Create Encryption Key File

The platform utilizes a key file to encrypt and decrypt usernames and passwords for use in connecting to your relational or Hive datastores. This keyfile provides an extra layer of security through symmetric encryption.

NOTE: You must create and deploy this keyfile in order to create and use relational or Hive connections.

Credentials are encrypted using the AES-128-CBC algorithm.

Requirements for the keyfile:

- This file is a plain text file stored within the Trifacta® platform.
- This file must be deployed before any database connection is created.
- This file must contain a text string that is the key to use.
- The text string can be any string. It should be randomized and not easy to guess.
- After creation, this file cannot be modified.
- This file is shared for all JDBC connections. It does not need to be shared with any database server.

You, the customer, are responsible for the security of this file. It should be secured such that 1) only the root user has read/write access and 2) the Trifacta user has read only access. After the file has been created, it cannot be modified. If it needs to be moved, use the steps below to indicate its new location for the platform.

You must store this file within the Trifacta deployment and reference it through the platform configuration.

You can apply this change through the *Admin Settings Page* (recommended) or

`trifacta-conf.json`

. For more information, see *Platform Configuration Methods*.

1. Locate the following configuration. Specify the path to the keyfile relative to the top-level deployment location. Include the filename:

   ```
   "encryption.keyFile": "/opt/trifacta/conf/.key/customerKey",
   ```

2. Save your changes.

A platform restart is required.