# **Encrypting property values**

By default, Teamwork Cloud properties are stored as plain text. If required, any of these properties can be encrypted. For property encryption and decryption, you need to generate a pair of keys using our property encryption tool. The tool is provided as the *encryptor.jar* file and the steps below explain how to use it.



#### Prerequisites

The encryption tool uses Java 11. Therefore, the system **PATH** variable needs to point to the location of the *bin* folder of the Java 11 home directory, e. g. *C:\Java\Java11\bin* or /opt/Java/Java11/bin.

#### To encrypt Teamwork Cloud properties

- 1. Click the link to download the encryptor.iar file.
- 2. Open the command-line interface and navigate to the directory where the encryptor.jar file is located.
- 3. Run the java -jar encryptor.jar command. You should see the information on how to use the tool as displayed below.



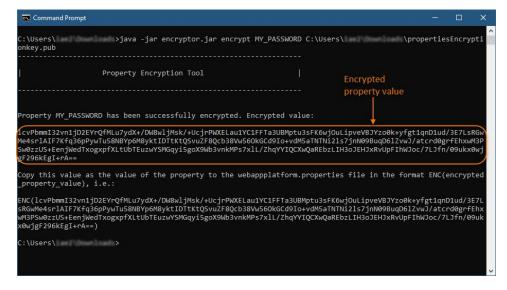
4. Run the java -jar encryptor.jar generate-keys <path\_to\_folder\_for\_keys> command to generate a pair of keys for property encryption and decryption. Make sure to replace the <path\_to\_folder\_for\_keys> placeholder with the actual path to the directory where you want to store the keys. You should see a confirmation that the keys have been successfully generated.



Keys for encryption and decryption

After executing the command, the following keys are created in the specified directory:

- propertiesEncryptionKey.pub a public key used to encrypt property values.
- propertiesEncryptionKey a private key used to decrypt property values.
- 5. To encrypt a property, run the java -jar encryptor.jar encrypt <unencrypted\_property\_value> <path\_to\_the public\_key> command. Make sure to replace the <unencrypted\_property\_value> and <path\_to\_the public\_key> placeholders with the actual property value and the path to the propertiesEncryptionKey.pub file. The tool will output the encrypted property value.



- 6. Go to the /opt/local/TeamworkCloud/configuration/ directory and open the application.conf file.
- In the application.conf file, replace the actual property value with the encrypted property value in the following format: ENC (encrypted\_property\_value).



### Example of an encrypted property

For example, an encrypted Cassandra password, should look similar to this one: password=ENC (lcvPbmml32vn1jD2EYrQfMLu7ydX+/DW8wljMsk/
+UcjrPWXELau1YC1FFTa3UBMptu3sFK6wjOuLipveVBJYzo0k+yfgt1qnD1ud
/3E7LsRGwMe4srlAlF7Kfq36pPywTu58NBYp6M8yktlDTtKtQSvuZF8Qcb38Vw56OkGCd9lo+vdM5aTN
TNi2ls7jnN09BuqD6lZvwJ/atcrd0grfEhxwM3PSw0zzUS+EenjWedTxogxpfXLtUbTEuzwYSMGqyi5goX9Wb3vnkMPs7xlL
/ZhqYYlQCXwQaREbzLlH3oJEHJxRvUpFlhWJoc/7LJfn/09ukx0wjgF296kEgl+rA==).

8. In the same application.conf file, add the esi.config.decrypt\_key\_file property and specify the path to the private key (the propertiesEncryptionKe file) as its value, e.g., esi.config.decrypt\_key\_file=C:\\shared\\keys\\propertiesEncryptionKey.



## Private key location

The private key (the properties Encryption Key file) should be in the location which Teamwork Cloud can access.

9. Save changes to application.conf file and restart Teamwork Cloud service.