Oracle Materials Control

MCweb Password Encryption

Table of Contents

Introduction

This document will explain the new functionality to use encrypted passwords in the configuration files of the Materials Control MCweb client application. Encrypted passwords are required to follow current security standards.

Deployment:

This new function is available with MCweb in version 7.00.33.1358 and higher

As a pre-requisite Microsoft .NET Framework version 3.5 or higher must be installed on the machine where the encryption tool is executed.

The Encryption Tool will be delivered as a single executable file and does not require any installation procedure.

In versions < 8.30.8.x it will be delivered as "MCweb_EncryptPassword.zip"
Unpack the archive to a directory of your preference or to the Materials Control application root folder.

In versions 8.30.8.x and higher it will be delivered with the standard application in the Materials Control application root folder.
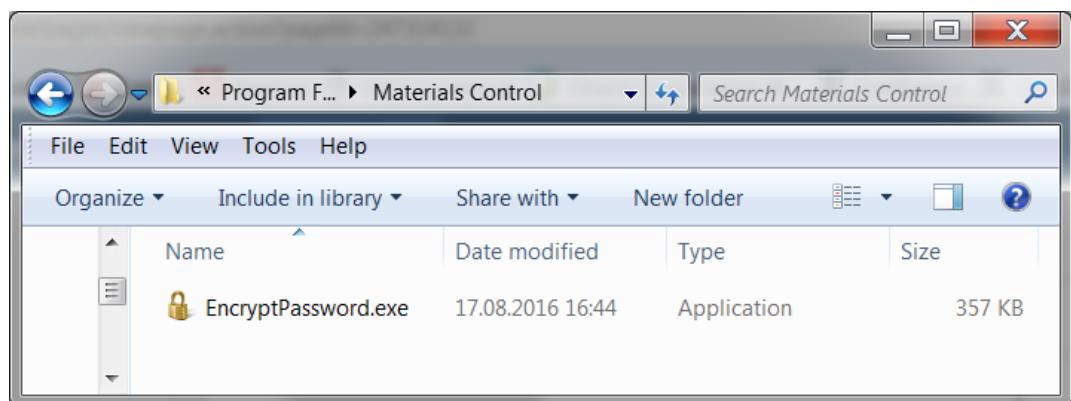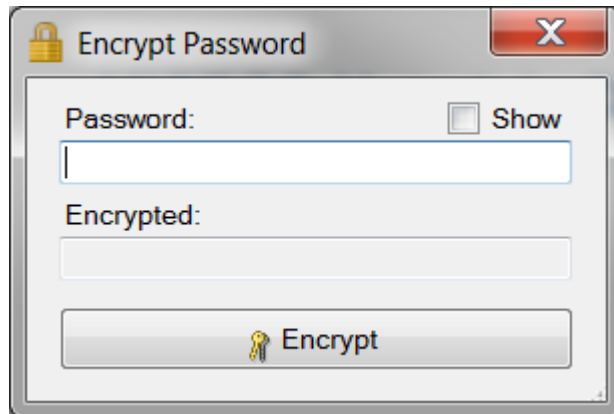
Encryption:

Simply double click the executable EncryptPassword.exe to start the application.

The GUI consists of …
- a text box to enter the password named "Password"
- a check box to unmask the entered password named "Show"
- a read-only field to show the encrypted password named "Encrypted" -   a button to start the encryption process named "Encrypt"

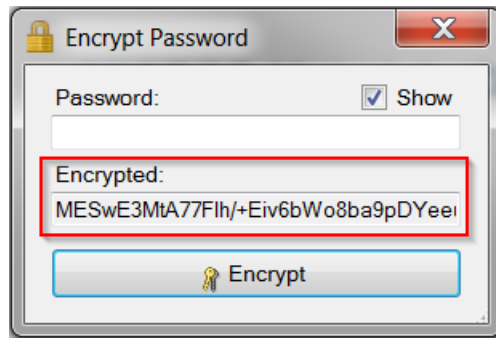Enter a password in the text box "Password":

If desired mark the checkbox "Show" to read the entered password in clear text instead of asterisks as mask characters:
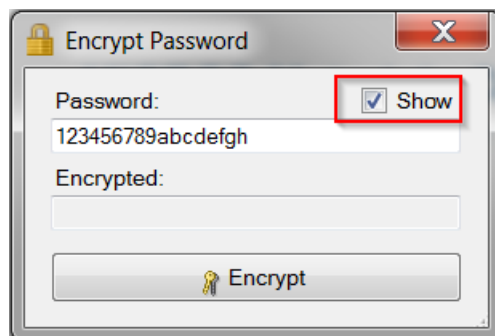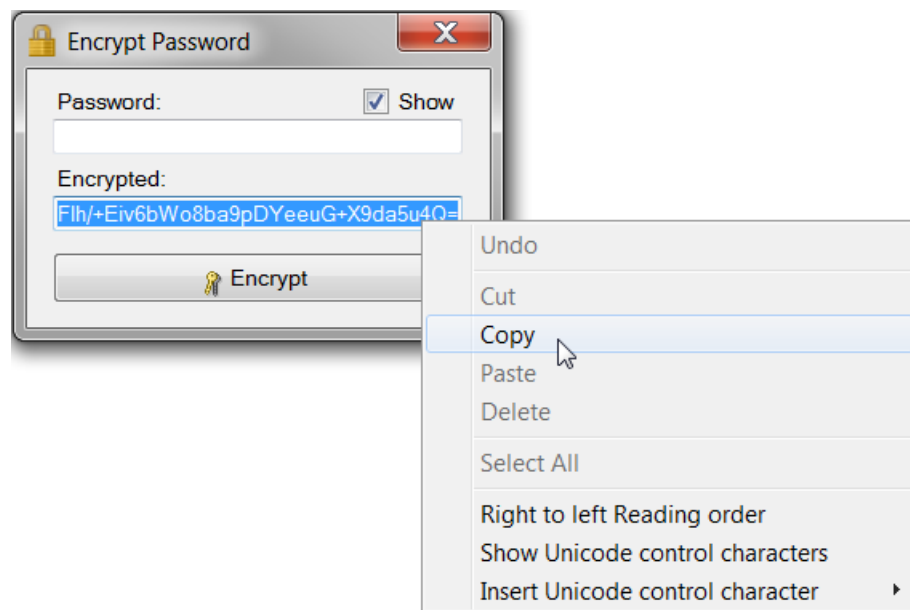

To start the encryption process, please click on the button "Encrypt":

The encrypted password will be displayed in the read-only field "Encrypted":

Now right click with the mouse into this field and select the function "Copy" from the context menu.
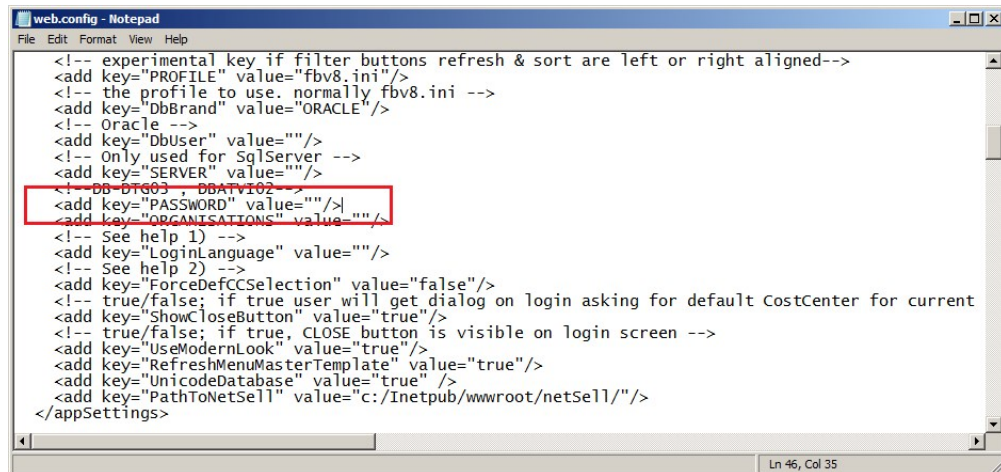
Modification WEB.CONFIG:

In the installation directory of the MCweb application the file named WEB.CONFIG can be found.

Before editing this file it is strongly recommended to create a backup of this file!
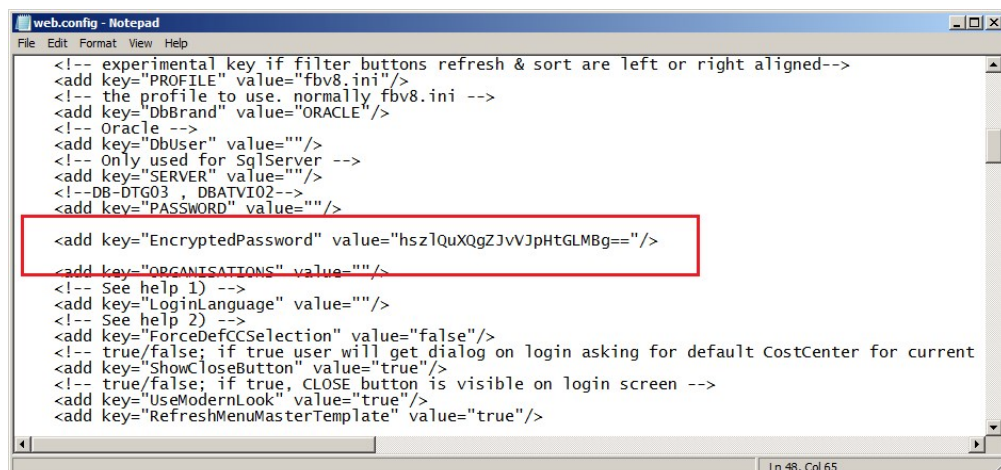
Open the WEB.CONFIG with an editor.

Here the key "PASSWORD" can be found. This usually is the place where the Oracle schema password must be defined.

In order to activate the support for encrypted passwords a line as below must be inserted:

   `<add key="EncryptedPassword" value="hszlQuXQgZJvVJpHtGLMBg=="/>`
(… where the **red** part must be the copied part from the password encryption tool).

Once this key is existing the system will no longer check the key "PASSWORD", but will check the value defined for "EncryptedPassword" only.

WEB.CONFIG for Mobile Solutions:

Same as in MCweb this encryption also can be used in the WEB.CONFIG file for the Mobile Solutions Web Services.

```
Web.config - Notepad
File  Edit  Format  View  Help
                              <sectionGroup name="webServices" type="System.Web.Configuration
                                  <section name="jsonSerialization" type="System.Web.Conf
                                  <section name="profileService" type="System.Web.Configu
                                  <section name="authenticationService" type="System.Web.C
                                  <section name="roleService" type="System.Web.Configurat
                              </sectionGroup>
                          </sectionGroup>
                      </sectionGroup>
                  </configSections>
                  <appSettings>
        <add key="PathToRoot" value="."/>
        <add key="LogPath" value="C:/temp"/>
        <add key="DbBrand" value="ORACLE"/>
        <add key="SERVER" value="YOUR_ORACLE_DB_NAME"/>
        <add key="CATALOG" value="YOUR_ORACLE_USER"/>
        <add key="USER" value="YOUR_ORACLE_USER"/>
        <add key="PASSWORD" value="YOUR_ORACLE_PASSWORD"/>
        <add key="EncryptedPassword" value="hszlQuXQgZJvVJpHtGLMBg=="/>
        <add key="PROFILE" value="FBV8.ini"/>
                  </appSettings>
                  <connectionStrings/>
                  <system.web>
                      <!--
                                                                          Ln 24, Col 68
```