Encrypting property values

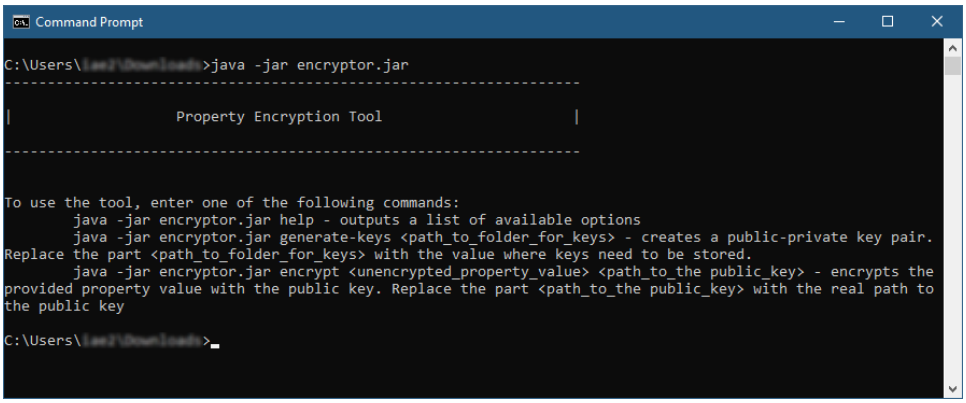
By default, Teamwork Cloud properties are stored as plain text. If required, any of these properties can be encrypted. For property encryption and decryption, you need to generate a pair of keys using our property encryption tool. The tool is provided as the *encryptor.jar* file and the steps below explain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



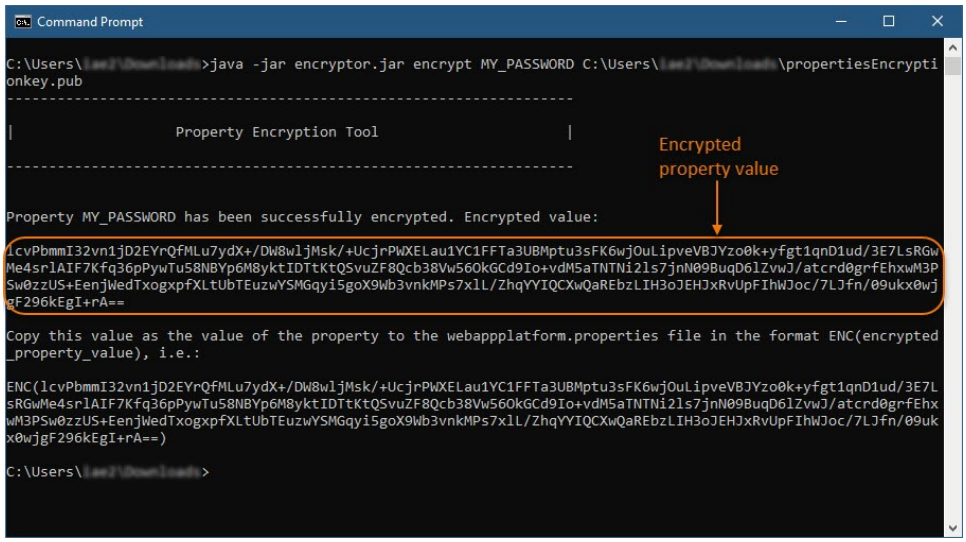
4. Run the **java -jar encryptor.jar generate-keys <path_to_folder_for_keys>** command to generate a pair of keys for property encryption and decryption. Make sure to replace the **<path_to_folder_for_keys>** placeholder with the actual path to the directory where you want to store the keys. You should 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.
7. 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 (lcvPbmmI32vn1jD2EYrQfMLu7ydX+/DW8wljMsk/ +UcjrPWXELau1YC1FFTa3UBMptu3sFK6wjOuLipveVBJYzo0k+yfgt1qnD1ud /3E7LsRGwMe4srlAIF7Kfq36pPywTu58NBYp6M8yktIDTtKtQSvuZF8Qcb38Vw56OkGCd9Io+vdM5aTN TNi2ls7jnN09BuqD6lZvwJ/atcrd0grfEhxwM3PSw0zzUS+EenjWedTxogxpfXLtUbTEuzwYSMGqyi5goX9Wb3vnkMPs7xlL /ZhqYYIQCXwQaREbzLIH3oJEHJxRvUpFIhWJoc/7LJfn/09ukx0wjgF296kEgI+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 *propertiesEncryptionKey* file) as its value, e.g., **esi.config.decrypt_key_file=C:\\shared\\keys\\propertiesEncryptionKey**.

> **Private key location**
>
> The private key (the *propertiesEncryptionKey* file) should be in the location which Teamwork Cloud can access.

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