

MICROS Materials Control

FMLOGIN.INI



Product Version **8.8.10.42.1528**

Document Title:	FMLOGIN.INI
Author:	Joerg Trommeschlaeger
Department:	Materials Control
Date:	20.01.2015
Version No. of Document:	1.5

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

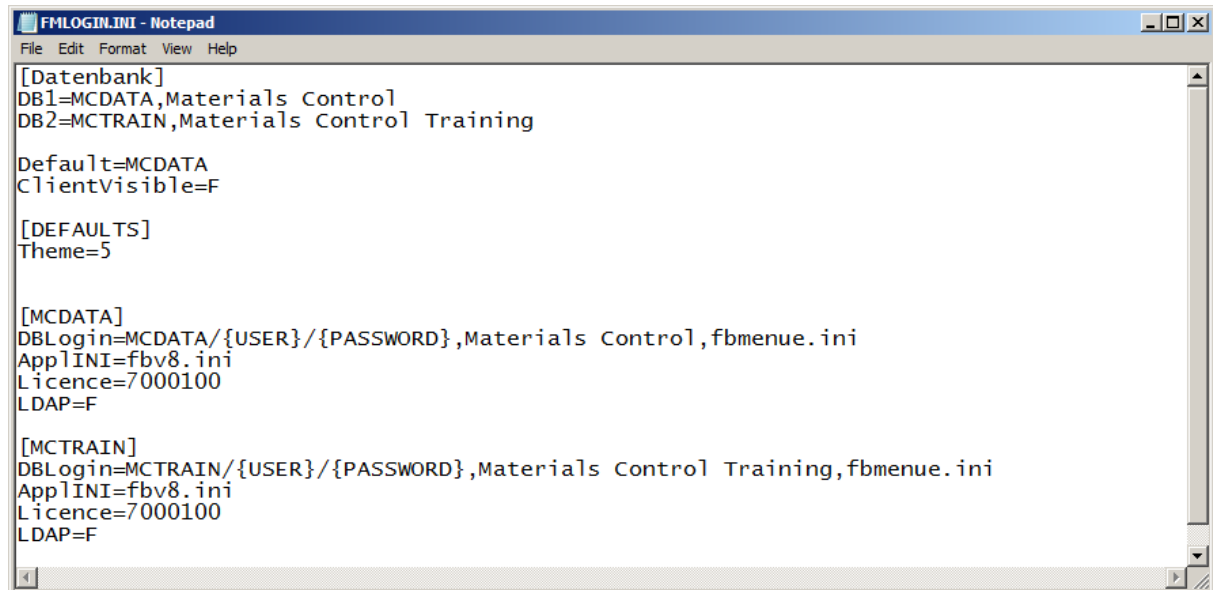
Table of Contents

CONFIGURATION FMLOGIN.INI:	4
HEADER SECTION:.....	5
DEFAULT DB SECTION:.....	6
OTHER DEFAULTS SECTION:.....	7
CONNECTION DETAILS SECTION:.....	8
ORACLE USER PASSWORD ENCRYPTION:.....	9
SELECTED LICENSE.....	12
DOMAIN USER SUPPORT.....	14
FMLOGIN.INI:.....	14
USER CONFIGURATION:.....	15
USING THE THICK CLIENT:.....	16
USING THE MCWEB CLIENT:.....	17
PRE-REQUISITES:.....	17
OVERVIEW:.....	17
ENABLING WINDOWS AUTHENTICATION IN IIS.....	18
ADJUSTING WEB.CONFIG.....	20
ACTIVE DIRECTORY (LDAP) LOGIN PAGE.....	21
BROWSER SUPPORT.....	22

Configuration FMLOGIN.INI:

This document describes the configuration of the login control file and features related to the login screen.

The file FMLOGIN.INI controls the access to the database files from the client application. This document will show the available features.



```
[Datenbank]
DB1=MCDATA,Materials Control
DB2=MCTRAIN,Materials Control Training

Default=MCDATA
ClientVisible=F

[DEFAULTS]
Theme=5

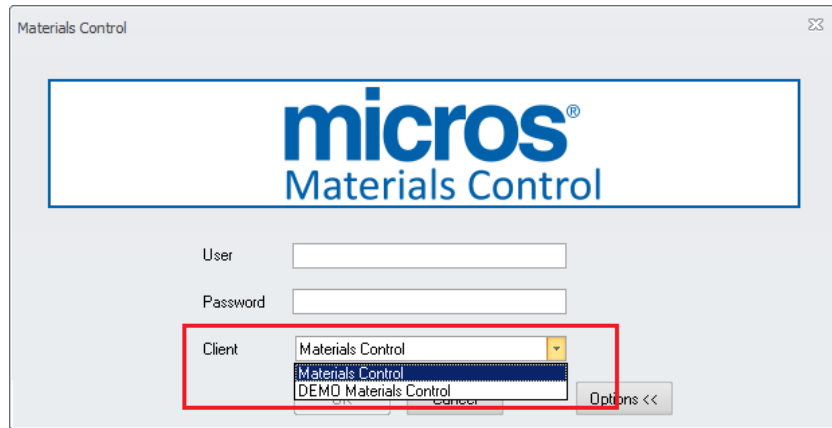
[MCDATA]
DBLogin=MCDATA/{USER}/{PASSWORD},Materials Control,fbmenu.ini
ApplINI=fbv8.ini
Licence=7000100
LDAP=F

[MCTRAIN]
DBLogin=MCTRAIN/{USER}/{PASSWORD},Materials Control Training,fbmenu.ini
ApplINI=fbv8.ini
Licence=7000100
LDAP=F
```

The file is divided into several sections:

Header Section:

This section contains the list of databases available to be selected in the login dialog.

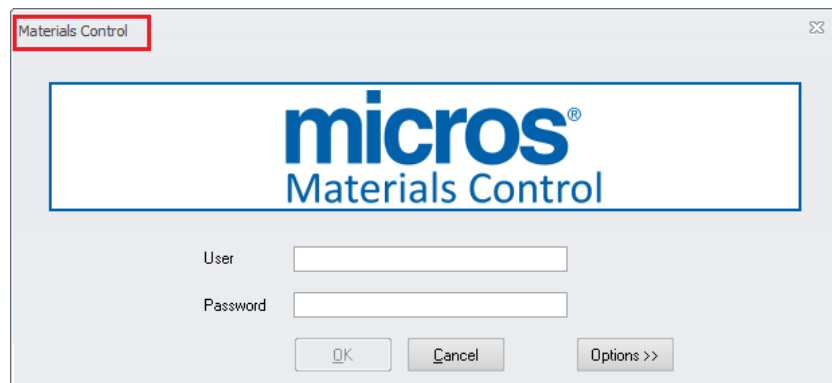


[Datenbank]

DB1=MCDATA,Materials Control

DB2=MCTRAIN,Materials Control Training

- "DB1=" Sequence number of the database, must be sequential!
- "MCDATA" Name of the database, unique identifier for the connection detail section below (-> link to SQL.INI)
- "Materials Control" Name of the database in the login dialog when selected



Default DB Section:

Here the default DB must be defined. The database defined here will be shown as default client after click on the button **Options >>**:

Default=MCDATA

Since version 8.8.10.xx the database selector could be shown by default, skipping the **Options >>** button:

ClientVisible=T

ClientVisible=F

Other Defaults Section:

In this section other default values can be defined.
(Available since version 8.6.6.30.xx)

[DEFAULTS]
Theme=5

Supported Themes:

- 4 = Office2010_R2_Blue
- 5 = Office2010_R2_Silver

Connection Details Section:

This section contains the connection settings per database.

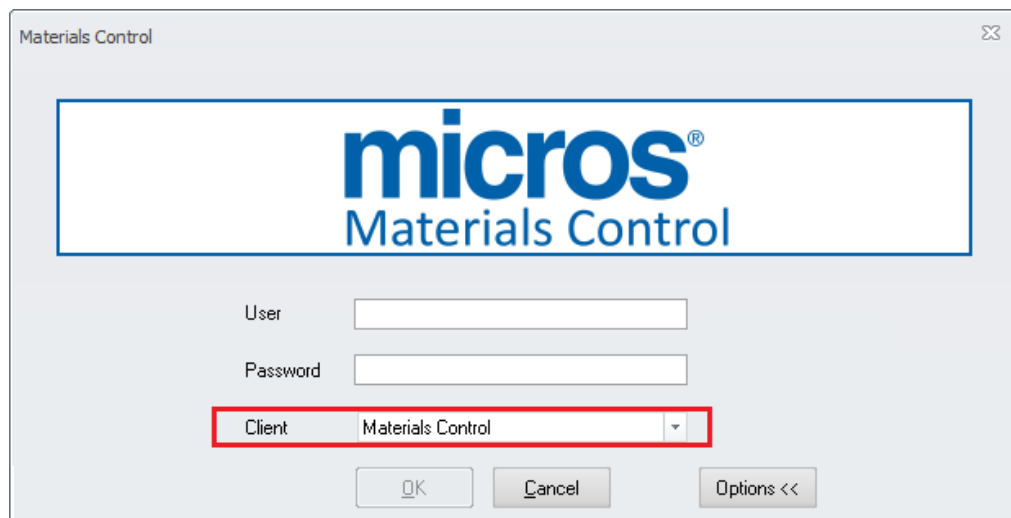
```
[MCDATA]
DBLogin=MCDATA/[USER]/[PASSWORD],Materials Control,fbmenu.ini
AppINI=fbv8.ini
```

[MCDATA]:
The first line of each connection block refers to the selection in the database list. Here in this example [MCDATA] is linked to the entry for DB1 in the header section. If the user selects "Materials Control" from the database list or does not select any database (default DB) the application will jump to this section.

```
DBLogin=MCDATA/[USER]/[PASSWORD],Materials Control,fbmenu.ini
```

This part contains the connection parameters:

- "MCDATA" represents the name of the Oracle table space
- "[USER]" represents the Oracle user name for the table space
Note: The user name must be written without [] -> USER
- "[PASSWORD]" represents the password for the Oracle User (without [])
Note: The password must be written without [] -> PASSWORD in clear text. Please see below for password encryption!
- "Materials Control" represents the text shown in the database list



- "fbmenu.ini" defines the menu structure file to be used. Please do not change this value!

```
AppINI=fbv8.ini
```

This value defines the standard control file to be used. Please do not change this value!

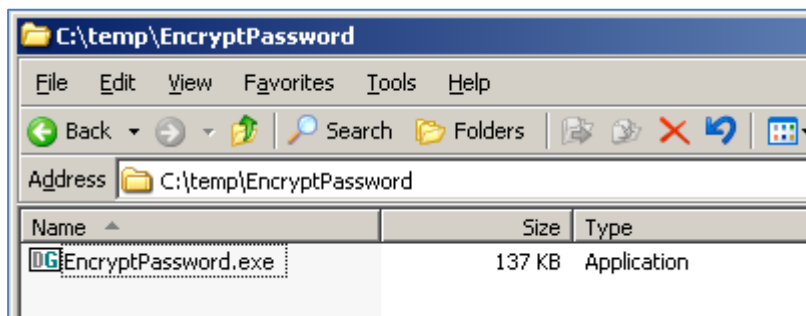
Oracle User Password Encryption:

Since version 8.7.10.xx the oracle password can be encrypted. Here the same logic as for MCweb is used.

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, delivered as "MCweb_EncryptPassword.zip" and does not require any installation procedure.

Unpack the archive to a directory of your preference.



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":



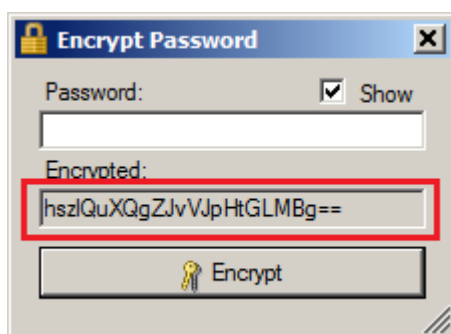
If desired mark the checkbox “Show” to read the entered password in clear text instead of asterisks as mask characters:



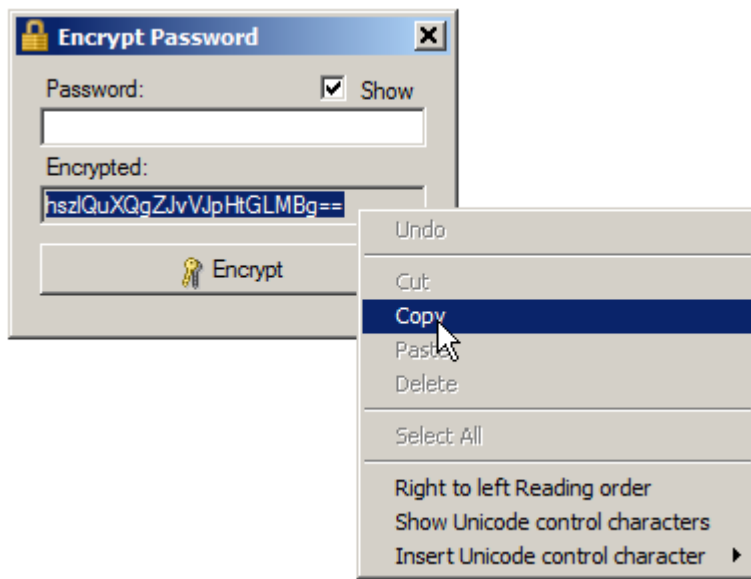
To start the encryption process, please click on the button “Encrypt”:



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.

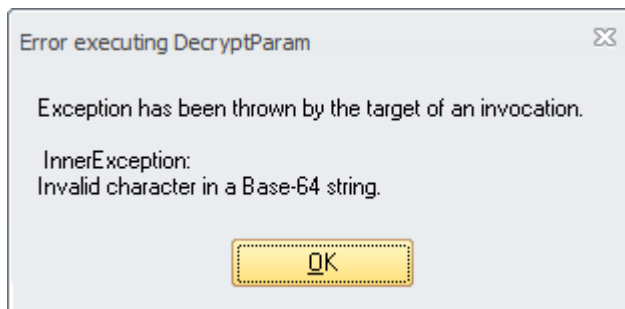


This encrypted password now can be used in the FMLOGIN.INI:

```
DBLogin=MCDATA/your_user/[sZUps1d2+jezgJpzaNz=],Materials Control,fbmenu.ini
```

The system expects an encrypted password if it is presented in []. A clear type password must be defined without [].

In case of an incorrect Oracle password the system will show the following message:

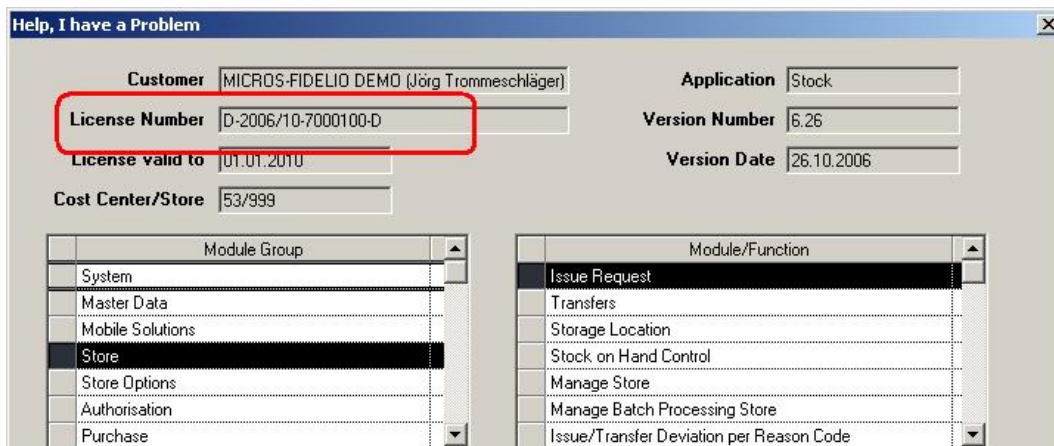


Selected License

In certain scenarios it is required to use one client application to connect to multiple databases. In this case it is important that the application could use the correct license file for the connected database since the license file controls the access to the modules and delivers the correct license name to the reports. (Available since version 8.4.02.xx)

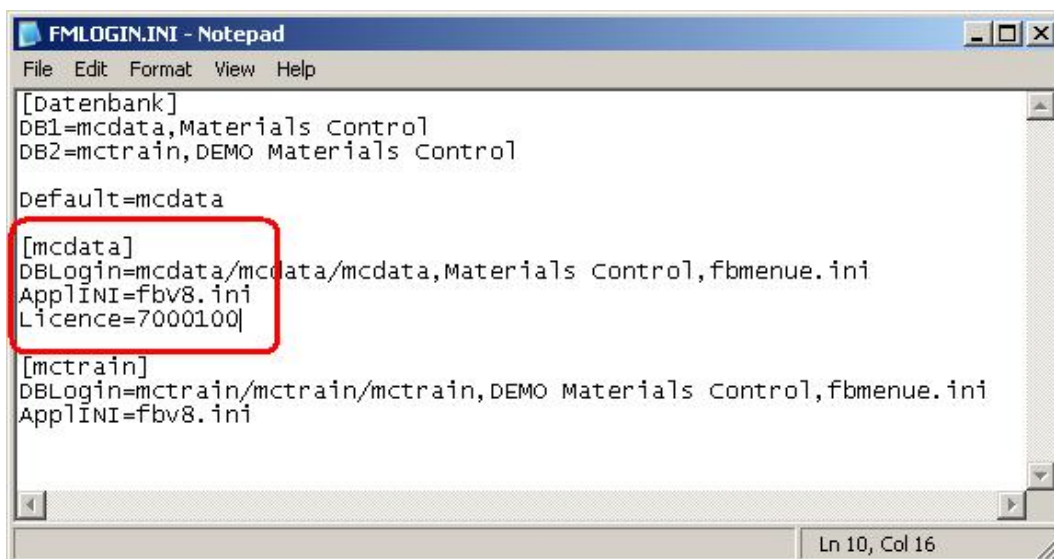
```
[MCDATA]
DBLogin=MCDATA/[USER]/[PASSWORD],Materials Control,fbmenue.ini
AppINI=fbv8.ini
Licence=700xxxx
```

The license information is stored in the ETC.DLL in the local client installation (\Program Files\Materials Control). This license file contains a unique license number. This number can be seen in the hotline function (accessible from all modules in the "Help" menu):



The important part is the 7-digit number starting with 7, in this case 7000100.

Open the login configuration file FMLOGIN.INI and search for the section of this database:

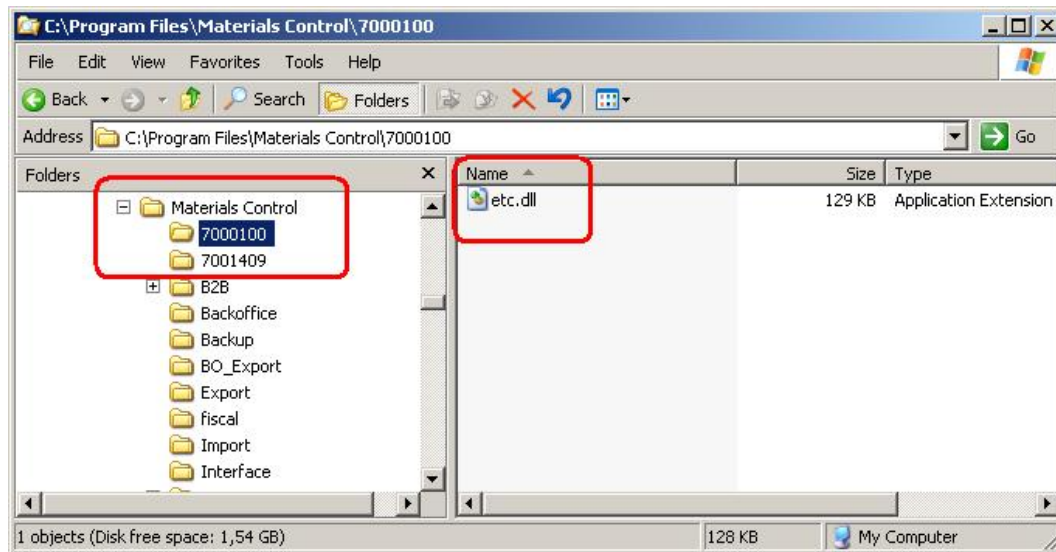


Add a new entry here in this section:

License=<license number>

Once this entry exists the main application FMSYSTEM (and all sub modules) will ignore the license file in the main application root directory.

The system will now search for a subfolder named like this number and use the license file stored in that folder. Please note that the system will check the license file in that folder against the used number.



If one client is used to access multiple databases now always the correct name will be used on all reports.

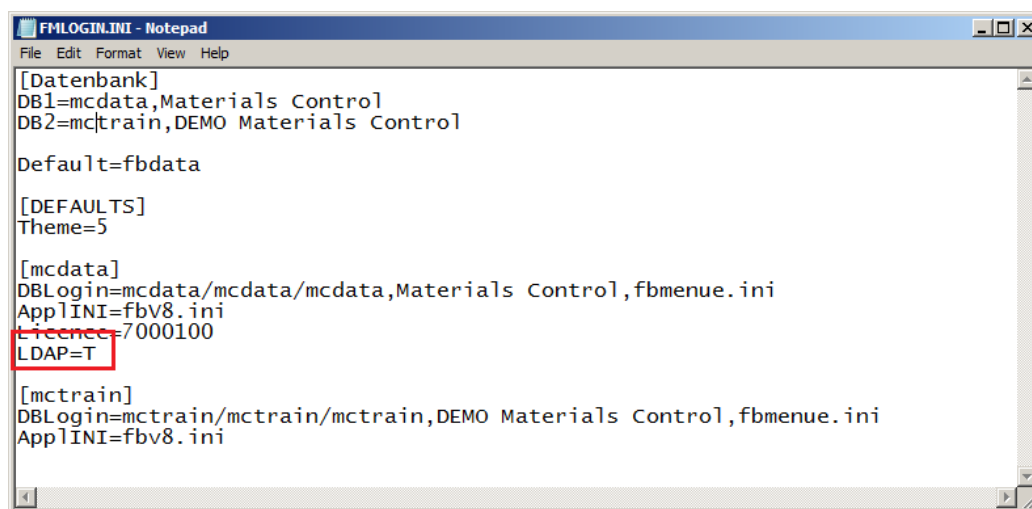
Domain User Support

Since version 8.7.30.xx the application allows to use the Windows Domain User to login into Materials Control. Using this feature Domain Users known to Materials Control do not need to enter the user name and the password anymore.

In order to use this function the following must be configured:

FMLOGIN.INI:

Open the FMLOGIN configuration file and select the section for the database to be configured.



```
FMLOGIN.INI - Notepad
File Edit Format View Help
[Datenbank]
DB1=mcddata,Materials Control
DB2=mctrain,DEMO Materials Control

Default=fbdata

[DEFAULTS]
Theme=5

[mcddata]
DBLogin=mcddata/mcddata/mcddata,Materials Control,fbmenue.ini
AppINI=fbv8.ini
Licence=7000100
LDAP=T

[mctrain]
DBLogin=mctrain/mctrain/mctrain,DEMO Materials Control,fbmenue.ini
AppINI=fbv8.ini
```

```
[MCDATA]
DBLogin= MCDATA/ MCDATA/MCDATA,Materials Control,fbmenue.ini
AppINI=fbv8.ini
Licence=7000100
LDAP=T
```

The new entry "LDAP=T" must be added. Once done please save and close the file. Now restart the application.

User Configuration:

Open the FMLOGIN configuration

Go to System > Users:

The screenshot shows the 'Manage Users' application window. The 'Login Name' field is set to 'admin' and is active. The 'User' field is empty, 'Password' is masked with asterisks, and 'Department' is set to 'Systems Management'. The 'Domain\Account Name' field is highlighted with a red rectangle and is currently empty. Other fields include 'Phone', 'Fax', 'E-Mail', 'Language' (set to 'English'), and 'Information'. A 'Default View Filter' section on the right has 'Department' and 'All' options.

Here now a new field is visible. For each user the domain account name should be defined.

Example:

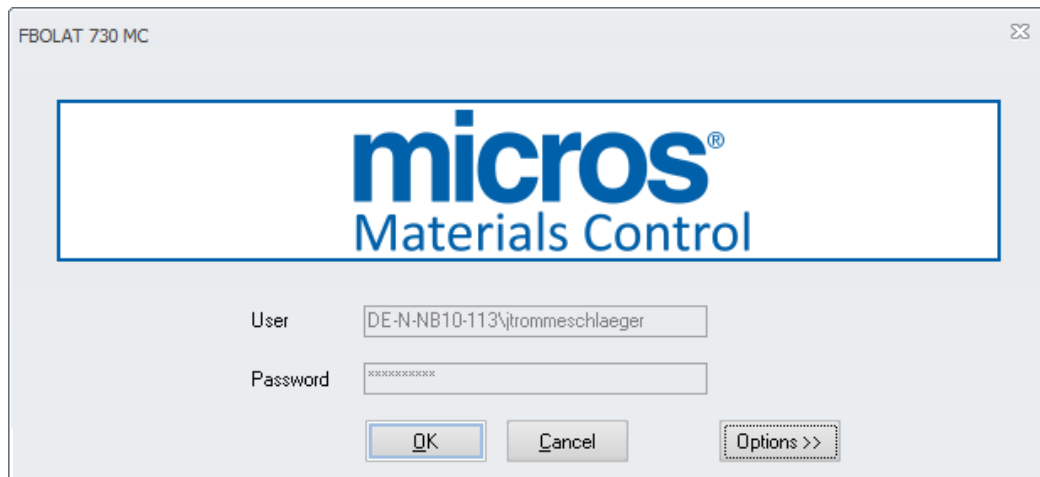
The screenshot shows the 'Manage Users' application window with the 'admin' user configuration. The 'Login Name' is 'admin' and is active. The 'User' field is 'SystemAdministrator', 'Password' is masked, and 'Department' is 'Systems Management'. The 'Domain\Account Name' field is now filled with 'DE-N-NB10-113\trommeschlaeger'. Other fields are the same as in the previous screenshot.

The application user “admin” is assigned to the domain user “DE-N-NB10-113\trommeschlaeger”.

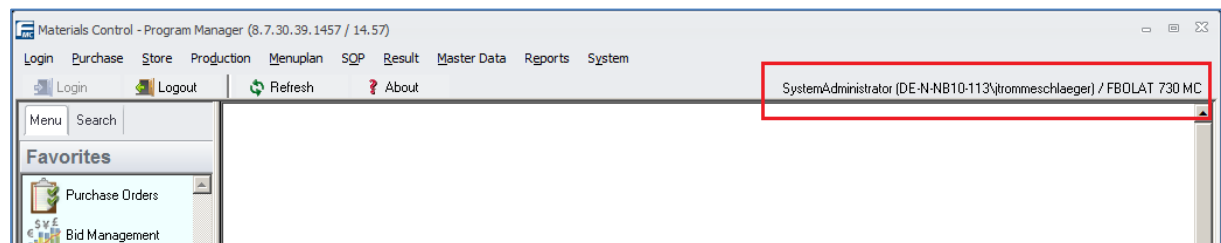
Using the Thick Client:

When starting the Materials Control the application looks if the current Windows user can be found in the MC user table.

If this exists ...



... the user does not have to enter the user name or the password anymore. He may select a different database using the Options button, otherwise he can just click OK to login.



In Materials Control now at the top right corner both, the application user as well as the Windows user, are shown.

For all Windows users not assigned to a Materials Control user the behaviour will be the same as without using this function. User name and password must be entered.

Using the MCweb Client:

This feature also could be used with MCweb.

Pre-requisites:

- Client Computers and Web server must reside in the same domain. Otherwise the current domain user will be unknown to the web server.
- Clients must have a direct connection to the server (no proxy in between)
- Intranet only

Technically, LDAP authentication via NTLM is possible over an Internet connection, but strongly advised against due to security and general feasibility concerns.

Overview:

To enable Active Directory (LDAP) authentication in MCweb, following steps have to be performed:

1. Enable Windows Authentication in IIS
2. Adjust the Web.config (use supplied default Web.config in install package)
3. Configure mappings from the Domain user to the MCweb user (in Materials Control / User Management)
4. Distribute links / train users to open the LDAP Login page

ENABLING WINDOWS AUTHENTICATION IN IIS

Windows Server 2008 (IIS 7):

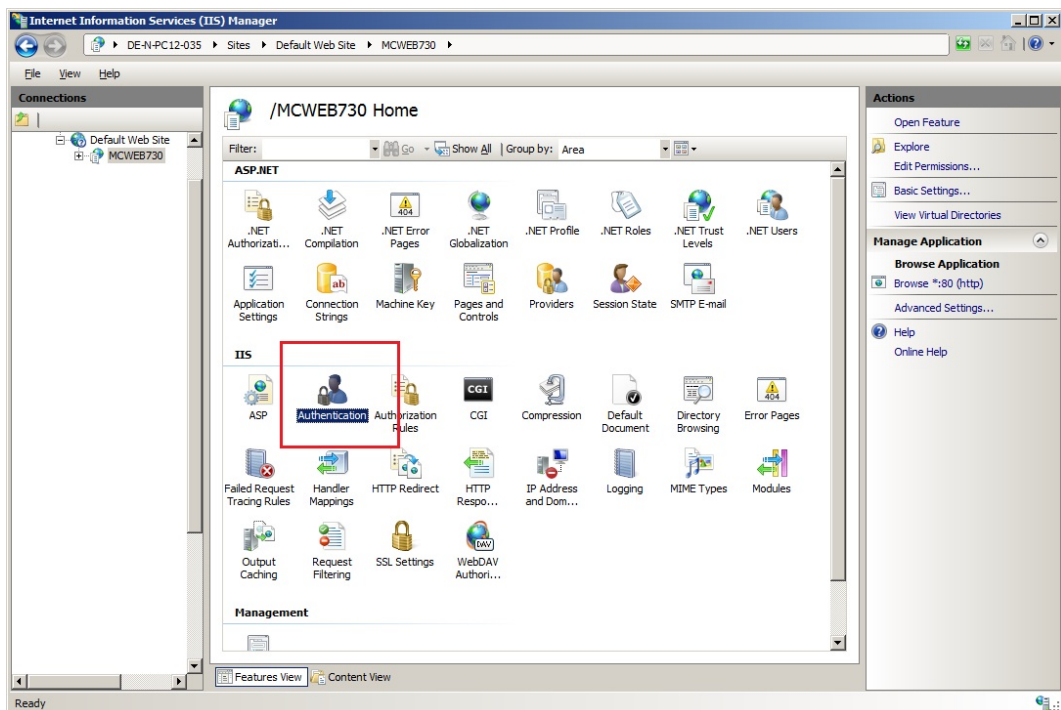
<http://technet.microsoft.com/en-us/library/cc754628%28v=ws.10%29.aspx>

Windows Server 2003 (IIS 6):

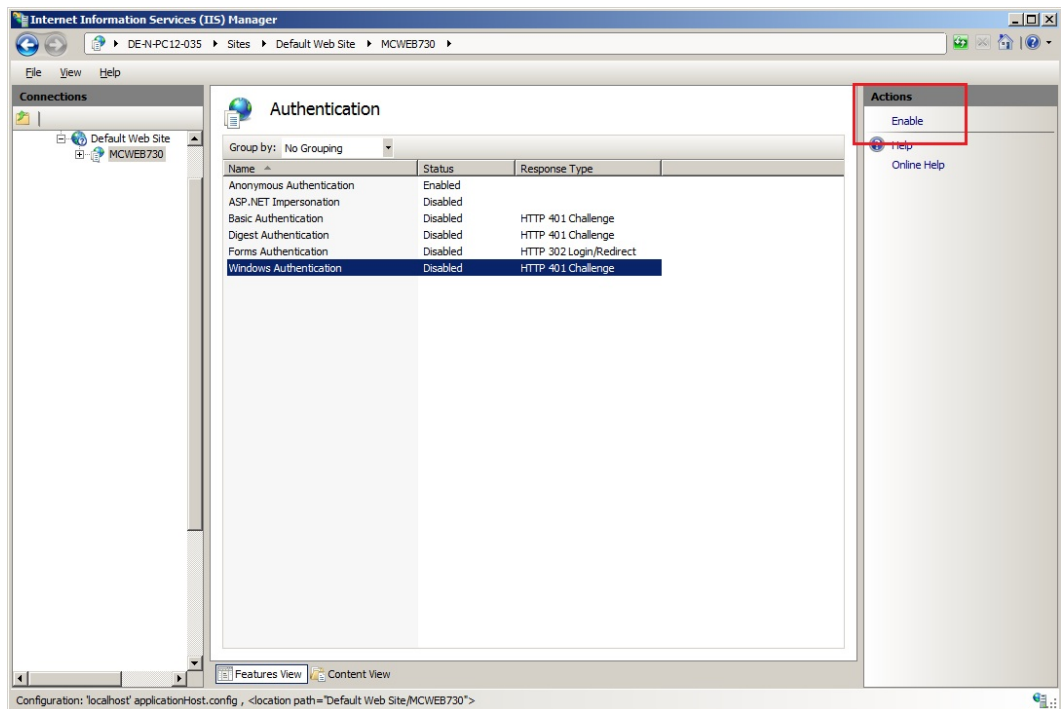
<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/5f8fe119-4095-4094-bba5-7dec361c7afe.mspx?mfr=true>

Example for IIS 7:

Open the Internet Information Services (IIS) Manager and browse to your MCweb instance:



Locate the feature „Authentication“ and open it:



Here the option „Windows Authentication“ is listed. In the top right corner the function could be enabled.

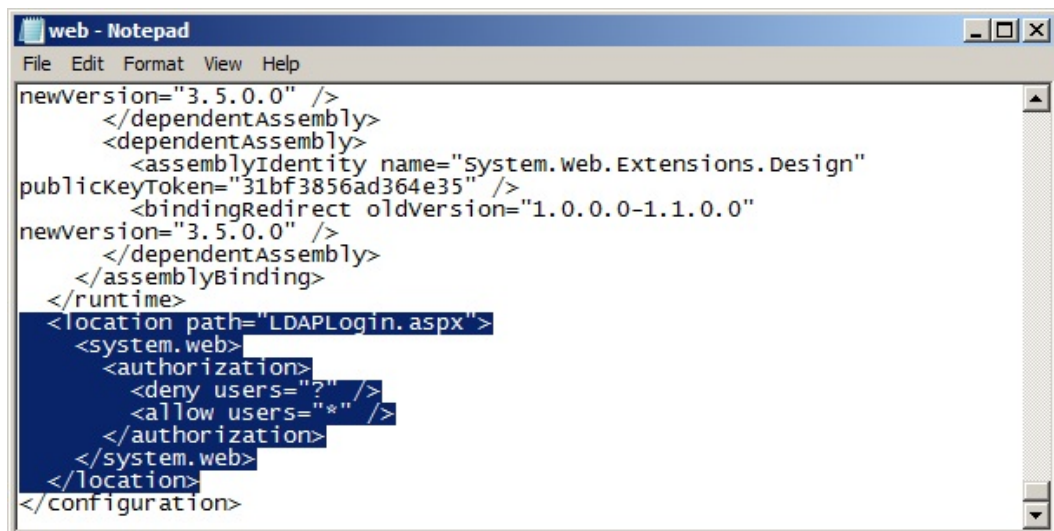
Note: The Windows Authentication is not visible if the Webserver is not connected to a domain.

ADJUSTING WEB.CONFIG

The Web.config needs to be adjusted to force client authentication on the LDAP Login page. This is necessary because “anonymous” access (via regular Materials Control user/password) to the application should still be allowed in general, and the browser/client does not send any authentication information by itself, unless it is explicitly forced to do so.

This can be accomplished in two ways:

1. Use the default Web.config supplied in the MCweb installation package
 - a. Make a backup of the original Web.config
 - b. Overwrite the original with the default included in the package
 - c. Copy the entire <appSettings> section from the backup and overwrite the empty/default values of the new Web.config
2. Alternatively, if the Web.config contains other adjustments besides <appSettings> that should not be lost, the new section can be added manually
 - a. Open the default Web.config and scroll to the bottom
 - b. Locate the <location path="LDAPLogin.aspx">[...]</location> section
 - c. Copy the entire section to the original Web.config



```
web - Notepad
File Edit Format View Help
newVersion="3.5.0.0" />
  </dependentAssembly>
  <dependentAssembly>
    <assemblyIdentity name="System.Web.Extensions.Design"
publickeyToken="31bf3856ad364e35" />
    <bindingRedirect oldVersion="1.0.0.0-1.1.0.0"
newVersion="3.5.0.0" />
  </dependentAssembly>
</assemblyBinding>
</runtime>
<location path="LDAPLogin.aspx">
  <system.web>
    <authorization>
      <deny users="?" />
      <allow users="*" />
    </authorization>
  </system.web>
</location>
</configuration>
```

Save & close the file.

Restart the IIS service using the command IISRESET.

ACTIVE DIRECTORY (LDAP) LOGIN PAGE

The LDAP Login page can be reached via the URL:

<http://<WebAppURL>/LDAPLogin.aspx>

If the Web.config is configured to allow connection to multiple databases, the Company/DB to log in to can be supplied as URL parameter:

<http://<WebAppURL>/LDAPLogin.aspx?company=DBName>

In general the LDAP Login page functions and looks similar to the regular login page:



The screenshot shows the login interface for Micros Materials Control. It includes the company logo, a 'User' text input field, a 'Company' dropdown menu, and a 'Login' button.

The “User” field in this case contains the read-only “DOMAIN\Username” that needs to be entered in the User Management module for a successful user mapping, and of course varies depending on the user who visits the site. If no valid authentication (data delivered by the browser) can be acquired, the user is automatically redirected to the regular login page.

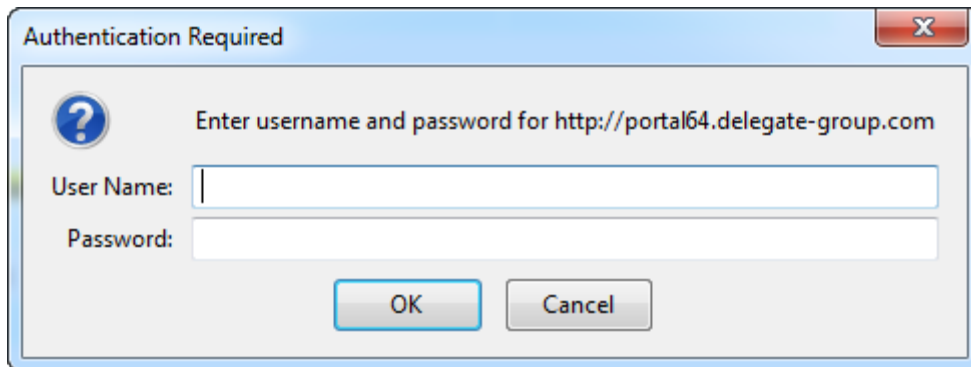
In the ideal case the user will not even see this page and be logged in seamlessly, but this depends on the information the user has provided and of course whether the login itself was successful.

The user will see this page, if:

- An unrelated error happened during login (DB connectivity, etc.)
- The current Domain user is not mapped to a Materials Control user on the selected DB.
- Multiple databases/Companies are configured in Web.config, but no Company was supplied via URL parameter

BROWSER SUPPORT

Both Firefox and Internet Explorer support Active Directory (LDAP) authentication, however there is a caveat when using Firefox; unlike IE, Firefox does not automatically have access to the user credentials of the currently logged on Windows user – instead, upon visiting the LDAP Login page, the browser will ask the user for his Windows credentials once¹, which are then used for the LDAP authentication:



If the user clicks Cancel he will be redirected to the regular login page. Note that this authentication prompt is a built-in browser feature and cannot be influenced by the Web application.

The credentials will be saved/cached until the browser is closed.

MICROS-FIDELIO GmbH
Europadamm 2-6
41460 Neuss
Germany
Phone: +49 2131-137 0 | Fax: +49 2131-137 777

¹ The credentials will be saved/cached until the browser is closed.