassandra, go to Client-to-node encryption. To configure Trust Store you will need to have Cassandra CA certificates and *cassandra.ssl.enabled* parameter should be set to *True.*

Authentication server Trust Store Configuration

CAC integration requires that a trust store exist, containing the Certificate Authority (CA) certificates who issues the user's certificates.

The following parameter properties need to be configured:

```
server.ssl.trust-store=config/truststore.jks
server.ssl.trust-store-type=JKS
server.ssl.trust-store-password=secret
server.ssl.client-auth=want
```

There is no need to manually generate the truststore. Create a directory, named truststore, under AuthServer/config/ and place all of the CA certificates into it. Upon startup of the authentication server, if truststore.jks does not exist, it will be created by importing the CA certificates located in Authserver/config/truststore. If you make changes to the certificates in the truststore directory, delete truststore.jks and restart the authentication service. This will recreate the truststore with the current set of CA certificates.

Cassandra Trust Store Configuration

In case, Cassandra parameter *require_client_auth* is set to *true:*

```
require_client_auth: true
```

You will need to Cassandra truststore: */usr/local/lib/cassandra/conf/server-truststore.jks* add TWCloud public certificate. More details how to configure Cassandra when *require_client_auth* is set to true >>