



Encrypting/Decrypting values using AMI's default encrypter

Instructions: Encrypting values inside properties files

For this example, let's say you have the following property in your local.properties and you want to encode the password

```
Secret=Password123456
```

Note: If you see the following error: Error: Could not find or load main class please modify the tools script to point to `com.f1.utils.encrypt.EncrypterTool` or `com.f1.encrypt.EncrypterTool` one of the two should work

Step 1: Under /script, use the tools.sh (tools.bat for Windows) to create a 256-bit strength key (feel free to adjust the strength).

```
Linux: ./tools.sh --aes_generate /opt/ami/secret.aes 256
```

```
Windows: ./tools.bat --aes_generate C:/ami/amione/secret.aes 256
```

Step 2: Add this option to your start.sh (start.bat for Windows) so that AMI knows where the secret key for decoding encrypted properties is located

```
Linux: -Dproperty.f1.properties.secret.key.files=/opt/ami/secret.aes
```

```
Windows: -Dproperty.f1.properties.secret.key.files=C:/ami/amione/secret.aes
```

Step 3: using the same tools.sh (tools.bat for Windows), Encode the password and copy the output text into your clipboard

```
Linux: ./tools.sh --aes_encrypt /opt/ami/secret.aes Password123456
```

```
Windows: ./tools.bat --aes_encrypt C:/ami/amione/secret.aes Password123456
```

```
Ex: fYjHz8Dr4o7XjZcOd1BhtKzV9U5MpZMpTyGlu-mpheL4qV-ZX-yUads
```

Step 4: Change your local.properties file to use the encrypted value instead, by enclosing with `${CIPHER:...}`

```
amiscrypt.variable.secret=${CIPHER:fYjHz8Dr4o7XjZcOd1BhtKzV9U5MpZMpTyGlu-mpheL4qV-ZX-yUads}
```

Using the above format produces the following warning when launching AMI:

```
WARNING: PROPERTY Secret IS USING LEGACY SYNTAX, SHOULD BE: ${CIPHER:ENCRYPTER:ciphertext}  
instead of ${CIPHER:ciphertext}, it is safe to ignore this message.
```

Step 5: Restart AMI

In the AmiOne.log you'll see that the value for the secret property is substituted with ***** for security purposes. You can also see the password listed in the AMI web interface. Go to Dashboard->Session Variables.