

# MICROS Materials Control

## Password & User Account Management



Product Version 8.7.30.37.1457

Document Title:	Password Handling
Author:	Joerg Trommeschlaeger
Department:	Materials Control
Date:	12.03.2013
Version No. of Document:	1.2

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

---

<b>INTRODUCTION:</b>	<b>4</b>
<b>FUNCTIONALITY:</b> .....	<b>4</b>
<b>PASSWORD ENCRYPTION</b> .....	<b>4</b>
<b>PASSWORD CASE-SENSITIVE</b> .....	<b>5</b>
<b>LAST LOGIN:</b> .....	<b>5</b>
<b>ENABLE PASSWORD MANAGEMENT:</b> .....	<b>6</b>
<b>FORCE PASSWORD CHANGE MANUALLY:</b> .....	<b>10</b>
<b>PASSWORD MASK:</b> .....	<b>11</b>
<b>PASSWORD LENGTH:</b> .....	<b>12</b>
<b>PASSWORD RE-USE:</b> .....	<b>12</b>
<b>PASSWORD RETRIES &amp; ACCOUNT LOCK:</b> .....	<b>13</b>
<b>PASSWORD EXCLUSION LIST:</b> .....	<b>15</b>
<b>FORBIDDEN PASSWORDS:</b> .....	<b>17</b>
<b>AUTOMATED ACCOUNT LOCKING:</b> .....	<b>22</b>
<b>SCHEDULER &gt; DAILY MAINTENANCE</b> .....	<b>22</b>

---

## Introduction:

This document will explain in detail the features related to password management in Materials Control.

The minimum required version of Materials Control is 8.6.6.30.17.1338.

## Functionality:

The application offers several features & functions to control password policies within Materials Control.

Some of the functions described below are available since older versions, some were introduced with the above mentioned version, some features were introduced in higher versions.

All features are supported by the classic thick client of Materials Control as well as MCweb (where applicable).

## Password Encryption

Version 8.7.20.xx and higher:

Since our customers are looking more on data security the user passwords are stored in the database as encrypted strings.

They cannot be viewed in clear text with any tool:

	BST_ID	BST_NAME	BST_PASSWD
	1	Admin	4GK7zKF7n5/GgeVYb1z57ueMhoc=
	1000001	albecig	e6FxuY/QjGP5T+2mAW82LU3Ceig=
	1000002	angegas	BX5wJcRLL93cNgeCai8W/UUvyT+0=
	1000003	danigra	U+V1BcqH8FEm182iG18dKCzG4b8=
	1000004	gianmas	1eDjgumP+D9qTfgwZAYC5/bFjkw=
	1000005	maurdej	Slit5Pm1T8BkaiHjY10cYsH0Xes=

The encryption algorithm used by the application also incorporates the user name as well. As a result of this a change of the user name always requires the change of the password as well:



**NOTE: There is no secret backdoor entry!**  
**If the passwords are lost the database is unusable!**

## Password Case-Sensitive

Version 8.7.20.xx and higher:

The user passwords are case-sensitive, means if the user enters “Micros” as password, the system will read it as “Micros” and not as e.g. “micros”.

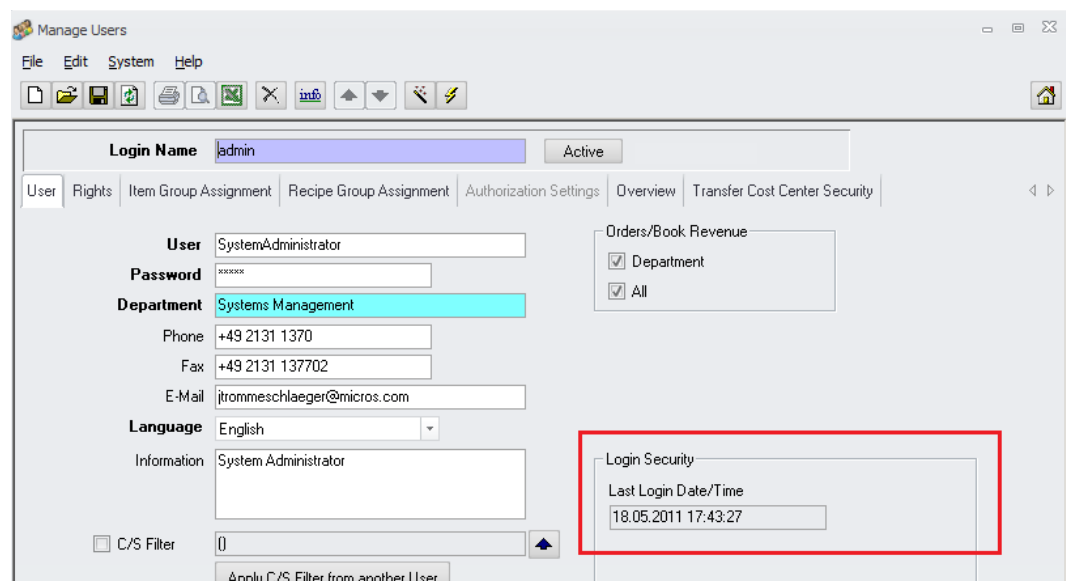
User passwords are mostly defined in lowercase only. On order to ensure the login after the update, all user passwords are converted to lowercase automatically during the update.

So if a user has had “MICROS” or “Micros” or “micros” (would not have made a difference since the application ignored the case until now!) as password before the update, it will be stored as “micros” after the update.

From now on the application will store the password as entered (and encrypted) in the application.

## Last Login:

Go to System > Users > select any user:



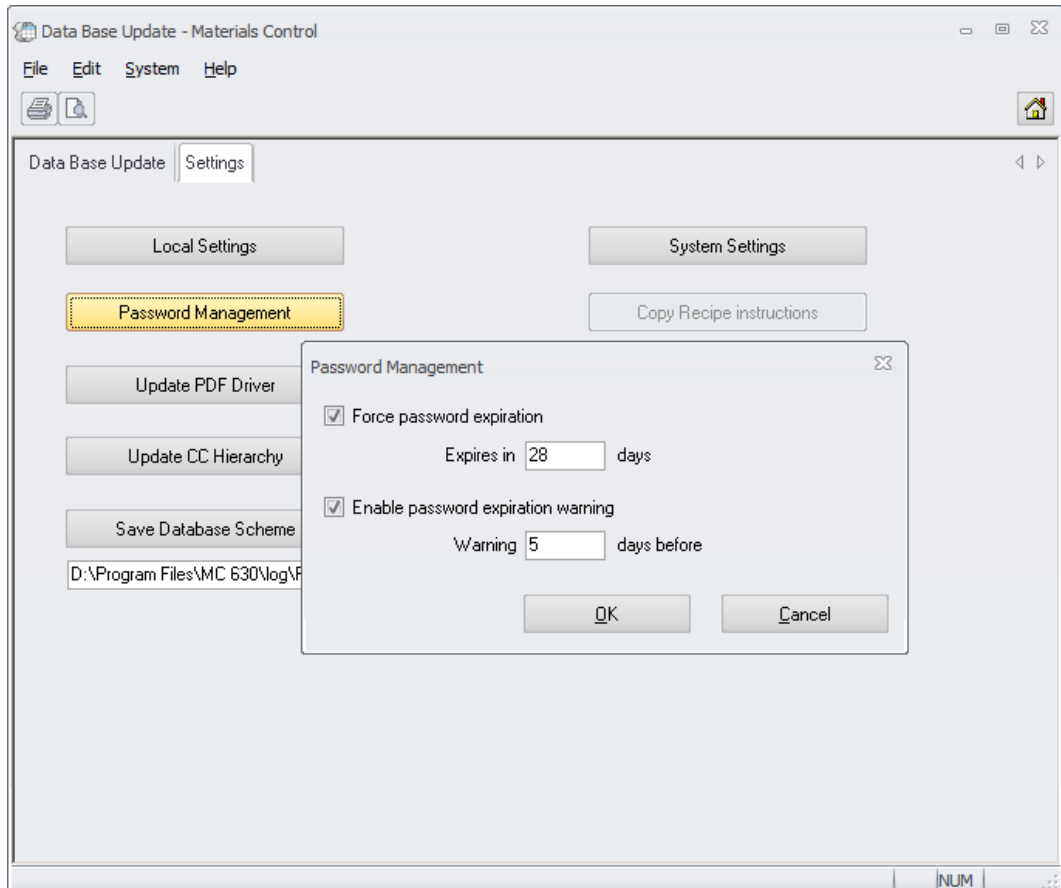
The screenshot shows the 'Manage Users' application window. The 'Login Name' is 'admin'. The user details include: User: SystemAdministrator, Password: [masked], Department: Systems Management, Phone: +49 2131 1370, Fax: +49 2131 137702, E-Mail: jtrommeschlaeger@micros.com, Language: English, and Information: System Administrator. The 'Last Login Date/Time' field is highlighted with a red box and contains the value '18.05.2011 17:43:27'.

Here the last login Date & Time stamp is shown.

## Enable Password Management:

This option will force the users to change their passwords after a defined time frame.

Go to System > Database Update > Settings > click on "Password Management":

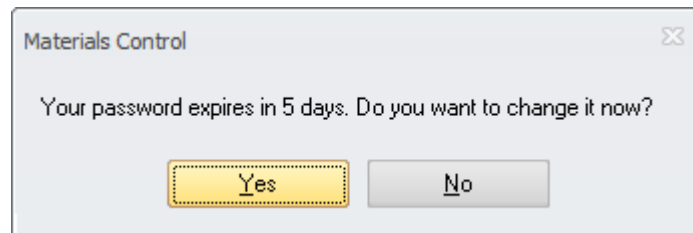


Here it can be defined ...

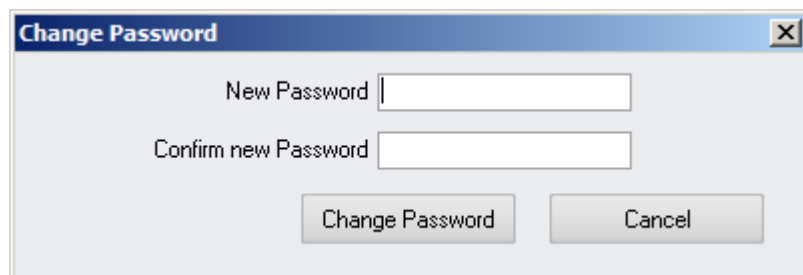
... after how many days the passwords will expire

... how many days before the warning will be displayed

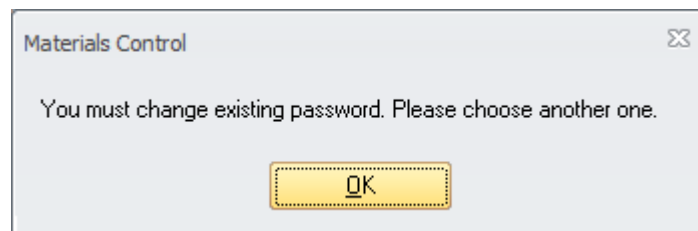
- Force Password Expiry
  - Expires in xx days
    - Here the user can define the number of days before the password expires.
- Enable Password Expiry Warning
  - Warning xx days before
    - Here the user can define how many days in advance a warning message will come up at login:



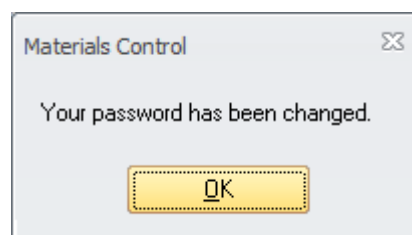
If the user clicks on “Yes” he can change the password directly:



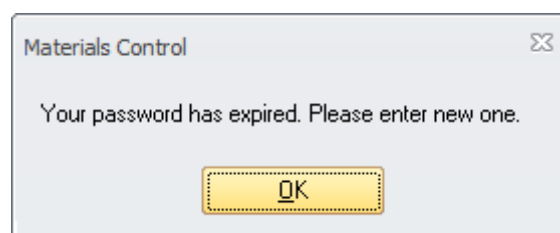
Here the user can now enter the new password. It is not allowed to use the same password again. If the user tries to do so, the system gives a message:



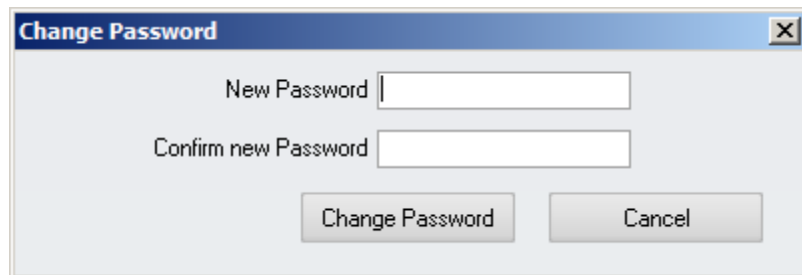
If the new password was entered and once more confirmed, the system will show this message:



In case the warning period is already elapsed the following message is shown:



Click on “OK” to change the password:



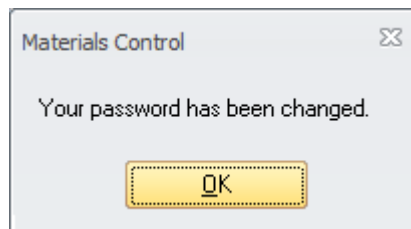
A dialog box titled "Change Password" with a close button (X) in the top right corner. It contains two text input fields: "New Password" and "Confirm new Password". Below the fields are two buttons: "Change Password" and "Cancel".

Here the user can now enter the new password. It is not allowed to use the same password again. If the user tries to do so the system gives a message:



A dialog box titled "Materials Control" with a close button (X) in the top right corner. The text inside reads: "You must change existing password. Please choose another one." Below the text is a yellow button with a dotted border and the text "OK".

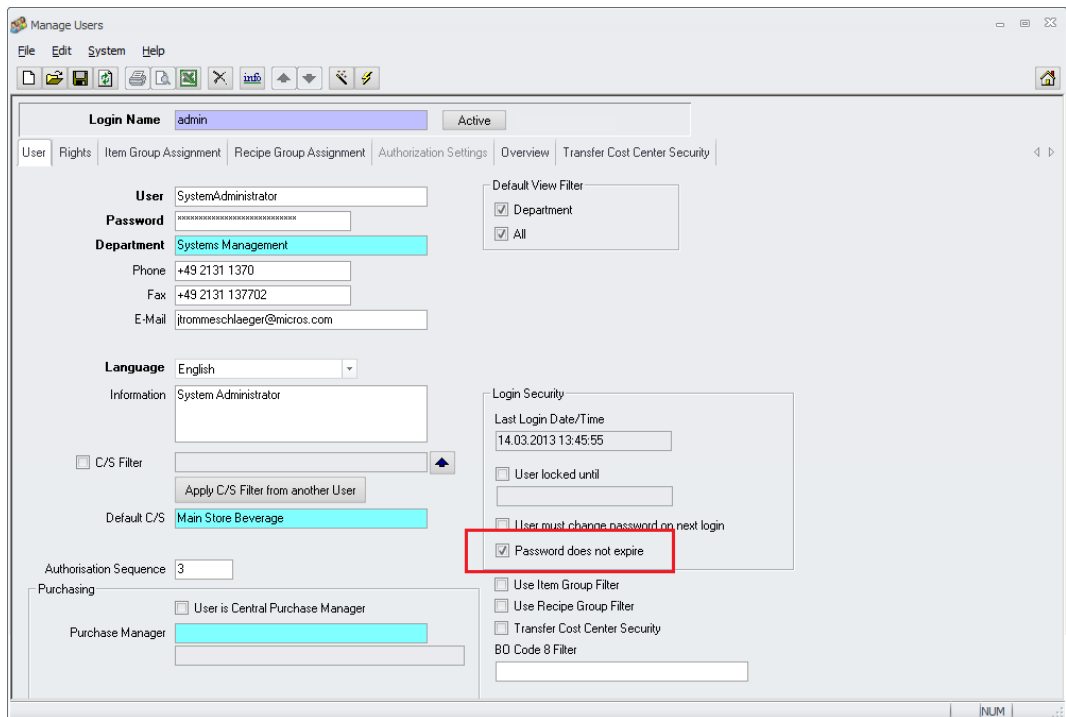
If the new password was entered and once more confirmed, the system will show this message:



A dialog box titled "Materials Control" with a close button (X) in the top right corner. The text inside reads: "Your password has been changed." Below the text is a yellow button with a dotted border and the text "OK".



In version 8.7.30 and higher selected users could be excluded from the password expiry.



Similar to the Microsoft Windows User Control it now can be defined per user that the password for selected users never expires.

But using the function "User must change password on next Login" it is still possible to force the user to change the password at next Login.

## Force Password Change manually:

If password management is enabled the application also offers to force the password change manually.

The screenshot shows a settings window with the following elements:

- Language:** English
- Information:** System Administrator
- C/S Filter:** [ ]
- Apply C/S Filter from another User:** [ ]
- Default C/S:** Main Store Beverage
- Authorisation Sequence:** [ ]
- Login Security:**
  - Last Login Date/Time: 18.05.2011 17:43:27
  - User must change password on next login
  - Use Item Group Filter

If this option is activated the user will receive a message at next login:

The dialog box contains the following text:

Materials Control

You must change your password before continuing.

OK

Now the user clicks OK to continue

The dialog box contains the following elements:

Change Password

New Password [ ]

Confirm new Password [ ]

Change Password Cancel

Here the user can now enter his new password. It is not allowed to use the same password again. If the user tries to do so, the system gives a message:

The dialog box contains the following text:

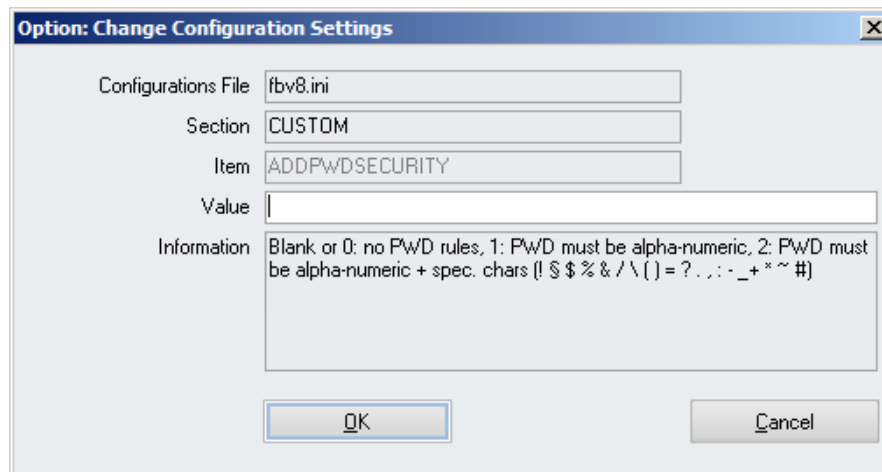
Materials Control

You must change existing password. Please choose another one.

OK

## Password Mask:

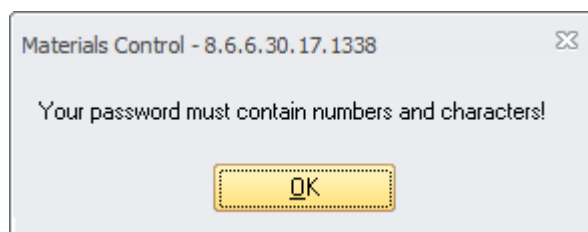
This parameter allows to define mask rules for the passwords:



### Allowed values:

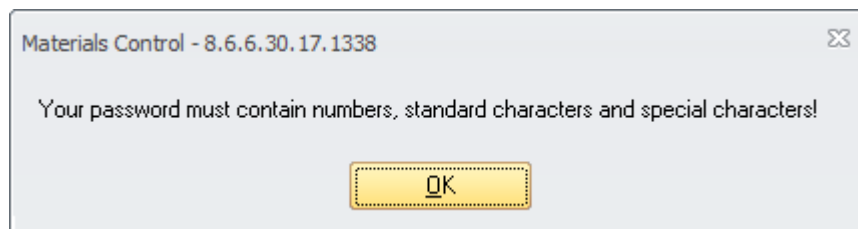
0 = No Rule. The password can be numeric only or alphabetic only, no requirement for special characters.

1 = The password must contain characters and numbers. If a password should be saved not fulfilling this rule, the following message is shown:



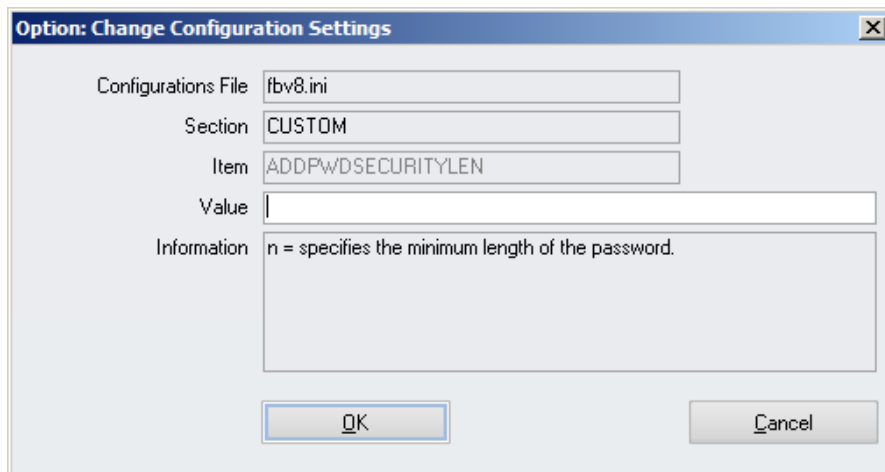
2 = The password must contain characters, numbers and special characters. These are the supported special characters: ! \$ % & / \ ( ) = ? . , : - \_ + \* ~ #

If a password should be saved not fulfilling this rule, the following message is shown:

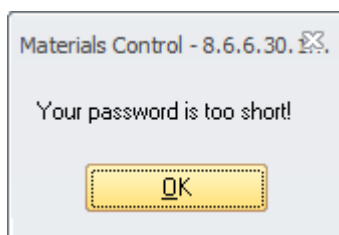


## Password Length:

Using this function the minimum length of the password can be defined:

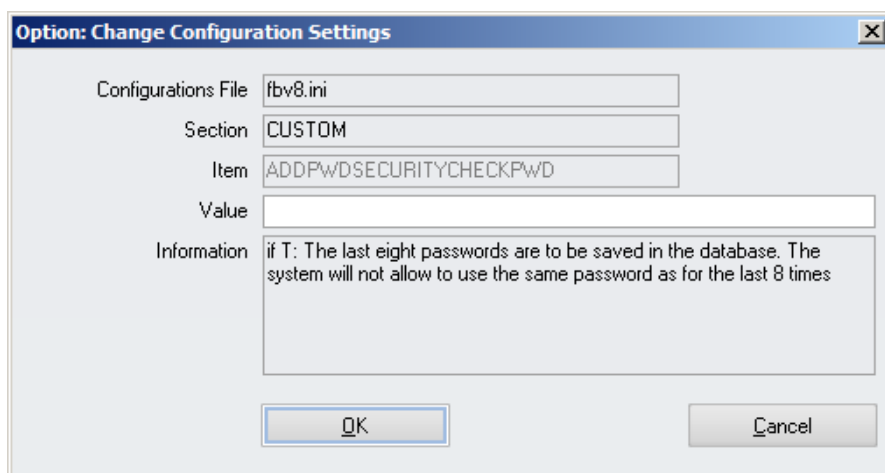


If the password is not long enough, the following message is shown:

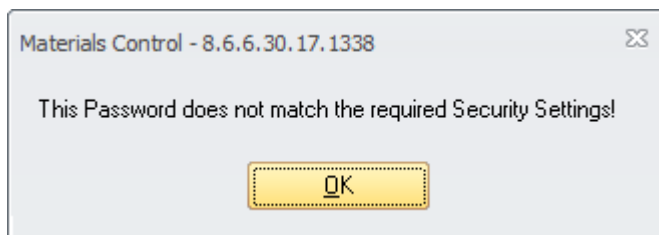


## Password Re-Use:

This parameter allows to forbid the re-use of passwords.

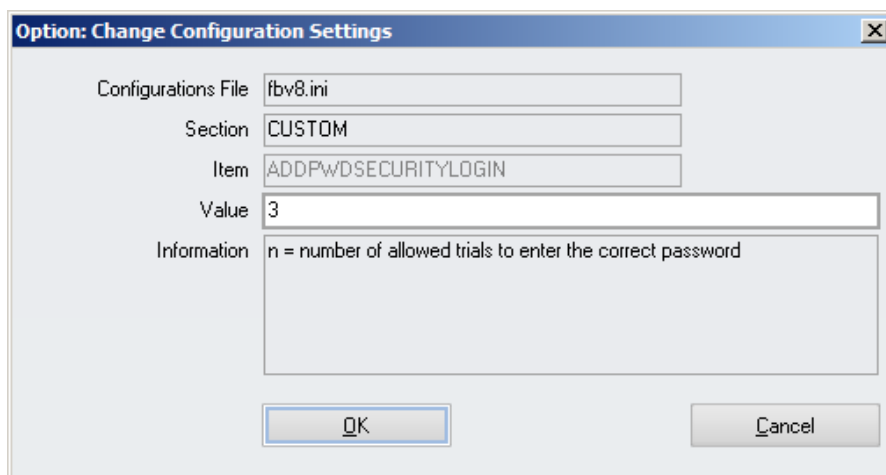


If set to T, the last eight passwords are saved in the database. The application will check these entries, if a user tries to change the password.

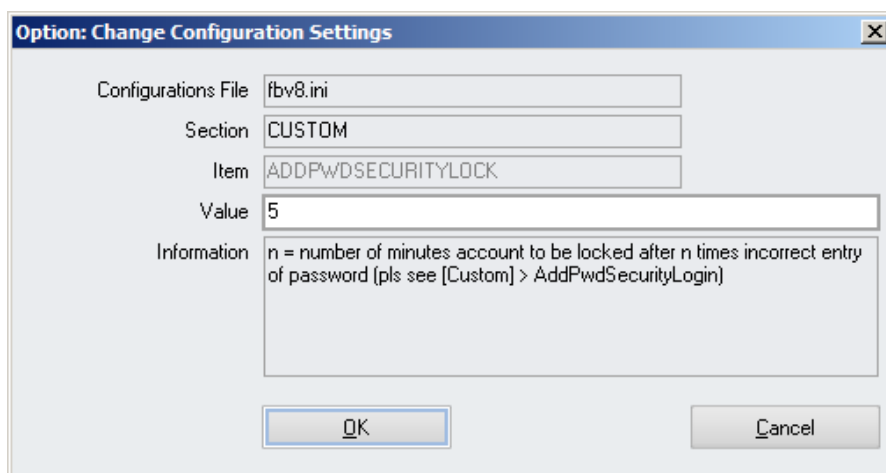


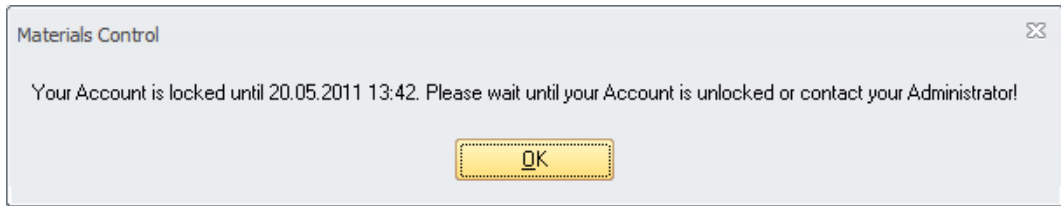
## Password Retries & Account Lock:

The following parameters can be used to define the number of allowed retries until the account will be locked for a defined time frame.



Here simply define the number of allowed re-tries. In case a user enters (here) 3 times the wrong password, the account will be locked for the number of minutes defined in the following parameter:

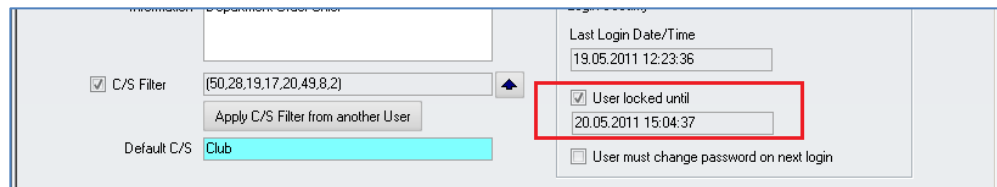




If no value is defined here, both parameters will not be considered.

After the account was locked by the system, the user now can...

- ... wait until the account will be opened by the system again (see message!)
- ... contact the system administrator, who can unlock the account in the user management

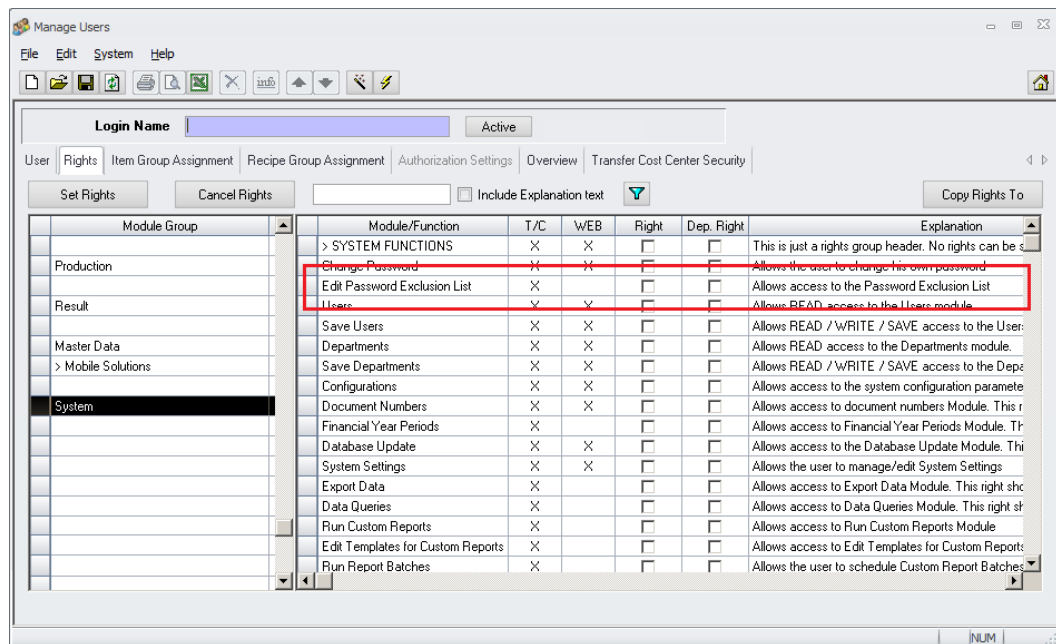


## Password Exclusion List:

Version 8.7.30.xx and higher:

A new function was added which allows the customer to specify forbidden passwords.

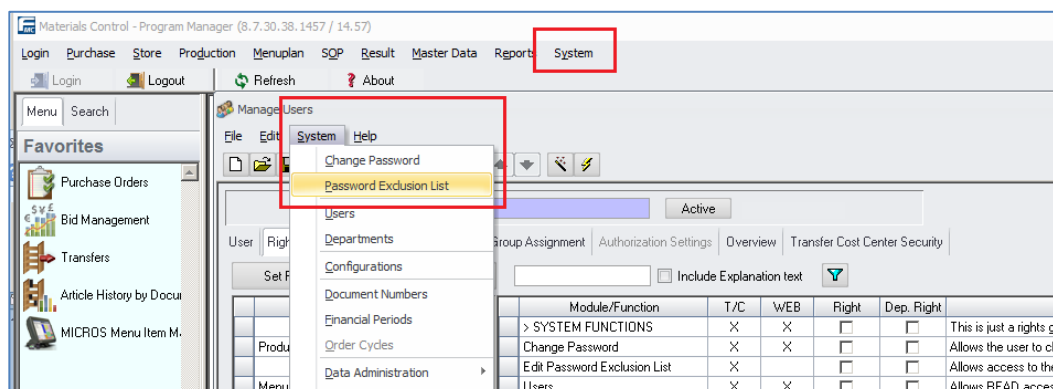
This list of passwords is secured by a user right. This can be found in the section "System", sub section "> SYSTEM FUNCTIONS" and is named "Edit Password Exclusion List":



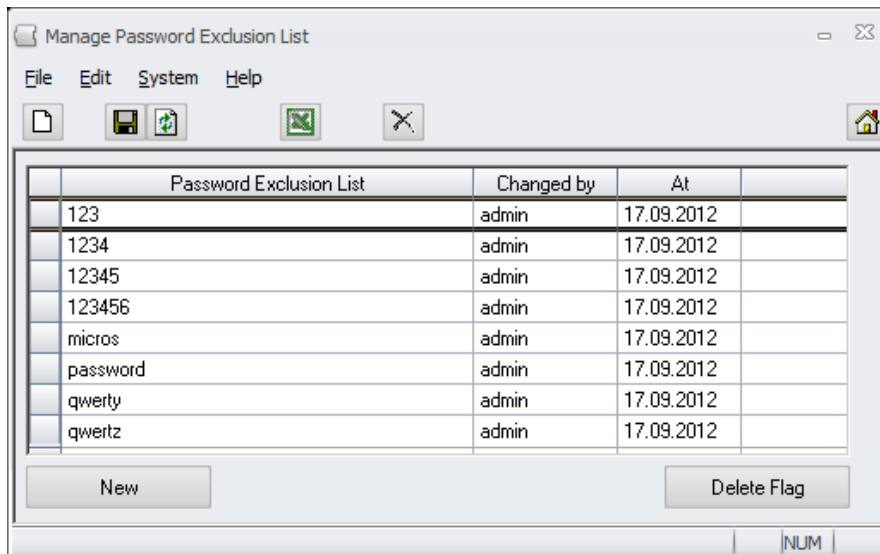
If set: The user can access and modify the list.

If not set: The user can not access the list.

The list itself can be accessed from any module in the System section of the menu "System":

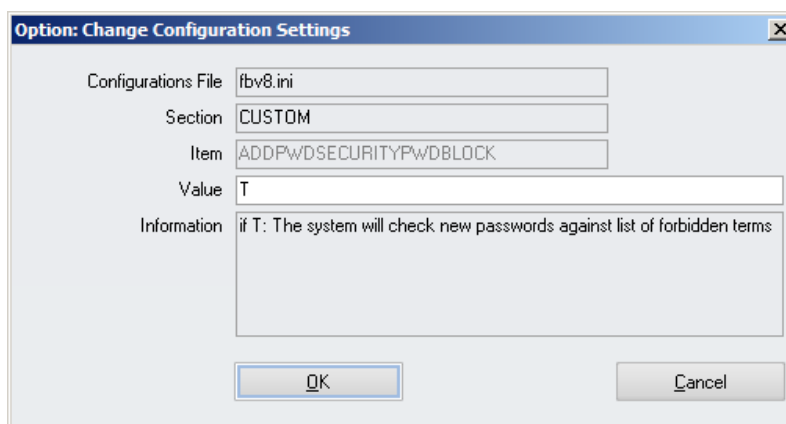


The list itself is a very simple tool.

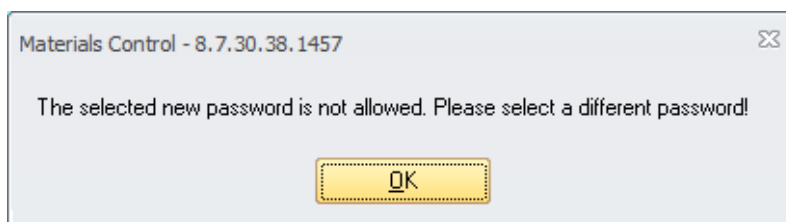


➤ Just use “New” button to add new terms or the “Delete Flag” to remove.

As next step the password check must be activated. Go to System > Configuration > CUSTOM and search for the parameter ADDPWDSECURITYPWDBLOCK:



Once this parameter is set to “T” the system will check every new entered password against the defined list:



The user now can confirm with OK, but has to define a different password.

**NOTE:** Existing passwords will not be checked. The application only checks new entered passwords!



## Forbidden Passwords:

Version 8.7.30.xx and higher:

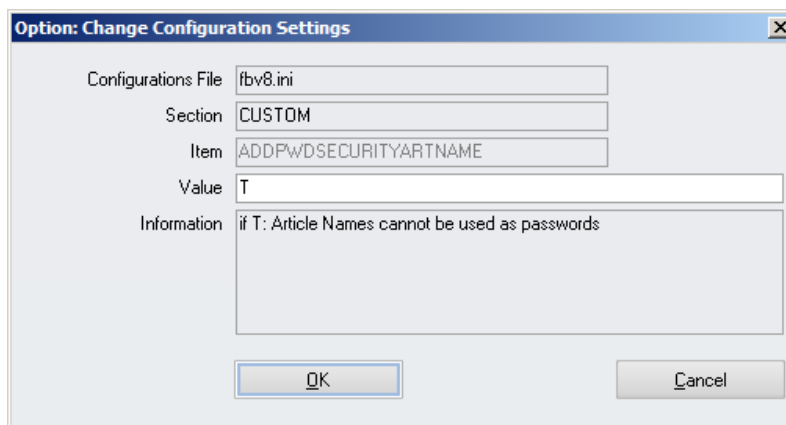
Besides the explicitly defined excluded terms also terms used in the application could be forbidden to be used as passwords.

It allows to block Article Names, Login Names, User Names, Supplier Names and Cost Center Names.

Go to System > Configuration > CUSTOM and search for the parameters shown below:

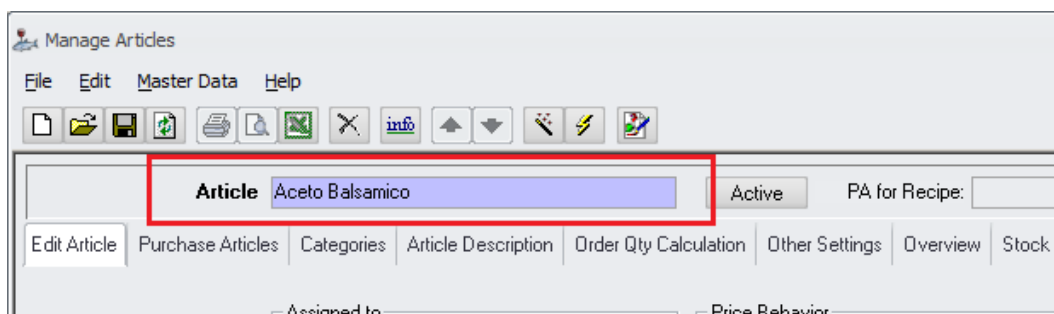
### Article Names:

In order to forbid the use of article names the parameter ADDPWDSECURITYARTNAME must be set to T:



Once activated, article names cannot be used as passwords anymore.

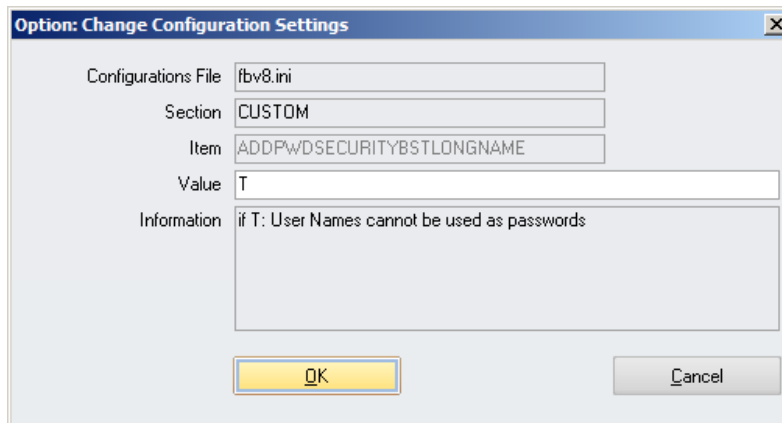
This function is not case-sensitive, means it does not check for small or capital characters.



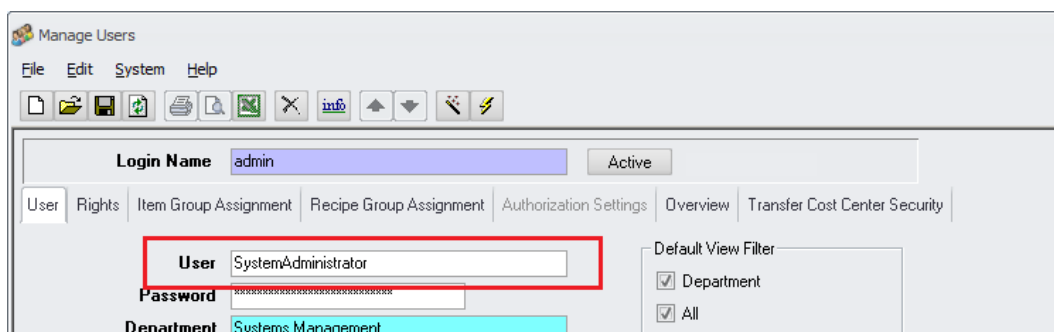
Using the example above "Aceto Balsamico" will not be allowed as well as e.g. "aCeto bAlsamico"

User Names:

In order to forbid the use of user names the parameter ADDPWDSECURITYBSTLONGNAME must be set to T:



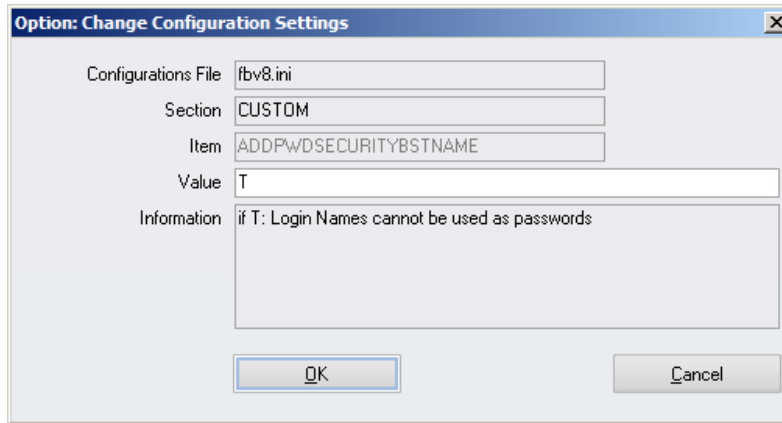
Once activated, user names cannot be used as passwords anymore. This function is not case-sensitive, means it does not check for small or capital characters.



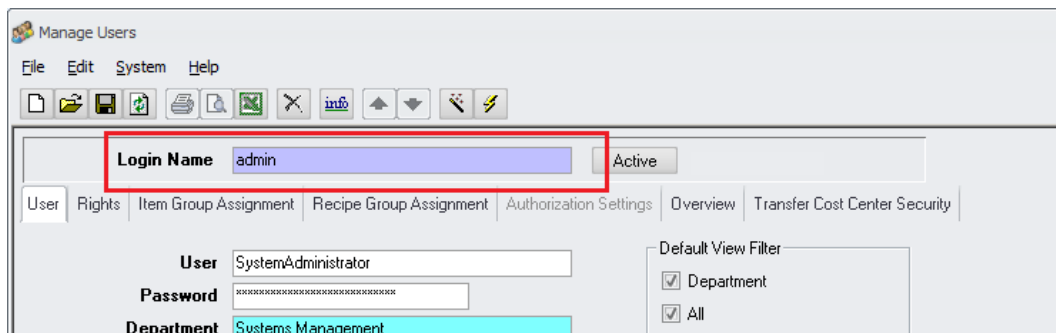
Using the example above “SystemAdministrator” will not be allowed as well as e.g. “sYsTemaDminIstRator”

Login Names:

In order to forbid the use of login names the parameter ADDPWDSECURITYBSTNAME must be set to T:



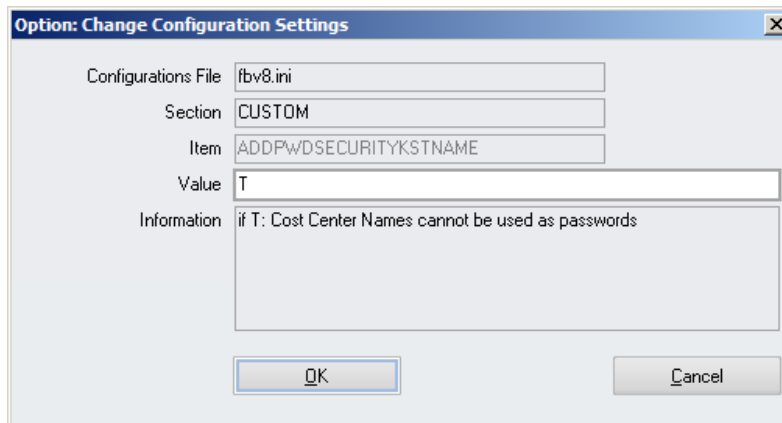
Once activated, login names cannot be used as passwords anymore. This function is not case-sensitive, means it does not check for small or capital characters.



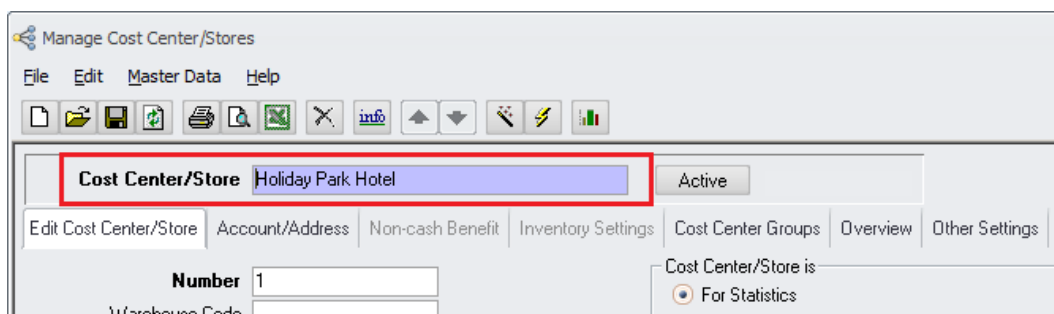
Using the example above “admin” will not be allowed as well as e.g. “AdMiN”

Cost Center Names:

In order to forbid the use of cost center names the parameter ADDPWDSECURITYKSTNAME must be set to T:



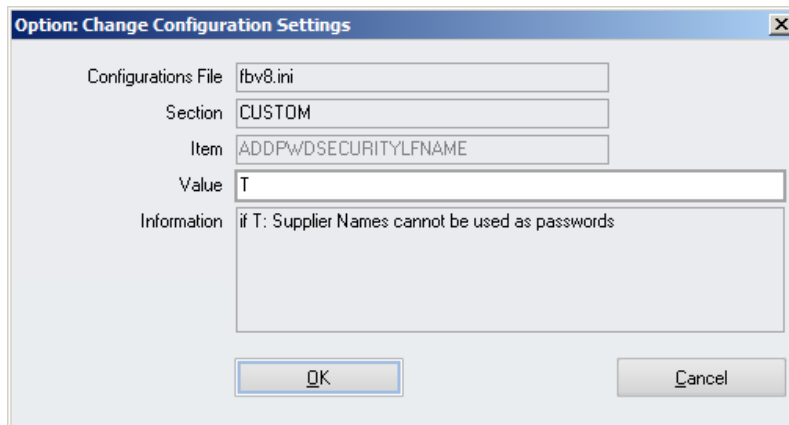
Once activated, cost center names cannot be used as passwords anymore. This function is not case-sensitive, means it does not check for small or capital characters.



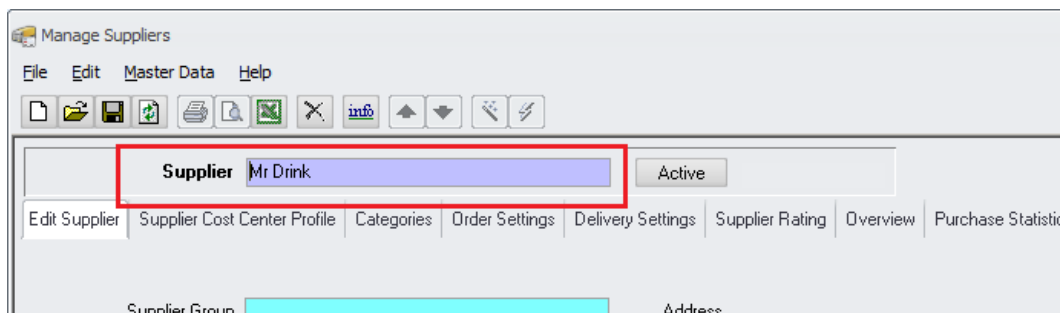
Using the example above “Holiday Park Hotel” will not be allowed as well as e.g. “hOliDay pArK HOtEl”

Supplier Names:

In order to forbid the use of supplier names the parameter ADDPWDSECURITYARTNAME must be set to T:



Once activated supplier names cannot be used as passwords anymore. This function is not case-sensitive, means it does not check for small or capital characters.



Using the example above “Mr Drink” will not be allowed as well as e.g. “mR dRiNk”

The configurations explained above will be considered every time a password is renewed or entered the first time.

Existing passwords are not affected unless they need to be changed.

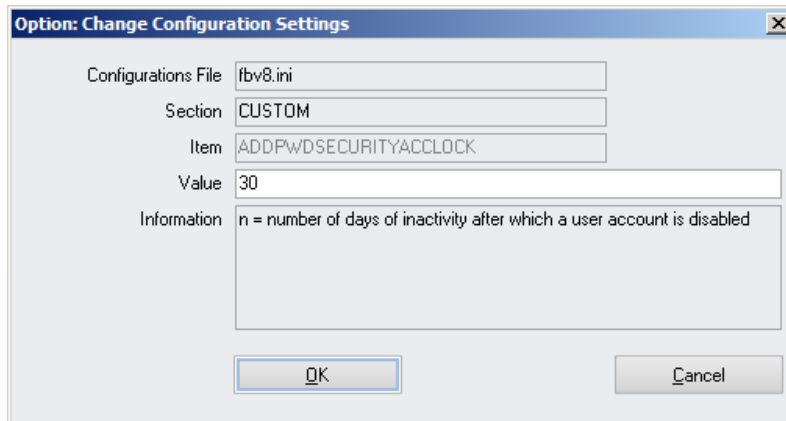
If then a not allowed password is entered the application will show the message below:



## Automated Account Locking:

A new function was added to enhance the security package. Pretty often, if an employee quits his job in the hotel, the user account remains active. This is a security risk. To avoid such forgotten active accounts a function was implemented to disable unused accounts.

Go to System > Configuration > [CUSTOM]:

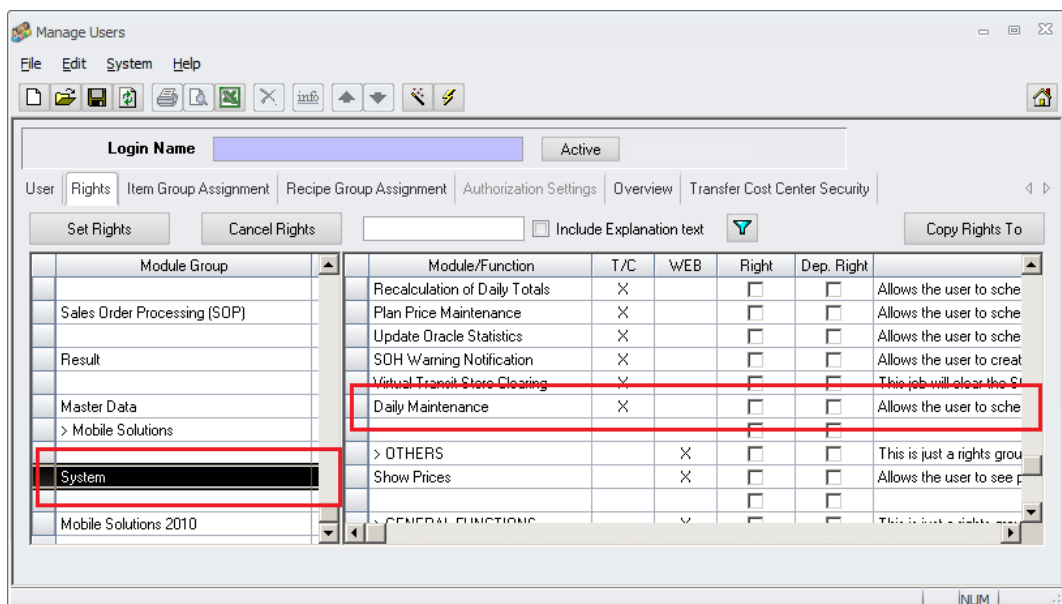


Here the number of days of inactivity must be defined. If a user did not login into Materials Control for e.g. 30 days this account would be considered in the new “Daily Maintenance” described in the separate chapter below.

## Scheduler > Daily Maintenance

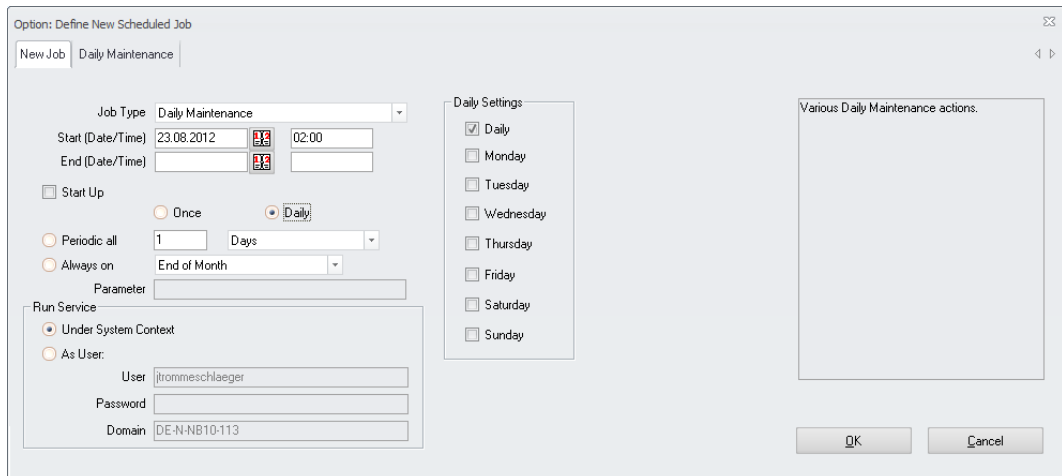
This function is used to summarize scheduled jobs which should be executed regularly at every Materials Control installation. The access to this function is secured by a new user right.

Go to System > Users > Rights:



This right will enable the access to the Daily Maintenance Job.

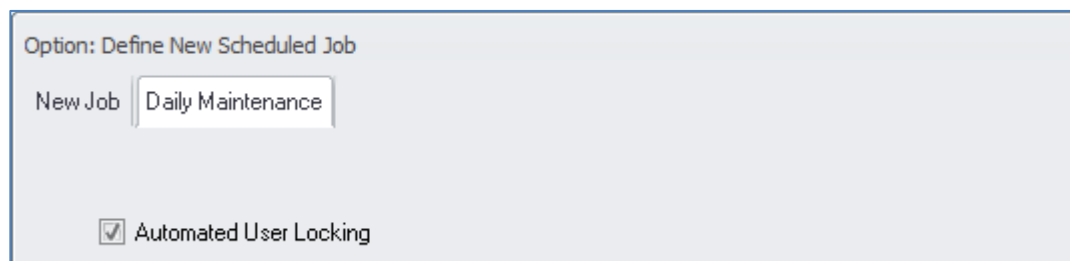
Go to System > Scheduler > click on “New Job”:



Here the new job “Daily Maintenance” can be selected now.

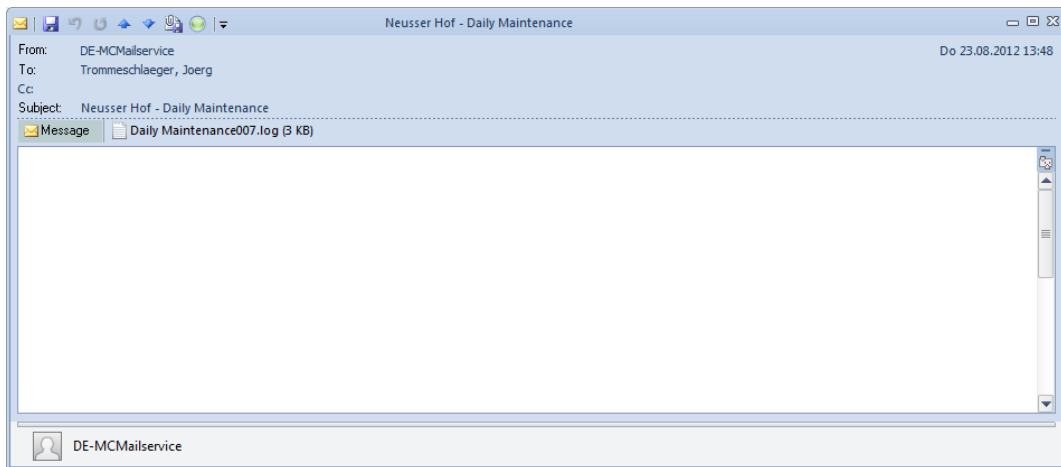
Define all scheduling parameters as needed. It is recommended to execute this job daily, during the night, after the POS Import.

Switch to the tab “Daily Maintenance”. Here the parameters for the single parts of this job are shown:

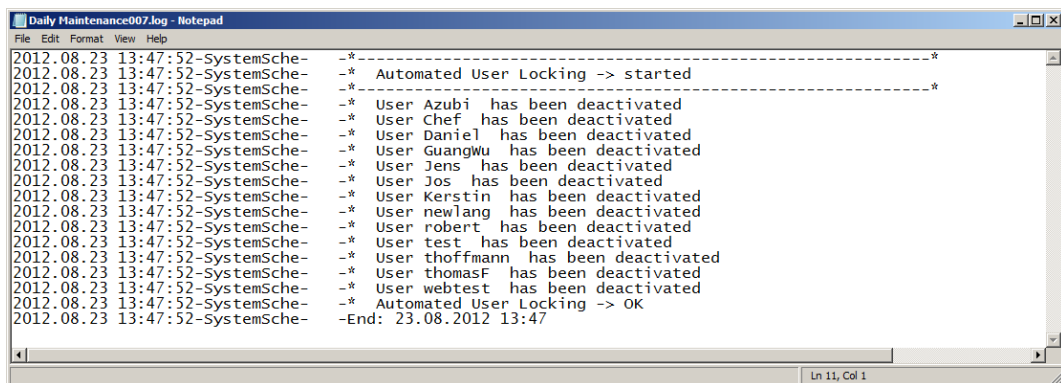


At this point of time just the job “Automated User Locking” is available in the Daily Maintenance. Mark the checkbox and save the job as usual.

After execution of the Daily Maintenance the application will try to send an email with the results.

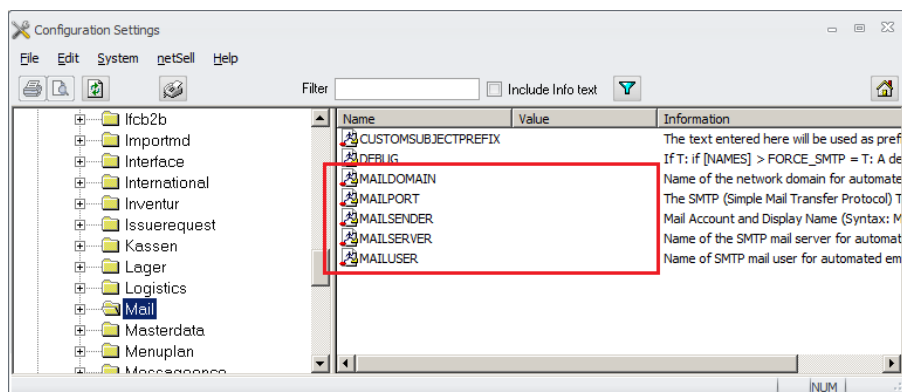


The attachment shows in detail which user accounts were disabled.



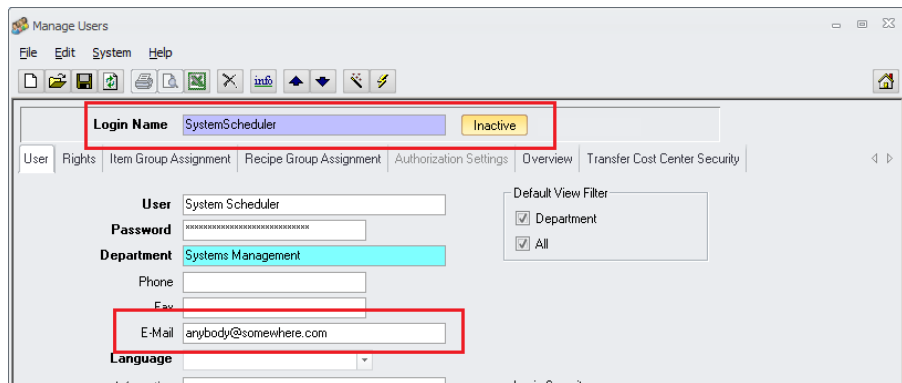
Pre-requisites:

- Email Configuration must be completed



- Scheduler User Definition



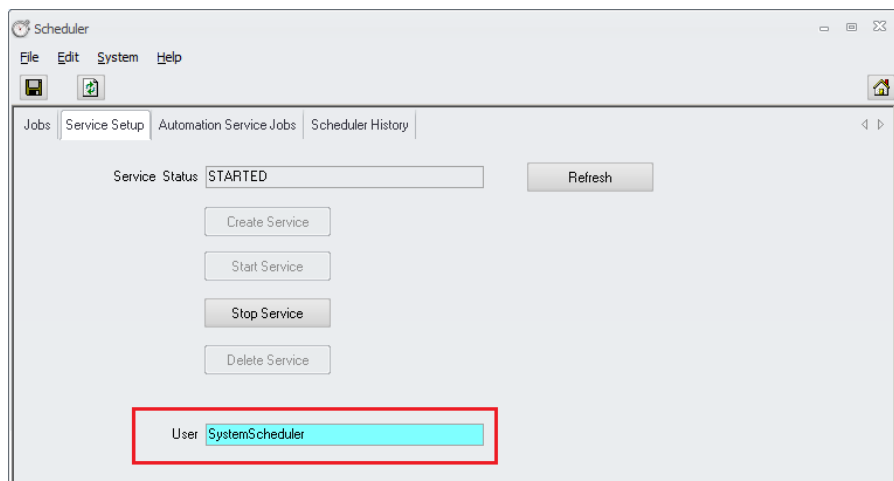


The defined scheduler user needs to be configured properly.

- Most important: the user should be inactive. This will make the use of this ID for any other purpose impossible.
- Email Address: Define the recipients email address. The scheduler will send the log of the Daily Maintenance to this address.

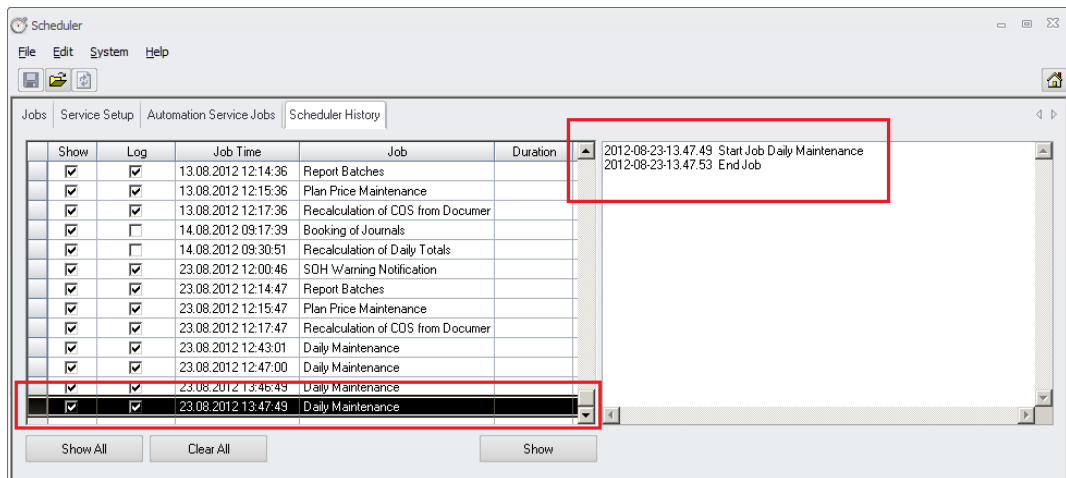
➤ Link "Scheduler User ":

In the module Scheduler switch to the tab "Service Setup":

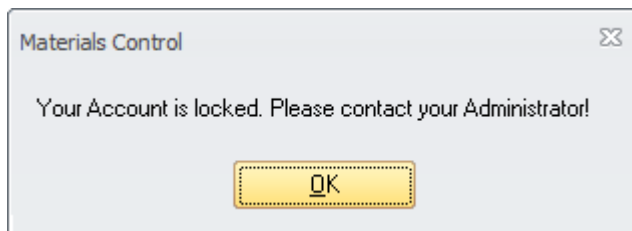


Here the Scheduler User must be linked.

Once finished the job will also create an entry in the Scheduler Job History:



Deactivated users now will receive the following message:



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