# Oracle® Hospitality Materials Control

Deployment Guide
Release 8.31
**E81345-04**

May 2017

ORACLE

# Contents

# Preface

This document describes the installation procedure for this version.

## Audience

This document is for administrators and technicians who are responsible for maintaining an 8.31 Oracle Hospitality Materials Control deployment.

## Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

## Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at
http://docs.oracle.com/en/industries/hospitality/

## Revision History

| Date | Description of Change |
|---|---|
| December 2016 | • Initial publication |
| January 2017 | • Added instructions for running a pre-configured installation. |
| March 2017 | • Added instructions for RSA access rights, and the permission requirements for the Authenticated Users group.<br>• Added information regarding database initialization in Thick Client as a requirement for fresh installations.<br>• Added instructions for installing Materials Control Mobile Solutions on a Zebra MC40.<br>• Corrected instructions for importing protected key |

| Date | Description of Change |
| --- | --- |
| | containers using the Secure Config tool.<br>• Clarified instructions regarding the custom reports folder for pre-configured installations. |
| May 2017 | • Updated instructions for Materials Control Mobile Solutions.<br>• Updated instructions for the Symbol Managed Class Libraries when installing Mobile Solutions on Zebra MC40.<br>• Added instructions for changing the battery on the Zebra MC40 while avoiding resetting the device. |

# 1 Overview

The purpose of this document is to provide instructions for new installations and for upgrading an existing Materials Control environment to version 8.31. It is assumed that the environment offers all necessary prerequisites of prior versions.

## Before Starting

See the *Oracle Hospitality Materials Control 8.31 Release Notes* for information about new or changed features and updates to system requirements and compatibility.

With this version Encrypted Configuration will be introduced.

## Files Included

The 8.31 release of Materials Control includes the following files:

- 161109_HMC_MaterialsContrrol_8.31.1.1555
- 161020_HMC_MCweb_8.31.4.1555
- 161020_HMC_MobileWebService_8.31.2.1555.zip
- 161104_HMC_MSClient_8.31.2.1555.zip
- 161024_HMC_MobileAuthWebService_8.31.3.1555.zip
- 161020_HMC_NutrientImport_8.31.2.1555.zip
- 161120_HMC_POSWebService 8.31.1.1555.zip
- 161104_HMC_MobileSolutionSetup_8.31.1.zip
- 161027_HMC_SecureConfig_8.31.1.1555.zip

## Prerequisites

- Microsoft .NET Framework (Full, not Client Profile) must be installed on PC.
- Oracle Database Client 32-bit must be installed.

# 2 Install Process

Logically, the Materials Control installation / upgrade can be broken into two sections:

- Thick Client application
- Web (IIS Based) applications

1. Thick Client Application

   This section will cover the installation of the first client PC, creation of the Key Container and preparation of the Install set for the remaining Thick Client PC installations. This will be done using a Setup executable.

   For this part the following is required:

   161109_HMC_MaterialsControl_8.31.1.1555

   Contains an installer (Setup.exe) that will be run to install a new or replace an existing Materials Control application.

2. IIS based applications

   The second section will cover all IIS based applications, such as MCweb, MobileWebService, POSWebService, MobileAuthWebService

   For this part the following files are required

   161020_HMC_MCweb_8.31.4.1555.zip
   Contains the builds that get copied to `C:\inetpub\wwwroot\<MCWebDir>` and to `C:\inetpub\wwwroot\aspnet_client`

   161020_HMC_MobileWebService_8.31.2.1555.zip
   Contains the build that gets copied to `C:\inetpub\wwwroot\<MobileWebServiceDir>`

   161020_HMC_POSWebService_8.31.1.1555.zip
   Contains the build that gets copied to `C:\inetpub\wwwroot\<POSWebServiceDir>`

   161024_HMC_MobileAuthWebService_8.31.3.1555.zip
   Contains the build that gets copied to `C:\inetpub\wwwroot\<MobileAuthDir>`

# Step by step instructions

This section will show how to install or upgrade a Materials Control system where all components are installed on one single Windows installation. These steps may differ if using more than one server, with different components on different servers.

It will also describe how to install or upgrade a Materials Control client installations.

Preparation:

Copy all necessary files to a temporary directory, from which the upgrade will be started.

## Thick Client

Extract the 161109_HMC_MaterialsControl_8.31.1.1555.zip file; it will create a folder named 161109_HMC_MaterialsControl_8.31.1.1555

There are three potential cases which are described separately below:

- New installation
- Update existing application
- Installation of an additional application

### Default Installation Files

When installing Materials Control usually some files are customized in advance and should be installed at each client. Such files are i.e. FMLOGIN.INI and SQL.INI. The handling of these files has not changed in general. The files should be copied to the folder \CUSTOM\ of the install set as usual.

### Encrypted configuration

Starting from release 8.31, database password and encryption-key defining parameters will be stored in Protected Configuration (https://msdn.microsoft.com/en-us/library/53tyfkaw%28v=vs.100%29.aspx). Storing sensitive information in a non-readable format improves the security of our applications by making it difficult for an attacker to gain access to the sensitive information, even if an attacker gains access to the file, database, or other storage location. Materials Control is using RSA machine-level key container, which enables us to use single one for all applications and simplifies the deployment on other PCs.

Make sure that user executing the installation as well as the Materials Control users have sufficient rights to access the RSA container. RSA Access Rights contains instructions.

During the installation of the first client installation, the Key Container will be generated. This will be used then in all following client installations.

Deployment of Materials Control applications must be done in following order:

- Install the Materials Control thick client application on one PC to create the master install setup. This will include the creation of the key container.
- Install the Materials Control thick client application on remaining PCs using the master install setup.
- Install IIS based applications (update can do, but with precautions explained below)
    - Use the “HMC_SecureConfig” tool to import the key container
    - Encrypt configurations
- Update database(s)

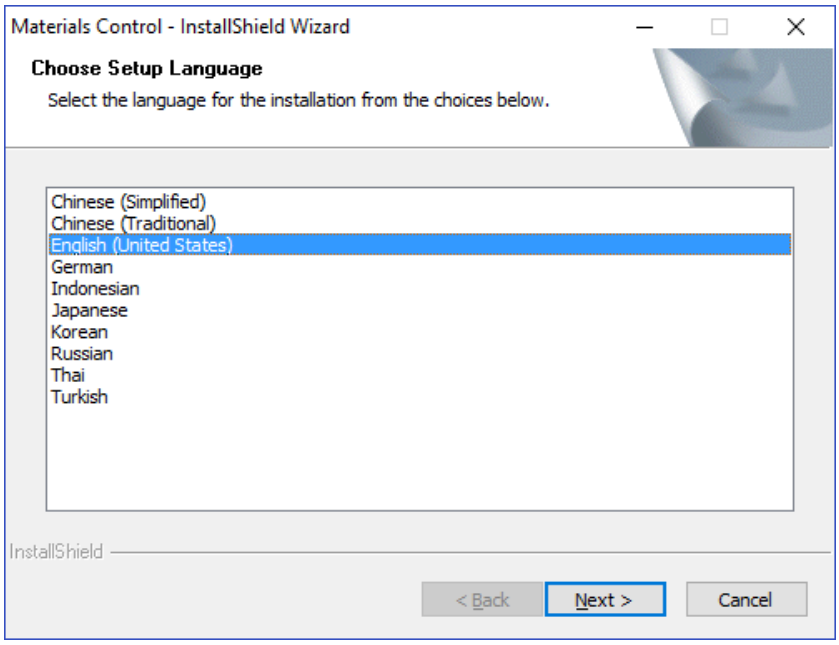
## Installation of 1st Client – Master Creation

### Installation of a new application

This section will describe the installation of the first client application in a new environment.

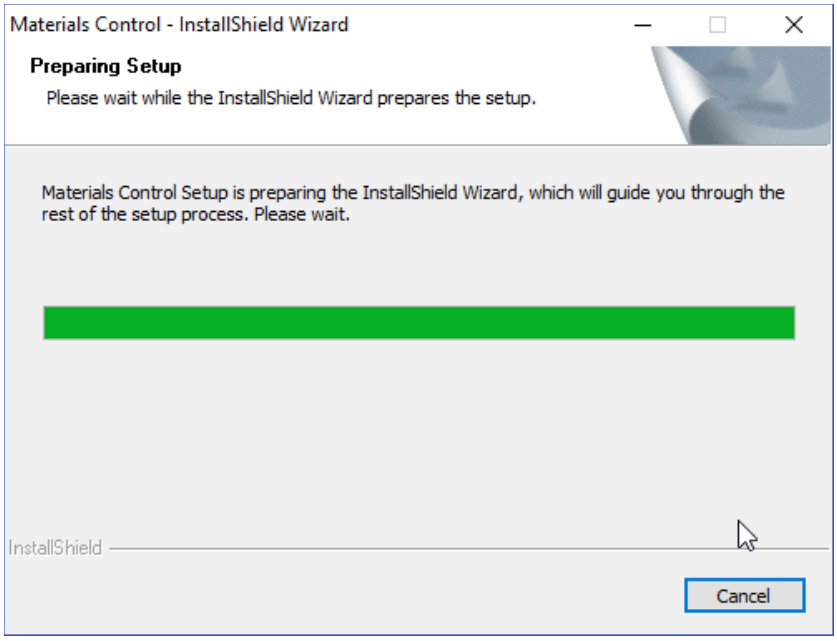
Start the installation by double click on SETUP.EXE in the installation file directory.

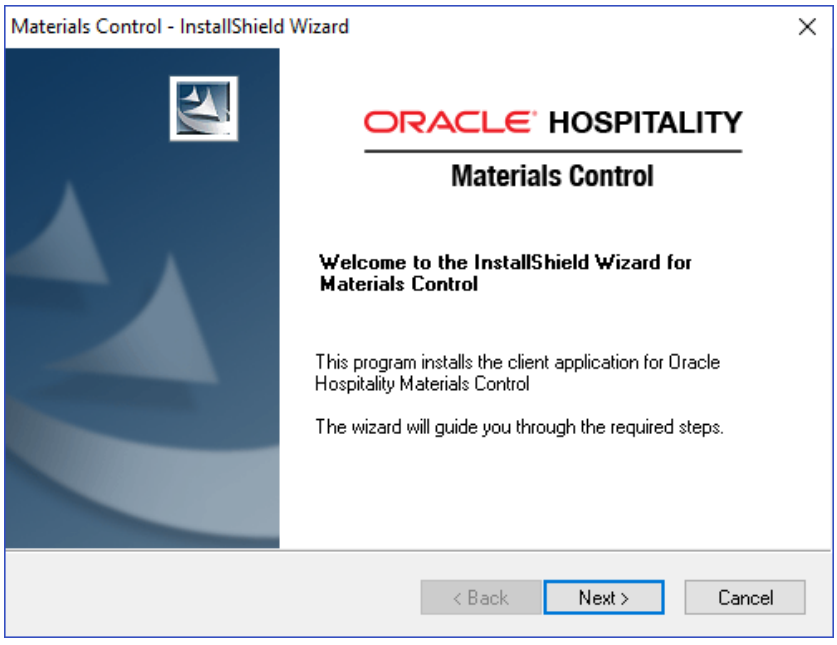
At first the procedure will ask for the Setup Language:



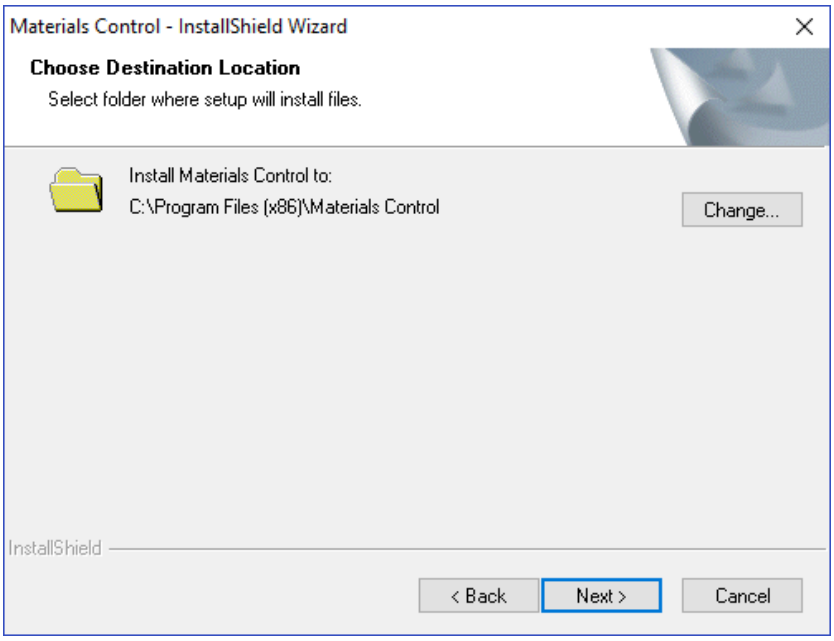

Select the language and click “Next”.

The setup process will now be prepared.



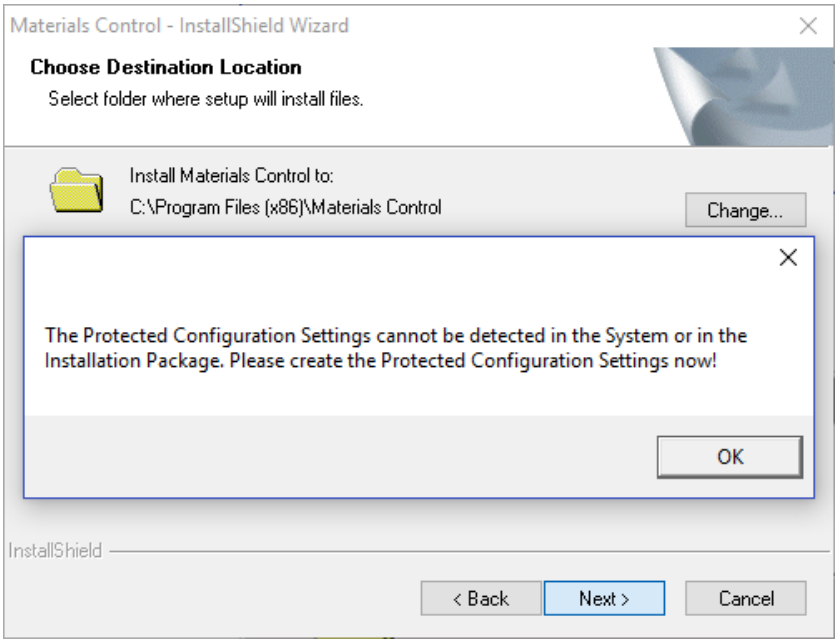




Click “Next" to start.



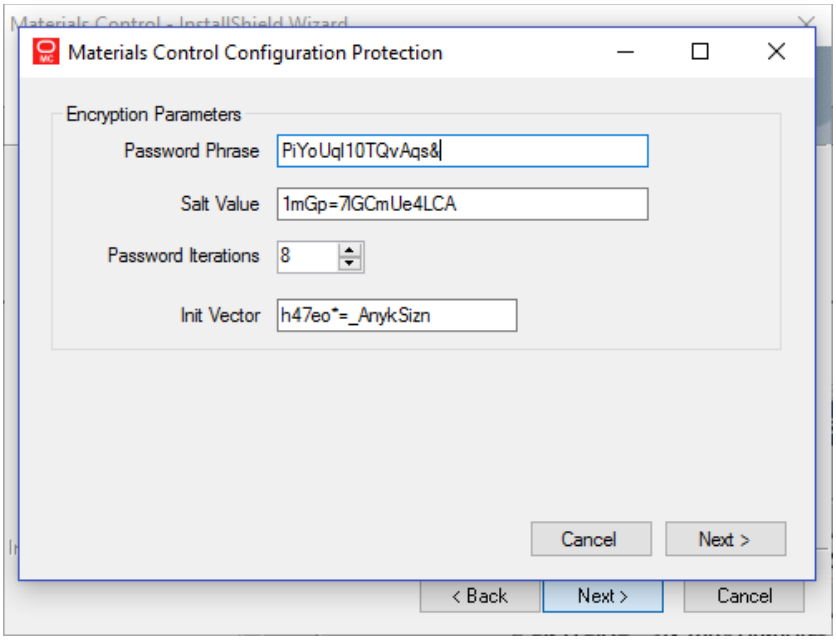

Accept or change the destination and click “Next”.

The installation routine will now check for the protected Configuration Settings.



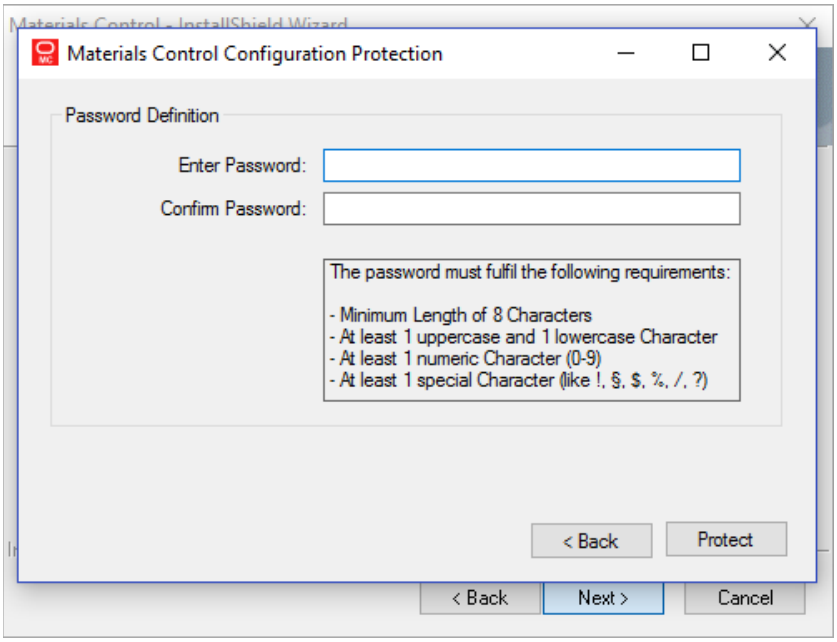

Since these could not be detected in this case, they must be created now.

Randomly generated Protection Settings will be offered.



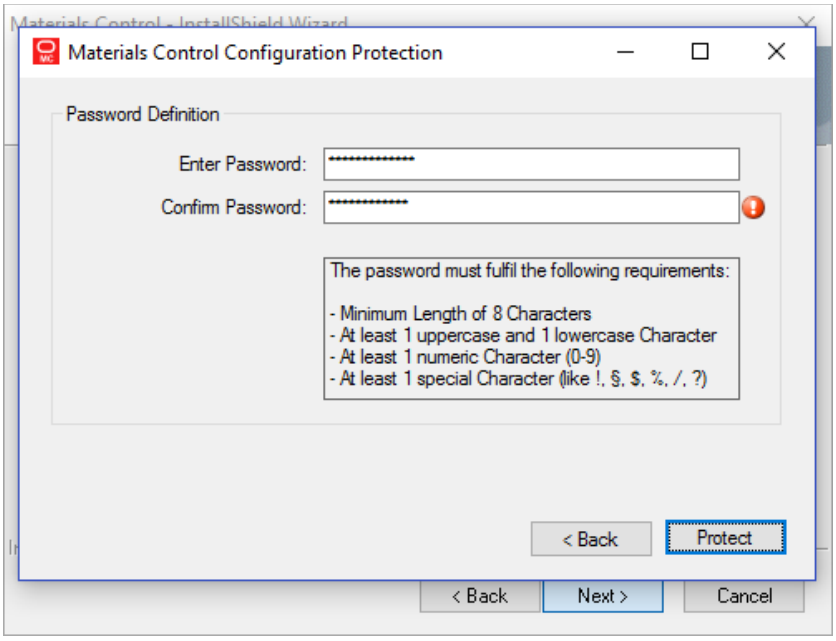

Accept or change the settings and click “Next” to proceed.

The settings must be protected with a password. This password must follow the displayed complexity rules.




Enter the password into both fields and click “Protect”.

The system will check if the confirmed password matches the entry in the upper field.

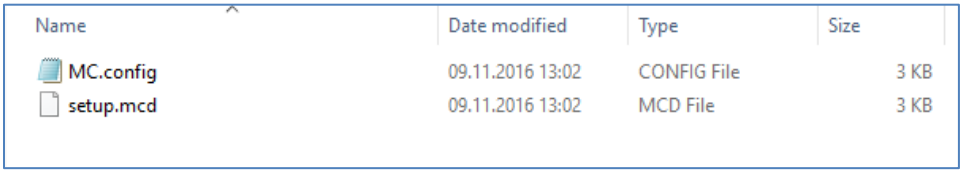



After the password was entered twice correctly the button “Protect” will create the configuration files.

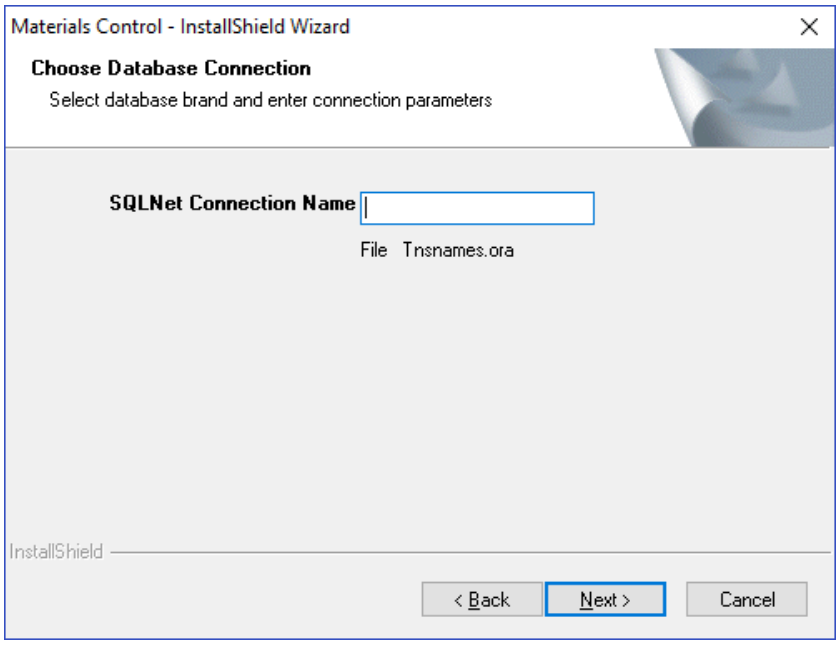
**IMPORTANT NOTE:**

- Store the entered password at a save location! There is no way to retrieve this password from any place in the database or the application!

- Store a copy of the generated configuration settings at a save place. There is no way to recreate these files from any place in the database or the application! The files can be found in the folder \CUSTOM\ in the install set directory

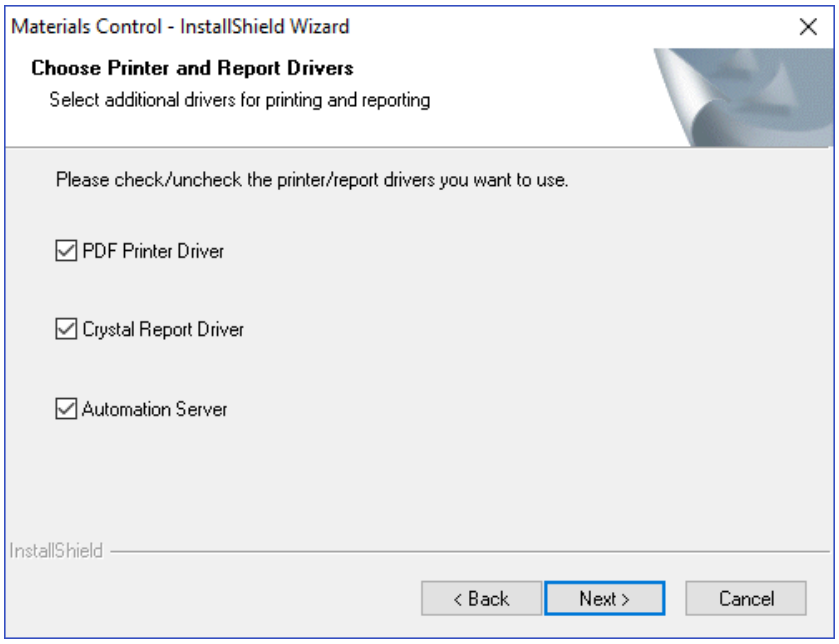


After successful creation of the protected configuration files, the installation process will check the Oracle database connection:




Enter the name of the Oracle instance and click “Next”.

Select the options to be installed with this client application:



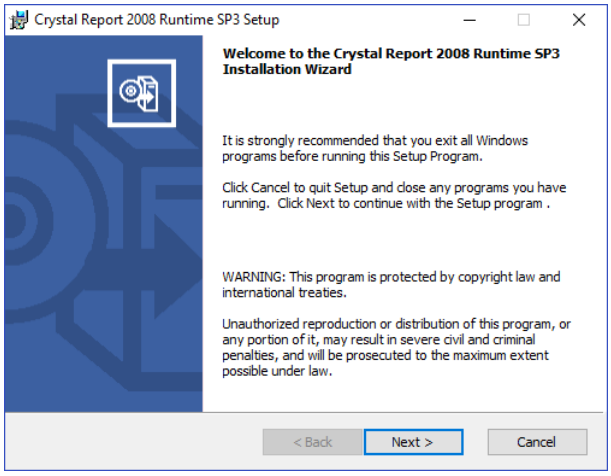

PDF Printer Driver

- This option will install a PDF Converter for documents printed out of the application. This should be selected always.

Crystal Report Driver

- This option will install the Crystal Reports Runtime files. These are required to use the module "Custom Reports" in Materials Control. This is required for most client installations.

  If selected the install process will force the runtime installation after the client application installation.

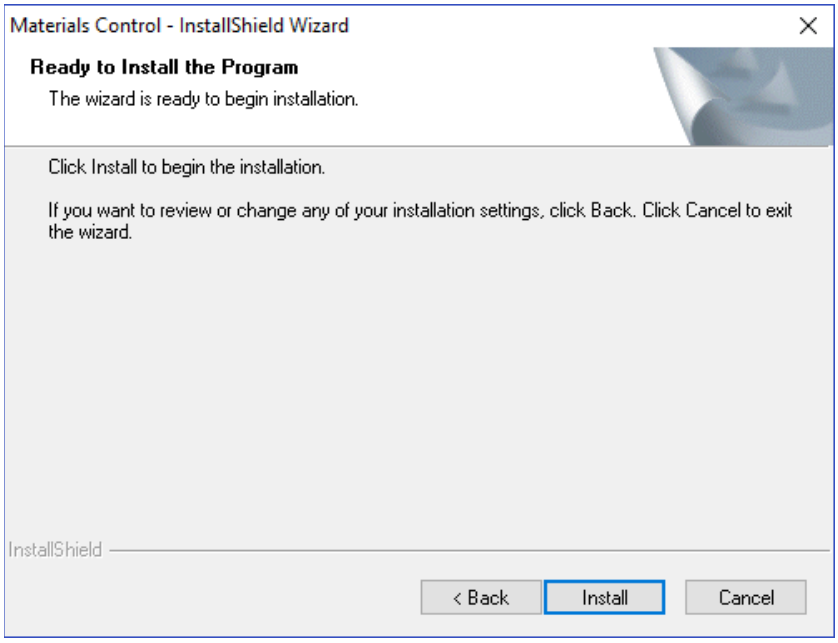


Automation Server

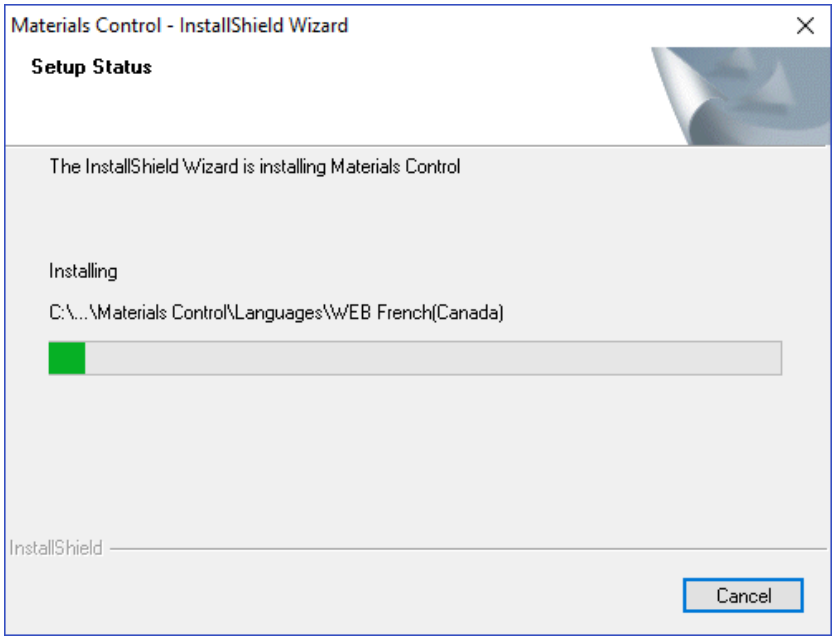
- This option will install a service-based scheduler for processing jobs defined in Materials Control.

After selecting the options click “Next” to proceed.

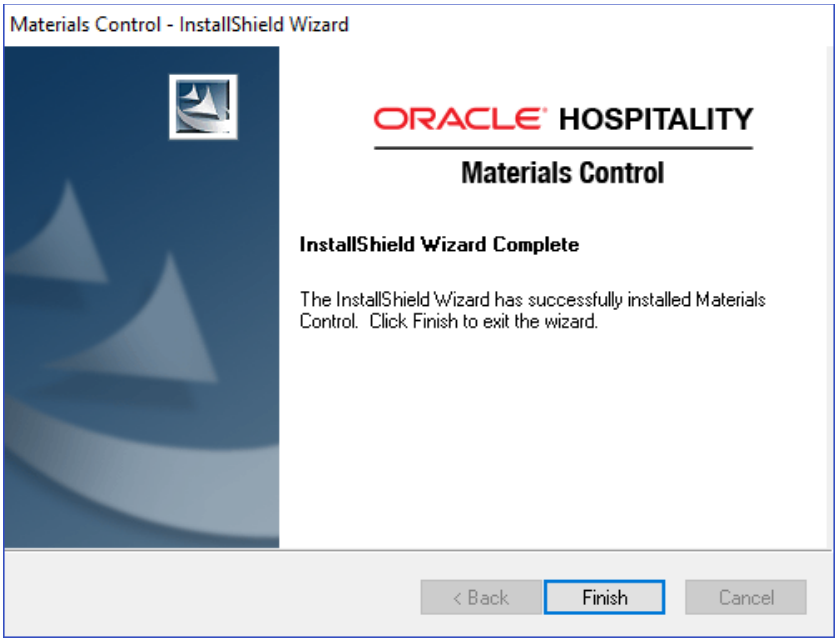
Since all required information is now available the main process can be started.




Click “Install” to proceed.



Once completed, the installation routine will show the following screen:



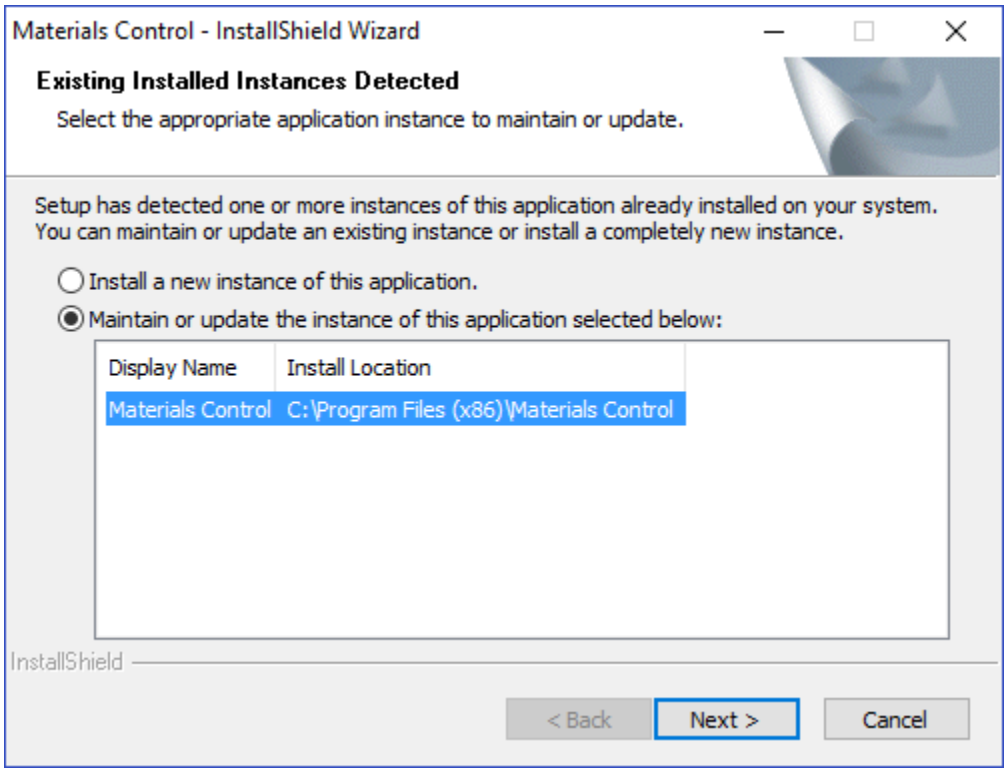

Click “Finish”.

### Update of an existing application

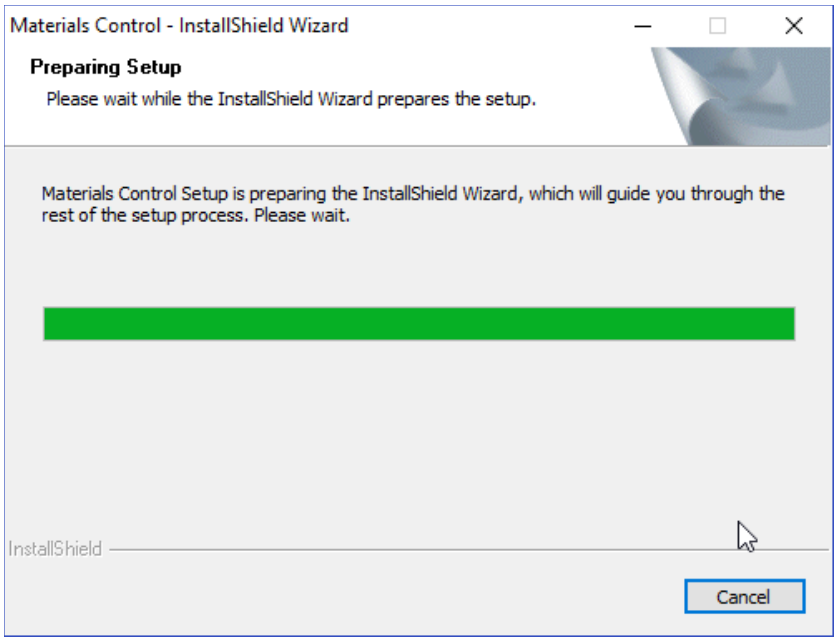
This section will describe the installation of the first client application in an existing environment running an older version of Materials Control. Environments running Materials Control version 8.7.10 and older must be upgraded to version 8.7.20 or higher, before the update to 8.31.*x* can be started.

Start the installation by double click on SETUP.EXE in the installation file directory.

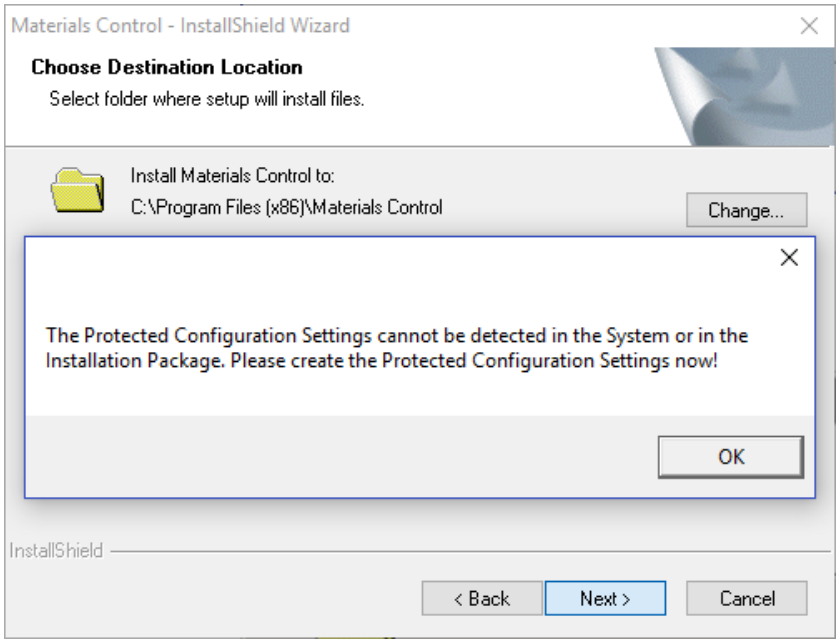
The installation routine will detect the existing installation of a Materials Control client application and will offer to update the existing application:




Select the installed application and click “Next”
The setup process will now be prepared.

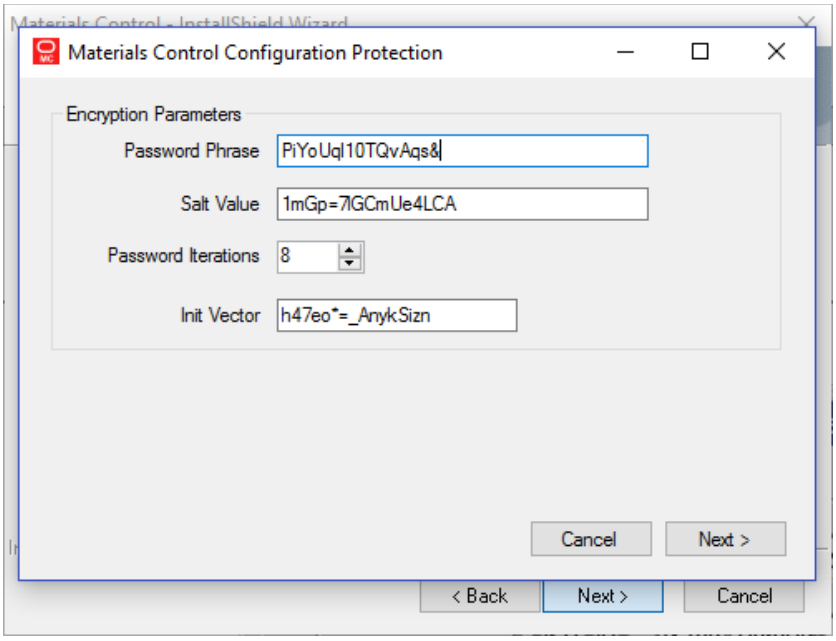



The installation routine will now check for the protected Configuration Settings.



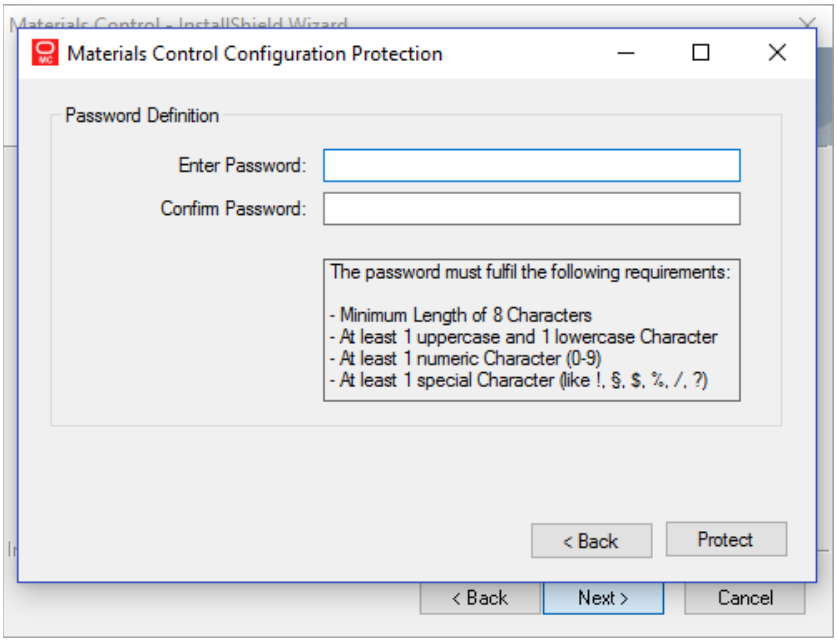

Since these could not be detected in this case, they must be created now.

Randomly generated Protection Settings will be offered.



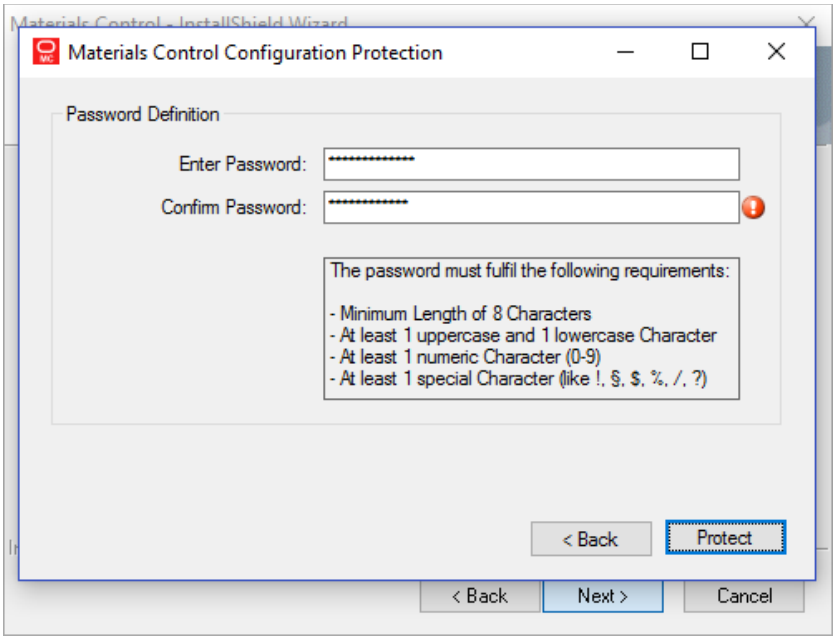

Accept or change the settings and click “Next” to proceed.

The settings must be protected with a password. This password must follow the displayed complexity rules.




Enter the password into both fields and click “Protect”.

The system will check if the confirmed password matches the entry in the upper field.

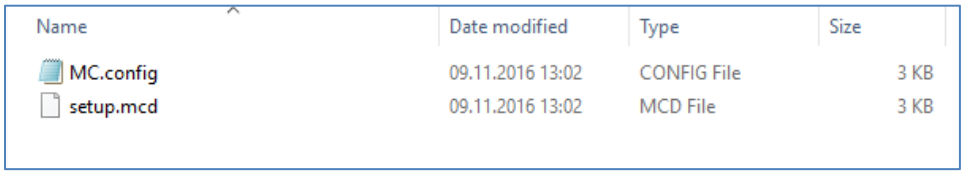



After the password was entered twice correctly the button “Protect” will create the configuration files.

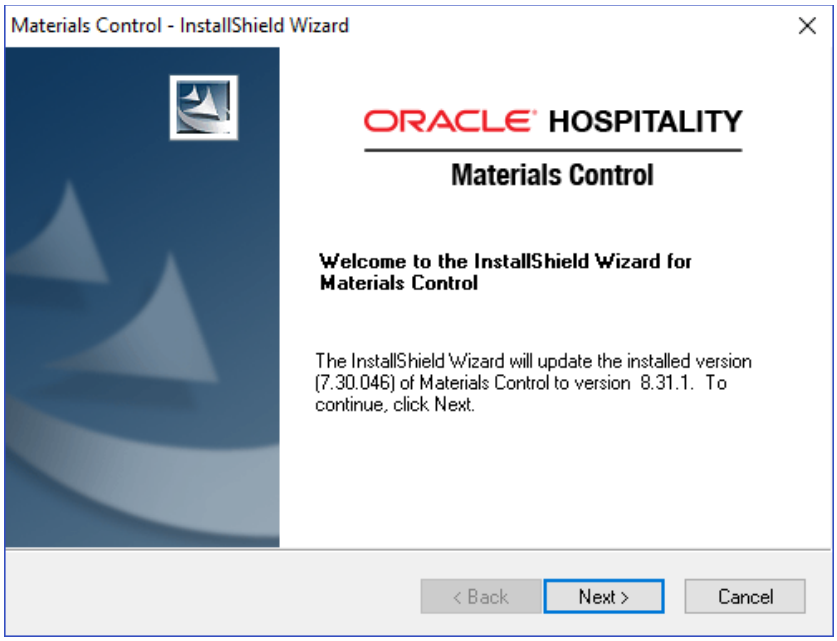
**IMPORTANT NOTE:**

- Store the entered password at a save location! There is no way to retrieve this password from any place in the database or the application!

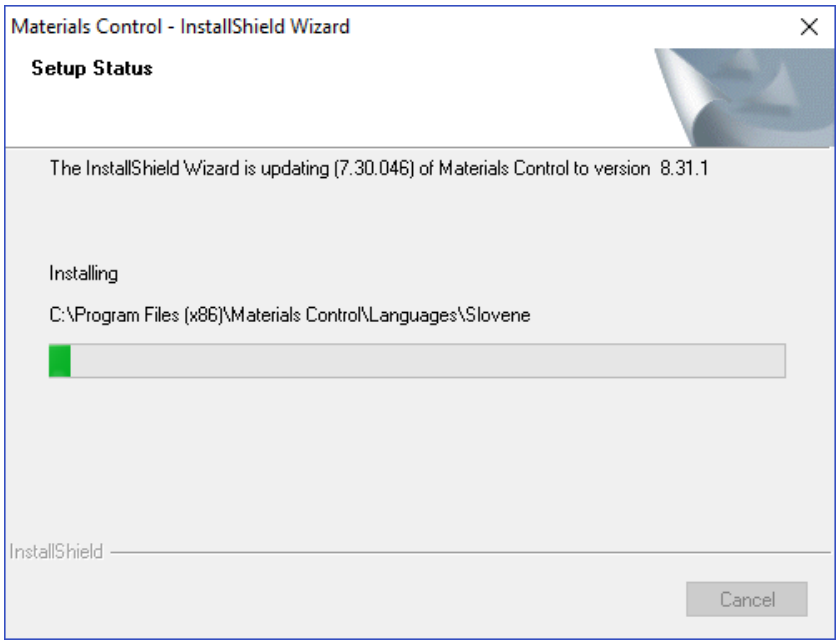
- Store a copy of the generated configuration settings at a save place. There is no way to recreate these files from any place in the database or the application! The files can be found in the folder \CUSTOM\ in the install set directory



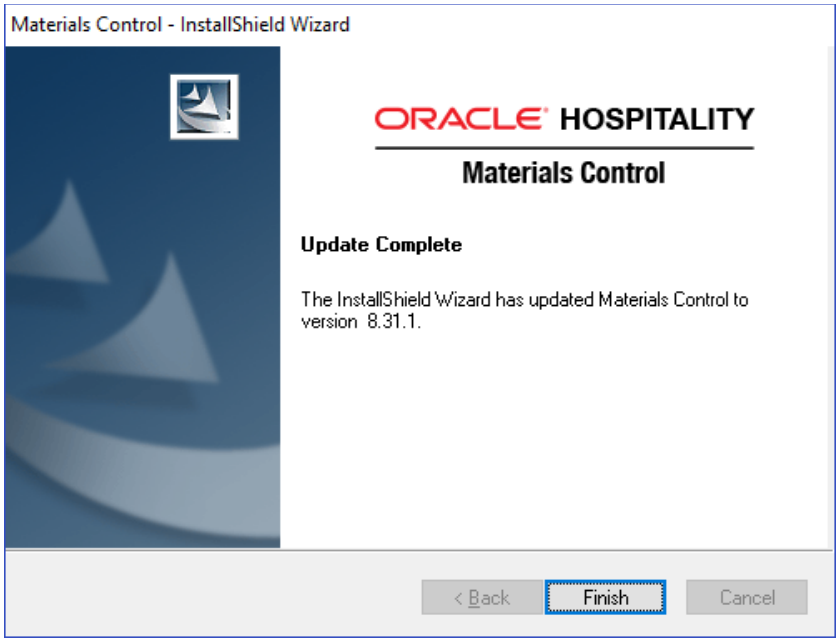
Since all required information is now available the main process can be started.




Click “Next” to proceed.



Once completed, the installation routine will show the following screen:




Click “Finish”

### Installation of an additional application

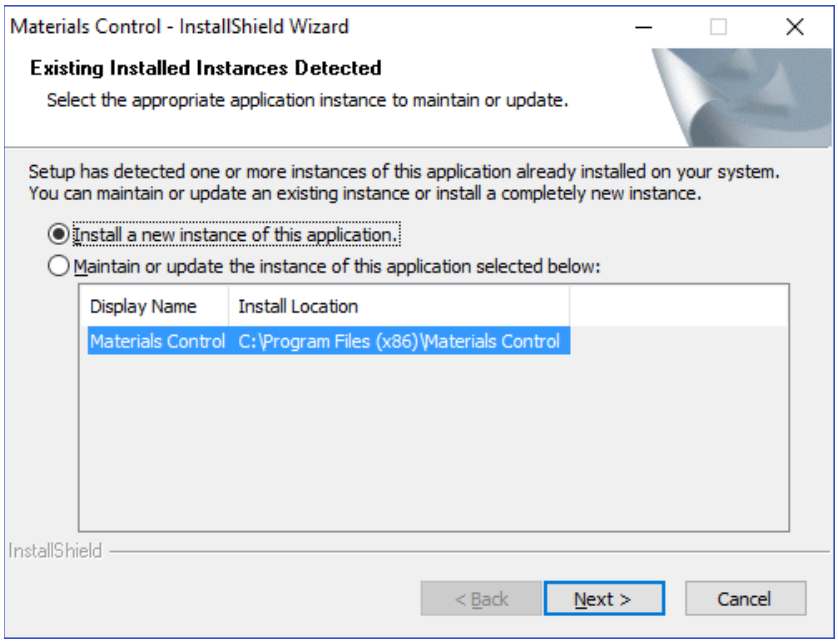
When maintaining a test lab it might be necessary to have different versions of Materials Control installed on one PC. This must not be the case in a production environment!

## Maintaining different client applications in different versions

This section will describe the installation of a new client application of Materials Control 8.31 in an environment having older releases of the application installed which should remain. This should be the case in test lab installations only.

Start the installation by double click on SETUP.EXE in the installation file directory.

The installation routine will detect the existing installation of a Materials Control client application and will offer to install an additional application:




Click "Next" to confirm. The installation procedure will now be exactly the same as when installing a new application, described in the chapter "Installation of 1st Client – Master Creation - Installation of a new application".

## Maintaining different client applications using protected configuration

This section will describe the installation of a new client application of Materials Control 8.31 in an environment having at least one application of Materials Control 8.31 installed already. This should be the case in test lab installations only.

The installation procedure will described in the chapter "Installation of further Clients – Installation of an additional application – Maintaining different client applications using protected configuration".

**NOTE:** Please keep in mind that all Materials Control client installations in version 8.31 or higher in the same environment must use the same Protected Configuration Key Container!

## Installation of further Clients

### Installation of a new application

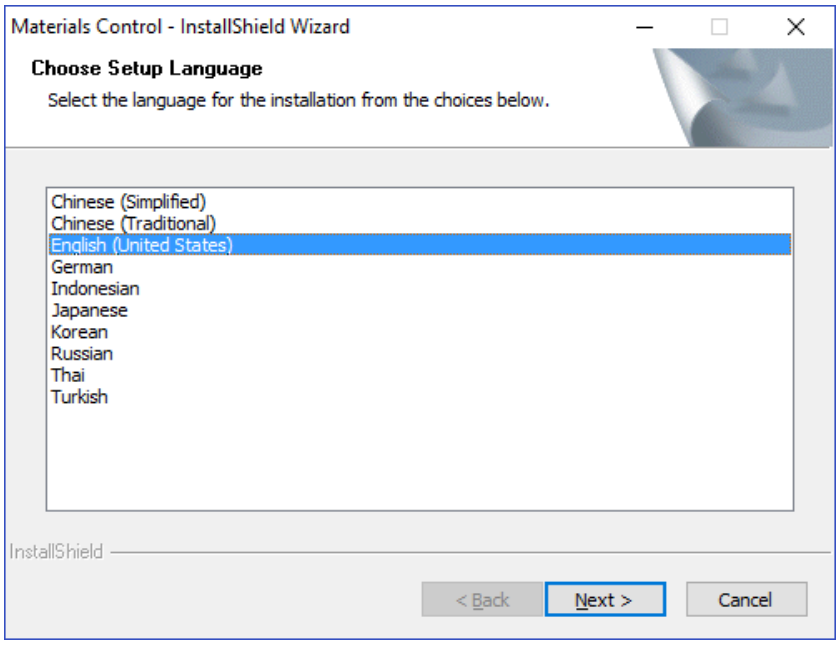
This section will describe the installation of further client applications on additional PCs after the protected key container configuration was created (Please see here!).

The install set prepared during the “Master” installation now contains the protected key container configuration in the folder \CUSTOM\.

**NOTE:** Please keep in mind that all client installations in one environment must use the same Protected Configuration Key Container!

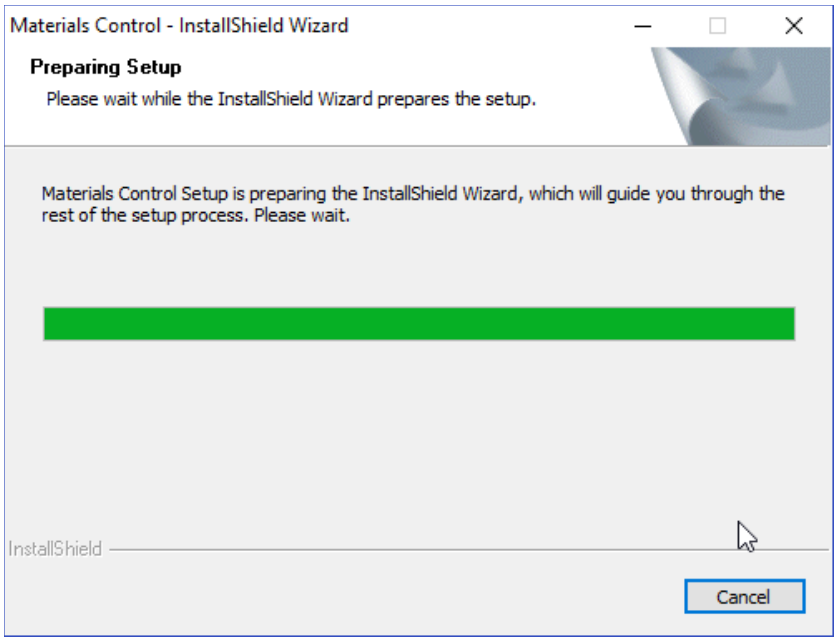
Start the installation by double click on SETUP.EXE in the installation file directory.

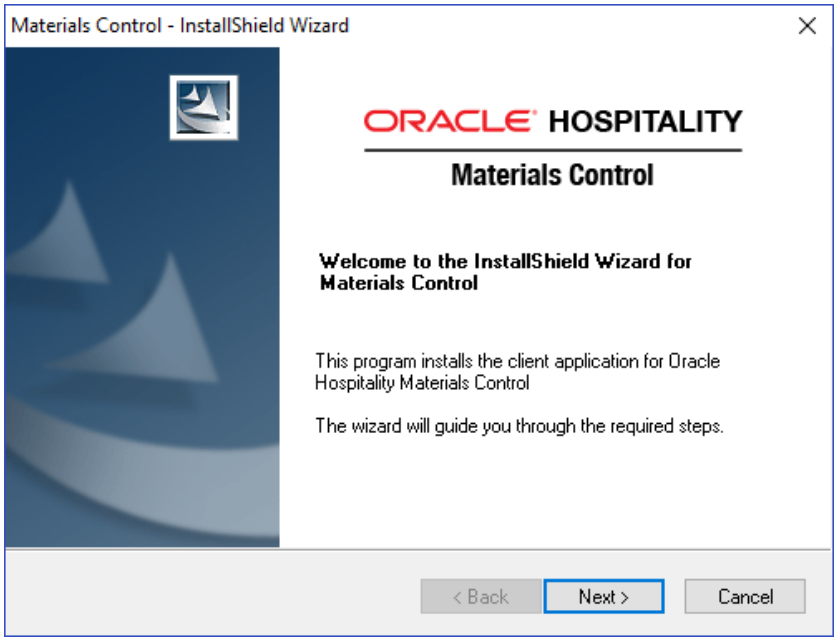
At first the procedure will ask for the Setup Language:



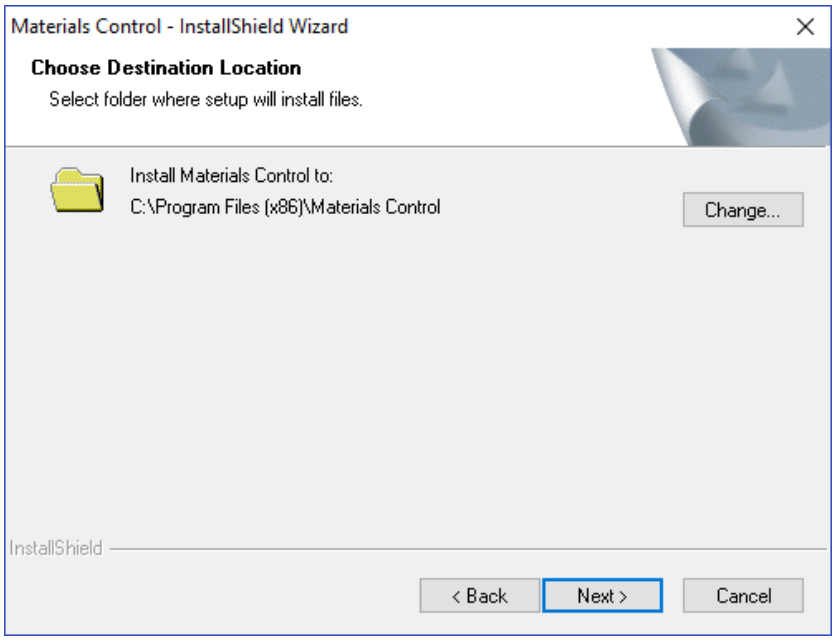

Select the language and click “Next”.

The setup process will now be prepared.



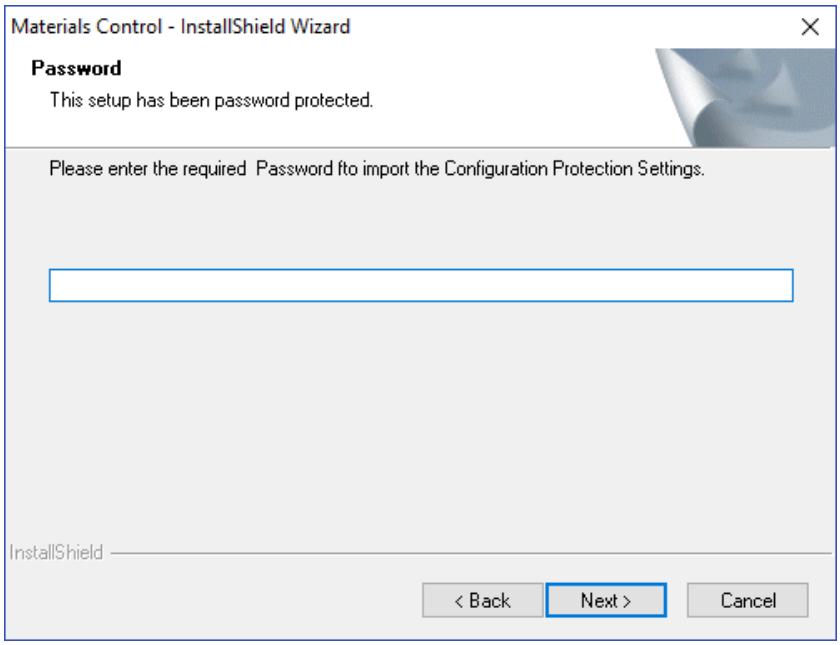




Click “Next" to start.



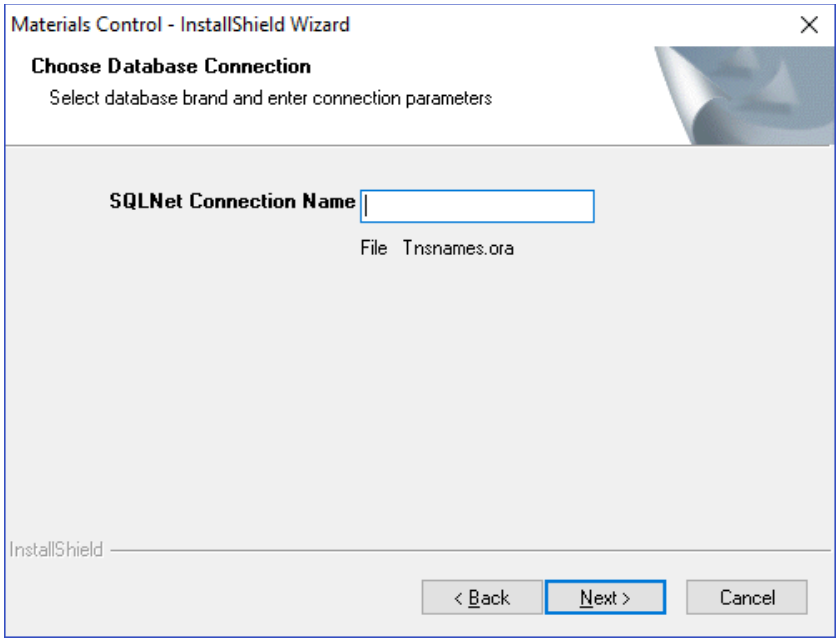

Accept or change the destination and click “Next”.

The installation routine will now check for the Protected Configuration Settings. The Protected Key Container Configuration (folder \CUSTOM\) will be read by the install process. Enter the password defined at the creation of the Protected Key Container Configuration:



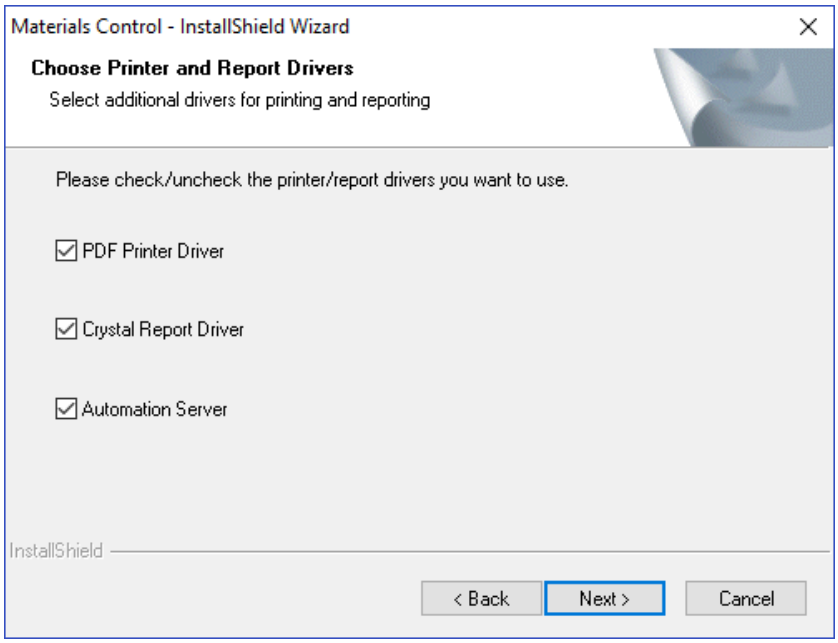

Enter the password and click “Next”.

After successful processing of the protected configuration files, the installation process will check the Oracle database connection:




Enter the name of the Oracle instance and click “Next”.

Select the options to be installed with this client application:



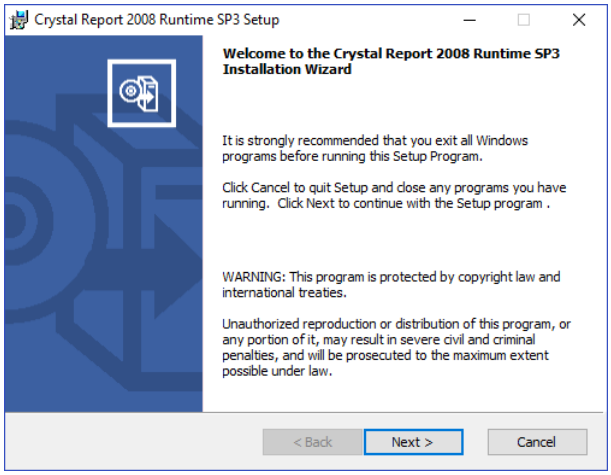

PDF Printer Driver

- This option will install a PDF Converter for documents printed out of the application. This should be selected always.

Crystal Report Driver

- This option will install the Crystal Reports Runtime files. These are required to use the module “Custom Reports” in Materials Control. This is required for most client installations.

  If selected the install process will force the runtime installation after the client application installation.

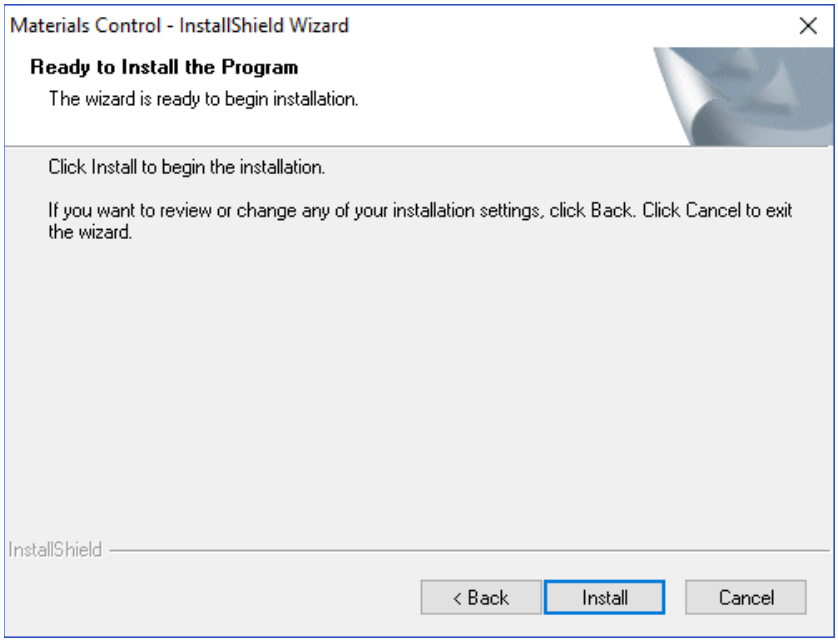


Automation Server

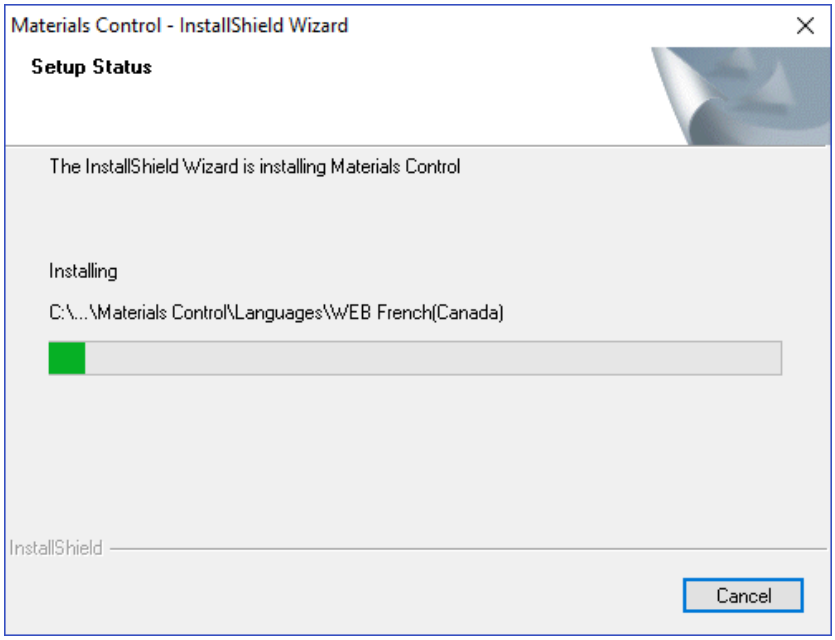
- This option will install a service-based scheduler for processing jobs defined in Materials Control.

After selecting the options click “Next” to proceed.

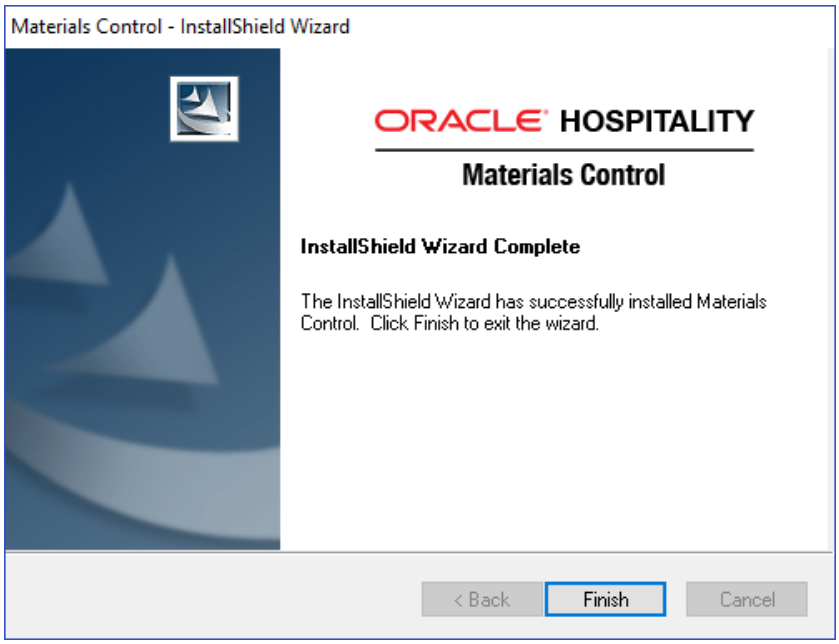
Since all required information is now available the main process can be started.




Click “Install” to proceed.



Once completed, the installation routine will show the following screen:



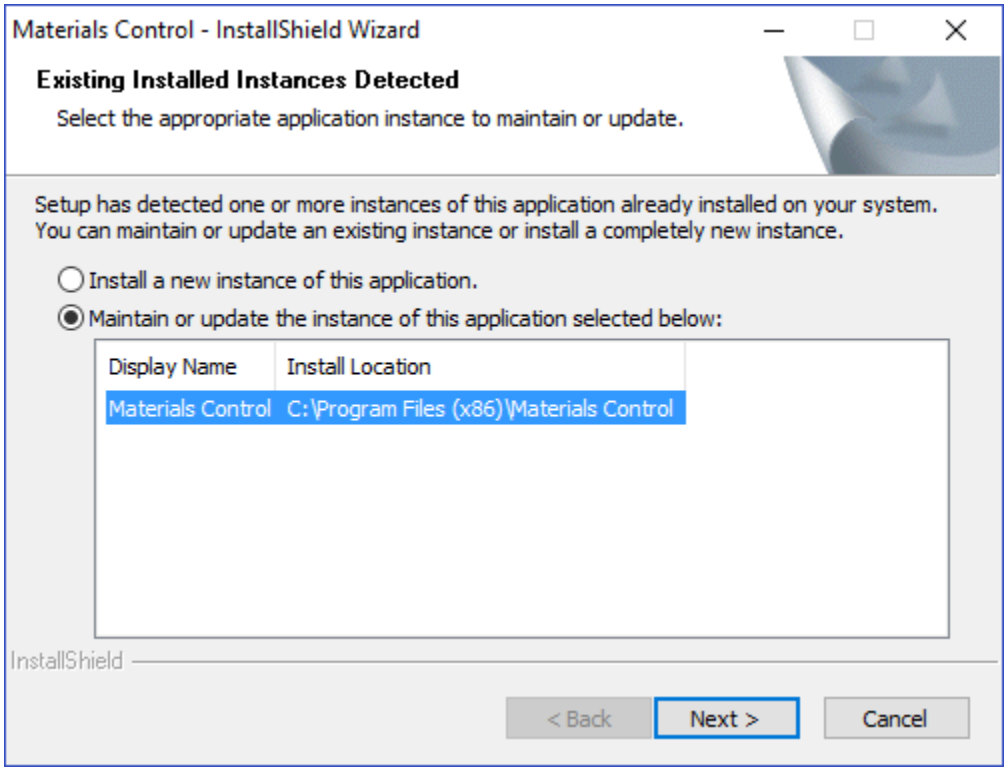

Click “Finish”.

### Update of an existing application

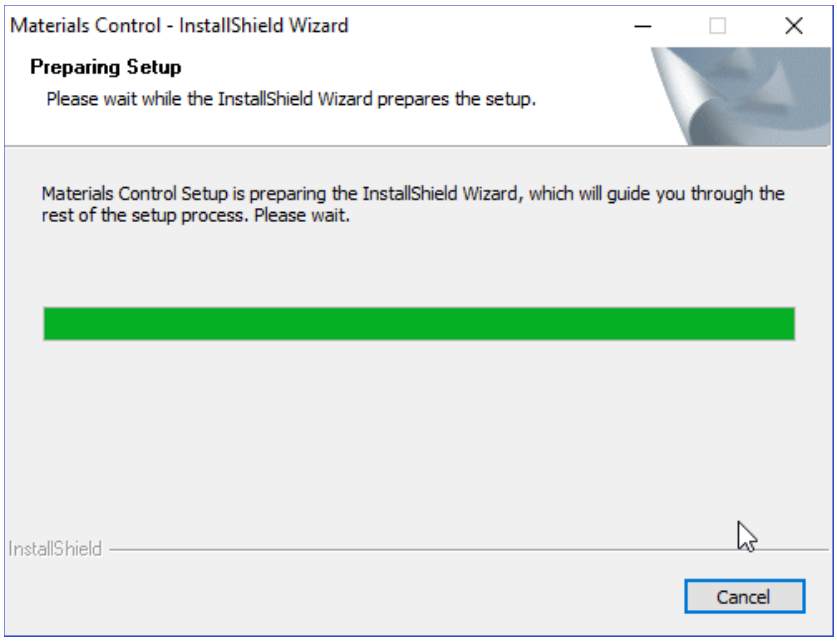
This section will describe the installation of further client applications on additional PCs after the protected key container configuration was created (Please see here!), in an existing environment running an older version of Materials Control. Environments running Materials Control version 8.7.10 and older must be upgraded to version 8.7.20 or higher, before the update to 8.31.*x* can be started.

Start the installation by double click on SETUP.EXE in the installation file directory.

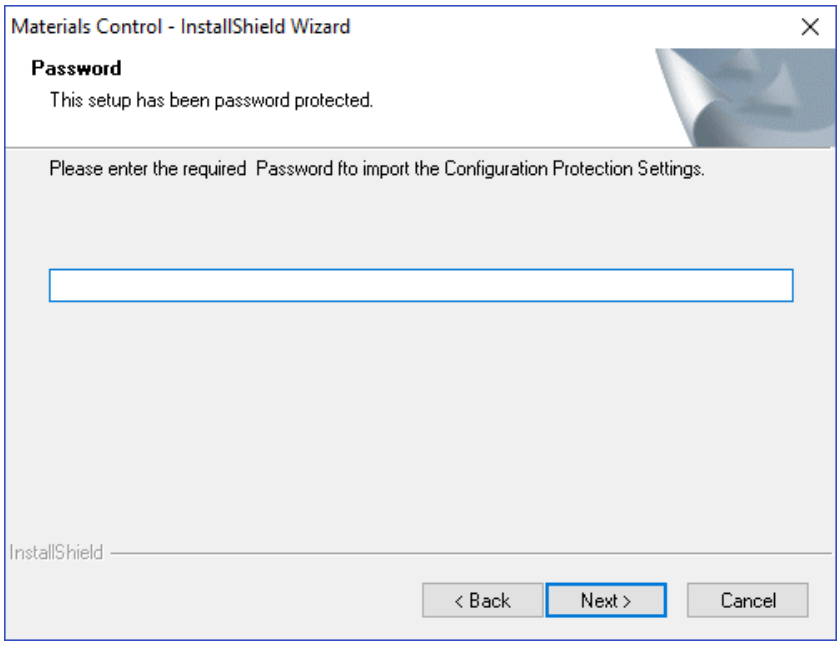
The installation routine will detect the existing installation of a Materials Control client application and will offer to update the existing application:




Select the installed application and click “Next”
The setup process will now be prepared.

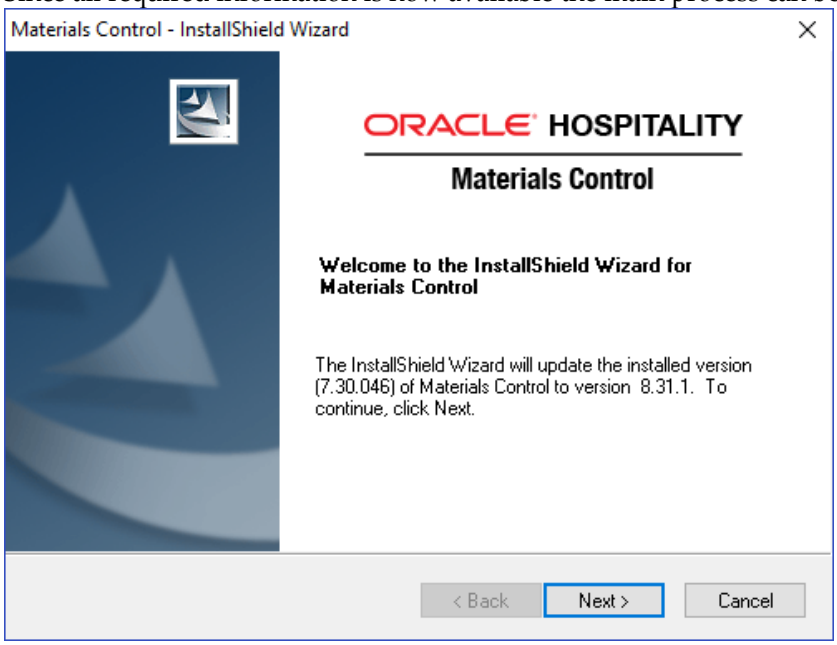



The installation routine will now check for the Protected Configuration Settings. The Protected Key Container Configuration (folder \CUSTOM\) will be read by the install process. Enter the password defined at the creation of the Protected Key Container Configuration:

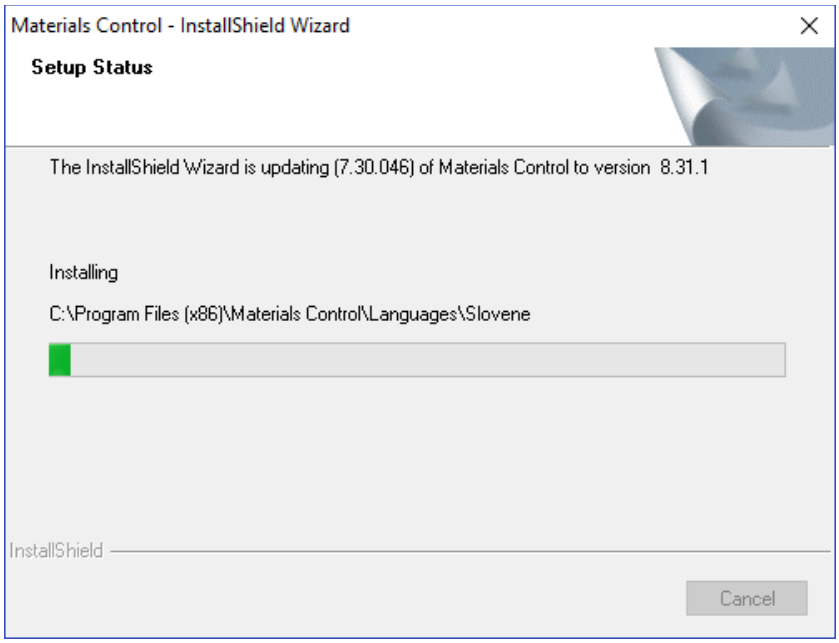



Enter the password and click “Next”.

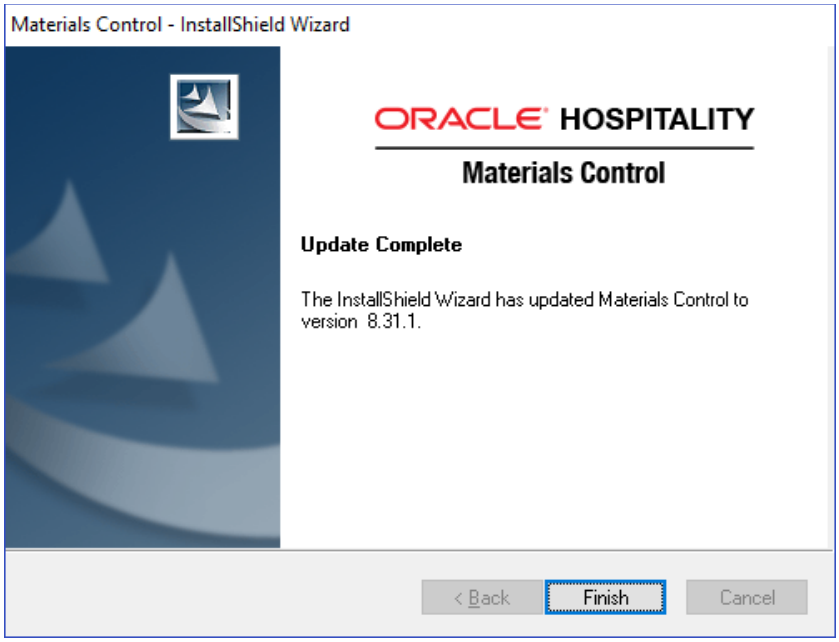
Since all required information is now available the main process can be started.




Click “Next” to proceed.



Once completed, the installation routine will show the following screen:




Click “Finish”

### Installation of an additional application

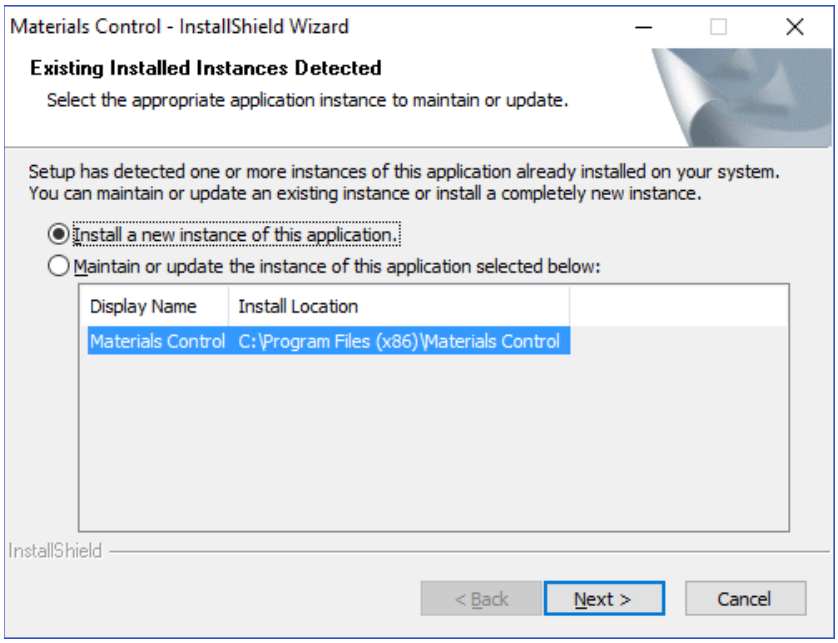
When maintaining a test lab it might be necessary to have different versions of Materials Control installed on one PC. This must not be the case in a production environment!

## Maintaining different client applications in different versions

This section will describe the installation of a new client application of Materials Control 8.31 in an environment having older releases of the application installed which should remain. This should be the case in test lab installations only.

Start the installation by double click on SETUP.EXE in the installation file directory.

The installation routine will detect the existing installation of a Materials Control client application and will offer to install an additional application:




Make sure that the option “Install a new instance of this application” is selected and click “Next” to confirm.

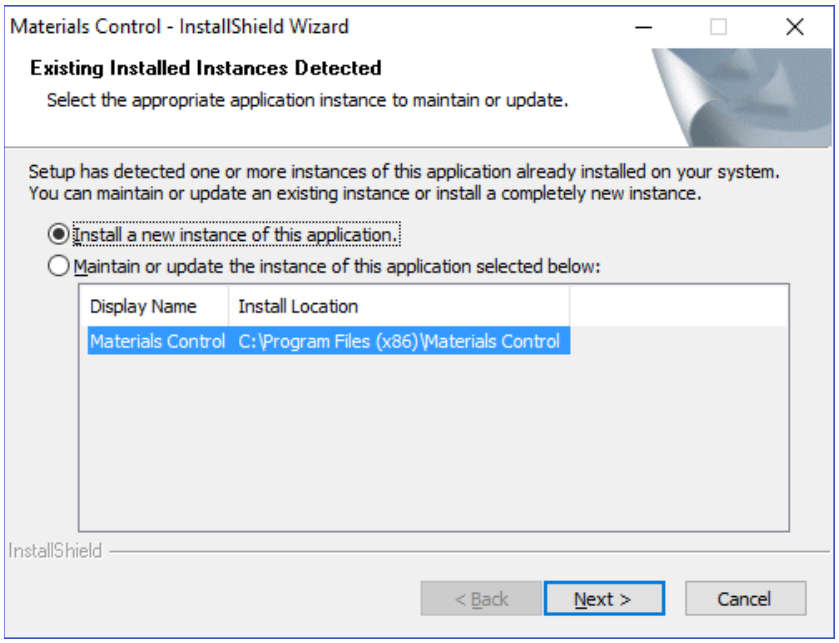
The installation procedure will now be exactly the same as when installing a new application, described in the chapter “Installation of further Clients –Installation of a new application”.

## Maintaining different client applications using protected configuration

This section will describe the installation of a new client application of Materials Control 8.31 in an environment having at least one application of Materials Control 8.31 installed already. This should be the case in test lab installations only.

Start the installation by double click on SETUP.EXE in the installation file directory.

The installation routine will detect the existing installation of a Materials Control client application and will offer to install an additional application:




Make sure that the option “Install a new instance of this application” is selected and click “Next” to confirm.

The installation procedure will now be the same as when installing a new application, described in the chapter “Installation of further Clients –Installation of a new application”.

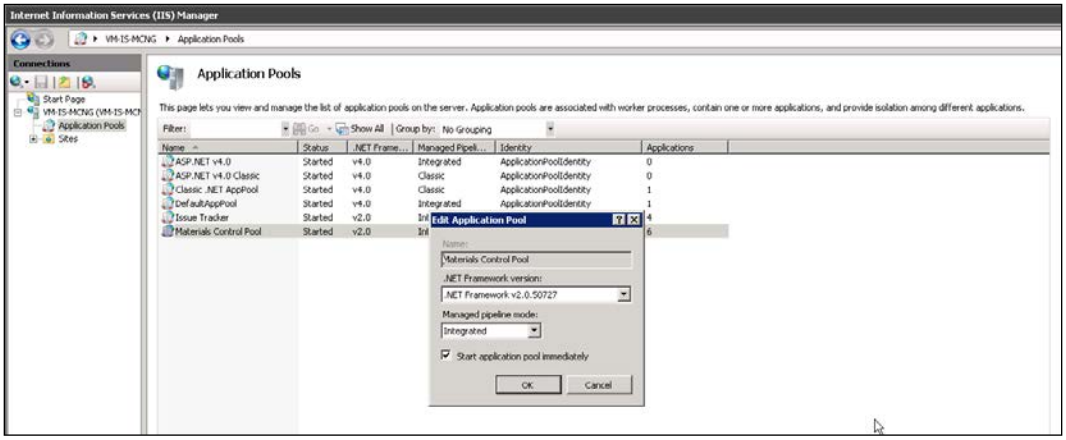
**NOTE:** Please keep in mind that all Materials Control client installations in version 8.31 or higher in the same environment must use the same Protected Configuration Key Container!

## Web Applications

### Prerequisites

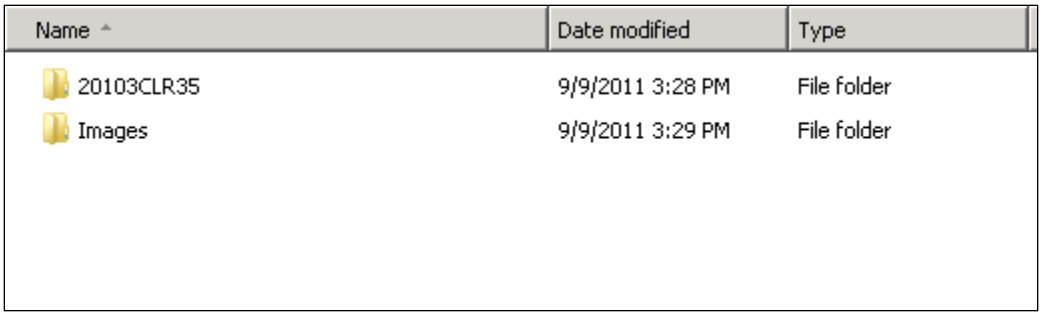
Microsoft Internet Information Server is installed properly and can be accessed/used.

Web applications must run in Application Pool that uses .NET2 and integrated managed pipeline mode.




Infragistics scripts for .NET 3.5 must be updated to the latest version. This can be found in MCweb package.

Copy to inetpub\wwwroot\aspnet_client\Infragistics.




It is recommended to install fresh 8.31 applications instead of updating them, since configuration files are changed. You can also do update, but before that, move the existing .config files to backup location.

### Application Installation

The new tool HMC_SecureConfig.EXE is used to import key container and encryption

> **Note:** The Materials Control IIS webpages for the following description are represented as
>
> <MCWebDir>
>
> <MobileWebServiceDir>
>
> <POSWebServiceDir>
>
> <MobileAuthDir>
>
> <NutrientImportDir>
>
> Replace these with the names of the IIS directories in your environment.

Unzip the following files to a temporary directory.

161020_HMC_MCweb_8.31.4.1555.zip will create the following folders when unzipped…

HMC_MCweb.Application
HMC_MCweb.Config
Infragistics Scripts

161020_HMC_MobileWebService_8.31.2.1555.zip will create the following folders when unzipped…

HMC_MobileWebService.Application
HMC_MobileWebService.Config

161020_HMC_POSWebService_8.31.1.1555.zip will create the following folders when unzipped…

HMC_POSWebService.Application
HMC_POSWebService.Config

161024_HMC_MobileAuthWebService_8.31.3.1555.zip will create the following folders when unzipped…

HMC_MobileAuthWebService.Application
HMC_MobileAuthWebService.Config

161020_HMC_NutrientImport_8.31.2.1555.zip will create the following folders when unzipped…

HMC_NutrientImport.Application
HMC_NutrientImport.Config

1) CASE Update:
   Once you have backup copies of the <MCWebDir>, <MobileWebServiceDir>, <POSWebServiceDir>, <MobileAuthDir>, <NutrientImportDir>, delete all the **contents** of these folders. The folders should be completely empty. Do not delete the folders!

**HMC_MCweb**

2) Browse to the HMC_MCweb.Application directory, select all contents and copy.

3) Browse to the C:\ inetpub\ wwwroot\ <MCWebDir> folder, and paste in all files from the HMC_MCweb.Application directory.

4) Browse to the HMC_MCweb.Config directory, copy the new web.config and paste it into the C:\ inetpub\ wwwroot\ <MCWebDir> directory.

5) Open this web.config and edit the section `<appSettings>` as required.
   **NOTE:** It is no longer necessary to enter the DB password here!

**Infragistics**

6) Browse to the Infragistics Scripts folder in the new MCweb build and copy the Infragistics.zip file.

7) Browse to C:\ inetpub\ wwwroot\ aspnet_client and delete the existing Infragistics folder.

8) Paste the new Infragistics.zip file into the aspnet_client folder and extract the contents. This should create a new folder named Infragistics

**HMC_MobileWebService**

9) Browse to the HMC_MobileWebService.Application directory, select all contents and copy.

10) Browse to the C:\ inetpub\ wwwroot\ <MobileWebServiceDir> folder, and paste in all files from the HMC_MobileWebService.Application directory.

11) Browse to the HMC_MobileWebService.Config directory, copy the new web.config and paste it into the C:\ inetpub\ wwwroot\ <MobileWebServiceDir> directory.

12) Open this web.config and edit the section `<appSettings>` as required.
    **NOTE:** It is no longer necessary to enter the DB password here!

**HMC_POSWebService**

13) Browse to the HMC_POSWebService.Application directory, select all contents and copy.

14) Browse to the C:\ inetpub\ wwwroot\ <POSWebServiceDir> folder, and paste in all files from the HMC_POSWebService.Application directory.

15) Browse to the HMC_POSWebService.Config directory, copy the new web.config and paste it into the C:\ inetpub\ wwwroot\ <POSWebServiceDir> directory.

16) Open this web.config and edit the section `<appSettings>` as required.
**NOTE:** It is no longer necessary to enter the DB password or the LoginPassword here!

**HMC_MobileAuthWebService**

17) Browse to the HMC_MobileAuthWebService.Application directory, select all contents and copy.

18) Browse to the C:\ inetpub\ wwwroot\ <MobileAuthDir> folder, and paste in all files from the HMC_MobileAuthWebService.Application directory.

19) Browse to the HMC_MobileAuthWebService.Config directory, copy the new web.config and paste it into the C:\ inetpub\ wwwroot\ <MobileAuthDir> directory.

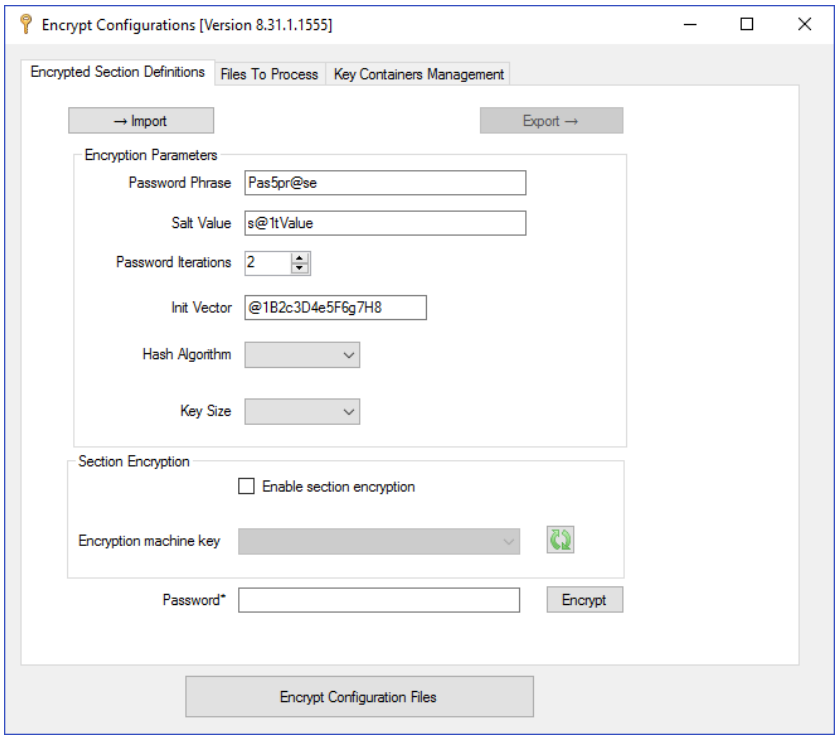
20) Open this web.config and edit the section `<appSettings>` as required.
**NOTE:** It is no longer necessary to enter the DB password here!

### HMC_SecureConfig

The new tool SecureConfig.exe is used to import key container and encryption definitions for add-on modules like MCweb, POSWebService and Nutrient Import. The Key Container Configuration can be either read from an existing Materials Control thick client application or from the install set.
Usually the Materials Control thick client is installed on the web server as well.

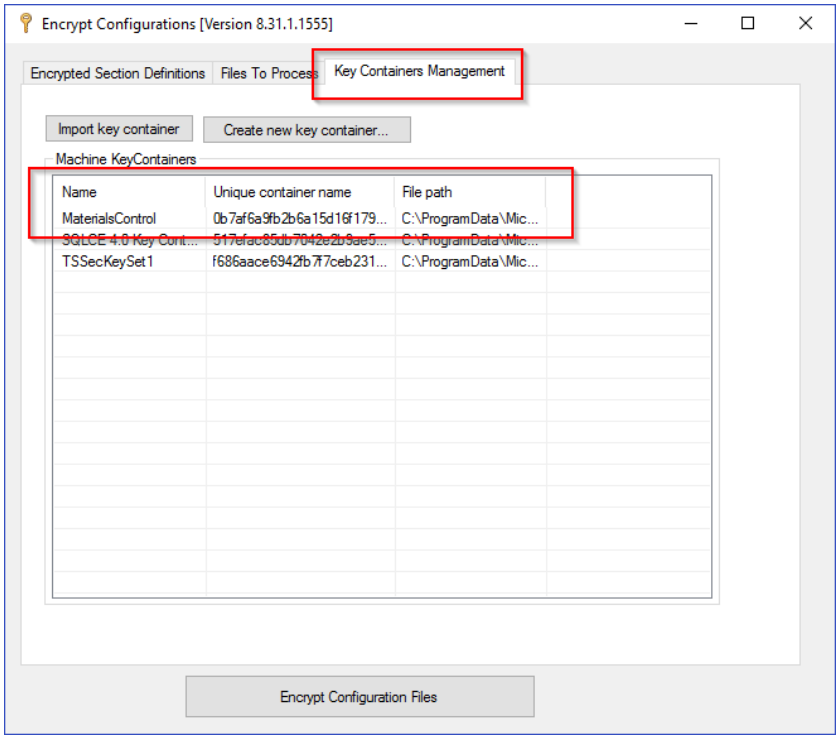
Extract the 161027_HMC_SecureConfig_8.31.1.1555.zip file to any location; it will create a folder named 161027_HMC_SecureConfig_8.31.1.1555.

Start contained SecureConfig.exe as Administrator.



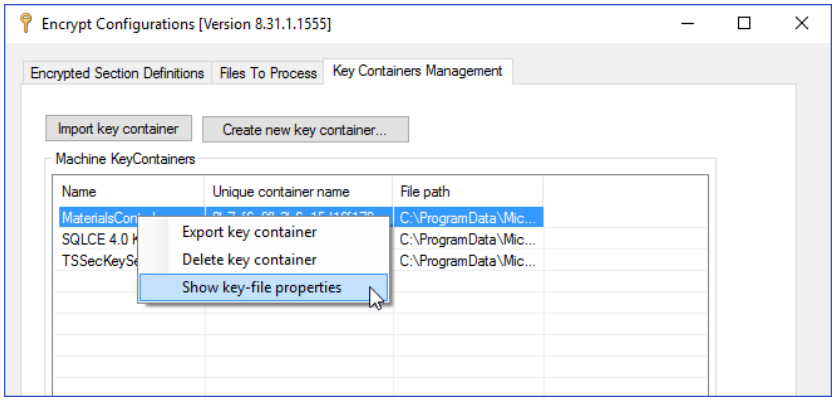

Select tab Key Containers Management:

If Materials Control thick client was already installed on this machine, you will find a Key Container named Materials Control in the list:

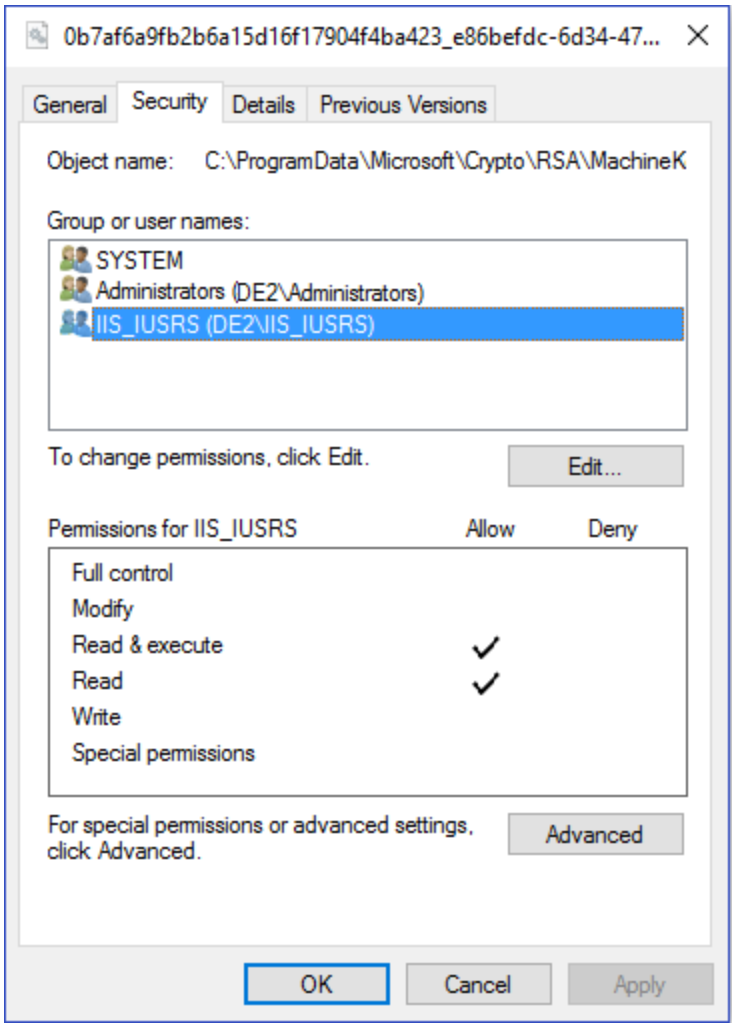



If the Key Container Materials Control is not listed, it must be imported. Please make sure that it is named "MaterialsControl". This process will be explained in the chapter "Importing Materials Control Protected Key Container".

Mark the record and right-click to open the context menu:




Select the option "Show key-file properties" and open the second tab "Security" in the opened screen:



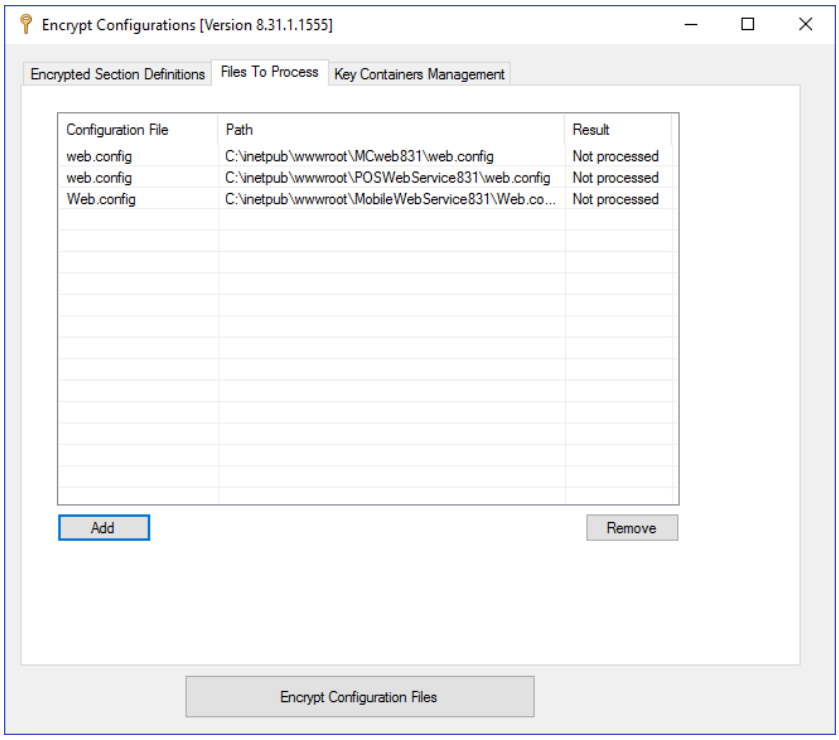

- SYSTEM requires full control (for applications running under system context, like Automation Service, WATCH.EXE)

- Group IIS_IUSRS (MCweb, web services) will require “Read” and “Read & execute” access.

- Group Authenticated Users will require will require "Read" and "Read & execute" access.

Confirm with ”OK” to close this screen.

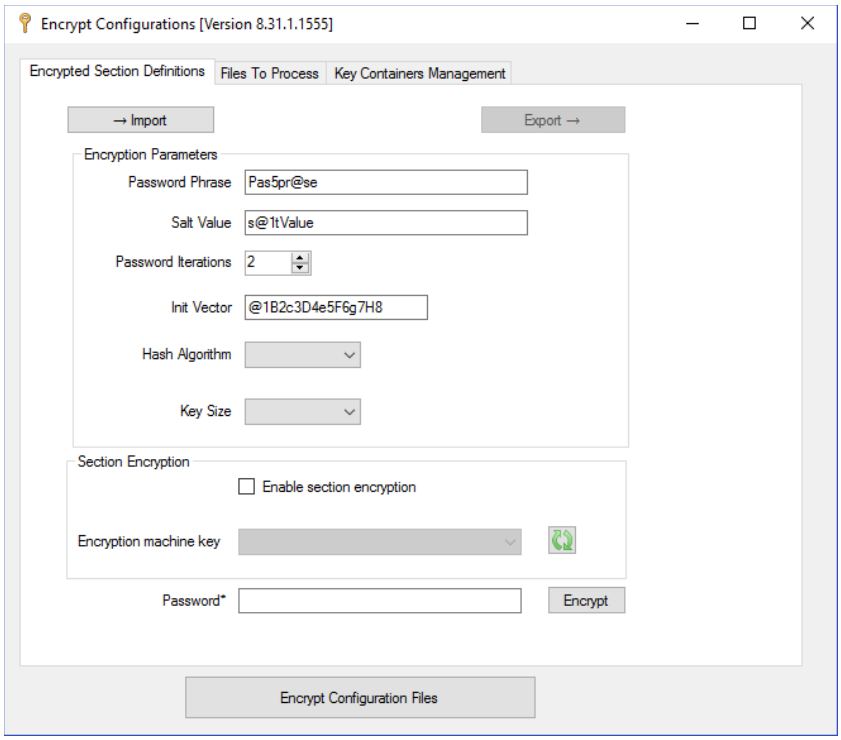
Switch to the tab “Files To Process”:



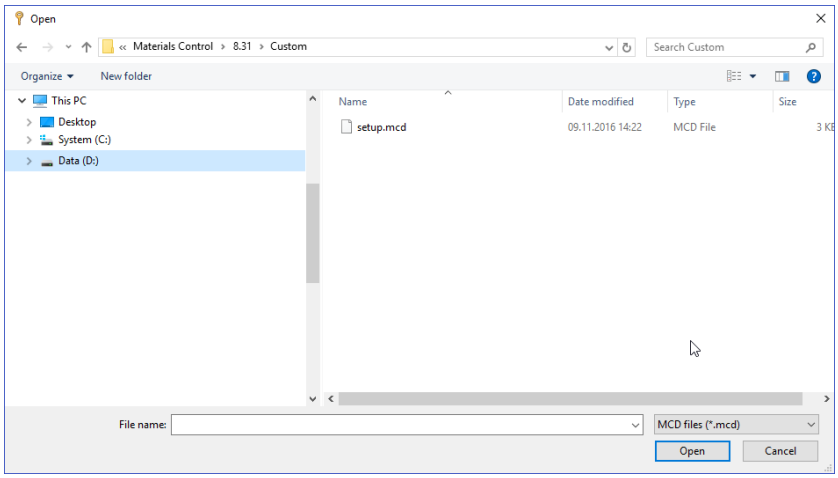

Here all Configuration files to be encrypted must be added.
These are depending on your installation:

| | |
|---|---|
| HMC_MobileWebService: | Web.config |
| HMC_MCweb: | Web.config |
| HMC_POSWebService: | Web.config |
| HMC_MobileAuthWebService: | Web.config |
| HMC_NutrientImport: | NutrientImport.exe.config |

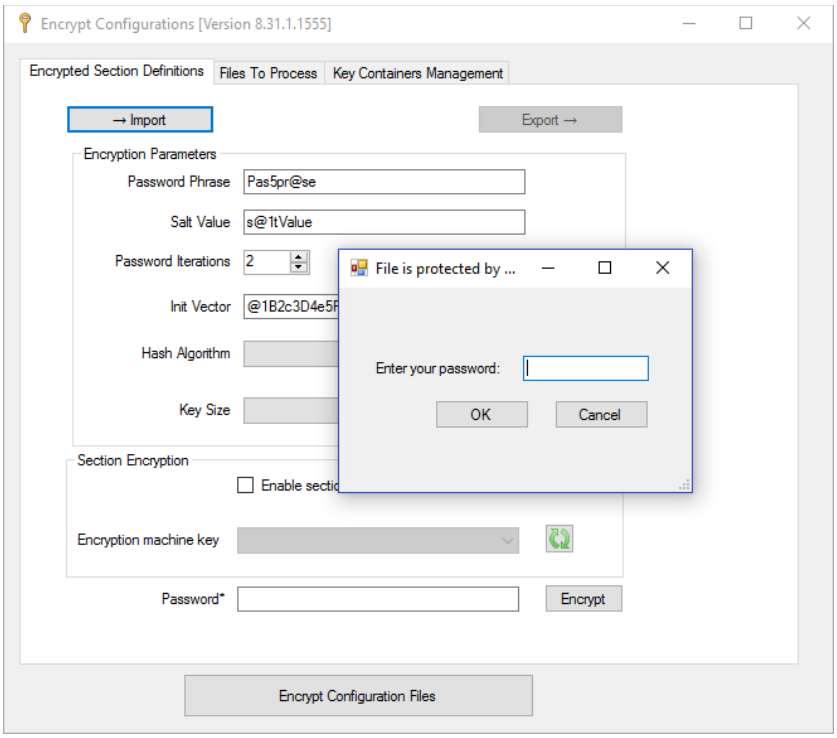
Once done, switch to the tab “Encrypted Section Definitions”:



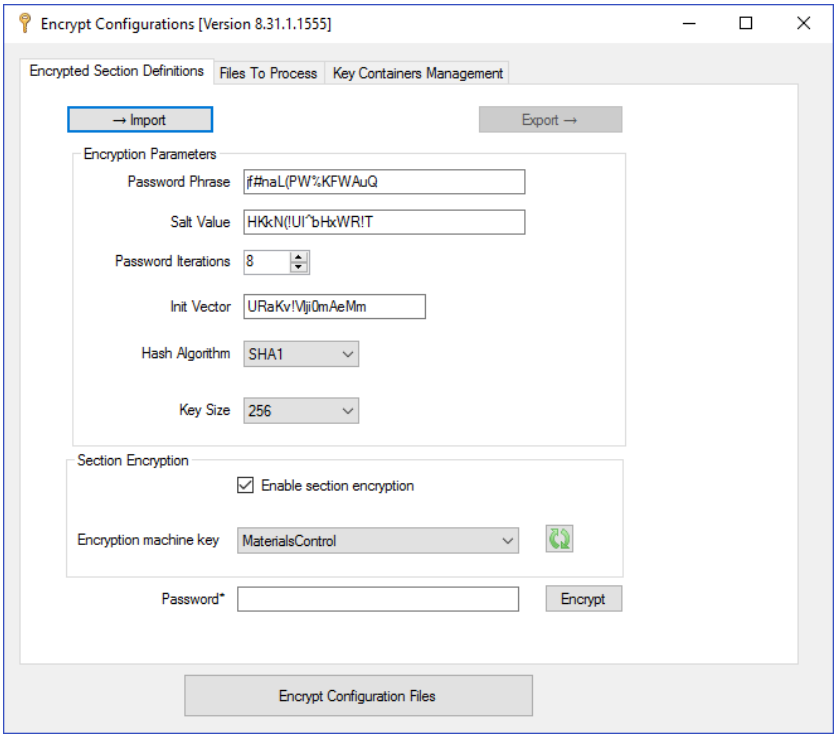

Click on the button “Import” and select the Container Definiton file “setup.mcd”. This can be found in the folder \CUSTOM\ in the Materials Control installation set.



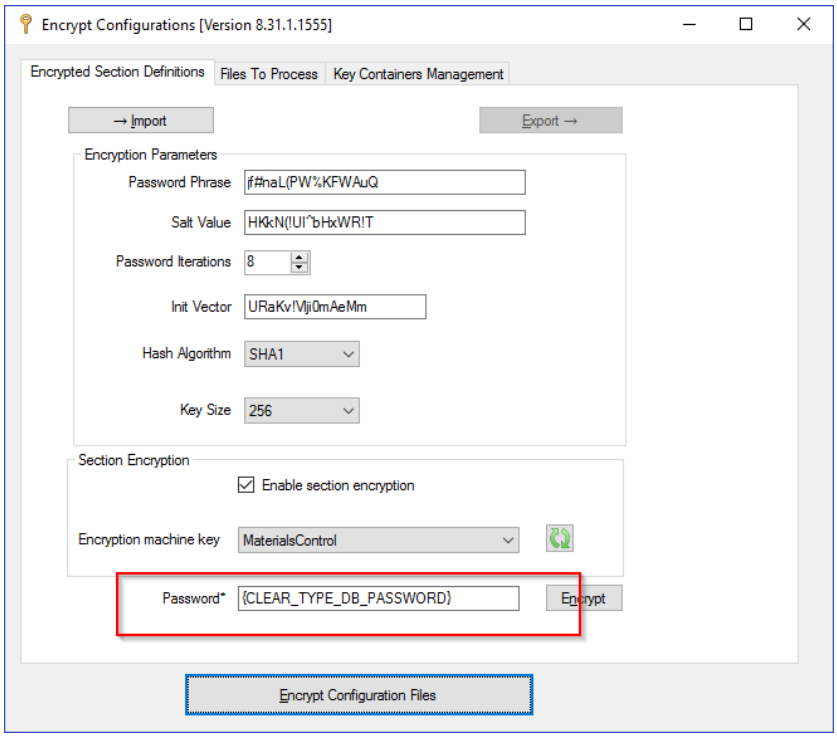

Select the file and click “Open”.




Enter the password defined at the installation of the Materials Control thick client and click “OK”.



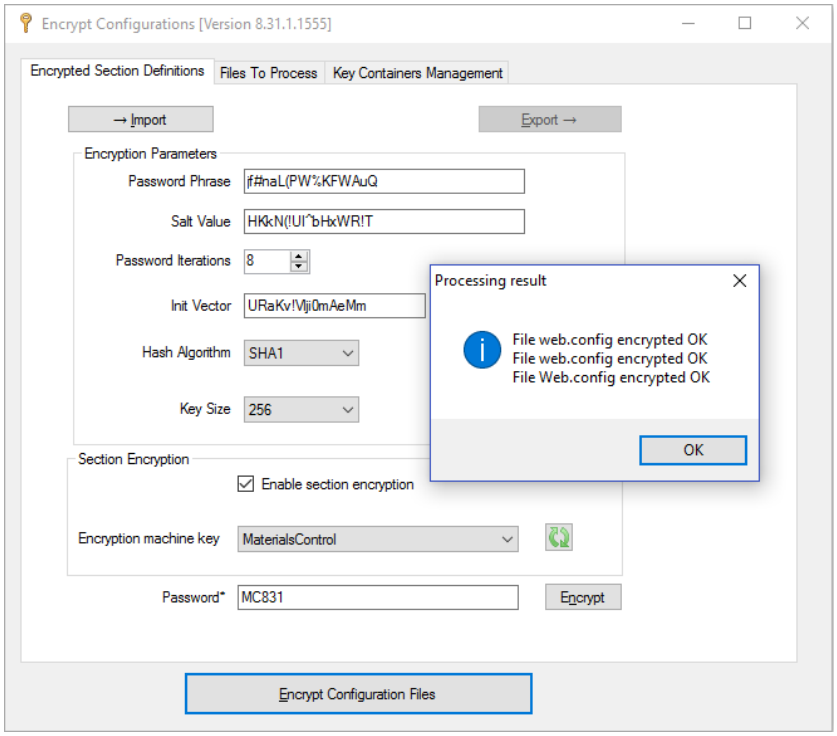

The application will now load the encryption parameters.




No value in the upper section should be changed!

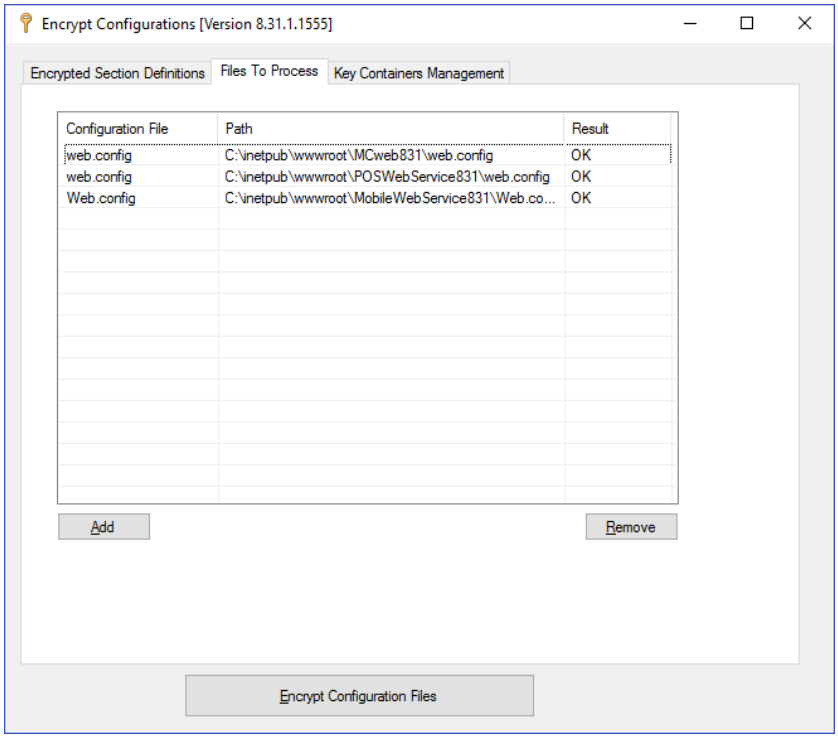
At the bottom of the screen a field “Password*” is shown. Here the database password in clear type must be entered.

The button “Encrypt Configuration Files” must be used to process the encryption.



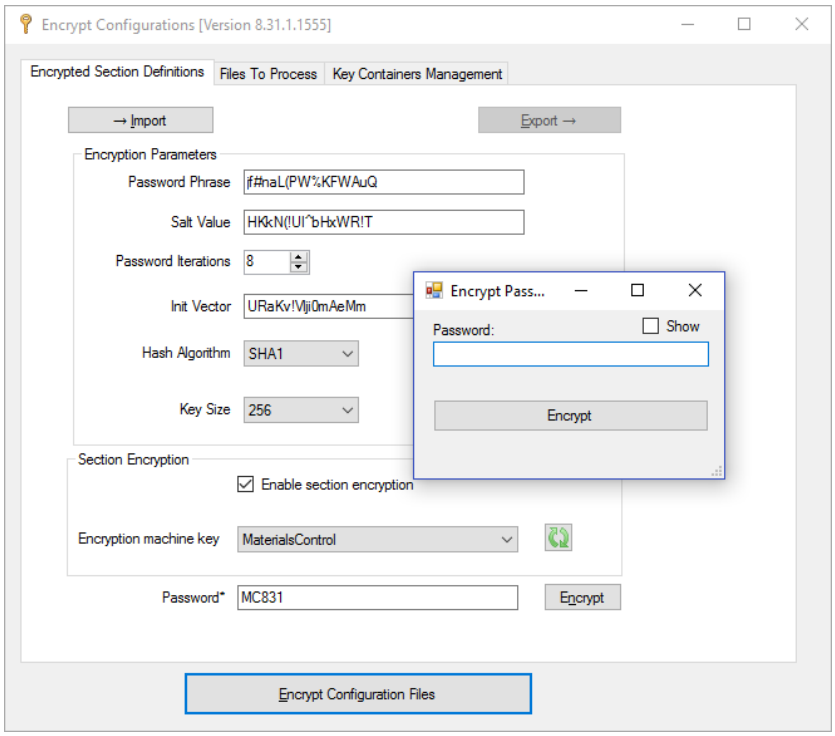

The success will be shown like above.

Switch to the tab “Files to Process” to check the details:



### Encryption of HMC_POSWebService

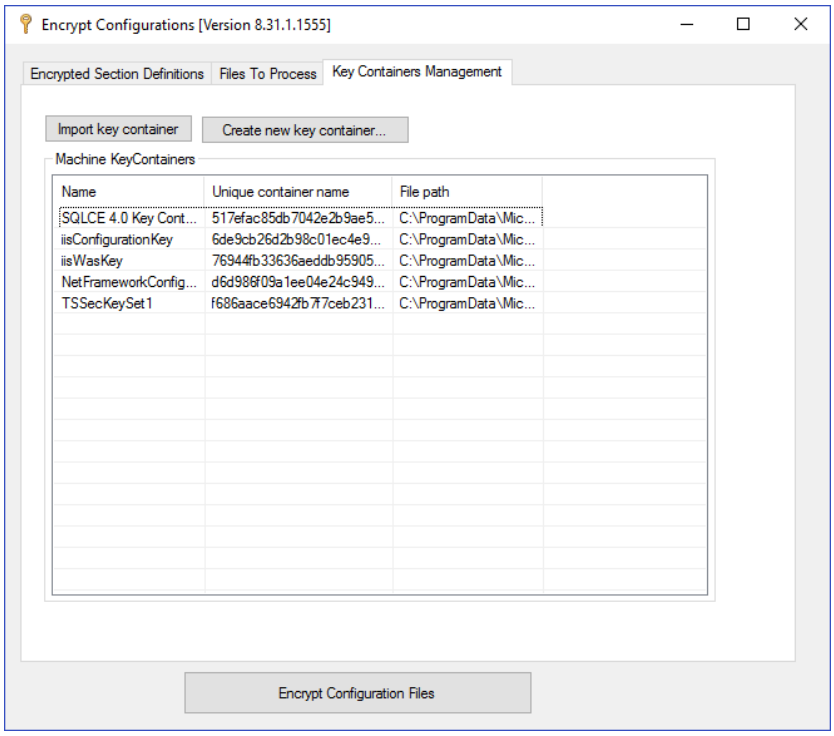
During the Encryption of HMC_POSWebService, the HMC_SecureConfig tool will ask for the password of the login user defined in the WEB.CONFIG.



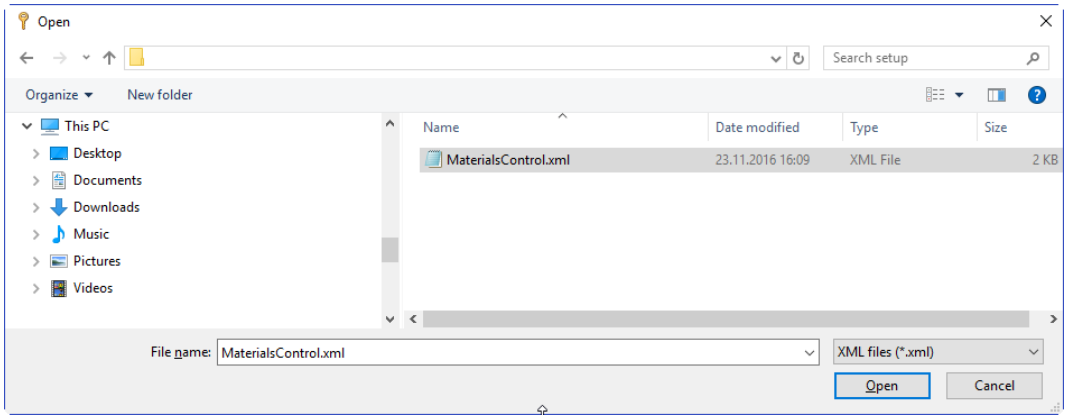

This password will be stored in the encrypted section as well.

### Importing Materials Control Protected Key Container

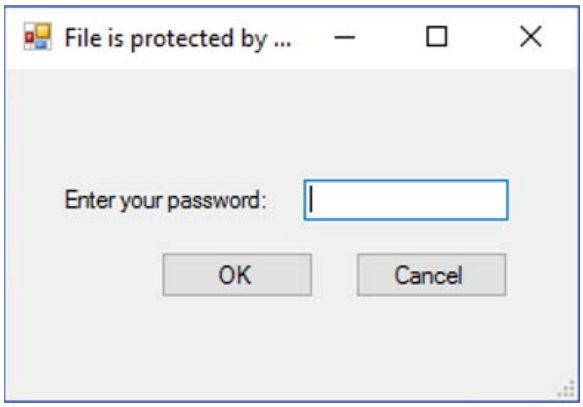
If the Key Container Materials Control is not listed, it must be imported. Open the SecureConfig.exe as Administrator and select the tab ”Key Containers Management”:




Click on the button “Import key container”:




Select the file MaterialsControl.xml (contained in the protected configuration files) and click “Open”.

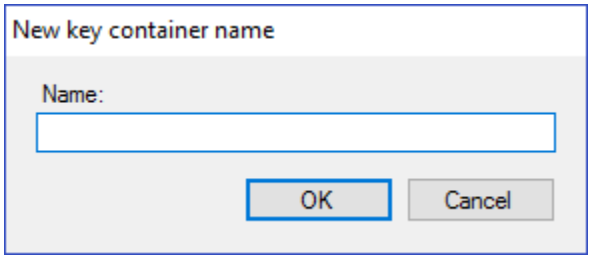



Enter the password used at creation of the protected configuration.

The new Key Container will be generated now. This may take some seconds.

### Creation Materials Control Protected Key Container

Click on the button “Create new key container”




Define the name as MaterialsControl and confirm with “OK”. The new Key Container will be generated now. This may take some seconds.
Once the new container is listed, it can be used to store the configuration.

# 3 Preconfigured Installation

The Materials Control installation wizard uses two .ini files to determine installation requirements and processes. You can configure the values in the files to install the application with predefined settings and definitions.

1. Download and extract the installation archive.
2. Create a folder named `\Custom\` in the extracted folder.
    a. Copy `SQL.ini` and `FMLogin.ini` into the root of `\Custom\`
    b. Copy key container configuration files into the root of `\Custom\`
    c. Copy the Order Sheet and other reports to `\Custom\QRP_LNG\` where *`LNG`* is the language code you want to use.
    The installation wizard creates and overwrites the content of the `QRP_ENG` folder with English reports. To use other languages, create a folder, copy your translated report templates into the folder, and then configure Materials Control to use the custom reports folder. For example, you can create, populate, and then direct Materials Control to the `QRP_FRA` folder containing report templates translated to French.
    d. Do not copy `setup.ini` and `janinst.ini` into the `/Custom/` folder.
3. Configure the .ini files:
    a. Configuring janinst.ini
    b. Configuring setup.ini
4. Assign required user privileges to the Key Container. HMC_Secure_Config contains information and instructions for using the SecureConfig tool to configure the Key Container.
5. Run the installation wizard.
    The installation wizard does not skip the requirement for entering the password required to load the Protected Key Container configuration.

## Configuring janinst.ini

### [Types]

**Table 1 - janinst.ini Types Parameters**

| Parameter | Description |
|---|---|
| Show | Do not change. |
| Unattended | Set to `T` to activate unattended installation. |
| ShowAbortMessages | Set to `T` to show a button to abort or cancel the installation. |

### [Environment]

**Table 2 - janinst.ini Environment Parameters**

| Parameter | Description |
|---|---|
| Path | Enter the target installation path. |
| Show | Do not change. |
| ShowCrystalPDF | Do not change. |
| installOLEDB | Do not change. |

### [Connectivity]

**Table 3 - janinst.ini Connectivity Parameters**

| Parameter | Description |
|---|---|
| Oracle | Do not change. |
| ORACLEP1Name | Enter the target name of the Oracle Database instance. |
| ORACLEP2File | Do not change. |
| Show | Do not change. |

## Configuring setup.ini

### [Startup]

**Table 4 - setup.ini Startup Parameters**

| Parameter | Description |
|---|---|
| EnableLangDlg | Set to `Y` to show the language selection page, or set to `N` to hide the page and use the system local language. |
| Product | Do not change. |
| ProductGUID | Do not change. |
| CompanyName | Do not change. |
| ErrorReportURL | Do not change. |
| MediaFormat | Do not change. |
| LogMode | Installation Method contains more information on the values you can enter to configure the installation type. |
| SmallProgress | Do not change. |
| SplashTime | Do not change. |
| CheckMD5 | Do not change. |

| | |
|---|---|
| CmdLine | Enter the following values separated by a space:<br>• Installation Method: configure the installation type.<br>• Language Codes: set a default language.<br>For example, `/hide_usd /l1028`<br>The language code entry must be placed after the installation method parameter. |
| ShowPasswordDialog | Do not change. |
| ScriptDriven | Do not change. |

## Installation Method

You can configure `LogMode` and `CmdLine` parameters in `setup.ini` to change installation defaults and prompts:

- To install a new instance:
  - Enter `4` in `LogMode`.
  - Enter `/hide_usd` in `CmdLine`.
- To prompt users to install a new instance or to select an instance to upgrade:
  - Enter `4` in `LogMode`.
- To upgrade the first existing installation (this may not select the oldest instance):
  - Enter `1` in `LogMode`.
  - Enter `/hide_usd` in `CmdLine`.
- To prompt users to select an instance to upgrade:
  - Enter `1` in `LogMode`.

## Language Codes

Enter `/LOWERCASE_L[`*`4-digit language code`*`]` to set a default language. For example: `/l1028`

Materials Control supports the following:

- 1028: Taiwanese
- 1031: German
- 1033: English
- 1041: Japanese
- 1042: Korean
- 1049: Russian
- 1055: Turkish
- 2052: Chinese

# 4 Additional Information

## Database Initialization

You must start the Materials Control Thick Client application to update the database and register the modules before you can log into the Materials Control web application. If you attempt to log in first, Materials Control returns the following message:

```
Login forbidden!
Please start the Materials Control Thick Client application to
configure the database for first use!
```

## Database Shells

### Country Shells

In some countries shell databases are maintained by the local offices or partners. In order to "release" the databases from the Protected Key Configuration used in the Shell Maintenance Environment, the field CTL_SHELL in table CONTROLTAB must be updated to 1 before connecting in the customer environment.

During the database update procedure the Materials Control application will detect this setting and maintain the database accordingly.

For further details please contact the Oracle Consulting team.

**It is recommended to update this field before creating the shell dump!**

### Customer Shells

Some customers maintain their shell databases by themselves. In order to "release" the databases from the Protected Key Configuration used in the Shell Maintenance Environment, the field CTL_SHELL in table CONTROLTAB must be updated to 1 before connecting in the customer environment.

During the database update procedure the Materials Control application will detect this setting and maintain the database accordingly.

For further details please contact the application specialists.

**It is recommended to update this field before creating the shell dump!**

## Nutrient Import

The Nutrient Import application also must be updated to use the encrypted configuration.

1. CASE Update: Once you have a backup copy of the <NutrientImportDir>, delete all the **contents** of this folder. The folder should be completely empty. Do not delete the folder!
2. Browse to the HMC_NutrientImport.Application directory, select all contents and copy.
3. Browse to the C:\ inetpub\ wwwroot\ <NutrientImportDir> folder, and paste in all files from the HMC_NutrientImport.Application directory.

4. Browse to the HMC_NutrientImport.Config directory, copy the new NutrientImport.exe.config and paste it into the C:\ inetpub\ wwwroot\ <NutrientImportDir> directory.
5. Open this web.config and edit the section `<appSettings>` as required.
6. **NOTE:** It is no longer necessary to enter the DB password here!
7. Protect the file NutrientImport.exe.config using HMC_SecureConfig as described above.

## Replication

All databases in a replication environment must use the same Protected Key Container files.

## Multi-Property Installations

In all environments where multiple databases must be accessed, the **same** Key Container must be used for **all** client applications accessing these databases!

# 5 Materials Control Mobile Solutions

Follow these instructions to install Materials Control Mobile Solutions on workstations and hand-held terminals.

## Installing Materials Control Mobile Solutions

1. Connect your workstation or device to the PC.
2. Download and extract the *date*_HMC_MobileSolutionSetup_*version* archive to a temporary folder on the PC.
3. Double-click SETUP.EXE, wait for the installation wizard to finish preparing the files, and then click **Next**.
4. Enter your name, your organization name, and then click **Next**.
5. Select the **Complete** setup type, and then click **Next**.
6. Fill out the Mobile Solutions Parameter form, and then click **Next**:
    a. Enter the URL for the mobile web service.
    b. Enter a time-out for verifying the status of the service. By default, enter 1000.
    c. Enter a time-out for scanning operations. By default, enter 10.
    d. Select **No auto-start** as the auto-start option.
7. Click **Install** and allow the installation wizard to begin installation components on the connected devices.

## Setting Up Zebra MC40 for Mobile Solutions

### Using the Zebra MC40

The *Zebra MC40 User Guide* contains information and instructions for using, configuring, and troubleshooting the Zebra MC40 device. The User Guide is located in the Support section of the Zebra website.

### Incompatible Components

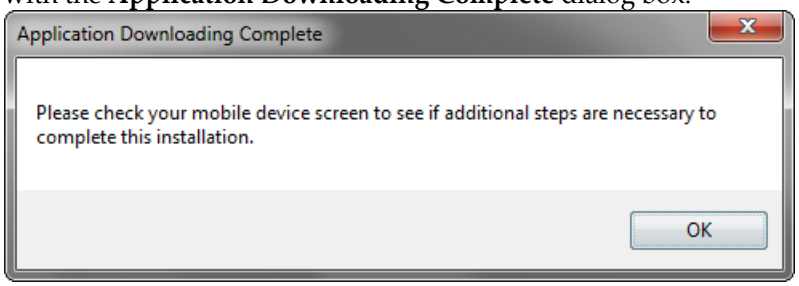
The installation wizard shows incompatibility warning messages when installing the following components on the Zebra MC40:

- Microsoft Windows .NET Compact Framework 3.5
- Microsoft SQL Server Compact 3.5
- Symbol Managed Class Libraries
- Oracle Hospitality Materials Control Mobile Solutions

You must follow these instructions to install the components correctly:

1. When the PC shows the **Unsupported Device Type** message, click **OK** to confirm that the device is not supported.
2. Click **OK** on the Add/Removal Programs screen.

3. For Symbol Managed Class Libraries, the installation wizard checks for existing installations. Click **OK** to proceed with the re-install/upgrade.
4. For each incompatible component, do not immediately click **OK** when prompted with the **Application Downloading Complete** dialog box.




5. Check the device for the message: `The program is not compatible with the operating system and, therefore, may not run on this device. Do you want to continue installation?`
6. Click **Yes** on the device, and then allow the component to install.
   For Symbol Managed Class Libraries, click **OK** to proceed with the re-install/upgrade.
7. You can now click **OK** on the dialog box on the PC.

## Setting the Screen Resolution

Set the Zebra MC40 to a screen resolution that supports Materials Control.

1. In Microsoft Windows Compact Edition 7, navigate to the **Control Panel**, and then click **Screen Resolution**.
2. Set the Screen Resolution to **WQVGA (240 x 400 pixels)**.
3. Select **Keep settings after Cold Boot**.
4. Click **OK**, and then click **Yes** to warm boot the device.

## Disabling Automatic Screen Orientation

The Mobile Client cannot dynamically re-size when the orientation changes. Therefore, auto orientation should be turned off in the device.

1. Click **Start**, click **Settings**, click **Control Panel**, and then click **IST Settings**.
2. Deselect **Auto Orientation**, and then click **OK**.

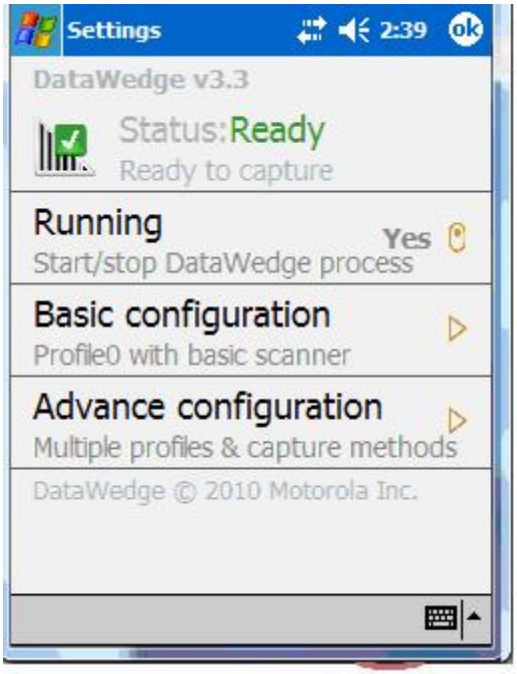
## Changing the Battery

When changing the battery for your Zebra MC40, use the following instructions to avoid resetting the device and needing to reinstall Mobile Solutions:

1. Press the power button.
2. Click **Safe Battery Swap**.
3. Let the device shut down, and then change the battery.

## Activating the Bar Code Scanner

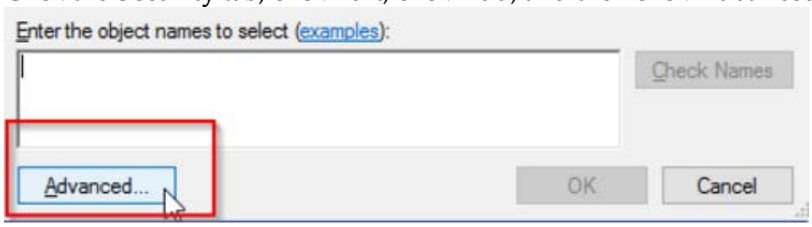
On the Zebra MC40, search for the DataWedge application and verify that the scanner is activated.



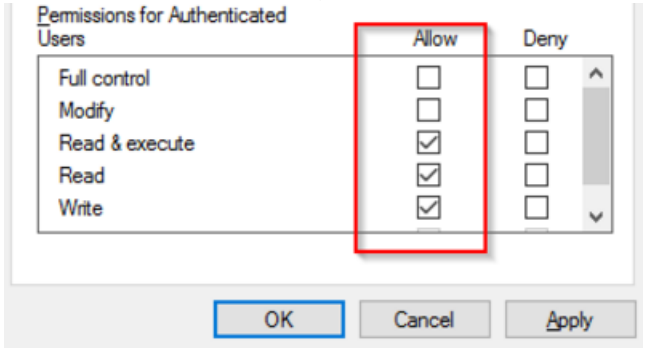
# 6 RSA Access Rights

Follow these instructions to ensure that users have sufficient rights to access the RSA container.

1. Open SecureConfig.exe.
2. Right-click the Materials Control container, and then click **Show key-file properties**.
3. Click the **Security** tab, click **Edit**, click **Add**, and then click **Advanced**.




4. On the Select Users or Groups page, click **Find Now**, select the **Authenticated Users** group, and then click **OK** twice.
5. Click **Authenticated Users**, and then select **Read & Execute**, **Read**, and **Write**.




6. Click **Apply**, click **OK**, and then close the SecureConfig tool.