# !MC5

# Software manual

Version 5.3.33



Bartsch Software

# !MC5 Software Manual



Printed: November 2019

# Introduction

# 1 Introduction

!MC5 is a modular communication software. In addition to OFTP and OFTP2 communication modules the module EDI allows (automated) evaluation and conversion of EDI messages, thus connecting your in-house ERP software. Using Add-Ons !MC5 can be extended with additional features, e.g. the capability to transmit CAD data using the ENGDAT specification.

## 1.1 Modules

### 1.1.1 OFTP

The Module OFTP (Odette File Transfer Protocol) provides direct digital data transmission according recommendations 4914/2 (Version 1, 2) of the VDA and RFC2204 ( ODETTE File Transfer Protocol) of the ODETTE Network Working Group. Data can be transmitted via ISDN or TCP/IP connections.

- Easy installation and operation
- Conformity according recommendation 4914/2 (Version 1) of the VDA
- Conformity according recommendation RFC2204 ( ODETTE File Transfer Protocol) of the ODETTE Network Working Group
- Data transmission via ENX (Communication network of the european automobile industries)

#### 1.1.1.1 Add-On OFTP/ISDN Channel

The Add-On OFTP/ISDN Channel provides one additional channel for simultaneously data transmission by Module OFTP. Incoming and outgoing transmissions can be executed at the same time. For connectivity a CAP 2.0 interface is required.

#### 1.1.1.2 Add-On OFTP/TCP Channel

The Add-On OFTP/TCP Channel provides one additional channel for simultaneously data transmission by Module OFTP. Incoming and outgoing transmissions can be executed at the same time. For connectivity a TCP/IP socket is required.

### 1.1.2 OFTP2

The Module OFTP2 (Odette File Transfer Protocol 2) provides direct digital data transmission according recommendation RFC5024 (ODETTE File Transfer Protocol 2.0) of the ODETTE Network Working Group. Data transmission is encrypted according the Transport Layer Security Protocol (TLS) via TCP/IP.

- Encrypted data transmission according to the Transport Layer Security Protocol (TLS) - TLS 1.2
- Authentification via certificates
- Data compression
- Time-controlled data transmissions, creation of scheduled jobs
- Conformity according recommendation RFC5024 (ODETTE File Transfer Protocol 2.0) of the ODETTE Network Working Group

#### 1.1.2.1 Add-On OFTP2 Channel

The Add-On OFTP2 Channel provides one additional channel for simultaneously data transmission by Module OFTP2. Incoming and outgoing transmissions can be executed at the same time. For connectivity a TCP/IP socket is required.

### 1.1.3 EDI

The Module EDI is the basis for automated processing of incoming and outgoing EDI messages. According to requirements Message Add-Ons EDIFACT, ODETTE, VDA and ANSI ASC X12 can be added individually. Because the Inhouse-Format is freely definable the Module EDI is customizable to every use case. Several automation features guarantee unattended operation. Nevertheless the user is able to monitor and control operation with help of a comfortable workbench.

The Module EDI is accessible from third party programs with the help of simple scripts. To use this feature the Add-On EP Scripting (External Process Scripting) is required.
An integrated editor provides structural ( tree view ) view of EDI messages in readable format. Coded fields will be resolved to readable text by using default code lists. The readable text can be printed out automatically.

- Full Process Automation
- Multiple conversion for each partner
- Scripts for validation of EDI messages prior conversion
- Adhoc Print out of messages and related forms
- Running transmissions via !MC5 or external program
- XML Support (e.g. as Inhouse format)
- Freely defined interfaces for Inhouse-Systems
- Flexible expandable with Add-Ons
- Communication with external transmission software via Add-On EP Scripting

#### 1.1.3.1 Add-On Message EDIFACT

One Add-On Message EDIFACT consists of one standardized EDIFACT-Message for the Module EDI.

- Incoming messages can be automatically identified and converted to a flatfile using pre-defined settings
- Automated print out of incoming messages using the standard description of the United Nations recommendations

#### 1.1.3.2 Add-On Message ODETTE

One Add-On Message ODETTE consists of one standardized ODETTE-Message for the Module EDI.

- Incoming messages can be automatically identified and converted to a flatfile using pre-defined settings
- Automated print out of incoming messages using the standard description of the ODETTE recommendations

#### 1.1.3.3 Add-On Message VDA

One Add-On Message VDA consists of one standardized VDA-Message for the Module EDI.

- Incoming messages can be automatically identified and converted to a flatfile using pre-defined settings
- Automated print out of incoming messages using the standard description of the VDA recommendations

#### 1.1.3.4 Add-On Message X12

One Add-On Message X12 consists of one standardized X12-Message for the Module EDI.

- Incoming messages can be automatically identified and converted to a flatfile using pre-defined settings
- Automated print out of incoming messages using the standard description of the ANSI recommendations

## 1.2 General add-ons

### 1.2.1 Client/Server

The Add-On Client/Server realizes the remote control of !MC5 from any client in a local area network. There are no limits on the amount of clients and users accessing !MC5 remotely.

- Simple installation of the client with included setup program
- Easy operation
- Clients connect to !MC5 via TCP/IP
- Creating outgoing data transfer from any client
- ENGDAT fully supported if Add-On ENGDAT is installed
- Actual order status displayed at the executing client
- If the client is off-line, all messages will be stored. No message will be lost
- Remote control of Add-On EngPart

### 1.2.2 Email

Sends Email Notfications of dispatch and arrival of data transmissions to pre-defined Email addresses. Inhouse transmitted files can be attached to the Email messages.

- Up to 2 Email servers can be configured
- Email messages to several recipients
- Set up Mailing rules for each Odette partner
- Automated Email distribution based on mailing rules
- Attachment quotas
- Create hyperlinks to transmitted files in Emails
- Cancellation of Email delivery by user

### 1.2.3 EngDat

The Add-On ENGDAT (Engineering Data) provides data transmission of CAD/CAM-Files and related information, e.g. Sender, Format, Drawing Number, according recommendation 4951 (VDA). The structured build of ENGDAT-Transmissions provides control and administration of CAD/CAM data. ENGDAT is usable with Modules OFTP and OFTP2.

- Easy installation and opration
- ENGDAT Version 1 to 3 according recommendation 4951 of the VDA

### 1.2.4 EngPart

The Add-On EngPart (Engineering Partner Message) provides an expansion and automation of the ENGDAT capability of the Add-On ENGDAT. It is an easy and comfortable way to edit partner information and creating jobs in ENGDAT-Format. Incoming ENGDAT messages will be identified and managed automatically. Does the partner also have the possibility to use the EngPart messages he can edit information about his company on your system on his own. Opposite you can edit all relevant information about your company directly in the system of your partner. With this method falsification and incidence of information transmission in the ENGDAT messages are nearly impossible. The administration reduces to a minimum.

The Add-On ENGDAT is required for the use of the Add-On EngPart.

- Extension of Add-On ENGDAT
- Administration and maintenance of partner information
- Management of incoming ENGDAT messages
- Administration of company profile
- Automated processes can be changed manually
- Formatted printing of own and incoming data
- Import function

### 1.2.5 EP Scripting

The Add-On EP Scripting (External Process Scripting) provides data exchange of messages of Module EDI with external processes and programs on the system or in the network. Communication will be established via batch files.

- No installation necessary
- Easy implementation of external processes
- Simple creation of batch files

### 1.2.6 HTTP Client

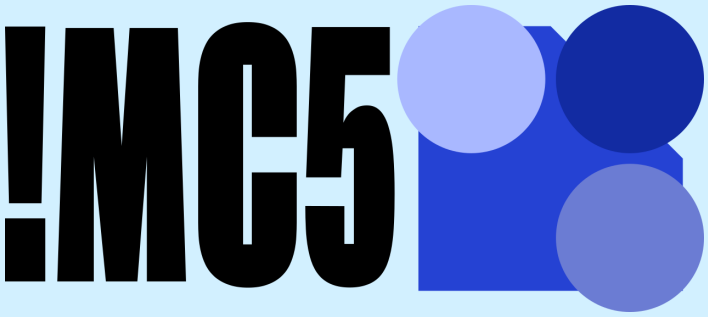
The Add-On HTTP Client provides client access for !MC5 via Web Browser. Modules OFTP and OFTP2 are supported.

- No Installation necessary
- Set up data transfers
- Download received files
- ENGDAT Support if Add-On EngPart is installed

### 1.2.7 Windows Service

Run !MC5 under Windows as a Windows Service without a logged in user.

- Execution of all automated functions
- Non-authorized changes of settings is blocked




# Installation

# 2 Installation

## 2.1 System requirements and required TCP ports

In order to use !MC5 the following system requirements have to be met:

- Windows Vista / Windows 7, 8, 8.1, 10 / Server 2008 - Server 2013
- 50 MB free disc space
- Free disc space for incoming and outgoing data (local and/or network)
- (OFTP/ISDN module only) A working CAP 2.0 installation with support for ISDN data calls ( requires either local or networked ISDN hardware, for virtual environments networked ISDN hardware is recommended )
- Internet connection for license validation

### 2.1.1 Requirements for OFTP2

Following conditions must be met to interchange data with a communication partner via *OFTP2*:

#### Network connection

Both Odette clients must be connected to the same network such as the internet or similar. At least one side must have a fixed IP address or host-name.

#### TLS availability on both sides

Both sides must support the TLS protocol. Connections between *OFTP/TCP* and *OFTP2* channels are not possible. Before ordering the software, contact your communication partner to find out about the required type of channel (*OFTP/ISDN*, *OFTP/TCP* or *OFTP2*).

#### Valid certificates

Both parties should have a valid digital certificate. Depending on the communication partner, the certificates are self-signed or provided via a certification authority. For incoming connections, a certificate must be configured within the address database holding the partner's connection details, for outgoing connections a certificate might be required. (Option *Request certificates from clients* *must be activated!)*

### 2.1.2 Network settings and required ports

#### Overview

| Module/Usage | Port | Protocol | Direction | Required | Proxy possible | Changeable |
|---|---|---|---|---|---|---|
| **!MC5 license validation** | 8920 | TCP | outgoing | yes | no | optional usage of port 80 (selectable during online registration) |
| | License validation uses the domains **oftp2.bartschsoft.com** (primary) and **register.bartschsoft.com** (secundary). | | | | | |
| **Update-Downloads** | 80 | TCP | outgoing | yes | yes | no |
| | Updates werden von der Domain **www.bartschsoft.de** heruntergeladen. | | | | | |
| **TSL-Downloads** | 80 oder 443 | TCP | outgoing | no, but recommended | yes | no (depends on used TSLs) |
| **CRL-Downloads** | 80 oder 443 | TCP | outgoing | no, but recommended | yes | no (dependy on used certificates) |
| **OCSP-Prüfung** | 80 oder 443 | TCP | outgoing | no, but recommended | yes | no (depends on used certificates) |
| **OFTP2, eingehende Verbindungen** | 6619 | TCP | incoming | yes | - | no |
| **OFTP2, ausgehende Verbindungen** | üblicherweise 6619 | TCP | outgoing | yes | no | individual setting per partner possible |
| **OFTP/TCP, eingehende Verbindungen** | 3305 | TCP | incoming | yes | - | no |
| **OFTP/TCP, ausgehende Verbindungen** | üblicherweise 3305 | TCP | outgoing | yes | no | individual setting per partner possible |
| **Add-On Client/Server** | 10000, 10001 | TCP | in- and outgoing | yes | no | yes |
| **Add-On HTTP Client** | 8080 | TCP | incoming | yes | - | yes |

#### !MC5 general

For registration and regular license validation !MC5 **requires** outbound traffic on **port 8920 (TCP)**, or optionally **port 80 (TCP)**, to be unblocked. Without license validation !MC5 its not possible to run !MC5 (short outages or network problems won't cause !MC5 to stop).

To install updates unblocked HTTP connections using port 80 (TCP) are required. Additionally HTTP and/or HTTPS connections using ports 80 or 443 (TCP) are required for TSL (Trusted Service Status List) and CRL (Certificate Revocation List) downloads and OCSP (Online Certificate Status Protocol) checks. If HTTP or HTTPS is used depends on the specific TSL or certificate.

For downloads and certificate validation a proxy can be used, which can be configured in Settings / !MC5 / Proxy. **License validation requires a direct connection!**

## Modul OFTP2

Inbound connections use port 6619 (TCP), the default port for secure OFTP2 connection. This port cannot be changed. Firewalls and port forwarding have to be configured accordingly.

Outbound connection usually also use port 6619 (TCP). For outbound connections this port can be changed per partner.

Additionally the above mentioned ports are required for TSL downloads and certificate validation.

## Modul OFTP/TCP

Inbound connections use port 3305 (TCP), the default port for unencrypted OFTP connections. this port cannot be changed. Firewalls and port forwarding have to be configured accordinly.

Outbound connections usually also use port 3305 (TCP). For outbound connections this port can be changed per partner.

## Add-On Client/Server

The add-on Client/Server by default uses ports 10000 and 10001 (TCP) in- and outbound. The first of the used port can be changed in Client/Server settings. Additionally to the selected port the directlyfollowing port will be used.

## Add-On HTTP Client

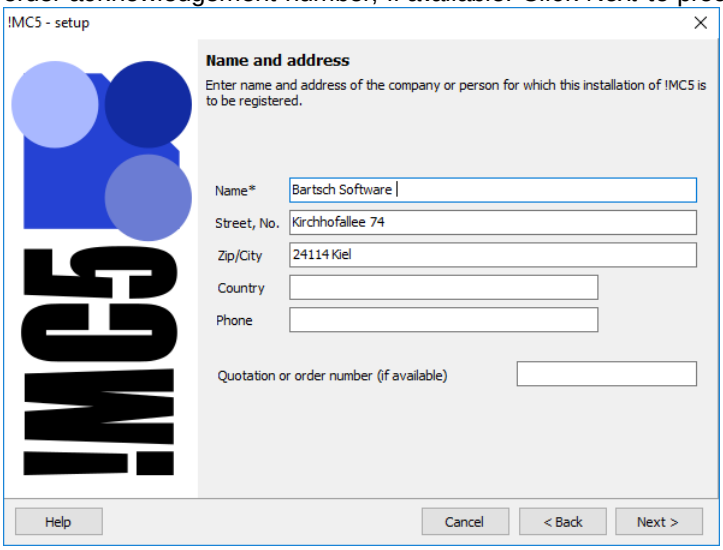
The add-on HTTP Client by default uses port 8080 for inbound traffic. This port can be changed in HTTP Client settings.

## 2.2 Installation and initial setup

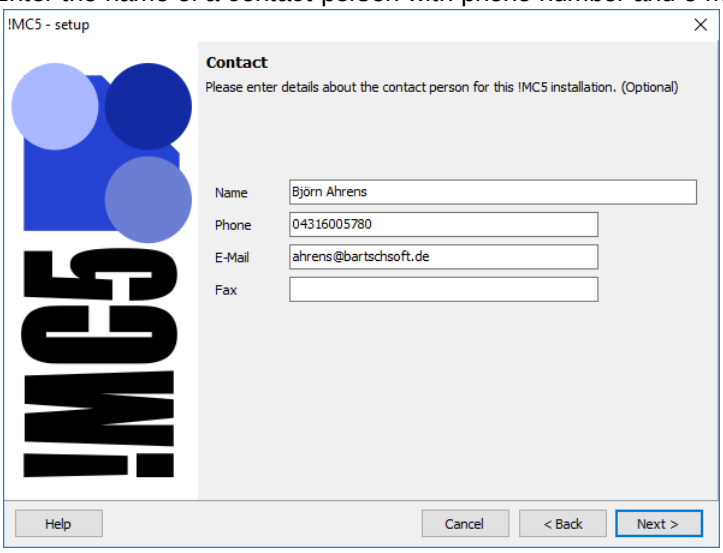
Follow these steps to install !MC5 with at least one ISDN channel.

**1** Execute the installer of !MC5 and follow the instructions as displayed on the screen. Once the installation is finished, start the product registration via Start / Programs / !MC5 / Online Registration. **!MC5 cannot be used unless the registration has been successfully transmitted!**

**2** Please enter name and address of the licensee. Also enter our quotation number or order acknowledgement number, if available. Click *Next* to proceed.



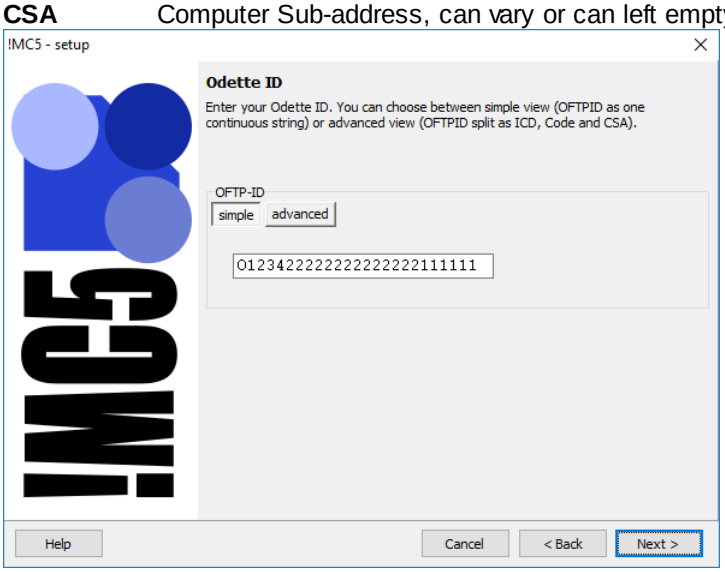

**3** Enter the name of a contact person with phone number and e-mail address.




> **Demo registration: Email address is required!**
> The demo registration requires a valid e-mail address. The license key will be sent to this address. The demo version will not start without the license key.

**4** Now enter your own Odette-ID. It consists of 4 parts:

**„O“** The first character is always an "O" (as in "Odette") and cannot be changed.
**ICD** Code of the organisation which provided this code, e.g. the VDA is represented by "0013",
**Code** Own unique code part of the Odette-ID.
**CSA** Computer Sub-address, can vary or can left empty



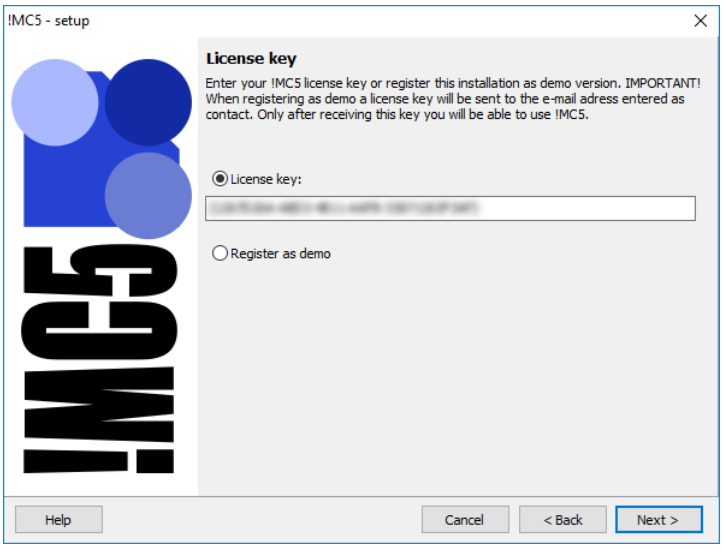

**Restrictions**
Only capital letters are allowed (no local characters), numbers and the following special characters: /-.&()
Spaces are allowed at the end of a field but not between the letters.

If you are installing !MC5 only for testing purposes you might enter any code. But it should be as uniquely as possible. Please avoid codes like "11111111111“ or similar. Your testing partner will get problems when trying to enter such a code in his system.

Use a better readable code instead, e.g.:
ICD: 0815, Code: 004711TEST, CSA stays empty
ICD: 0013, Code: 005555BARTSCH

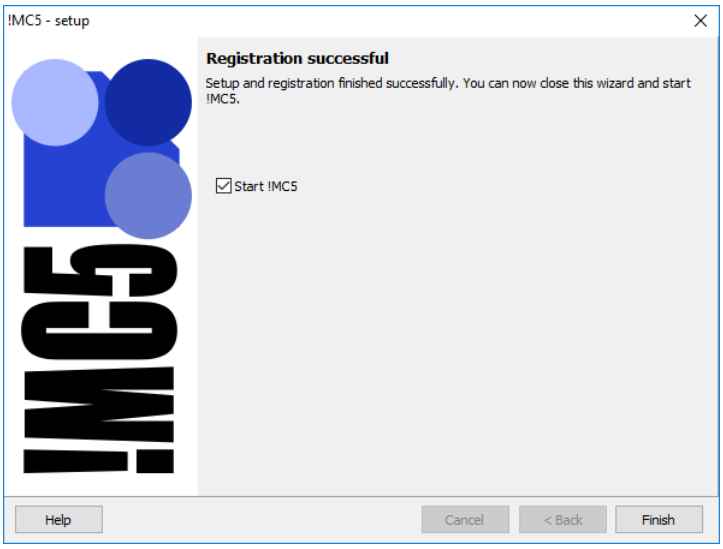
Please do not use these examples but integrate a short name of your own company into the code!

**5** Enter your license key here or select *Register as demo*. A click onto *Next* will start the registration process.




**6** The license server will be contacted and the registration data will be sent. The connection can be aborted by clicking *Cancel*. After successful registration click *Next* to finish the setup.

**7** After finishing the registration process successfully !MC5 can be started. The registration of the demo version requires a license key which will be sent by E-Mail. This key has to be entered when !MC5 is first started.




**Configuration of OFTP2**

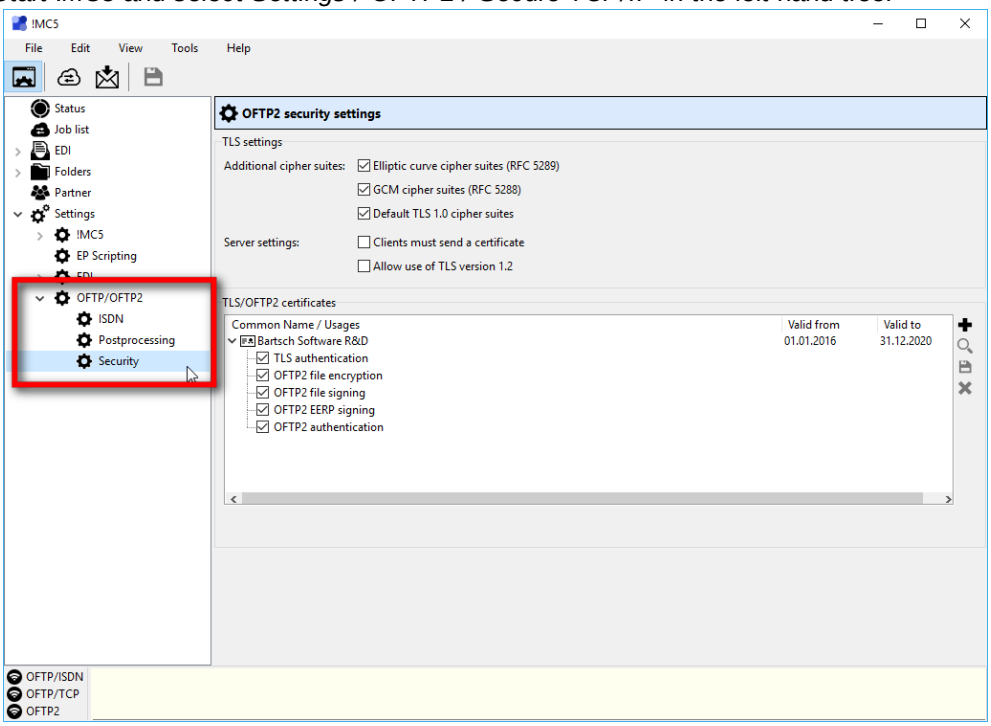
To use the module OFTP2 additional setup steps are required. Please consult the chapter Configuring OFTP2.

### 2.2.1 Configuring OFTP2

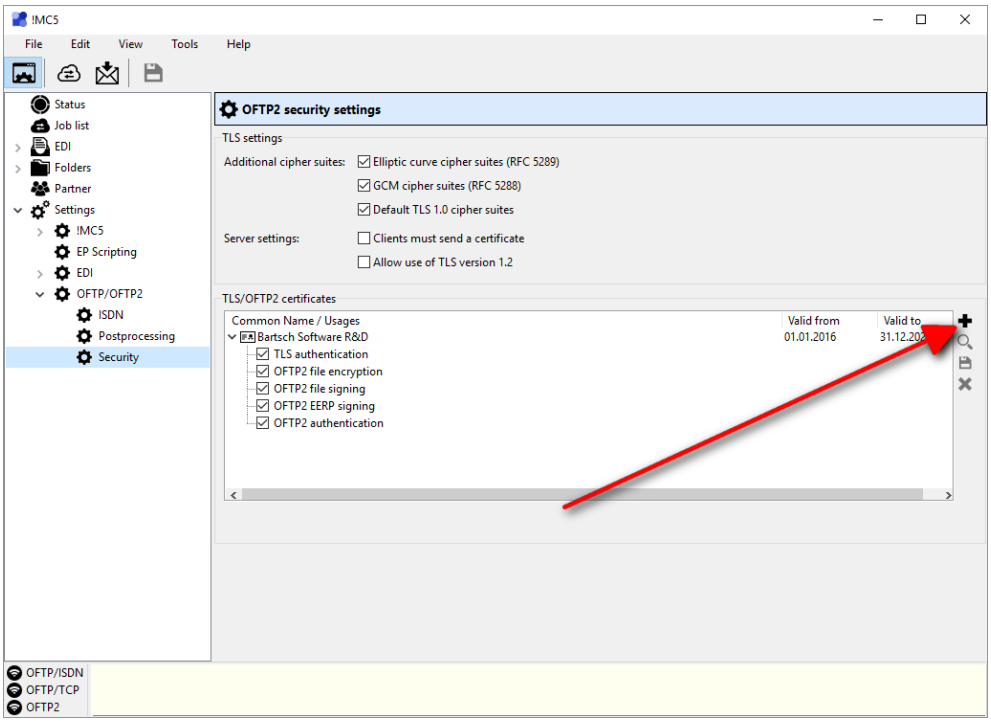
In order to use *OFTP2* channels there must be at least one certificate assigned to the TLS-connection. Whenever a connection over *OFTP2* is established the type of certificate will be negotiated. There are two types allowed: RSA and DSA encryption. Both sides must support the selected type of certificate. RSA is the more commonly used mode of encryption in certificates.

To create an own certificate please proceed as follows:

**1** Start !MC5 and select *Settings / OFTP2 / Secure TCP/IP* in the left hand tree.

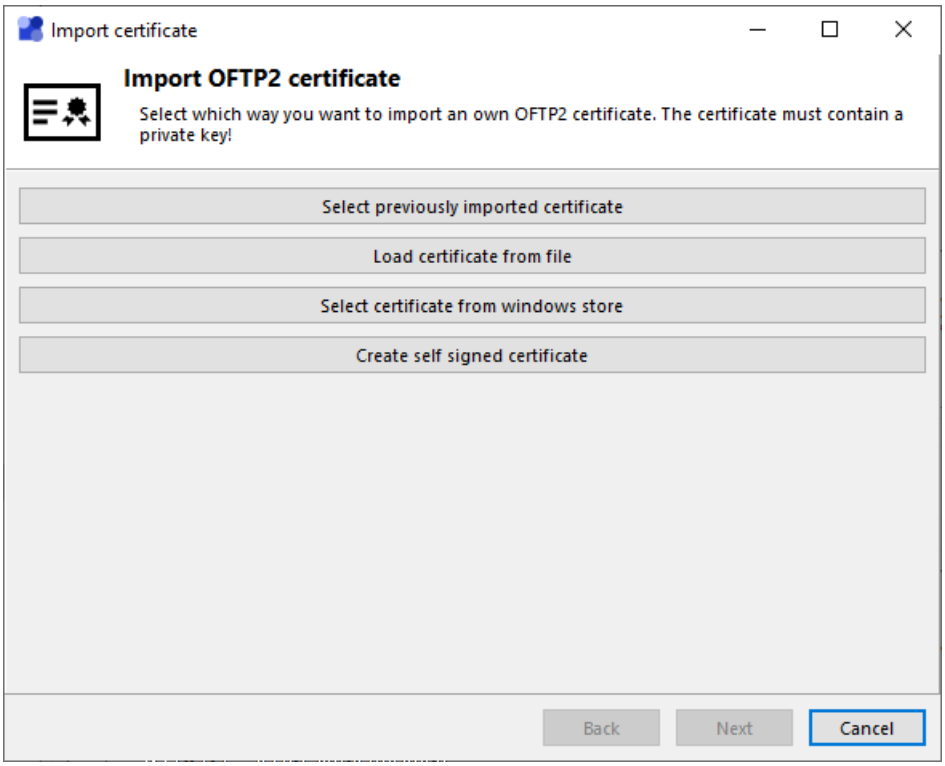



**2** Click the button *Add certificate*.

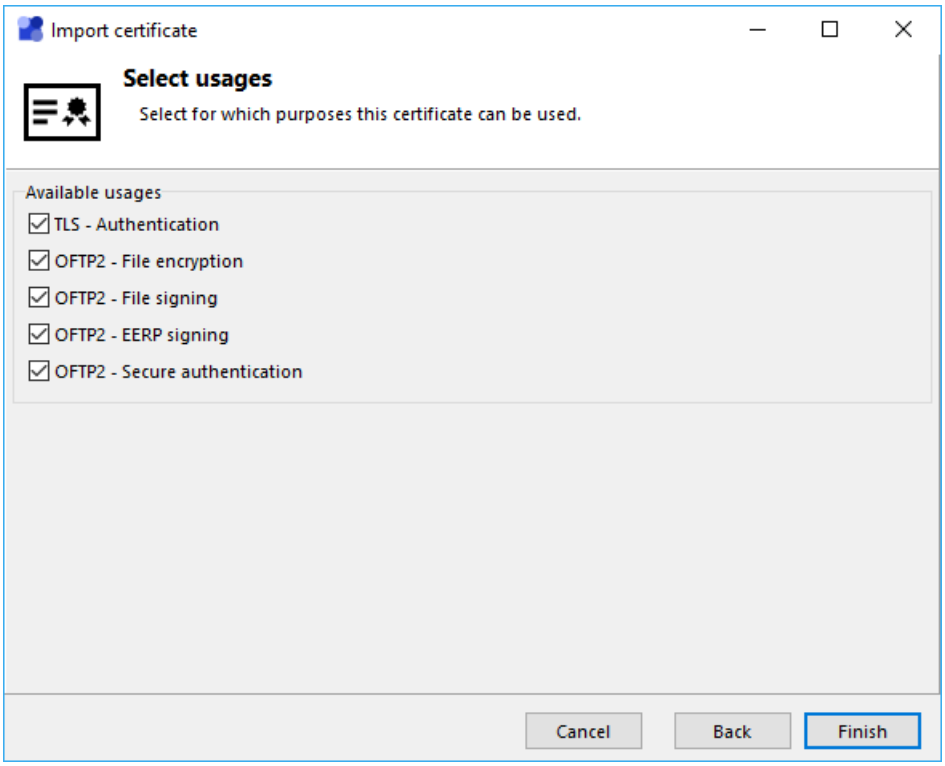


**3** If you already have got a valid certificate please choose *Import certificate from file* or *Select certificate from certificate store*. !MC5 uses the personal certificate store of Windows, which is different for every Windows user, so its contents depend on the currently logged in user. You can also use *Create self-signed certificate*, but be aware that in order to use a self signed certificate, your partner(s) must agree to that. Select the appropriate import method and follow the instructions of the import assistant.

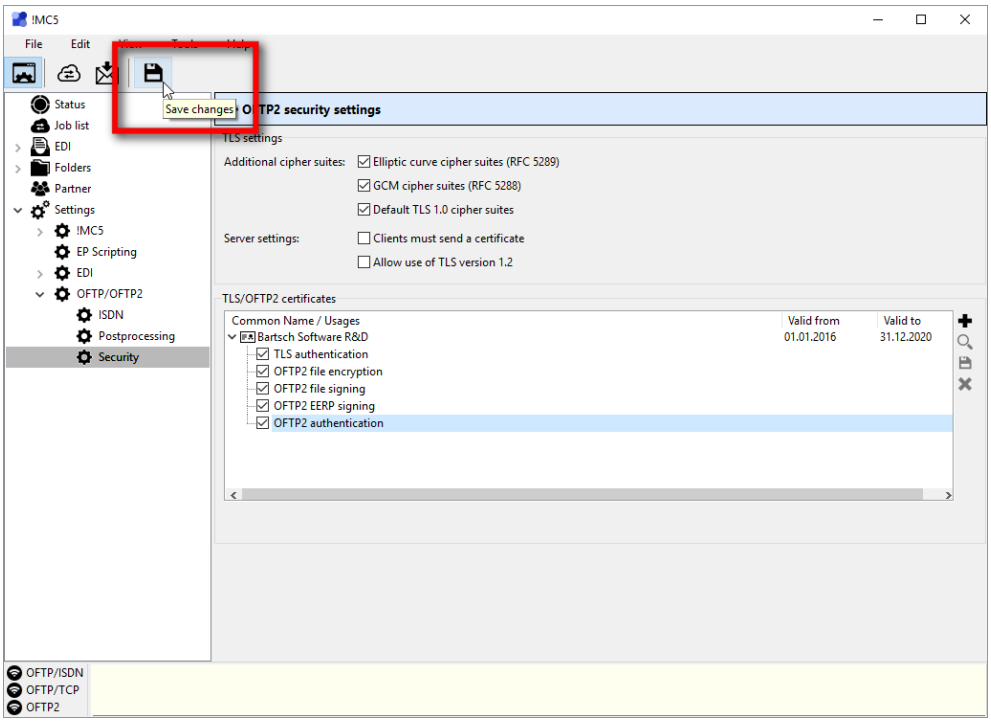
> **Certificates must include private key**
> Own certificates always have to include the private key. When importing from file, the certificate file has to have the extension *.pfx* and while importing you will be asked for the password for that file. If you have a certificate issued by the Odette organization (requested at https://www.odettesecure.com) Odette offers instructions on how to create a pfx file using the downloaded certificates: https://www.odette.org/repository/odette-ca-help.pdf




**4** After selecting the certificate select the usages for the selected certificate and then close the assistant by clicking on If you want to use one certificate for all usages select all options or import further certificates for different usages.




**4** Save all changes by clicking on *Save changes*. !MC5 is now ready to establish OFTP2 connections.



### 2.2.2 Installing Windows Service

(*Windows Service add-on only*)

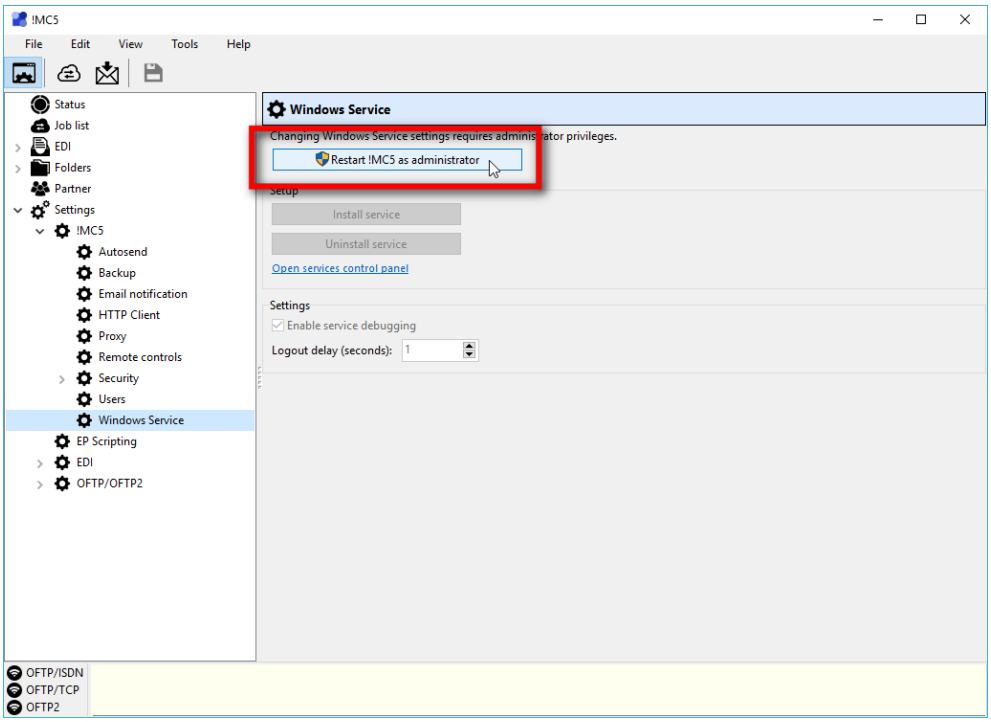
The add-on *Windows Service* allwos to run !MC5 as background process without the need for a logged in windows user. While !MC5 runs as background service the !MC5 GUI can not be used. Receiving data any automated functions are unaffected by this. Starting !MC5 while the *Windows Service* is running results in a prompt to pause the service. It will get restarted when the !MC5 GUI is closed.

The *Windows Service* starts !MC5 as background task using a special service mode. It also permanently monitors if an instance of !MC5 is running. If !MC5 gets closed, the service will restart it immediately. When starting the !MC5 GUI the service gets paused and as soon as the GUI is closed, monitoring is resumed. If the GUI doesn't close properly, the *Windows Service* will restart !MC5 as background task after ten minutes of inactivity.

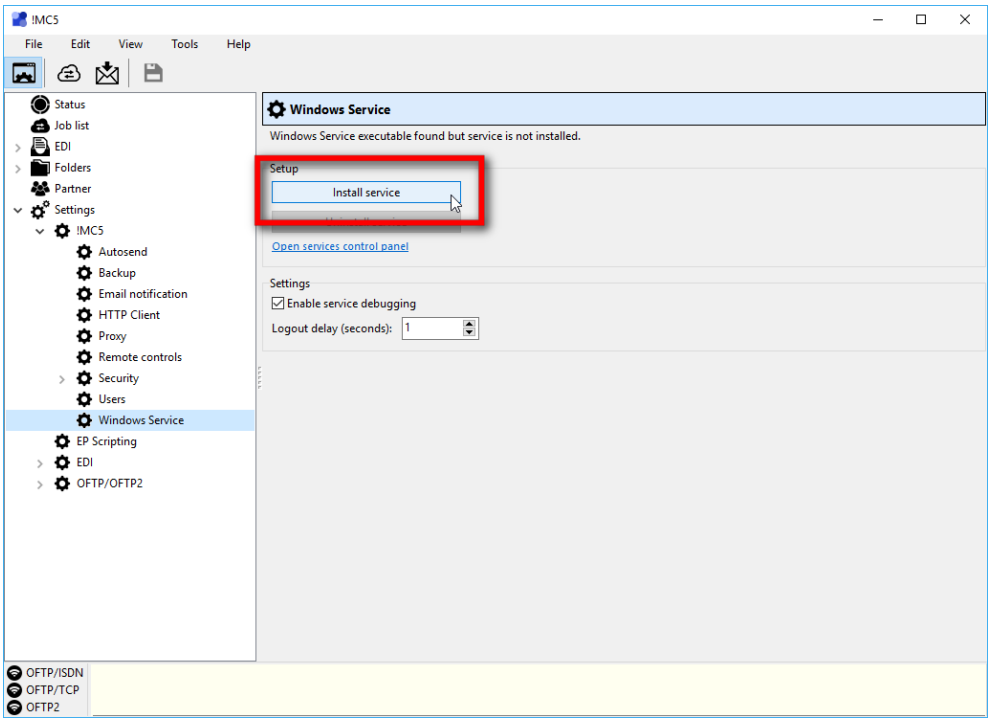
If the *Windows Service* is licensed proceed as follows to install and run the service:

**1** If necessary start !MC5 and navigate in the left hand tree view to *Settings / !MC5* and select the entry *Windows Service*.

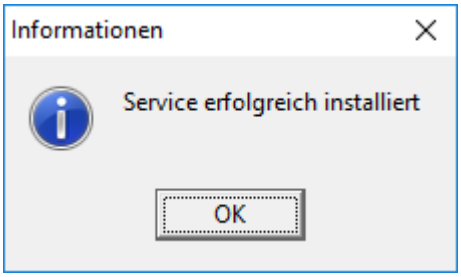
**2** To configure the Windows Service !MC5 has to be started with windows administrator privileges. If elevated privileges aren't available !MC5 can be restarted as administrator using the button *Restart !MC5 as administrator*.




**3** To install the Windows Service click the button *Install service*.




**4** Successful installation of the service should get confirmed.



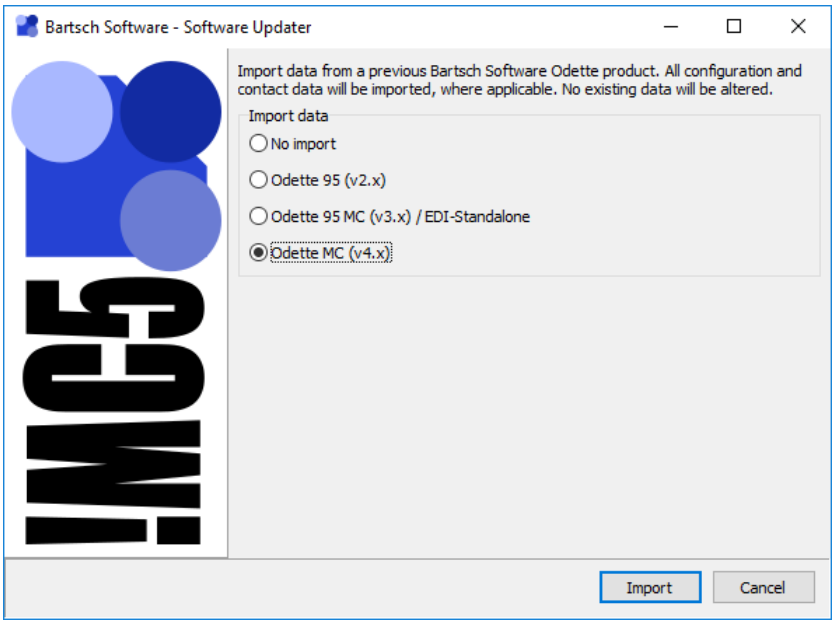

**5** If the installation was successful, the *Windows Service* gets started automatically when !MC5 is closed.

## 2.3 Upgrade from previous Bartsch Software products

### Upgrade on the same computer

An upgrade of Odette 95 (version 2.x), Odette 95 MC (version 3.x), EDI-Standalone or Odette MC (Version 4.x) requires the complete setup of !MC5 (*MC5_e.exe).* The setup will install !MC5. The last page of the installer will offer to import data from previous Bartsch Software products.

The import tool will copy all available data without changing the old installation. The tool can be found in the program folder of !MC5 as *UpdateMC.exe*. It can be used at any time.




### Upgrade on a new computer

If you plan to install the upgrade on a new computer you need to have access to the old installation folders to import the data. If in doubt, copy the existing installation from the old system first.

For Odette 95 / 2K / 95 MC the default paths are "*C:\Program Files\Odette95*" (Version 2.x) or "*C:\Program Files\OdetteMC*" (Version 3.x).

An upgrade from Odette MC (version 4.x) requires access to the programs data folders. These are located under *C:\ProgramData\Bartsch Software\Odette MC* (*C:\Documents and Settings\All Users\AppData\Bartsch Software\Odette MC* for Windows version prior to Windows Vista).

Now can do the upgrade as described above.

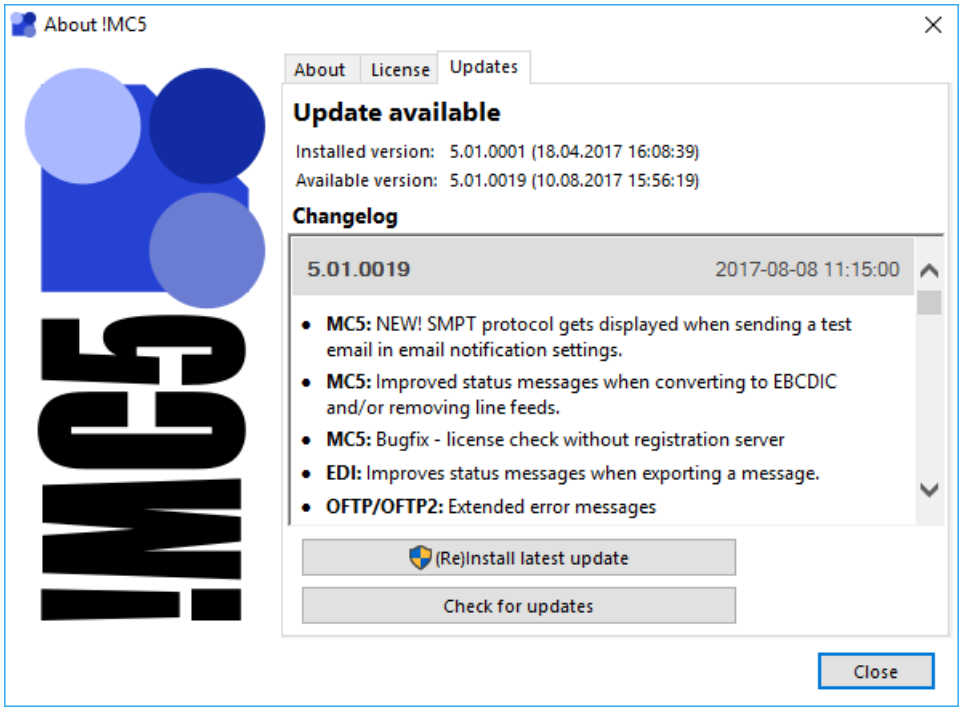
**Special attention with the EDI module**

If the EDI module is used with the existing installation, upgrade and data import should be done on the old computer. All versions prior to 4.0 store counter variables in the Windows registry. Since version 4.0 these are store in a file. The update will recognize the variables in the registry and will copy them into the file.

Meanwhile !MC5 can be installed on the new computer. After that the data folder of !MC5 can be copied from the old computer. It is located in "*C:\ProgramData\Bartsch Software*" or "*C:\Documents and Settings\All Users\AppData\Bartsch Software*". All existing files must be overwritten.

Is an update on the old machine impossible all counters must be set manually in the automatic settings of the EDI module.

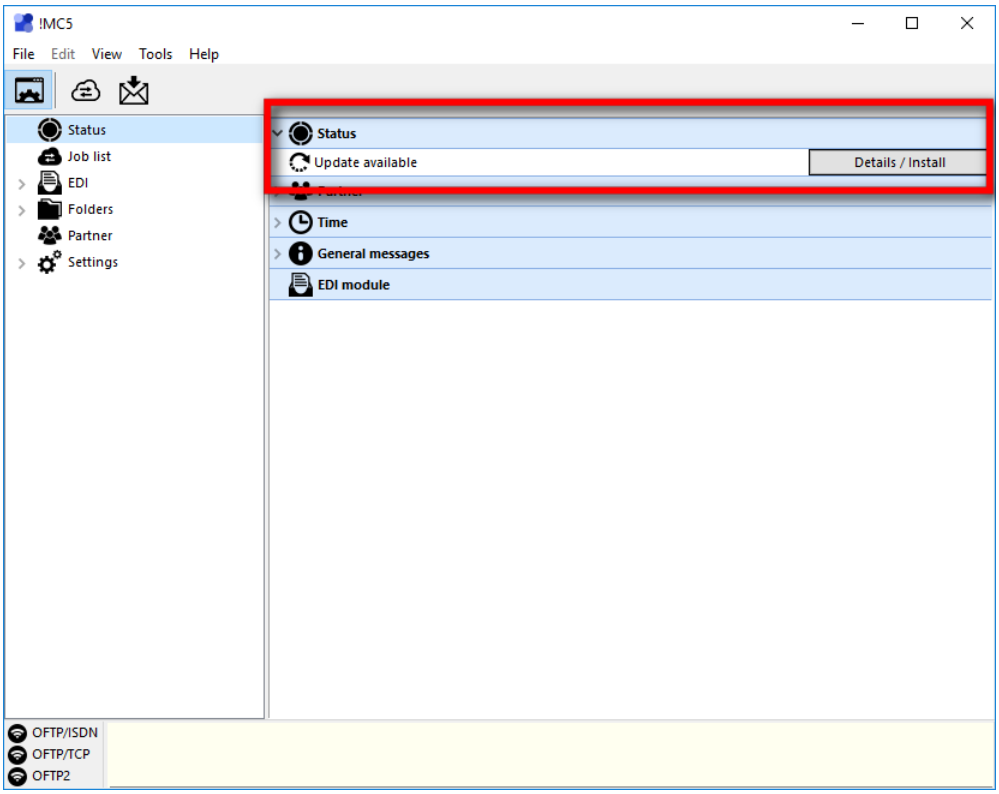
## 2.4 Product updates




Information about available update can be found in !MC5s about dialog (available in the main menu via *Help / About*). At least once per week !MC5 checks automatically for new updates. To manually check for updates use the button *Check for new updates* in the about window. Using the email notifications it is also possible to notify about new updates by email.

If a newer version, than the currently installed one, is available version number and release date of the new version are displayed. Changes in the new version are displayed under *Changelog*.To install the available update click *Install update*. Administrative rights are required to install any update and will be requested if necessary. The installation will close !MC5 and restart it, after the successful update.

**Backup before updates**
Prior to every update !MC5 automatically creates a configuration and data backup. In case any problem occur after the update this backup can be restores using the !MC5 tools. To be sure you can manually create a backup using the function *Backup now* in the *Backup settings* of !MC5.

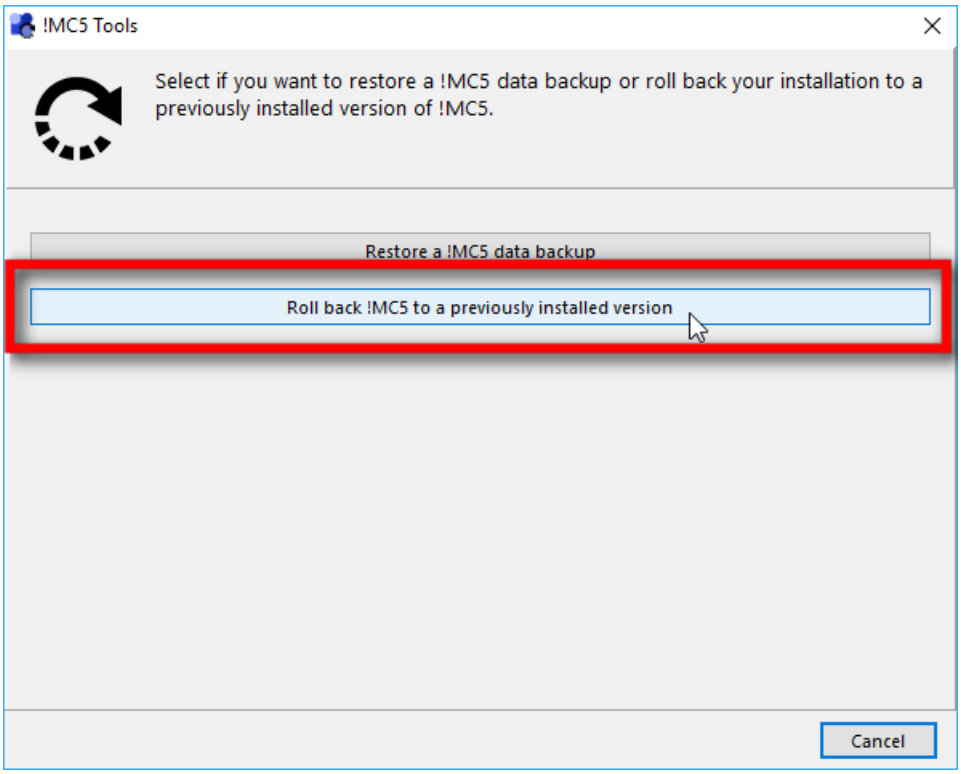



**Availability of newer versions of your !MC5 product will be displayed in the status view.**

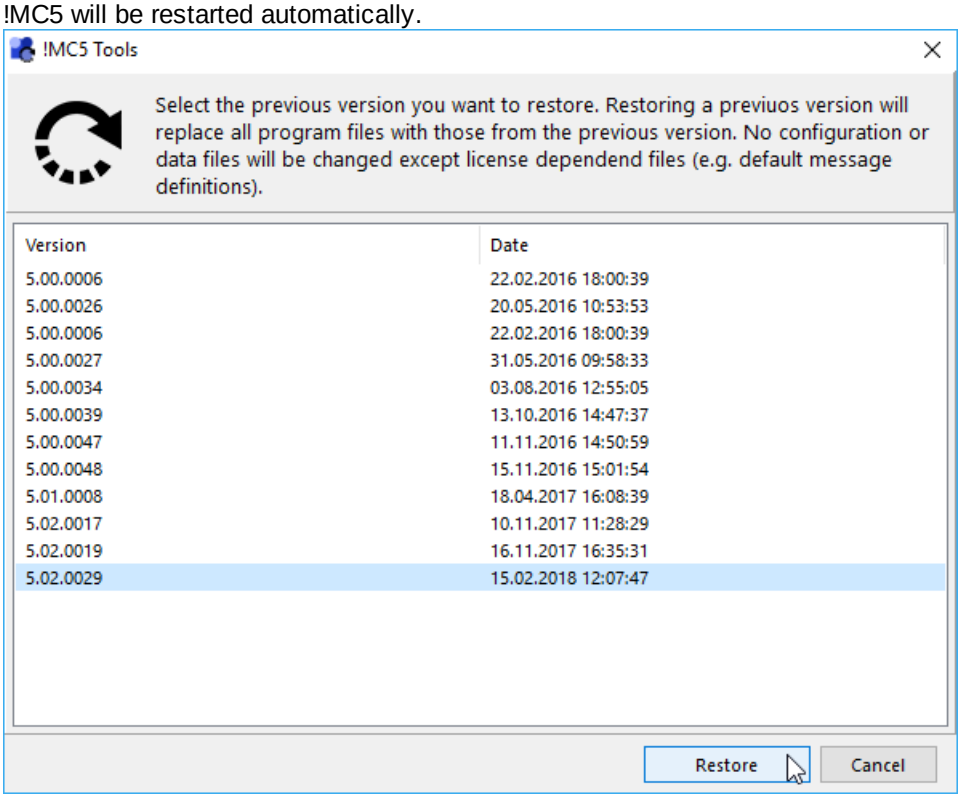
### 2.4.1 Restoring previous versions

Should an update case any issues you can restore any previously installed version of !MC5.

1. Start the !MC5 Tools using the corresponding entry in the windows start menu or via File / Open !MC5 Tools the main menu of !MC5. You can also start the file *mcre-starter.exe* found in the !MC5 installation folder, typically *C:\Program Files(x86)\MC5*.
2. Click the button *Roll back !MC5 to a previously installed version*.




**3** Select the version you want to rollback to and then click *Restore*. The currently installed version will **not** be displayed in the list. After restoring the selected version !MC5 will be restarted automatically.



## 2.5 License management

The registration of !MC5 uses a unique license key. The registration process binds that key to the computer from which it was initiated. The license key cannot be used on any other machine, regardless if it is a real computer or a virtual machine.

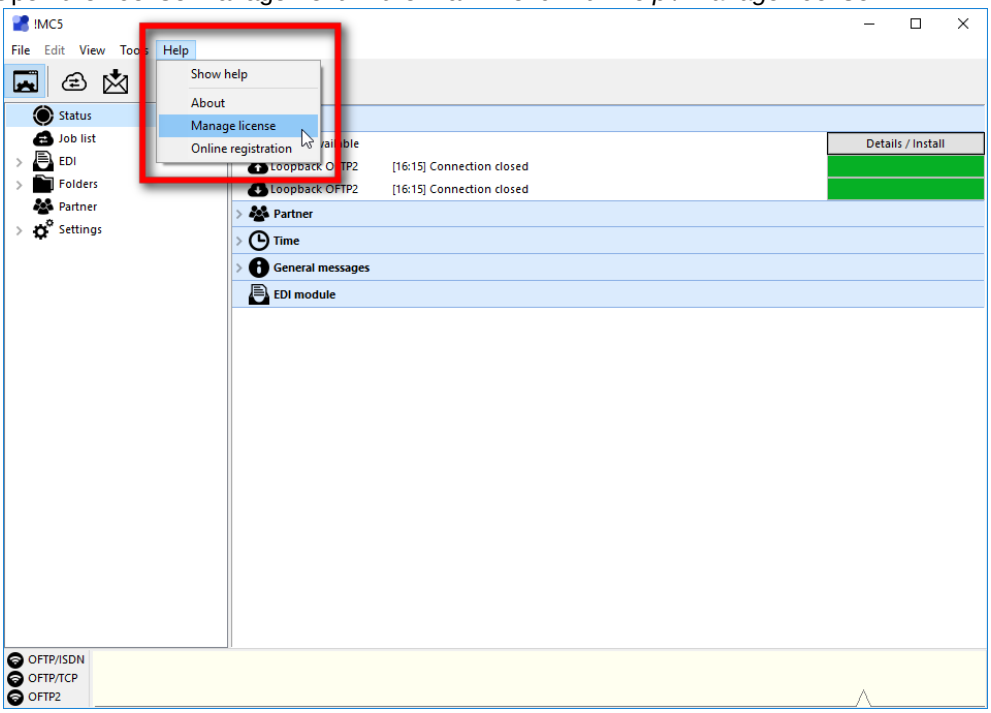
**Before installing !MC5 on a new computer the license must be deactivated on the old one first.** The new installation can only be started when the old one is deactivated.

### 2.5.1 Deactivate license

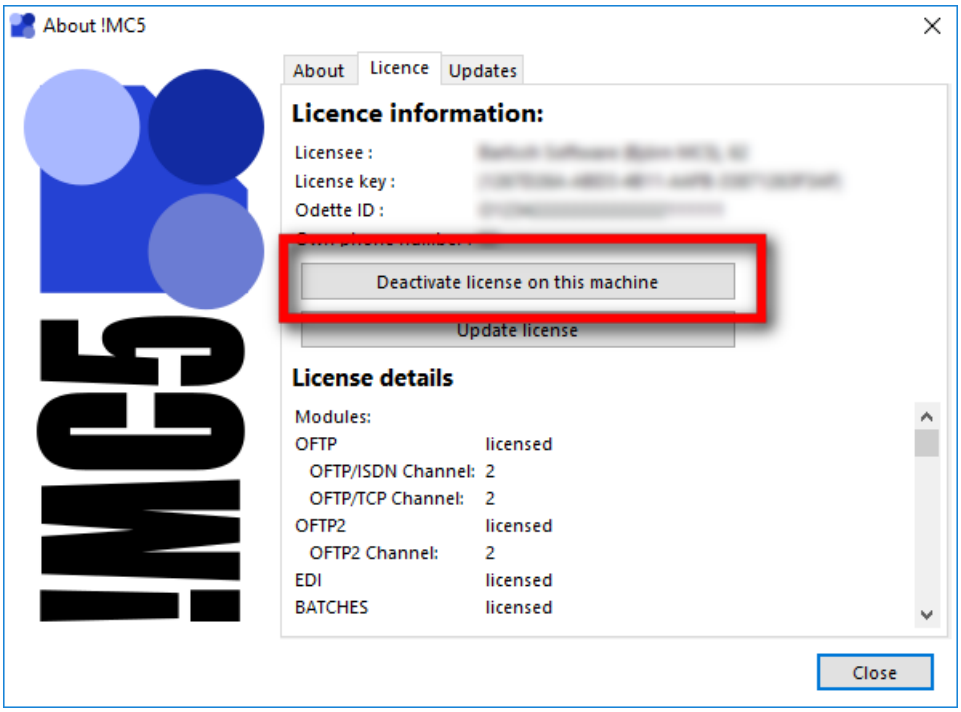
To deactivate the license of an active system please proceed as follows:

**1** Start !MC5.

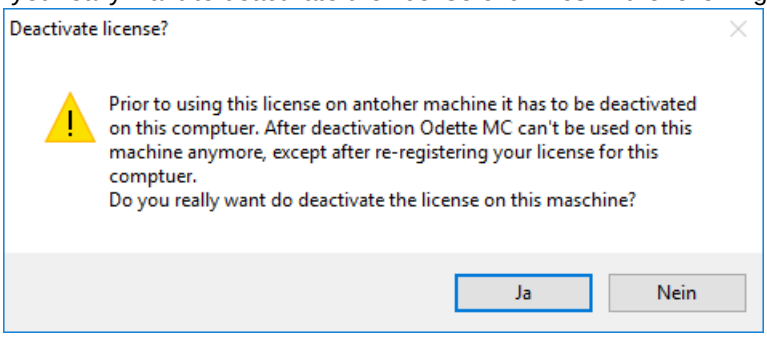
**2** Open the license management in the main menu with *Help / Manage license*..




**3** Click the button *Deactivate license on this machine*.




**4** If you really want to deactivate the license click *Yes* in the following window.



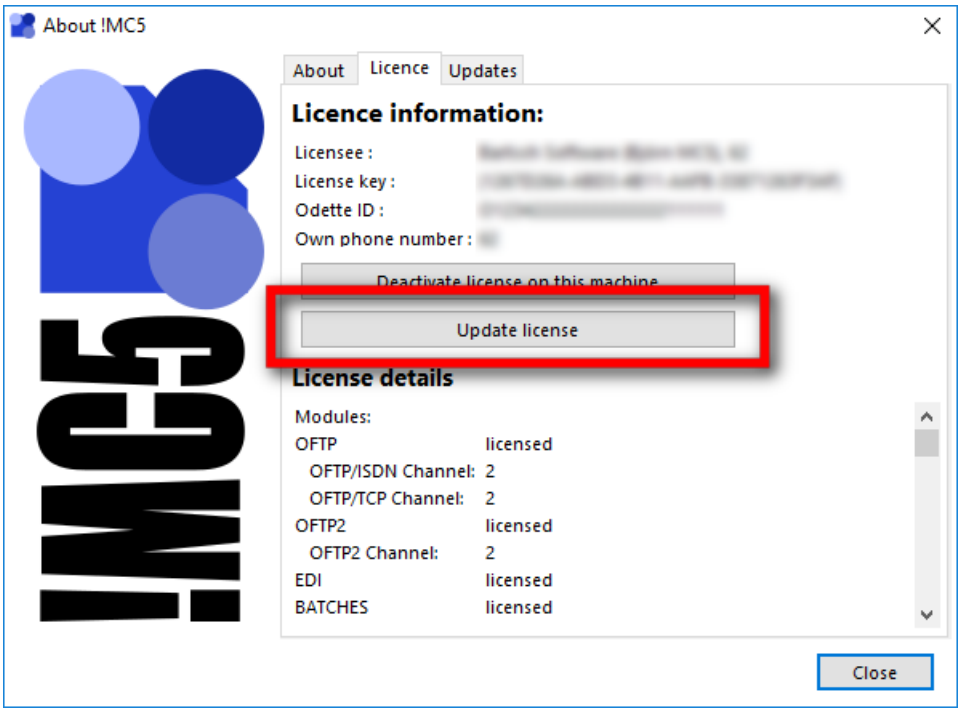

**5** A message box will state that the license was deactivated. Close !MC5 now and register your new installation.

### 2.5.2 Update license

A license update can be necessary when new modules were purchased. They only will be available when the license is updated.

**1** Open the license management in the main menu with *Help / Manage license*.

**2** Click *Update license*.

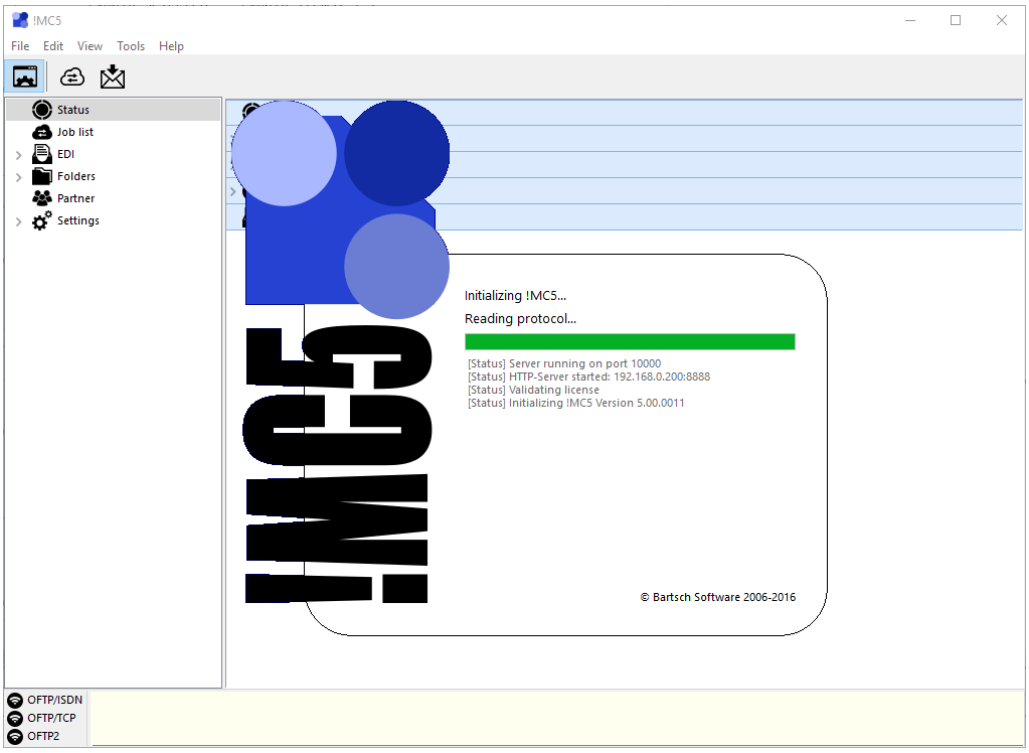



**3** After a new license was received restart !MC5 to initialize the new modules.

# Basic usage

# 3 Basic usage

## 3.1 Main window




The main windows of !MC5 is divided into four sections. The upper part contains the main menu and a tool bar for quick access to the most used functions. The lower Part shows the current usage of the available channels. Via the left hand navigation tree the the various functions of !MC5 are available, including the program settings. The main part of the !MC5 window, to the right side of the tree, show the selected section.

The following functions are always available, regardless which section is selected in the navigation tree:

### Tool bar

Enable/disable admin view.

**Create New Job** - (*OFTP, OTFP2 Add-Ons only*) Opens the wizard for the creation of a new sending job.

**Import EDI message** *(EDI Add-On only)* - Import of an EDI message into !MC5.

### Main menu

- **File**
  ***New Job*** - (*OFTP, OTFP2 modules only*) Opens the wizard for the creation of a new sending job.
  ***Import EDI message*** *(EDI Add-On only)* - Import of an EDI message into !MC5.
  ***Import Data from Odette 95/MC*** - Import data and configuration from a previous

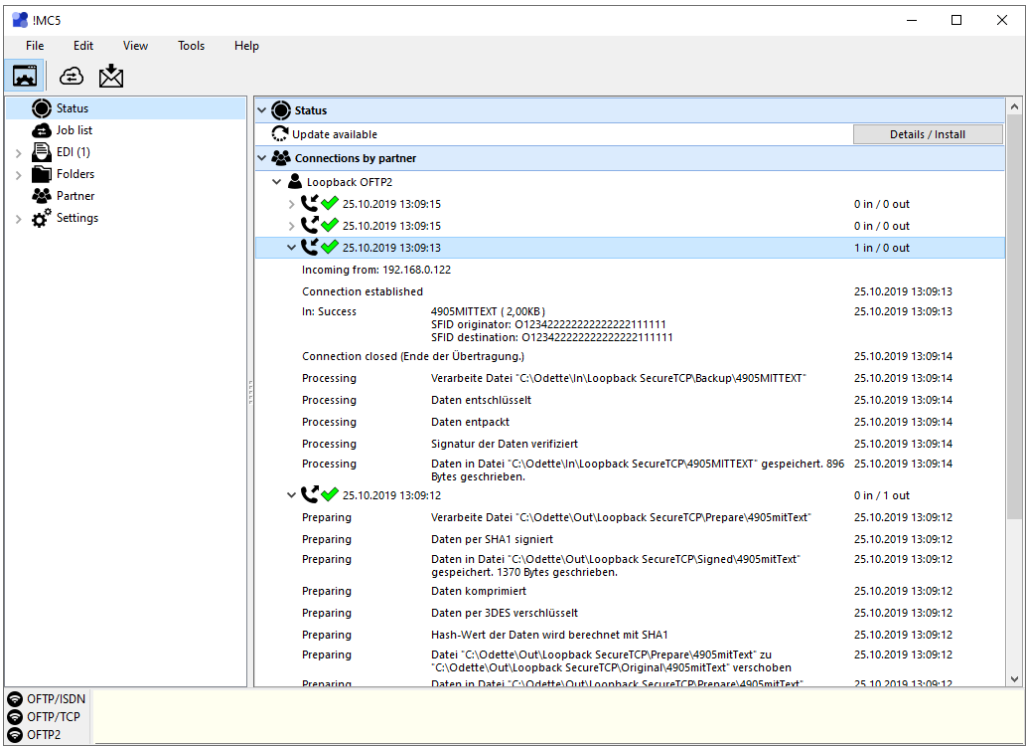
product from Bartsch Software.
***Open !MC5 Tools*** - Open the !MC5 Tools. Using the !MC5 Tools you can restore (automatically created) backups or perform a rollback to a previously installed version of !MC5.
***Close*** - Close !MC5.

- **View**
  ***EngPart ...*** - *(EngPart Add-On only)* Shows the main window of the EngPart Add-On.
  ***Protocol analyser*** - Starts the external *Protocol Analyser.*
  ***Show Logfiles*** - Opens the folder containing the log files of !MC5 in Windows Explorer.

- **Tools**
  ***File tools*** *(OFTP2 module only)* - Using the file tools you can apply OFTP2 features (encryption, compression, signature) directly to a file. If more than one feature is applied to a file, the steps have to be applied in the given order.
  ***1 . Decrypt file*** - Decrypt an encrypted file. Decryption uses all certificates with the usage *OFTP2 - File encryption* specified in Settings / OFTP2 / Security.
  ***2. Decompress file*** - Decompresses a compressed file.
  ***3. Verify file signature*** - Test if the signature of a signed file is valid. You have to select the partner who has signed the file. !MC5 tries to verify the signature using alls certificates with the usage *OFTP2 - File signing* specified for the selected partner.
  ***Automatic file import*** - *(EDI Addon only)* - Shows the settings of the automatic file import.
  ***EDI-Convert Manager*** *(EDI Addon only)* - Starts the EDI-Convert Manager.
  ***Package Manager*** - Shows all installed packages.
  ***Revoke and replace certificate*** - Using this you can revoke a compromised certificate using the OFTP2 automatic certificate exchange and replace it with a new, valid certificate.

- **Help**
  ***Open software manual*** - Open !MC5 software manual. An installed PDF viewer is required.
  ***About*** - Displays information the version of !MC5.
  ***Check for updates*** - View information about and install the latest available !MC5 update.
  ***Manage license*** - Shows details about your license and allows to deactivate the license for the current system in order to install it on another computer.
  ***Online registration*** - Closes !MC5 and starts the online registration.
  ***Show contact sheet*** - Shows a simple contact sheet which you can print or save and send to your partners.
  ***Remote support download*** - Open a webpage to download the remote support tool for support via TeamViewer.

### 3.1.1 Status



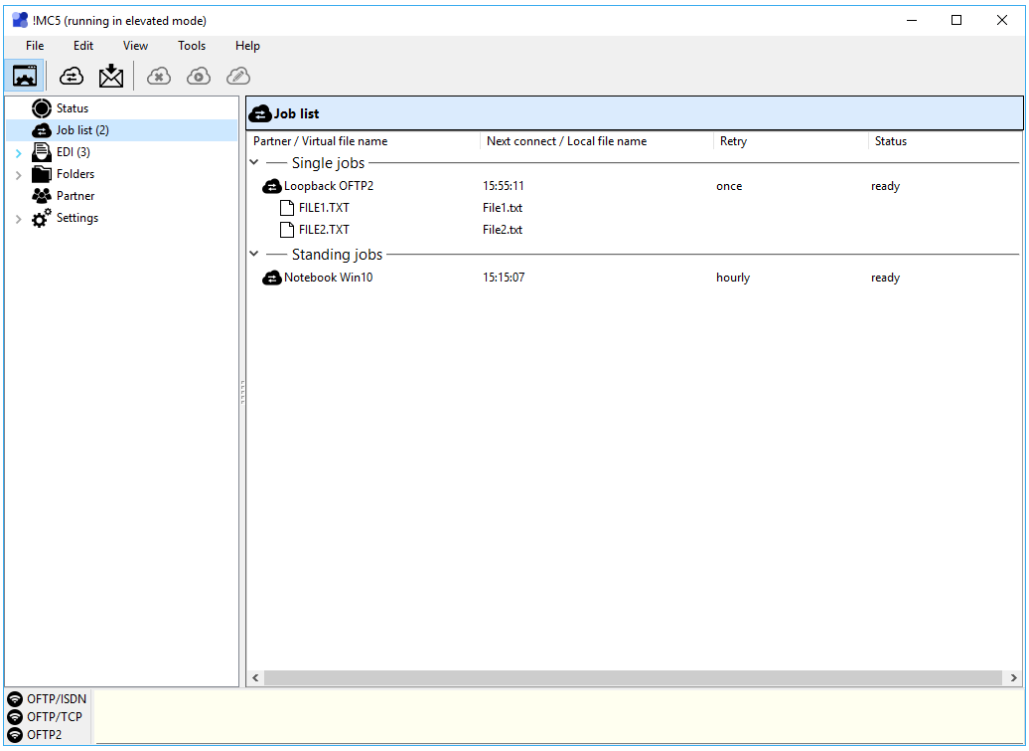

The status page in the main windows shows the current transfer status of all open connections and the protocol of previous transmissions. The status tree will keep these protocols for 14 days by default. This setting can be changed in the !MC5 settings. The Status consists of the following sections:

- **Current connections**
  This part lists all open or currently closed connections.
- **Partner**
  The protocols of previous connections are listed here, sorted by communication partner.
- **Time**
  This part also contains the protocols. Here the connections are sorted by the time they were initially opened.
- **General Messages**
  This section contains general messages and messages concerning data transmissions which are not associated with one partner.
- **EDI** *(EDI Add-On only)*
  Shows all messages produced by the automatic mode of the EDI Add-On.

### 3.1.2 Job list

*(OFTP and OFTP2 modules only)*

This section shows all pending jobs and their current status.

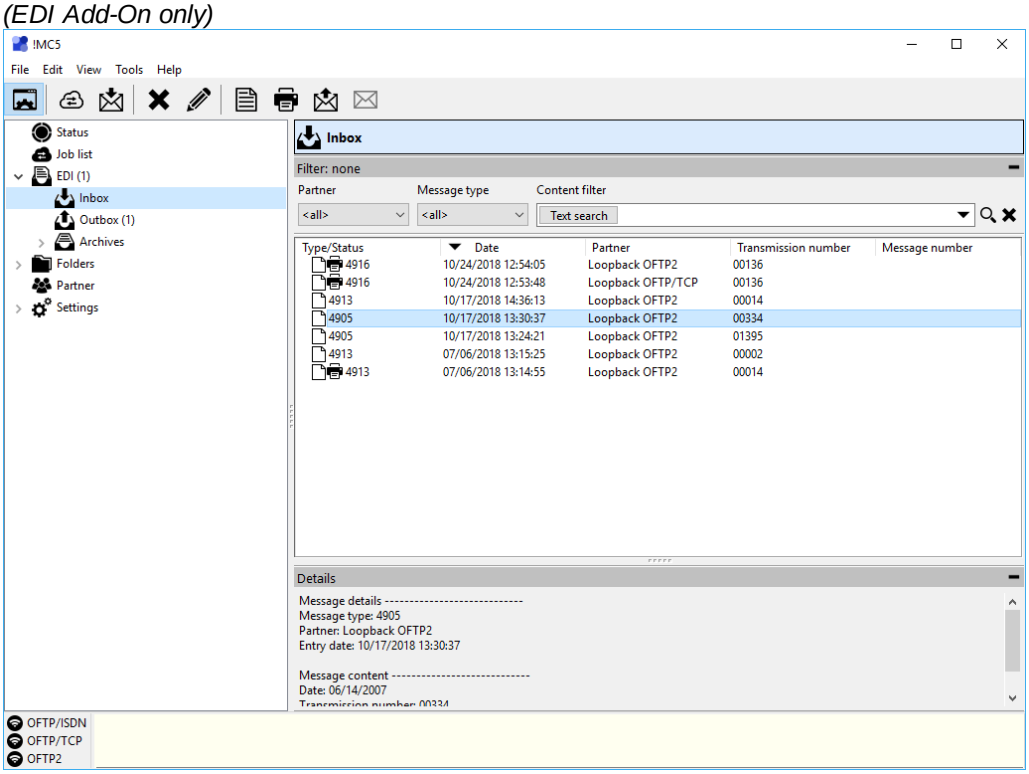



The following functions are available:

- **New job** - Create a new job for a specific partner.
- **Edit job** - Edit a pending job. Running jobs can't be edited.
- **Delete job** - Delete a pending job. If you try to delete a running job a warning will be displayed. Files associated with a job can be deleted, moved or kept for a later job.
- **Execute job** - Execute a pending job immediately. The job will be started as soon as a matching channel becomes available.

### 3.1.3 EDI

*(EDI Add-On only)*




The page EDI messages gives an overview of recently sent (Outbox) and received (Inbox) messages. These entries will be deleted after a given period of time. The databases still contain all EDI messages.

The following options for handling EDI messages are available:

**Delete entry** - deletes the currently marked entry (not available in database view).

**Show message** - Opens a quick-view for the marked message.

**Edit message** - Opens the message in an editor window. The message contents will be given in readable text-format. This text can be edited, printed and saved. This will **not** change the message itself in the database.

**Print message** - Prints the marked EDI message. Depending on message type there might be message specific options available.

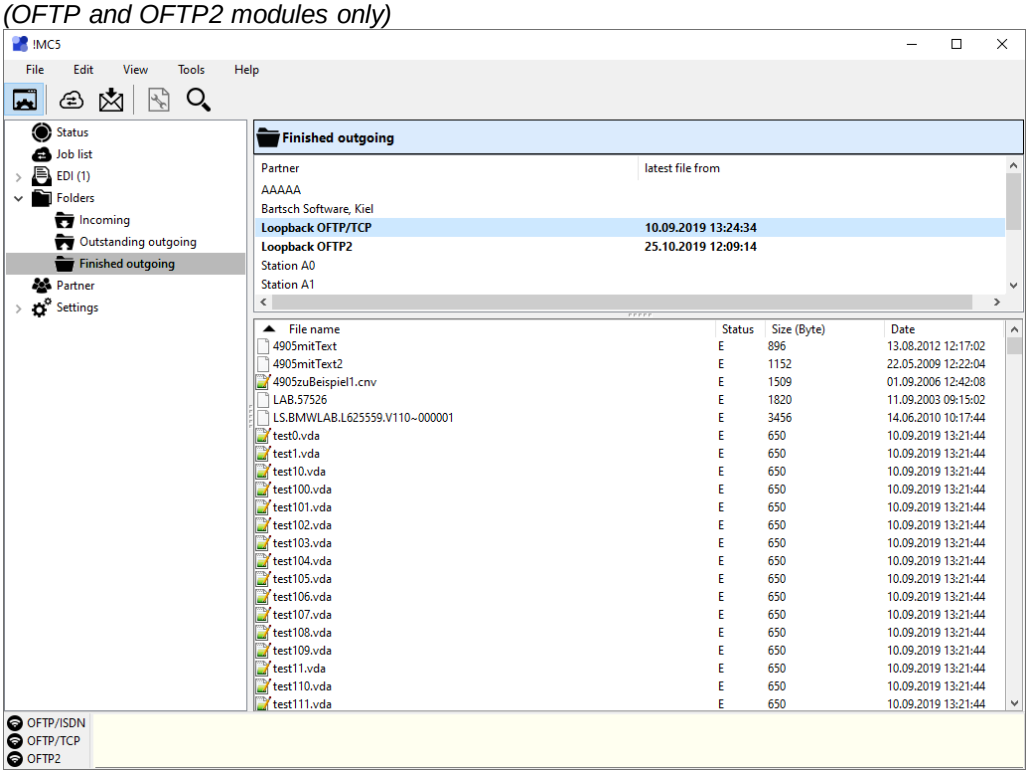
**Send message** - This option initiates a sending job. The message will be sent to the partner indicated in the marked list entry (not available in database view).

**Export message** - The selected message will be exported to hard-disk. The message can be converted during export process or it can be left unchanged.

The messages shown in database view can be copied to the Inbox or Outbox. Right-click the message can choose the option *Move entry to Inbox* or *Move entry to outbox*.

### 3.1.4 Folders

*(OFTP and OFTP2 modules only)*




The page Folders offers a quick overview of all folders for incoming and outgoing files. There is one folder pair for each partner account. The folder for outgoing files has got the two sub folder *Backup* and *Sent*, additionally. !MC5 moves all successfully sent files here.

The view can be switched by three options on the left hand *Incoming*, *Outstanding outgoing* and *Finished outgoing*. Then select a partner account for which the folder contents is to be shown. Partner accounts with non-empty folders are shown in bold letters. The time stamp of the newest file is also listed.

**File status shown in directory listing**

The column Status displays different information depending the type of displayed directory:

**E** (*Finished outgoing*) - The EERP for this file has been received.

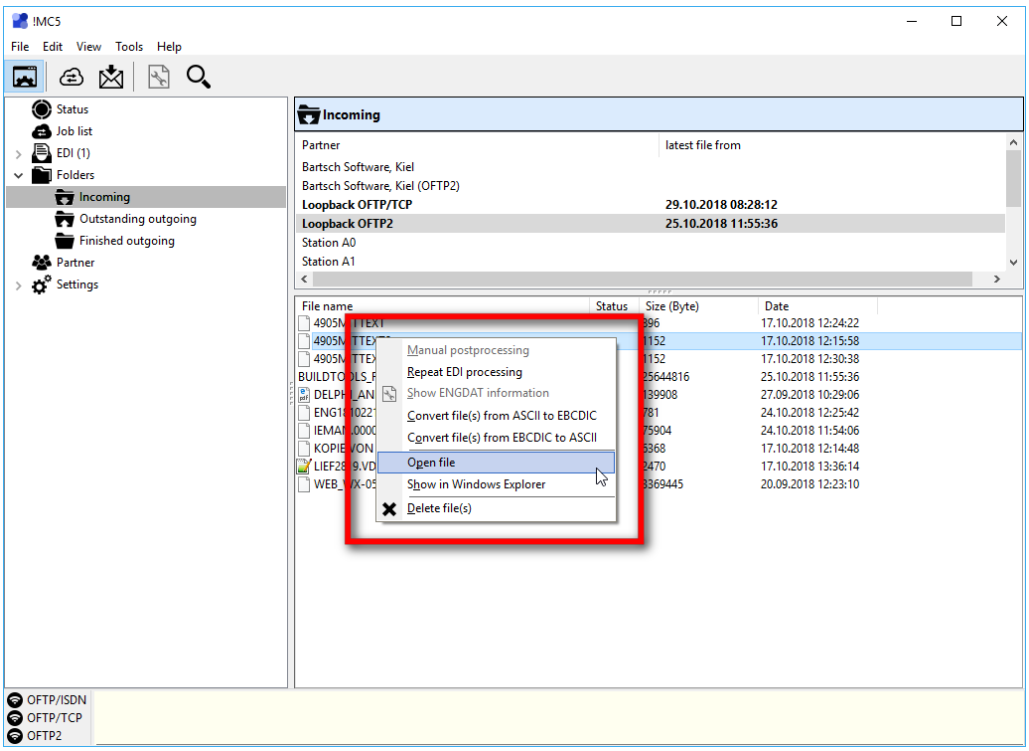
***** (*Incoming*) - Postprocessing for this file (e.g. character set conversion, decryption, etc.) hasn't been executed for this file (yet).

The following additional functions are shown in the tool bar:

**Analyze ENGDAT** - (ENGDAT Add-On only) Are ENGDAT files available in the current folder, this function will be enabled. It can be used to display the ENGDAT information in readable format.

**Show only directories containing files** - with this option activated only partners with folders containing files are listed.

## Extended functions for received files and finished outgoings




When viewing the incoming or the finished outgoings folders additional functions are available using the file views context menu. All functions will be applied to all selected files.

**Manual postprocessing** - Using this function, postprocessing, e.g. decrypting or character set conversion, of received files can be started manually. This function is only available for files that aren't postprocessed yet, marked by an asterisk (*) in the status column (*S*).

**Repeat EDI processing** - The marked files will get processed again by the module EDI. The files will get a new internal ID. As a result in the protocols the repeated processing will not be linked to the receiving process!

**Show ENGDAT information** (ENGDAT Add-On only) - Evaluate the selected ENGDAT file. This displays the corresponding ENGDAT information and allows you to rename (and decompress) all files from the ENGDAT transmission to their original file names.

**Convert file(s) from ASCII to EBCDIC** - Convert selected files from ASCII character set to EBCDIC character set. The converted data will be saved as a new file using the same name as the original file with the addition of "*.ebcdic*". The original file won't get changed!

**Convert file(s) from EBCDIC to ASCII** - Convert selected files from EBCDIC character set to ASCII character set. The converted data will be saved as a new file using the same name as the original file with the addition of "*.ascii*". The original file won't get changed!

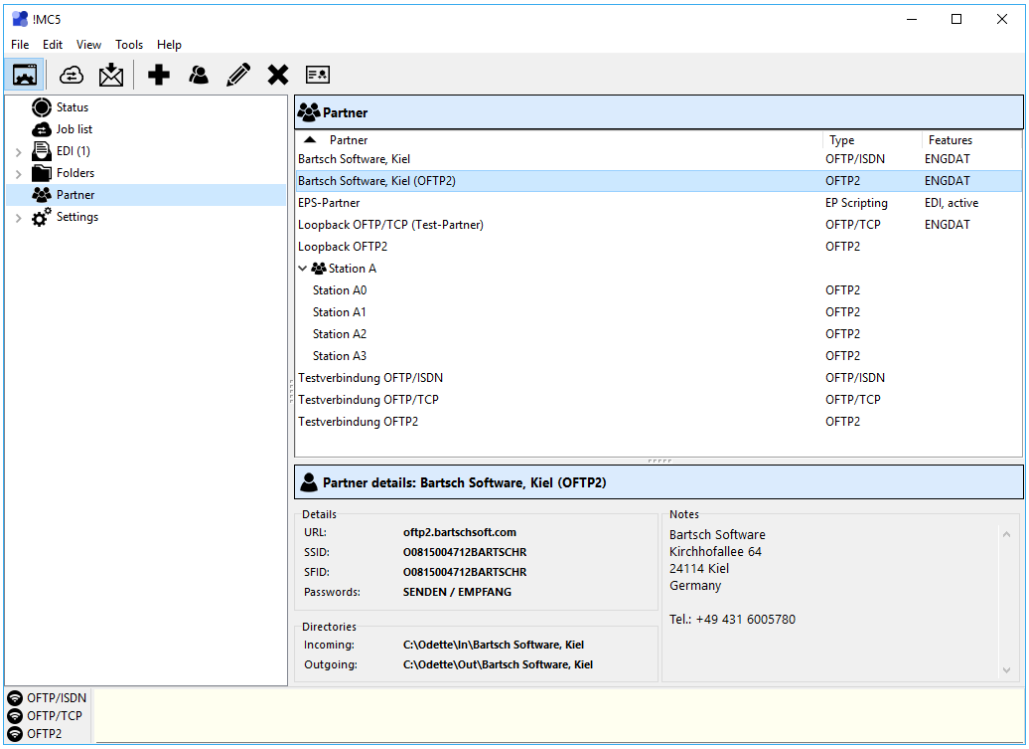
**Open file** - Opens the file with the associated windows program.

**Show in Windows Explorer** - Opens a Windows Explorer showing the incoming folder of the currently selected partner with the respective file selected.

**Delete** - Received files and successfully transferred files can be moved to Windows' recycle bin using this function. If you have many file transmissions and received or sent files aren't moved or deleted otherwise, the respective folders might fill up quite fast. In this case regularly delete files from these folders as too many files might decrease system performance.

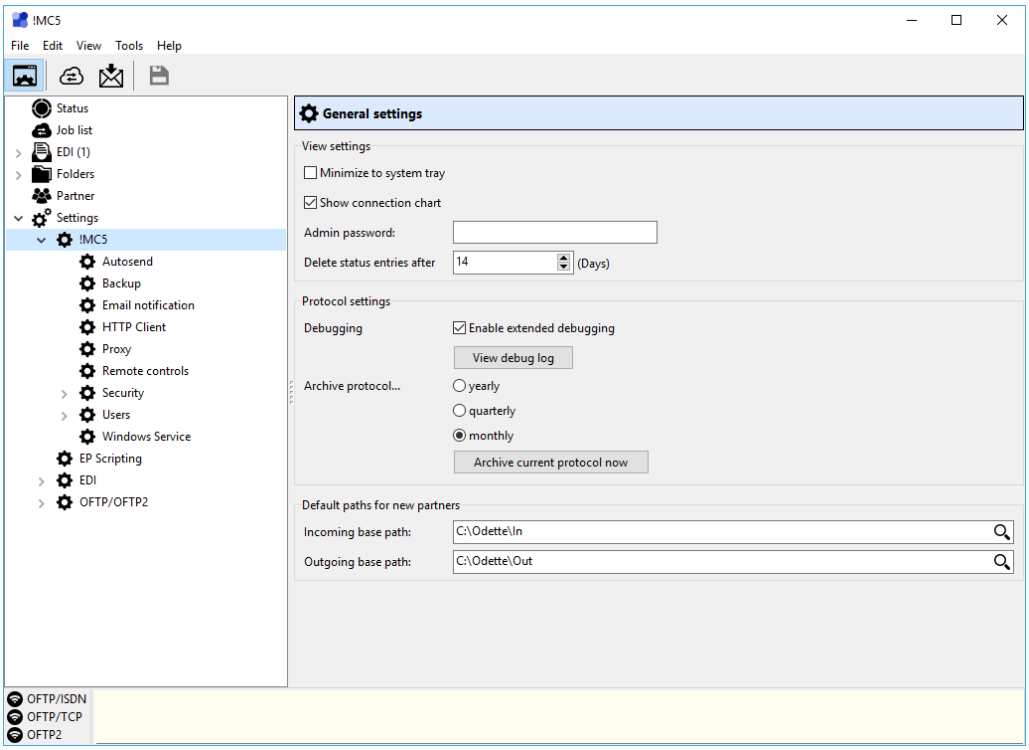
### 3.1.5 Partner

(*OFTP, OFTP2 and EP Scripting only*)




List all available partner connections. You can create new partner connections or edit or delete existing ones. A detailed description of all available functions can be found at Partner management.

### 3.1.6 Settings




In the settings section of the tree navigation all settings for !MC5, its Add-Ons and modules can be found. Which subsections are available depends on the registered modules and Add-Ons. A detailed description of each page can be found in the reference.

## 3.2 Sending and receiving via OFTP/OFTP2

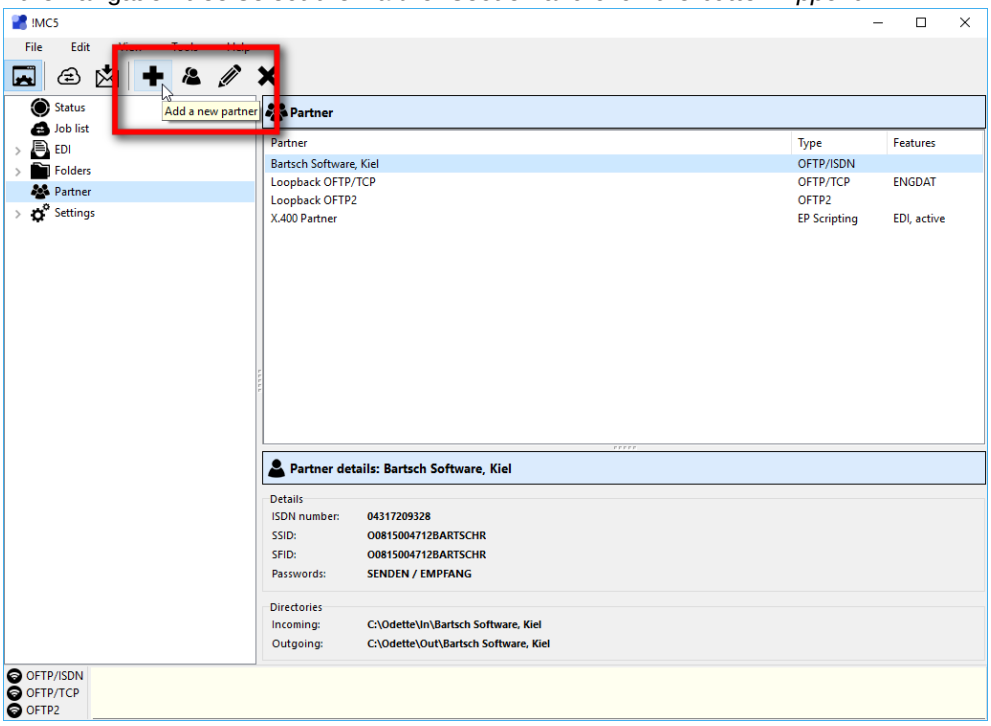
In order to receive files from a partner company, the partner companies data must be entered into the addresses database (see section Create a new partner account). As soon as !MC5 is ready to receive the partner can send files. It is also possible to poll files from the partner with the use of an empty sending job. For more details see Sending files.

The same requirements are necessary to send files to a partner: Before any data can be sent to a partner company its communication parameters (ISDN-number, IP-address, Odette-ID, ...) have to be filled into the addresses database. Only one partner account is necessary to send and receive files.

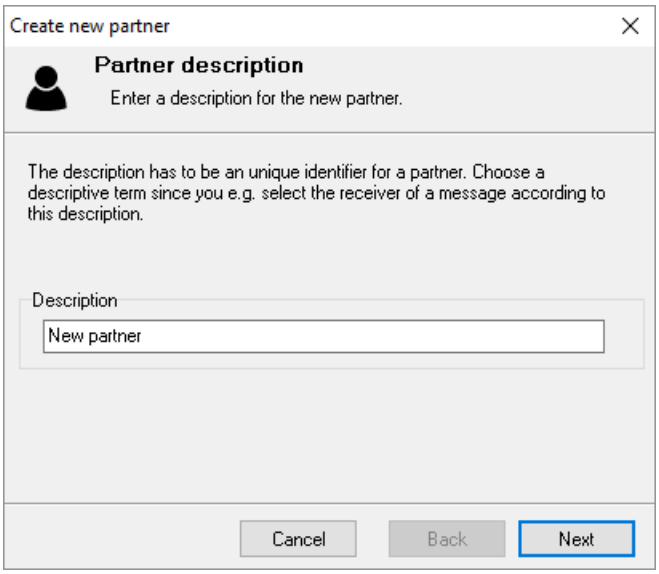
### 3.2.1 OFTP partner setup

To create a new partner account with connection type *OFTP* please proceed as follows:

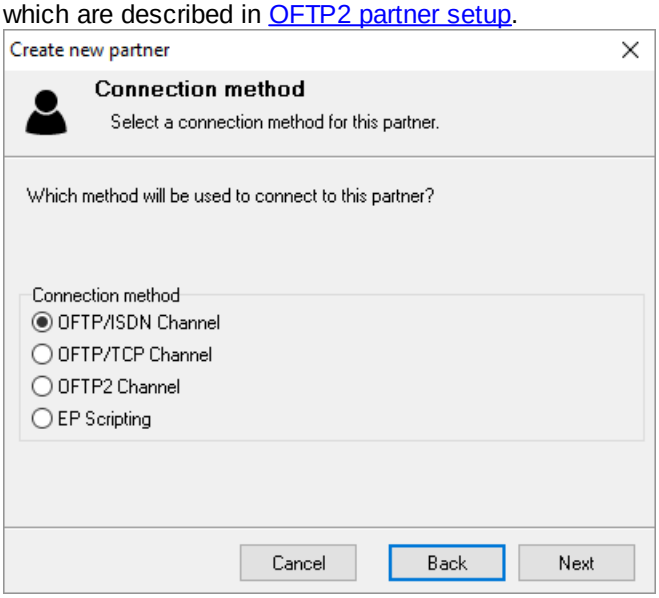
**1** In the navigation tree select the *Partner* section and click the button *Append*.



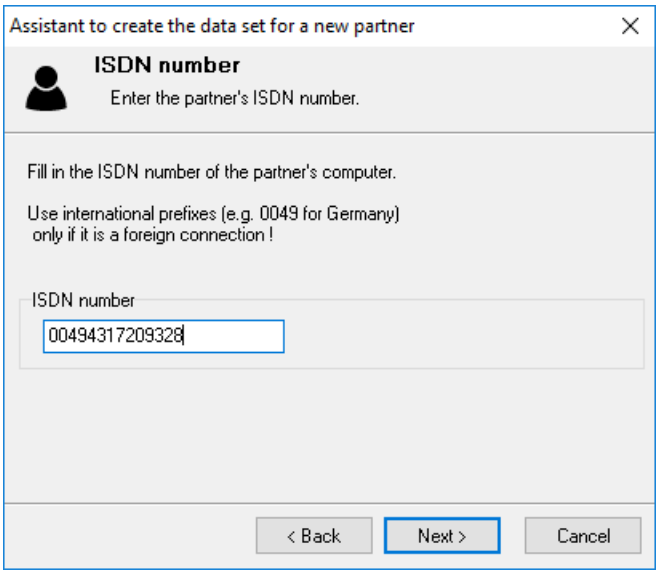

**2** Please enter unique identifier for the partner company. This name will be used later on to identify this dataset. A given name cannot be used twice. Then click *Continue*.



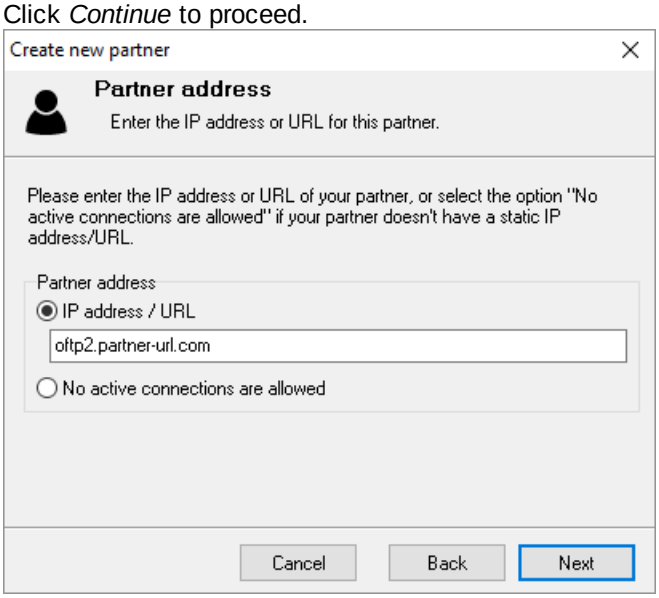

**3** If your license includes more than one connection module you will have to choose the connection type next. Click *Continue* afterwards. Depending on the license the choices are: OFTP/*ISDN*, OFTP/*TCP* and *OFTP2*. *OFTP2* requires additional steps which are described in OFTP2 partner setup.




**4.a** (*OFTP/ISDN*) Enter the ISDN number of the partner company and click *Continue*. Enter the number completely, including area code. Only numerals are allowed. Please do not use spaces, the plus symbol or any other non-numerals. The international area code should only be used in case of a connection across the border.




**4.b** (*OFTP/TCP and OFTP2*) Enter the IP-address or URL of the partner company's server. If your partner has got no fix IP-address then set the option *No active connections are allowed*. In this case your partner will always have to initiate the connection. Click *Continue* to proceed.



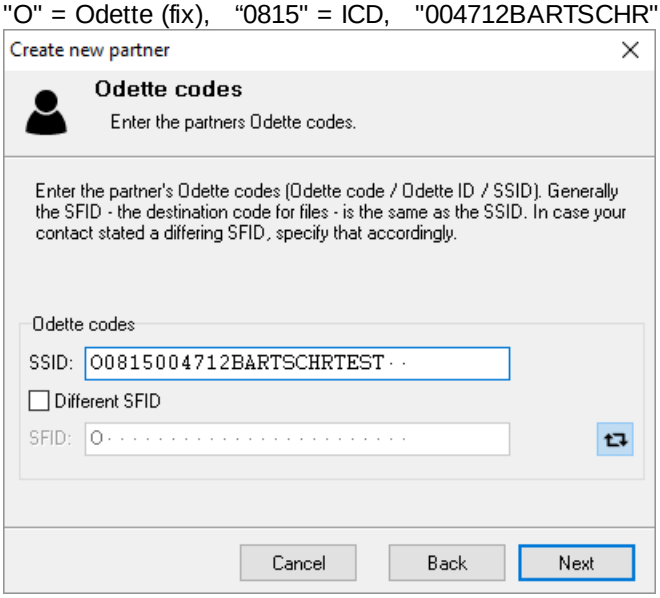

**5** Now enter the Odette-ID of the partner company. This ID has to be provided by the partner. Without the correct ID it is not possible to establish a connection. The edit field for Odette-ID can be shown as a single field or divided ICD, Code and CSA. All position left empty will be filled with spaces automatically. The Odette-ID, including the leading "O", always consists of 25 characters. Click *Continue* after entering the ID.

The SFID is the destination ID for files to be sent. In most cases it is identical with the Odette-ID. It should only be changed on Partner's request.

The maximum lengths are:
ICD = 4 characters,
Code =14 characters,
CSA = 6 characters.

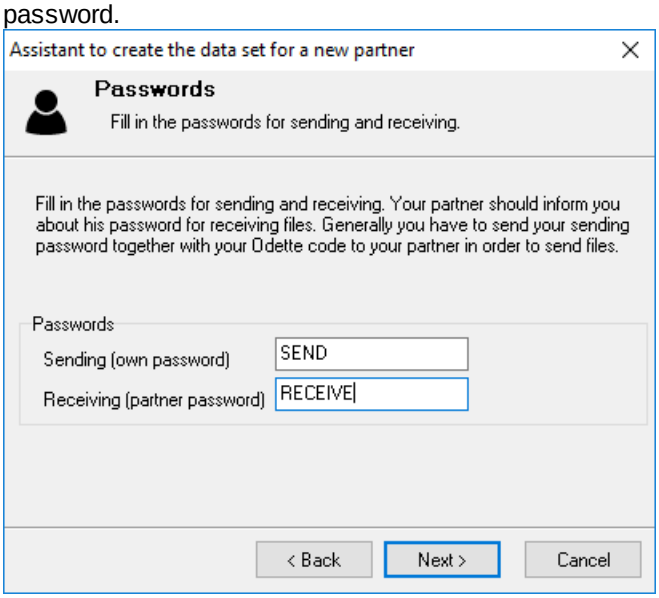
Example for an Odette-ID:

"O0815004712BARTSCHRTEST", as where are:
"O" = Odette (fix), "0815" = ICD, "004712BARTSCHR" = Code, "TEST" = CSA



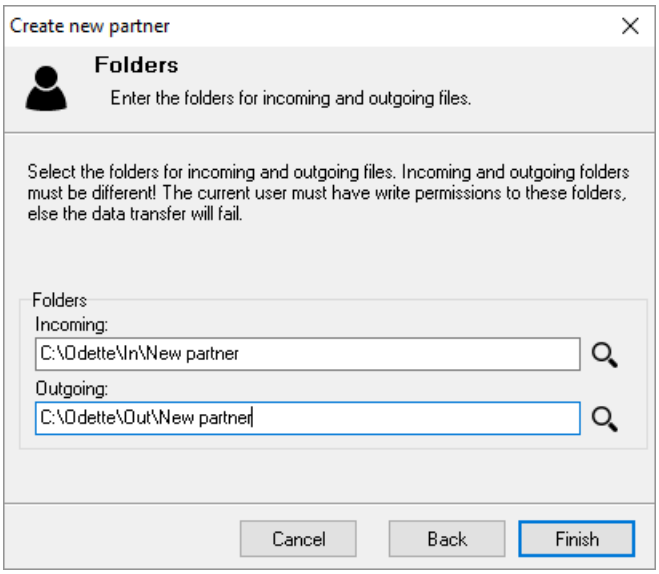

**6** Enter your own password into the upper field. It must also be provided to your partner. The password given by your partner belongs into the lower field. You might use the same password for all partners but it is recommended to choose a different for each of them.

Limitations: Allowed are only capital letters, numerals and the following special characters: / - . & ( ) . Not allowed are country specific characters and spaces within the password.




**7** On the last page the folders for received files and files to be sent have to be entered. The folders for sending and receiving must not be identical. Close the assistant by clicking *Finish*. The new account is now created.

Choose new and unique folders for each partner account. Please make sure that full access rights are granted for these folders under Windows.

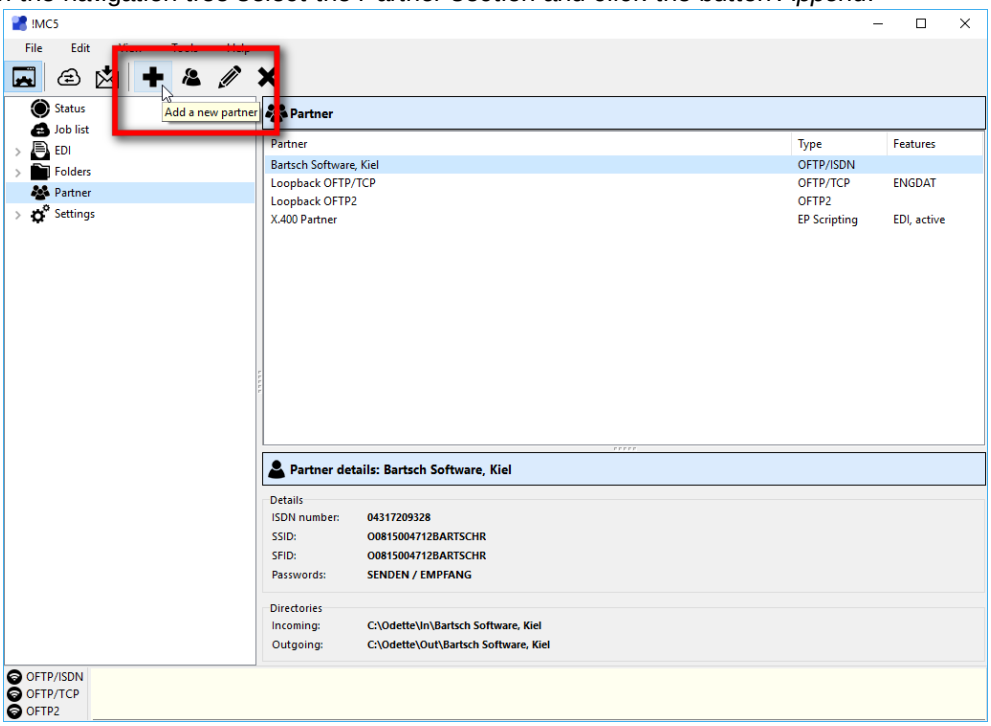



If all data are entered correctly the new account will be available at once. All data, except the connection type, can be changed later on with the edit function. The edit windows also provides additional settings as file formats and ENGDAT. To open the edit window first select the dataset from the database then click the *edit* button.

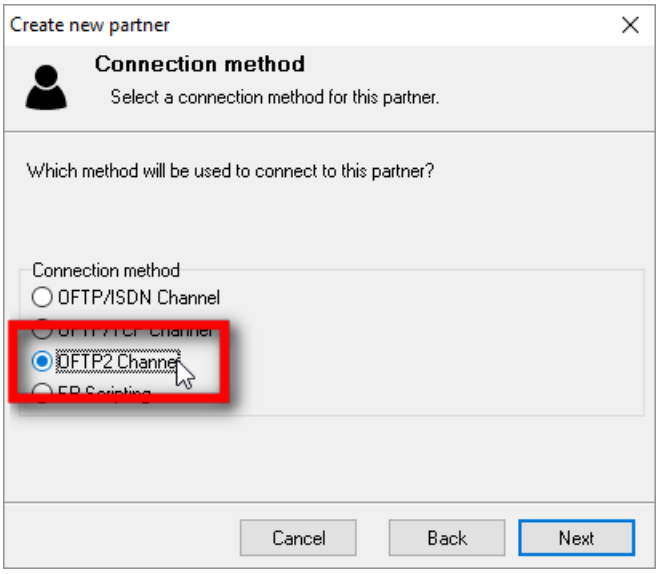
### 3.2.2 OFTP2 partner setup

To create a new partner account with connection type *OFTP2* please proceed as follows:

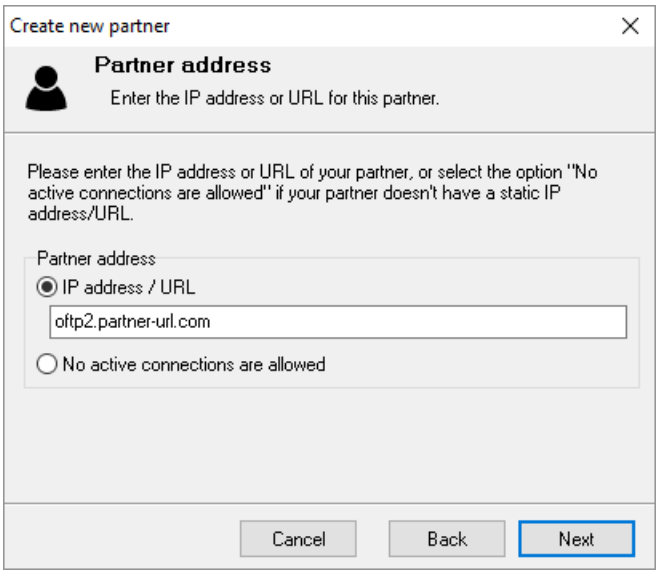
**1** In the navigation tree select the *Partner* section and click the button *Append*.



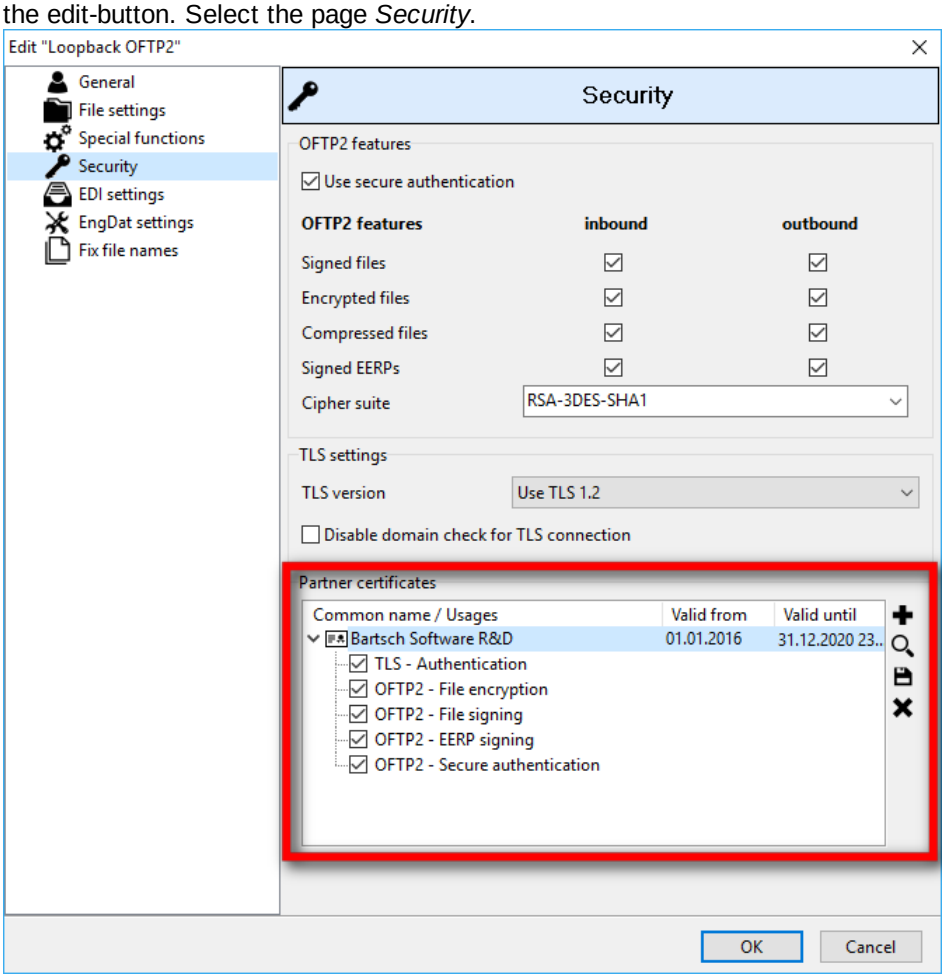

**2** Follow the instructions given on screen, then select *OFTP2* on the page *Connection method*.




**3** Enter the IP-address or URL of the partner company's server. If your partner has got no fix IP-address then set the option *No active connections are allowed*. In this case your partner will alwys have to initiate the connection. Click *Continue* then finish the assistant as usual.




**4** After finishing the assistant select the new account from the address list and press the edit-button. Select the page *Security*.



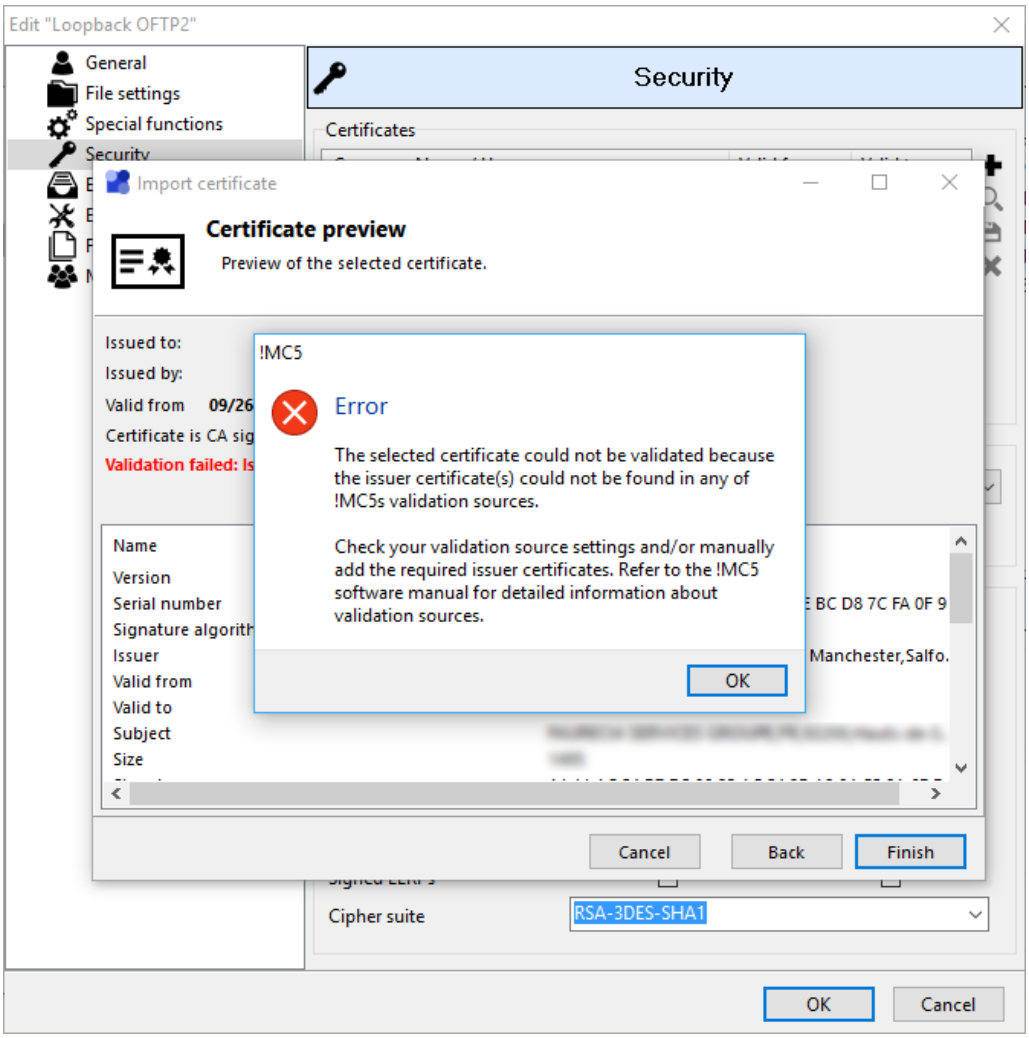

**5** Insert the certificates, provided by partner company, here by using the button *Select Certificate*. At least one certificate is needed in order to establish an outgoing connection to this partner. A certificate is also needed for incoming connection when the option *Clients must send a certificate* is activated. There are various options to add a certificate. The public certificate of the partner company can be imported from a file or it can be selected from the Windows certificate store *Trusted People*. !MC5 is also

able to download it by direct connection. **Please check the downloaded certificate very carefully before accepting it!**

6 For each certificate select the usages it will be used for. In most cases one certificate is used for all available usages. But depending on the partner, different certificates may be used for different usages.

7 Save the settings by clicking *OK* and close the addresses database. The account can be used to exchange data with the partner company.

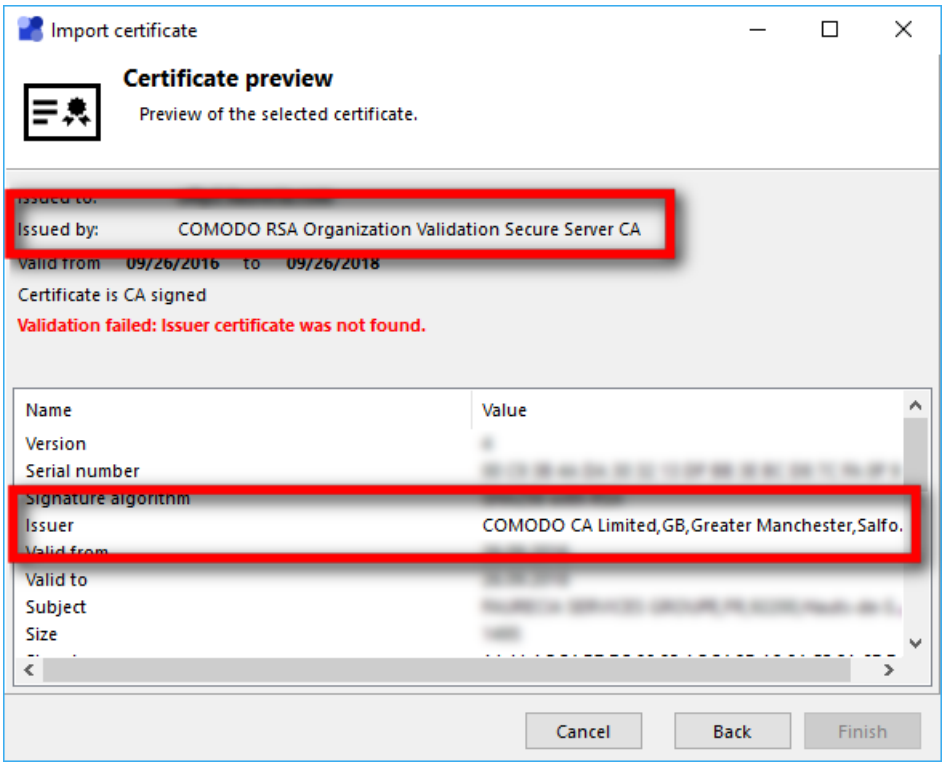
### 3.2.2.1 Adding missing issuer certificates




For a (niot self signed) certificate to validate, all required issuer certificates have to be present in one of !MC5s validation sources. !MC5 uses up to four different validation sources: Windows' certificate storage, the in !MC5 included default store, Trusted Service Status Lists downloadable via internet and user defined certificates. Which of these are used can be specified using the Security settings. User defined certificates are always being used.

So if a partners certificate cannot be validated because of a missing issuer certificate you can try to activate additional validation sources or install the required issuer certificates manually.

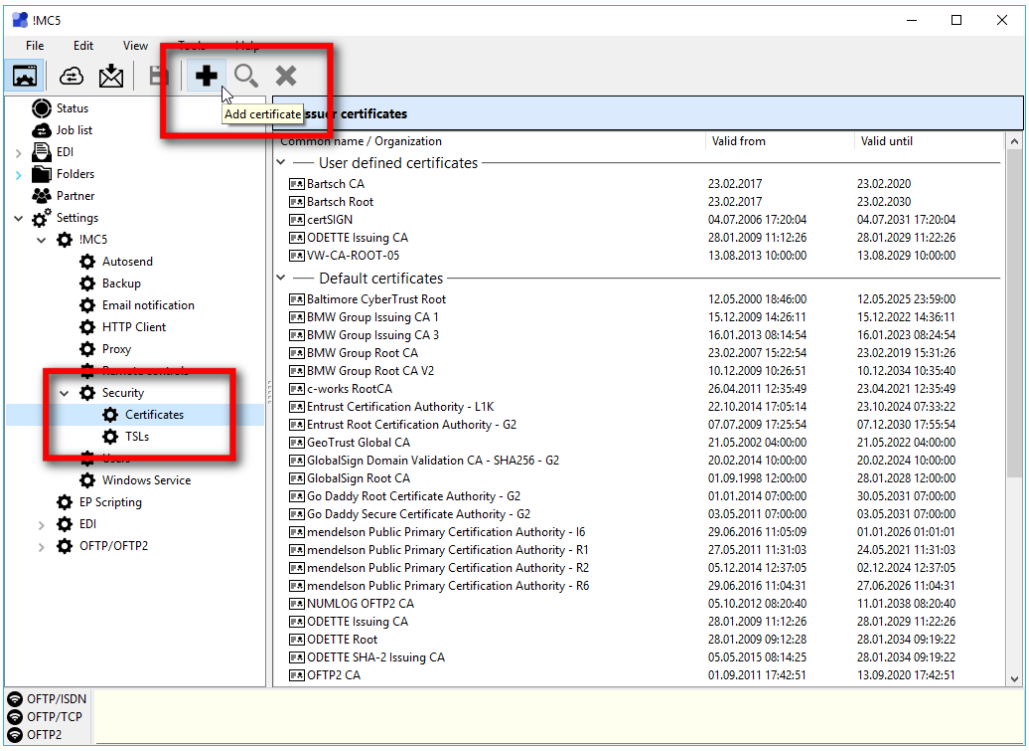
#### Determining required issuer certificates




To validate a not self signed certificate at leat one issuer certificate is needed, in most cases two are needed, one CA certificate (Certificate Authority) and one root certificate, and some cases require even more than two. All these certificates form a certificate chain, beginning at the root certificate up to the partners certificate, each certificate signed by the previous certificate in the chain, except the root certificate, which is self signed. When viewing a certificate in !MC5s certificate preview the common name of the directly preceding certificate in this chain is displayed two times as "Issued by" and "Issuer". **To successfully validate the certificate the iusser certificate with exactly the displayed common name has to be present in one validation source.**

Additionally to their own certificate partners will often send you the required root and CA certificates, which most times contain "Root" or "CA" in their file name. If your partner doesn't send you the required issuer certificates you can try to download them from the issuers website for which you might have to search on the internet. **When downloading certificates from the internet always make sure to only download from trusted websites!**

## Install user defined issuer certificates



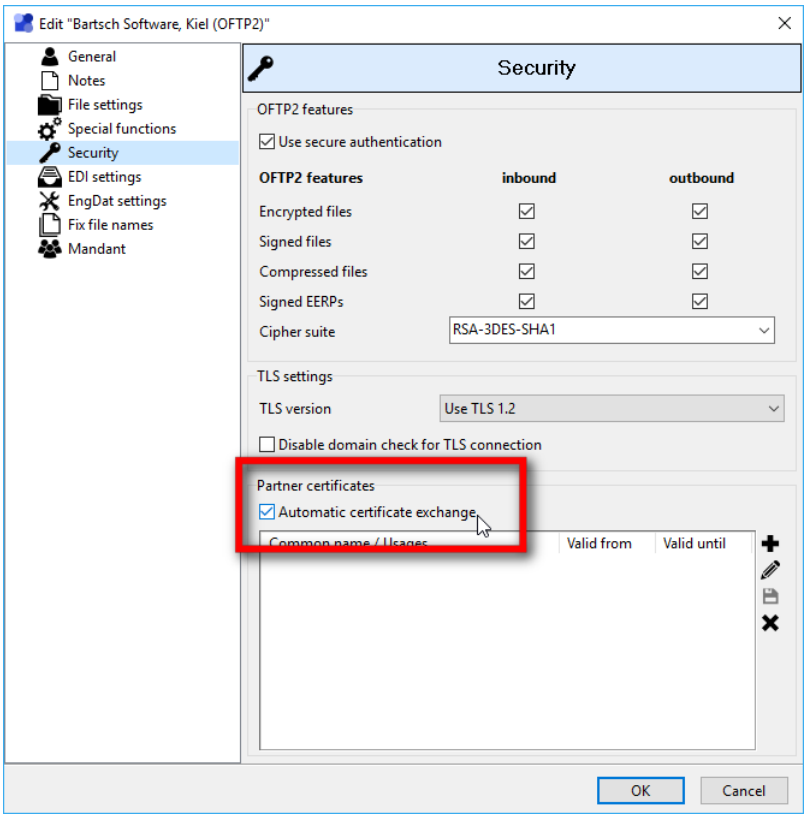

When you ave the required issuer certificates you can install them in the settings using *Settings / !MC5 / Security / Certificates*. You have to start installing the root certificate, followed by the CA certificate. Trying to import in the wrong sequence will cause validation errors while importing. When all required issuer certificates are installed you can import the partners certificate without validation errors.

#### 3.2.2.2 Automatic certificate exchange

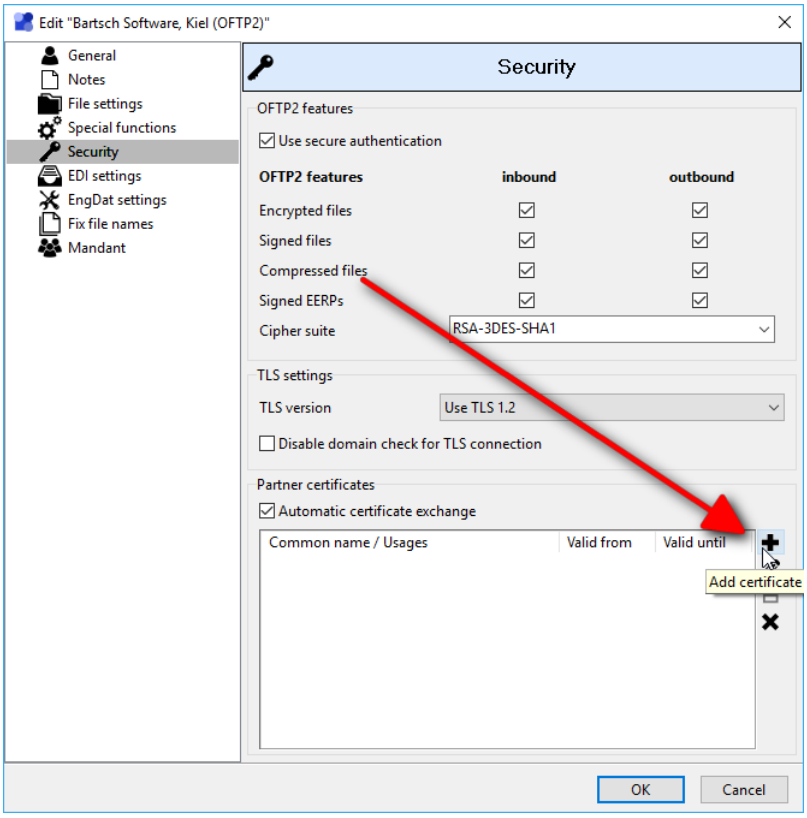
!MC5 supports the automatic certificate exchange complying to the OFTP2 Implementation Guidelines. This allows exchange of certificates via OFTP2: Certificates can be delivered to a partner and requested or revoked from a partner. Delivery and requests are possible without prior exchange of certificates, but require exchange of information about the certificate as only known certificates can be replaced by new ones. In order to use the automatic certificate exchange it has to be activated for the corresponding partner. Also the partner must support the automatic certificate exchange.

### Initial partner setup for automatic certificate exchange

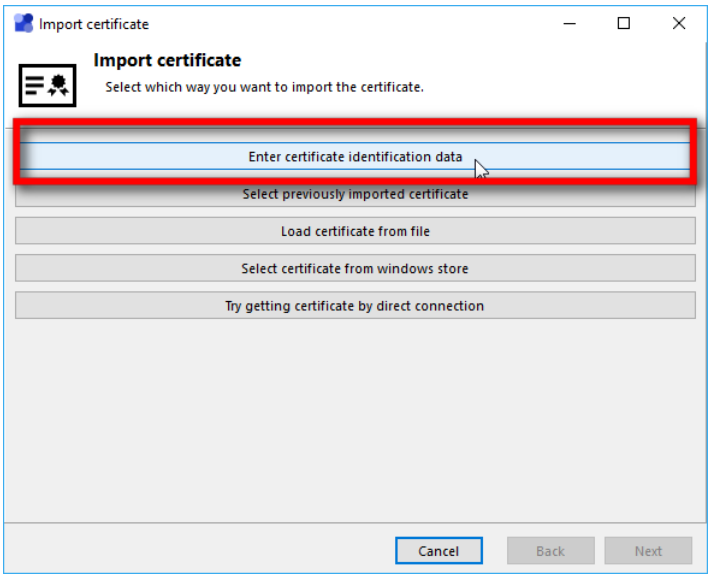
1. Open the partner management and edit the corresponding partner.
2. In the partners settings open the page *Security*.
3. Enable the option *Automatic certificate exchange* in the box *Partner certificates*.



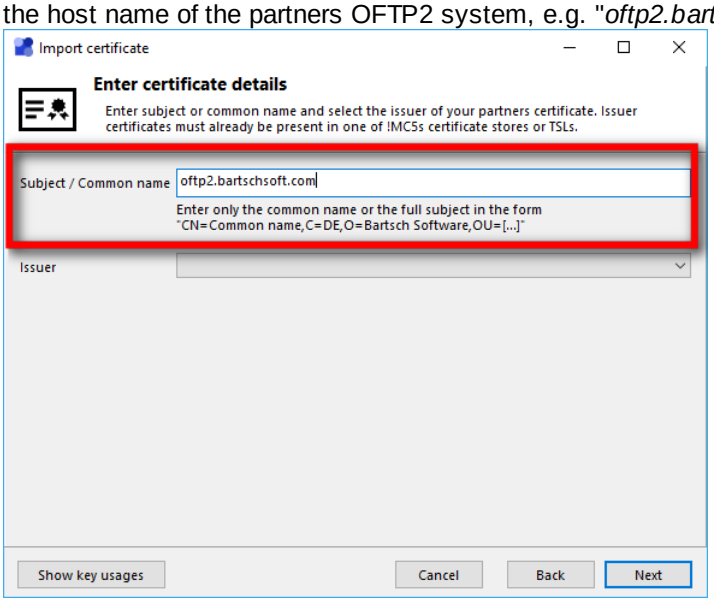

**4** Click the button *Add certificate*.



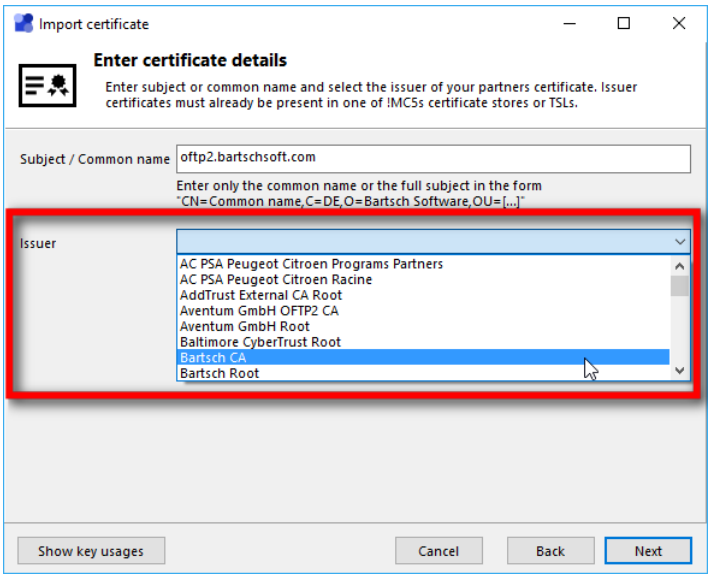

**5** Select the option *Enter certificate identification data*.




**6** Enter the subject of the partners certificate in the form "*CN=oftp2.bartschsoft.com,C=DE,O=Bartsch Software,[...]*". You should have received this information from your partner. Alternatively you can enter only the common name of the partners certificate. In most cases the common name is identical to the host name of the partners OFTP2 system, e.g. "*oftp2.bartschsoft.com*".



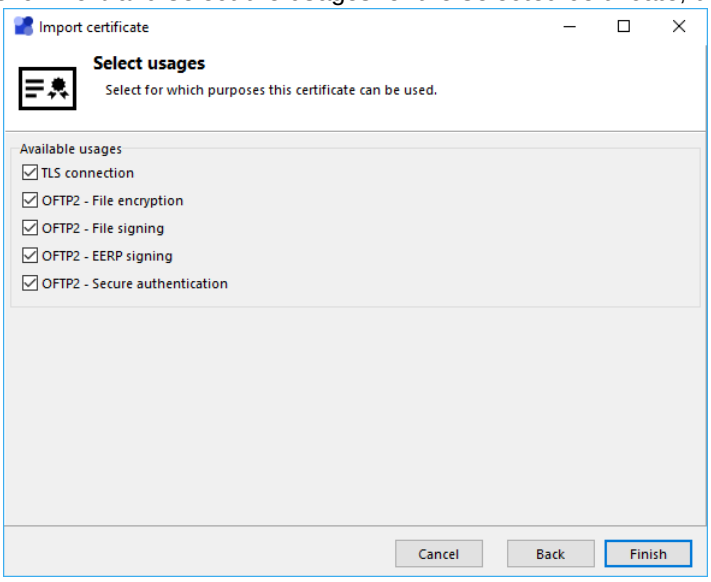

**7** Select the issuer of the partners certificate. Again you should have received this information from your partner. Only issuers known to !MC5 are available. If the partner uses an issuer not listed, you have to install the issuer certificate(s) via *Settings / !MC5 / Security / Certificates*.



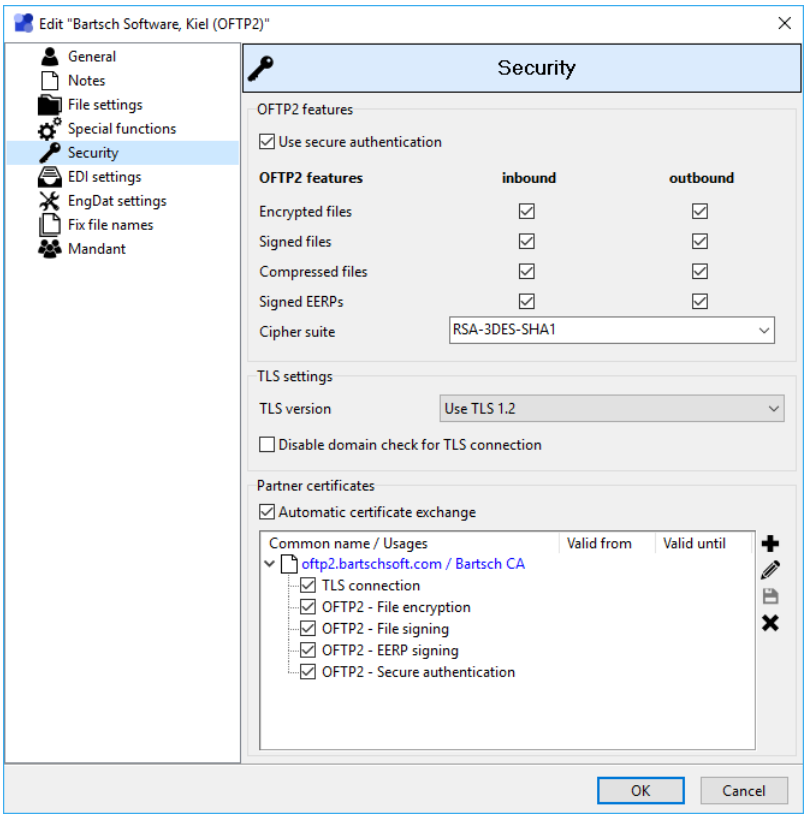

**8** If the partner explicitly requires certain key usages those can be entered using the button *Show key usages*.

> **Direct use of partner certificate**
> Instead of entering the certificate information you can directly use the partners certificate. This also allows usage of the automatic certificate exchange with some limitations. If you use the partners certificate directly you might not be able to send or receive certificates from the partner before the partner also enters your certificate in his system. If both sides only enter certificate information an exchange of certificates is possible bypassing secure OFTP2 authentication. This is needed, as secure authentication would require a certificate to be present. But as soon as a certificate is present this bypass isn't possible any more. So when using the automatic certificate exchange you and your partner have to agree as to what way for the initial setup has to be used.

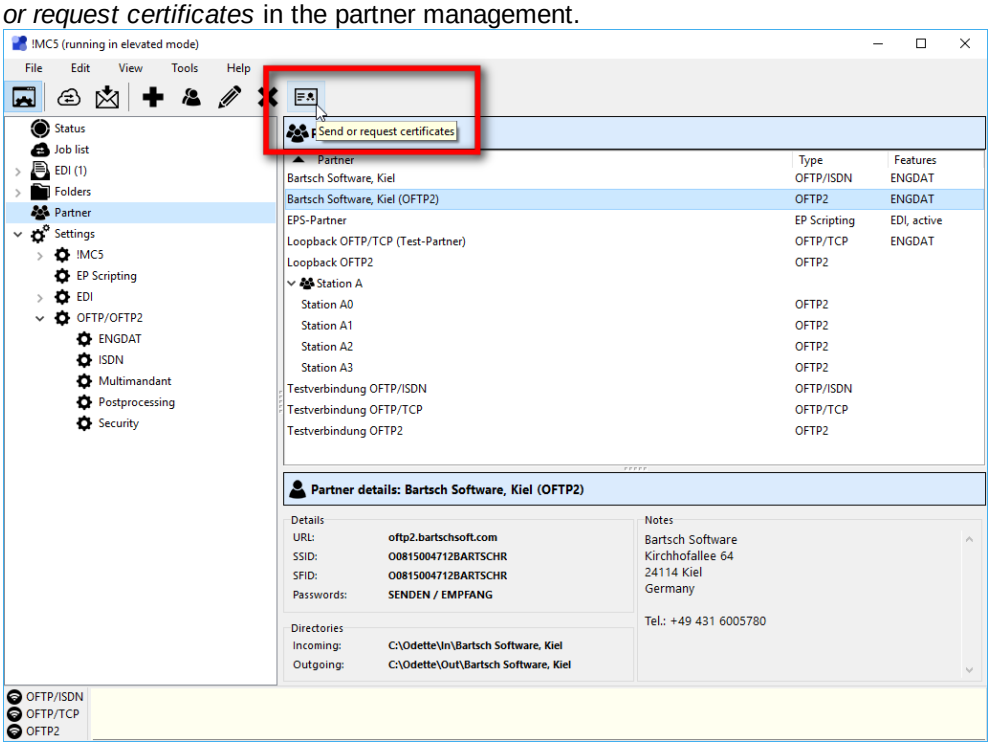
**9** Click *Next* and select the usages for the selected certificate, then click *Finish*.




**10** The partner is now configured for automatic certificate exchange. The certificate information are displayed blue and using a different icon. The can be edited any time using the edit function. Save the changes by clicking *OK*.




**11** Now you can deliver or request certificates to or from a partner using the button *Send or request certificates* in the partner management.



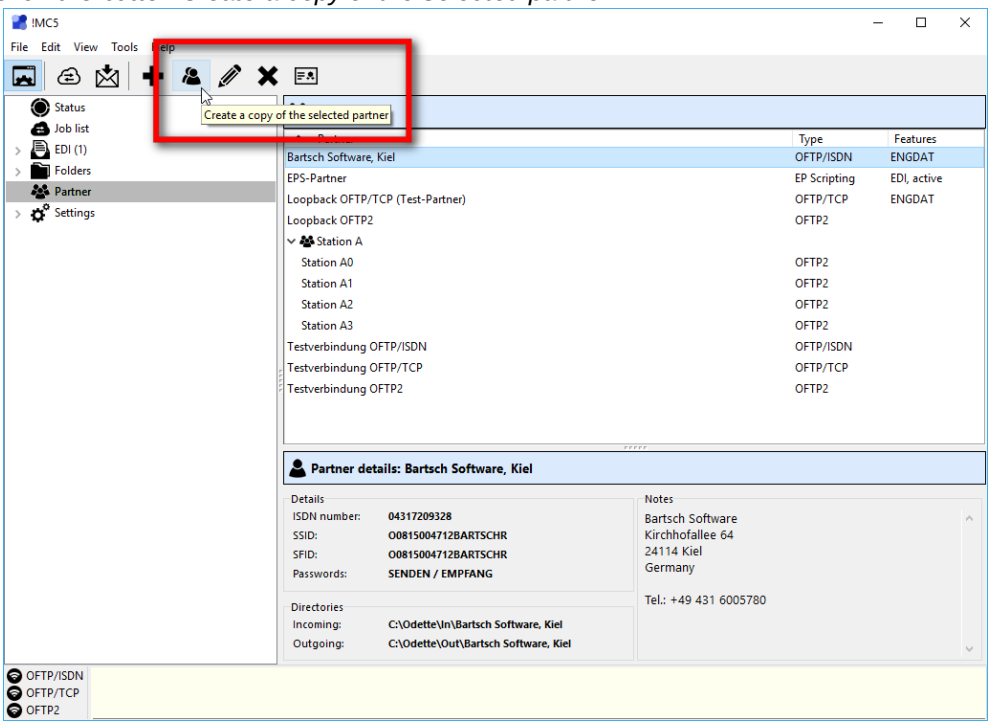
### 3.2.3 Change OFTP connection type

It is not possible to simply change the connection type of an OFTP partner, e.g. from OFTP/ISDN to OFTP2. But when creating a copy of a partner you can select a new connection type for the copy. This limitation is implemented to prevent breaking the communication with an existing partner. By creating a copy the new connection the existing configuration be be used further until the new one is fully tested.

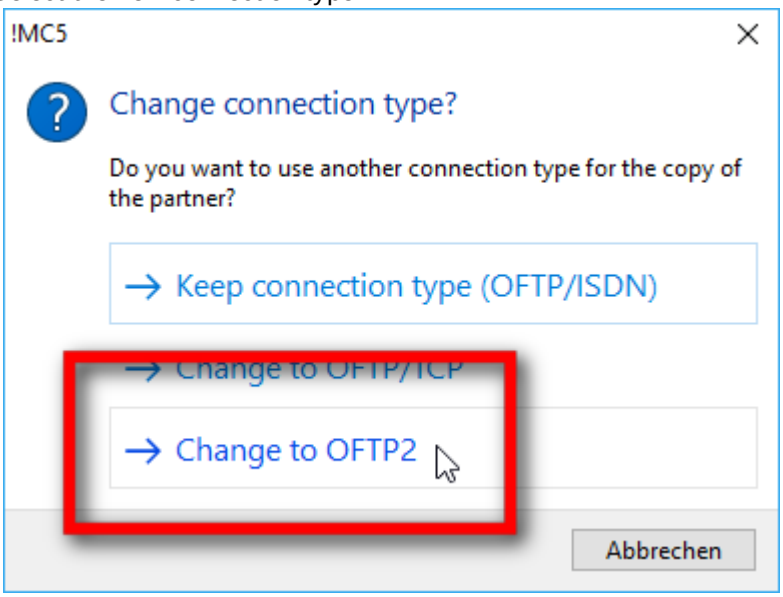
To create a copy of a partner and change its connection type follow these steps:

**1** Open the partner management and select the partner you want to create a copy of.

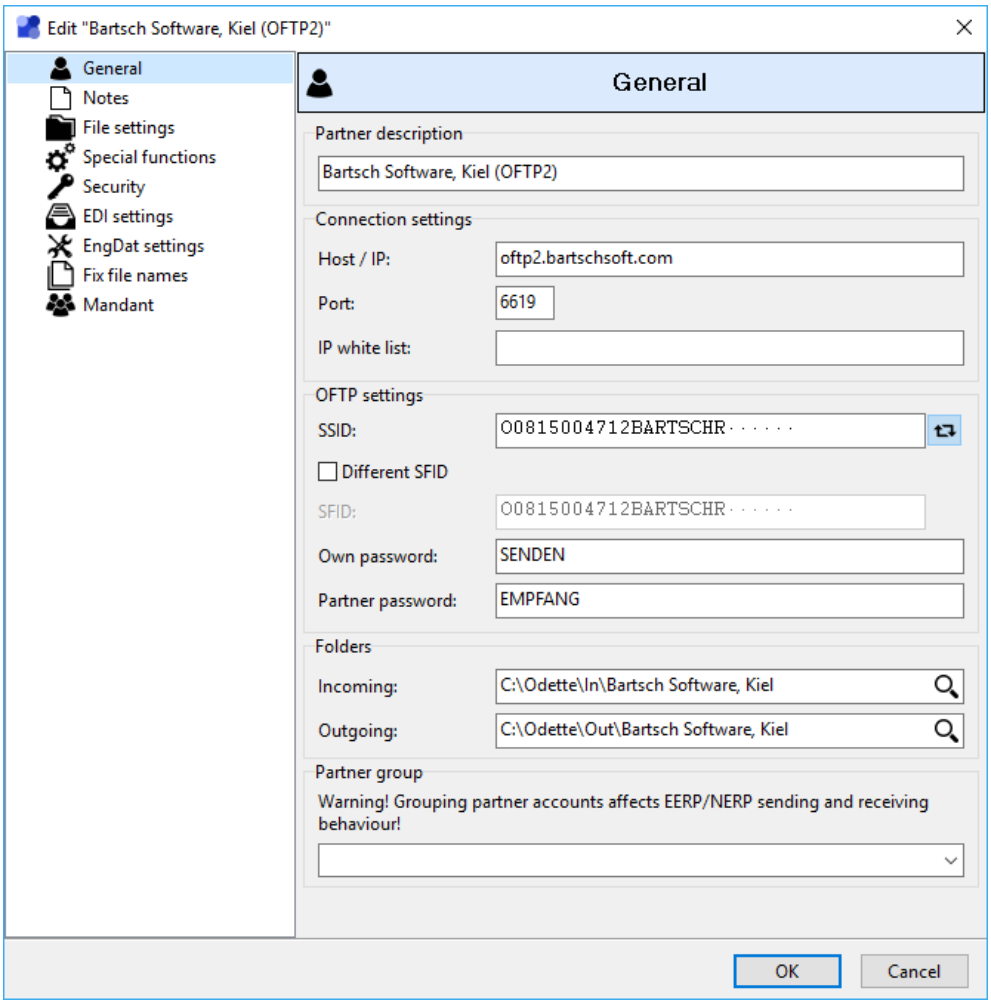
**2** Click the button *Create a copy of the selected partner*.




**3** Select the new connection type.




**4** Edit the partner settings according to the new connection type and save them by clicking *OK*.




It's recommended to thoroughly test the new partner account. If all test are finished successfully, existing auto send, EDI import and EDI export rules have to be switched manually to the new partner account. Also, when creating a copy of a partner, the copy uses the same folders for incoming and outgoing files, as the original partner. To prevent any problems that might be caused by this it is recommended to use at least a different outgoing folder until the original partner account isn't used for production data any more.

### 3.2.4 Partner groups

It is possible to group multiple partner accounts. Grouping is **not** intended to be used for simple sorting of partners but affects, amongst others, handling of files and EERPs.

#### 3.2.4.1 Sending files to one partner using different settings

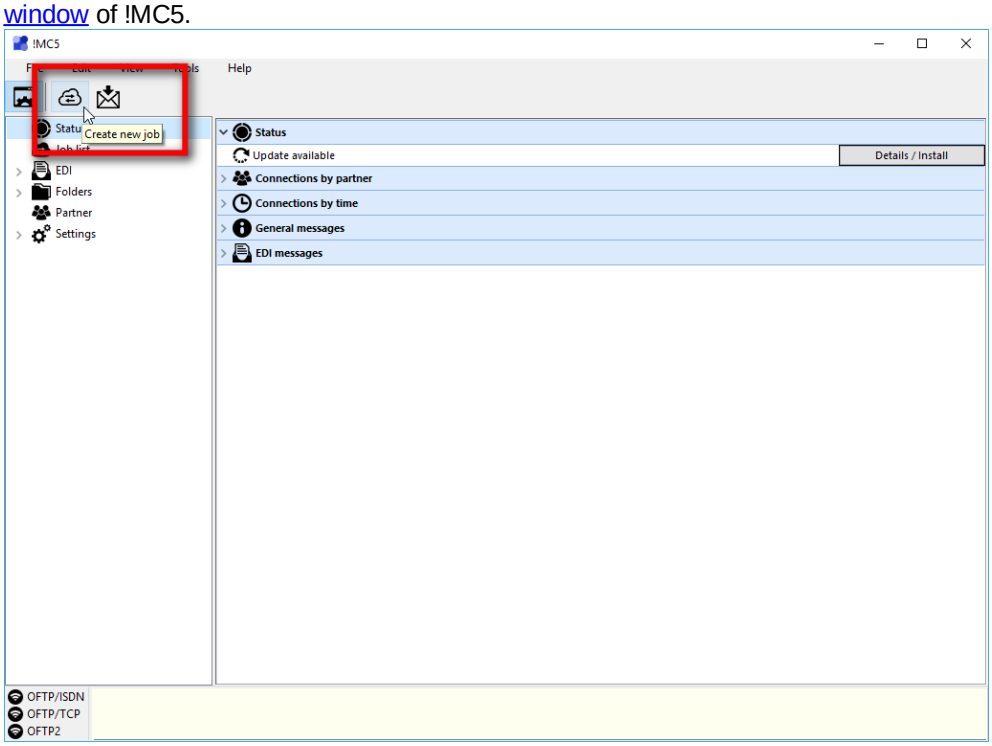
Files are to be sent to one partner using different settings, e.g. different SFIDs. One way to achieve this is to use two partner accounts which differ only by SFID (or any other setting that is required to be different). This way you can use the corresponding partner account in autosend or EDI import rules. In such a case both partner account have to be in the same group to avoid issues regarding EERPs/NERPs if those are being sent asynchronously. When an EERP (or NERP) is received !MC5 all partner account in the same group for the file the EERP is sent for. And outstanding EERPs are sent when any of the partners in a group establishes a connection.

#### 3.2.4.2 Sort received files by SFID

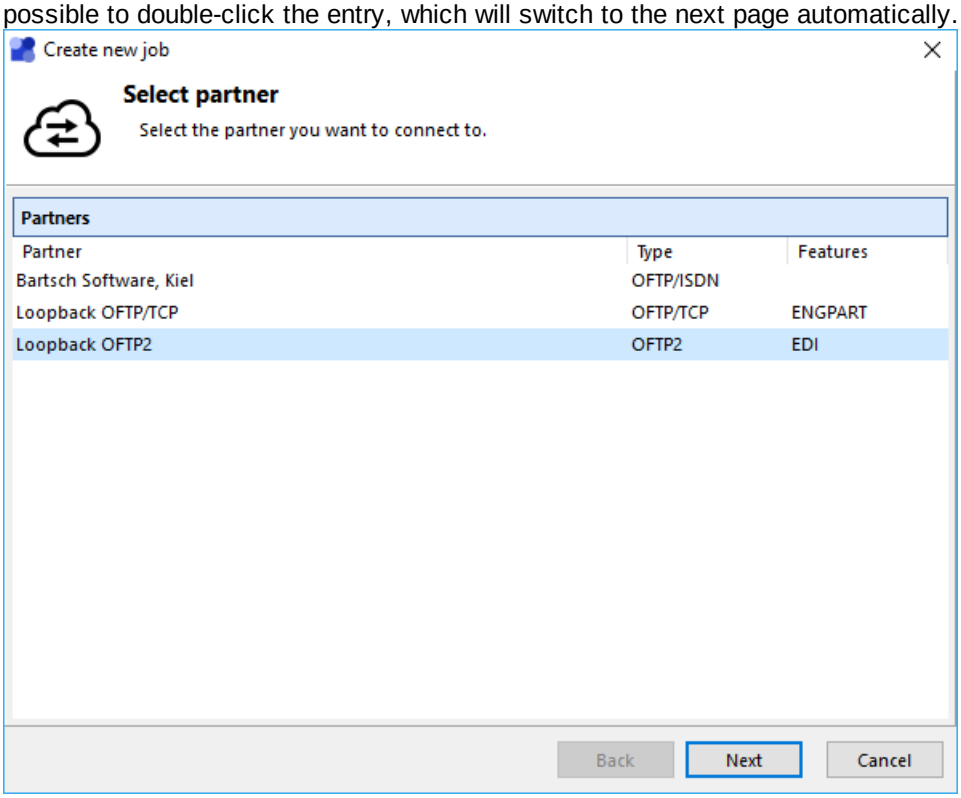
Another use for partner groups is the sorting and processing of received files by SFID. If a partner sends files using different originator SFIDs, e.g. CAD data using one SFID and EDI data using another, you can create two partner accounts, one for each originator SFID. Received files will be saved into the incoming folder of that partner accounts, which matches the files originator SFID. Also the postprocessing options of the matching account will be used.

### 3.2.5 Sending files

**1** Start the assistant for creating new jobs by clicking the button *New job* in the main window of !MC5.

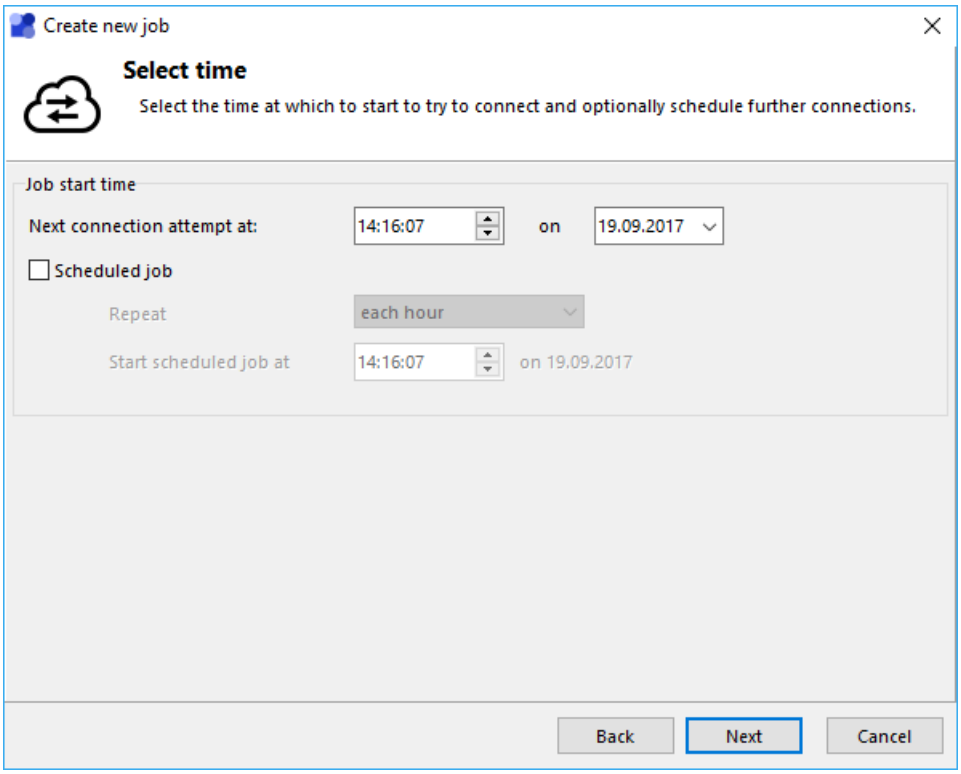



**2** First select the required partner account, then click *Continue* to proceed. It is also possible to double-click the entry, which will switch to the next page automatically.



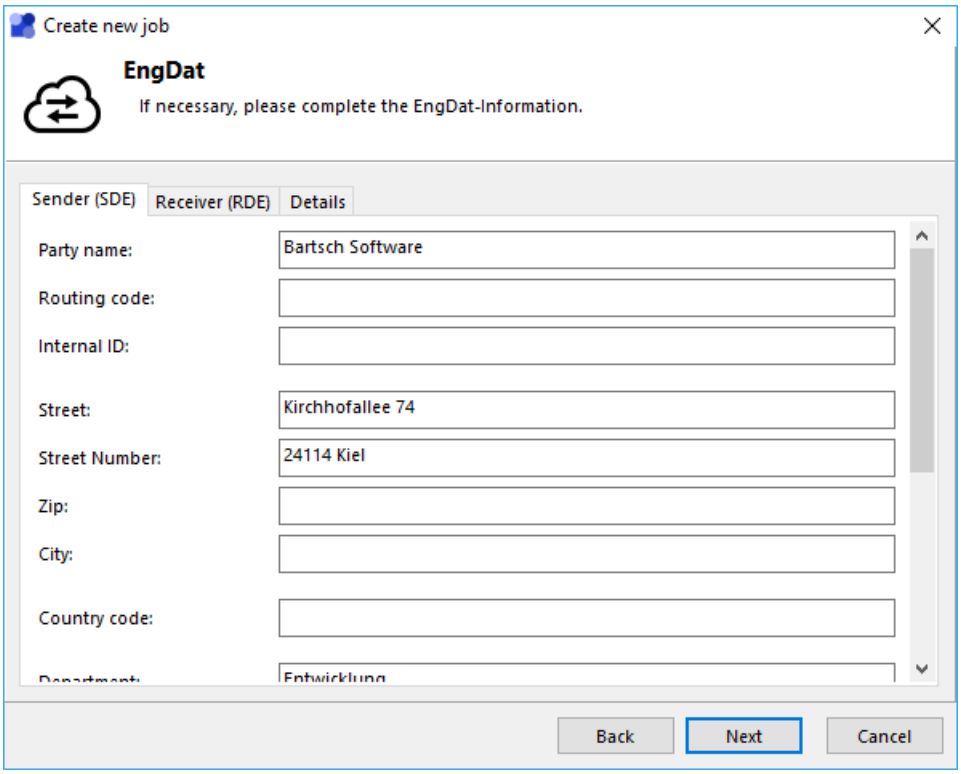

**3** Then choose the point in time when the first connection attempt has to be done. Default setting is the current time. If the point lies in the past the job will be started immediately after the assistant has finished.

If the option *Scheduled job* is activated all files in the folder for outgoing files will be sent at the given point in time. The interval, in which the connections have to be done, can be selected over the drop-down list. With *Start scheduled job at* the initial starting of this job can be chosen. **Exception**: If *Individual* is selected as interval this field will determine the period between connections.



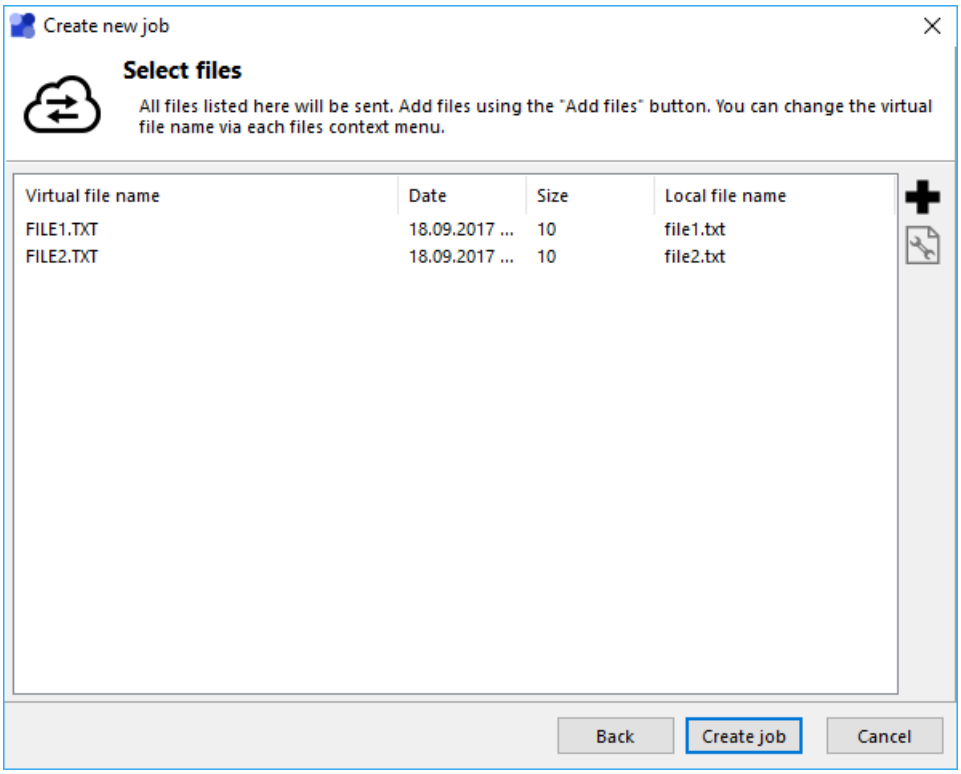

**ISDN connection speed**
The time required for a file transfer over ISDN can be estimated with the following rule: One Megabyte of data requires approximately 2,5 minutes for transfer. 24 Megabytes should be transferred in an hour. The duration will always be determined by the slower side.

**4** If ENGDAT is activated for the selected partner account the ENGDAT settings page will appear next. Verify the given settings and change them accordingly. Information regarding files can be entered in the following file-list page. The settings-window is opened there by double-clicking a file entry.



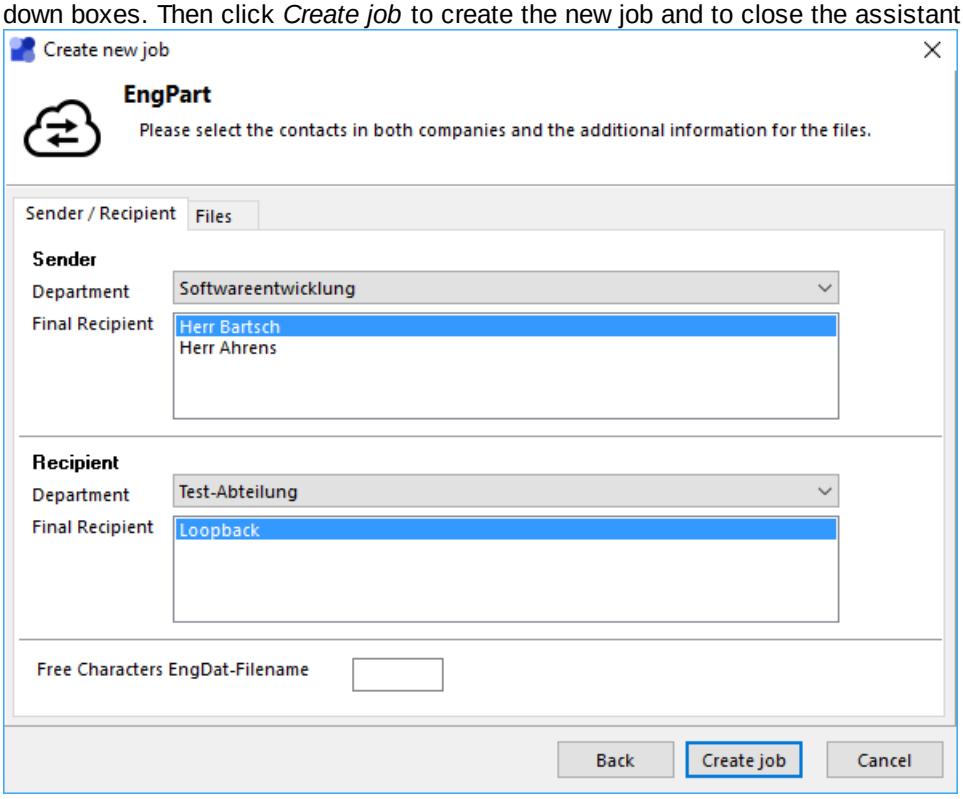

**5** If ENGDAT is not activated the list of files will appear after the time selection. These files are located in the folder for outgoing files associated with the selected partner account. All files in this folder will be sent within the next connection. Files can be added by Drag & Drop or by clicking the Add-button.
The filename used during transmission can be changed over the popup-menu. The local filename will be kept unchanged, only the name transmitted to the partner will be affected. Several files can be be combined into a Tar-archive by first selecting them and then clicking the function *Merge files to .tar archive*.

Click *Create job* to create the new job and to finish the job wizard. The job will be started on the selected point in time. After successful transmission the files will be moved into the sub-folder *backup*. This prevents a repeated sending of already transmitted files.




**Jobs without files**
It is possible to create sending jobs without files. If you expect that the partner company has got files prepared for you, you are able to poll them by creating an empty sending job.

**6** If EngPart is activated for the selected partner the EngPart page will appear instead of the file-list. Select sender, receiver and file-depended parameters from the given drop-down boxes. Then click *Create job* to create the new job and to close the assistant.



## 3.3 EDI

The EDI Add-On enables !MC5 to process EDI message of various standards. Received messages can be printed, converted and exported into a file. Inhouse files can be imported, converted, printed and sent to a partner company. !MC5 supports messages of the standards ASCX12, EDIFACT and VDA.

Additionally XML files and freely definable flatfiles can be imported and exported. Flatfiles are specialized text files which are constructed by given rules. A common example are csv files which are also used by Excel. Because of this free choice of format !MC5 can be easily adapted to any given inhouse format.

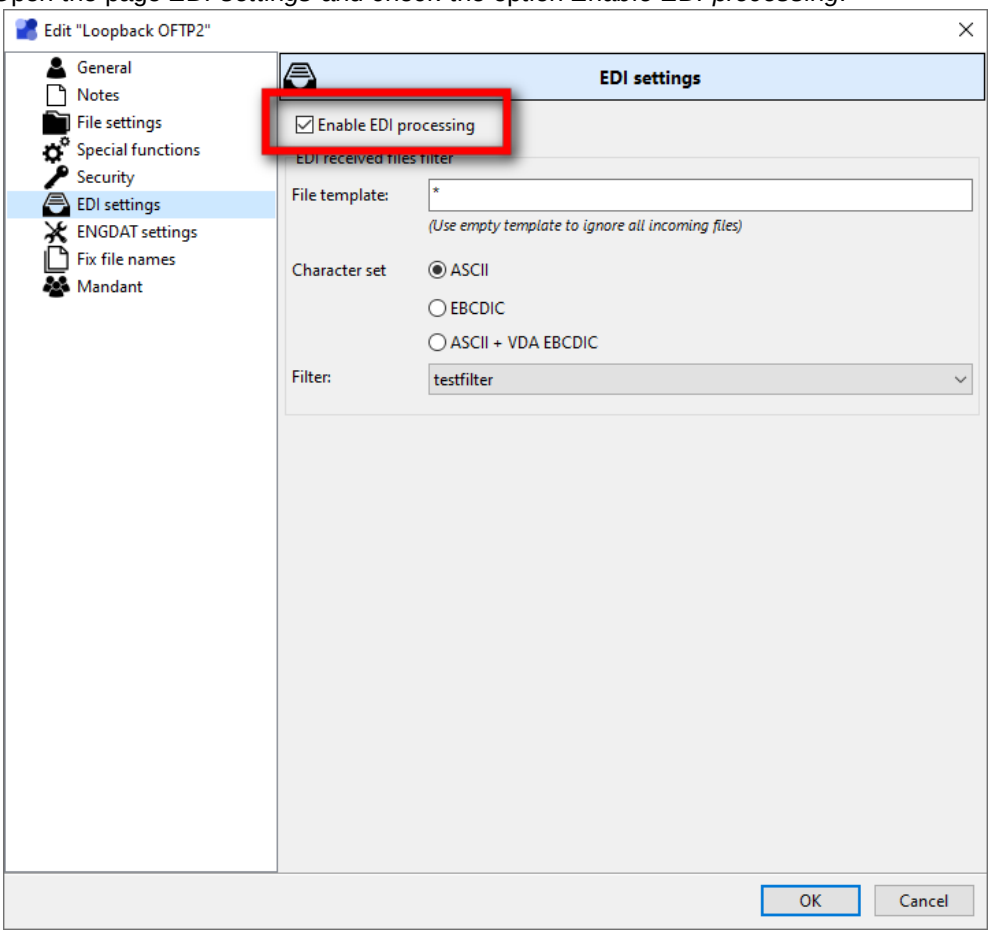
The functions of the EDI module are able to run fully automated.

### 3.3.1 Partner setup

To activate the automated processing of incoming EDI message from a partner please proceed as follows:

1 Start !MC5, open the addresses database by selecting the *Partner* section in the left hand navigation tree and double-click the partner entry.

2 Open the page *EDI settings* and check the option *Enable EDI processing*.




3 Enter a *File template* to select files for processing. The incoming files are selected by their file names. The template * will forward all files to the Module EDI, **.txt* will select files with the suffix *.txt*. The template *ab??.** will allow all files which names are 4 digits long and start with *ab*, any suffix is ok. The characters *?* and * can be used as wild cards, the usual rules of Windows apply. The default setting is * (all files).

4 Select the *Character set* of the received files. *ASCII* is mostly used for EDIFACT messages and EBCDIC is a very common format for VDA messages.

5 A *Filter* can check or reformat incoming files prior to processing. Non matching files can be excluded from further processing.

6 Save the settings by clicking *OK*. From this point on matching incoming files from this partner are automatically forwarded to the Module EDI.

### 3.3.2 EDI in- and outbox

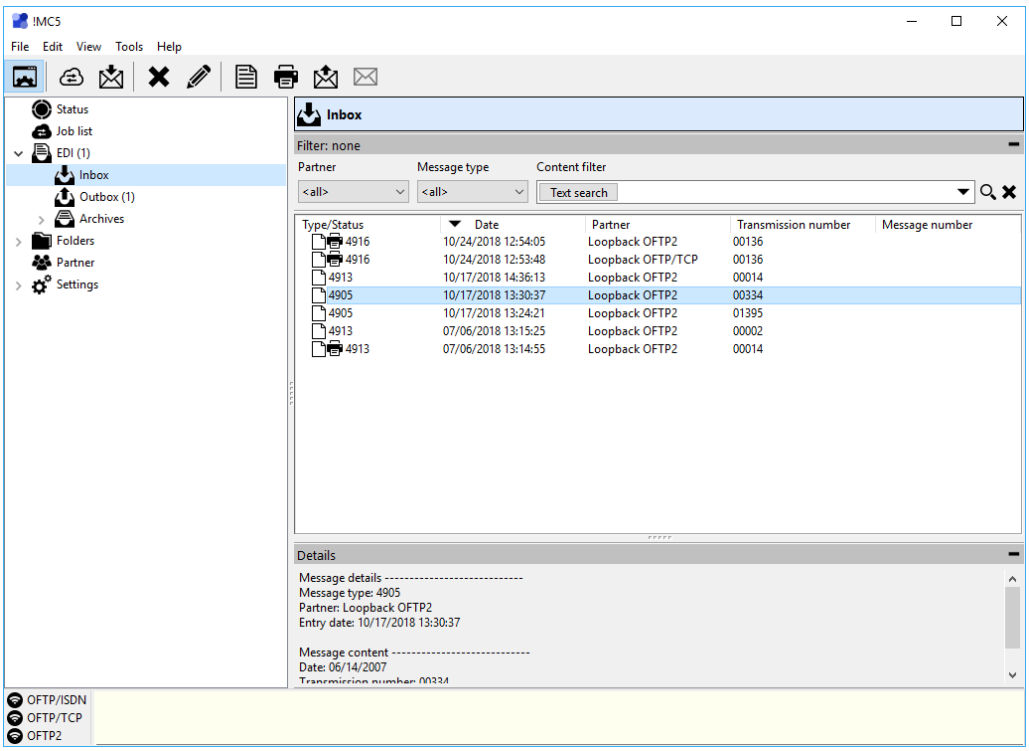
*(Module EDI only)*

Inbox and outbox provide an overview of recently received or sent EDI messages. Received messages are displayed in the inbox, send and not yet sent messages are displayed in the outbox. The archives provide access to all messages received by !MC5, even if the aren't listed in in- or outbox anymore. For each message detailed information about its processing status are displayed.

In- and Outbox can also be used to manually process EDI messages. Messages can be imported to both in- and outbox and afterwards get e.g. printed, exported or sent.

## Messages in the inbox

The inbox lists EDI messages received by !MC5.




The message lists displays the following details:

**Type** - This column lists the message type and processing status of received messages. If a received file contains more than one EDI message, FILE will be displayed as type and the contained messages are displayed as child entries. The processing status will be displayed individually for each contained message.

**Status** - The processing status of a message is displayed using different symbols. E.g. printed messages display a printer symbol, exported messages the export symbol. If, during automatic processing, a certain step failed, the respective symbol will be displayed with a red X.

**Date** - Date and time the message was processed first by the module EDI.

**Partner** - The partner, from whom the message was received.

**Transmission number** - Transmission number of the EDI message as extracted from the message. The message type determines which content of the message will be extracted and displayed as transmission number. Usually this value gets extracted from header segments.

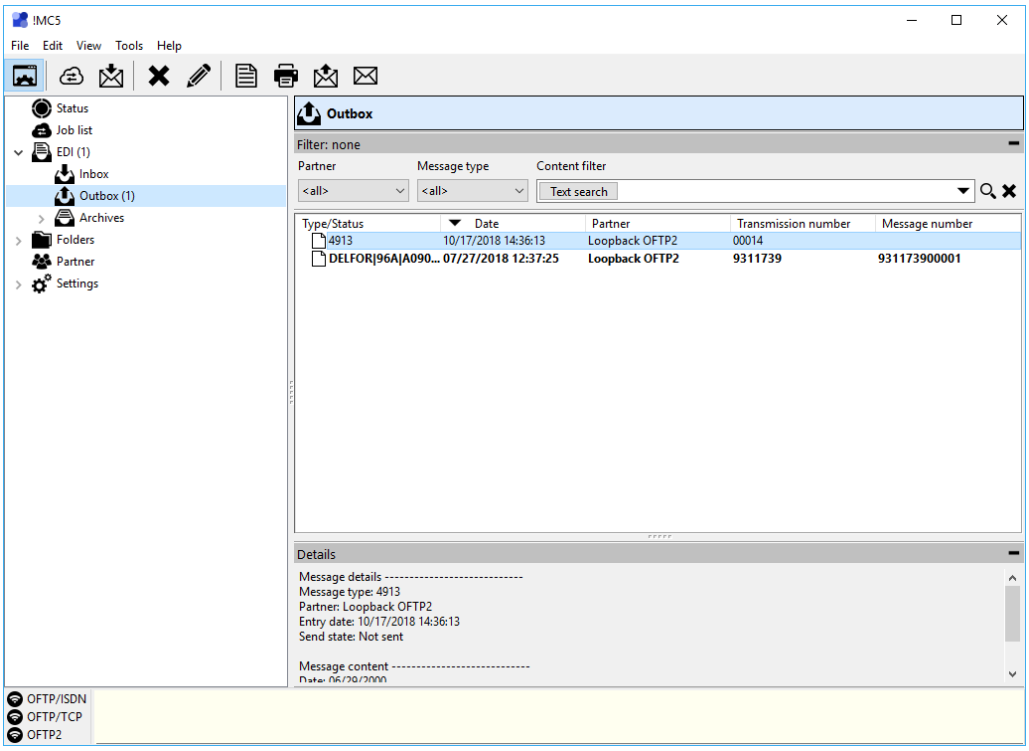
**Message number** - Message number of the EDI message as extracted from the message. The message type determines which content of the message will be extracted and displayed as message number. Usually this value gets extracted from header segments.

The *Details* (below the message list) show extended information for the selected message. These include exact dates and times certain processing steps were last executed as well as additional information extracted from the message.

Messages can't get sent from the inbox. Only messages in the outbox can get sent.

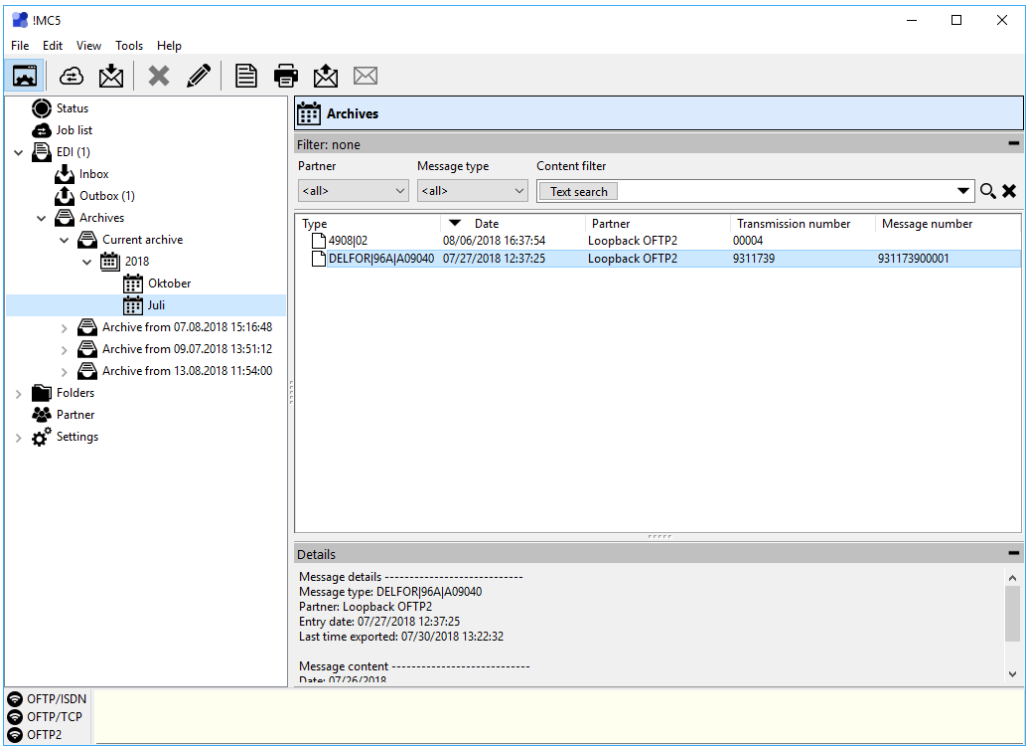
## Messages in the outbox

The outbox displays messages that are to be sent to partners or have already been sent.




The message list of the outbox displays the same details, as the inbox, except for additional status symbols. Messages for which a sending job was successfully created are marked with an envelope and when an EERP is received for the sent file, a ticket symbol is displayed. Further details for the status of a messages can be found in the details section below the message list.

## Archives

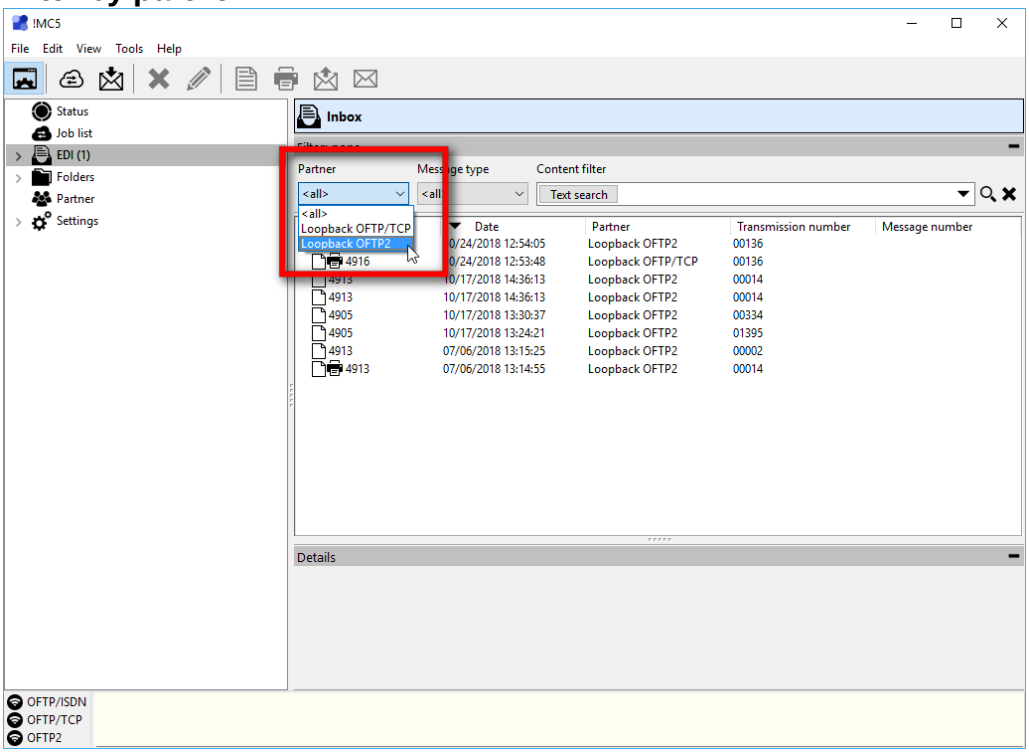



All messages processed by the module EDI automatically get archived. Entries in the in- or outbox are only references to these archived messages. Deleting a message from in- or outbox only deletes that reference, not the archived message itself. The actual message can still be accessed and processed via the archives.

### 3.3.2.1 Filter displayed messages

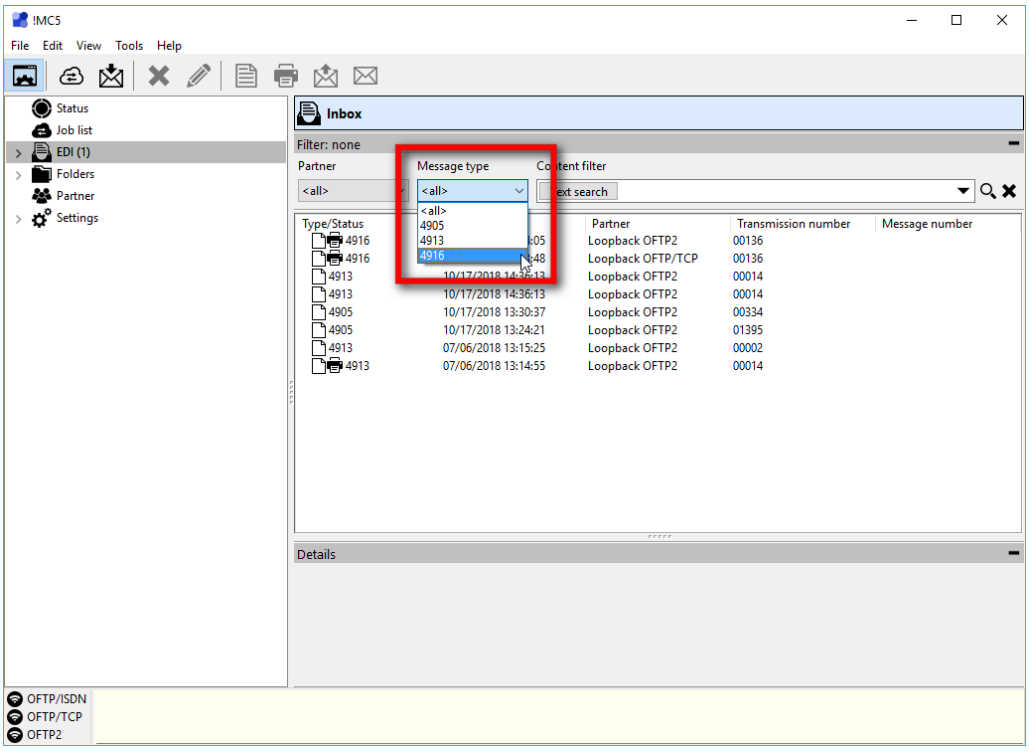
If in-, outbox or archives contain many messages it can be helpful to filter the displayed messages by certain criteria, so you can find a specific message faster. All message lists can be sorted by column. To do so, simply click the column you want to sort the list by. Additionally the displayed messages can be filtered by partner, message type an message content. If any filter is applied, only those messages matching the selected criteria are being displayed. All the types of filter criteria can be combined.

#### Filter by partner



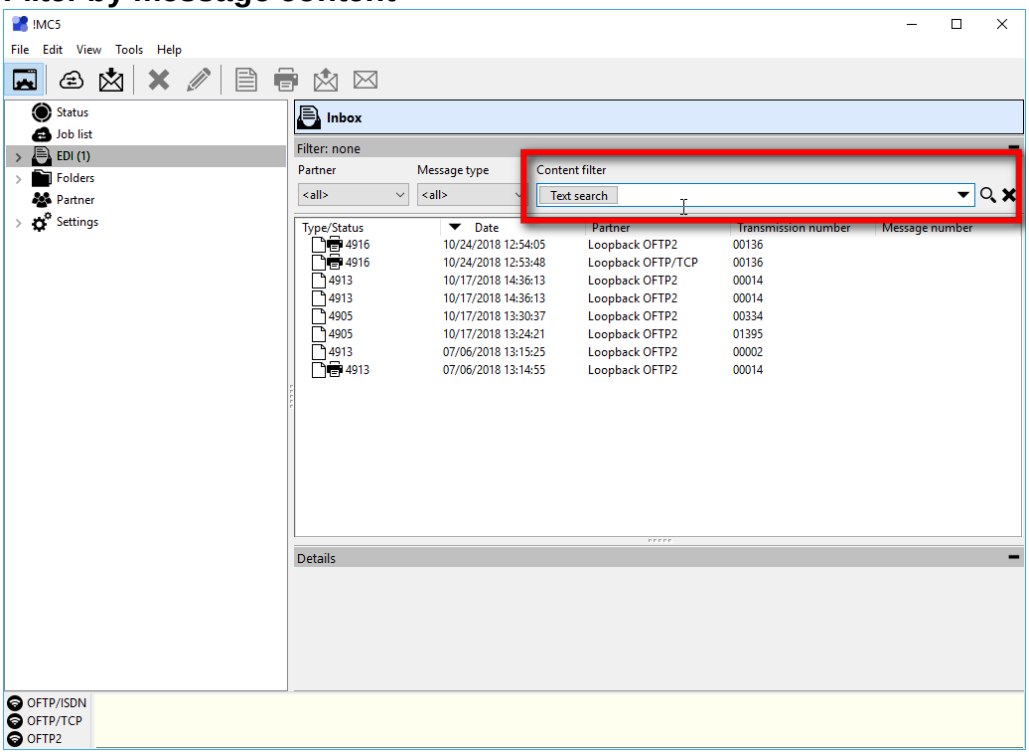

Using the list Partner you can restrict the displayed messages to those that were received or sent to a specific partner. Further filters will only apply to those messages listed which might improve the performance of those filters. Only those partners are listed, of which any messages are present in the in-, outbox or archive selected.

#### Filter by message type




Using the list Message type you can restrict the displayed messages matching a certain message type. Further filters will only apply to those messages listed which might improve the performance of those filters. Only those message types are listed, of which any messages are present in the in-, outbox or archive selected.

## Filter by message content

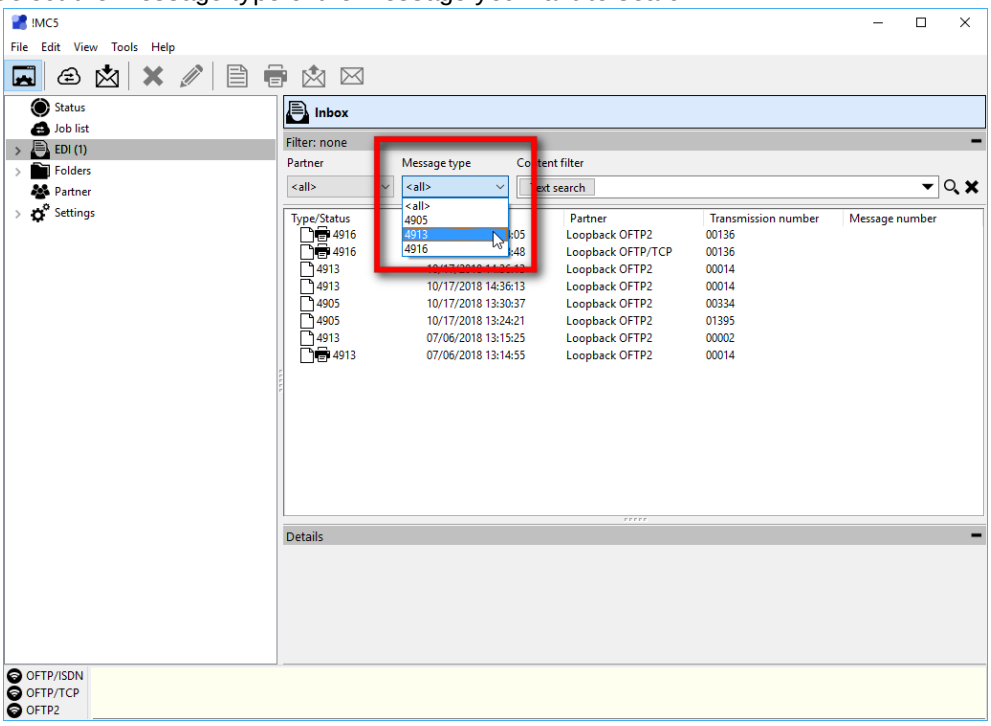



To filter by message content two methods are available: The full text search and the search for text only in a certain field of a message. When using text search the whole message text of all displayed messages is searched for the text entered in the edit field.

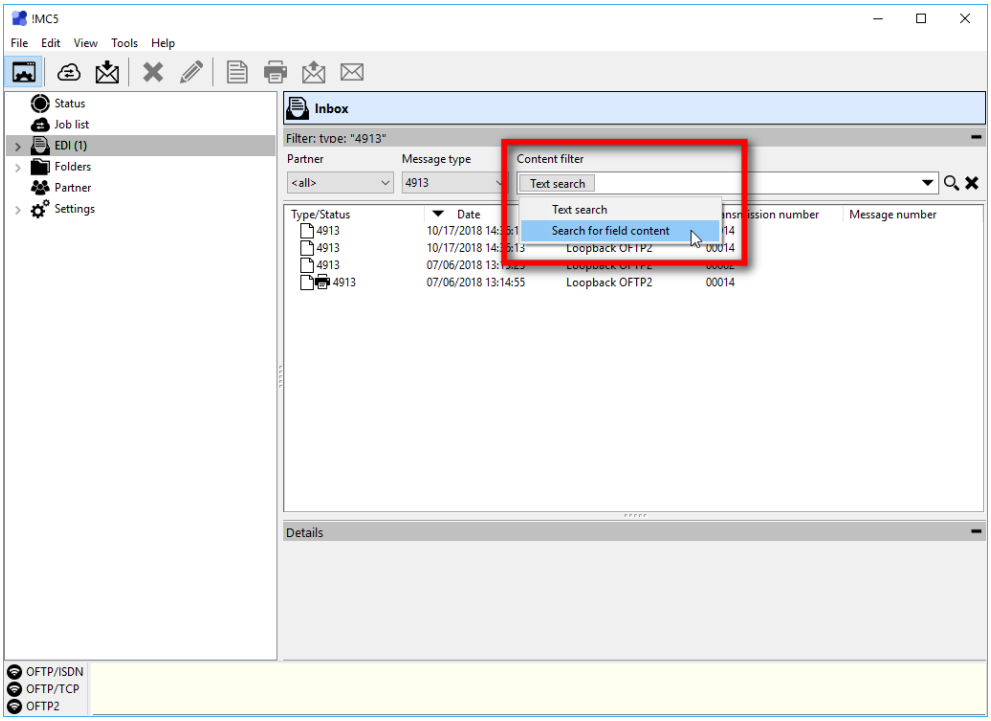
To search, enter a search text and then click the magnifier button next to the edit field. To clear the current content filter click the X button next to the magnifier.

To search for text contained in a specific field of a message you can use the *Search for field content*. For this a message type filter has to be selected:

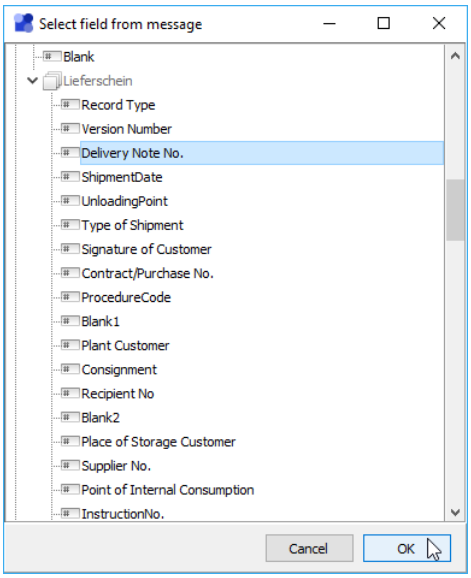
**1** Select the message type of the message you want to search in.



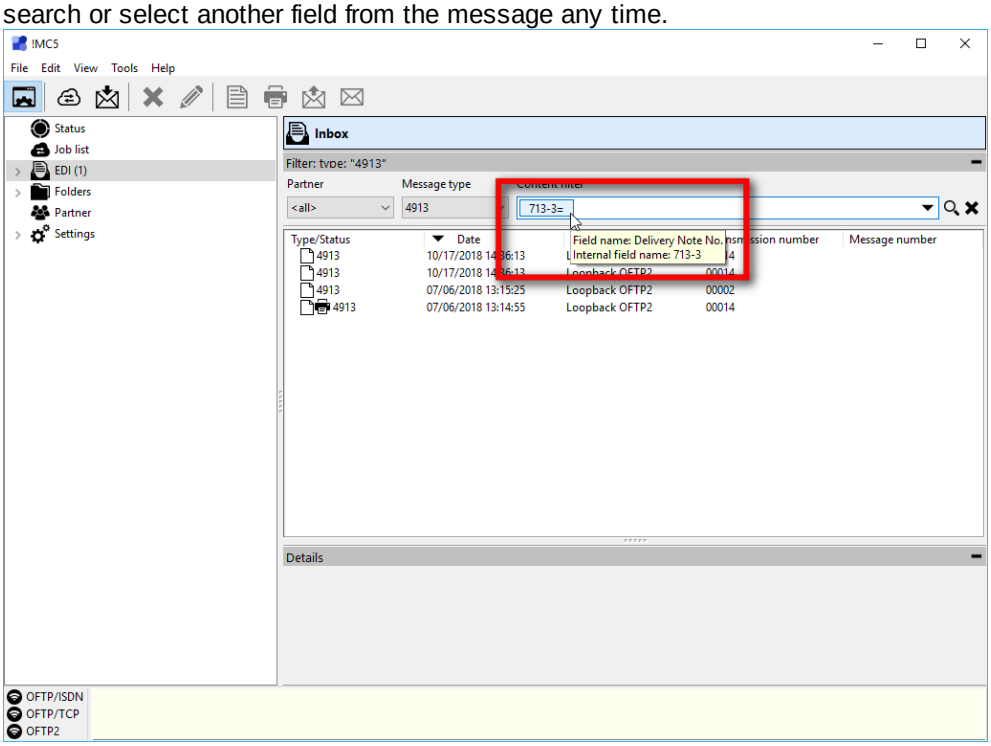

**2** Then click the button inside the content filter edit field and select the option Search for field content.



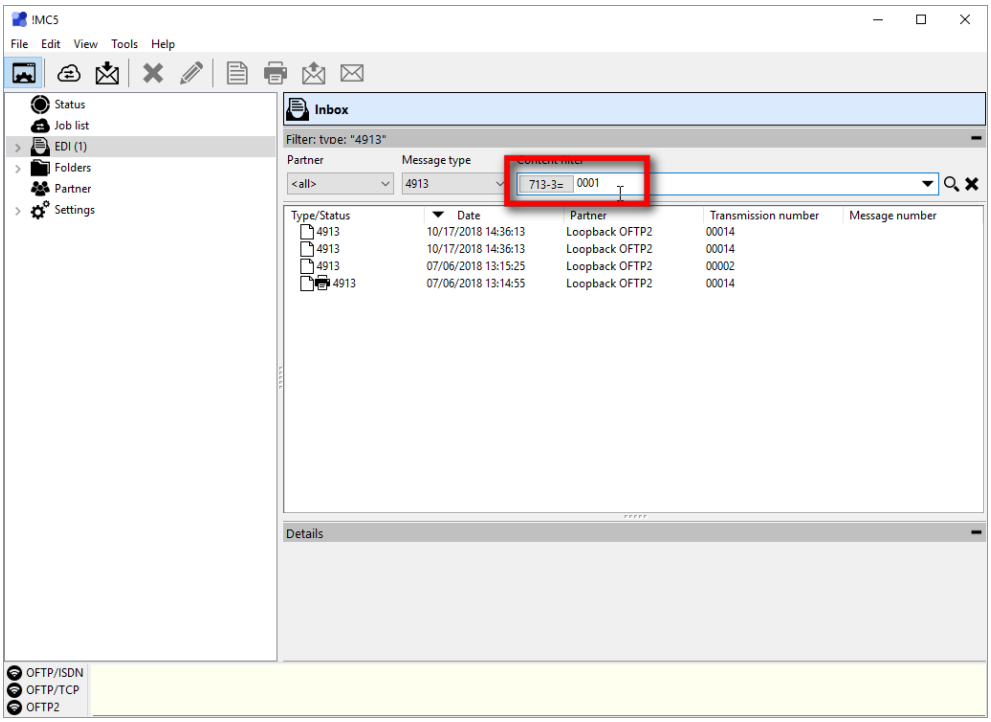

**3** Select the field you want to search in and click OK.



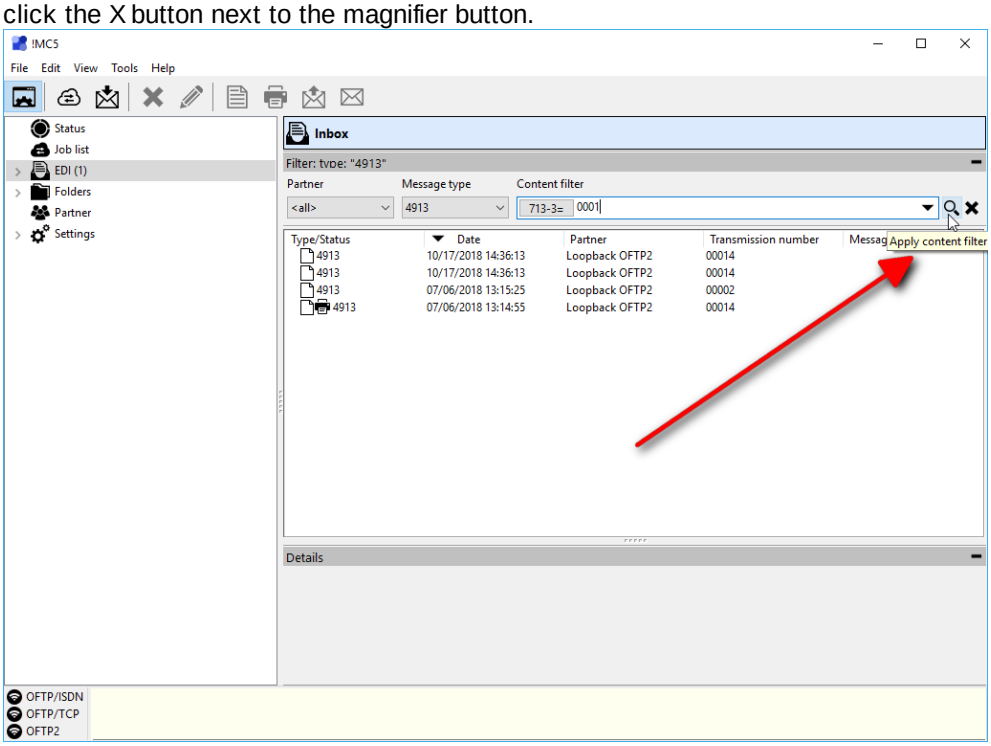

**4** The button inside the edit field now shows the fields internal name. If you hover the mouse cursor over the button, the full field name and the full internal name will be displayed as hint. By clicking the button again you can swith back to the simple text search or select another field from the message any time.




**5** Enter the text you want to search for into the Content filter edit field.




**6** Apply the filter by clicking the magnifier button (Apply content filter) next to the edit field. Now only those messages that contain the entered value in any occurrence of the selected field will be displayed. So if you entered e.g. 1 as value, all those messages will be displayed in which on occurrence the selected fields value contains a 1. Filtering might take a while if many messages have to be searched. To reset the filter click the X button next to the magnifier button.




!MC5 saves for each message type your last ten content filters. Those saved filters can be selected using the drop down menu of the edit field. If you select a saved filter it wont be applied automatically, so you have to click the magnifier button to apply the selected filter.

## 3.4 ENGDAT

ENGDAT is the abbreviation of ***Eng****ineering* ***Dat****a.* The ENGDAT format is widely used as a standard form for transmissions of technical data. It is not used for commercial data.

Currently there are three versions of ENGDAT available. They are not compatible to each other. All three version of ENGDAT are supported by !MC5. Because of the lack of compatibility both parties have to agree to one version. Version 1 is still the most common version of ENGDAT.

!MC5 supports the receiving of files in ENGDAT format as well as the sending of files in this format.

### The ENGDAT-format

ENGDAT can be seen as an envelope for files. Additional information regarding sender, receiver, file type, etc. can be included in the transmission. ENGDAT uses a naming convention for files which identifies each set of files uniquely. A small file is added to the set of files which is called the ENGDAT abstract file. It contains the additional information. Because ENGDAT includes several mechanisms for forwarding major companies use it to route the file internally. This enables you to address a single employee directly.

### Example

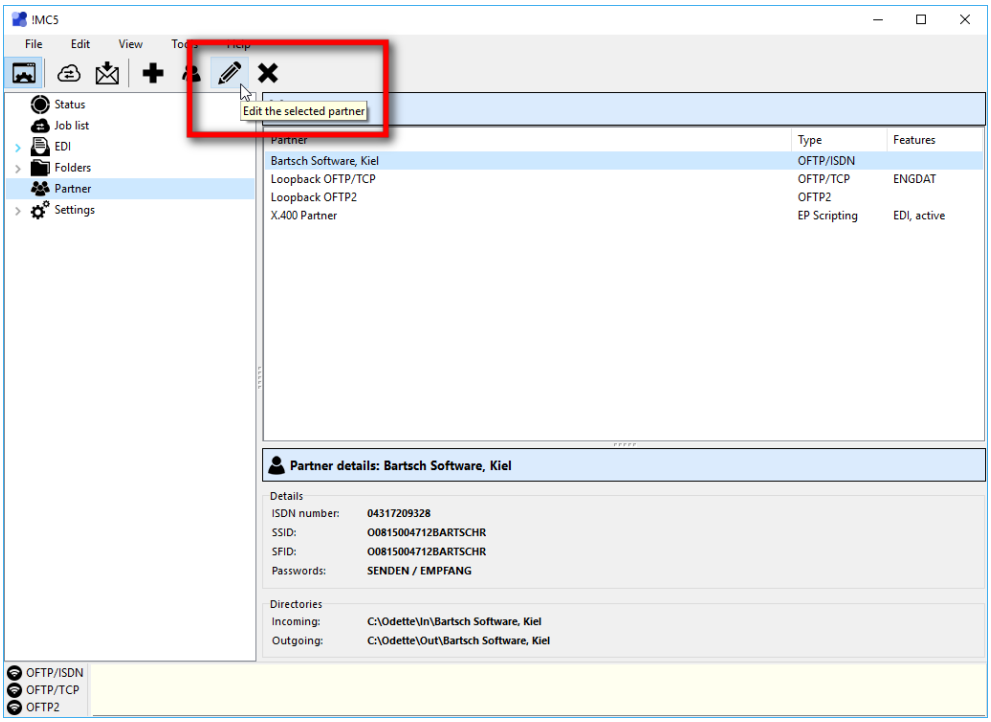
*ENG0408121635540000003001*
*ENG0408121635540000003002*
*ENG0408121635540000003003*

In this example two user files (...*002* and ..*003*) are sent with ENGDAT. The first file (*ENG0408121635540000003001*) contains only information about sender, receiver and the two files. The naming of the files indicates ENGDAT which needs further processing. The filenames also a include a timestamp which identifies this set of files uniquely. In this example it is August, 12th 2004, 16:35:54 (...*040821163554...*).

### 3.4.1 Sending ENGDAT files

A partner account can be setup to send all files in ENGDAT format. Please proceed as follows:

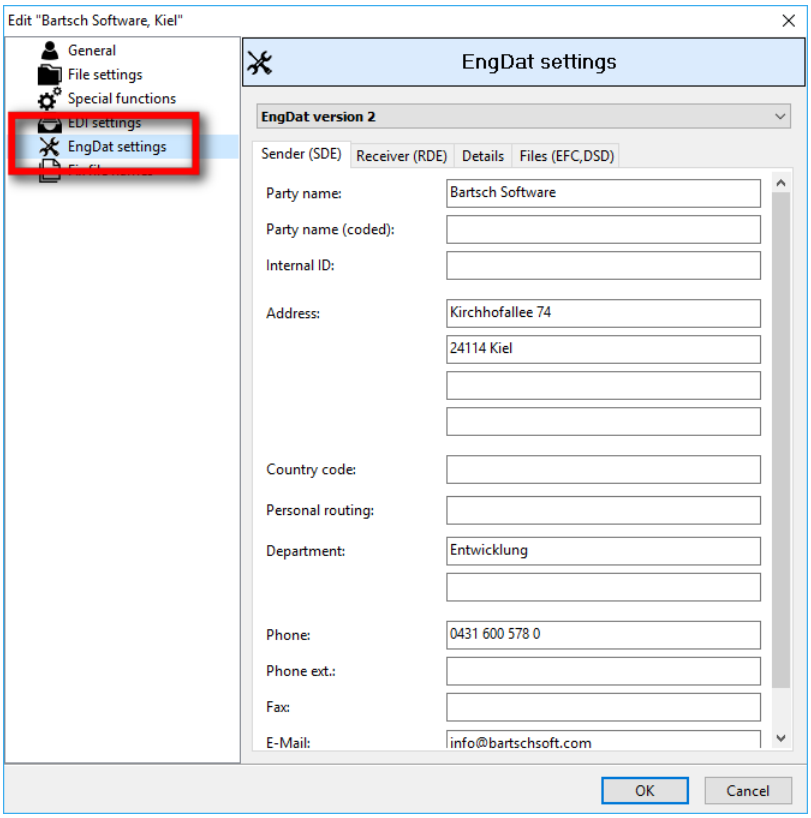
1. Start !MC5 and select the *Partner* section in the navigation tree.
2. Select the partner account by double-clicking it or by marking it and then by clicking the button *Edit*.




**3** Select *ENGDAT settings* in the edit window, then select the ENGDAT version. This selection will activate ENGDAT for the account. In order to deactivate it simply choose *No ENGDAT* as version. The text fields can now be filled as needed. If your partner needs some specific fields to be filled he must give you the according information.

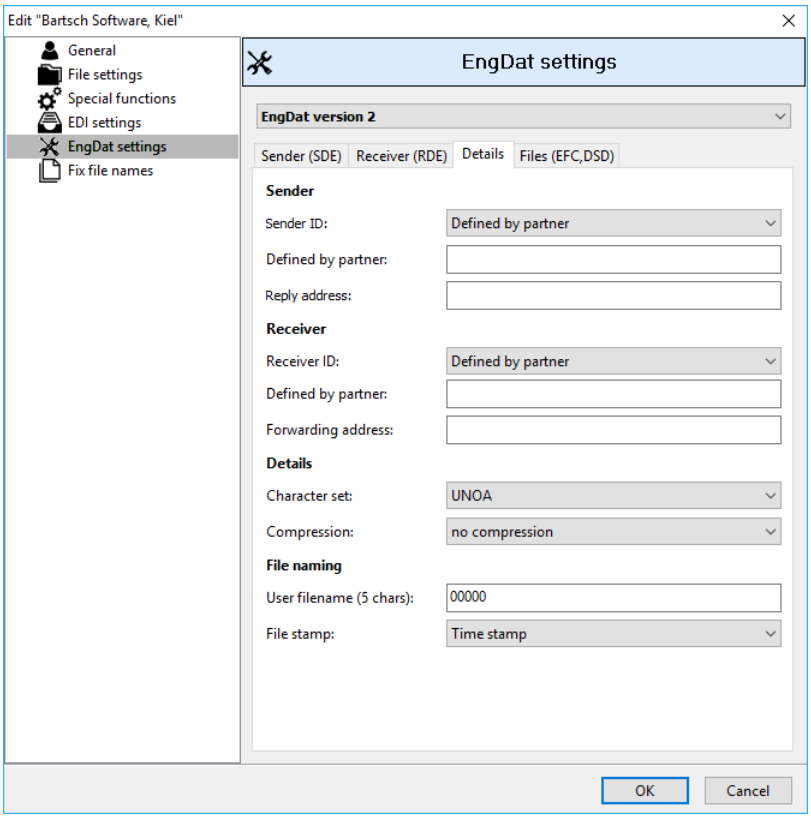
The settings made here are used as default for all outgoing transmissions in ENGDAT format. They can be changed during the creation of a new sending job.

**4** Enter your own company description on the page *Sender*. The data entered here will also be used as default when another ENGDAT account is created.

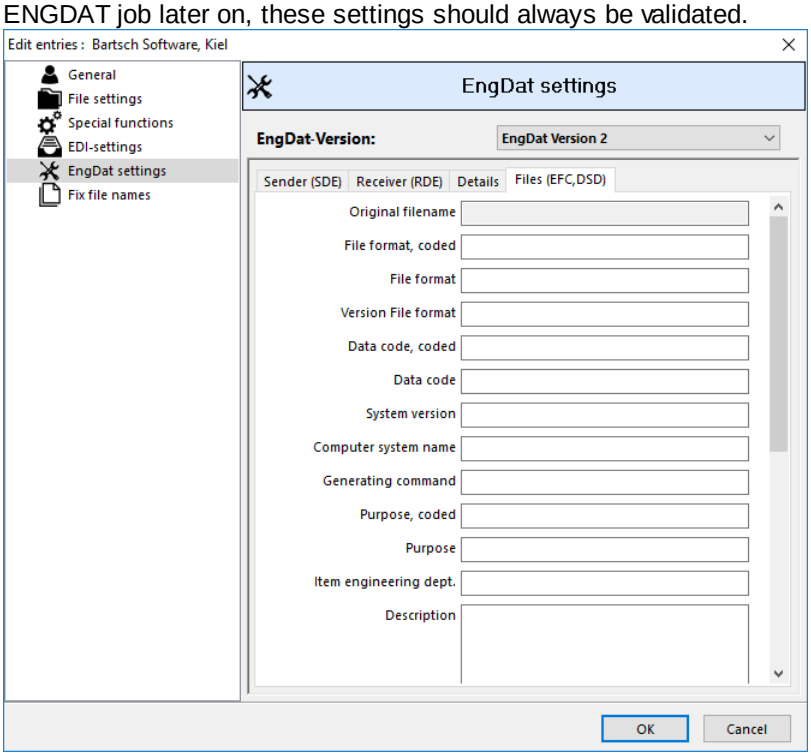



**5** The page *Receiver* contains a description of the partner company. The fields here are similar to those on the page *Sender*. If the partner uses data from this page for routing purposes enter the data exactly as given.

**6** Enter the user defined part of the filename on the page *Details*. It always consists of five characters and is often used for forwarding. In this case the partner must provide you with exact codes for this field. The recommended character set is *UNOC*, which is identical to the standard Windows character set. For connections with German companies always use *Time stamp* as *File stamp* (VDA recommendation 4951). The Galia standard uses a counter instead of the time stamp.




**7** Use the page *Files* to enter default settings for transmitted files. When creating an ENGDAT job later on, these settings should always be validated.

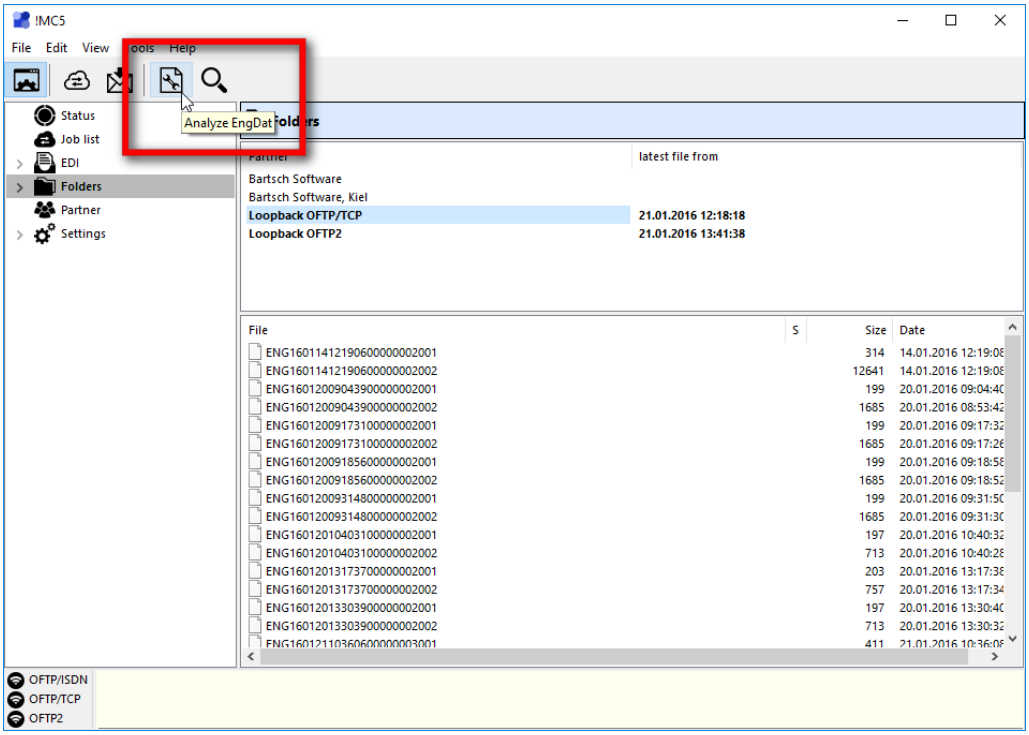



**8** Save the setting by clicking *OK*. From this point on all files for this partner will be transmitted only in ENGDAT format. See also Sending files.

### 3.4.2 Receiving ENGDAT files

ENGDAT files are received the same as regular files. Because ENGDAT provides additional information there are further processing steps available. The ENGDAT information (from the ENGDAT abstract) can be shown in a readable form and files can be brought back into their original state prior to sending.

Open the page *Folders* in the main window of !MC5. If there are files available in ENGDAT format the button *Evaluate ENGDAT* will be enabled. Click this button to open an editor window containing the ENGDAT information. If no file is selected in the list the editor will be opened for the first ENGDAT file from the list.



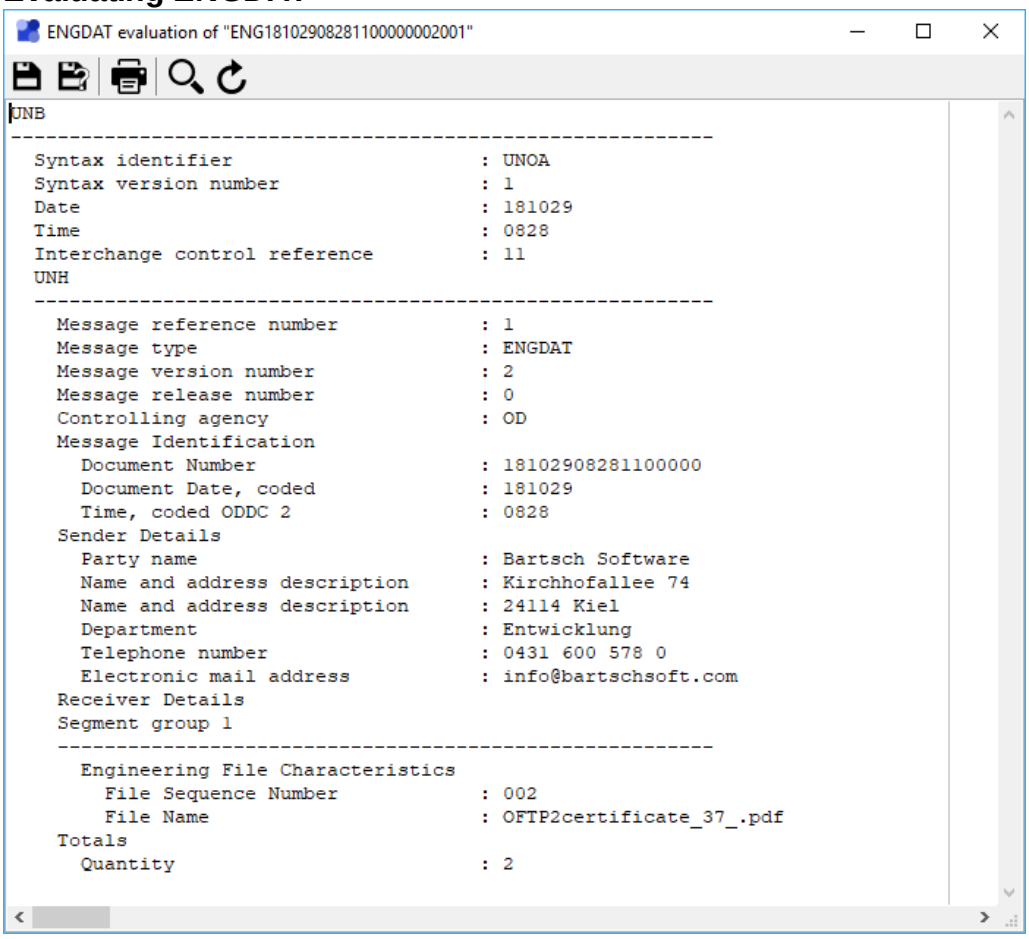

The editor can also be opened by double-clicking on an ENGDAT entry in the list.

**The ENGDAT abstract file is needed for the evaluation process**

Some obsolete software uses only the ENGDAT naming-convention without supplying an ENGDAT abstract file. By definition this is no valid ENGDAT transmission. !MC5 cannot extract additional information from the abstract if it is not available. Because the abstract also contains the original filenames, the files cannot renamed back to their original names. Valid ENGDAT always consists of at least two files where the first one is always the ENGDAT abstract.

### 3.4.2.1 Evaluating ENGDAT

**Evaluating ENGDAT**




The functions of *Evaluate ENGDAT* are similar to those of a common text editor. The information can be saved and printed.

The ENGDAT abstract also contains the original filenames. The editor window provides two functions to restore the ENGDAT files to their original names. Click the button *Extract all* or *Extract as* to bring the files back to their original state. The first function will rename files, decompress them (if they were compressed with GZip) and stores them into the same folder. If a file already exists a number will be added to the new filename. The function *Extract as* provides a save-dialog for each file in the ENGDAT transmission. Filename and location can be chosen in this dialog.

The following functions are available:

**Extract all files** - Extract all files of the corresponding ENGDAT transmission, i.e. renaming them to their original file name and decompressing them if necessary. The extracted files will be saved to the incoming directory of the partner. Naming conflicts will result in counters added to the file names.

**Extract files as** - The same as Extract all files but save folder and file names are selectable for each file.

**Print** - Print the shown text.

**Search** - Search in text.

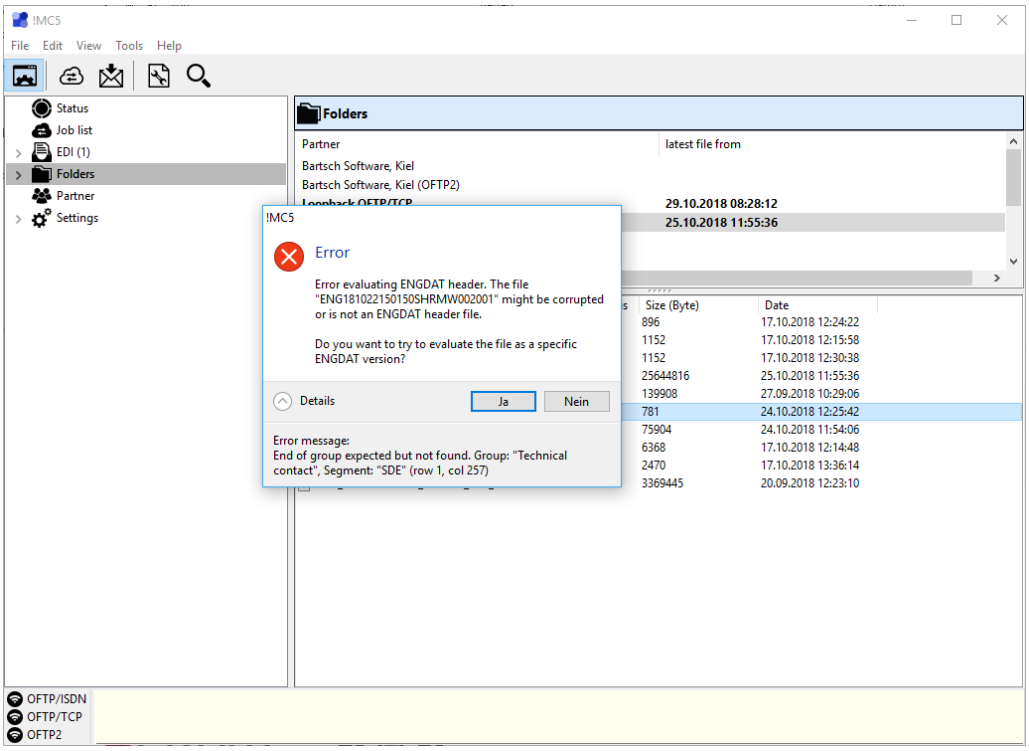
**Replace** - Search and replace parts of the text.

Using the context menu the following additional functions are available:

**Copy** - Copies the selected text to the windows clipboard.
**Cut** - Copies the selected text to the windows clipboard and deletes the selection from the text.
**Paste** - Paste contents from clipboard to the text. The text will be inserted at the current cursor position.

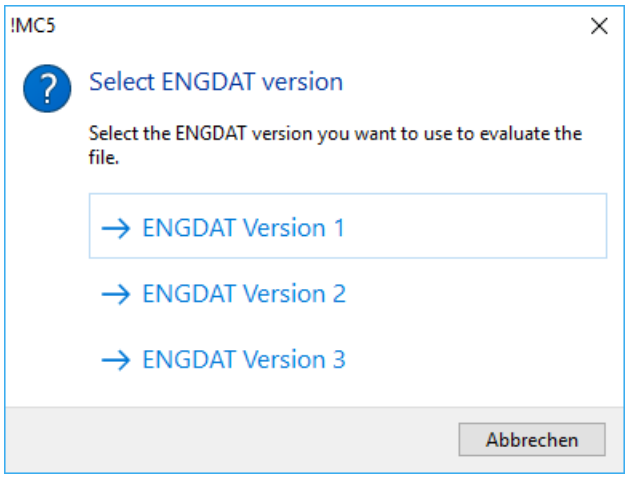
## Evaluate ENGDA files using a specific ENGDAT version

Some times partners may send you ENGDAT files which can't be read by !MC5 due to errors. In many cases these errors are cause by a wrong ENGDAT version identifier used in the file. Usually !MC5 tries to determine the used version automatically and tries to evaluate the file using the corresponding version.




**Trying to evaluate a corrupted ENGDAT file.**

If this fails, you can try to evaulate the file using a specific ENGDAT version. This may help, eg. when your partner sends a file using the version 1 identifier, but uses fields from version 2 inside the message.



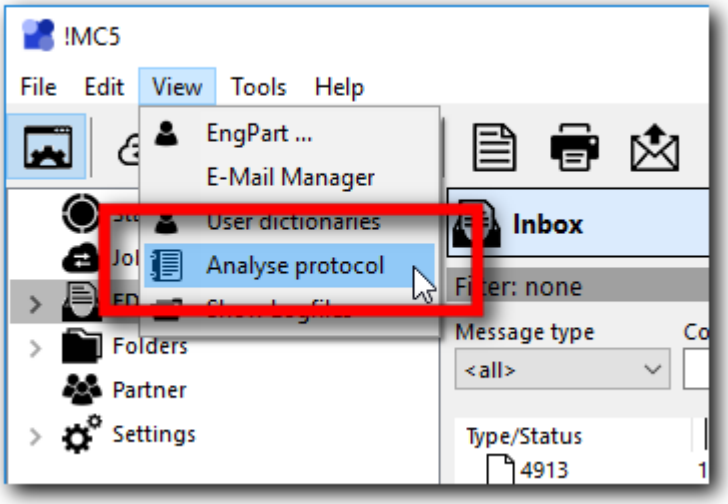

**Repeat ENGDAT evaluation using a specific version.**

This isn't guaranteed to work, as the file might be acutally corrupted or not even an ENGDAT file.

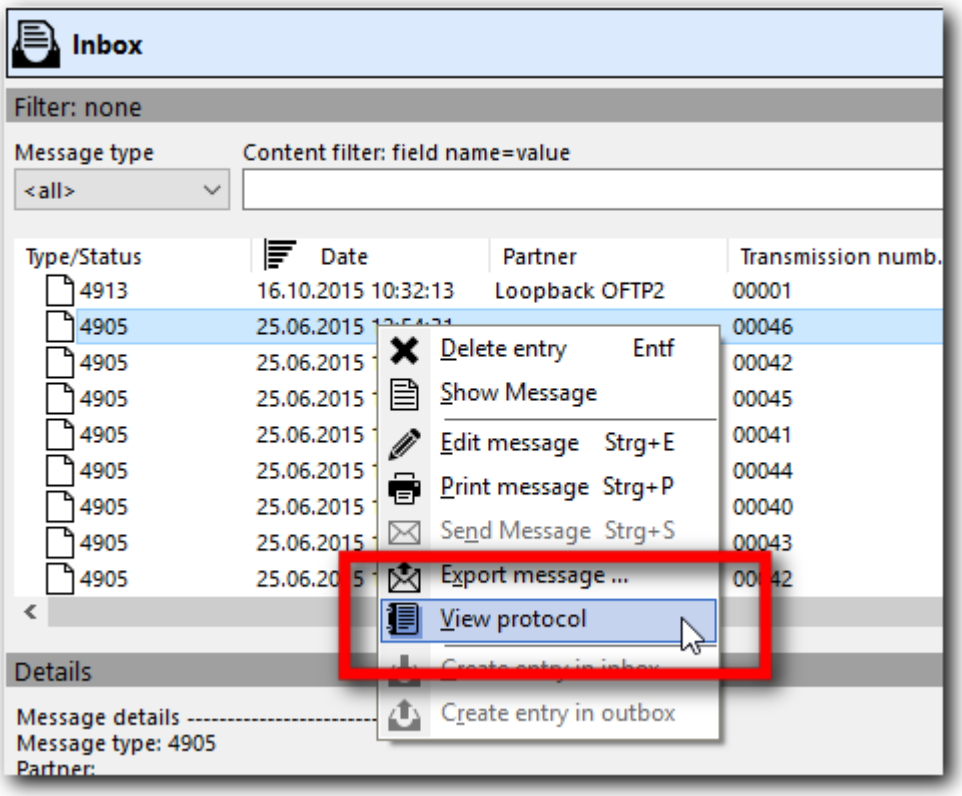
## 3.5 Protocol Analyser

Information about all processing steps of !MC5 are kept in several detailed protocols. The most current events can be found in the main screen of !MC5 by selecting the *Status* section. The complete log-file can be opened directly or be analyzed with the help of the external *Protocol Analyser*. It can be started over the main menu of !MC5 *View / Analyze protocol*.

**Other log files**
!MC5 creates various protocols, depending on current settings. These logs are all stored in the sub folder *Log* in the data folder of !MC5. The folder can be opened in Windows Explorer by using the main menu *Tools / Show Log-files*.



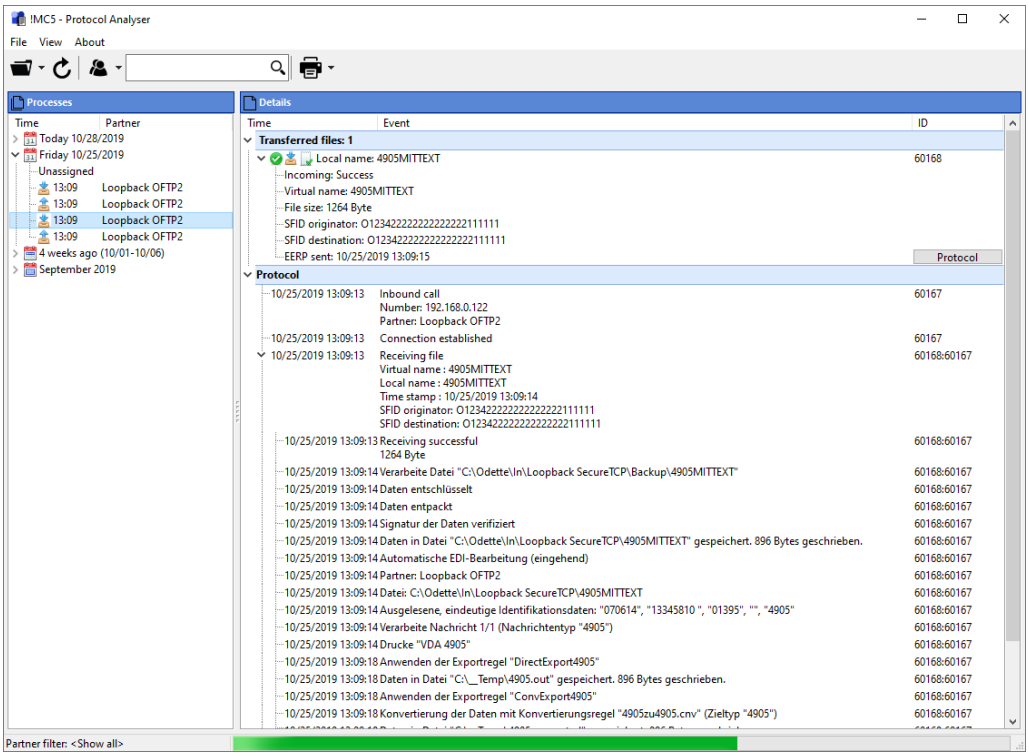

When using the EDI Add-On the *Protocol Analyser* can be started, so that only log entries for a specific EDI message are shown: Right click an entry in the EDI in- or out-box, and select the function *View protocol*. This starts the *Protocol Analyser* with a filter set to the responding messages internal ID.




The function *Delete Filter* will remove the filter that was set at startup and all entries will become visible.

### 3.5.1 Functions

The Protocol Analyser provides easy access to the !MC5 log. Log entries can be filtered by partner or internal process ID. It is also possible to print the protocol of a single process sequence.




The Protocol Analyser is divided into two sections: The left tree contains all processing sequences sorted by date and time. All filter functions will affect this view. If for example a partner filter is set, the tree view will only contain processes concerning this particular partner. By choosing an entry of the tree view the protocol of the corresponding messages will be displayed in detail on the right side.

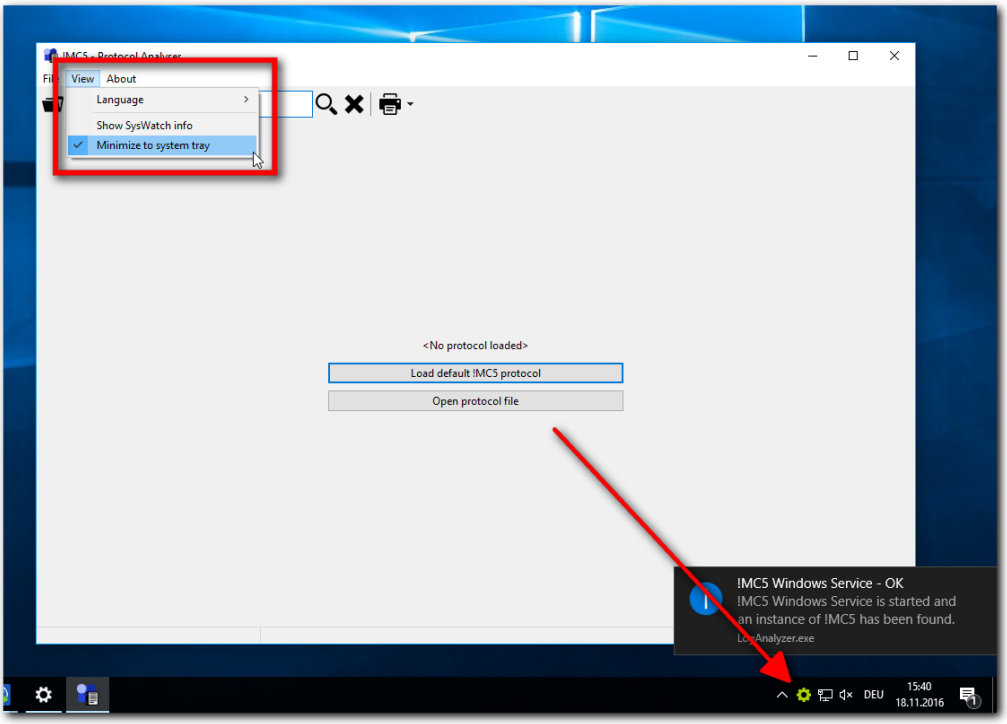
The following functions are available in the Protocol Analyser:

- ***Open protocol*** - Opens an !MC5 log file. During startup Protocol Analyser will automatically load the current log. Older protocols are stored in the backup sub folder.
- ***Refresh protocol*** - Refreshes the current view. Only new messages will be appended to the current view. This function can be used as a simple monitor for !MC5. This can be useful e.g. when using the Windows-Service Add-On.
- ***Partner-Filter*** - This function filters the entries of the tree view by a given partner name. The partner name can be chosen from a drop-down list. The entry *<Show All>* will reset the view and all entries will become visible again.
- ***File / ID-Filter*** - With the file and internal ID filter it is possible to extract protocols for given files or protocol IDs. Enter a file name into the edit field *Filter value* and press then button *Filter entries*. This will hide all entries from the tree view in which the given file name does not occur.
- ***Print Detail*** - Prints the text from the detail view. This function can be used to document the sending of a specific EDI message.

- ***Save Detail*** - Saves the detail view into a file as text.

### 3.5.2 Windows Service Monitor

If the add on Windows Service is licensed and the service is installed (see Installing Windows Service), the Protocol Analyser can be used to monitor the service state. The default !MC5 protocol isn't loaded automatically at startup (except when started via EDI in- or outbox) and an icon showing the service state is displayed in the system tray. Additionally an option to minimize the Protocol Analyser to the system tray is available under *View* in the main menu.




A service status change will get displayed as message and using the system tray icon color:

- ***Red***: The Windows Service is installed, but not started.
- ***Yellow***: The service is started but no running instance of !MC5 is found.
- ***Green:*** Service and !MC5 are both started.

Once minimized to the system tray, to restore the Protocol Analysers main window use the system tray icon context menu or double click the icon.

# Advanced usage

# 4 Advanced usage

## 4.1 Automation

Enter topic text here.

### 4.1.1 Automatic file transmission

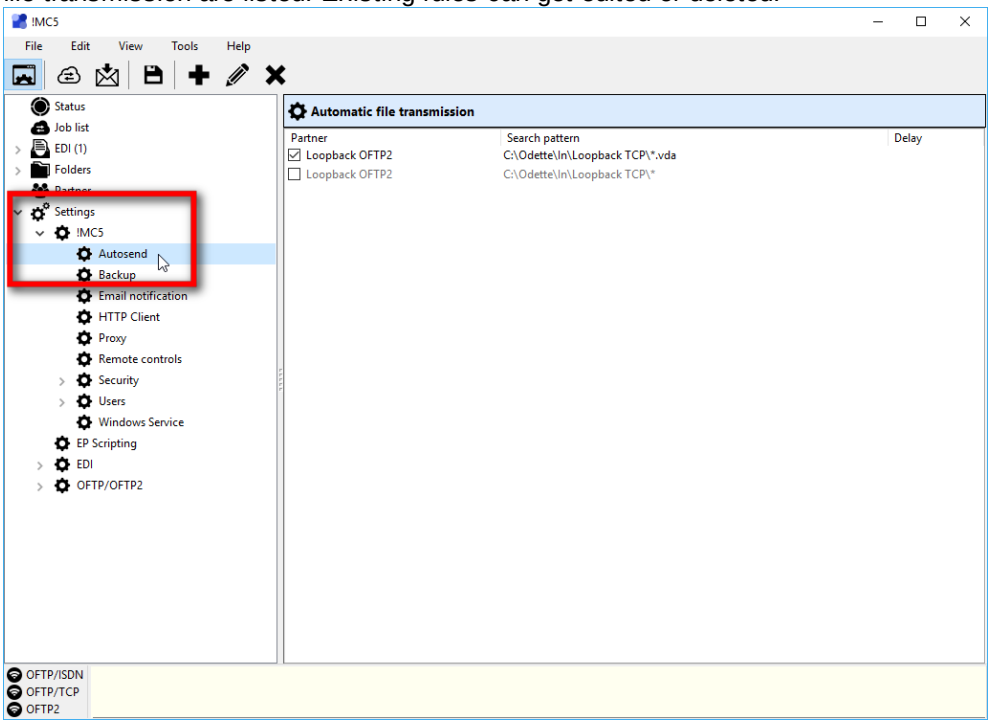
!MC5 uses a rule based system for automated sending of files, i.e. without user interaction. Each rule defines a folder and a file pattern to control which files will be sent. !MC5 checks in regular intervals for new files. Matching will be sent to the partner specified in the rule. File will be processed according to the partner settings.

> **Use EDI import/export for EDI messages!**
> When sending EDI files using the Automatic file transfer, those messages will **not** be processed by the module EDI. For EDI processing and the messages to appar in the EDI outbox, use the automatic import of the module EDI.

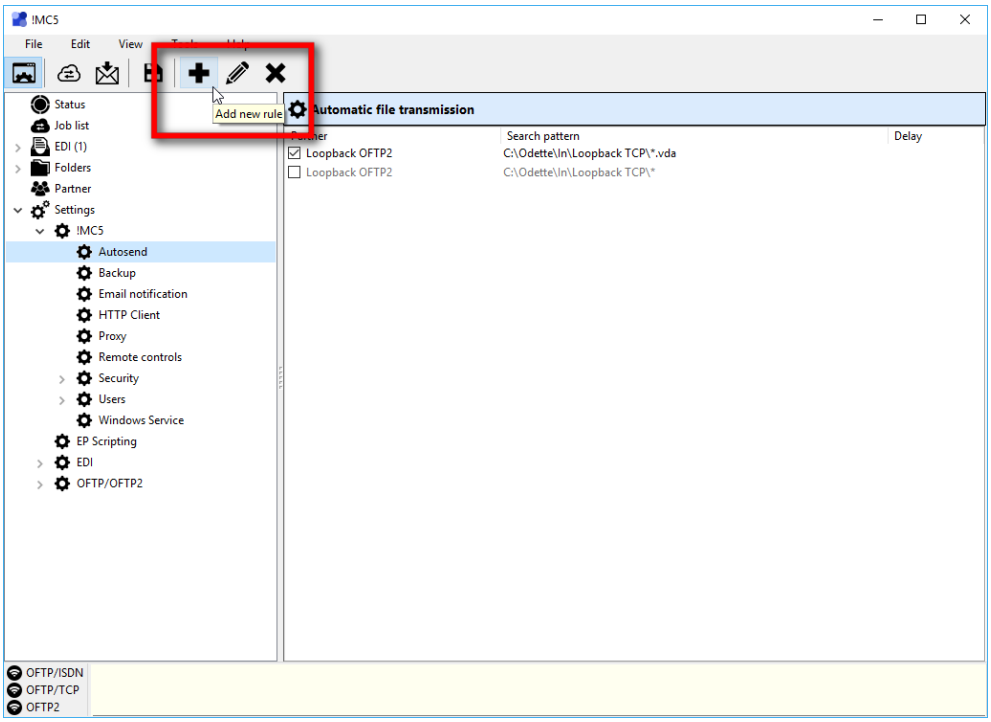
The list of rules for automatic file transmission is sorted by partner name. The second column of the list shows the concatenated search path and search pattern.

To add a new rule for automatic file transmission proceed as follows:

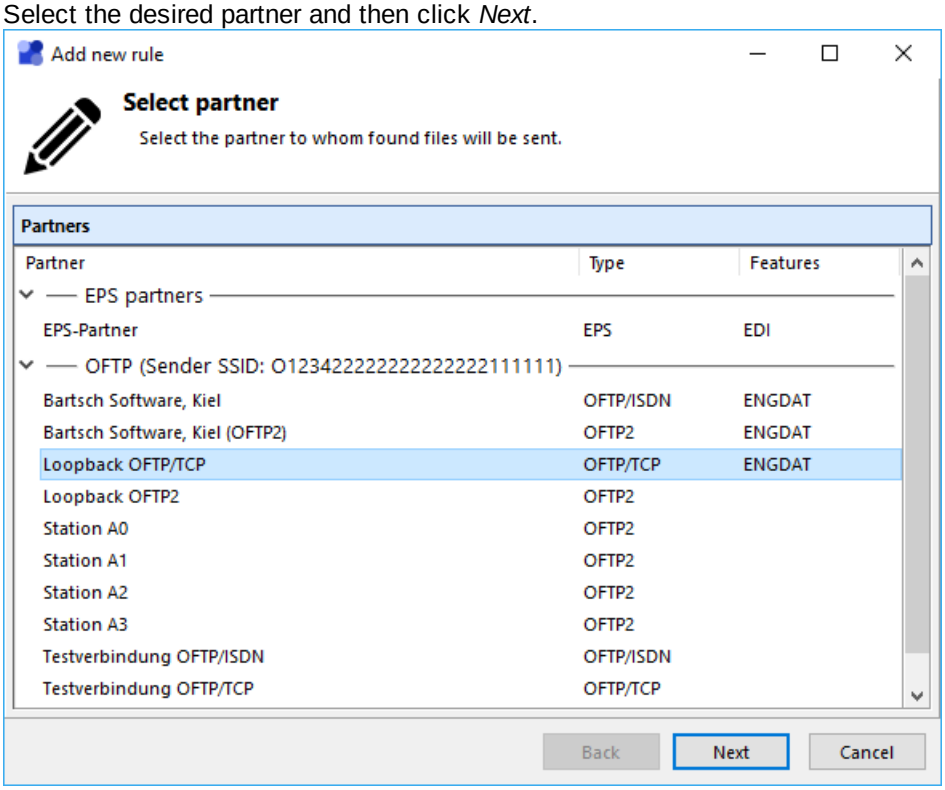
1 In the *Settings* select the Node *!MC5 / Autosend*. On this page, all rules for automatic file transmission are listed. Existing rules can get edited or deleted.



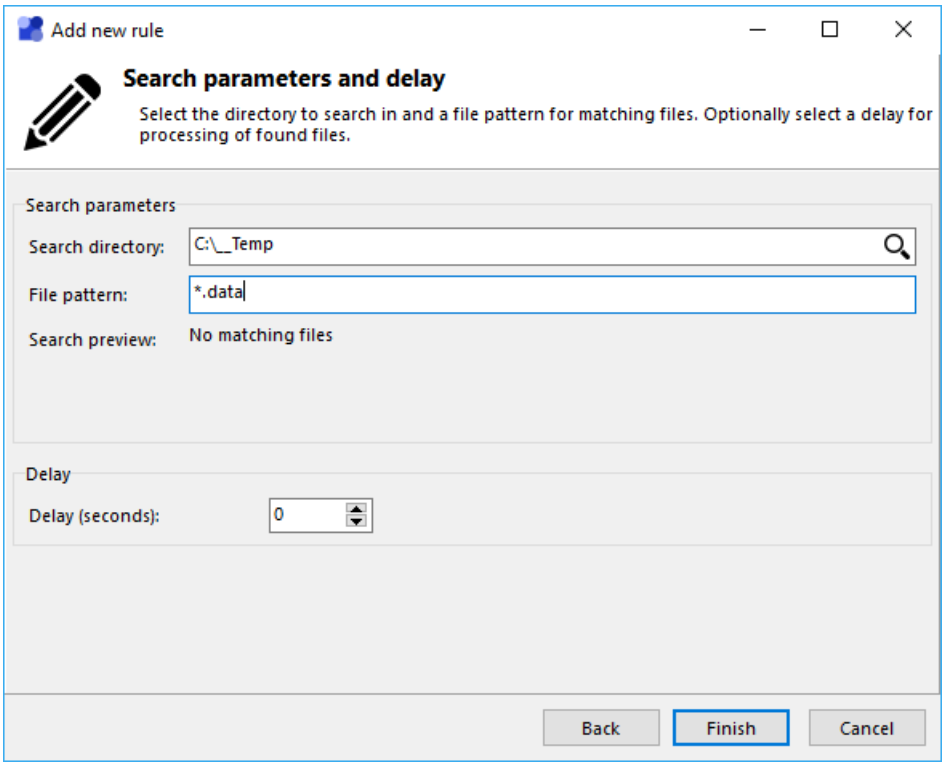

2 To add a new rule click the button *Add new rule* in the top tool bar.




**3** First you have to select the partner to whom matching files will get sent. Be advised that files being sent using the automatic file transmission won't get processed by the module EDI. Also sending data in ENGDAT or EngPart format isn't possible, as this requires user interaction for each transmission.
Select the desired partner and then click *Next*.




**4** Next select the directory, in which !MC5 is to search for new files. Only files inside this folder (and matching the search pattern) will get sent. Subdirectories won't get searched for files.




**Don't use outgoing directories for automatic file transmission**

Folders specified as outgoing directory for an OFTP/OFTP2 partner can't be used as search directory for automatic file transmission rules, as this could disrupt file processing. If you try to select a folder as search path, that is already being used as outgoing folder for any partner an error message will be displayed. Best practise is to use a separate folder structure for automatic file transmissions, similar to that of !MC5 default incoming/outgoing folder structure.

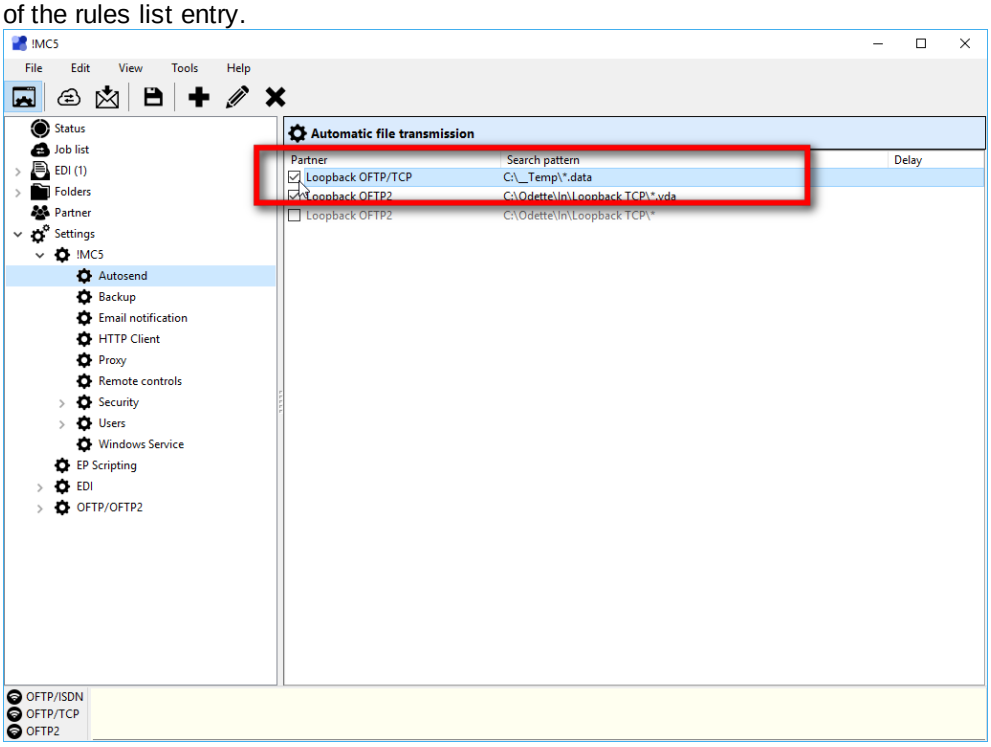
**5** Specify a search pattern which files have to match for the rule to apply to them. The usual windows search patterns can be used: E.g. use "*" to match any file inside the search path (**without** quotes!), "**.ext*" for only files having the extension "*.ext*", or "*BARTSCH*.ext*" for files beginning with "*BARTSCH*" and ending with "*.ext*". Search patterns are case insensitive! If there are matching files in the search directory, they will be displayed under *Search preview*.

All files matching the pattern "*~*.job*" will be ignored, as those were used for control in legacy versions of !MC5. Control files are no longer supported, so !MC5 ignores those files to prevent unwanted errors.

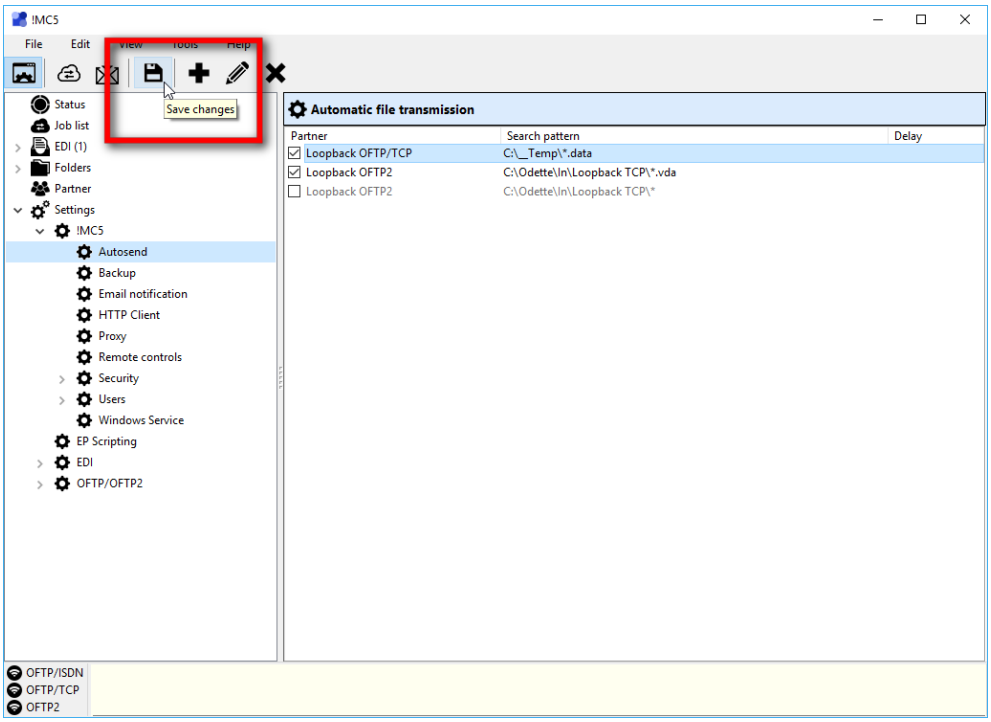
**6** In the box *Delay*, you can enter a delay for the new rule. By default found files will be processed directly. If a delay is specified, processing of the found files is delayed until no new files matching the file pattern are found within the delay period. So if a delay of 60 seconds is used and a matching file is found the file will be processed after 60 seconds, but only if within these 60 seconds no further files matching the search pattern are found. As soon as another matching file is found the delay timer gets reset and starts again from 60 seconds.

**7** Click *Finish* to create the new rule.

**8** New rules are deactivated by default. To enabled the rule check the checkbox in front of the rules list entry.




**9** To finish save your changes by clicking the button *Save changes* in the top tool bar. The new rule will be active from now on.




For editing an existing rule double click its list entry or select its list entry and then click the button *Edit rule* in the tool bar. To delete a rule select its entry and then click *Delete rule*.

### 4.1.2 The automatic file transmission process

!MC5 check in regular intervals the search paths of all active automatic file transmission rules for matching files. If a matching file is found it's being processed as follows:

1. The found file will get moved to the outgoing directory for the specified partner and a new sending job will get created.
2. If any processing is needed, e.g. a character set conversion or encryption, the file will then get moved to the sub folder *Prepare* and a copy of the unprocessed file will get created in the subfolder *Original*. As soon as the preparation is finished the file will be moved back to the outgoing directory.
3. Then the sending jov will get executed. If the file gets sent successfully, it will be moved to the sub folder *Sent*.
4. The file stayes inside this folder until either a EERP or a NERP for that file is received.
5. If a NERP is received, the file get moved to the sub folder Error.
6. If an EERP is received, the file gets moved to the sub folder *Backup*.
7. This concludes the file transmission process.

### 4.1.3 EDI

In order to automate sending and receiving EDI data several steps are necessary, depending on the automation grade.

1. To process any EDI messages for a partner, that partner has to be set up up for EDI processing. read more...

2. For each licensed message type different kinds of general automated processing tasks can be enabled. read more...

3. Received messages can be automatically exported and converted by defining export rules for further processing by inhouse systems. read more...

4. To automatically send data, files can be imported by defining import rules. While importing data can optionally be converted from any inhouse format (e.g. flatfile, CSV, XML) to the required EDI message type (e.g. VDA, EDIFACT, ASC X12) and the get sent to the respective partner. read more...

#### 4.1.3.1 Automatic processing of received data

The Module EDI allows you to automatically process received EDI messages. Messages are processed in three steps: If EDI processing is activated for a partner (Reference / Partner management / EDI settings), all matching received files are tested for contained (licensed) EDI messages. If messages are found, they get added to the EDI inbox of !MC5.

As second step messages get printed if automatic printing is activated in the EDI settings for the respective message type (Reference / EDI / Message types).

In the last step one or more export rules can get applied to the message to convert the message into a format readable by your ERP or to save a copy of the message for archiving purposes.

## Sequence of automatic EDI processing of received messages

1. A file was received and processed (eg. decrypted) by one of !MC5s communication modules (eg. via OFTP2).
2. The file gets passed to the Module EDI if *EDI processing* is activated for the partner (*Partner settings / EDI / Enable EDI processing*) from which the file was received and if the file matches the file pattern specified in the partner settings (*Partner settings / EDI / File mask*).
3. The data gets converted from EBCDIC to ASCII character set, if *EBCDIC* is selected as character set in *Partner settings / EDI / Character set* or if *ASCII + VDA EBCDIC* is selected and the file contains one or more VDA messages using EBCDIC character set.
4. If a filter is selected in *Partner settings / EDI / Filter* that filter is applied to the data. A filter can block, accept or change data.
   a. If the filter blocks the data (*filterRes* = *fiAbort*), the processing is cancelled.
   b. If the filter accepts the data (*filterRes* = *fiUseInput*), the original data is processed.
   c. If the filter changes the data (*filterRes* = *fiUseOutput*), the changed data is processed.
   d. If an error occurs during execution of the filter (either is a fatal error occurs or if *filterRes* is set to *fiError*), processing gets cancelled.
5. !MC5 tries to identify the contained message(s). If identification fails or the identified message type isn't licensed, processing is cancelled.
6. The message is added to the inbox and message archive.

7. The message gets printed, if the option *print messages* (or equivalent) is enabled for the identified message type (*Settings / EDI / Message types / …*).
8. All export rules are tested if they match the received message. Each matching rule (the rule is enabled and both message type and partner match) then gets applied to the data:
   a. !MC5 tests if the target directory for the export exists or can be created (see *f*) and if it is writeable. If this fails, processing of this export rule is cancelled.
   b. The data gets converted, if the option *Convert data* is enabled and a valid conversion is selected.
   c. (Only VDA messages) If the option *insert CR/LF after each record* is enabled for the message type (the target type of the conversion, if *Convert data* is enabled) in *Settings / EDI / Messages types / … / Export options* a carriage return and line feed get inserted after each 128 byte record.
   d. The selected filter is applied, if one is selected. This filter too can accept, block or change the data. If the filter blocks the data or an error occurs the processing of this export rule is cancelled.
   e. The data gets converted to EBCDIC, if *Convert data from ASCII to EBCDIC* is enabled.
   f. The data gets saved to the export file. File name and target directory for the exported file are are created using the *Export file name* settings of the rule, which may contain different placeholders (see Reference / Settings / EDI / Automatic import/export rules / Export rules for further details).
   g. Steps a to f will be repeated for each matching export rule.

**Inbox export status when using multiple export rules**
The export status shown in the inbox only reflects the status of the last export. So if more than one export rules are applied to one message during EDI processing, only the result of the last applied rule is seen here. For detailed information about EDI processing always refer to the protocol.

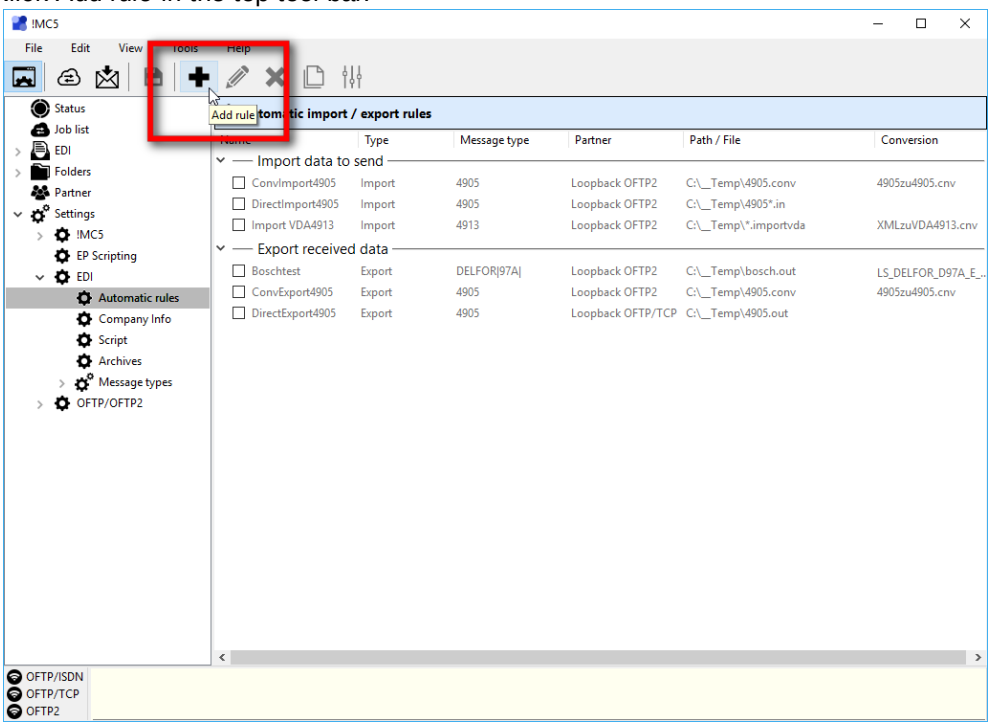
9. Steps 7 and 8 are repeated for each message contained in the data.
10. EDI processing is finished.

### 4.1.3.2 Create a new export rule

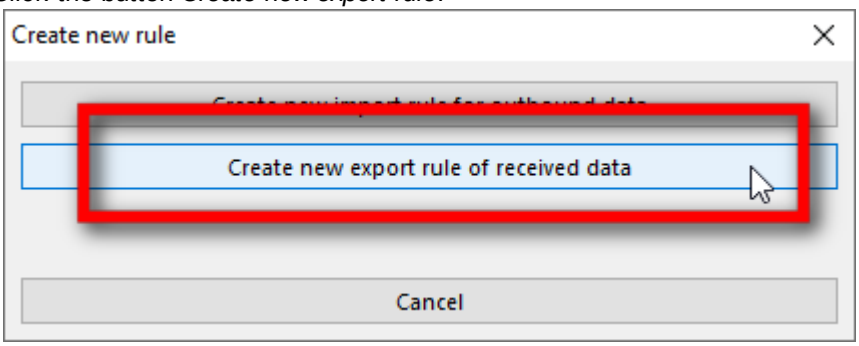
To create a new export rule proceed as follows:

**1** In the *Settings* section open *EDI / Automatic Rules*.

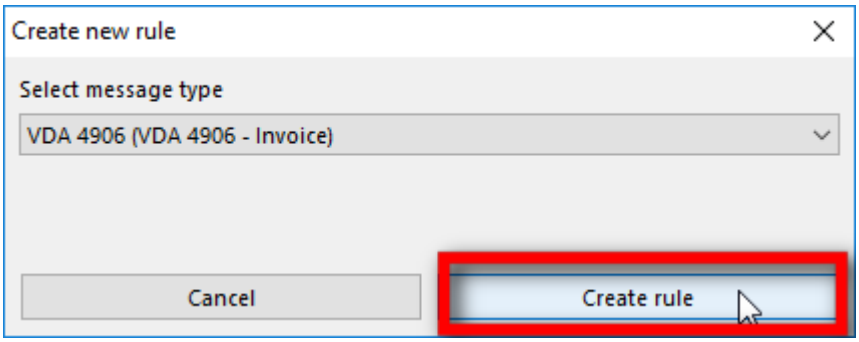
**2** Klick *Add rule* in the top tool bar.



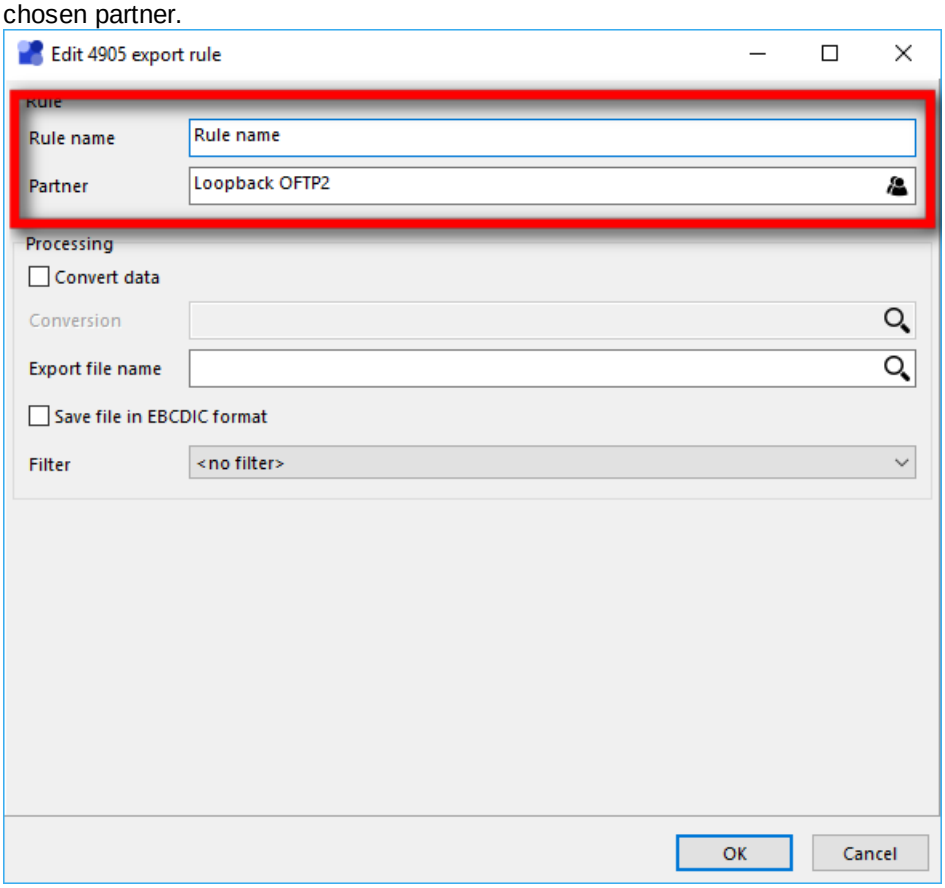

**3** Click the button *Create new export rule*.



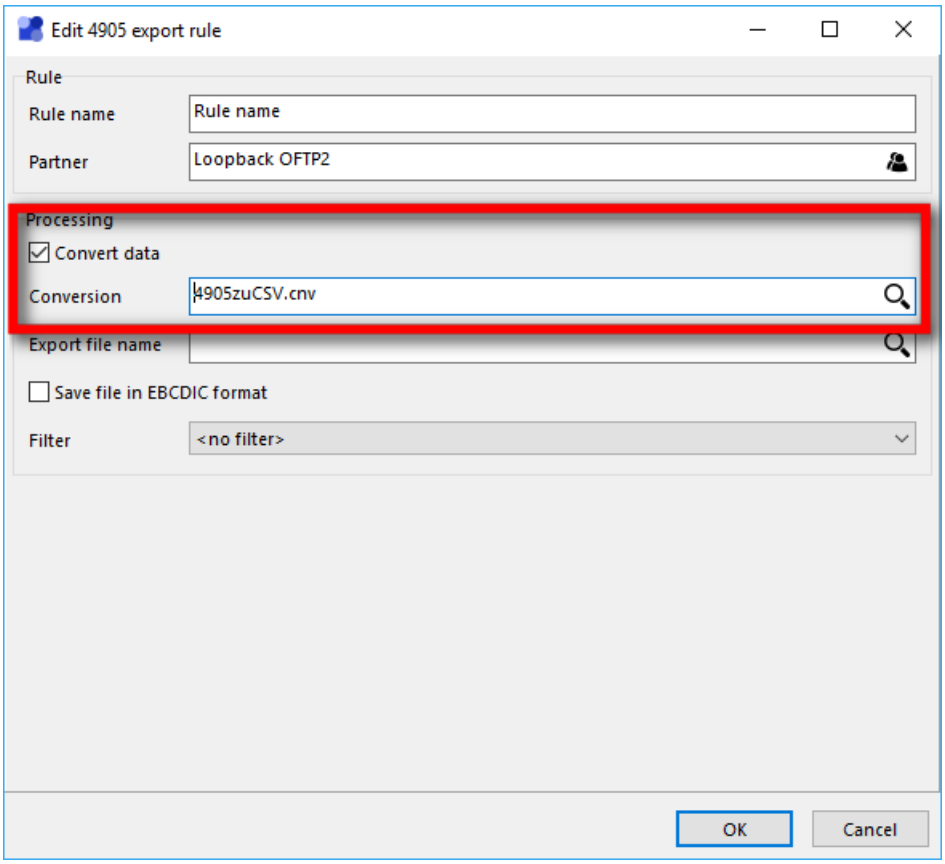

**4** Next select the message type to which the rule should apply, then click the button *Create rule*.



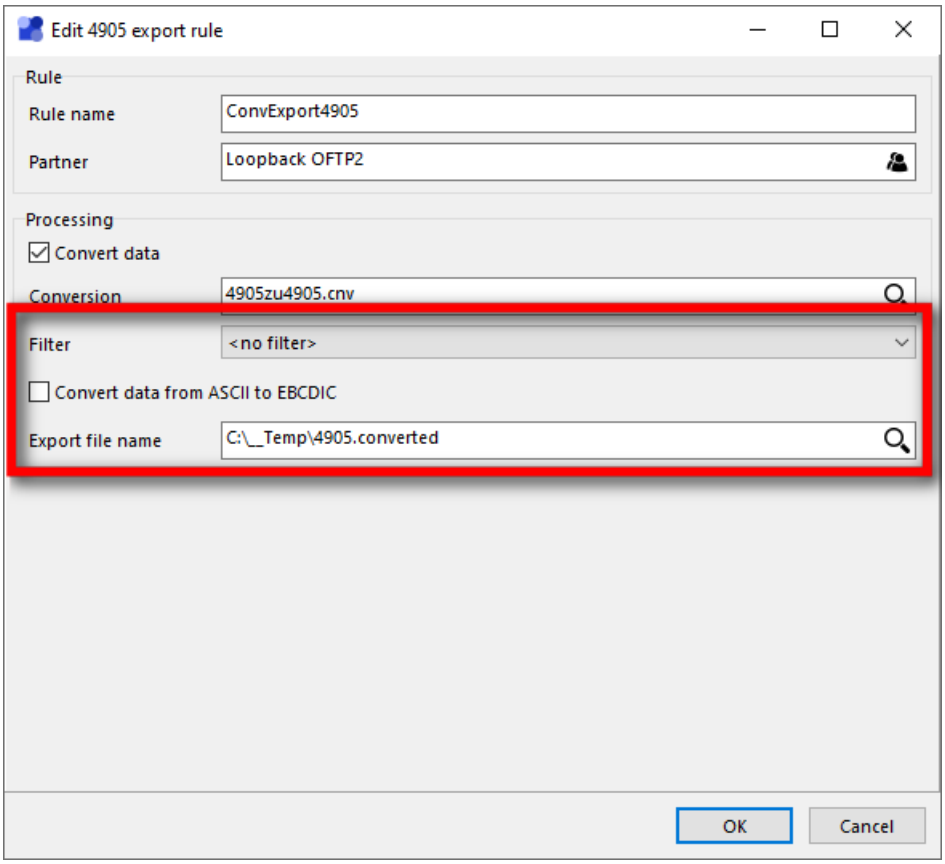

**5** First choose a partner from the !MC5 partner database. The partner name will also be used as name for the export rule. You can change this name if needed. The rule will apply to all messages of the selected message type which will be received from the chosen partner.



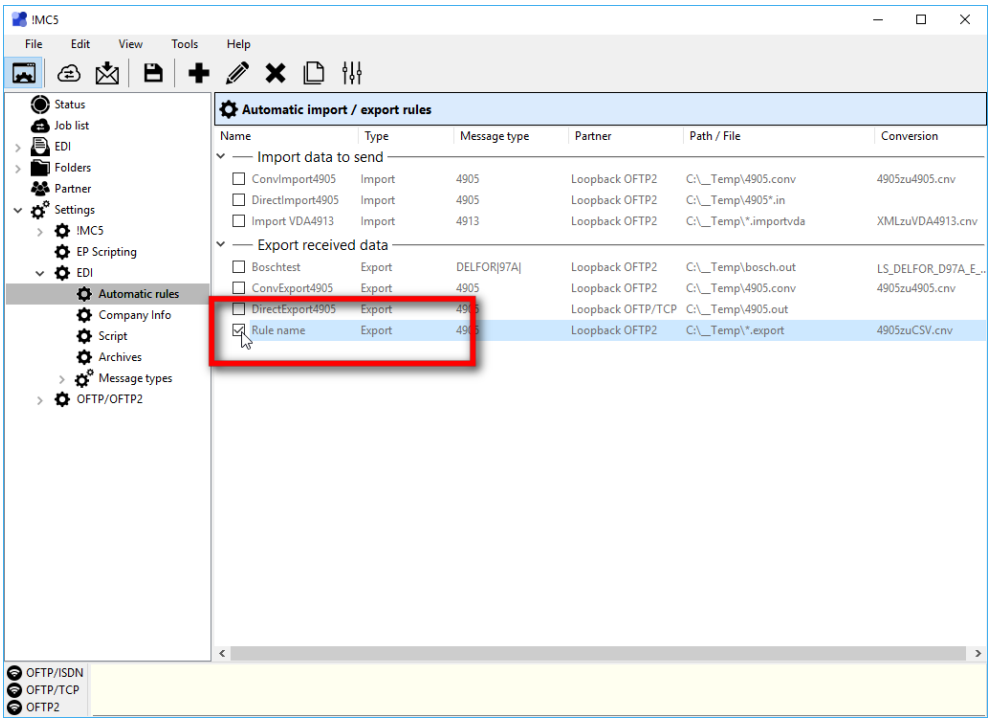

**6** If the received data as to be converted when exporting it using this rule, activate the option *Convert data* and select the conversion rule to be used. When selecting the conversion rule only those will be displayed, that use the select message type as source.



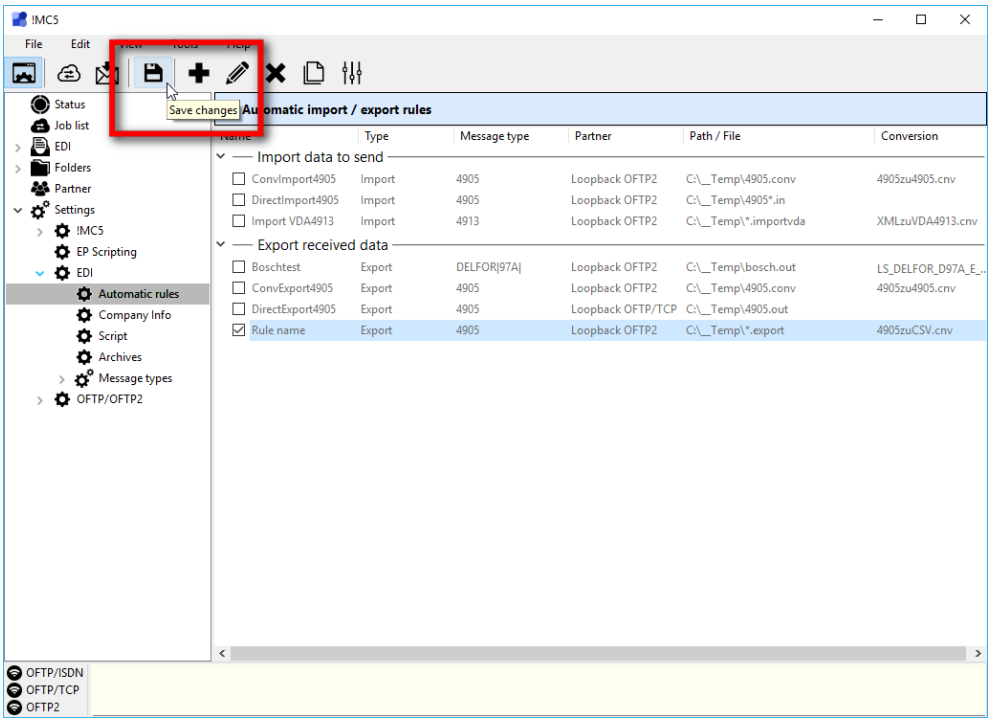

**7** Next enter the target folder and file name for the exported data. More detailed information can be found in the reference for Export rules. Additionally you can select a filter script which will be executed before the message is saved into a file. Files can also be saved with EBCDIC character set instead of ASCII. The EBCDIC conversion is applied on the filtered data, if a filter is selected.




**8** Click *OK* to create the new rule. New rules aren't activated by default. To activate the rule click the checkbox in front of the rules entry. Only activated rules will be used by !MC5.




**9** Save your changes by clicking the *Save changes* button on the top tool bar. From now on the new rule will be used by the EDI Add-On.



#### 4.1.3.3 Automatically import and send data

Using the Module EDI externally created EDI messages (e.g. created by an ERP software) can be imported and processed.

!MC5 regularly tests all active import rules for new matching files. Found files are then imported into the EDI outbox. If enabled the data gets converted before the import. Once imported the messages are automatically printed and sent to the respective partner. Afterwards the file is moved to a subfolder so it is not imported twice.

### Sequence of automatic EDI processing of outbound data

1. !MC5 regularly runs through all import rules and tests for every active rule if files matching the file mask are found in the search directory specified in the rule. Each matching file is then processed further.
2. If the option *Convert data from EBCDIC to ASCII* is enabled, the data is converted from EBCDIC to ASCII.
3. If a filter is selected, the data is processed by the filter. A filter can accept, block or change the data.
   a. If the filter blocks the data (*filterRes* = *fiAbort*), the processing is cancelled.
   b. If the filter accepts the data (*filterRes* = *fiUseInput*), the original data is processed.
   c. If the filter changes the data (*filterRes* = *fiUseOutput*), the changed data is processed.
   d. If an error occurs during execution of the filter (either is a fatal error occurs or if *filterRes* is set to *fiError*), processing gets cancelled.
4. If *Convert data* is enabled, the selected conversion is applied to the data, if not the data get imported directly if it can be identified as the message type the rule applies to.
5. The message gets added to the message archive and EDI outbox.
6. The message gets printed, if the option *print messages* (or equivalent) is enabled for the rules message type (*Settings / EDI / Message types / …*). The default printing option can be overridden in the import rule.
7. The message gets prepared for sending, if the option *send imported messages* is enabled for the respective message type (*Settings / EDI / Message types / …*) or if it is set as override in the import rules settings.
   a. The data is saved into the outgoing folder of the selected partner. The file name is constructed using the *Local send name* pattern. This can be a fixed name or it can contain various placeholders (see Reference / Settings / EDI / Automatic import/export rules / Import rules). If a file with the constructed name already exists in the outgoing folder, or in its subfolder *Prepare*, a counter is added to the file name.
   b. A sending job for the file gets created and passed to the communication module used for the partner.
8. If the import was successful, the subfolder *EDIImport_Success* is created inside the search folder of the import rule and the imported file is moved to this folder. If an error occurred during import, the file is moved to the subfolder *EDIImport_Error*. If a file using the same name already exists in the target folder, a counter is added to the moved files name.
9. EDI processing is finished.

**Only one import rule is applied to each file**

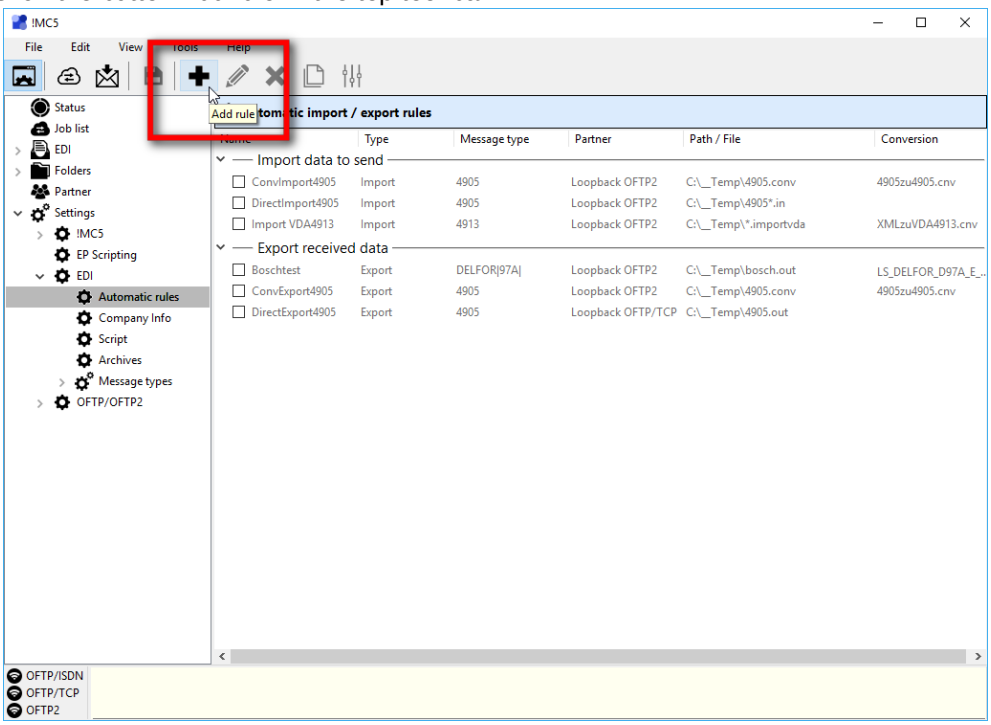
After one import rule is applied to a file and the file is moved to *EDIImport_Success* or *EDIImport_Error* no further import rule gets applied. So in contrast to export rules, where multiple rules can be used for one received message, when importing only the first matching import rule is used.

### 4.1.3.4 Create a new import rule

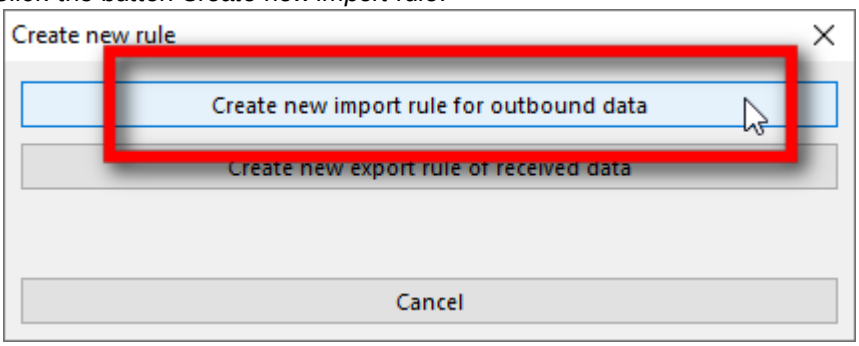
To create a new import rule proceed as follows:

**1** In the *Settings* section open *EDI / Automatic rules*.

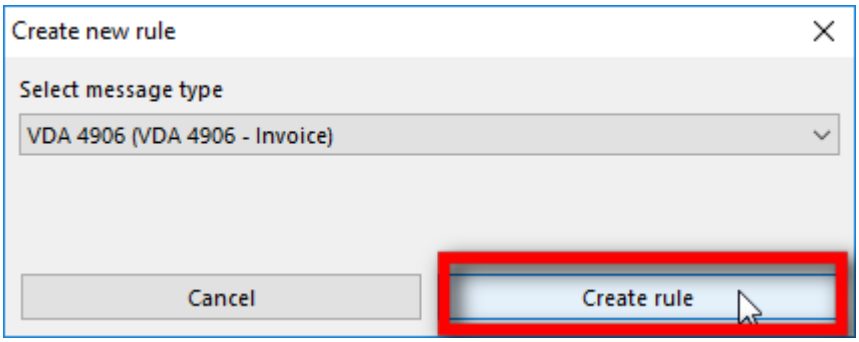
**2** Click the button *Add rule* in the top tool bar.



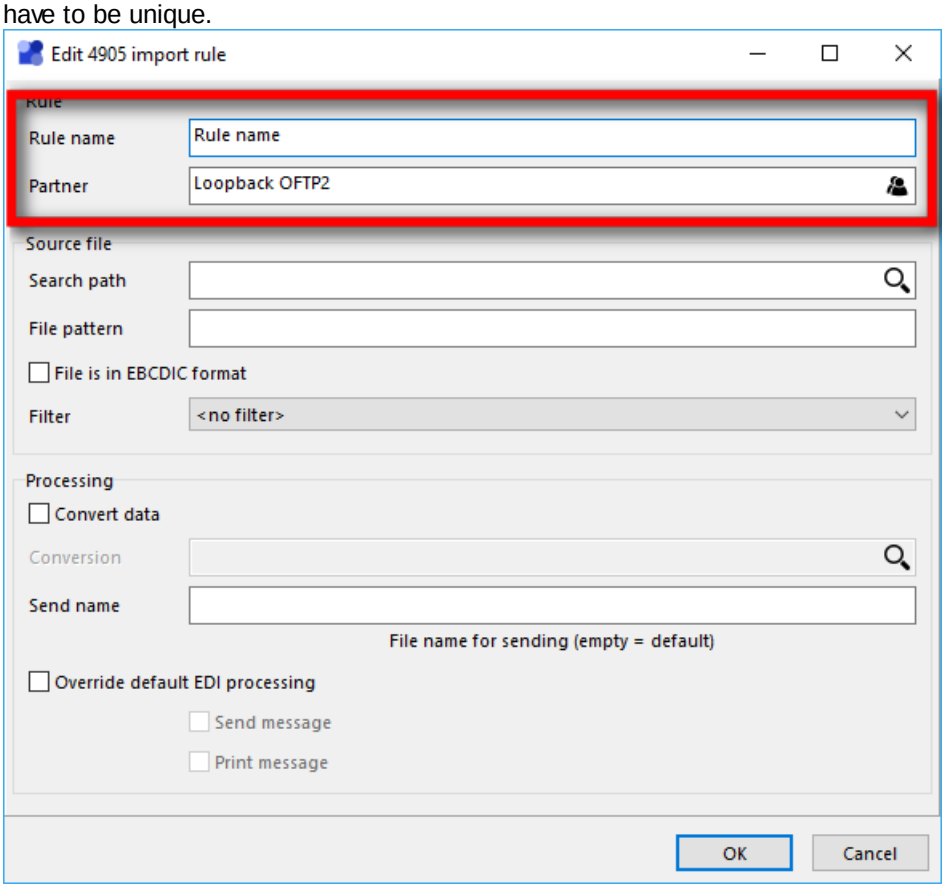

**3** Click the button *Create new import rule*.



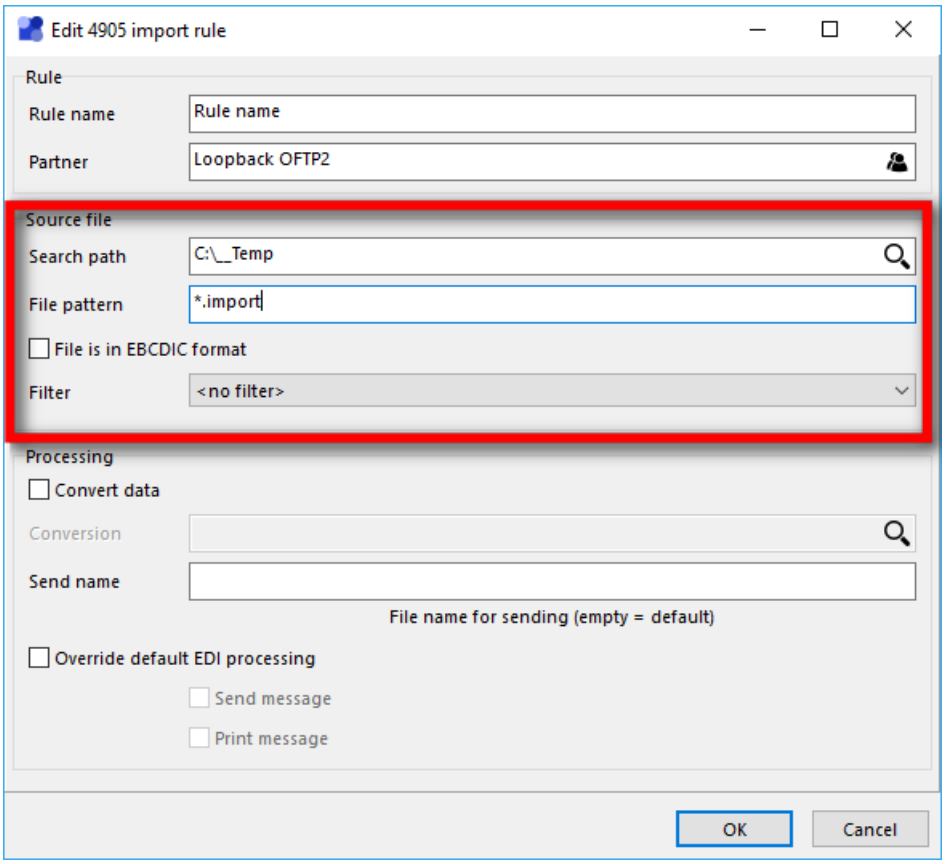

**4** Next select the message type to which the rule should apply, then click the button *Create rule*.



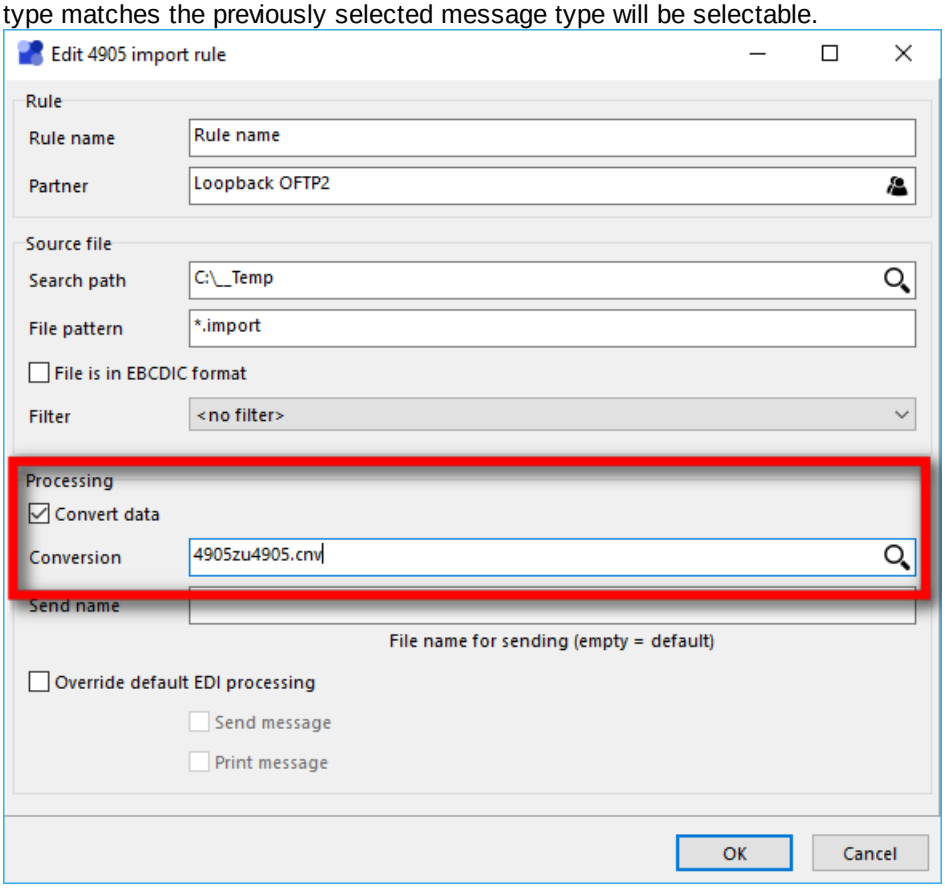
**5** First choose a partner from the !MC5 partner database. The partner name will also be used as name for the import rule. You can change this name if needed. Rule names have to be unique.



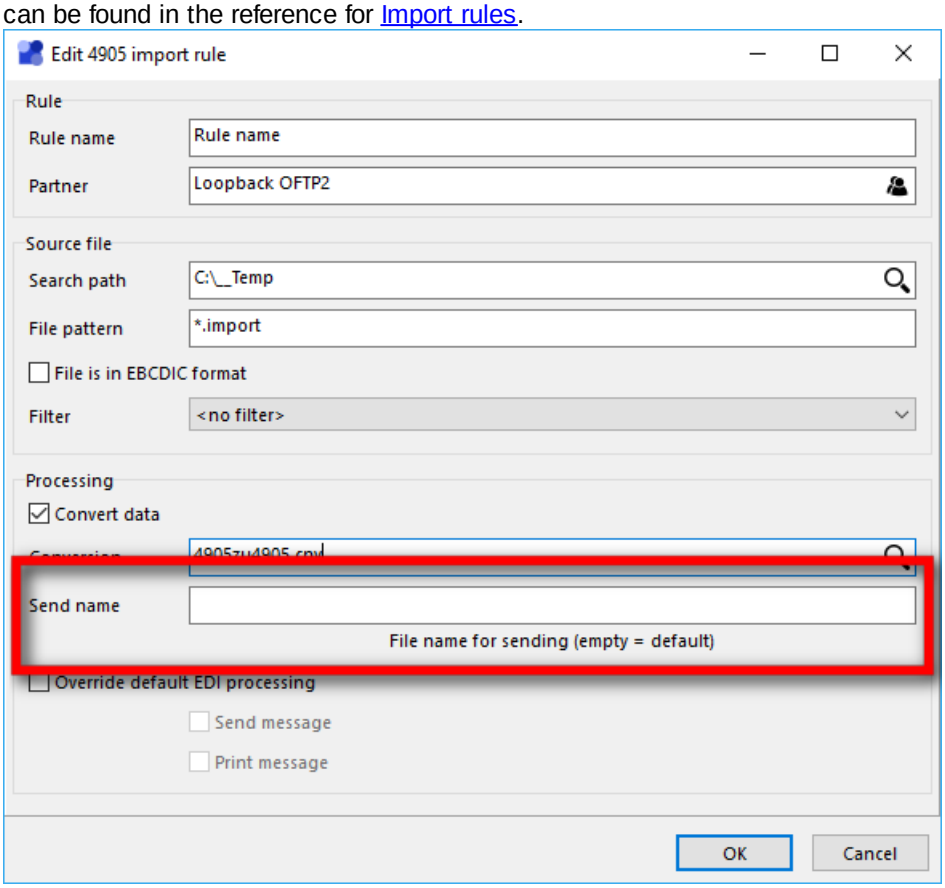

**6** Choose a folder where the EDI Add-On should scan for new files later on. Enter the folder name into the field *Search path*. If all files stored in the folder have to be converted enter * as *File pattern*. You might also enter a more exact pattern to exclude unwanted files from processing. The wild card for various character is *, a single character can be represented by a ?. The usual Windows rules for file patterns apply. The check-mark *Files in Ebcdic format* has to be set if the source files use the Ebcdic character set.
Additionally a filter can be selected, to either filter out files by their content, or to alter the content of the file prior to import.



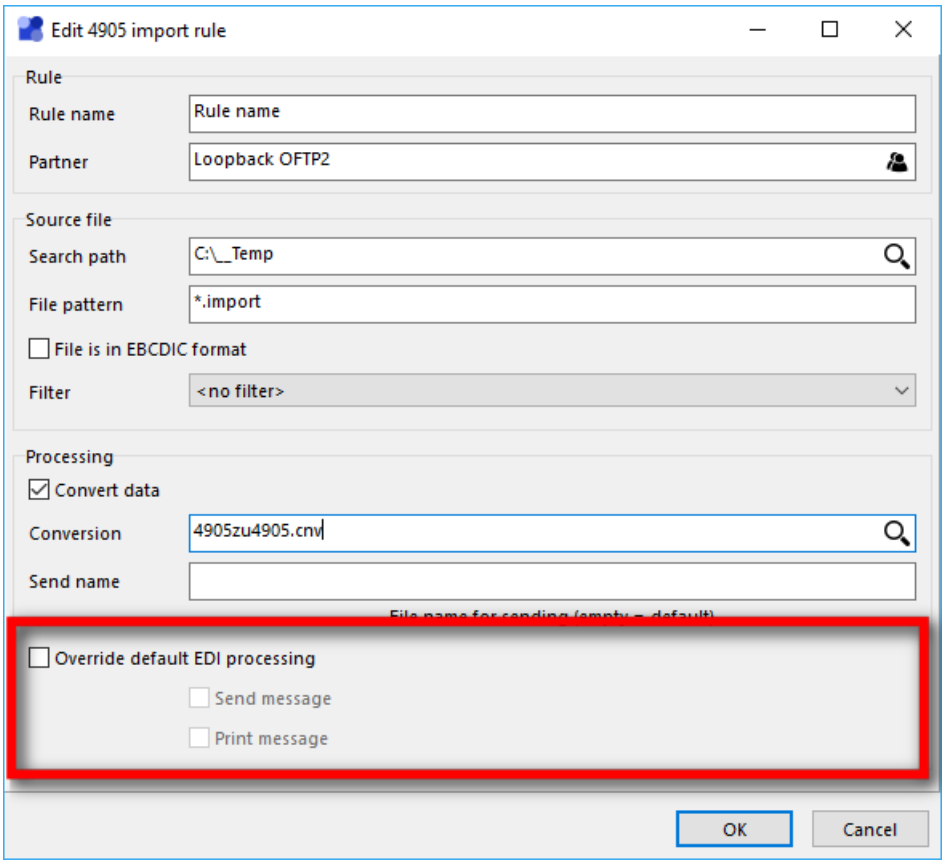

**7** If the data has to be converted when importing activate the option *Convert data* and select the conversion rule to be used for this import. Only conversion rules whose target type matches the previously selected message type will be selectable.



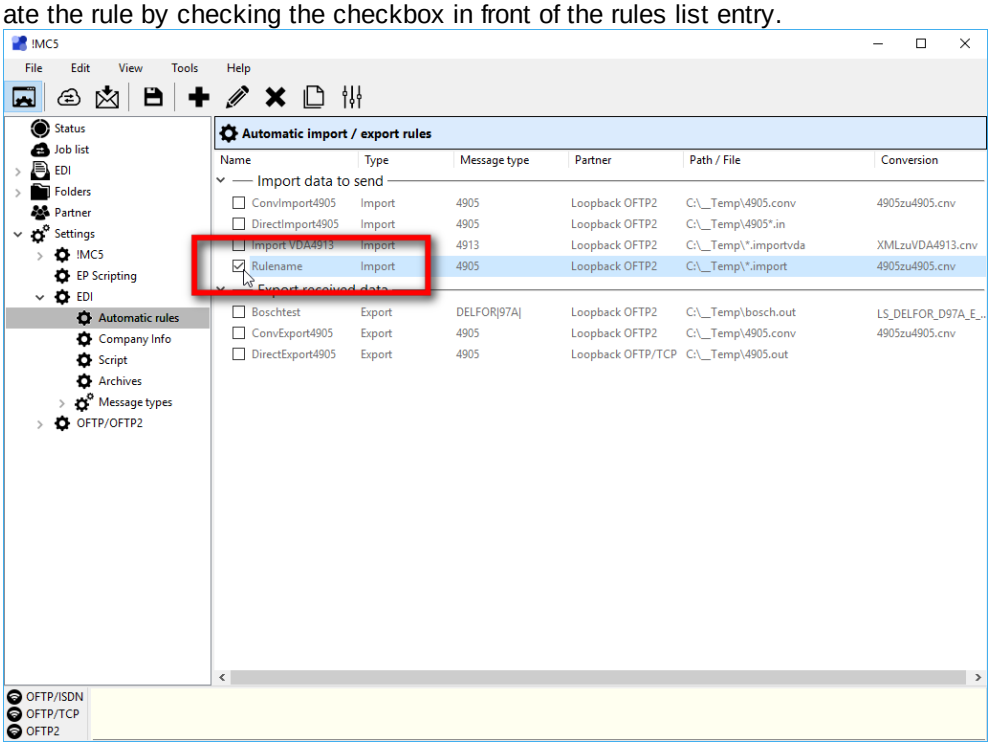
**8** Enter the *Send name* into the corresponding edit box. To use the default name leave this box empty. Further information regarding the formatting options for file names can be found in the reference for Import rules.



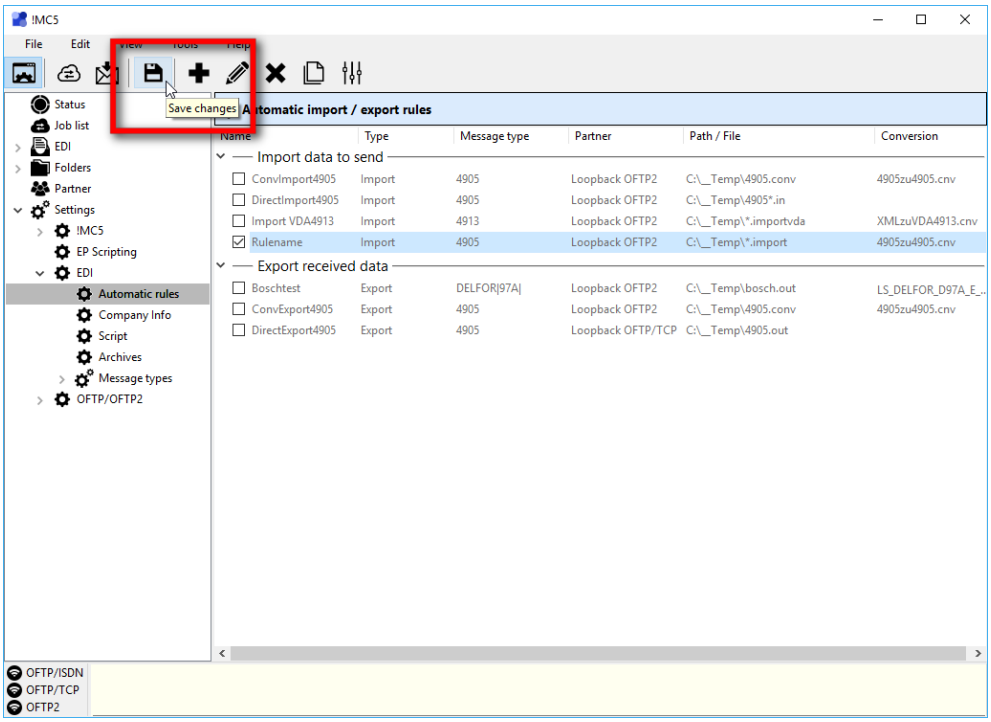

**9** *Override default EDI processing* if this rule is not intended for regular processing. Then choose the tasks this rule has to execute.




**10** Click *OK* to create the new rule. Newly created rules are always deactivated. Activate the rule by checking the checkbox in front of the rules list entry.




**11** Save your changes by clicking the *Save changes* button on the top tool bar. New files matching the rule set will be imported automatically from now on.

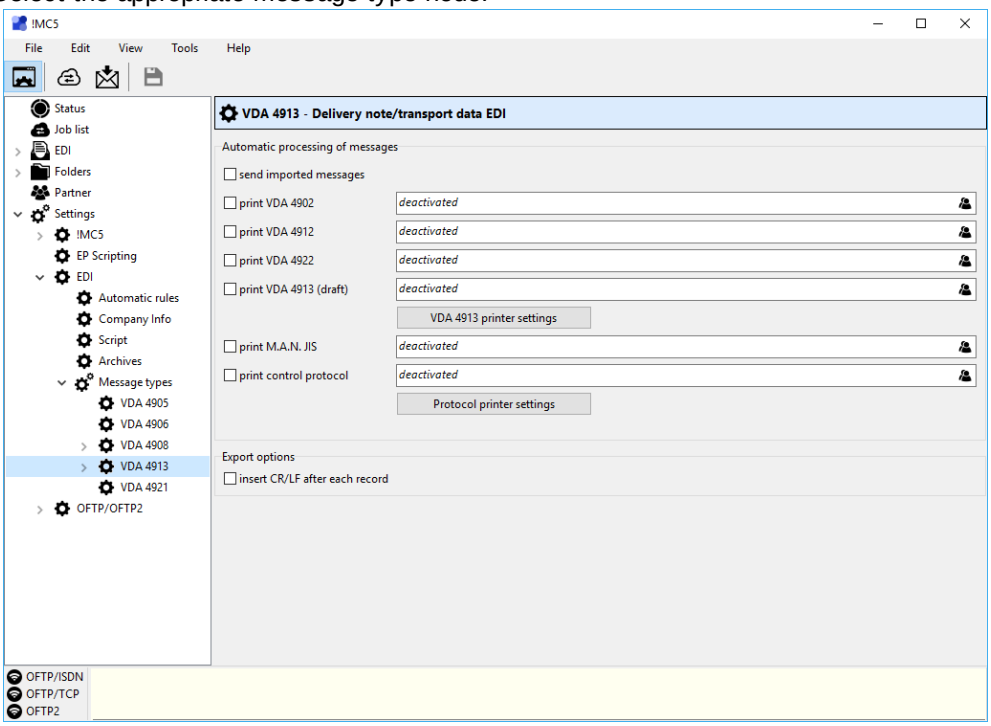


### 4.1.3.5 Configure EDI tasks

To setup tasks for the automatic processing of EDI messages please proceed as follows:

**1** Start !MC5 and open the *Settings / EDI* section in the left hand navigation tree.

**2** Select the appropriate message type node.




**3** Activate the tasks, which are to be executed automatically, in the box *Message processing*. The option *print* will activate the automatic printing for incoming and outgoing messages of this type. The option *send* will only work for outgoing messages. Depending on the message type more options might be visible.

> **Additional info for printing**
> The printing of some message types requires additional information, e.g. the name and address of the own company. This can be done in the option page Own addresses. These proceedings are necessary when information has to be printed which is not included in the message itself.

**4** For automatic printing select the printer by clicking *Printer settings*. If no printer is chosen the standard printer of Windows will be used.

**5** Save the settings by clicking the *save* button.

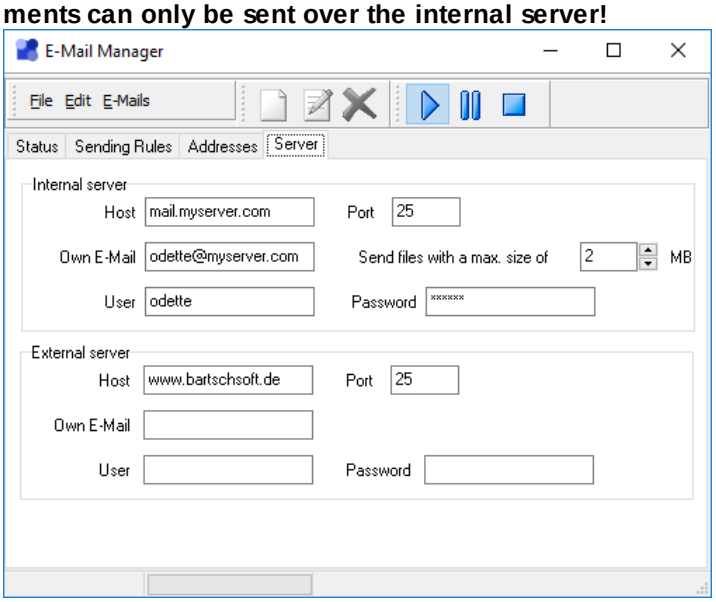
## 4.2 Sending emails using Addon Email

The *Addon Email* offers functions for automatic sending of emails whenever files have been successfully sent or received. Received files can be forwarded within the own company. Also employees of partner companies can be notified that new files are waiting to be picked up by them.

### 4.2.1 Email setup

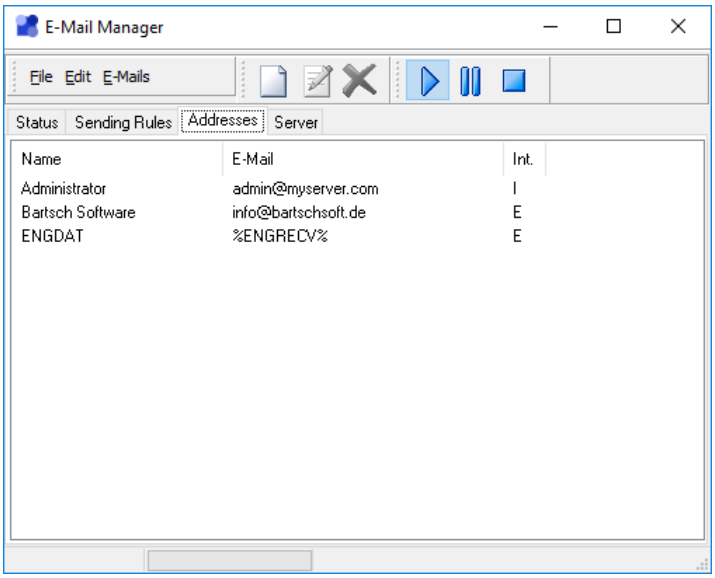
**1** Start !MC5 and open the Email Add-On over the main menu *View / E-Mail Manager*.

**2** At first you will have to enter the parameters of the mail-server. Select the page *Server* and enter the data for the internal and external server. The internal server is used for mails within the own company. At least one server must be entered. **Attachments can only be sent over the internal server!**

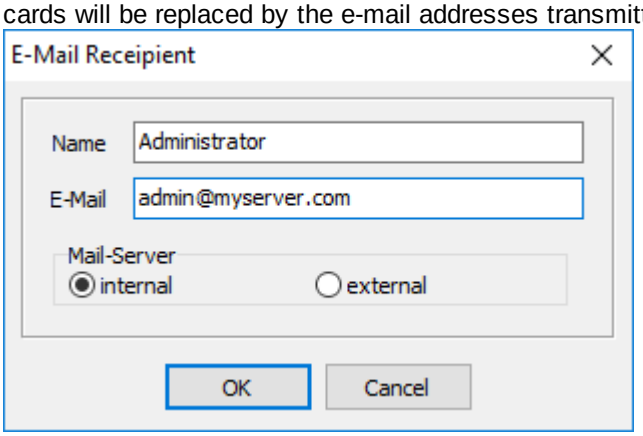



> **Difference between internal and external server**
> Only a computer within the local network should be used as internal server. If a server in the public domain (Internet) is used, you might transfer confidential data without any encryption or other security measures. This would undo the secure transmission by the OFTP! Such a server must always be entered as external server. The add-on will send no attachments over the external server. If the internal server is enabled to send mails to the external addresses, it should be entered as internal as well as external server.

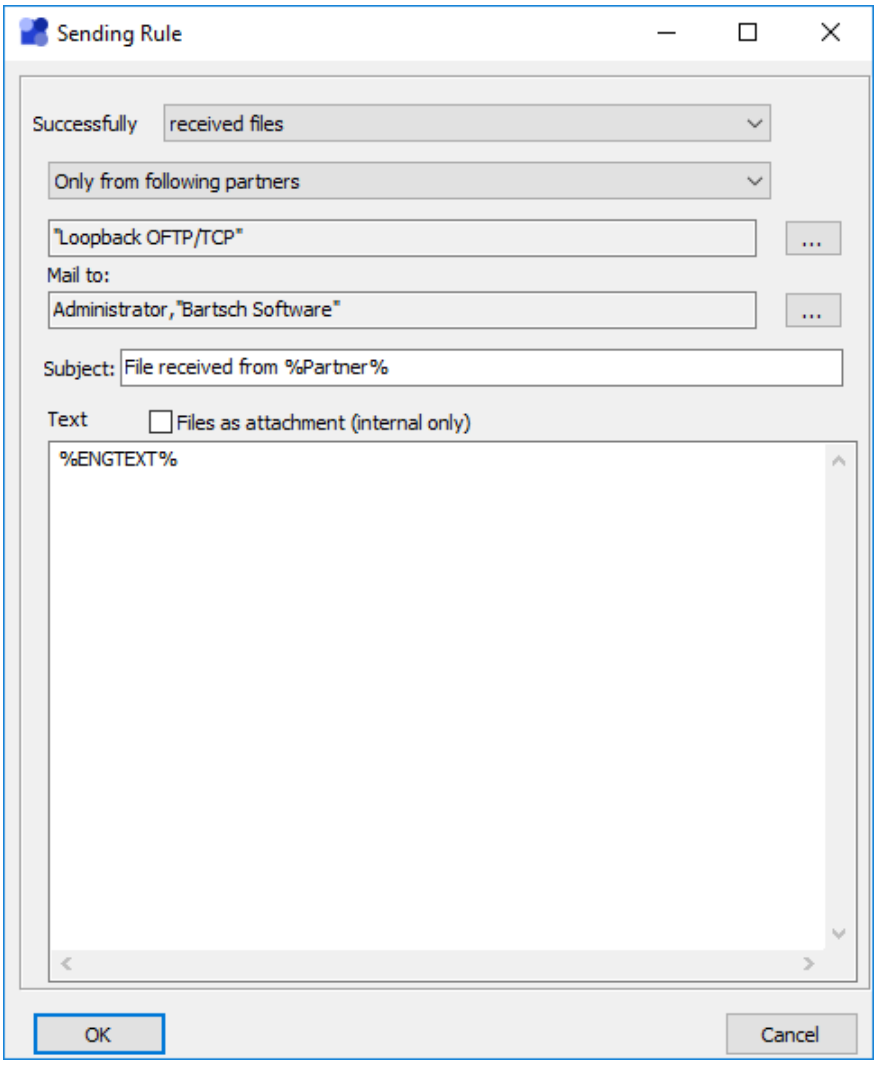
**3** Open the page *Addresses* to enter all e-mail addresses which shall receive mails.




**4** Use the menu *Edit / Add* to create a new entry. In addition to the mail address the name of the receiver has to be entered. The server can be selected in the box *Mail-Server*. When using the add-on ENGDAT the wildcards *%EngSend%* and *%EngRecv %* can be entered into the field *E-Mail* instead of a regular mail address. These wild-cards will be replaced by the e-mail addresses transmitted in the ENGDAT abstract.




**5** In order to connect mail addresses with sending and receiving events sending rules have to be created. Open the page *Sending Rules* and create a new rule with the menu *Edit / Add*.

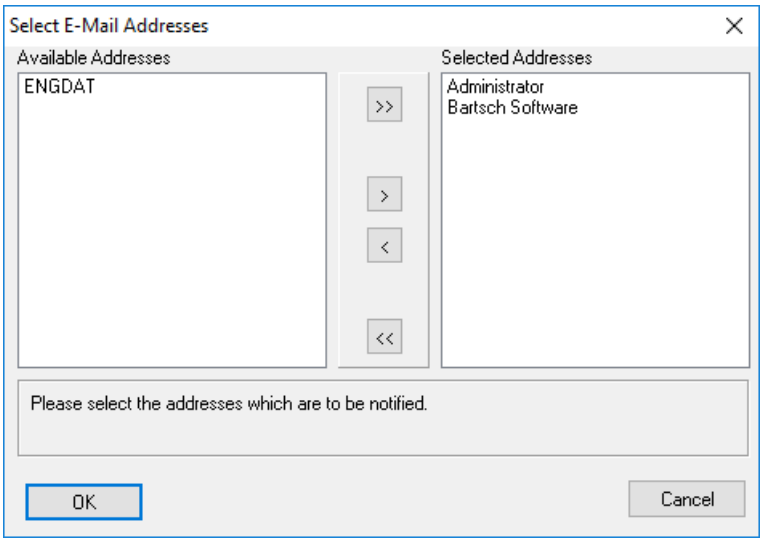



**6** At first select an event on which a message has to be sent. The following events are available:

- ***Successfully received files*** - This event will be signalled as soon as a sending is successfully finished (at least one file has be sent within the connection).
- ***Successfully sent files*** - This event occurs at the end of a connection if one or more files were received.
- ***Successfully prepared files for polling*** - This event is intended for partner companies to whom an active connection is not possible (see Addresses / General / No active connections are allowed). After successful creation of a sending job this event will be signalled. It can be used to notify the partner that there are files available for polling.
-

**7** Please choose now for which partner account or data contents an e-mail shall be sent. There are the following options available:

- ***From all partners except*** - The chosen event will be signalled with all partner except the selected ones. (Partner can be added to the list with the button ... ).
- ***Only from following partners*** - An e-mail will only be sent after connections with partners from the list below.
- ***ENGDAT Filename (requires add-on ENGDAT)*** - The ENGDAT-Filename (by VDA recommendation) possesses 5 freely definable digits. These digits can be entered in the selection box below. An event will be triggered whenever an ENGDAT-message with these 5 digits is sent or received.



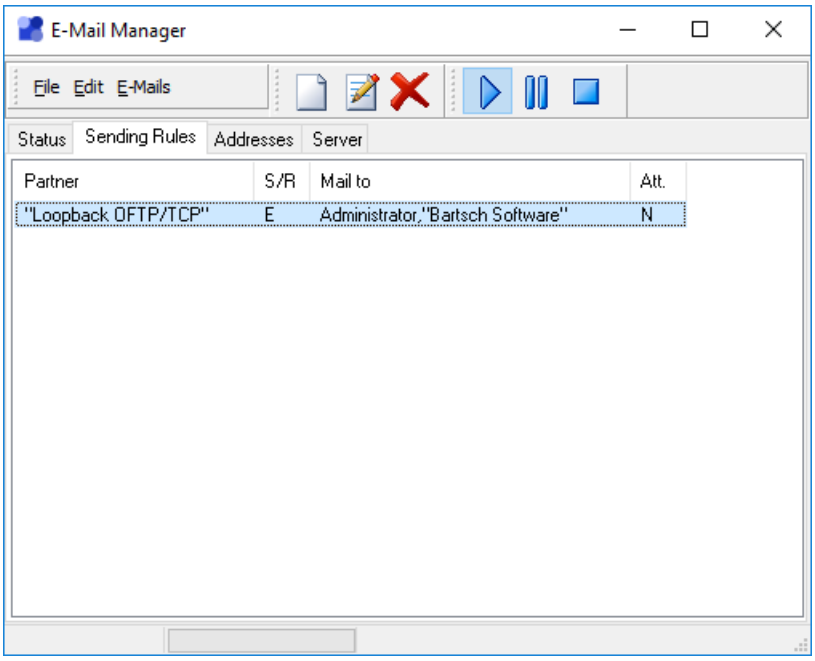

**8** Now select all e-mail recipients in the field *Mail to*.

**9** Enter the headline into the field *Subject*. The wildcard *%Partner%* can be used to fill in the name of the partner from the addresses database.

**10** The text of the e-mail can be entered into the field *Text*. The following wildcards can be used (they are not case sensitive):

- ***%Partner%*** - Name of the communication partner from the addresses database of !MC5.
- ***%Link%*** - This will create a list of all transmitted files. In order to allow the e-mail recipient access to these files only UNC paths should be used in the addresses database. If the folder for incoming and outgoing files is not located on the PC !MC5 is installed on, the e-mail module will translate the paths automatically into UNC format.
- ***%Filenames%*** - This wildcard will produce a list of all transmitted files without a path.
- ***%EngText%*** (requires ENGDAT) - The transmitted ENGDAT abstract will be inserted in plain text.
- ***%EngFiles%*** (requires ENGDAT) - A list of the files included in the transmission using their original filenames.
- ***%HTTPIN%*** (requires HTTP Client) - This wildcard will be replaced by a link for the add-on HTTP Client. By clicking this link the browser will open and the folder for incoming files will be shown.
- ***%HTTPENGIN%*** (requires ENGDAT and HTTP Client) - Did the partner send files in ENGDAT format the wildcard will be replaced by a HTTP-link. The browser will show the decoded ENGDAT message. The files transmitted with the message can be downloaded.

**11** Save the new rule by clicking *OK* and add further rules if needed.




**12** Activate the module over the menu *E-Mails / Send*. By default it will already be activated. Now e-mails will be sent as soon as one of the implemented rules apply.

## 4.3 EngPart

The ENGPART file (subject to the German VDA recommendation 4951) represents a substantial result of the efforts to describe content and format of an automated transfer of information.

The file is used to set-up and update partner relations largely without verbal or written exchange of information. Phone conversations or fax messages are normally only required for setting up the initial connection.

Following information is sent to the partner company by transmitting an ENGPART file:

- all departments and people participating in the exchange of data
- the parameters relevant for the data transmission
- contacts and recipients of the partner company

The ENGPART file is – in accordance with the recommendation mentioned above – a readable text file that can be inspected with a standard text editor.

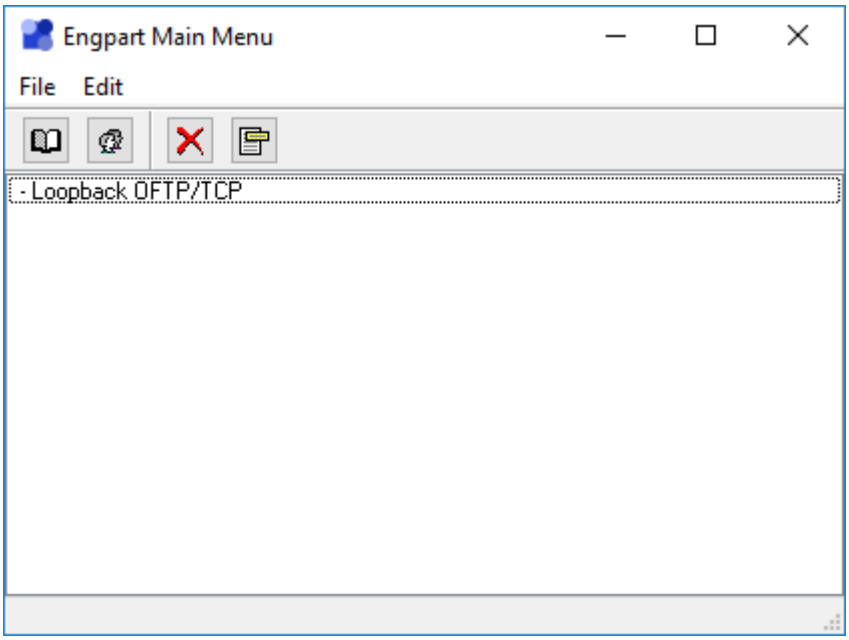
The ENGPART module automatically prepares an ENGPART file based on the available information. If desired, the module transmits the file to a selected partner. It is also used to manage the information received from your partners and the information that has been freely entered into the database. Partner entries as well as own entries can be viewed and changed at any time.

The add-on EngPart !MC5 simplifies the data exchange of ENGDAT substantially. The required information is set up as soon as both partners have exchanged their ENGPART files. The ENGPART module also assists you in sorting and analyzing received files, provided they have been sent in ENGDAT or ENGPART format.

!MC5 implements the versions 2 and 3 of EngPart.

### 4.3.1 EngPart main menu

Open the add-on module ENGPART over the menu View / Engpart of the !MC5 Main Window. The EngPart Add-On starts up with its main menu.




In the lower section of the window, received ENGDAT files are listed according to the partner description entered in the address database.

> **Hint**
> The ENGPART Main Menu window opens automatically when ENGDAT or ENGPART files have been received.

In !MC5 settings the function “Find received EngPart Files” must be enabled. Otherwise the window will not display any files (see ENGDAT-Settings).

## Functions

The following functions are available in the EngPart Main Menu:

***Edit base data*** - Modify or add data concerning your own company

***Edit partner data*** - After setting the type of administration, partner information can be viewed and if necessary modified.

***Delete entry*** - Remove selected entries from the list. The file itself will not be deleted. To evaluate ENGPART files at a later time use “Edit Partner Data”.

***Evaluate entry*** - The program evaluates the selected file. Depending upon the file format this is done in different ways:

ENGDAT Evaluation of !MC5 is started for ENGDAT file.

ENGPART information is saved for ENGPART file and is accessible via “Edit Partner Data”.

These functions are also available in the menu. The function *Refresh List* is also located here. It removes files that are no longer available from the list, but does not add any new entries.

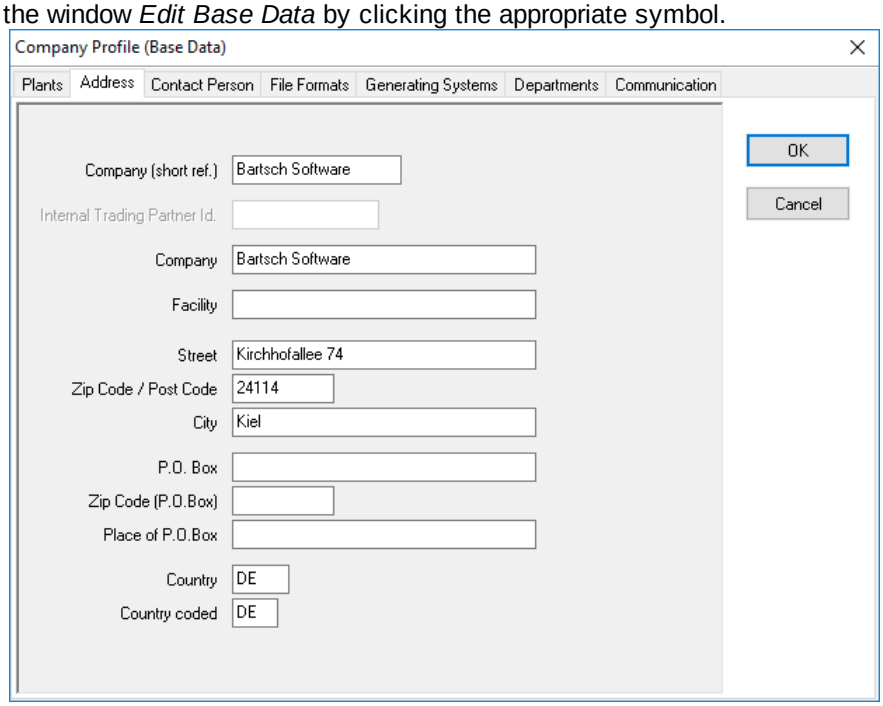
**Hint**
The function *Refresh List* cannot be used to cancel the process “Delete entry” ! Make sure to delete items of the list only if you are convinced that they have already been evaluated.

### 4.3.2 EngPart setup

After the initial installation the EngPart Add-On provides only the technical requirements for transmitting EngPart files. The information which shall be transmitted to a partner company needs to be entered first.

Following steps are required to enter the information:

Open the window *Edit Base Data* by clicking the appropriate symbol.

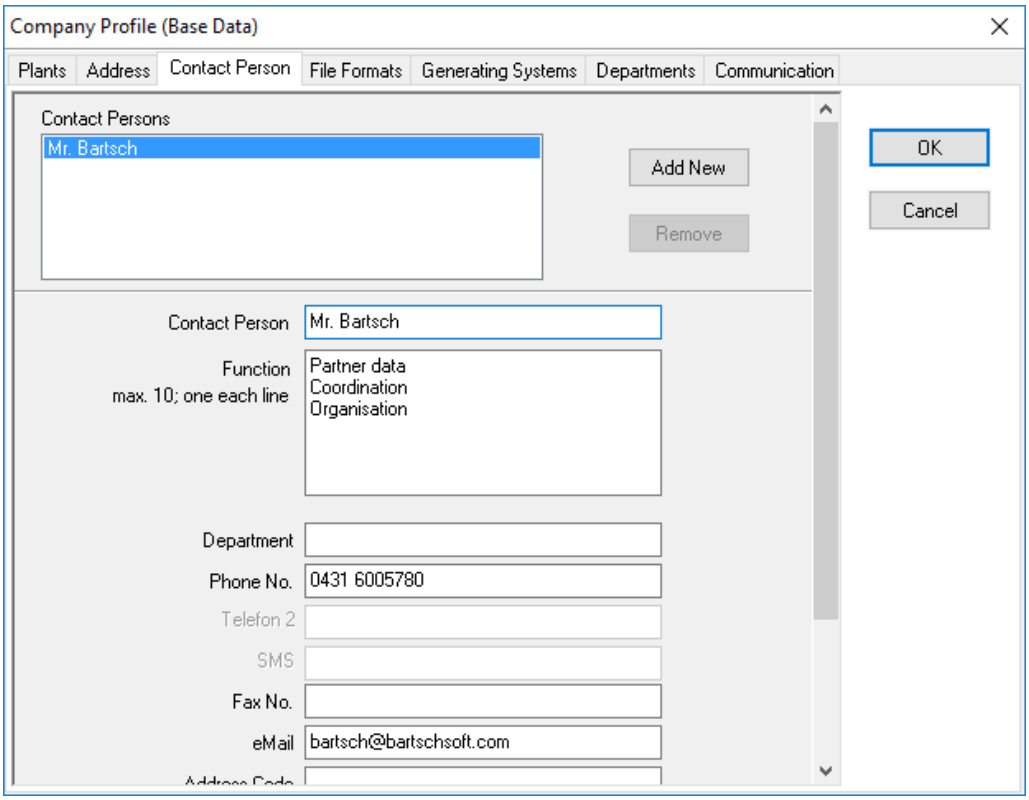



The input page “Address” and the following pages are intended for entering details of your own company. You can move through the individual pages by clicking the header of the required page. By starting with version 3 of EngPart it is possible to enter several plants with different addresses.

In order to comply with the VDA recommendation there are fields that need to be filled in before the first time transmission. When moving the mouse pointer over a field, a popup flag shows the associated EngPart code and the letter “M” if the field is mandatory. For detailed information regarding „Mandatory Fields“ see chapter Appendix A: EngPart (VDA-recommendation 4951) Mandatory Fields

Press “OK” to save your changes and return to the main menu. Press “Cancel” to return without saving changes.

## Example

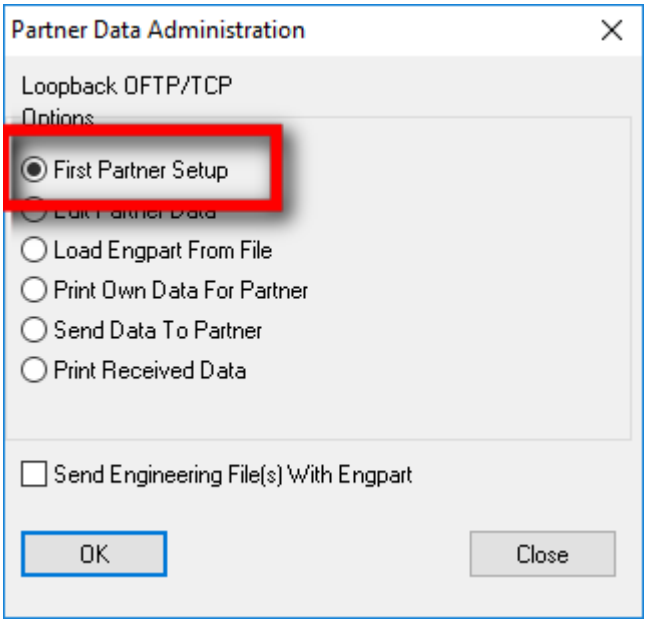



**Note:**
The window above can be used if the details of your own company need to be changed at a later time (change of telephone number, name of employees etc). Please ensure that an update containing the modifications is transmitted to all EngPart partners, who might be affected by them.

### 4.3.3 First time transmission

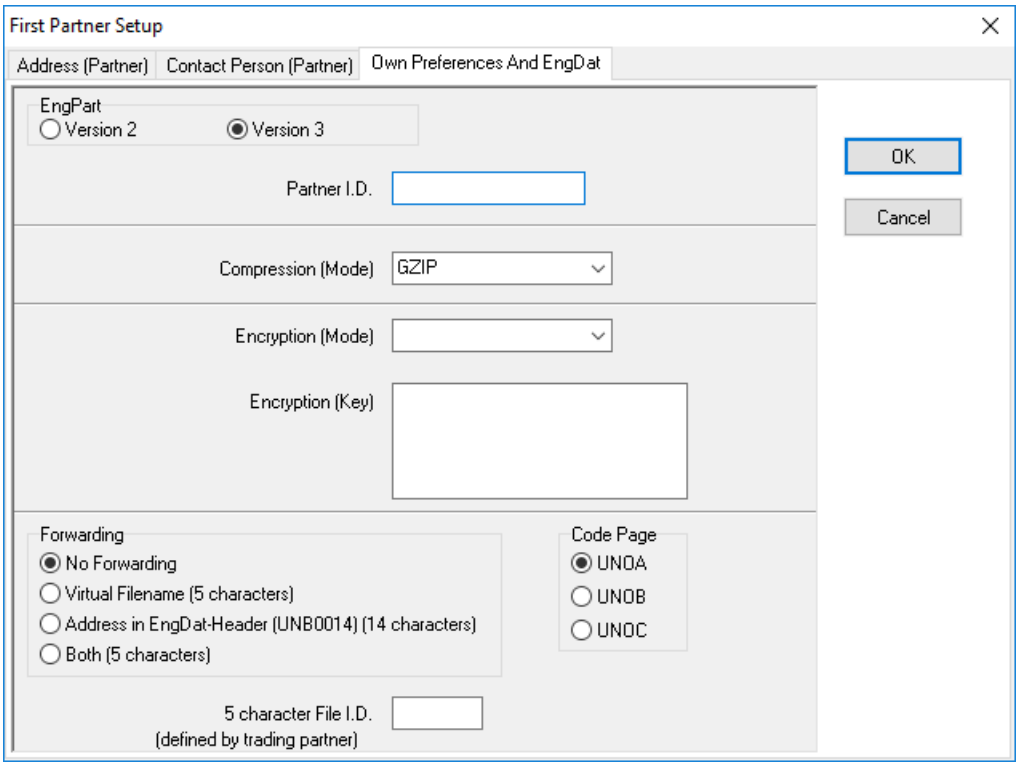
Prior to the first EngPart connection both partners must send their data to the opposite partner. If your partner has already sent data there are fewer entries to be filled in manually.

After filling in all mandatory fields for your company (see EngPart Settings), select the button *Edit Partner Data* to open the *Partner Data Administration*. Choose the desired company from the list of your Odette partners. At the top the name of the selected partner company is shown. If you have **not received EngPart data** from your partner yet, select option *First Partner Setup* and click *OK*.




In the window *Partner Company Profile* enter the information for the selected partner similar to entering your own details. For detailed information regarding *Mandatory Fields* see chapter Appendix A: EngPart (VDA-recommendation 4951) Mandatory Fields. Enter the address and the name of your contact person. This information is needed only for the first transmission and will be replaced later by the information send to you by your partner.

The free 5 character identifier is part of the ENGDAT file name and is usually given to you by the partner company or agreed upon with you. By all means this field must be filled in. The EngPart Version must also be chosen by partner preferences. Information on the versions can be found at Compatibility EngPart Version 2 and 3.




If you have already received EngPart data from your partner, select the option *Edit Partner Data* and select the page *Own Preferences And ENGDAT*. Information transmitted to you by your partner should not be modified unless it is absolutely necessary, since your partner is responsible for the correctness.

When the fields under *First Partner Setup* or *Edit Partner Data* have been filled in, return to the previous window by clicking the *OK* button.

You are now able to transmit your first EngPart file to your partner. Select option *Send Data To Partner* to transfer the information via data transmission or select *Print Own Data For Partner* instead and send the information in printed form.

### 4.3.4 Evaluating received data

In addition to the usual information displayed in the !MC5 main windows the add-on module EngPart checks incoming files whether any of them are EngPart or ENGDAT files. In this case the EngPart Main window opens automatically if it is not already open. In the list you will now find the name of the company that has just transmitted ENGDAT / EngPart data to you.

If the partner company has transmitted an EngPart file, there will be a special reference to it at the beginning of the line. Otherwise files in ENGDAT standard have been transmitted. To evaluate the transmitted data select an entry from the list and click the *Evaluation* symbol. For ENGDAT the usual ENGDAT-evaluation window will be opened, see ENGDAT Evaluation

For EngPart files the data transmitted will be read and stored by the EngPart module immediately. As soon as the message *EngPart file has been read* is shown, the information is accessible via *Partner Data Administration*.

Select the option *Edit Partner Data* within *Partner Data Administration* to view the information. If you have already sent an EngPart file to the partner company you are now able to send engineering files in ENGDAT standard to this company. If you want to view a received EngPart file after evaluating it, you can select the option *Print received data* in the menu *Partner Data Administration*. The program will provide you with a printout of the received EngPart file.

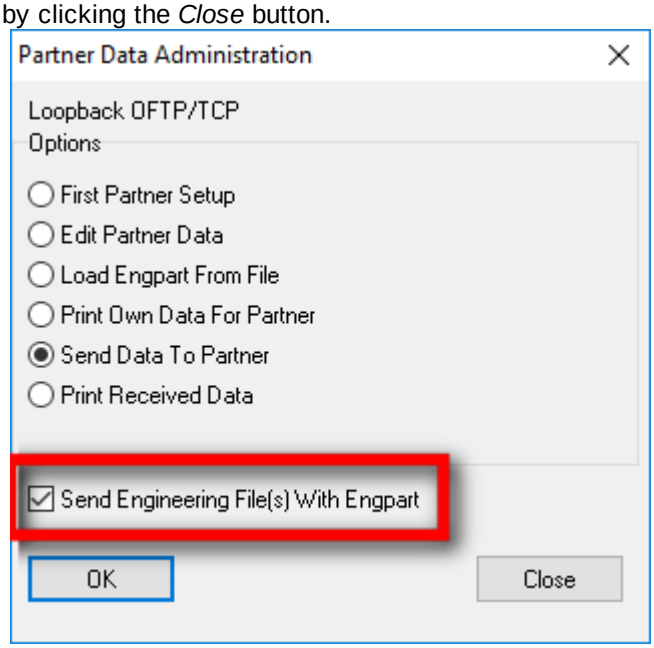
**Hint:**
If the partner company cannot send its data in EngPart standard you have to enter relevant information, e.g. final recipients in the departments, manually. When done you can use the EngPart module to transmit data in ENGDAT standard to the partner company.

### 4.3.5 Sending and receiving engineering data

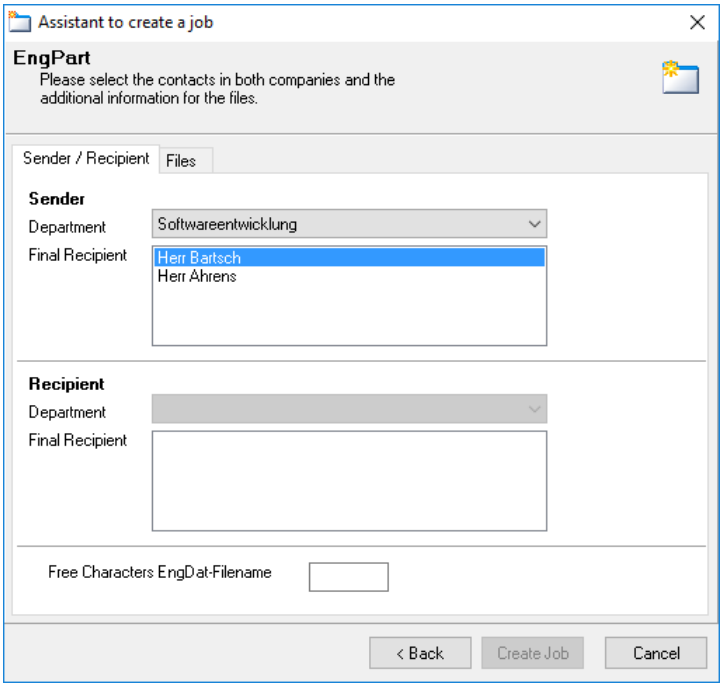
The exchange of company profiles with EngPart is necessary to exchange construction data with ENGDAT in an effective way. By providing the company profile type mismatches in ENGDAT can be avoided. Manual input is only needed for additional file information which cannot be provided by EngPart

#### 4.3.5.1 Sending engineering data

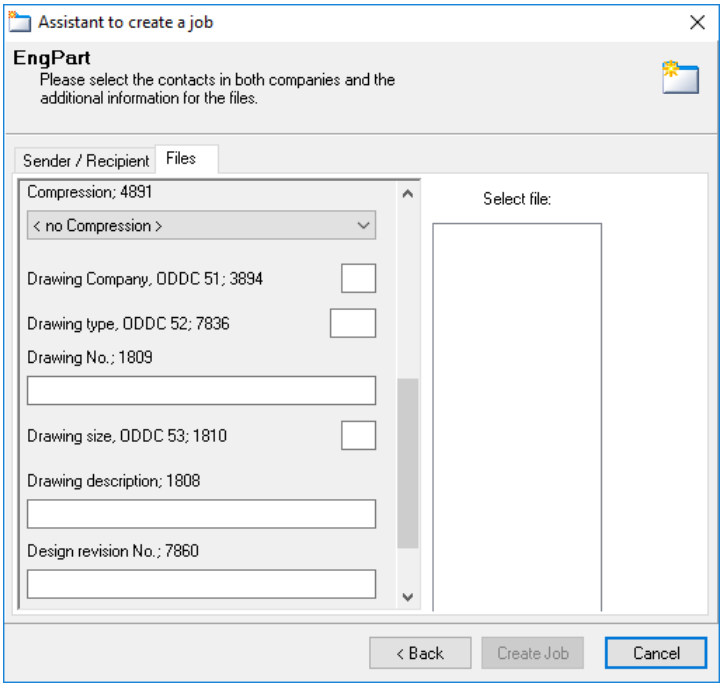
Own and other information entered in the EngPart module can be used to create new sending jobs to a large extent automatically. For this the appropriate option in the Partner Administration (EngPart) has to be activated once. Just check the box *Send engineering file(s) with EngPart* at the bottom of the menu *Partner Data Administration* and leave the menu by clicking the *Close* button.




Now click the button *New Job* in the main tool bar of !MC5 and select the appropriate partner. The following window appears:



First select the correct sender. Choose the department and the final recipient within. Repeat the same steps for the recipient. When done move to the second page named *Files*.




On the right side of the window all files are listed for which you can enter ENGDAT information. Select the correct file format and generating system. Additionally you can enter intended purpose and a description. The default setting for the item engineering department is the sender department selected before. This may be modified if requested. In the lower section of the window (not visible in the screenshot above) a drawing description can be added.

If you are done with the input for one file, you can use the input as default setting for all other files by clicking the corresponding button. From now on you must edit only the fields which differ for each file. Close the window by clicking *OK* and proceed in creating the sending job as usual.

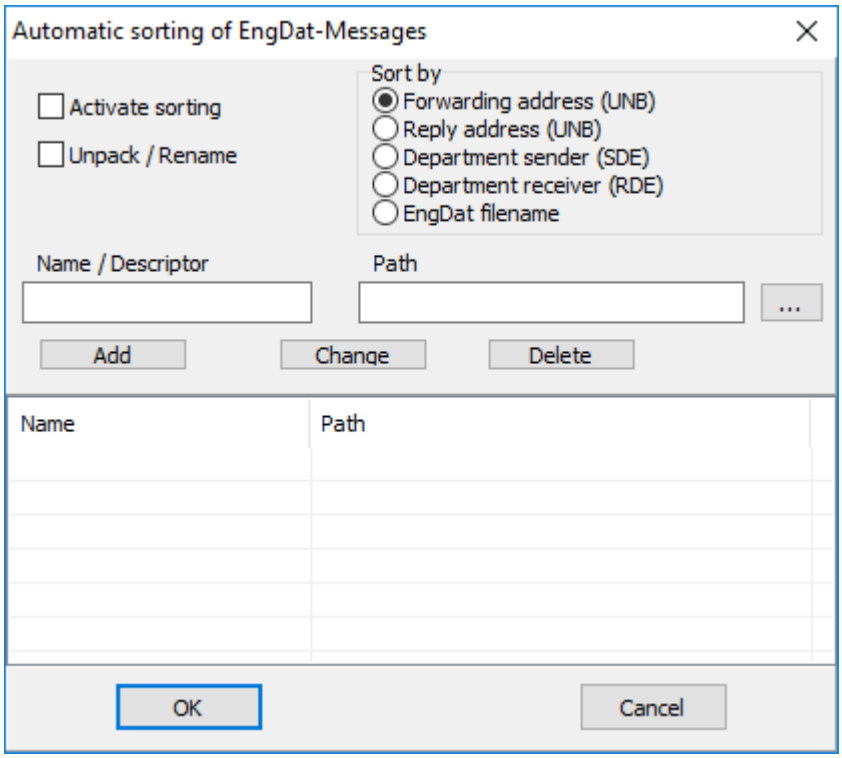
#### 4.3.5.2 Receiving engineering data

Each entry in the EngPart main window list without the addition EngPart represents an ENGDAT file with engineering data. The evaluation is started the same way as with EngPart files by clicking *Evaluate Entry*. This will open the window *Evaluation ENGDAT Header*. More information can be found at ENGDAT Evaluation.

If the automated search for EngPart is deactivated the ENGDAT-Evaluation can also be started from Section *Folders* in the main window, see chapter Folders. The modules Client/Server and HTTP Client also support the evaluation of ENGDAT. Only the processing of the administrative EngPart file must be started from the EngPart main window, see Evaluating received data.

### 4.3.6 Sorting of incoming EngDat-Messages

The EngPart Add-On provides a function to automatically sort incoming ENGDAT messages. There are five criteria for sorting provided. The sorting function can be accessed from the main menu of the EngPart-window at *File / Sort*.




- ***Activate sorting*** **-** This enables the sorting function.
- ***Unpack / Rename*** **-** With this option set the files will not be stored with their ENGDAT file names but with their names provided by the ENGDAT abstract. Are the files compressed with GZIP they will be decrompressed. Without this option the files will only be moved into the target folder while their ENGDAT file names.
- ***Sort by*** **-** The ENGDAT messages can be sort by one of the following criteria:

| | |
|---|---|
| Forwarding address (UNB) | The column „Name“ must be filled with all available forwarding addresses from the EDIFACT header. These can be up to 14 characters long. |
| Reply address (UNB) | The reply address is the forwarding address of the sender. With this option it is possible to sort by sender. |
| Department sender (SDE) | The segment SDE contains the address information of the partner company and the sending department. This option is case sensitive. |
| Department receiver (RDE) | This option will sort by the department names in your own company. |
| ENGDAT-Filename | In the ENGDAT-filename as recommended in VDA4951 there are 5 characters for free use. These must always be filled. If there exists an agreement about how to fill this position it can also be used as an sorting criterion. |

- ***Add*** **-** The contents of the two edit fields above will be added to the table. To ensure that sorting always takes place the character * can be put into the name field. This entry will always be used when no other entry fits the criterion.

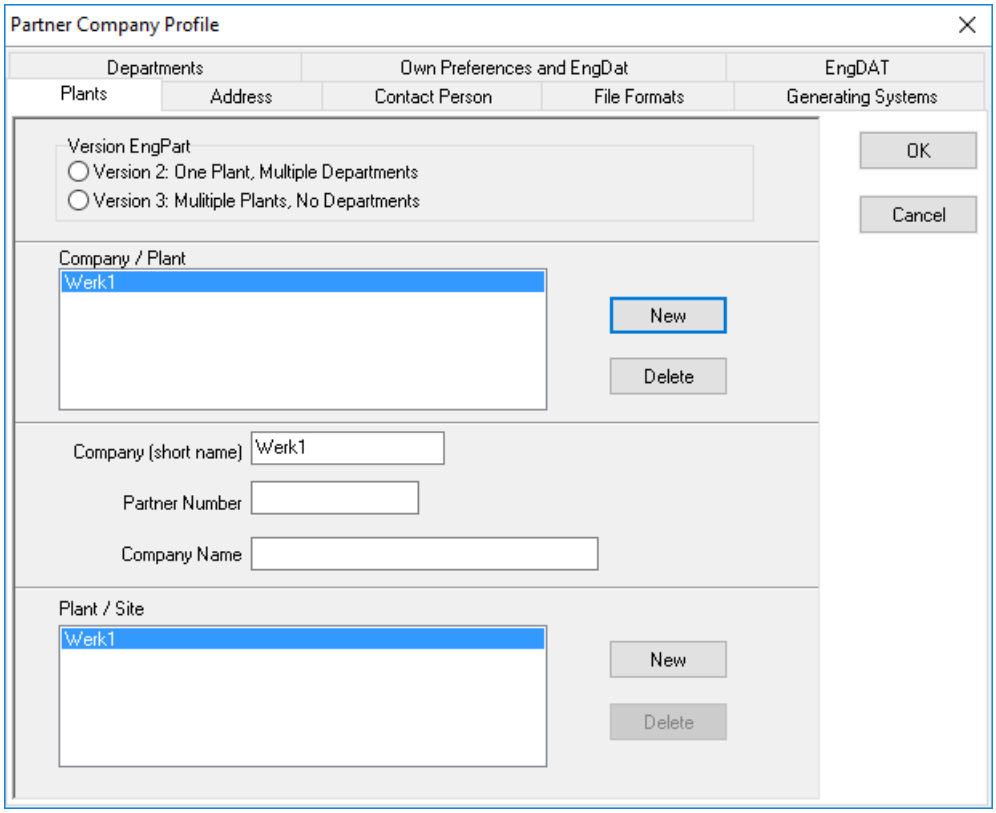
- ***Change*** **-** The contents of the two edit fields will be copied into the marked entry of the table.
- ***Delete*** **-** The entry that is marked in the table will be deleted.

> **Hint:**
> The moving of the files out of the in-folder of !MC5 might influence other integrated ENGDAT functions. The Add-Ons Client/Server and HTTP Client can only access received files. Therefore they might no longer be able to access these files.

### 4.3.7 EngPart versions 2 and 3 compatibility

The versions 2 and 3 of EngPart are highly compatible to each other. EngPart Version 3 supports multiple plants. The EngPart version can be selected for each partner individually. When an EngPart-file version 2 is upgraded to version 3 there will be no data loss. In case of an downgrade to version 2 only the first plant of version 3 will be used. As long as only one plant is used in the own EngPart settings the version used does not matter.

Switching between the versions will cause no data loss. When using version 2 version 3 will be stored as well. After switching back to version 3 it will be accessible again.




**EngPart Version 3 supports several plants.**

While supporting several plants, departments are declared as optional in version 3. In order to keep compatibility to version 2 all contacts without a department will be assigned to default department. This will be used when generating a new sending job.

## 4.4 EP Scripting

Using the add-on EP Scripting, files can be sent and received by calling external programs. This way you can use !MC5 to send data, especially EDI merssages, via FTP or X.400 (e.g. using T-Systems FileWork). EP Scripting is designed to be as flexible as possible to control as many external programs and processes as possible. The external programs are controlled using scripts using the Windows Batch syntax in combination with additional parameter files that can be passed to called programs. Both scripts and parameter files are created dynamically to be adjusted for each individual call.

**Windows Batch programming**
EP Scriping saves and executes scripts as Windows Batch Scripts (.bat). For Links to additional information about Windows Batch Scripting refer to the following links:

Windows Batch Scripting on WikiBooks: https://en.wikibooks.org/wiki/Windows_Batch_Scripting
Guide to Windows Batch Scripting: http://steve-jansen.github.io/guides/windows-batch-scripting/index.html
Windows Batch Scripting on WikiBooks: https://en.wikibooks.org/wiki/Windows_Batch_Scripting

!MC5 uses three kinds of scripts, which are executed at different times in different contexts:

- **Inbound scripts** - Get executed when files are found in an EPS partners incoming folder.
- **Outbound scripts** - Get executed for each file sent to an EPS partner.
- **Timer scripts** - Get executed in regular intervals independently of any partner.

### Processing of incoming Data

In regular intervals !MC5 checks the incoming folders of all EPS partners for new files. When new files match the file pattern specified for that partner, the incoming script gets executed, if one is selected. Afterwards each file is being processed by hte module EDI. The detailed process is as follows:

1. Matching files are found.
2. (optional) The files get converted from EBCDIC to ASCII character set. Copies of the original files are saved into the sub folder *EPS_EBCDIC*.
3. (optional) The incoming script specified for that partner gets executed (the variable *FILENAME* will be assigned the value of the incoming file pattern).
4. Each file will be queued for processing by the module EDI individually.
5. (optional) The for the partner specified filter gets executed.
6. Further processing according to EDI settings.
7. If accepted by the filter in step 5, the file gets moved to the sub folder *EPS_Received*.

### Sending data

Files can only be sent by EP scripting using automatic file transmission od EDI import rules. When files get sent using one of those functions, the specified outgoing script will be executed for each file. The detailed process is as follows:

1. One or more files are processed by either an automatic file transmission or an EDI import rule.
2. The file get saved to the respective partners outgoing folder.
3. (optional) The file gets converted from ASCII to EBCDIC character set. A copy of the original File gets saved into the sub folder *EPS_ASCII*.
4. (optional) The outgoing script specified for that partner gets executed (the variable *FILENAME* will be assigned the files name).

## Partner independent timer scripts

Timer scripts get executed independent of any partner settings in regular intervals. They can be used for instance to regularly execute an external program like FileWork to receive new files and save these to the incoming folders of the respective partners. From there the files will get processed automatically (see processing of incoming data). Timer scripts also can be used to send data e.g. only once a day instead of using outgoing scripts which execute as soon as a new file is processed.

## !MC5 script variables

!MC5 EPS scripts can use additional variables, which will each time be replaced with their assigned values prior to execution of the script. You can use global variables, which have to be defined and set using the windows registry, and local variables, which have script or partner dependent values. Partner dependent values can only be used in incoming and outgoing scripts and can be defined using the partner management.

These variables can be used in both scripts and parameter files.

**Global variables**

- ***%GLOB:Name%*** - Get assigned values defined in the windows registry in the registry key *HKEY_LOCAL_MACHINE\Software\Bartsch Software\GlobalVars*.

**Local variables**

- ***%VAR:BATCH%*** - File name of the script itself.
- ***%VAR:PARAMTEXT%*** - File name of the parameter file.

**Partner dependent variables**

- ***%VAR:P1%*** ... ***%VAR:P8%*** - Variables containing values freely definable for each partner.
- ***%VAR:FOLDER%*** - Incoming or outgoing folder of the respective partner, depending on script type.
- ***%VAR:FILENAME%*** - Value of the field *File pattern / name* as specified in the partner settings or, in case of an outgoing script, the file name of the processed file.
- ***%VAR:FILEMASK%*** - Value of the field *File pattern / name* as specified in the partner settings.

### 4.4.1 Example: X.400 using FileWork

The following example shows how to use the add-on EP Scripting to realise file transfer via X.400 using the program FileWork by T-Systems. The example is kept simple. Both Windows Batch Scripting and the FileWork Scripting Interface offer advanced features for more complex processing, that demonstrated in the example.

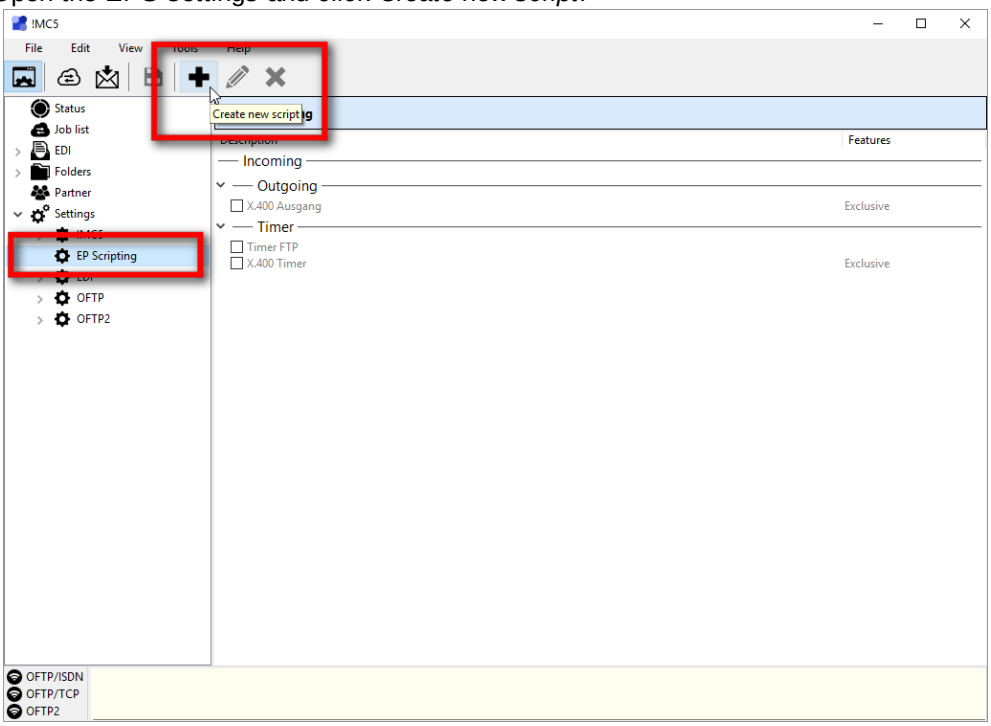
#### FileWork Setup

Prior to set up X.400 settings in !MC5, FileWork has to be configured to work with EP Scripting. To use the FileWork Scripting Interface a valid login to FileWork is required. The option "Status bei Verbindungsende" has to be deactivated in FileWork.

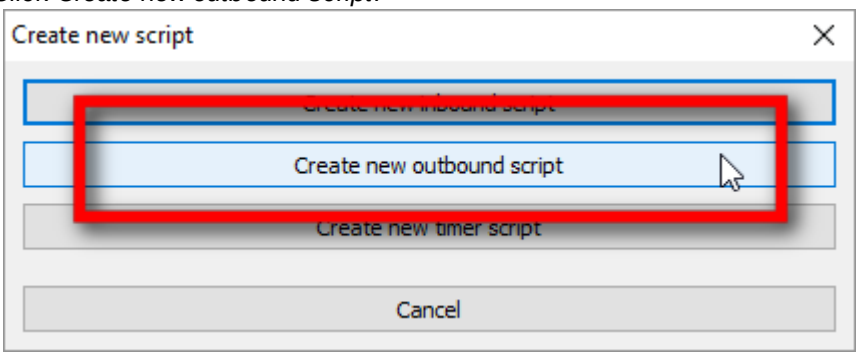
#### Ausgangs-Skript anlegen

The first step in !MC5 is to create a new sending script:

**1** Open the EPS settings and click *Create new script*.

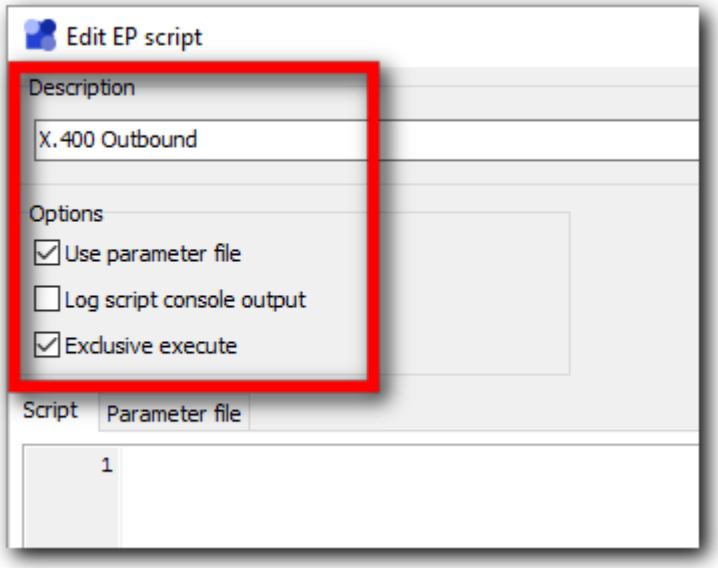



**2** Click *Create new outbound script*.

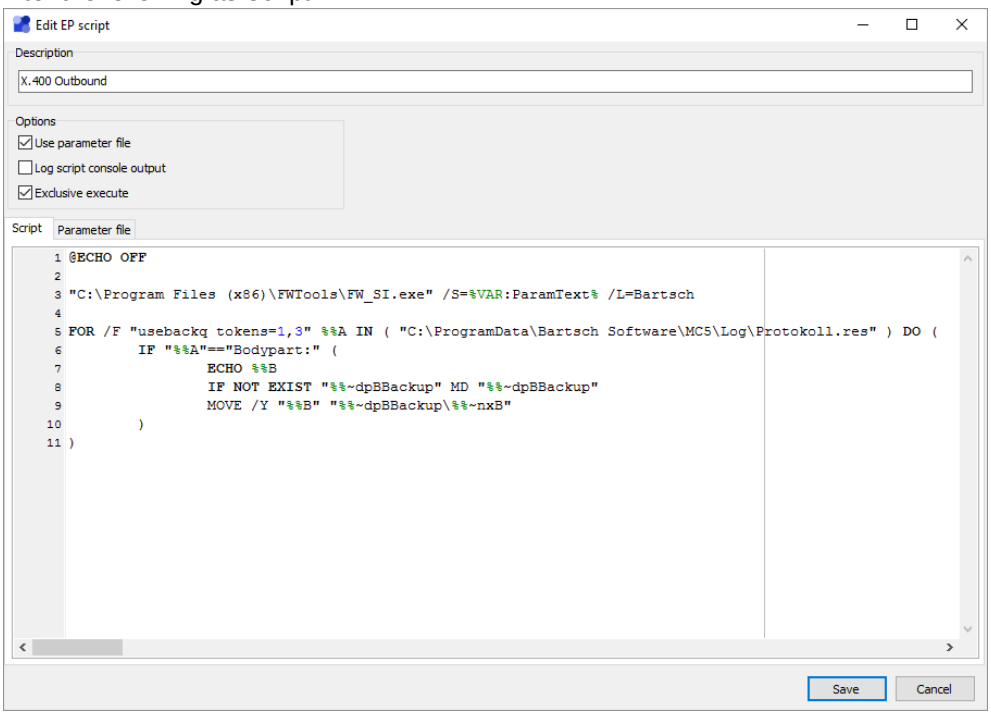



**3** Enter a script description (this description will be used as the script name), e.g. "X.400 sending". Then activate *Use parameter file* and *Exclusive execute* in the Options box. The parameter file is used to control FileWork, exclusive execution of the

script is necessary to not run FileWork multiple times at once, as that could cause problems when evaluating the result protocol.




**4** Enter the following as script:



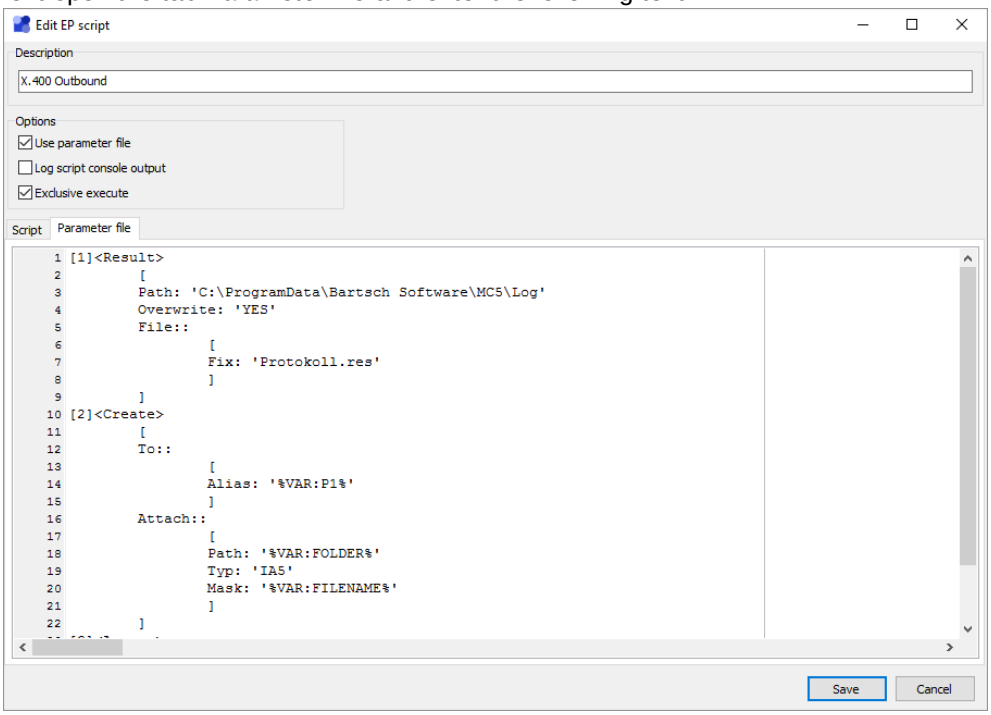

```
@ECHO OFF

"C:\Program Files (x86)\FWTools\FW_SI.exe" /S=%VAR:ParamText% /L=Bartsch

FOR /F "usebackq tokens=1,3" %%A IN ( "C:\ProgramData\Bartsch Software\MC5\Log\Protokoll.res"
     IF "%%A"=="Bodypart:" (
            ECHO %%B
            IF NOT EXIST "%%~dpBBackup" MD "%%~dpBBackup"
            MOVE /Y "%%B" "%%~dpBBackup\%%~nxB"
     )
)
```

The script is made up of essentially two parts. The line `"C:\Program Files (x86)\FWTools\FW_SI.exe" /S=%VAR:ParamText% /L=Bartsch` calls the FileWork Script Interface and passes the parameter file as parameter */S=%VAR:ParamText%*. This file contains the commands for FileWork. Login data is passed using the parameters */L=Bartsch* for the login name, and, if necessary, the parameter */P=Password* for the password. Replace the values with your login credentials.

The lines following the FileWork call parse the result protocol and move sent files into the sub folder *Backup*.The protocol gets parsed for the Text Bodypart. Each line, that starts with Bodyparts contains the name of a sent file as third "word".

The script starts with the command *@ECHO OFF* to suppress echoing each call to the console. Inside the loop *ECHO %%B* outputs each parsed file name. Those commands are for logging, if the option to log console output to the protocol is activated.

**5** Next open the tab *Parameter file* and enter the following text:




```
[1]<Result>
     [
     Path: 'C:\ProgramData\Bartsch Software\MC5\Log'
     Overwrite: 'YES'
     File::
            [
            Fix: 'Protokoll.res'
            ]
     ]
[2]<Create>
     [
     To::
            [
            Alias: '%VAR:P1%'
            ]
     Attach::
            [
            Path: '%VAR:FOLDER%'
            Typ: 'IA5'
            Mask: '%VAR:FILENAME%'
            ]
```

```
     ]
[3]<Access>
     [
     Submit: '0'
     ]
```

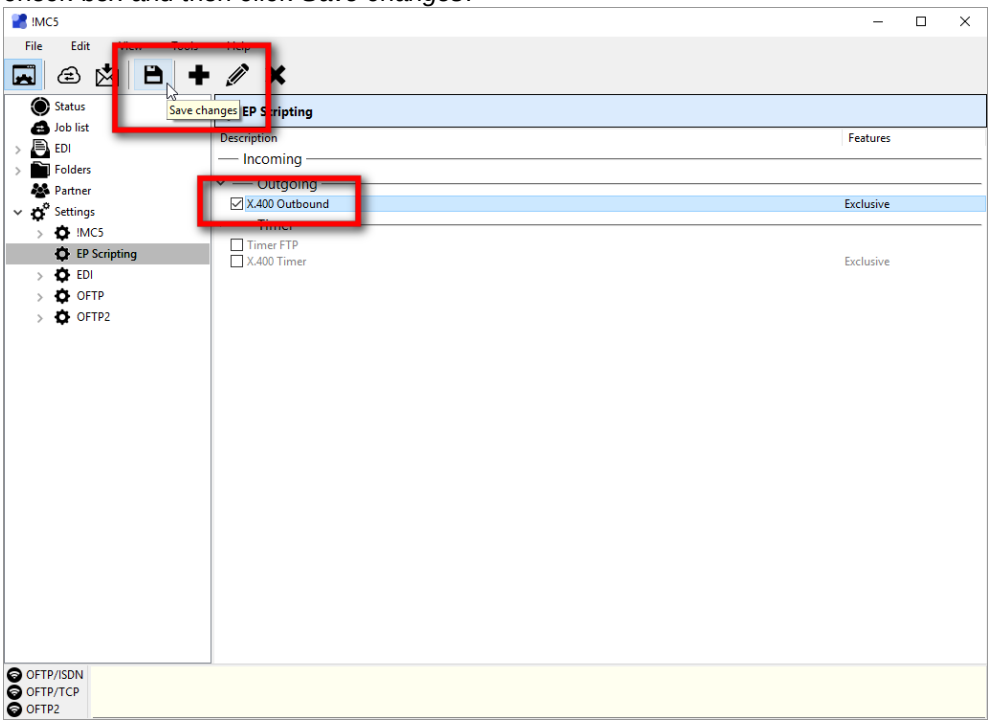
The parameter file contains commands for the FileWork Scriptinterface. Result defines protocol file settings. The path for the protocol has to be the same as used in the for loop of the script. The file name specified as *Fix* also has to be the same as the one in the loop.

*Create* tells FileWork to create a X.400. The receiver can either be specified using an alias, which has to be set in FileWork, or as X.400 address. If using an alias use the parameter *Alias*, else the parameter *Address*. The value for the parameter gets set using the !MC5 variable *VAR:P1* which gets defined in the partner settings. The attachment type is set to *IA5* in this example. *VAR:FOLDER* and *VAR:FILENAME* get replaced by the respective fields in the !MC5 partner settings.

*Access* tells FileWork to connect to the X.400 mailbox and send all previously created messages.

Refer to the FileWork manual for further details about available commands and parameters.

**6** Save the script by clicking *Save*. To activate the script, check the corresponding check box and then click *Save changes*.

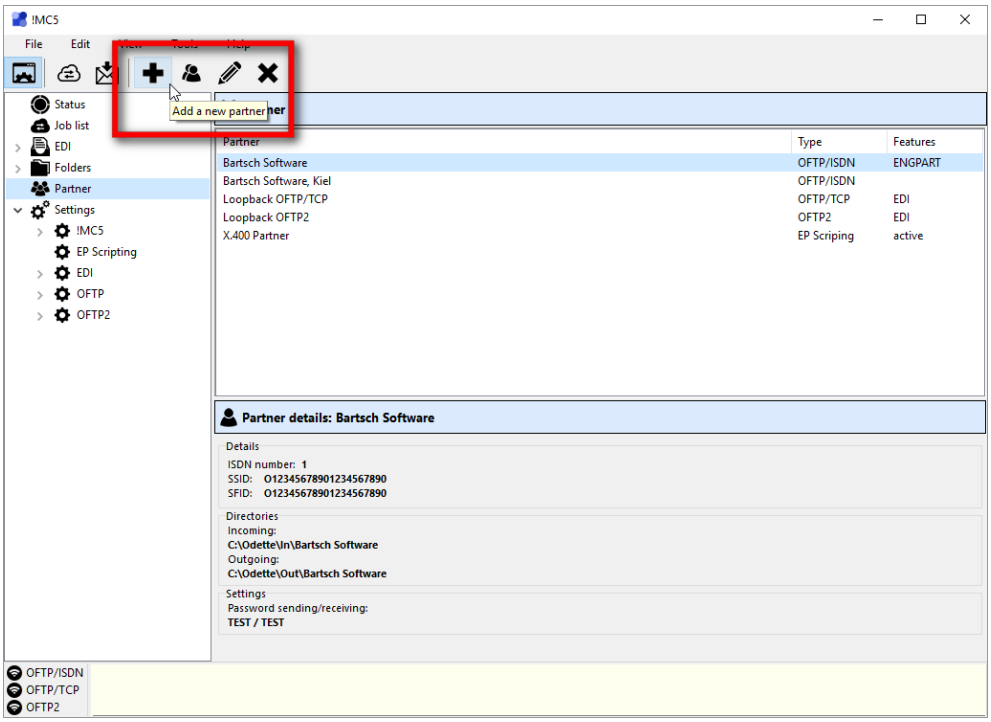



By using !MC5 script variables this script can be used to send files via X.400 for any EPS partner.

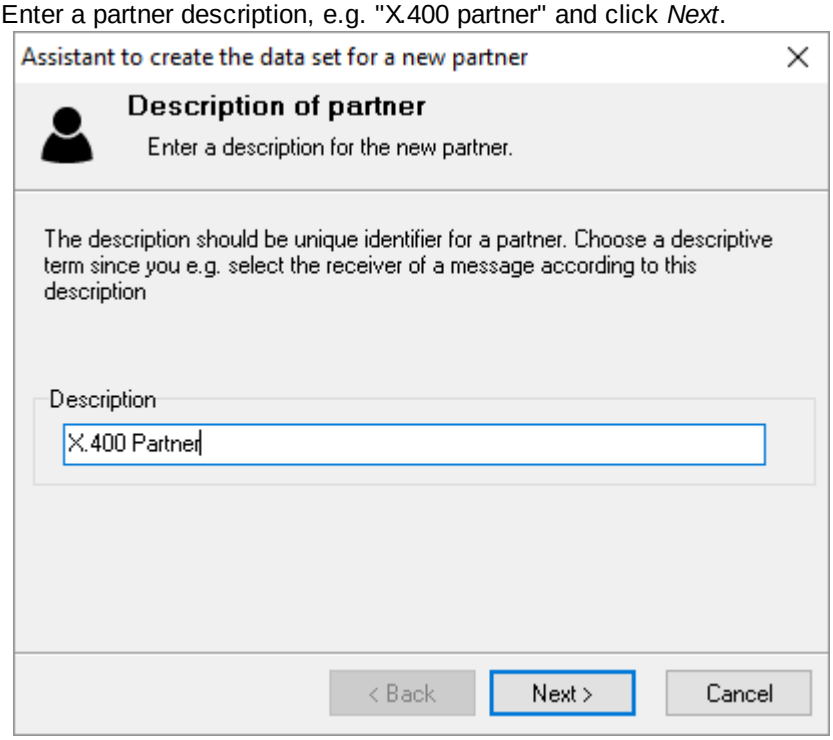
## Create a new EPS partner

To use the newly created outbound script, an EPS partner has to be created:

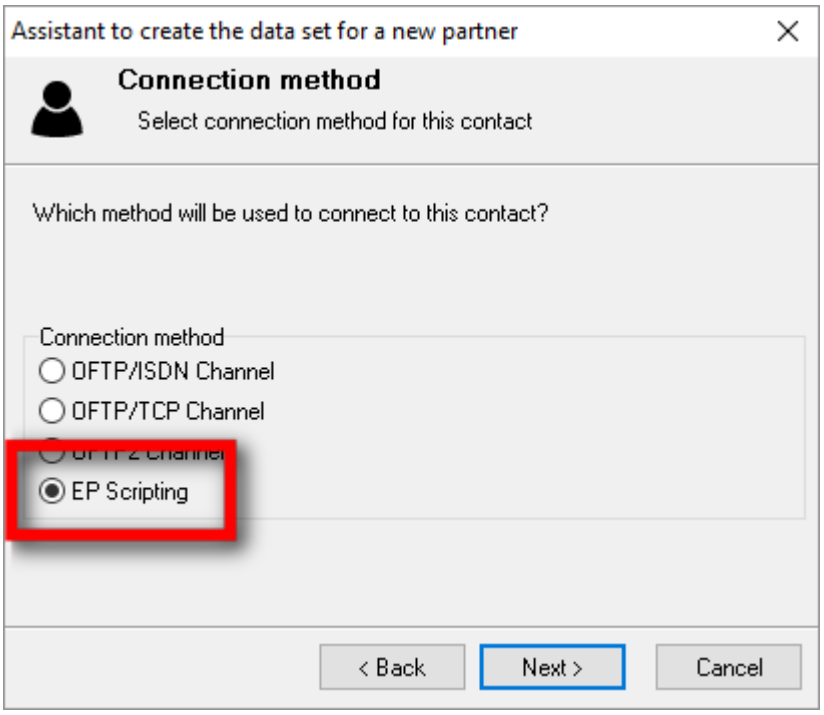
**1** Open the partner management and click *Add a new partner*.



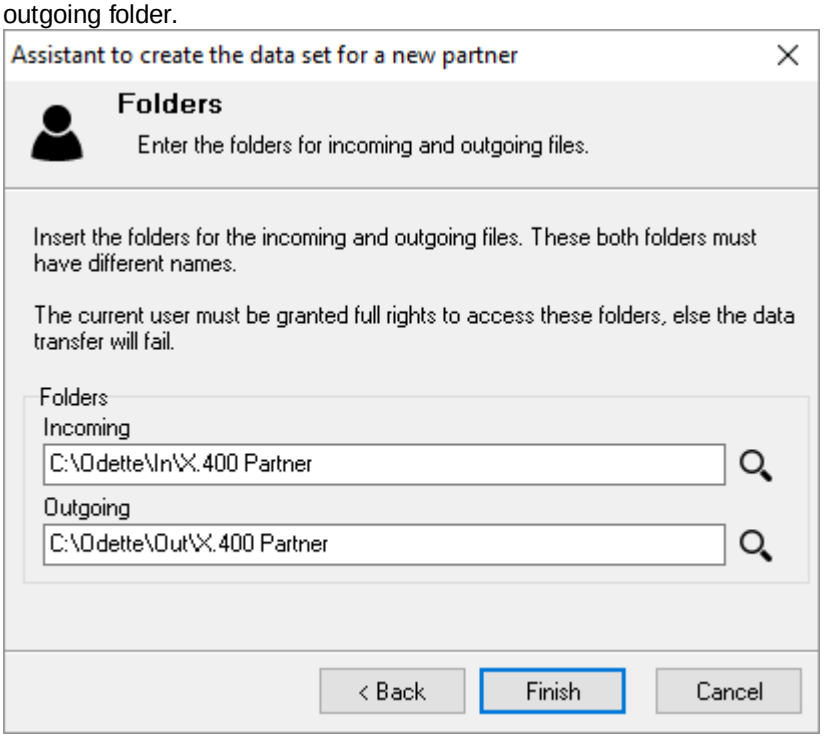

**2** Enter a partner description, e.g. "X.400 partner" and click *Next*.




**3** Select the option *EP Scripting* as connection type and click next.

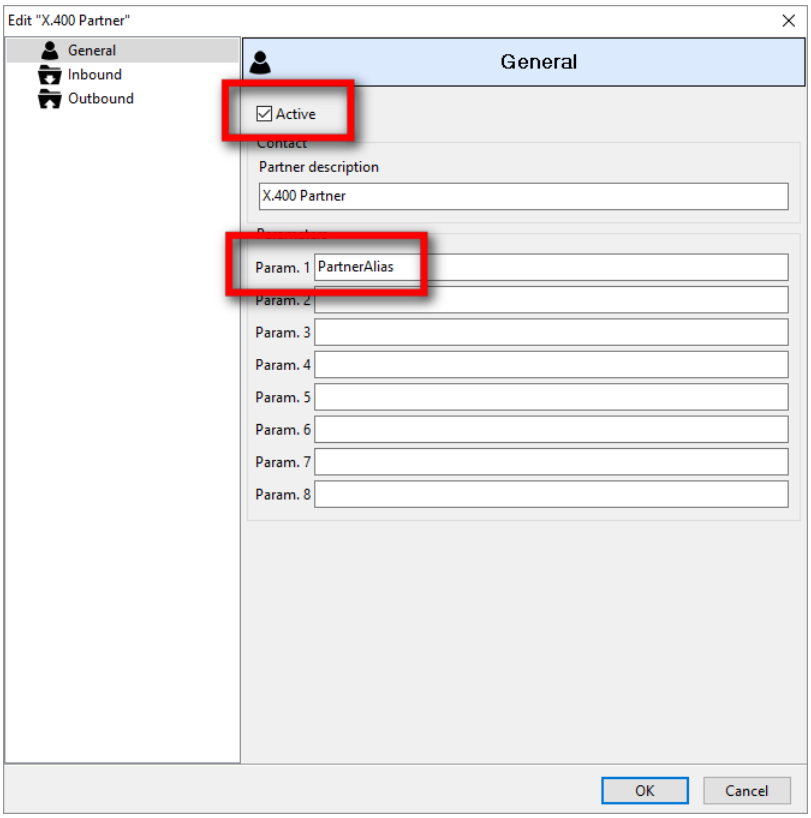



**4** Select incoming and outgoing folders, then click *Finish*. !MC5 scans the incoming folder in regular intervals for new files and saves file to be sent to this partner into the outgoing folder.

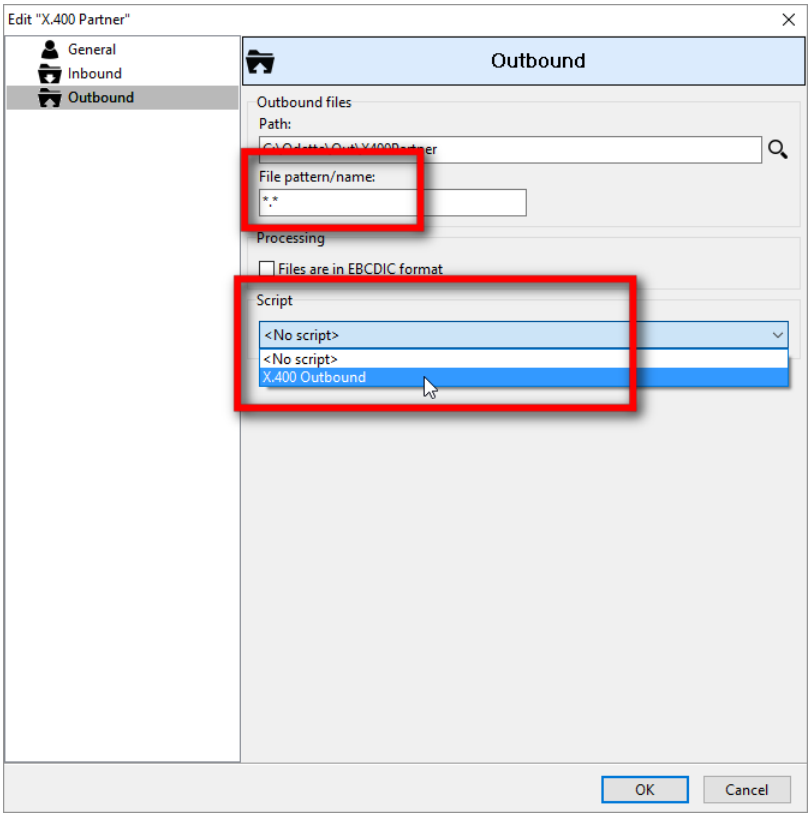



**5** Now edit the partner by either double clicking its entry or marking it and then clicking the *Edit partner* button.

**6** Open the *General* page and activate the option *Active*. This activates scanning for incoming files and execution of inbound and outbound scripts. Enter into the field *Param. 1* either the X.400 alias or X.400 address depending on which parameter you used in the parameter script.




**7** Change to the page *Outbound* and select the previously created script "X.400 Outbound". Enter a file pattern for the files to be sent to this partner into the field *File pattern/name*.

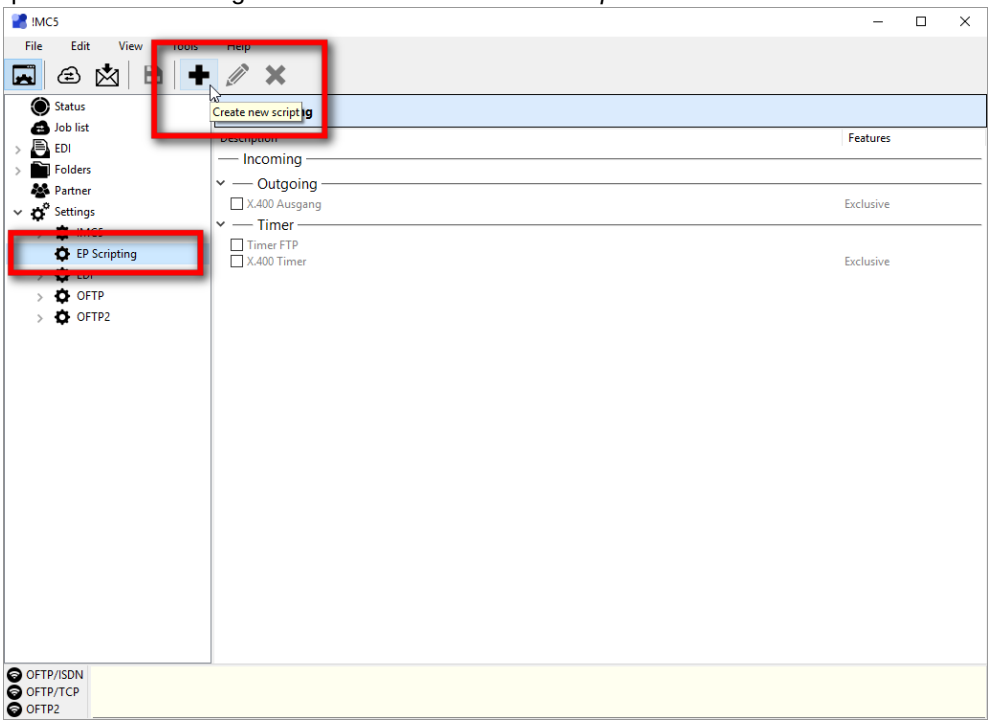


**8** Save the settings by clicking *OK*. From now on you can use this partner in import or automatic file transmission rules to send files via X.400.

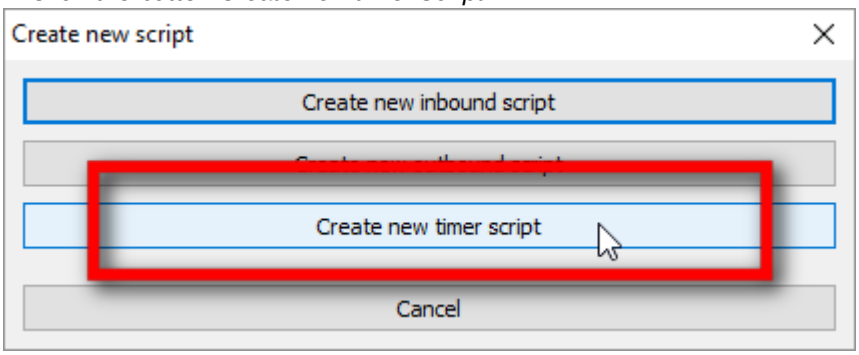
## Timer script for receiving files

Receiving files via X.400 using FileWork can be done using a timer script, which executes regularly and saves new files into the incoming directory of a partner:

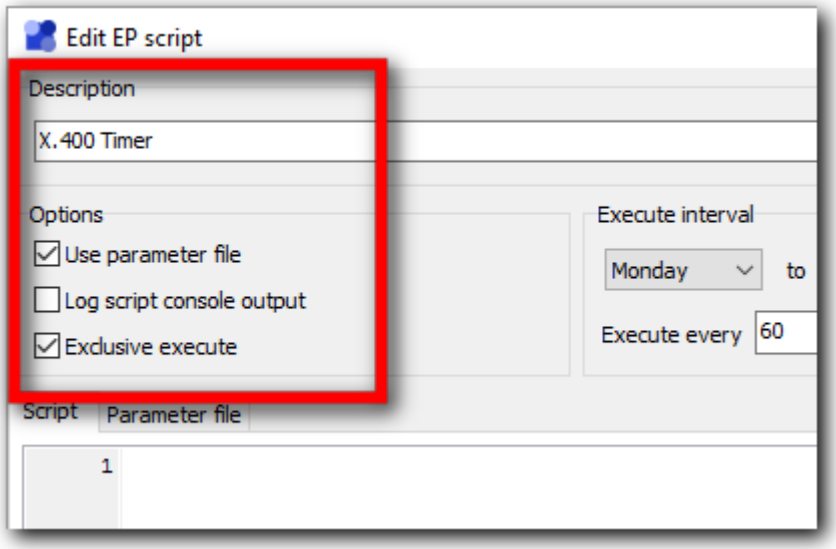
**1** Open the EPS settings and click the *Create new script* button.



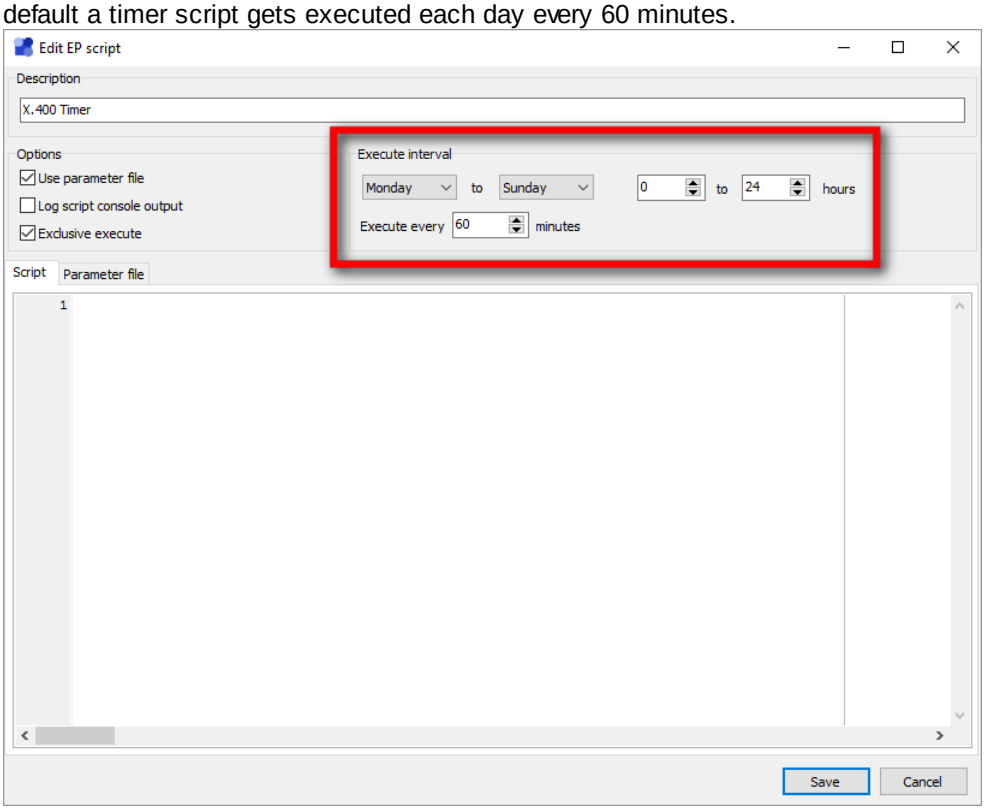

**2** Click the button *Create new timer script*.



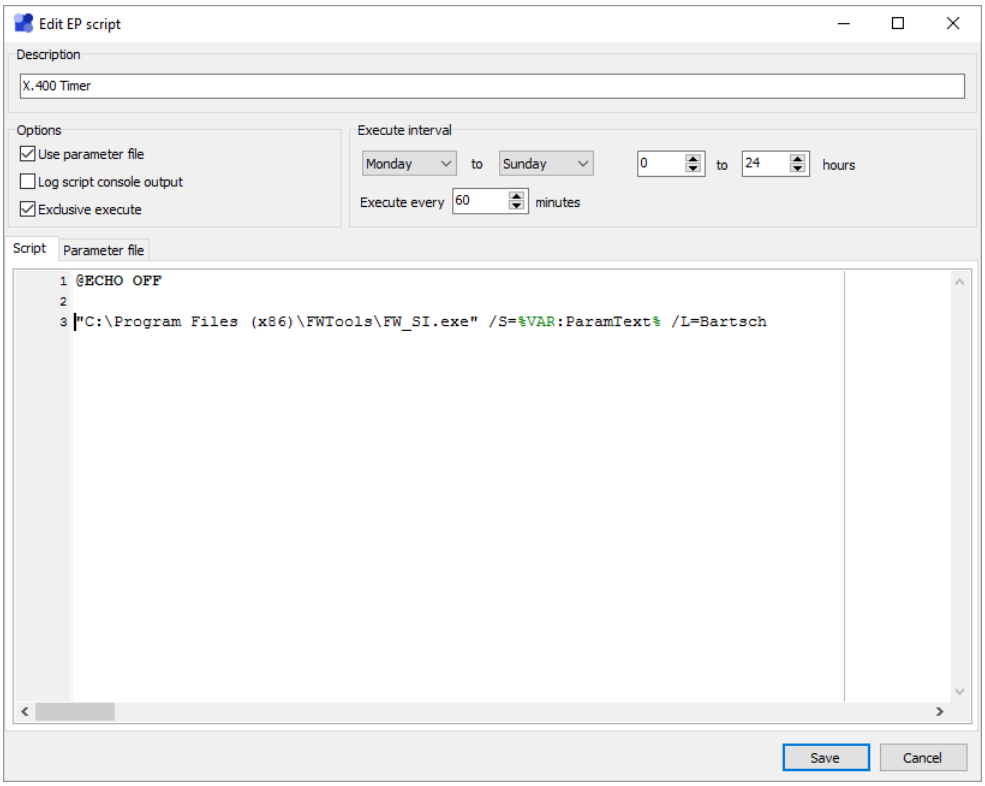

**3** Enter a script description, e.g. "X.400 Timer". This description will be used as script display name throughout !MC5. Then activate the options *Use parameter file* and *Exclusive execute*.




**4** Define the time interval, in which the script is to be executed. You can select start and end day of week and start and end time for each day. Then select the interval in minutes in which you want the script to get executed under *Execute every [...]*. By default a timer script gets executed each day every 60 minutes.

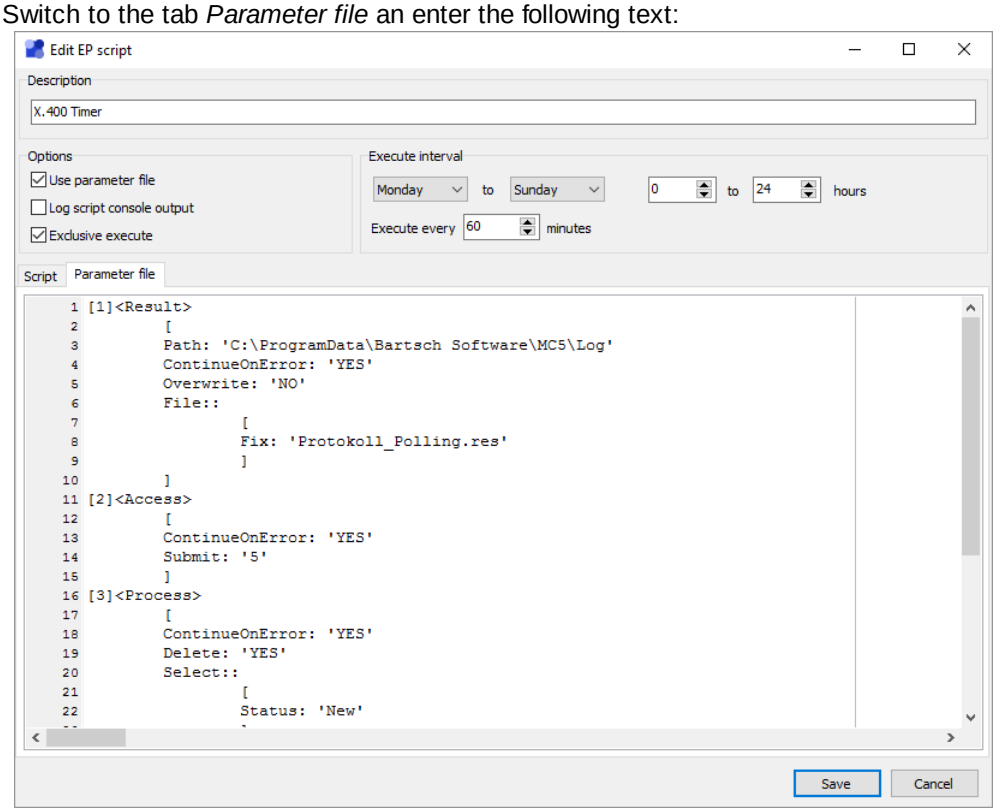



**5** Enter the script in the tab *Script*. The script itself is quite simple. Nothing has to be moved, only FileWork has to be called:




```
@ECHO OFF

"C:\Program Files (x86)\FWTools\FW_SI.exe" /S=%VAR:ParamText% /L=Bartsch
```

**6** Switch to the tab *Parameter file* an enter the following text:

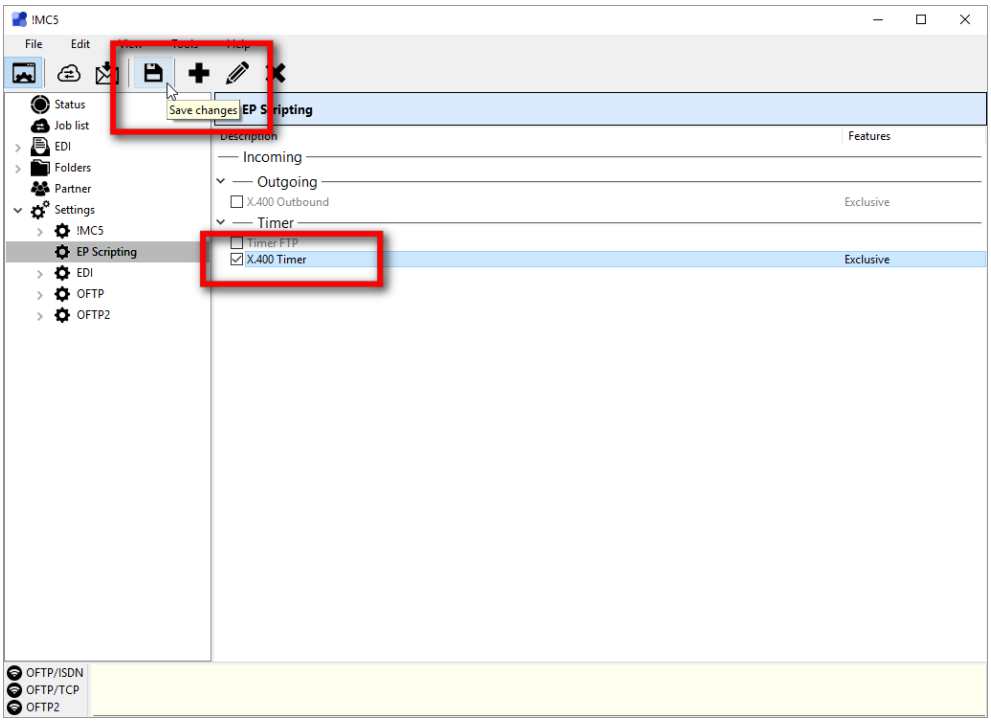



```
[1]<Result>
     [
```

```
        Path: 'C:\ProgramData\Bartsch Software\MC5\Log'
        ContinueOnError: 'YES'
        Overwrite: 'NO'
        File::
                [
                Fix: 'Protokoll_Polling.res'
                ]
        ]
    [2]<Access>
        [
        ContinueOnError: 'YES'
        Submit: '5'
        ]
    [3]<Process>
        [
        ContinueOnError: 'YES'
        Delete: 'YES'
        Select::
                [
                Status: 'New'
                ]
        Extract_File::
                [
                Path: 'C:\Odette\In\X.400Partner'
                ]
        Extract_Data::
                [
                Path: 'C:\Odette\In\X.400Partner'
                ]
        Extract_Txt::
                [
                Path: 'C:\Odette\In\X.400Partner'
                ]
        ]
```

This parameter file tells FileWork to download all new messages and save attached files to the specified partner incoming directory. Once saved there, !MC5 will detect the new files once it scans the EPS partner incoming directories and then will start processing the files.

**7** Save the script by clicking *Save*, then activate it by checking the check box in front of the scripts entry and click *Save changes*. The timer script is now active.



## 4.5 !MC5 remote control

### 4.5.1 Client/Server TCP/IP

The Add-On Client/Server for !MC5 enables the use of a separate client software. The client can be installed onto an unlimited number of local PCs. It allows the starting of sending jobs and the download of previous received files. The client also receives status messages regarding the sending jobs it initiated. The access rights of clients can be managed with the group and user settings in !MC5. The server part also supports the forwarding addresses of ENGDAT. This enables partners to address users and user groups directly.

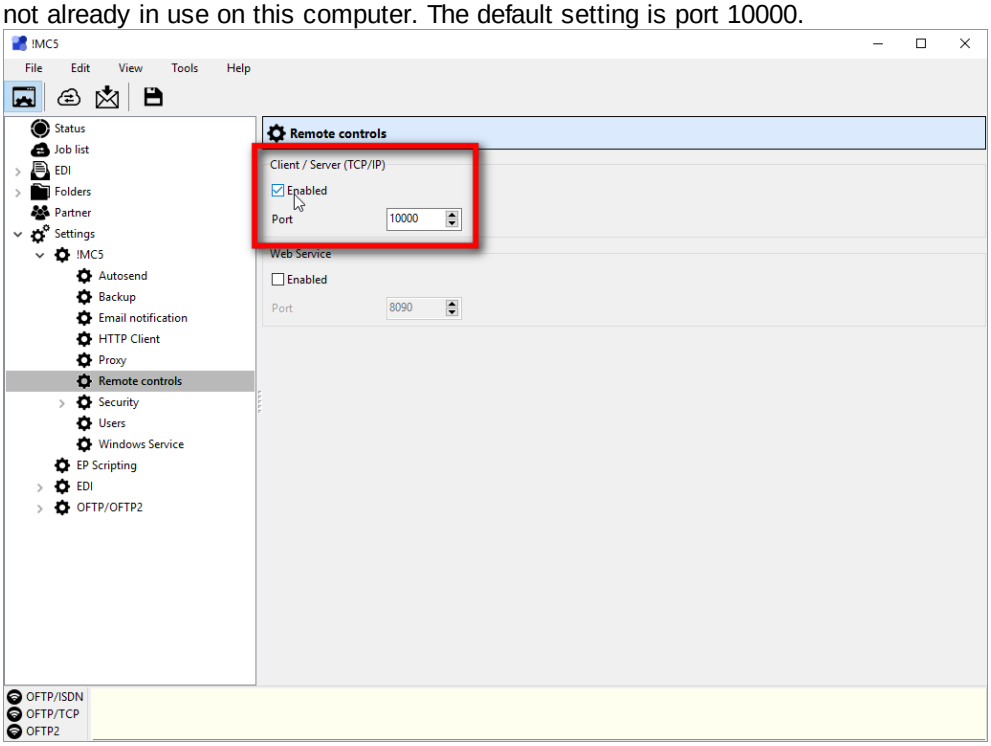
#### 4.5.1.1 Installation and setup

Prior to working with the Add-On Client/Server the server and the clients must be set up first:

1 Install the !MC5 TCP/IP Client on all client PCs. The client setup can be found in the program folder of !MC5. It is named *SetupClient_e.exe*.

2 Start !MC5, and open the section *Settings / !MC5 / Remote control* in the navigation tree.

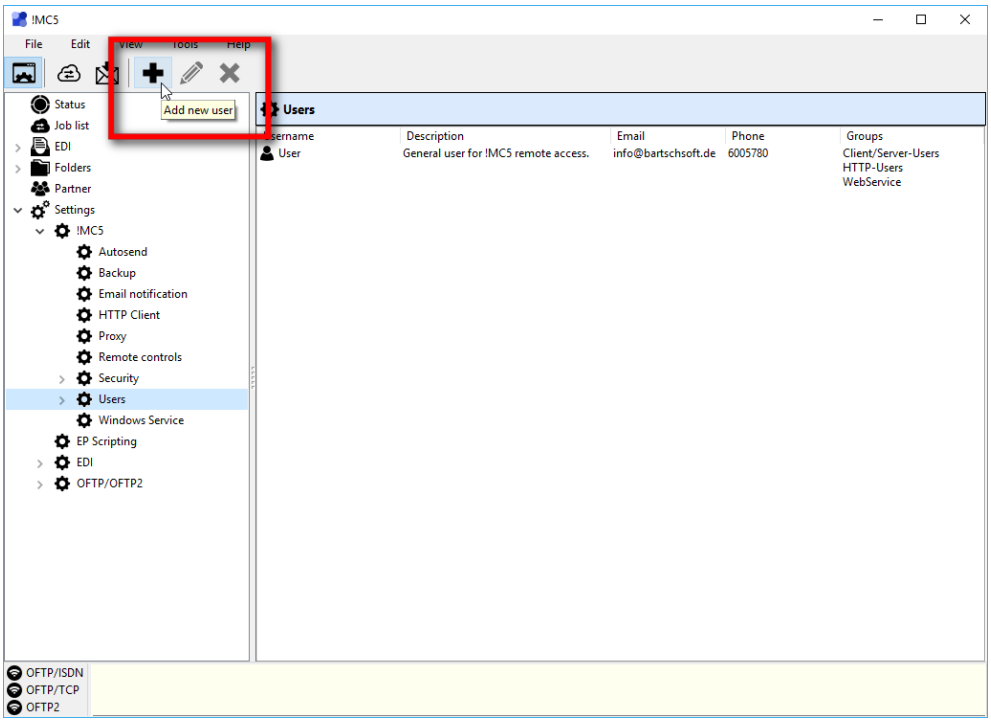
3 Activate the option *Active* in the box *Client/Server (TCP/IP)* and assign a *Port* that is not already in use on this computer. The default setting is port 10000.



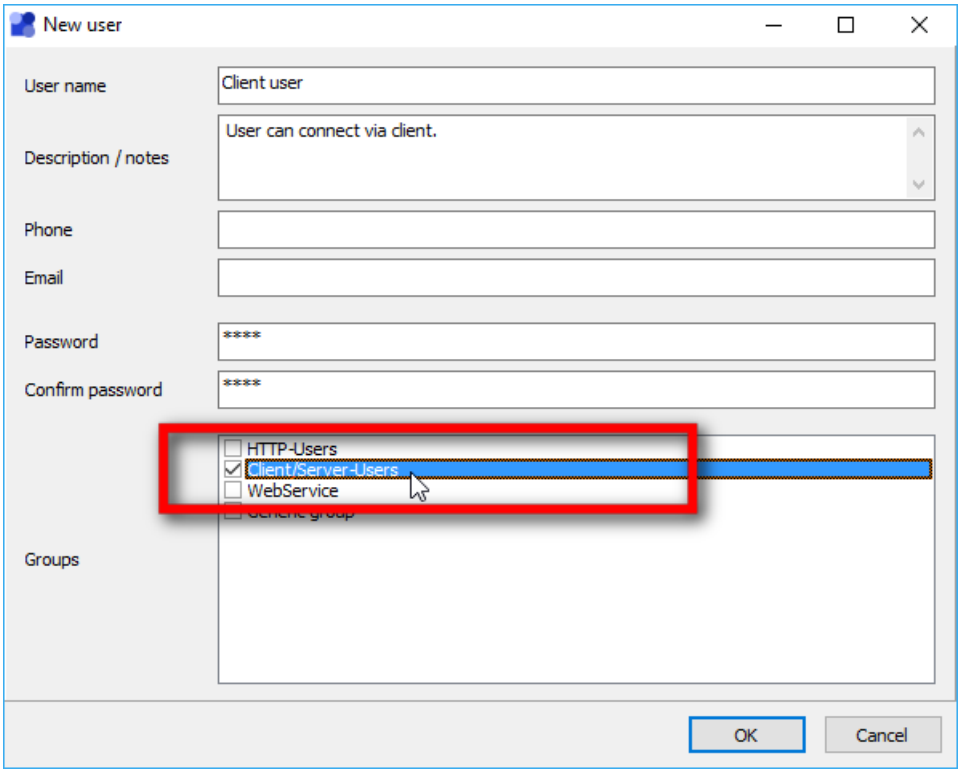

> **Open the port in Windows-Firewall**
> If there is a local firewall installed you will most likely have the open the assigned port here. Please consult the manual / helpfile of the firewall. Most firewalls will open a notification automatically when the port is used the first time. As long as the port is blocked there will be no client-server interactions possible.

4 Clients require a valid user name and password in order to connect to the server. These users need to be set up in !MC5. Open the user database found under *Settings / !MC5 / Users*.

**5** Click the button *Add new user.*




**6** The fields *User name* and *Password* are mandatory. Also click check the entry *Client/Server-Users* in the list Groups. This will enable access to !MC5 using the !MC5 Client for this user.




**7** Save the the new user by clicking *OK*. The server is now active and clients can connect using the created user account.

**Hint**

It is not possible that two client use the same user account. There should be a user account available for each client. When naming the user accounts please keep in mind that the forwarding address of ENGDAT can be used to address users directly. For this reason the length of the user names should not exceed 14 characters.

#### 4.5.1.2 User permissions and groups

The access rights granted to client users depend on their membership in groups. For the sending of files user access can be limited to a fixed set to partners. Following rules apply to the access rights:

### Incoming files

Files received by !MC5 are checked by the following rules and assigned accordingly to the clients. The rules are applied in the here stated sequence. Only the first matching will be applied.

- ***(ENGDAT only) Fowarding address of ENGDAT matches a User-ID*** - Whenever there are files received in ENGDAT format the contained forwarding address will always be checked first (Field used is S0003-0014 in the UNB segment). If it matches an existing User-Id the files will be available to this user alone. All other rules will not be tested.
- ***(ENGDAT only) Fowarding address of ENGDAT matches a Group-ID*** - Does the forwarding address of ENGDAT not match with any User-ID it will be tested next whether it matches a Group-ID. In this case the files will be forwarded to all members of this group. The following rules will not be tested.

> **Hint**
> The use of a Group-ID as forwarding address is in most cases much more useful than the single User-ID. The membership of the group is controlled locally. So the partner does not need to care if the composition of the group changes.

- ***A group is assigned to the partner account*** - Without ENGDAT forwarding this rule will be tested next. In the address window on the page *Special functions* user groups can be assigned to the partner account. When this is the case the files will be forwarded to all users of all groups assigned here.
- ***Access Right: Users get unassigned incoming files*** - When none of the rules above apply the files will be forwarded to all users which are members in a group with this access right set. If there is no user with this access right available there will be no forwarding at all.

### Outgoing files

For the outgoing direction the client access to partner accounts can be limited. The users must be assigned to a group with the option *Users are restricted to a limited partner selection* set. With this option set only the user will see no partner accounts at all. In order to make specific accounts visible to user the group must be assigned to the partner in the *Special functions* page of the address.

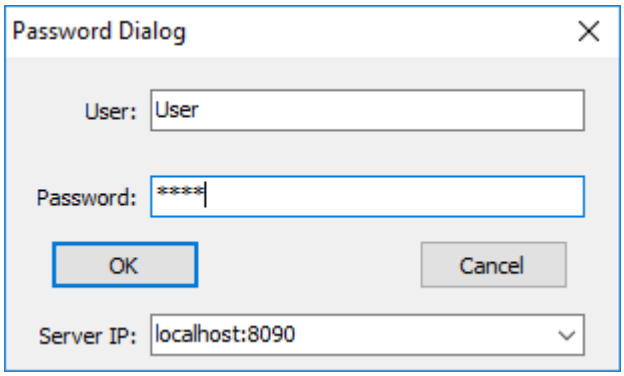
The visibility of a partner does not influence ENGDAT forwarding. The user is able to receive ENGDAT when it is directed to him. But he will not be able to send any files to this partner.

### 4.5.1.3 Using the client

!MC5 can be operated as usual. The sending jobs generated by clients are visible in !MC5 and can be deleted.

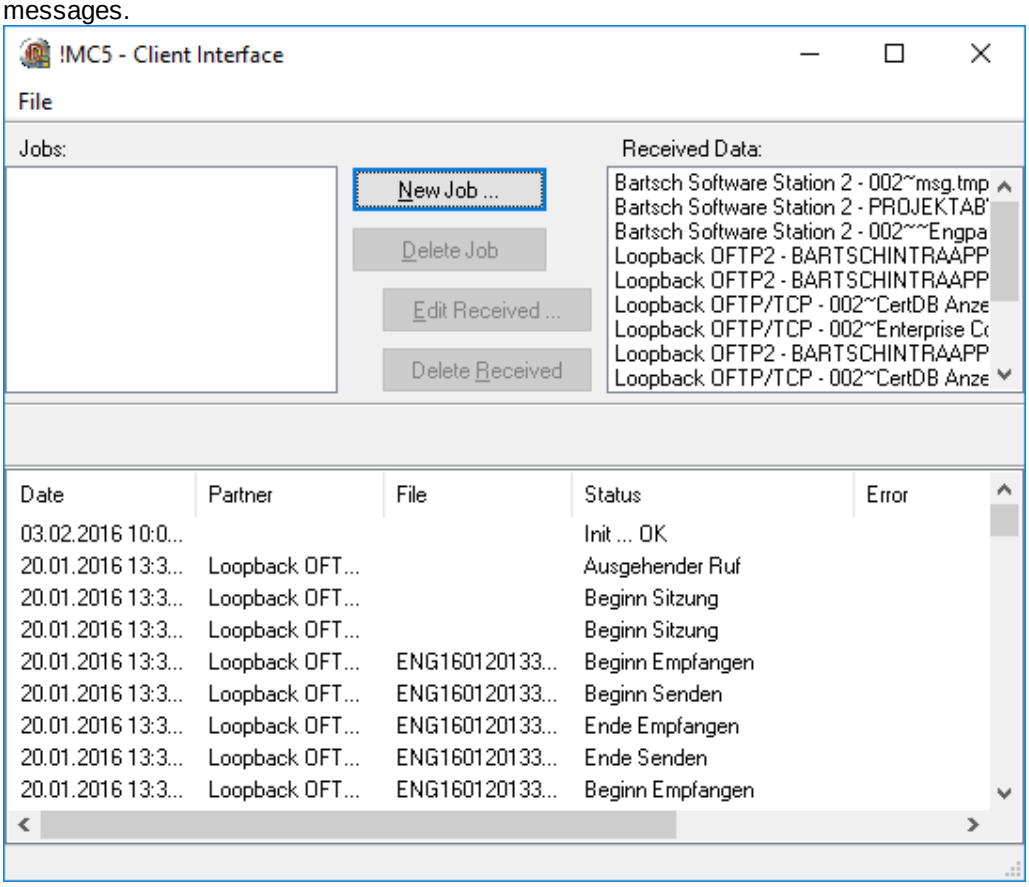
## Connecting to the server

After starting the client user name and password have to be entered (see also Installation and Setup). When the client is started first you will also have to enter the IP-address or the computer name. If the port is changed from the default 10000, it must also be entered in common notation, e.g. *Server:5555*.




## Client functions

The Odette-client implements three functions: creating of new sending jobs, giving status messages regarding the sending jobs to the user and notifying the user about received files. Each client gets only status messages regarding the sending jobs which were generated by itself. The user can be assigned to a group with the right to see more status messages.




**Hauptfenster !MC5 TCP/IP-Client**

The list *Jobs* in the upper left of the client window contains all partner names with pending jobs generated by this client. By marking an entry the progress of this sending will be shown below.

When a sending is marked it can also be deleted with the button *Delete job*. All successful finished jobs will be deleted automatically. Jobs that are already being processed can be deleted also. This will close the transmission immediately but will not influence files that are already have been transmitted. The files belonging to a deleted job can be deleted, kept in the out folder or moved into an error folder.

The list *Received Data* on the upper right of the window contains the names of all partners which have recently sent files to this client. When the files are in ENGDAT form the button *Edit Received* will show the assigned ENGDAT text. If an list entry is no longer needed it can be deleted with the button *Delete Received*. This function will not delete any files but only the list entry.

The list at the bottom of the window contains the status messages belonging to the sending jobs which were generated by itself. When the client is not connected to the server the server will store all messages regarding this client. They will be shown the next time client connects to the server.

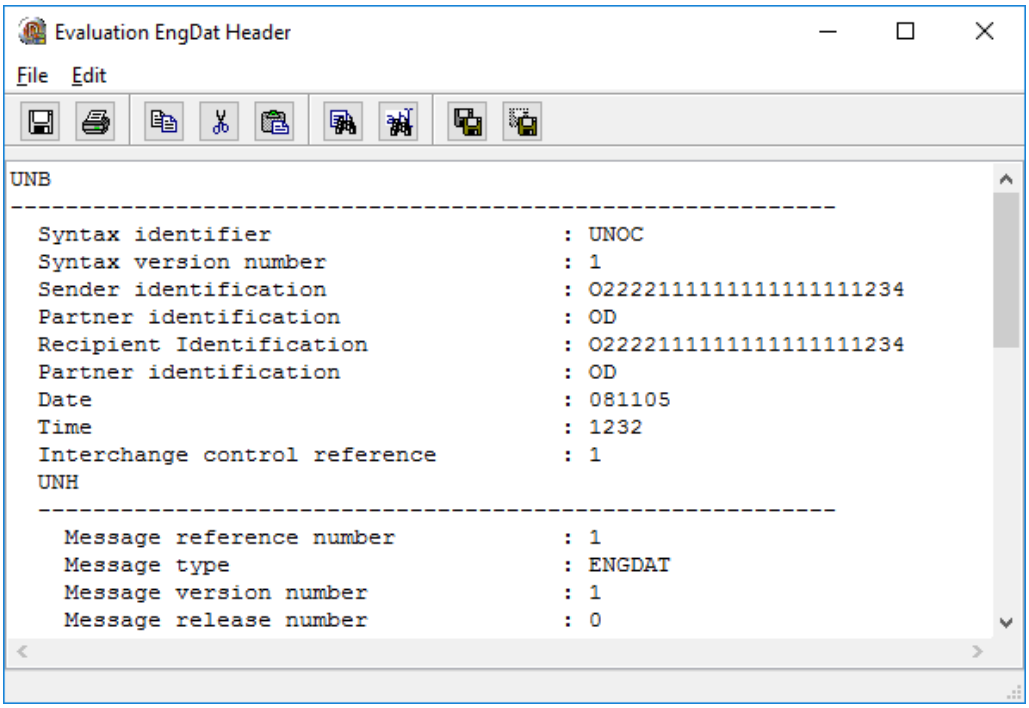
#### 4.5.1.3.1 Receiving files

### Receiving files in ENGDAT format

All files in ENGDAT format will be checked about the forwarding address by !MC5. If it matches an User-ID or a Group-ID the ENGDAT file set will be forwarded accordingly. It will be available for single user or all members of the group as soon as they log in.

If no match is found the other forwarding rules will apply (see User permissions and groups).

Received files will be shown in the client only after !MC5 has finished the complete transmission successfully. A list entry in *Received Data* always represents a set of files received in one transmission. By double-clicking an entry or by clicking on *Edit Data* the evaluation of the ENGDAT header-file will be shown.

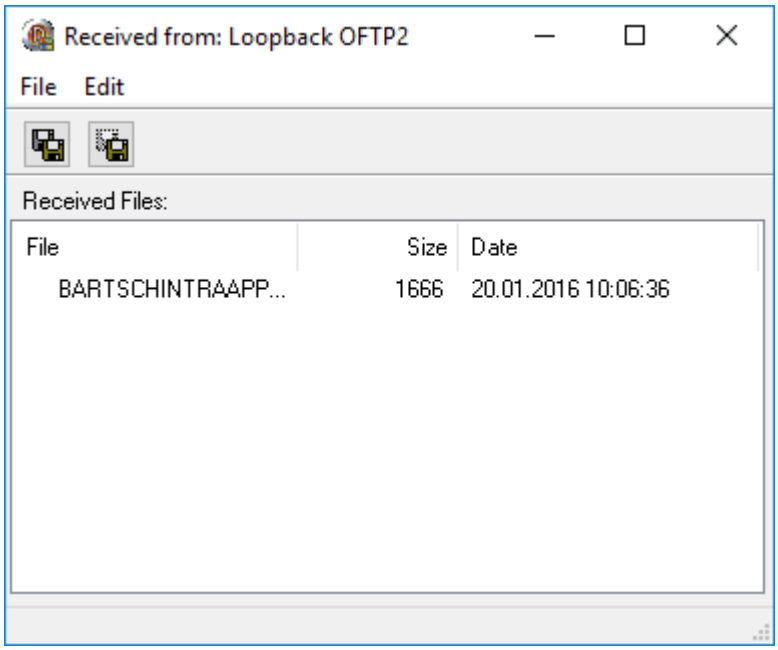



The contents of the ENGDAT header will be shown in a readable format. It can be edited with the usual text editor functions. In order to access the appended files there are the following functions available:

- - The received files will be copied into a local folder.
- - The received files will be moved into a local folder. After the files were successfully downloaded they will be deleted from the in-folder of !MC5. This function is available only to users with a membership in a group with right *Users can delete / move files*.

### Receiving other files

For all other files received the function *Edit Received* will only show a simple file list. As above there are also functions available for copying and moving files. Because there is no direct forwarding available the files will only be shown to group members with the according rights set (see User permissions and groups).

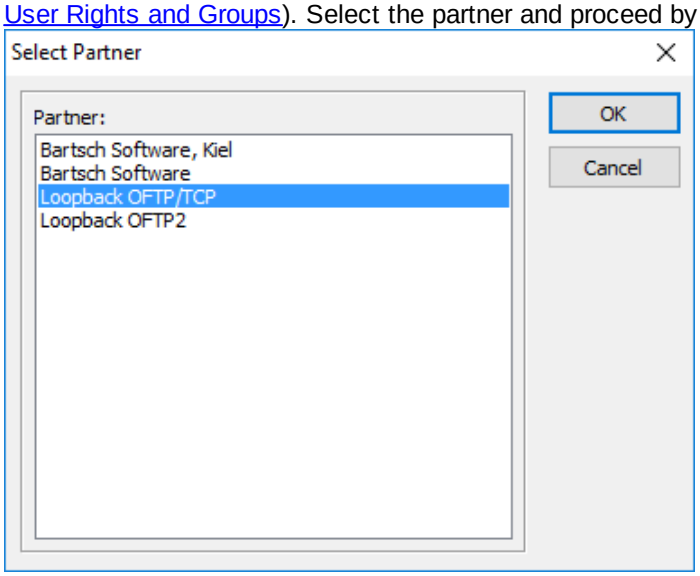


#### 4.5.1.3.2 Sending files

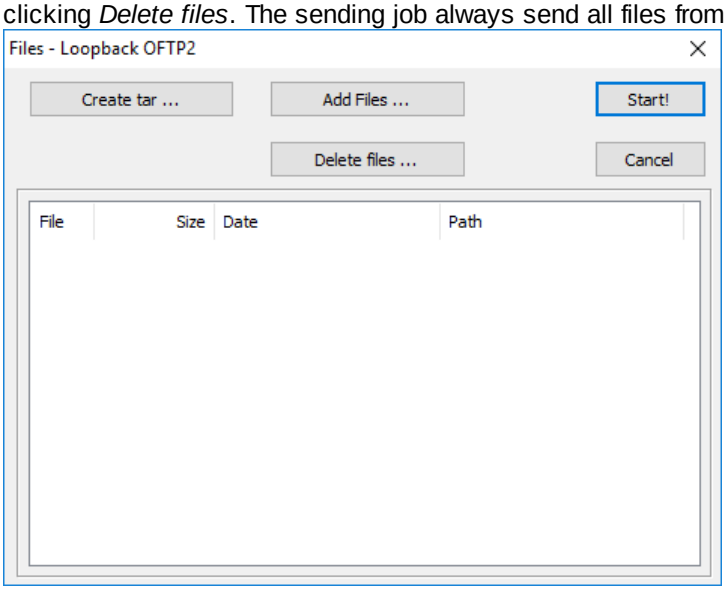
In order to send files from a client please proceed as follows:

1 Start the client and log in.

2 Click the button *New Job*. This will open a list of all partners available to this user (see User Rights and Groups). Select the partner and proceed by clicking *OK*.




3 The next screen shows the contents of the out-folder assigned to the partner on the server. Add files to the folder by clicking *Add files* and remove unwanted files by clicking *Delete files*. The sending job always send all files from this folder.

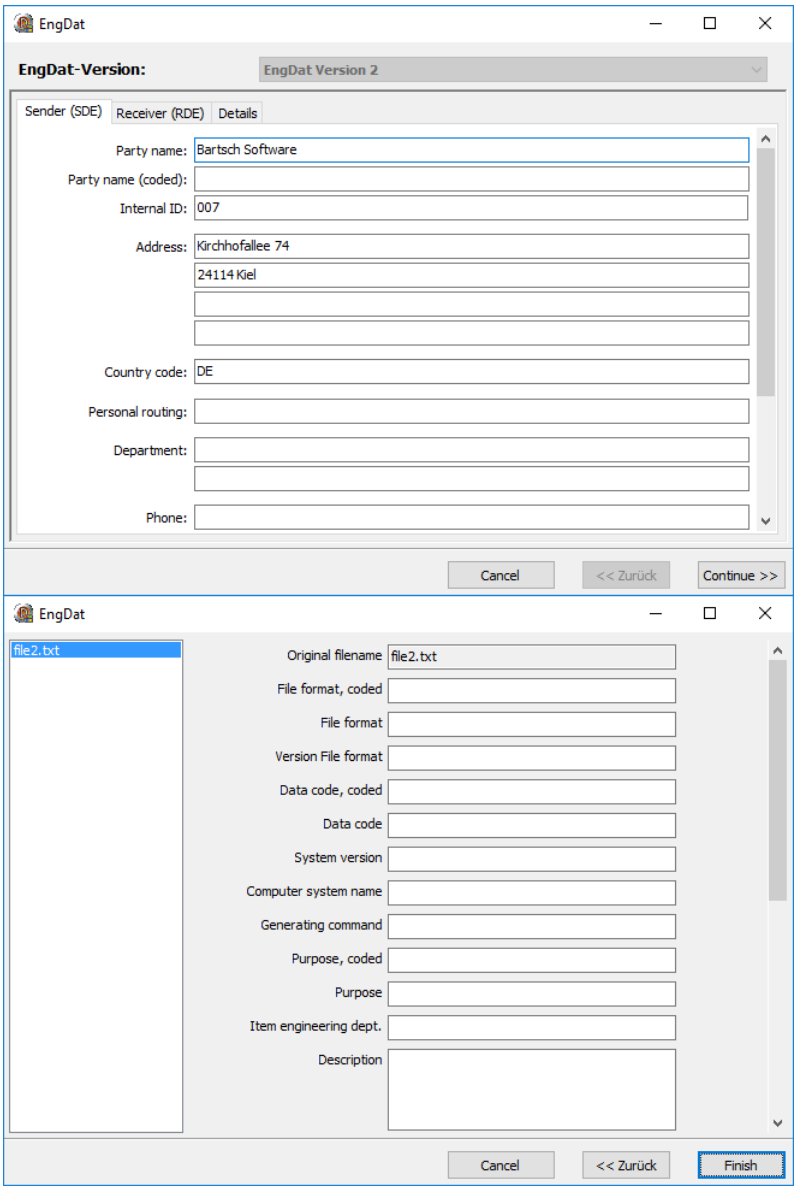



4 When ENGDAT and EngPart are disabled click *Start* in order to start the sending job. !MC5 will send the files to the partner as soon as possible.

> **Hint: ENGDAT / EngPart**
> A client cannot choose whether ENGDAT / EngPart is used or not. These settings can only be done in !MC5. The client user must ensure however that all mandatory ENGDAT fields are filled with valid data.

5 With ENGDAT or EngPart active the creation of the sending job continues with the ENGDAT settings.

6 The windows for ENGDAT and EngPart can be filled with additional information regarding single files and the complete file set.




**7** Click *Finish* in order to start the job. The files will be copied to the server, put into ENGDAT format and the sending job will be added to the job list.

### 4.5.2 HTTP Client

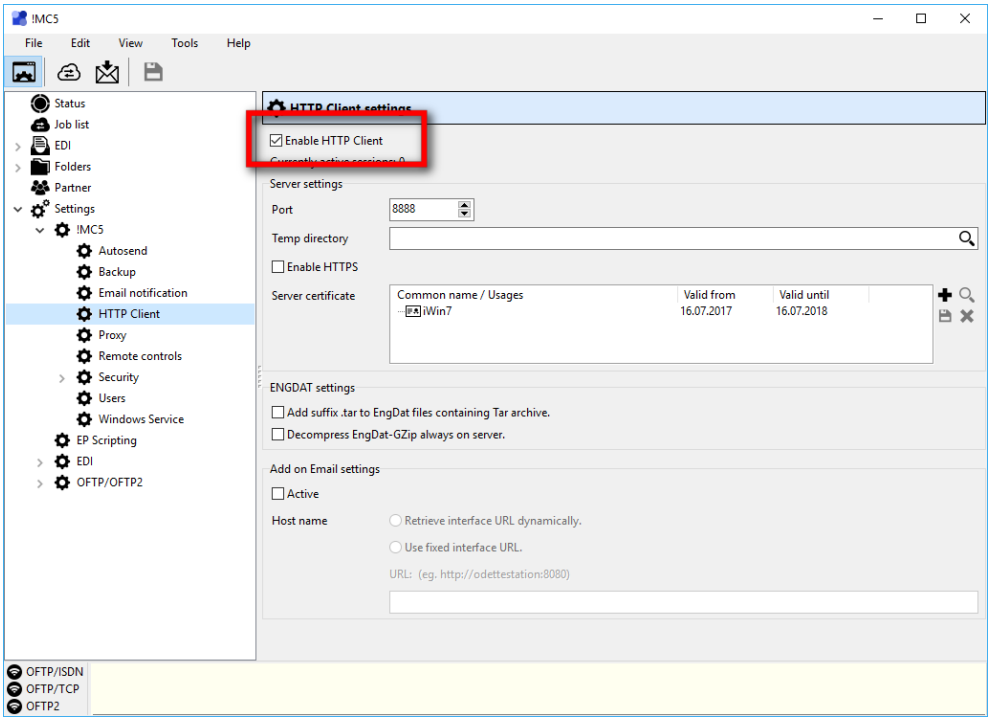
The HTTP Client enables remote control of functions of !MC5 with a normal web browser. It supports the sending of files, including ENGDAT / EngPart and the download of previous received files.

#### 4.5.2.1 Setup

Setup the HTTP Client as follows:

1 Start !MC5 and select the section *Settings / !MC5 / HTTP Client* in the navigation tree.

2 Click the option *Enable HTTP Client* and choose an unused TCP/IP port. This port will be used for connections to the HTTP Client later on.

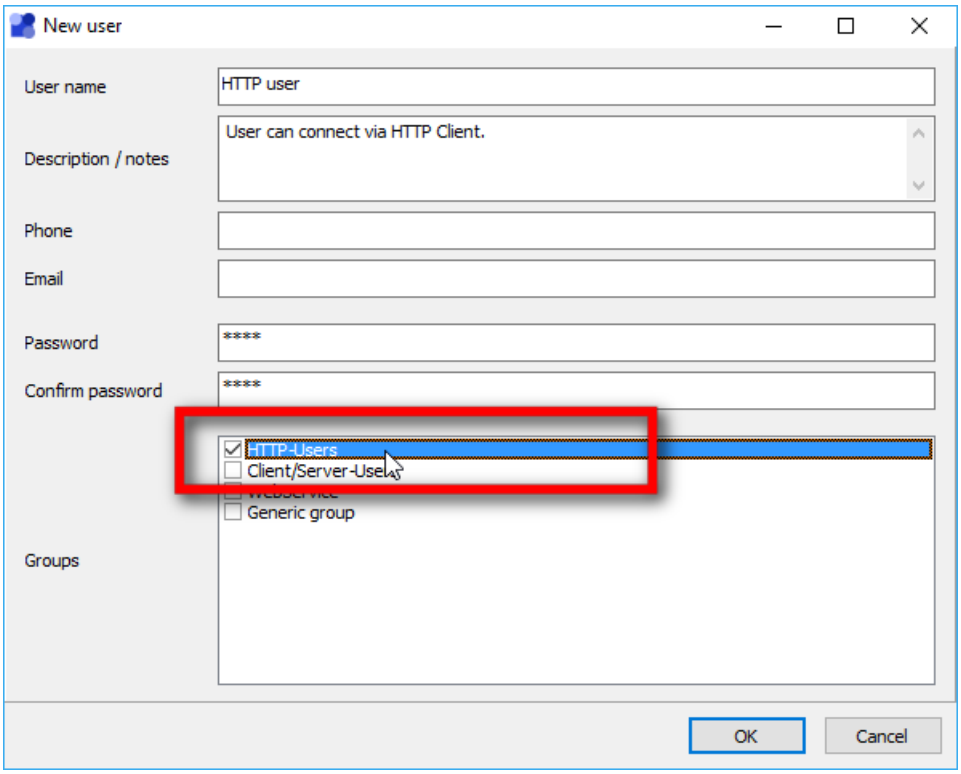



3 If necessary choose a *HTTP temp directory*. This directory will store temporary files during operation. The temporary directory of the current Windows user account will be used when no directory is entered here. Never choose a folder that contains data. The temporary directory will be deleted completely with each start of !MC5.

4 Before users can connect to the HTTP Client they will have to be added to the user database. For this select the section *Settings / !MC5 / Users*.

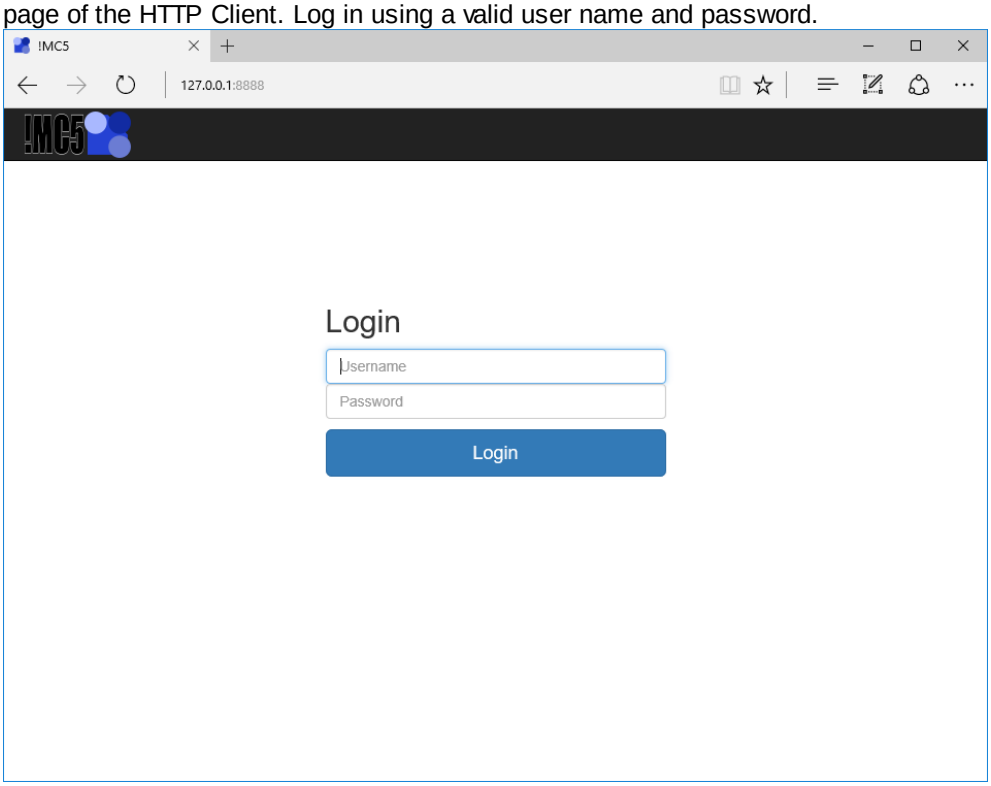
5 Add a new user or edit an existing one.

6 Check the entry *HTTP-Users* in the list *Groups* in order to grant this user access to the HTTP Client. Save the new setting by clicking *OK*.




**7** When all options are saved you can start your web browser.

**8** Enter *http://127.0.0.1:Port* into the address field of the browser. *Port* must be substituted with the previously selected port from the HTTP Client settings. Press enter to open the web page. If all settings are correct the browser will now show the login page of the HTTP Client. Log in using a valid user name and password.



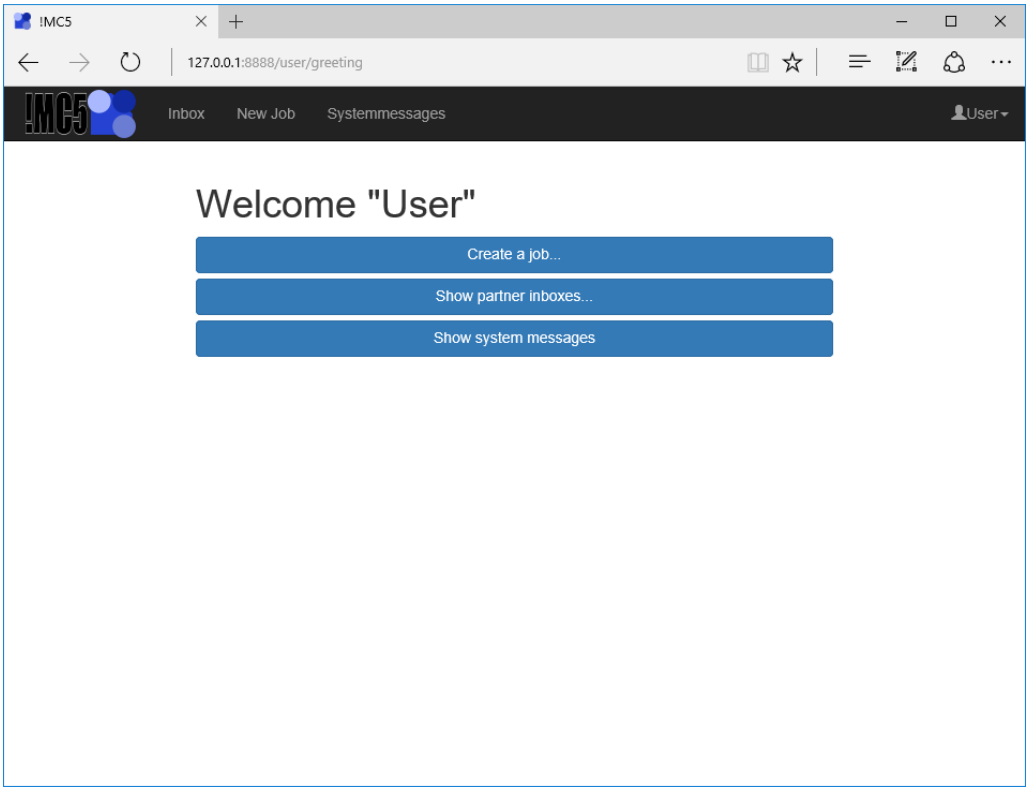
**Restriction of partners that are available to a user**

The selection of partners available to a user can be limited by membership in one or more groups with option *Users are restricted to a limited partner selection* set. The user will only see those partners that are assigned to at least one group that the user is a member in. The groups can be chosen in special functions section of the partner address account.

#### 4.5.2.2 Usage

In order to start the HTTP Client in your browser you will have to type the server name or its IP-address into the URL field. When a port other than 80 is used you also have to add the port, e.g. *http://192.168.0.100:1234*. This opens the login screen. Type in your user name and password here.

> **Hint:**
> Some browsers require the text *http://* before the IP or server name, whenever a port other than 80 is used. For proper operations Java-Script must be active.



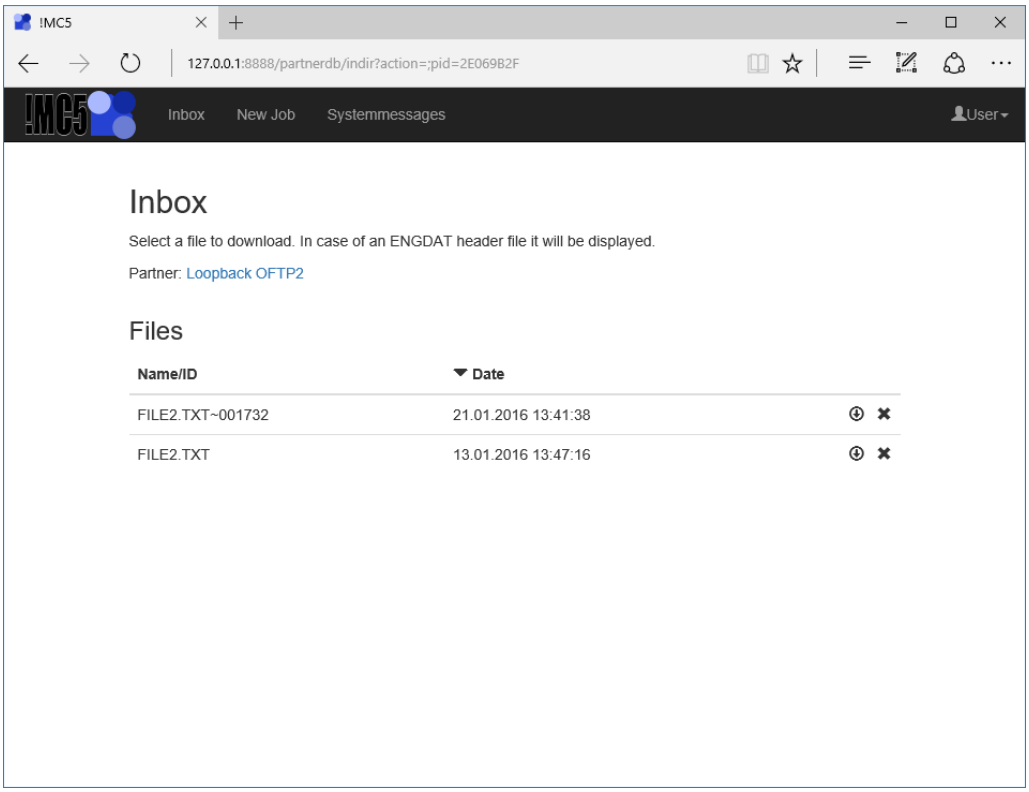

**!MC5 HTTP Client main menu.**

The welcome screen will appear after login. Following functions are available:

- ***!MC5 logo*** - Clicking the !MC5 logo brings you back to the main menu.
- ***Inbox*** - This function will show the contents of the in-folders of !MC5. Received files can be downloaded and ENGDAT will be shown in plain text.
- ***New Job*** - A new sending job can be generated with this function.
- ***System messages*** - Shows a list of system messages which were forwarded to this user.

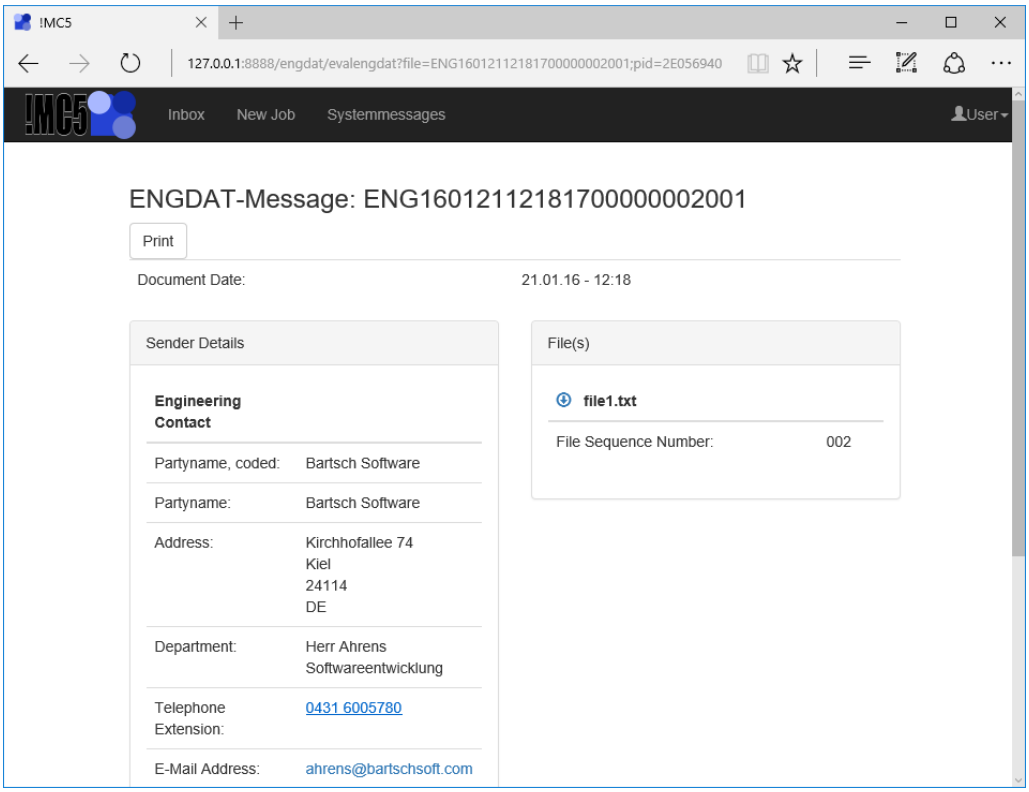
#### 4.5.2.2.1 Downloading files

A click on *Inbox* shows a list of all available partners. After selecting the partner all files previously received from him are shown.




**List of received files for the selected partner.**

There are two types of entries. Regular files have got an icon for download on the right side. When ENGDAT was received only the file of the set is shown. A click onto it will open the ENGDAT window.

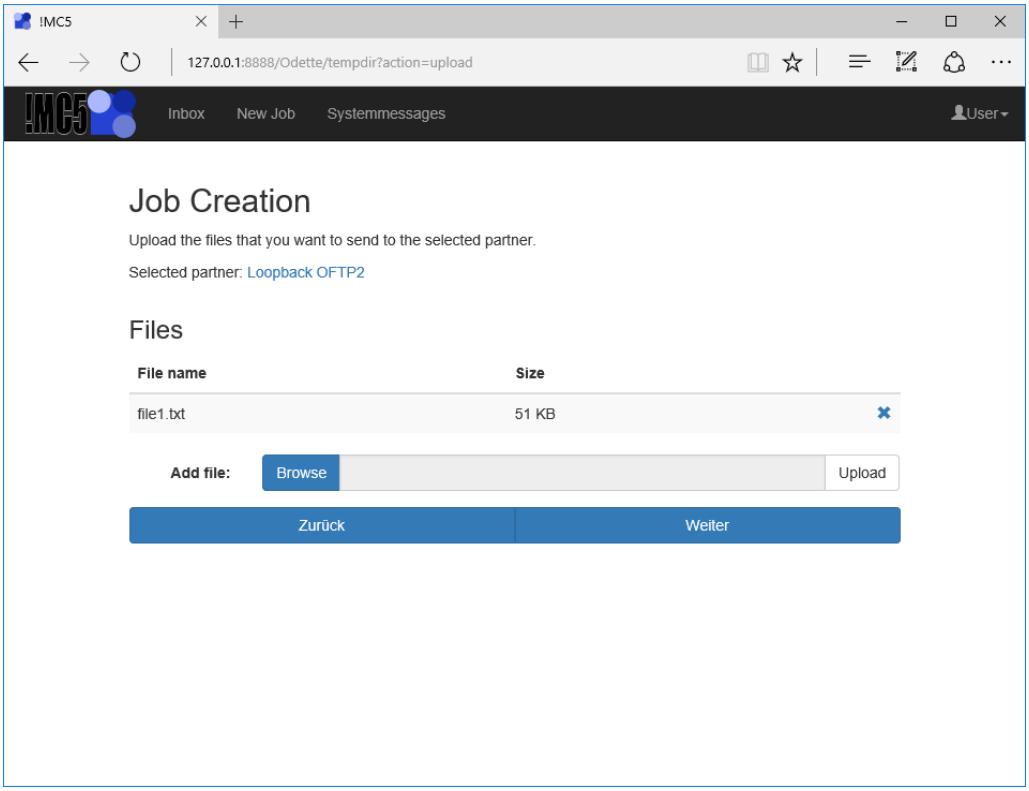



**Detailed view of a received ENGDAT transmission.**

The descriptions of sender and receiver are shown left hand. On the right side all files of the set are shown. Each file can be downloaded with the download symbol right of its original filename. The plus symbol opens more detailed information. The complete ENGDAT message can also be printed.

#### 4.5.2.2.2 Sending files

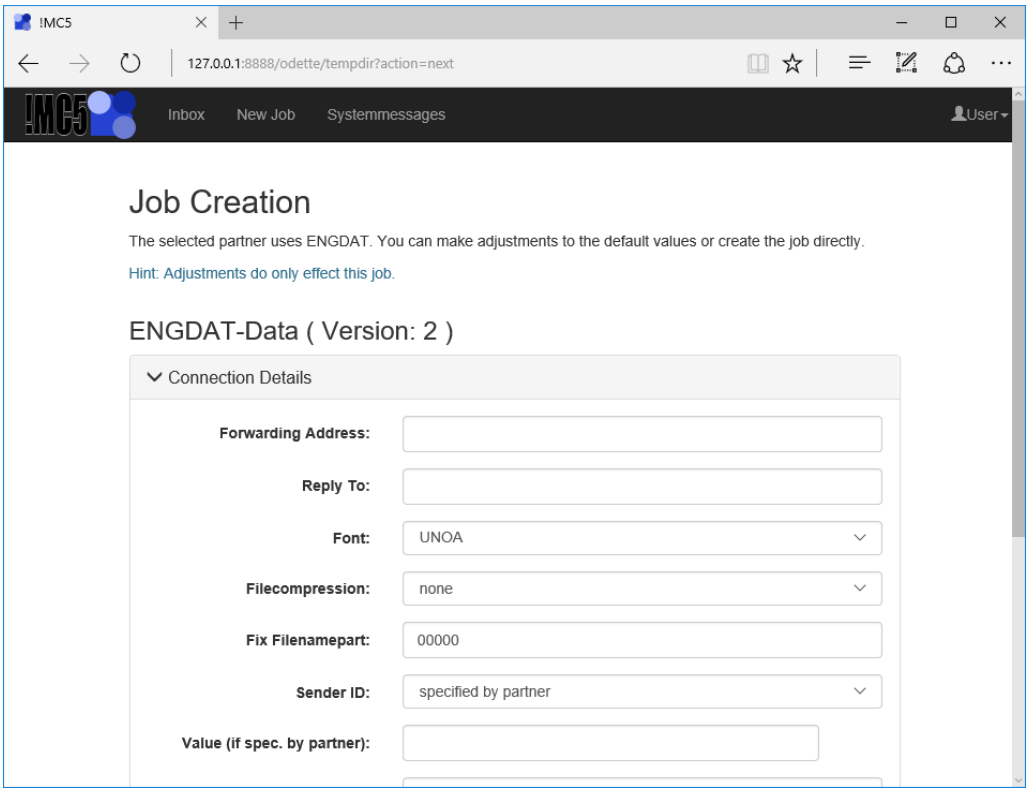
Click *New Job* in order to generate a new sending job. First select the partner that shall receive the files. On the following page you can upload the files to the server. The files are stored in a temporary folder. They will only be moved to the out-folder of !MC5 when the job creation is finished successfully. As long as the job creation is not finished the files can be removed from the temporary folder again.




**New job file upload.**

The job will be generated by clicking *Next*. Is ENGDAT or EngPart active for this partner extra pages for ENGDAT / EngPart will follow instead. After a job was generated successfully it can only be edited or deleted in !MC5 directly.

### ENGDAT/EngPart partner

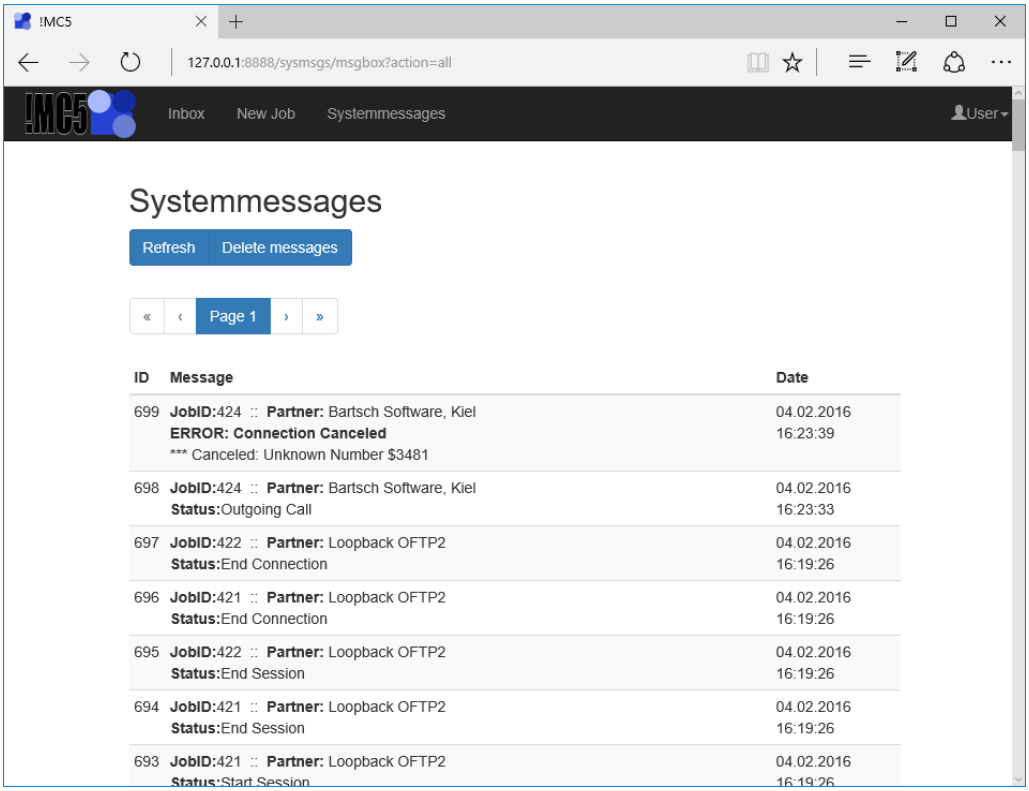



**Editing of ENGDAT data using the HTTP Client.**

The plus symbol opens a section and various input fields become visible. The ENGDAT page will always be pre-filled with the settings done in the address database of !MC5. By clicking *Create Job* the server will first generate valid ENGDAT and then start the sending job.

#### 4.5.2.2.3 System messages

The click onto *System messages* shows a page containing all status messages forwarded to this user. These messages can also be found in the status page of !MC5. By default only messages will be shown here that regard the sending jobs started by the user. This enables the user to check on the progress of his sending jobs. The list will be kept until the function *Delete Messages* is used.




**System messages for the logged in user.**

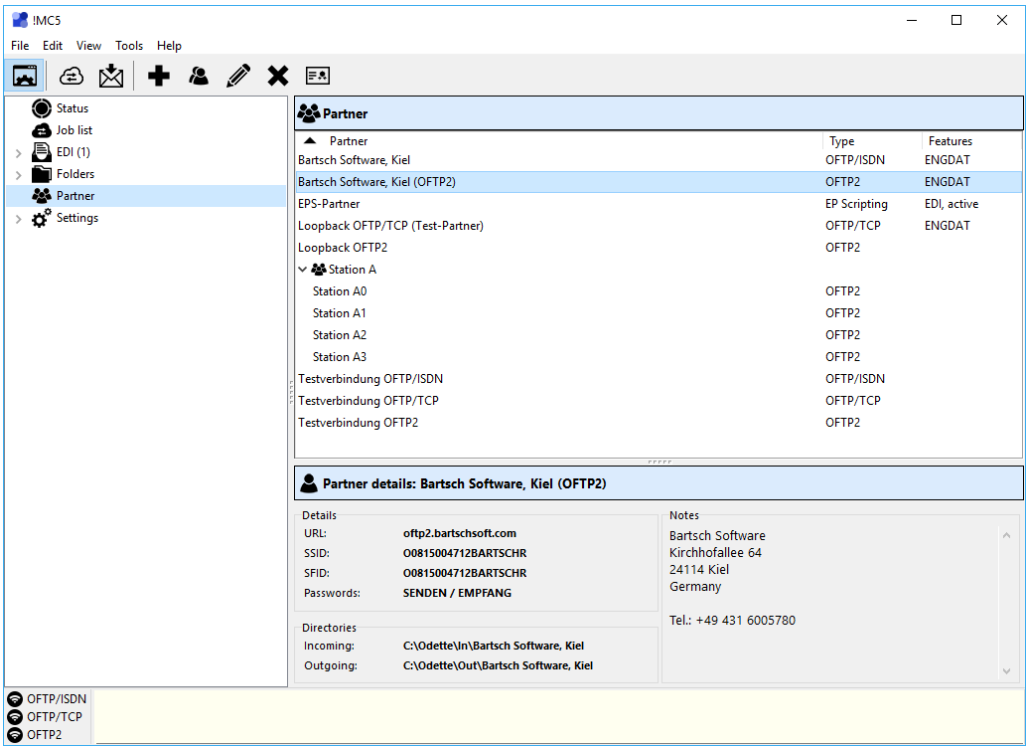
Which messages will be displayed depends on the permissions assigned to this user or to the groups the user is a member of.

!MC5

# Reference

# 5 Reference

## 5.1 Partner management




Prior to any data transmission, you have to create a new partner account which specifies connection type, parameters and settings. To edit, copy or delete a partner address choose the entry in the list and then press the designated button.

**Add** - Adds new partner account.

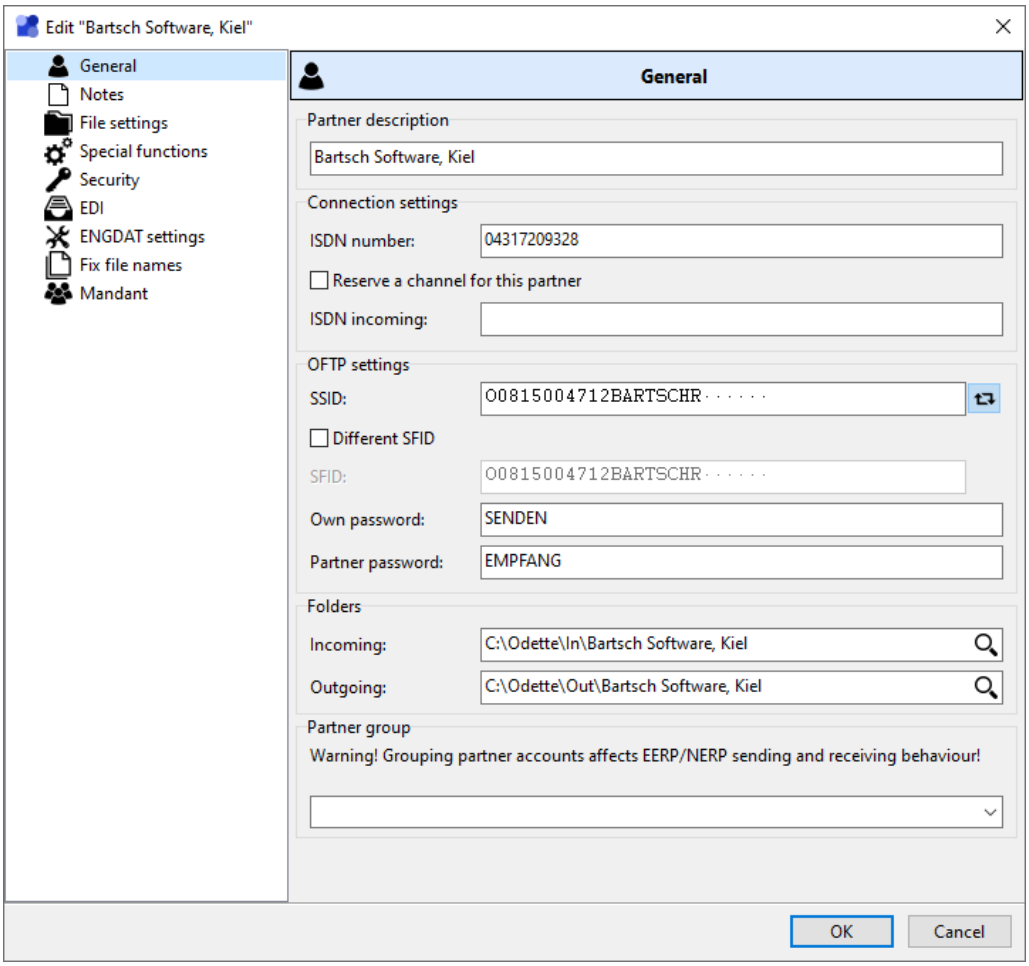
**Copy** - Copies an existing partner record. The copy can then be used as template for a new, but similar address account.

**Edit** - Opens an edit-window for the selected partner record.

**Delete** - Deletes the selected account.

### 5.1.1 General

This page contains the basic settings of a partner account.




## Partner description

Name or description of a the partner. The name entered here will identify the partner account throughout !MC5.

## Connection settings

**ISDN-Number ( Host / IP )**
This field contains the ISDN number or IP address / host name of the partner system.

**Port**
Only OFTP/TCP or OFTP2. The port the partner system uses. Usually OFTP/TCP uses port 3305, OFTP2 uses port 6619.

**Reserve a channel for this partner**
One channel will always be reserved for all partner accounts which have got this option activated. When the option is not active in any partner account all channels will be freely available. !MC5 will ignore all settings when there is only one channel available at all.

**ISDN incoming** *(only OFTP/ISDN)*
The incoming ISDN number of partner as displayed by the status tree of !MC5. An incoming call from this ISDN number will be assigned to a reserved channel when *Reserve a channel for this partner* is enabled. Otherwise this account will only be selected when the incoming number matches with of those entered in this field. If

the edit field is left empty the partner will only be identified by his Odette ID. Multiple numbers have to be separated by comma.

**IP white list** *(only OFTP/TCP and OFTP2)*
Only OFTP/TCP or OFTP2. If not empty !MC5 only accepts incoming transmissions for this partner from one of the entered IP addresses. Multiple addresses have to be separated by comma.

## OFTP2 settings

**SSID**
The Odette ID (SSID) the partner uses when connecting to !MC5.

**SFID**
The Odette ID (SFID) used as destination ID when files are sent to the partner.

**Own password**
Password sent by yourself during identification process.

**Partner password**
This password will be sent by the partner.

## Folders

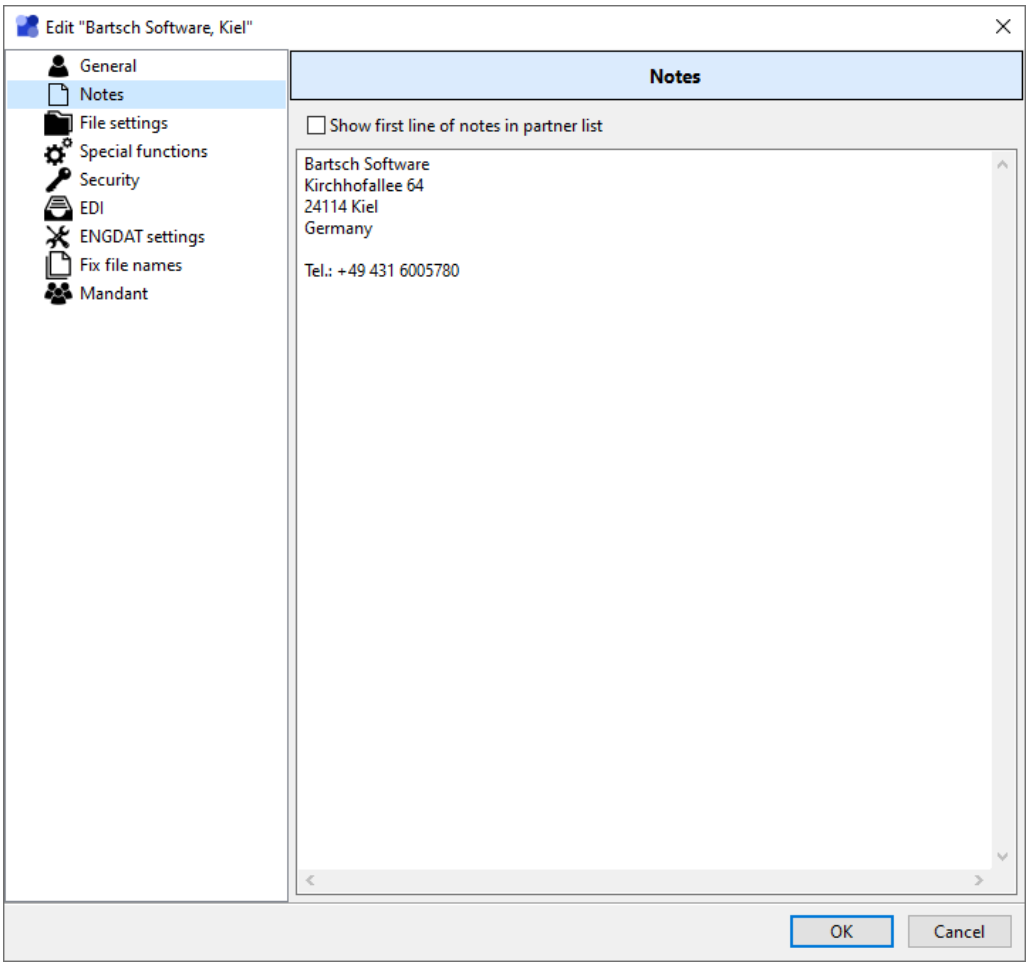
Folders for incoming and outgoing files.

## Partner group

The account can be assigned to a group optionally. This can be useful when there are several accounts created for a single partner company, e.g. accounts using the same SSID but with different SFIDs. When receiving End-To-End-Responses !MC5 will search all members of a group for the matching file.

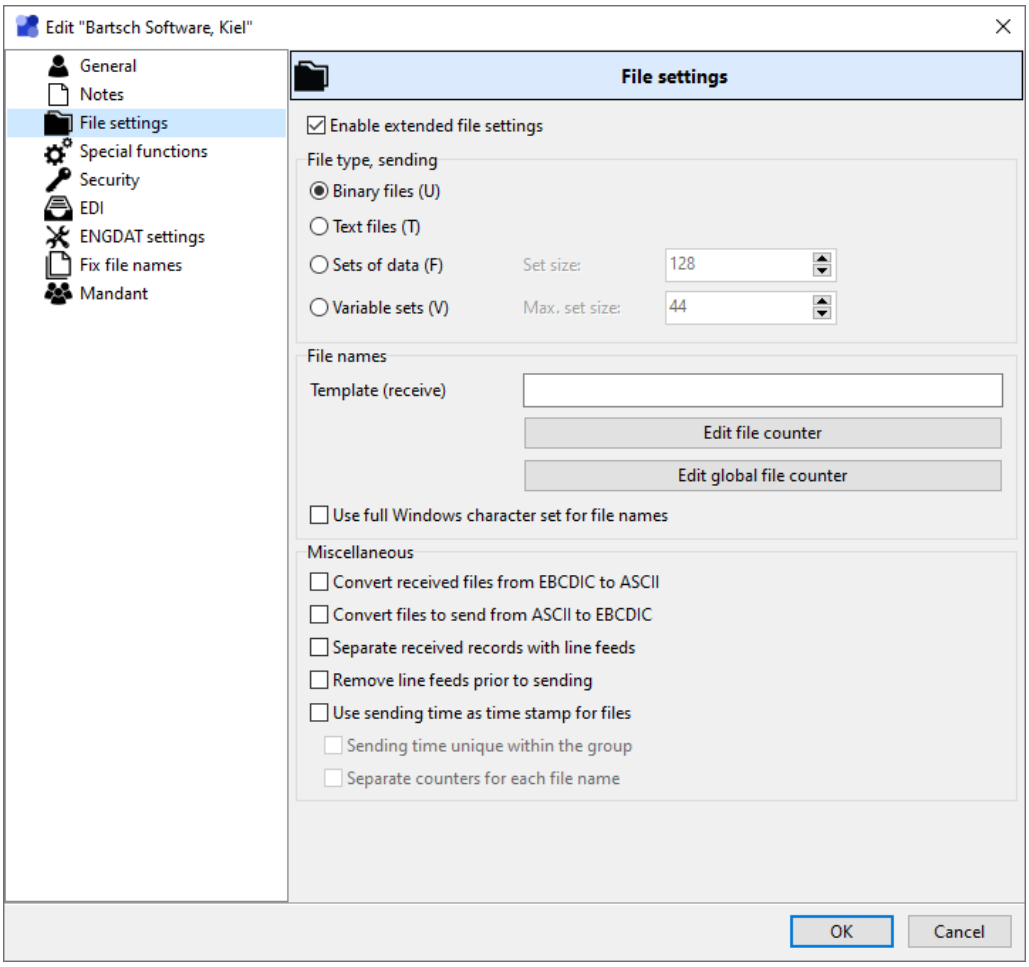
**Outbound EERPs will be sent at arbitrary partners of a group**
Scheduled EERPs or NERPs will be sent with the next connection of any partner in a group, independent of the partner account by which the original file was received. Only group partner accounts together for which this won't cause any problems. Never group accounts from totally different companies.

### 5.1.2 Notes




The page notes allows you to enter any text. You can use this to e.g. enter contact data for the partner or any comments regarding the partners configuration. If the option *Show first line of notes in parter list* is activated, the first line of the notes will be displayed in brackets after the partners description in the partner list. Additionally, an extra edit field for the first line of the notes will be displayed on the page *General* for faster access to it.

### 5.1.3 File settings




## Enable extended file settings

Activate this option in order to use the extended file settings. **Usually the settings in this data sheet do not have to be changed. Only make changes if requested by your partner.**

## File types

By default, the *File type* is set to *Binary files*. Only change the file type at your partner's request. The setting *Fixed records* splits a file into records of equal length. The size can be determined in the field *Set size*. This option is primary used for transfers with commercial data. When using V*ariable sets* the maximum set length is specified in the field *Max. set size*. If ENGDAT is used, the setting has to be *Binary files*. The type *Text* can be used to mark text files as such. The partner can use this option for formatting or converting purposes. Use this type only when it is request by your partner.

## File names

**Template (receive)**
This template is used to specify the file name used to save received files locally.

# - Gets replaced by a partner specific counter. The number of # chars determines the number of digits for the counter and thus its maximum value. Only one block of # chars can be used. When the counter reaches its maximum value it gets reset to zero.

***$*** - Gets replaced by a global counter. The number of $ chars determines the number of digits for the counter and thus its maximum value. Only one block of $ chars can be used. When the counter reaches its maximum value it gets reset to zero.
******* - Gets replaced by the virtual file name of the received file.
***%o*** - Gets replaced by the destination SFID of the file (your SFID).
***%p*** - Gets replaced by the origin SFID of the file (the partners SFID).

Example:

| | |
|---|---|
| Template : | *AB*###* |
| Original file name: | *invoice.txt* |
| Local file names: | *ABinvoice.txt001* |
| | *ABinvoice.txt002* |
| | ... |

**Using a template deactivates the default overwrite protection!**
By default !MC5 never overwrites files in the incoming directory of a partner. When receiving a file and a file already exists in the incoming directory using the same file name, !MC5 appends a counter to the file name of the newly received file. This counter is a global counter for all files received for any partner and runs from 0 to 999999. Only if the counter reaches its maximum value it gets reset to zero and existing files might get overwritten. This overwrite protection gets deactivated when using a template for received files. When using a template !MC5 always saves a received file using the file name after applying the template, overwriting any existing file using the same name. So when using a template it is recommended to use a counter in the template, either partner specific (#) or global ($). Be sure to choose a sufficiently large counter (counter size is determined by the size of the counter symbol block), as files could get overwritten when the counter reaches its maximum value and gets reset to zero.

**Use full Windows character set for file names**
!MC5 by default only uses upper case letters and no umlauts or other special characters for file names. This is to assure correct file name processing by the opposite side, regardless of the used operating system. By activating this option !MC5 uses the local Windows file names when sending the file. The maximum file name length of 26 characters still applies. **Only use this option if the partner uses a Windows based system!**

## Miscellaneous

**Convert received files from EBCDIC to ASCII**
This option converts received files from EBCDIC character set to ASCII character set. The original file will be kept in the sub-folder Backup

**Convert files to send from ASCII to EBCDIC**
Files are converted from ASCII character set to EBCDIC character set before being sent.

**Separate received records with line feeds**
When using *sets of data* as file type, received records are separated by an invisible separator bit. By activating this option a carriage return (ASCII code 13) and a line feed (ASCII code 10) will be inserted after each record. Thus each line in the local file represents one record.

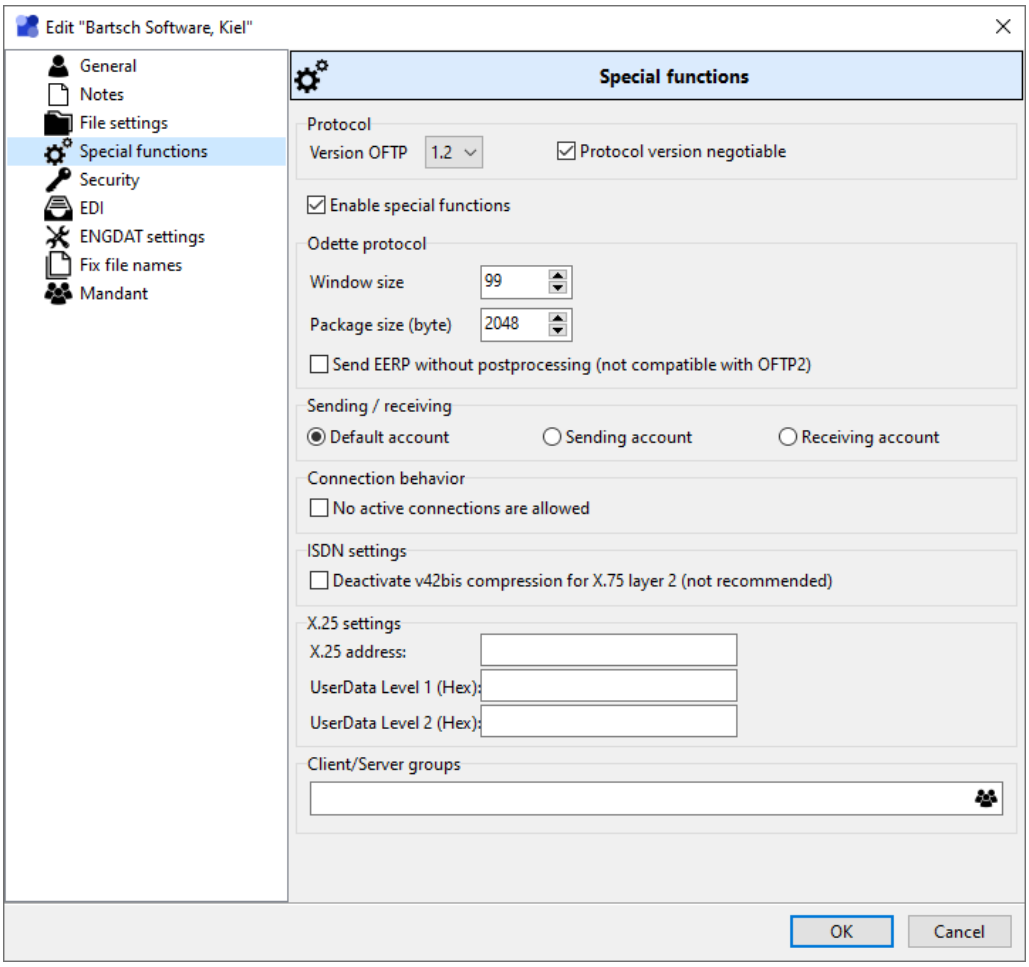
**Remove line feeds prior to sending**
When using set of data as file type, by activating this option all lines feeds in a file will be removed prior to sending the file.

**Use sending time as time-stamp for files**
By using this option each file will get a unique time stamp. This can be necessary when fix file names are used for sent files. Individual time stamps will be used for each partner. Two options are available for a mor flixbile control of how time stamps are applied:

1. **Sending time unique within the group**
   Time stamps will be unique within the group of partners this partner belongs to. The option has to be activated for all partners within that group.
2. **Separate counters for each file name**
   When using more than one fixed file name each file name gets its own unique time stamp.

Both options can be combined at will.

### 5.1.4 Special functions




## Protocol

**Version OFTP**
Defines the highest protocol version that should be used for this partner.

## Enable special functions

Enables editing of special functions. **Use any special function only when absolutely necessary. Most connections don't need any of these settings.**

## Odette-protocol

**Odette-package size, Odette-window size**
By default the Odette protocol defines that package and window sizes are negotiated on each connection, but some partners require fixed sizes. Be aware that smaller package and windows sizes reduce the connection speed. **Wrong fixed values can corrupt your connection to that partner!**

**Send EERP without postprocessing**
When files need postprocessing, e.g. because they are encrypted or signed, !MC5 sends the EERP or NERP for received files using a new connection after the files are processed. Only this way NERPs can be sent, if files are not correctly encrypted or signed. If this option is activated, an EERP is sent directly after receiving a file

using the same connection. This does **not** comply with default OFTP2 behaviour! **Only activate this option if absolutely necessary!**

## Settings Sending/Receiving

The option *Standard account* allows both to send to and receive files from a partner. A *Sending account* will be ignored for incoming connections and can only be used for actively send files. A *Receiving account* will never send but only receive files, tough it can be used to initiate a connection to that partner. When using a sending and a receiving account for one partner - e.g. to use different settings for receiving and sending files - both should be combined in a group.

## Connection behaviour

**No active connections are allowed**
With this option active !MC5 will never try to connect to the partner. Only the partner can open a connection for file transfer. The option is intended for partners without a fix IP.

## ISDN-settings *(OFTP/ISDN only)*

**Deactivate v42bis compression**
v42bis compression improves connection speed even when sending already compressed data by compressing X.25 control blocks too. By default the usage of v42bis gets negotiated by the CAPI interfaces of both sides. Some CAPIs don't support v42bis and don't negotiate this correctly. Deactivate compression in only such a case.

## X.25 Settings *(OFTP/ISDN only)*

**X.25 address**
The X.25 protocol can transmit an additional number which is irrelevant for normal ISDN connections and for which !MC5 uses the ISDN number of the partner by default. If the partner uses an internal X.25 network a routing address might be required which has to be entered here.

**User Data Level1 (Hex), User Data Level2 (Hex)**
Some Odette connections require fixed keys for these fields. The data has to be entered in hexadecimal format, e.g. 3FA0.

## Client/Server groups

Each partner can be added to one or more groups. This affects visibility of the partner for connections using the HTTP Client or the Client/Server add-ons, depending on the groups to which the connecting user belongs and the groups settings. See User groups and permissions for more details.

***Example:***
User A is added to groups G1, G2 and G3. Group G1 has the option *Users are restricted to a limited partner selection activated*. The following partners with respective group memberships do exist:

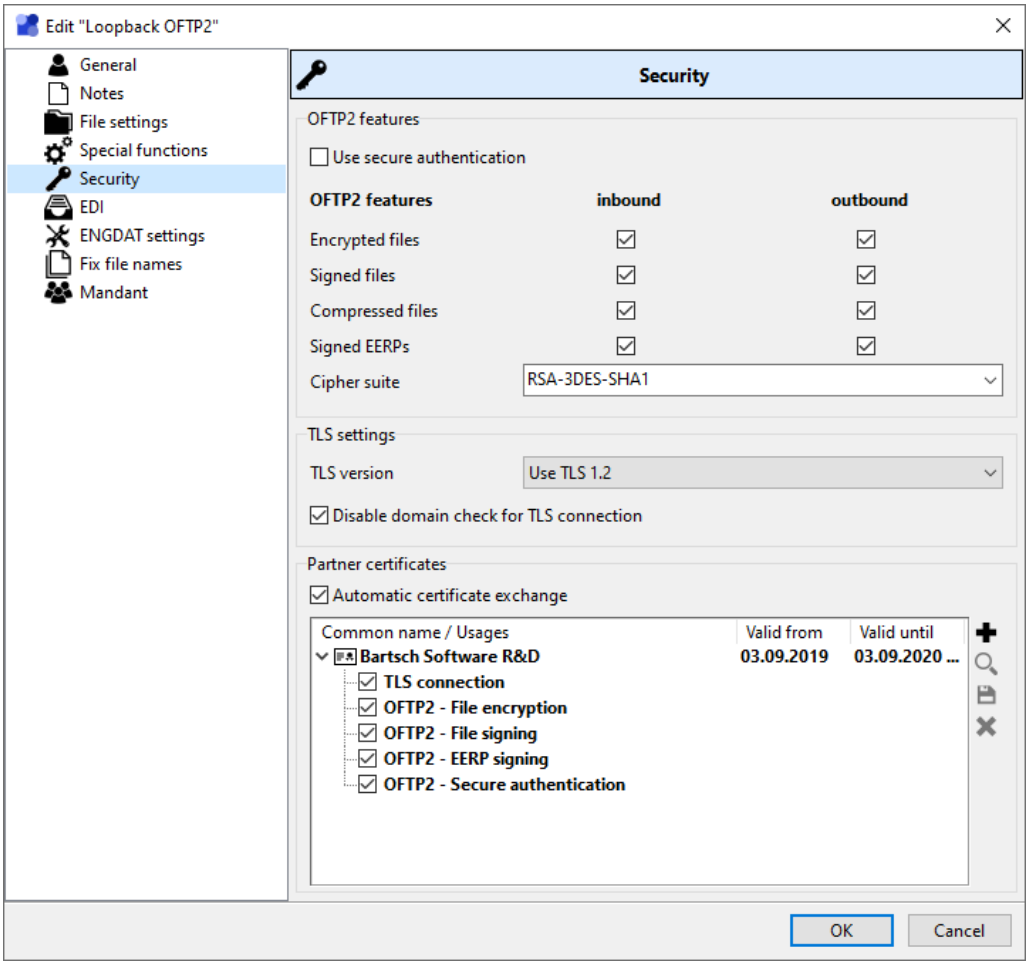
| Partner | group memberships |
|---|---|
| P1 | (none) |
| P2 | G1, G3, G4 |

| | |
|---|---|
| P3 | G4 |
| P4 | G2 |

User A can "see" the following partners: P2 (A is member of the groups G1 and G3) and P4 (A is member of G2). P1 and P3 are "invisible" for user A.

### 5.1.5 Security

(OFTP2 module only)




## OFTP2 features

**Use secure authentication**
Both sides authenticate themselves using their certificate in addition to Odette identifier and Odette passwords.

**OFTP2 features**

- ***Encrypted files*** - Specifies if encrypted files are received and if files should get encrypted before being sent. The ciphersuite to use can be chosen further down. Encryption is used to secure access to the content of transmitted files.
- ***Signed files*** - Signing of files authenticates their origin and validates that the file wasn't altered during transmission. Outgoing files will be signed before they are sent, for incoming files !MC5 tries to validate the signature after receiving them. The result of the validation will be logged in the !MC5 protocol.
- ***Compressed files*** - Specifies if files should get compressed before being encrypted or signed. File compression can reduce transmission times due to smaller files.
- ***Signed EERPs*** - Signing of end to end responses assures their origin authenticity and data integrity.
- ***Cipher suite*** - The cipher suite used for OFTP2 features.

Security features have to match your partners requirements. Activate any of these features only if required by the respective partner or if you want to require them from him. If e.g. encrypted file transmission is activated and an unencrypted file shall get sent, encryption has to get deactivated before sending. Security features are set on a partner base not a transmission base.

## TLS settings

**TLS version**
The TLS version to be used, when connecting to this partner. A higher version equals higher security.

**Disable domain check for TLS connection**
When establishing a TLS connection to an OFTP2 partner !MC5 tests if the domain name contained in the received certificate matches the host specified in the field *General / IP address*. If both don't match, the connection gets closed. Some partners require to connect to hosts or IP addresses that don't match the domain name contained in their certificate. For those partners, this option has to be activated in order to actively connect to them. When the domain check is disabled the received certificate has to match exactly the certificate specified for the usage *TLS authentication*.

## Adding partner certificates

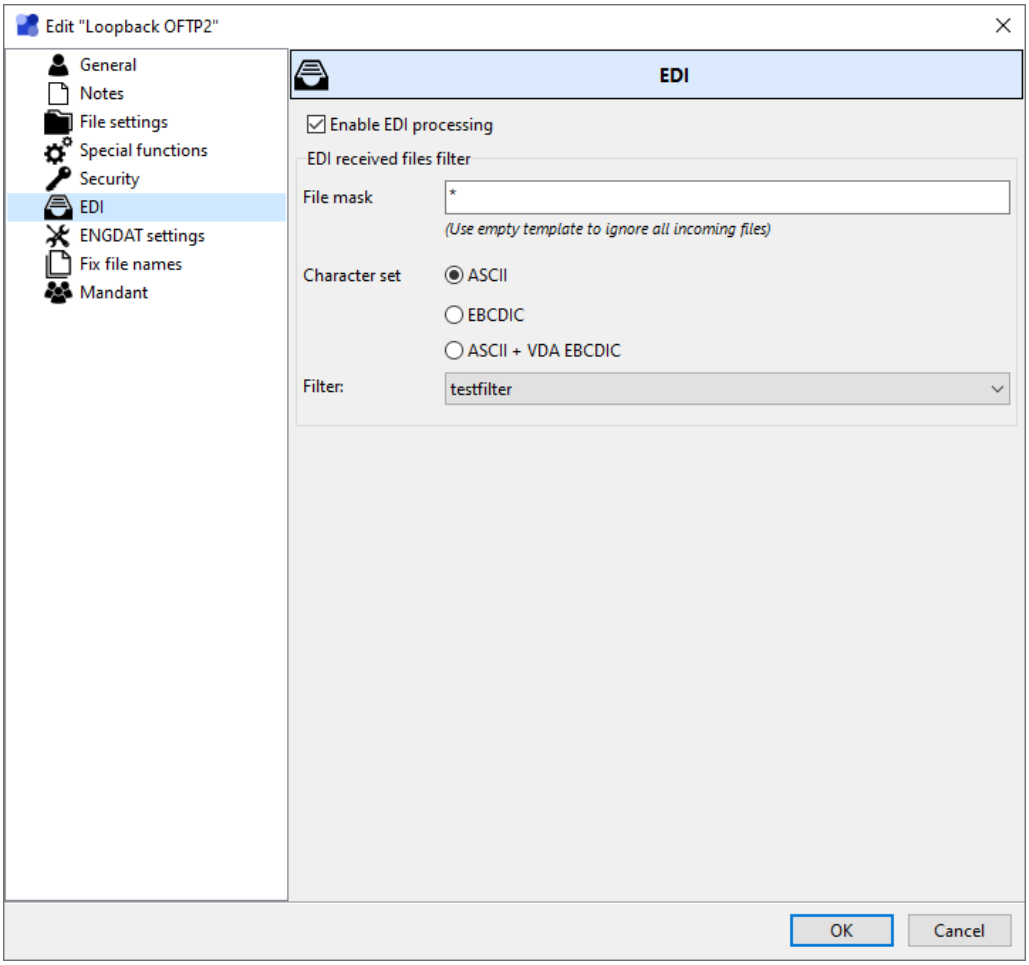
In the box *Partner certificates* one or more partner certificates can be added. For each certificate usages have to be specified. For which usages certificates are required depends on which OFTP2 features are activated. One certificate can be used for all usages or different certificates for different usages. If multiple certificates are specified for the same usage(s), !MC5 automatically uses the newest certificate.

## Automatic certificate exchange

!MC5 supports automatic certificate exchange (complying to the OFTP2 Implementation Guidelines). To use the automatic certificate exchange with a partner, the option Automatic certificate exchange has to be enabled. Also the partner has to support the automatic exchange.

### 5.1.6 EDI

*(EDI add-on only)*




## Enable EDI processing

Without enabling this option no incoming EDI messages will be added to the EDI inbox in any other way processed by the EDI add-on. Also only partners with this option enabled will be available for any of the EDI functions, e.g. sending messages and automatic import or export of messages.

## EDI incoming filter

### File template

The *File template* defines which received files are processed by the EDI add-on. Only those files who match the template will get proxessed. E.g. the file template * will process all incoming files, whereas the template **.txt* would process only files with the extension *.txt*.

### Filter

Using a pre filter incoming files can get filtered out or get modified for processing by the EDI add-on. Filters can be created using the *EDI Convert Manager* tool. The drop down box will show all available filters. The test button will perform a syntax check on the selected filter.

## Character set

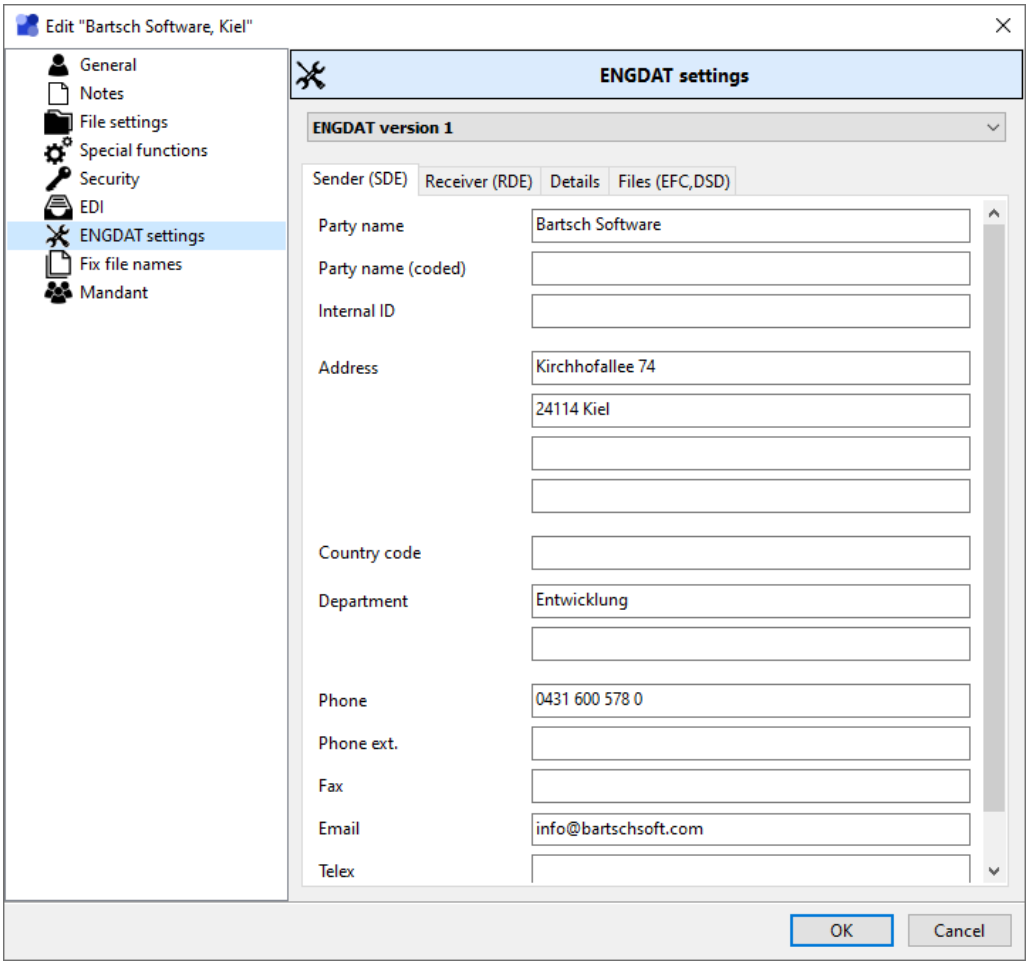
**ASCII, EBCDIC, ASCII + VDA EBCDIC**
The default character set for EDI messages is ASCII. EDIFACT messages always use this character set.

VDA messages are some times transmitted by using the EBCDIC character set. In those cases use set option EBCDIC as character set. This only affects data while being processed by the EDI add-on. The received files themselves will not be converted. **Do not use this option set when incoming files are already converted from EBCDIC to ASCII using the respective options in the *Special functions*.** Else the data will get converted twice which results in unreadable data.

The setting *ASCII + VDA EBCDIC* tests for every file, if it is a VDA message. Only as VDA recognized messages will get converted. Use this setting if you receive both messages using ASCII (e.g. EDIFACT) and VDA messages using EBCDIC from a partner.

### 5.1.7 ENGDAT settings

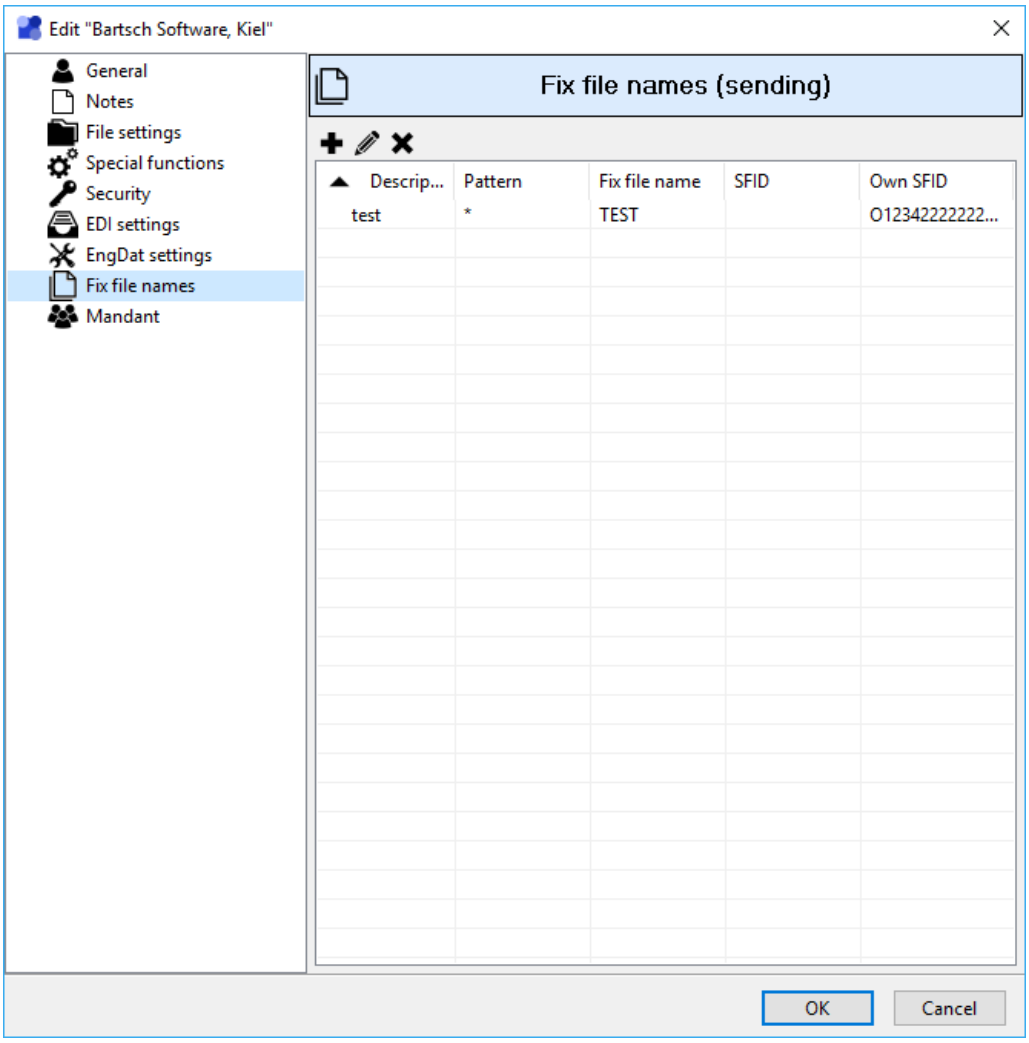
(ENGDAT add-on only)




The ENGDAT settings allow to activate ENGDAT for the partner. All files outgoing files will get converted to the ENGDAT format. ENGDAT-Version allows to select the version of ENGDAT to be used.

After selecting a version presets can be entered. All entered data will be used as default when creating a new ENGDAT job, so e.g. Sender and receiver information don't have to be entered again with each new transmission. These default values will be still editable at job creation.

### 5.1.8 Fix file names

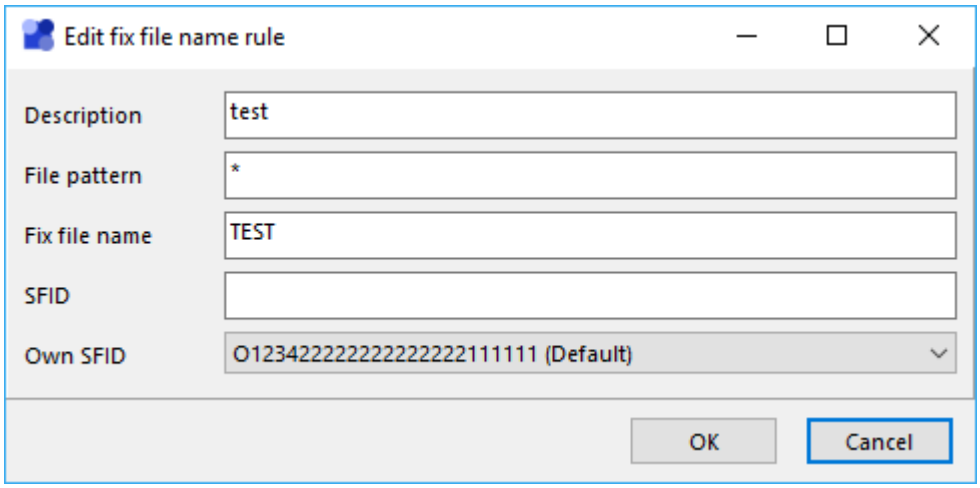



Some partners require that all files, especially EDI messages, are sent using the same file name, which they require for further processing of the messages. For this requirement !MC5 allows to define rules for *Fixed file names*. You can define file patterns so that files matching those will be sent using a fixed virtual file name. The local file name wont be changed.

The following functions are available:

- **New** - Add a new rule
- **Edit** - Edit the selected rule
- **Delete** - Delete the selected rule

#### Add new rule / Edit rule




In the most simple case, when all files should be sent using the same name, only one rule is required. Use the *Pattern* *, which matches any file, and enter the *Fix file name* into the respective field.

If files should get different fixed names, the files have to be distinguishable by their local file name, in a way that the respective files can be matched by a certain file pattern. Taht pattern can then be used to create a new rule for a fixed file name. If a file doesn't match any rule, it is sent using the local file name.

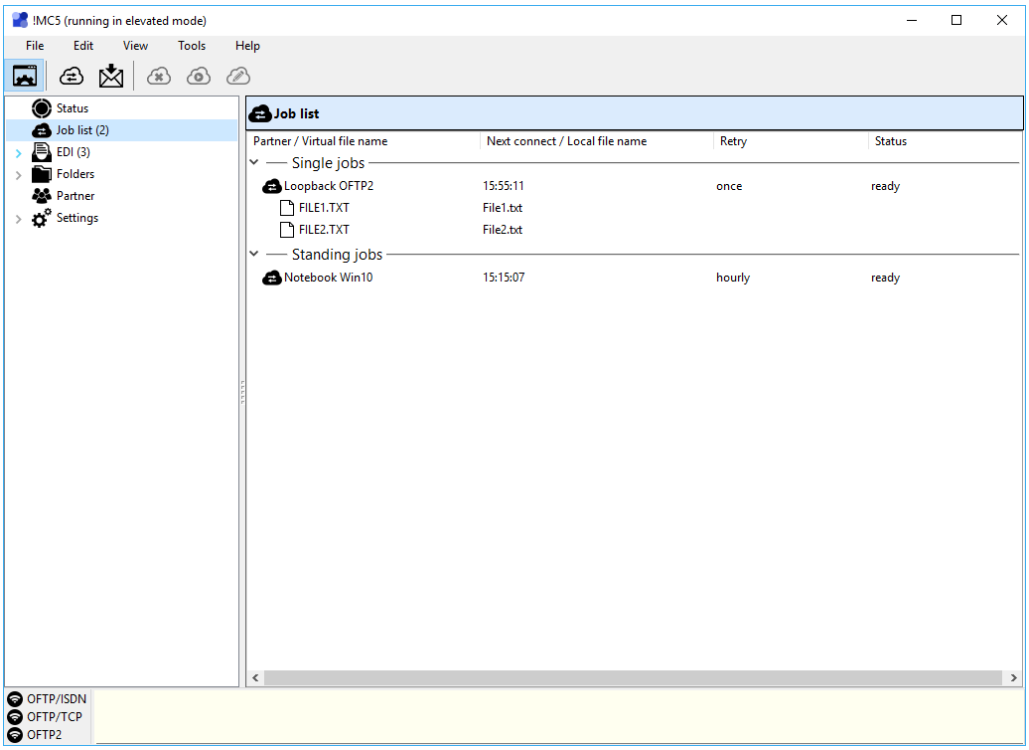
In addition to a fixed file name an alternative SFID can be specified, which will be used when files matching the file pattern are sent. Contrary to the general settings, here the leading character of the Odette ID (i.e. an *O*) has to be entered also.

The fixed name can contain certain special characters:

- # will get replaced by a consecutive number. The number of # characters defines the width of the counter. Each partner gets its own counter.
- The character $ will also be replaced by a consecutive number, in the same way the # character does. The difference being that $ will use one global counter for all partners.
- The character * will be replaced by the original file name. If the resulting file name is longer than 26 characters it will get truncated to a length of 26 characters.
- The placeholder *%DATE:<format>%* gets replaced by the current date (and/or time) depending on the given format. E.g. on January, 1st 2019 at 12pm *%DATE:hhmmssMMDDYYYY%* gets replaced by *12000001012019* and *%DATE:MMDDYYY%* would get replaced only by the date.

## 5.2 Job list

The job list allows to view, edit and delete pending and running transmission jobs.




The following functions are available:

**New job** - Create a new job.

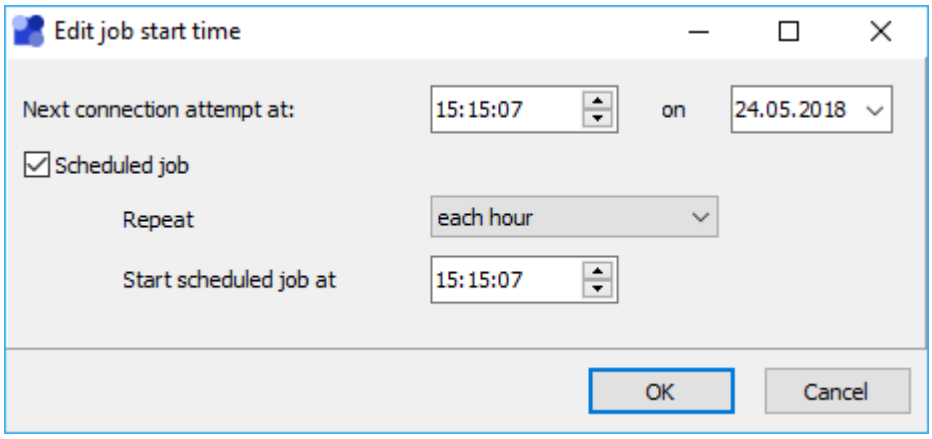
**Delete job** - Delete the selected job. Files in this job can either get deleted, moved or remain untouched upon deletion of the job.

**Execute job** - Execute the selected job as soon as a respective channel is available.

**Edit job** - Edit the settings of the selected job. The time of the next connection, or the connection interval can be edited. For single connection jobs the files which will get sent will get displayed. Recurring jobs will check for outgoing files when upon each connection and will therefore display no files when editing the job.

> **Running jobs can't get edited or deleted. Successfully finished job get deleted automatically**
> Job which are currently running can neither be edited or deleted. A successfully executed job will get deleted automatically (if it isn't a recurring job). If a partner connects to !MC5 and a job for this partner is in the job list, it will get executed with the established connection and gets deleted upon success.

### 5.2.1 Job start time




#### Next connection attempt at

The assigned time for the next connection attempt is displayed and can be edited. !MC5 executes all jobs which assigned time is reached or has passed.

#### Scheduled job

Activating this option sets this job as a recurring job. The connection will be repeated in the given interval each time sending all files present in the out folder of the partner at the connection time and also receiving new files from the partner, if applicable.

**Repeat**
The interval in which the job gets executed.

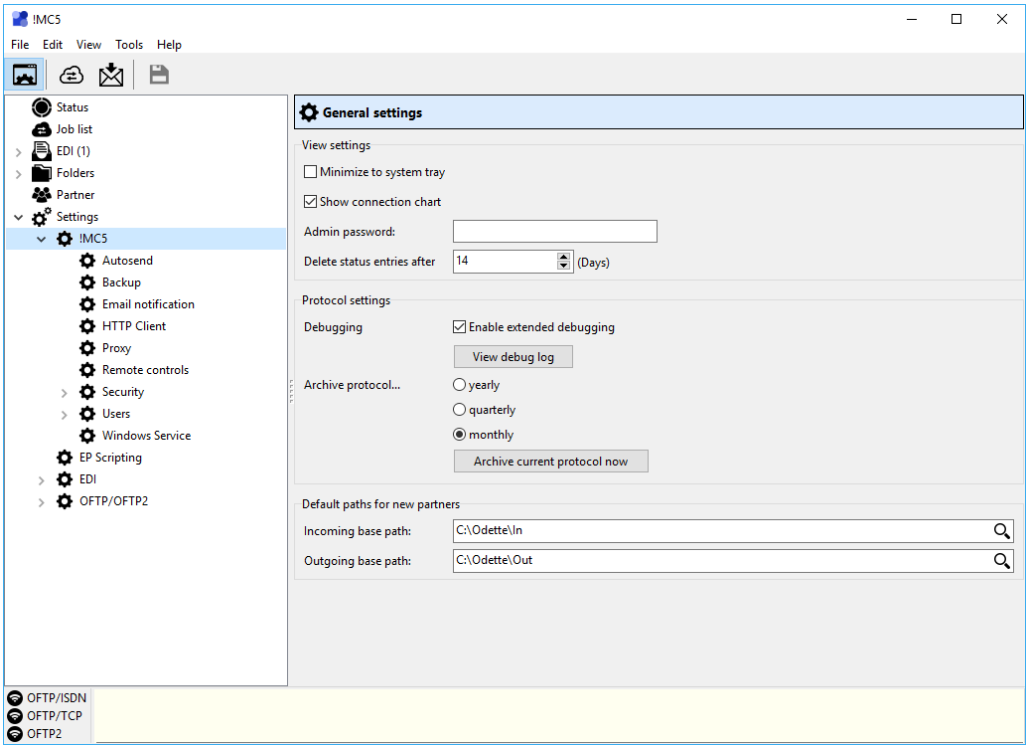
**Start scheduled job at**
The time of the first connection of the scheduled job.

**Repeat interval**
If *individual* is selected as repeat interval this field is used to specify the interval (in hours, minutes and seconds) in which the job will get executed. The time of the first connection has to be specified using the *Next connection attempt*.

## 5.3 Settings

### 5.3.1 !MC5 settings

#### 5.3.1.1 General settings




### View

**Minimize to system tray**
If this option is activated, the !MC5 main window, when minimized, won't be displayed on the Windows task bar but as an icon in the Windows system tray instead.

**Show connection chart**
Show or hide the connection chart at the bottom of the main window.

**Admin password**
Specifying an admin password activates the admin view, which can be enabled or disabled using the first button in the main tool bar. If the password is left blank, the admin view is always enabled. Only when the admin view is enabled !MC5 settings and partner management are shown. At program start up admin view is disabled by default, thus not allowing a user to change any settings without entering the admin password.

**Delete entries after x days**
Defines the maximum age of status messages displayed on the status page of !MC5 in days. Messages are deleted only from the status page but still remain in the !MC5 protocol and are still accessible using the *Protocol Analyzer*.

### Protocol settings

**Debugging**

***Enable extended debugging***
Extended debugging creates additional debug log files and more detailed protocol messages. This can be helpful for analyzing issues, but should be disabled if possible due to the larger amount of data written to the !MC5 protocol files.

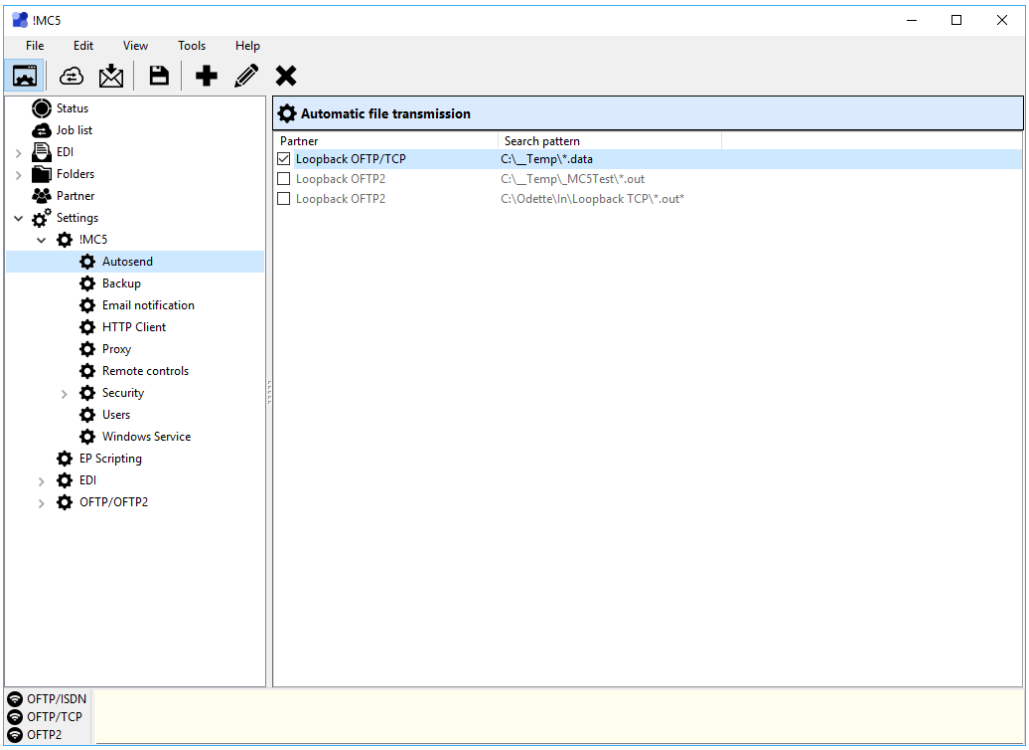
***View debug log***
Opens the extended debug log file, if present, using the Windows' default text editor.

**Archive protocol...**
To keep the protocol a reasonably size, the main !MC5 protocol is archived up regularly. Here you can select if an archive is created each month, quarter or year. Select the appropriate interval depending on your traffic. After archiving a log file a new protocol is created. Archived protocols are still accessible using the *Protocol Analyzer*.

## Default paths for new partners

Here the default base paths for incoming and outgoing folders, which will be used when creating a new partner, can be adjusted. E.g. if incoming and outgoing folders aren't located on drive C: then by adjusting the default base paths accordingly the paths don't have do be edited each time a new user is created.

### 5.3.1.2 Automatic file transmission




## Autosend rules

The automatic file transmission uses rules to automatically send files to different partners. A rule defines a search path, a file pattern and a partner, to which file from that directory matching the file pattern should get sent.

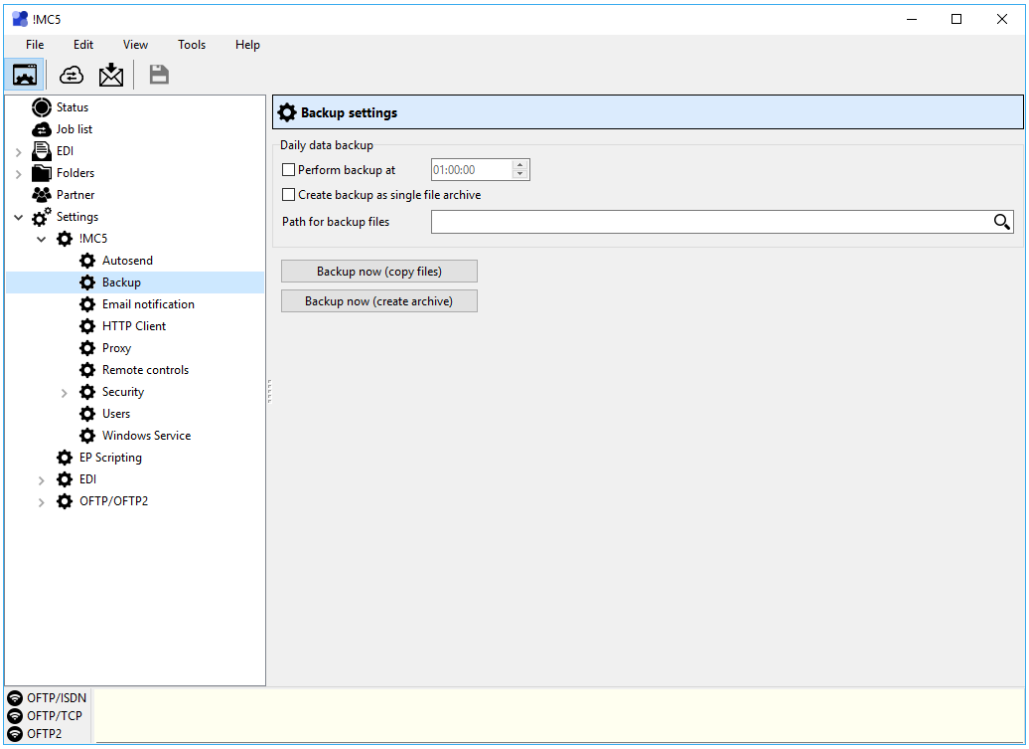
**Automatic file transmission does not work for partners using ENGDAT or EngPart as those formats require additional data for each transmission.**

**Never use a folder for outgoing files of a partner as search path for an auto-send rule!**

New rules can be added using the add button, existing rules can be deleted using the delete button. Rules can be activated or deactivated by clicking the checkbox in front of the rule entry.

### 5.3.1.3 Backup settings

Many of the files that !MC5 uses are locked exclusively by the program. This can cause some backup software to not being able to backup those files. To allow backing up of these files !MC5 has the in-build feature to create copies of all configuration, data base and other files !MC5 uses, while the software is running.




## Daily data backup

**Perform backup at**
When activated a backup of !MC5 files will be created every day at the given time. Each backup overwrites the previous one.

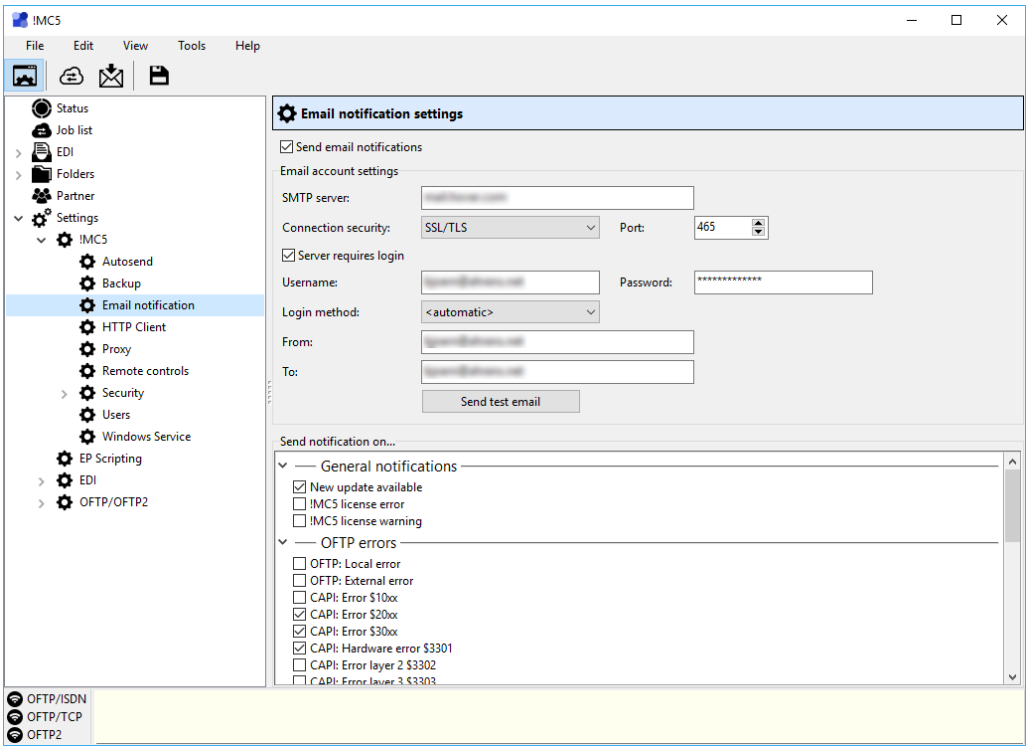
**Create backup as single file archive**
Instead of copying all files and directories to the target path, a single archive containing all files is created at the backup location. This file can be restored using !MC5s restore backup function.

**Path for backup files**
The path, to which the backup function will copy !MC5 files or save the backup archive.

**Backup now (copy files)**
Copy all files to a selectable destination folder.

**Backup now (create archive)**
Create a backup archive at a selectable destination.

### 5.3.1.4 Email notification




## Send email notifications

This option activates email notification. Deactivating keeps all settings. It is recommended to deactivate email notification while setting up and testing a new partner connection.

## Email account settings

**SMTP-Server**
SMPT server address of the mail server which should be used to send email notifications.

**Connection security**
Specify the type of connection security. The following settings are available:

***no security*** - Connect to the server without any security enabled.
***SSL/TLS*** - Connect to the server using SSL/TLS.
***STARTTLS*** - Connect to the server without security enabled and switch to SSL/TLS, if supported by the server.

> **Certificates used for secure SMTP connections**
> !MC5 uses only those root and CA certificates located in !MC5s default certificate storage and !MC5s user storage. No certificates from TSLs will be used, as email notifications might already get sent before TSLs are loaded. If a secure SMTP connection fails due to missing certificates add those to the user store (*Settings / !MC5 / Security / Certificates*).

**Port**
SMPT server port (usually port 25).

**Server requires login**
Internal SMPT servers often don't require extra authentication. In such a case deactivate this option.

**User name, Password**
SMPT user name and password, if needed by the server.

**Login method**
Select method to login to SMPT server:
- ***<automatic>*** - !MC5 and the SMPT server negotiate the method to be used automatically.
- ***CRAM-MD5*** - Use *Challenge-Response Authentication Mechanism, Message Digest 5* (CRAM-MD5).
- ***DIGEST-MD5*** - Use *digest access authentication*.
- ***NTLM*** - Use *NT LAN Manager authentication*.

**From**
Email address that is to be used as sender for error notifications.

**To**
Email address error notification will be sent to.

## General notifications
Select for which general notifications an email should be sent.

## Report following error classes
*(OFTP and OFTP2 modules only)*

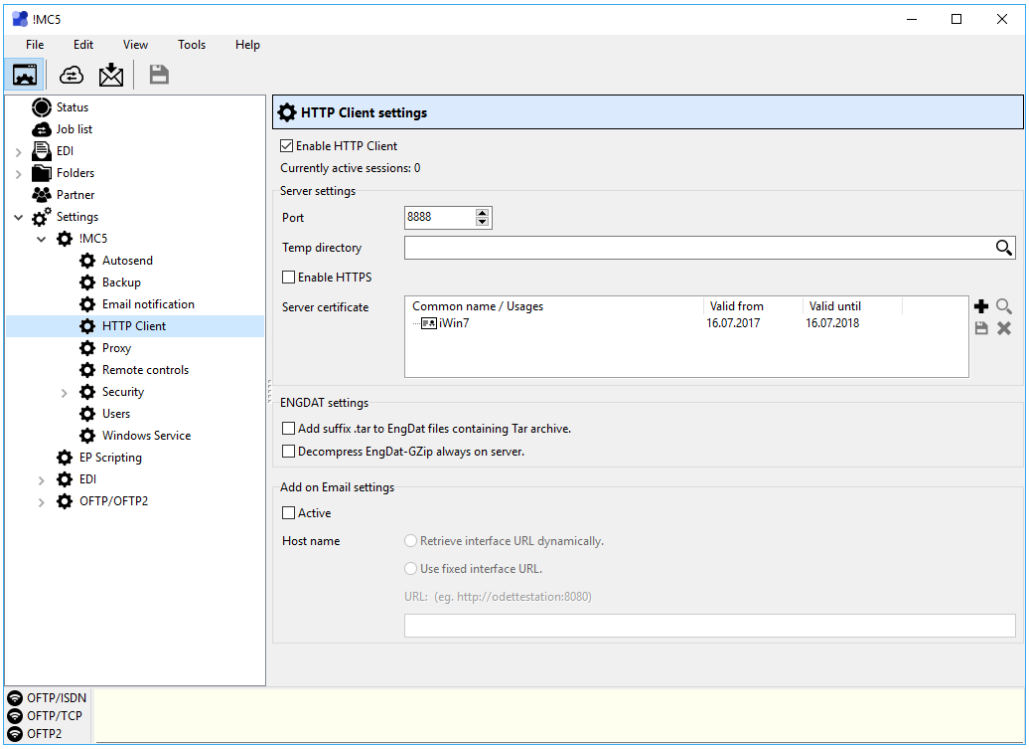
Select for which errors an error notification shall get sent. Errors are represented in error classes to allow exclusion of common errors, e.g. ISDN errors $349x which includes errors like "No user responding" or "User busy".

## EDI errors
Select which EDI processing errors should generate an email notification.

### 5.3.1.5 HTTP Client

*(HTTP Client add-on only)*

Using the HTTP Client some features of !MC5 can be accessed using a web browser. To access the HTTP Client a user has to exist which is assigned to the HTTP Client group (see Manage users).




## Enable HTTP Client

Activate this option to enable the HTTP Client server.

## Server settings

### Port

The port to use to access the HTTP Client add-on. The default is 8080. If this port is already used by another application it has to be changed.

### Temp directory

The local directory in which the HTTP Client saves temporary files, e.g. file uploads for unfinished jobs. !MC5 needs write access for the specified directory. If left blank, !MC5 will use a sub directory inside the temp directory of the logged in user (default: *C:\Users\Username\AppData\Local\Temp*). It is important to use a directory which doesn't contain any other files as the used directory will be cleared at program start.

### Enable HTTPS

Activate this option to enable secure HTTPS connections to the HTTP Client server. If enabled, a certificate to use for encryption has to be added in the *Server certificate* box.

**Only change server settings when no users are connected!**
Changing the server settings will result in all currently connected user to get disconnected. Any not saved changed made by those users will get lost. The number of currently connected users is displayed below the option *Enable HTTP Client*.

## ENGDAT settings

**Decompress ENGDAT-GZip always on server**
If enabled, received, compressed ENGDAT files will get decompressed on the host computer when being downloaded using the HTTP Client interface. Enable this if the HTTP Client is accessed using browsers that don't support HTTP deflate or use incompatible deflate algorithms.

**Add suffix .tar to ENGDAT files containing Tar archive**
When activated !MC5 will add the extension .tar to files names, if the corresponding ENGDAT file is stated to contain a tar archive.

## Add on Email settings *(Email add-on only)*

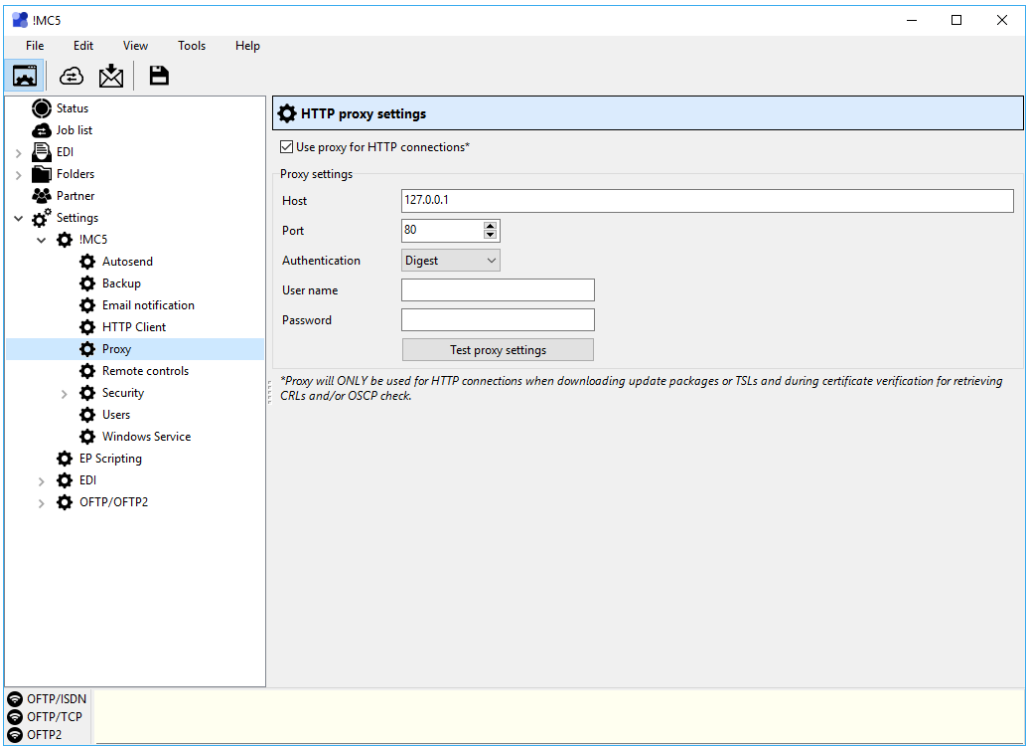
The Email add-on can be used to send email notifications about newly received files containing links to those files. If using both HTTP Client and Email add-ons those file links can be redirected to the HTTP Client interface.

**Active**
Enables link substitution.

**Host name**
Select which host name should be used for file links. *Retrieve interface URL dynamically* will use the local IP address of the host computer (e.g. *http://192.168.0.1:8080...*). Alternatively a host name can be specified using the option *Fixed interface URL*.

### 5.3.1.6 Proxy

For some connection !MC5 requires access to internet resources, such as CRLs, TSLs or update packages. For those connections usage of a proxy server can be configured here.




## Use proxy for HTTP connections

Enables or disabled the use of a proxy server for HTTP connections. The proxy will only be used for HTTP connections when downloading update packages or downloading TSLs and during certificate verification when downloading CRLs or performing OSCP check.

## Proxy settings

**Host**
Host name or IP address of the proxy server.

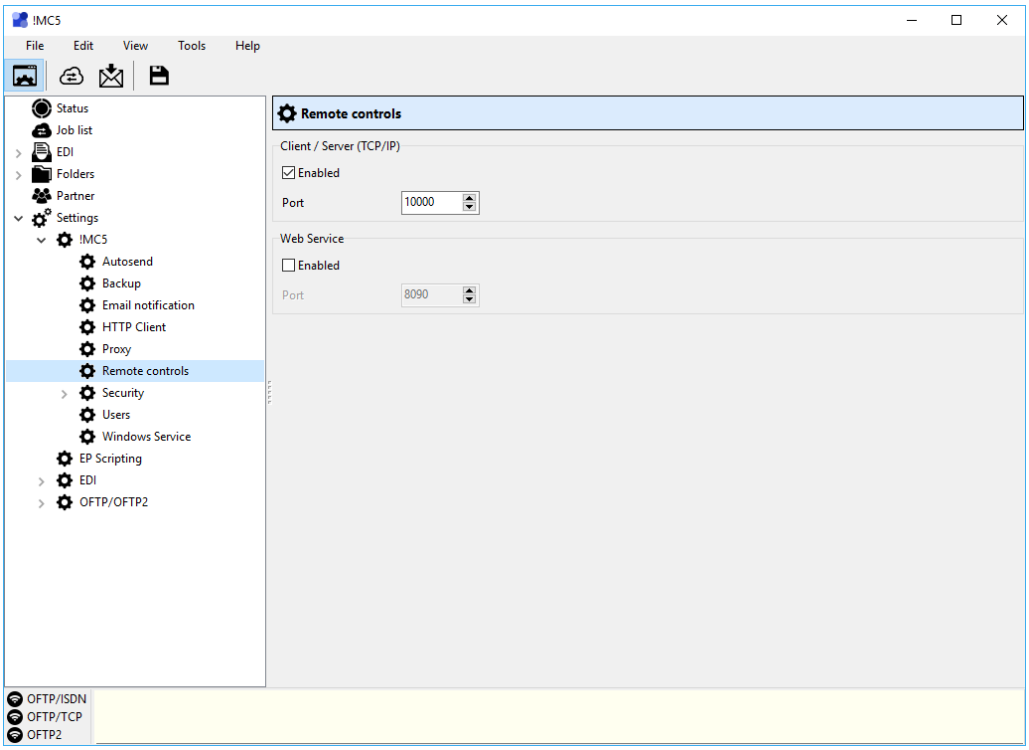
**Port**
Port used by the proxy server.

**Authentication**
Authentication method used to log on to proxy server.

**User name / Password**
User name and password for log on to proxy server. These are required depending on the selected authentification method.

**Test proxy settings**
Use this button to test the proxy settings.

### 5.3.1.7 Remote controls




## Client / Server (TCP/IP)

*(Client/Server add-on only)*

**Active** - Activates the server part of the Client/Server add-on. Deactivating this option or changing the associated TCP port will disconnect all connected clients.

**Port** - The port used by the server. Always two neighbouring ports will be used, the selected port and the directly following port (default: 10000 and 10001).

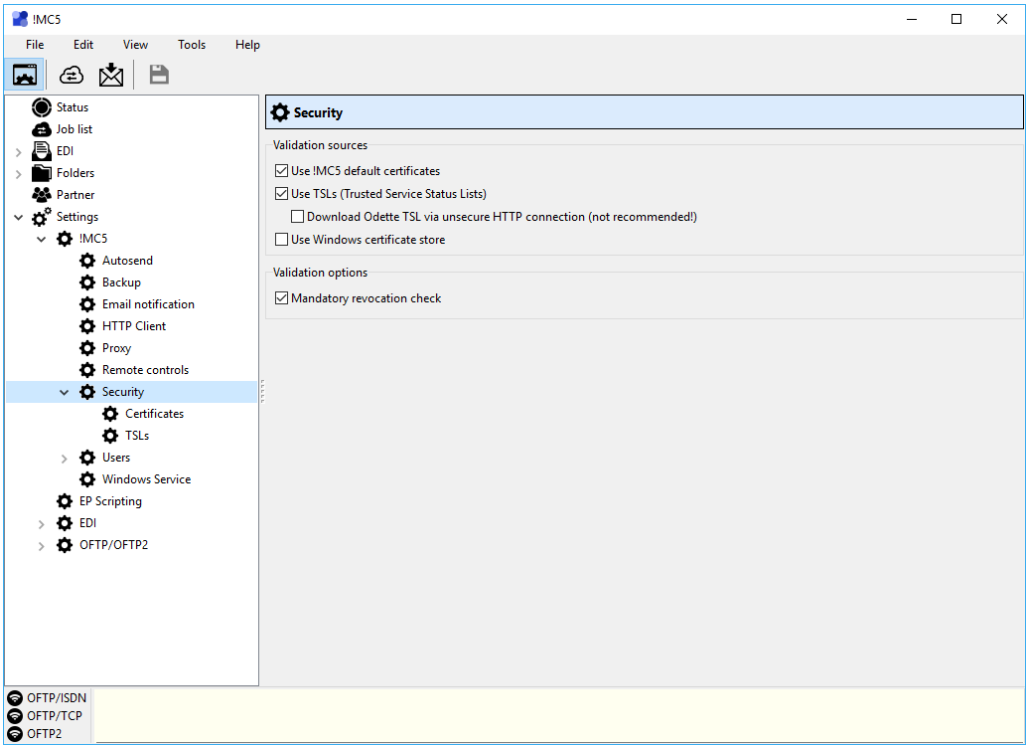
## Web Service

*(Web Service add-on only)*

**Active** - Enables the integrated Web Service add-on for remote control of !MC5.

**Port** - The TCP port the Web Service add-on will use.

### 5.3.1.8 Security




## Validation sources

Used to specify, which sources !MC5 should use to validate certificates. In order to successfully validate a certificate, the issuer certificate has to be present in one of the validation sources.

**Use !MC5 default certificates** - !MC5 has a default certificate store containing issuer certificates, that is maintained by Bartsch Software. It contains often used issuer certificates, that are not present in the windows certificate store, e.g. root and CA certificates of the Odette organisation. If the module OFTP2 is licensed, then this option is activated by default. The !MC5 default certificates can be viewed in the *Certificates* section.

**Use TSLs** - Trusted Service Status Lists (TSLs) are lists of trusted issuer certificates published by different organisations. Activating this option includes the TLSs listed in the section TSLs for certificate validation. If the module OFTP2 is licensed, this option is enabled by default. The *Odette OFTP2 TSL* is always present so it is then used as recommended by Odette.

> **Download Odette TSL via unsecure HTTP connection (not recommended!)** - By default the Odette TSL get downloaded using a encrypted HTTPS connection. By enabling this option the TSL get downloaded using an unencrypted HTTP connection. This might be useful, if the secure download isn't possible due to local network settings. Though the downloaded TSLs signature is always validated before using it, downloading it using an encrypted HTTPS connection is recommended for security reasons.

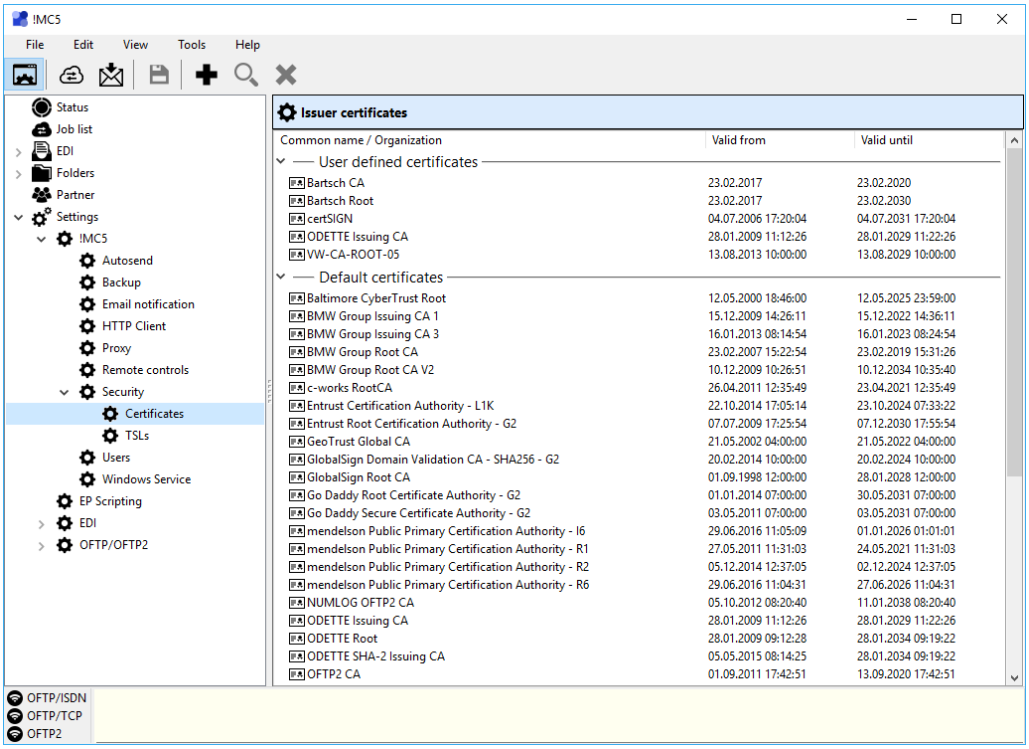
**Use Windows certificate store** - Activate this option to use certificates from Windows' certificate store for validation. Be advised that certificates present in the Windows store might depend on the user account used to start !MC5, as each user account has its own certificate store.

Next to the de-/activated validation sources user defined certificates (see *Certificates*) are always used for validation.

## Validation options

**Mandatory revocation check** - When validating certificates !MC5 can automatically check for certificate revocation using CRLs (*Certificate Revocation Lists*) or OSCP (*Online Certificate Status Protocol*). If this option is activated, a successful revocation check, either CRL or OSCP, is mandatory (if one or both methods are available for the specific certificate). If the revocation check fails, validation fails. Depending on the local network configuration, the revocation check can fail due to firewalls blocking access to the respective resources. In such a case deactivte this option or change the firewall/network configuration.

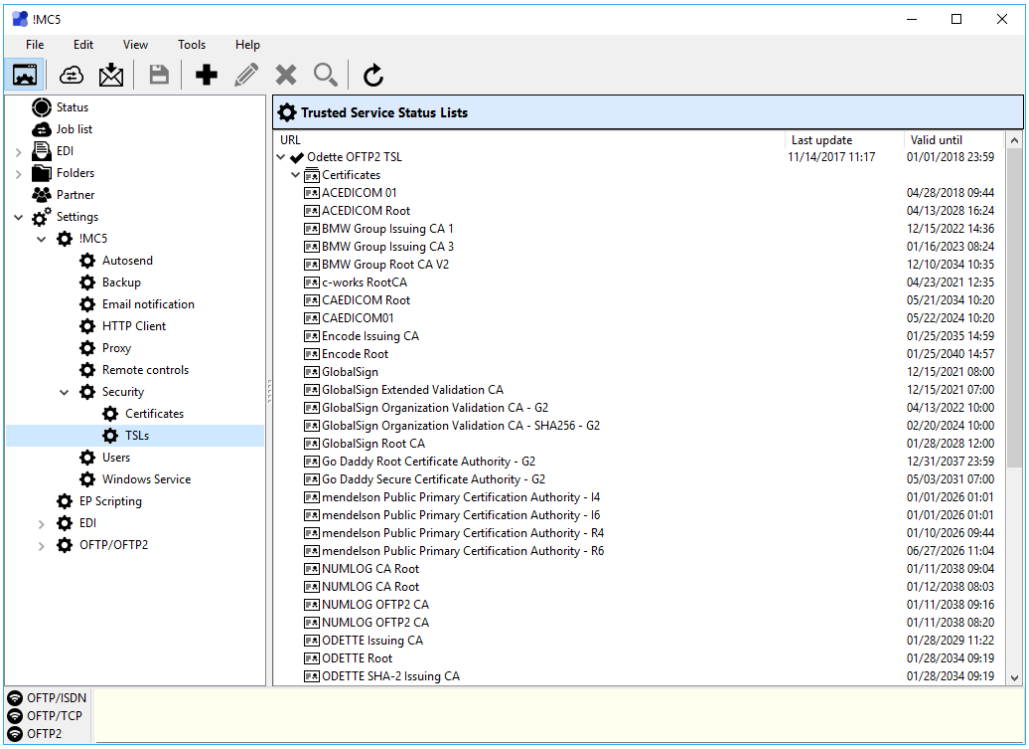
### 5.3.1.8.1 Certificates




The *Certificates* section allows to view the !MC5 default certificates, that are used for validation, if the respective option in the *Security* section is enabled.

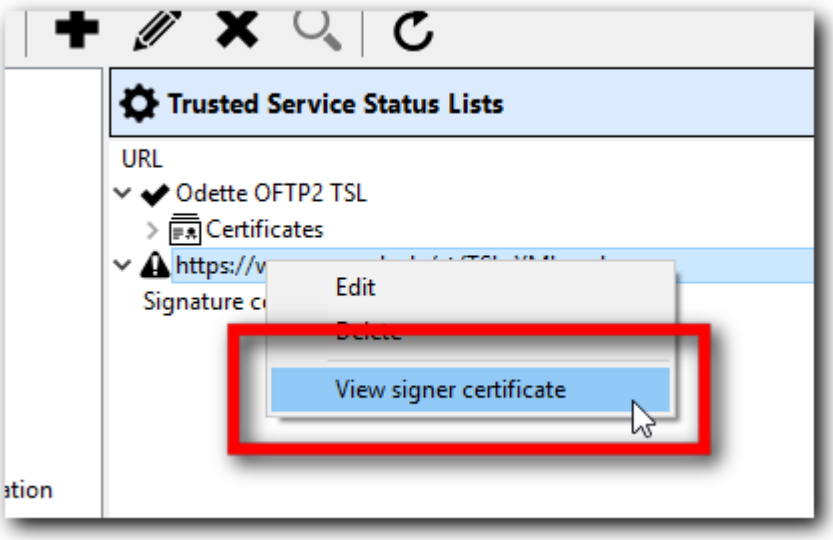
Additionally user defined certificates can be imported, viewed and deleted. User defined certificates are always used for certificate validation, regardless of other de-/activated security options.

### 5.3.1.8.2 TSLs




## Trusted Service Status Lists

Trusted Service Status Lists (TSLs) are lists of trusted services, published by different organisations, e.g. the Odette organisation. Those lists contain trusted issuer certificates, which are needed to validate certificates. Only certificates, whose issuer certificates are present in one of the activated validation sources can be validated successfully. If the module OFTP2 is licensed !MC5 by default activates the usage of the Odette OFTP2 TSL and it's internal default certificates, which are needed to verify the signature of the OFTP2 TSL.



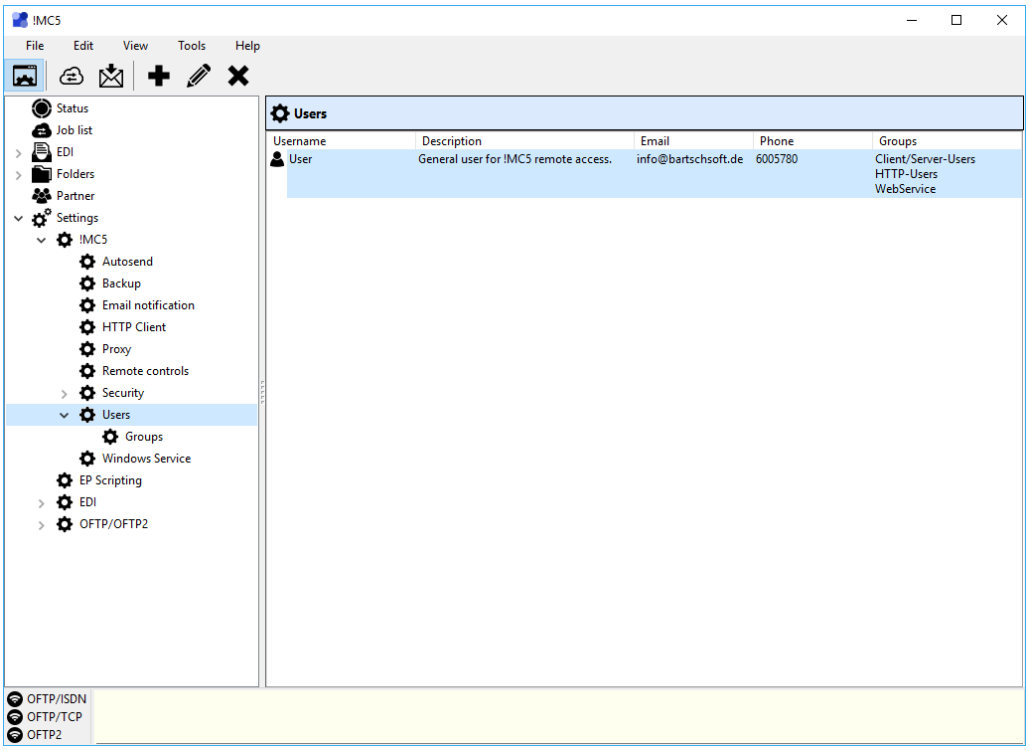
Every TSL is signed by its publisher. To use the certificates contained in a TSL, that signature must validate. If the List is signed using an issuer certificate, it can be added to the user defined certificates by viewing the signer certificate and then clicking the Save certificate button inside the certificate preview dialog.

### 5.3.1.9 Users and groups

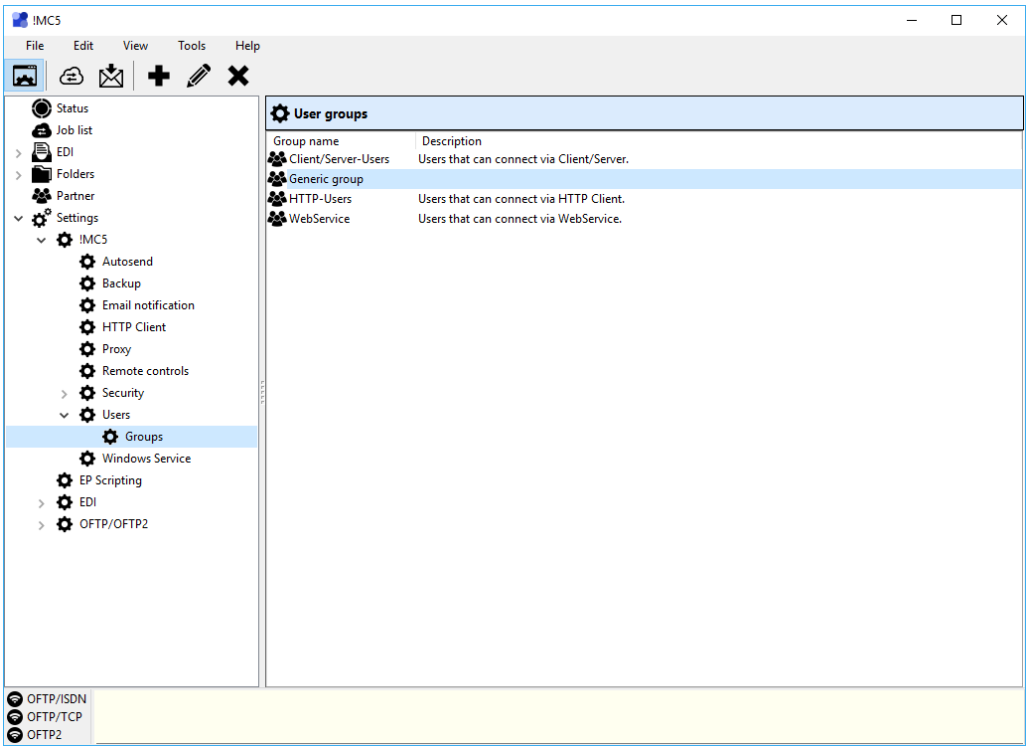
(Client/Server, HTTP Client and Web Service add-ons only)

The add-ons Client/Server, HTTP Client and Web Service require a login using a username and password. Those users can be managed here. Each user has specific access permissions and can be added to different groups, which have access rights of their own. For access to the HTTP Client, the Web Service or via Client/Server a user has to be added to the corresponding predefined group *HTTP-Users*, *Client/Server-Users* or *WebService*.

Both users and user groups can be managed on this settings pages.




**User management**




**User group management**

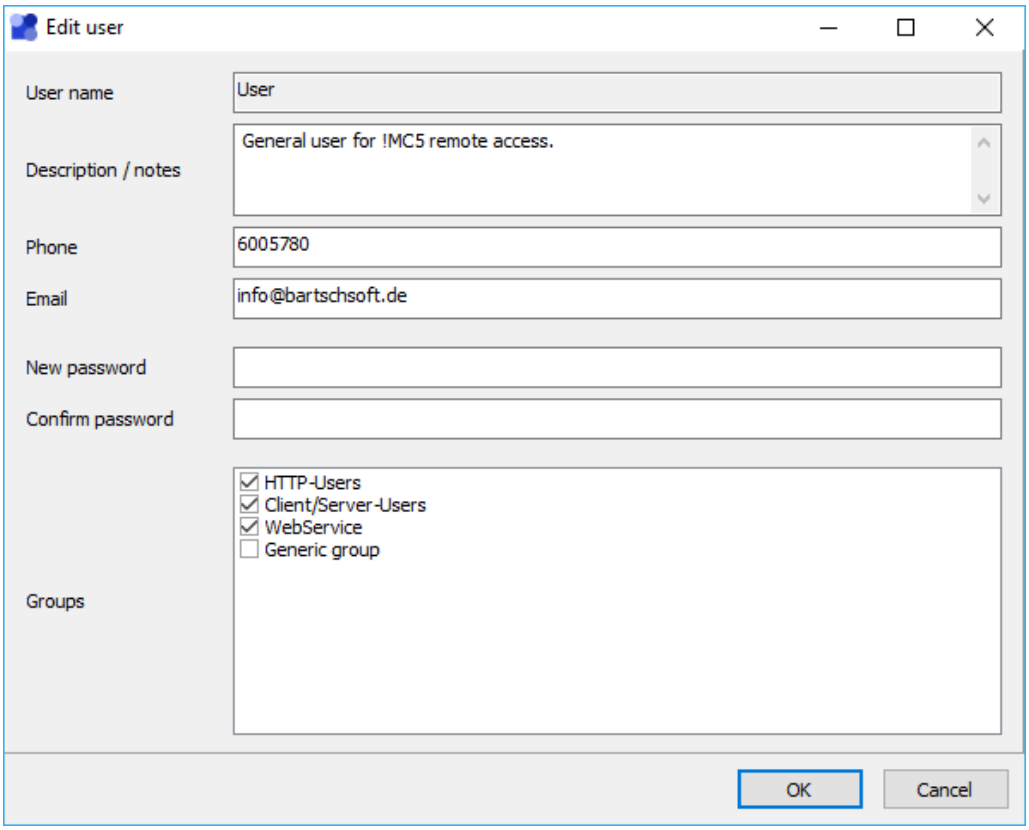
## Available functions

**Add new user / group** - Create a new user or a new user group.

**Edit selected user / group** - Edit the in the list selected user or user group.

**Delete selected user / group** - Delete the in the list selected user or user group.

#### 5.3.1.9.1 Create/edit a user



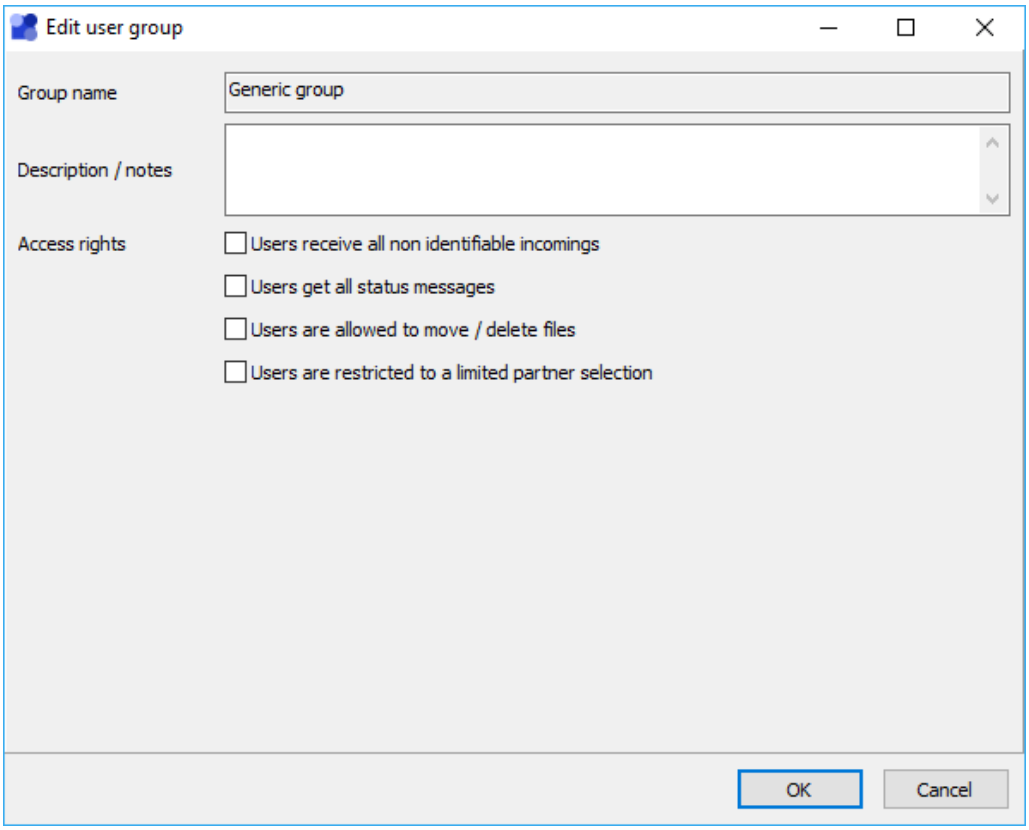

The *User name* is the login that has to be used to log in using the Client/Server, HTTP Client or Web Service. The *User name* can only be edited when creating a new user.

*Description*, *Phone* and *Email* are for internal use only.

A *Password* has to be entered upon creating a new user. When editing an existing user you can change the users password by entering it into the field *New password*. If this field is left blank, the existing password won't be changed. A new password always has to be confirmed in the field *Confirm password*.

Most important, next to *User name* and *Password*, are the group memberships. To gain any access permissions a user has to be added to the respective group. The user is added or removed to or from a group by checking the respective entry in the list *Groups*.

### 5.3.1.9.2 Create/edit a group




For a user to gain certain permissions he has to be member of a group that is granted those permissions. Any amount of groups can be created granted different sets of permissions. The *Group name* can only be edited when creating a new group.

The following permissions are available:

**Users receive all non-identifiable incomings** *(Client/Server only)*
Members of this group see all incoming files which are not ENGDAT formatted or whose forwarding address is not an user name. If deactivated group members only see those incoming files, for which the ENGDAT forwarding address matches their user name.

**Users get all status messages**
When deactivated members of this group only see status messages concerning jobs created by the respective user. If activated members see all status messages which are shown on the status page of !MC5.

**Users are allowed to move / delete file**
Without this permission a user has read only access to received files. When activated Client/Server users can move files from the server to the client and HTTP Client users can delete files on the server. Deleted or moved files are no longer available to other users.

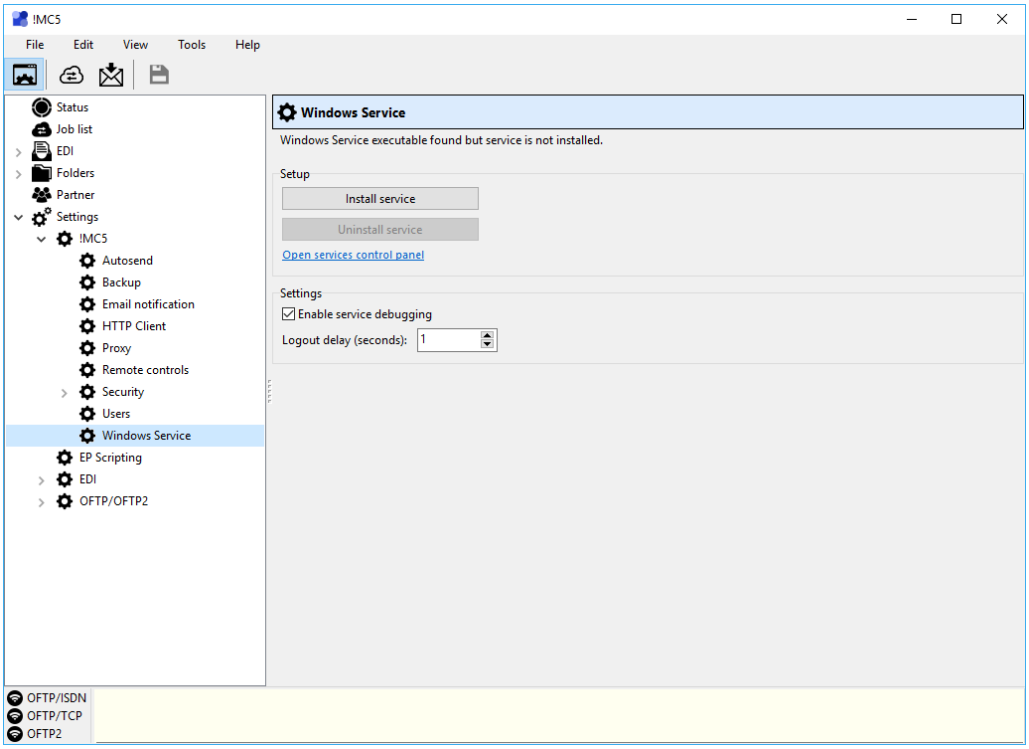
**Users are restricted to a limited partner selection**
When activated members of this group only see those partners, for which this group is specified in the special functions of the partner (see Special functions / *Client/Server groups*). By this you can limit the partners a user can send files to restrict access to received files only from certain partners. As soon as a user is mem-

ber of one group using this option the limitations are applied. All partners which are at least assigned to one group the user is member of will be accessible to the user.

Changed group permissions are applied to all members of that group.

### 5.3.1.10 Windows Service

(*Windows Service add-on only* )




Configuring Windows Service requires !MC5 to be started with administrator privileges. If not started using the appropriate privileges !MC5 can be restarted as administrator using the button on the settings page.

## Setup

**Install service**
Installs the windows service. Only available if the Windows Service executable is present and the service is not already installed.

> **Service access rights**
> When installing the service by default it will log using the local system account. Verify that the user account used to run the service has proper access rights to all directories and network paths used by MC5. If needed either grant the user all needed access rights or change the user used to run the MC5 Windows Service (you can use the link *Open services control panel* to change the user).

**Uninstall service**
Uninstalls the Windows Service. Only available if the service is installed.

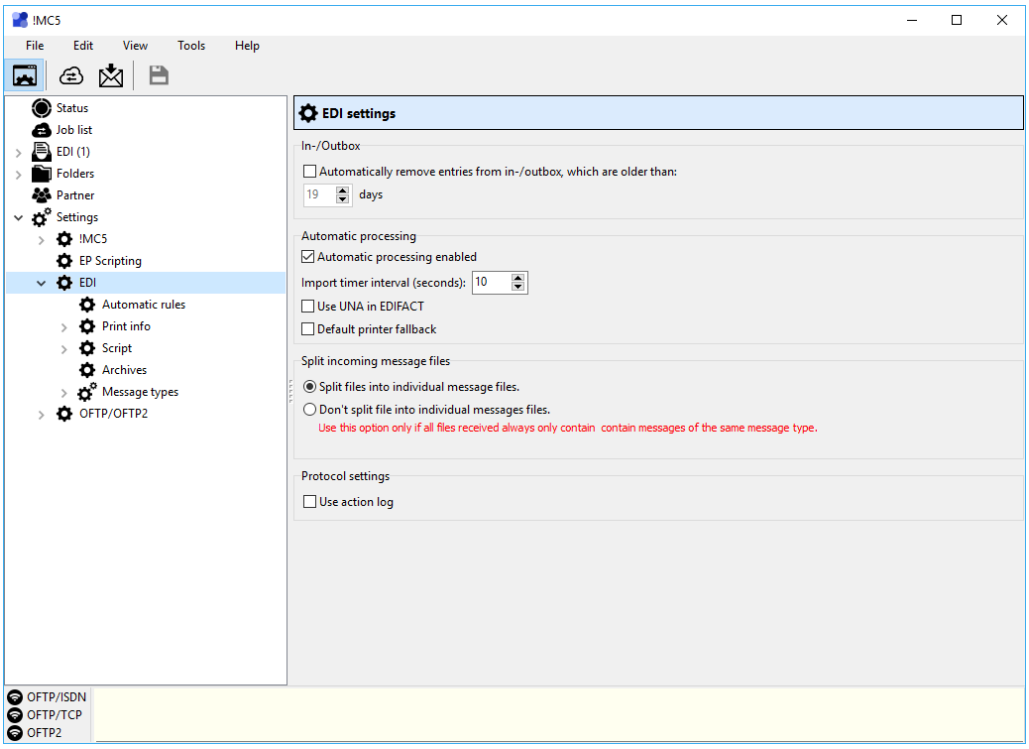
## Settings

**Enable service debugging**
If debugging is activated the Windows Service logs errors and certain events in a special log file saved to the !MC5 log folder. This option can also be activated using *-d* as service startup parameter.

**Logout delay (seconds)**
When a Windows user logs out, the !MC5 background process gets stopped and restarted as soon, as the Windows login screen shows. If the restart happens too fast this can result in !MC5 not starting up correctly. When this is the case increase the *Logout dealy*. The default delay is one second. This logout delay value can also be set using *-tnn*, with *nn* replaced by the number of seconds, as service startup parameter.

## 5.3.2 EDI

### 5.3.2.1 EDI settings




## In-/Outbox

**Automatically remove entries from in-/outbox, which are older than:**
This settings determines if and after how many days messages will automatically get deleted from the EDI in- and outbox. Only the respective entries in the in- or outbox will get deleted. The message will still be accessible using the archives.

## Automatic processing

**Automatic processing enabled**
Enables or disables all automatic processing (import and export rules) of EDI messages.

**Import timer interval (seconds):**
The interval, in seconds, in which !MC5 searches for new files to import.

**Use UNA in EDIFACT**
Enable this option, if created EDIFACT messages are to contain the UNA segment.

Default printer fallback
If this is activated and a selected printer isn't found during automatic processing, !MC5 tries to use the systems default printer for printing. Use this option with caution, especially when using the Windows Service.

## Split incoming message files

**split into messages**

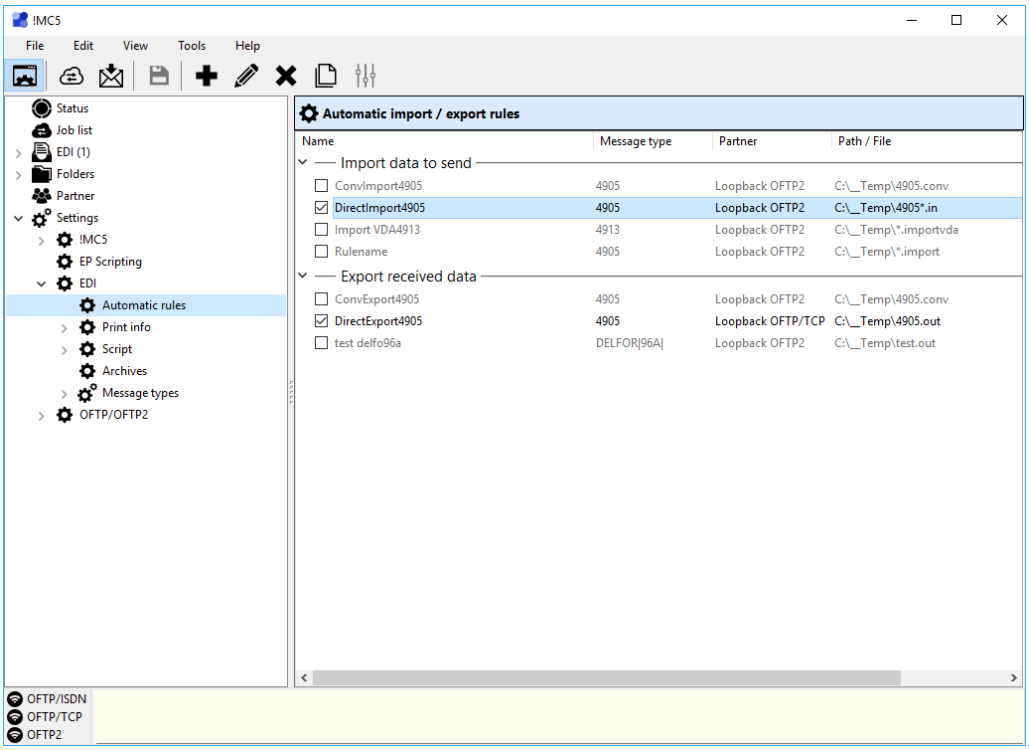
Tests all incoming message files, if their contain more than one message and if so, splits the file into multiple message so the get processed independently. This is necessary if you receive files containing multiple messages of different types.

**always treat as single message**
With this settings no check for multiple messages in a single file will be performed. Only use this setting if all files you receive contain either a single message or all contained messages are of the same type.

## Protocol settings

**Use action log**
If activated the additional log file *action.log* will be created in the log folder in which information about imported EDI messages and their processing state are logged.

### 5.3.2.2 Automatic import/export rules




Message import and export rules allow the automatic import of EDI messages into !MC5 and export of received messages from !MC5 into external files. *Rules* lists all import and export rules, grouped by type (import or export), sorted by rule name.

The *Message type* of a rule is the target typ for imports and the source type for exports. Individual rules can be activated or deactivated using the list entries checkbox.

The following functions are available:

**New rule** - Create a new rule.

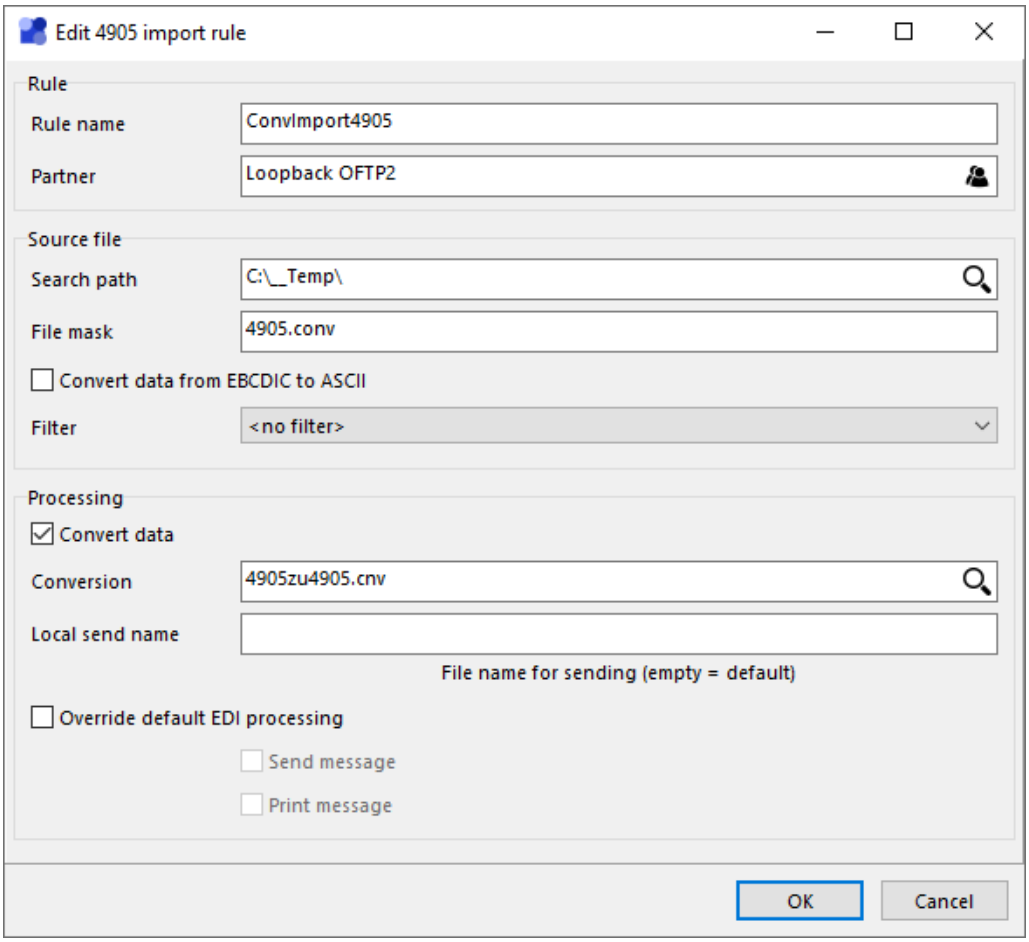
**Edit rule** - Edit the selected rule.

**Delete rule** - Delete the selected rule.

**Copy rule** - A copy of the selected rule will be used to create a new rule.

**Edit auto increments** - Edit auto increment values of the selected rule.

#### 5.3.2.2.1 Import rules




The dialogs for new rules and for editing existing rules are identical.

## Rule

**Rule name**
Name of the rule as displayed in the rule list.

**Partner**
Partner for which this rule will be applied, i.e. messages imported through this rule will be sent to this partner.

## Source file

Source file information.

**Search path**
The folder in which to search for matching files.

**File pattern**
The file pattern which files in the search path have to match, so this rule will get applied. The special characters * and *?* can be used in the file pattern. * stands for any number of characters, *?* for one arbitrary character. E.g. only * as file pattern will select any file inside the search path, **.txt* only files with the extension *.txt*, *ABC?.**

selects all files whose file name is four characters long and starts with *ABC*, *file.txt* only selects files named exactly *file.txt*.

**File is in EBCDIC format**
Activate this option, if the file to import uses the EBCDIC character set. This option doesn't affect the character set used for sending the imported message!

**Filter**
An additional filter can be specified that will be applied to matching files before the conversion. This filter can be used to filter out files based on their content or to modify the file content prior to conversion.

## Processing

**Convert data**
Choose if imported data should get converted and if so, which conversion to use. If no conversion is specified, only files which already are in the source type format will get imported.

**Send name**
The filename that should be used when sending the imported file. If left empty, the original name of the imported file will be used. Different place holders can be used for specifying the file name:

* - Original file name of the imported file.
# - # characters will get replaced by a counter which increases with each file imported using this rule. The maximum value of the counter is limited by the number of # characters used. # will count up to 9, ## up to 99 and so on.
*$SCRIPTNAME$* - Gets replaced with the value of the script variable *OutputFilename* after executing the conversion. This variable can be set anywhere in the conversion script to e.g. create a file name using contents of the source or destination message. If not set during conversion the place holder get substituted by *default.out*.

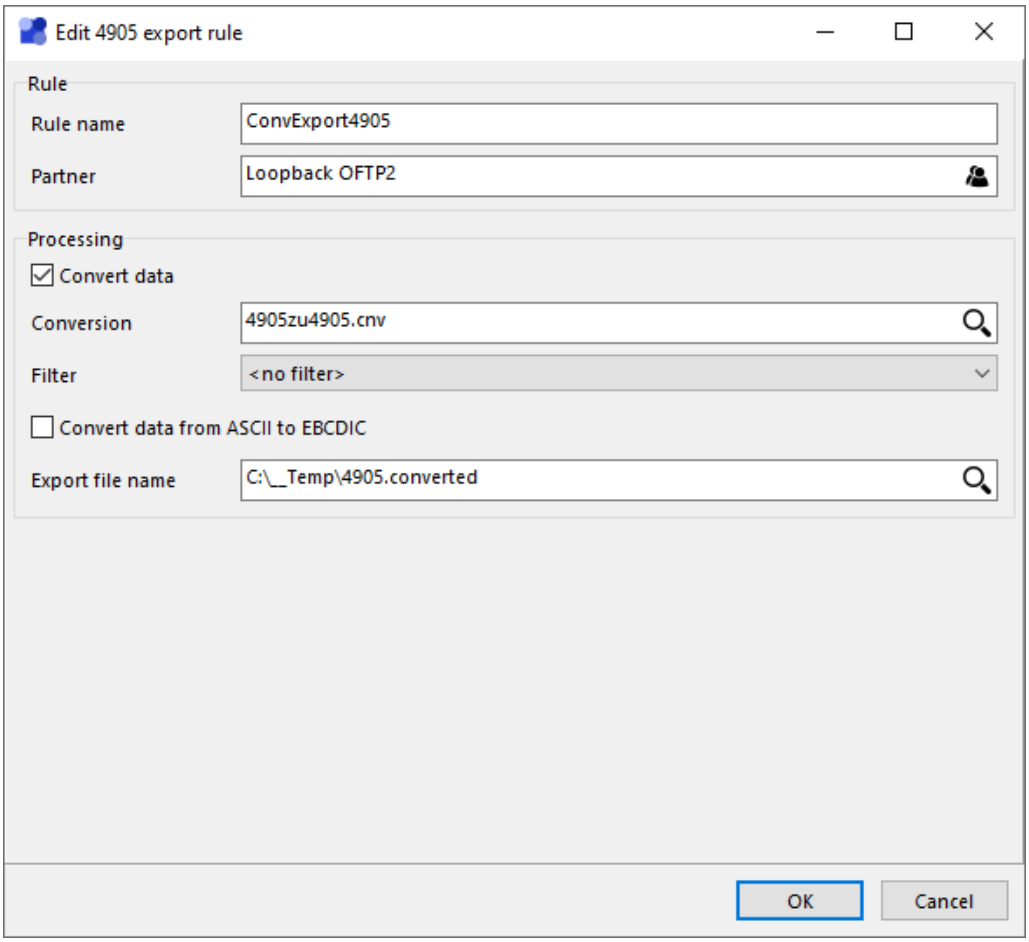
All three place holders can be combined at will.

**Override default EDI processing**
Activate this option to override the settings made in automatic processing for the selected message type.

**Send message**
Activate to automatically send the imported message to the partner.

**Print message**
Activate to automatically print the imported message (after conversion).

#### 5.3.2.2.2 Export rules




The dialogs for new rules and for editing existing rules are identical.

## Rule

**Rule name**
Name of the rule as displayed in the rule list.

**Partner**
Partner for which this rule will be applied, i.e. only messages received from the selected partner will get exported using this rule.

## Processing

**Convert data**
The conversion used to export the received message. Exporting without conversion saves the received data as is to the target file.

**Export file name**
Target file name for the converted file including the full path where the file will be saved. The following place holders can be used:

# - # characters will get replaced by a counter which increases with each file imported using this rule. The maximum value of the counter is limited by the number of # characters used. # will count up to 9, ## up to 99 and so on.
*$SCRIPTNAME$* - Gets replaced with the value of the script variable *OutputFilename* after executing the conversion. This variable can be set anywhere in the con-

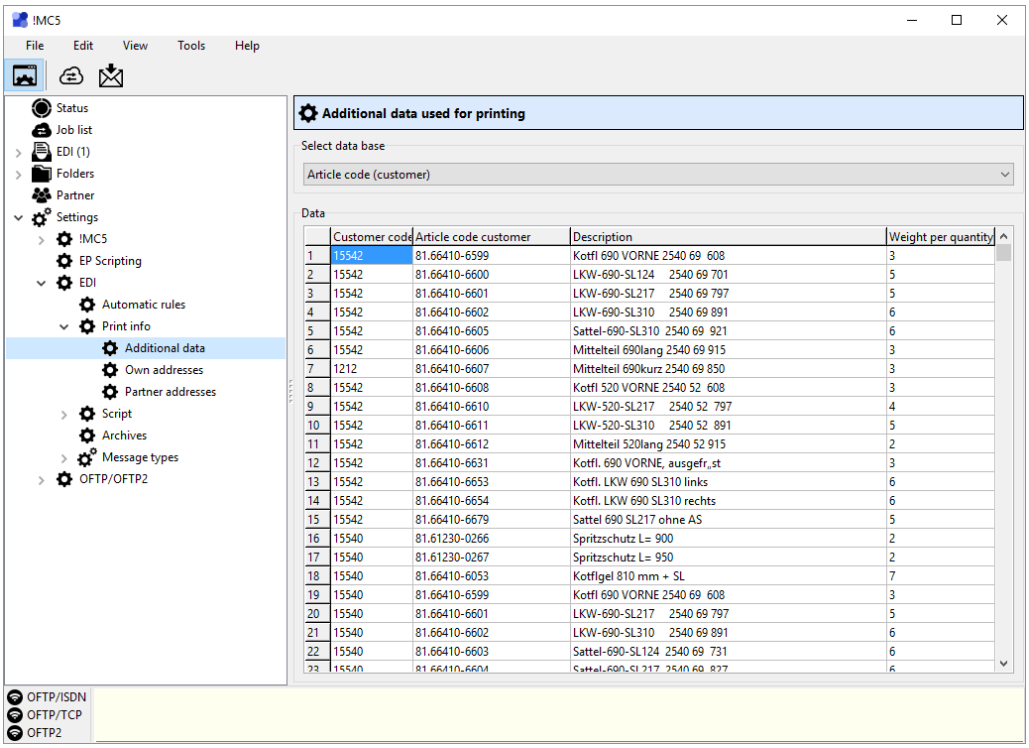
version script to e.g. create a file name using contents of the source or destination message. If not set during conversion the place holder get substituted by *default.out*.

**Filter**
An optional filter that will get applied to the data after conversion. The filter can be used to e.g to alter the exported data.

**Save file in EBCDIC format**
Activate to save the converted data using the EBCDIC character set.

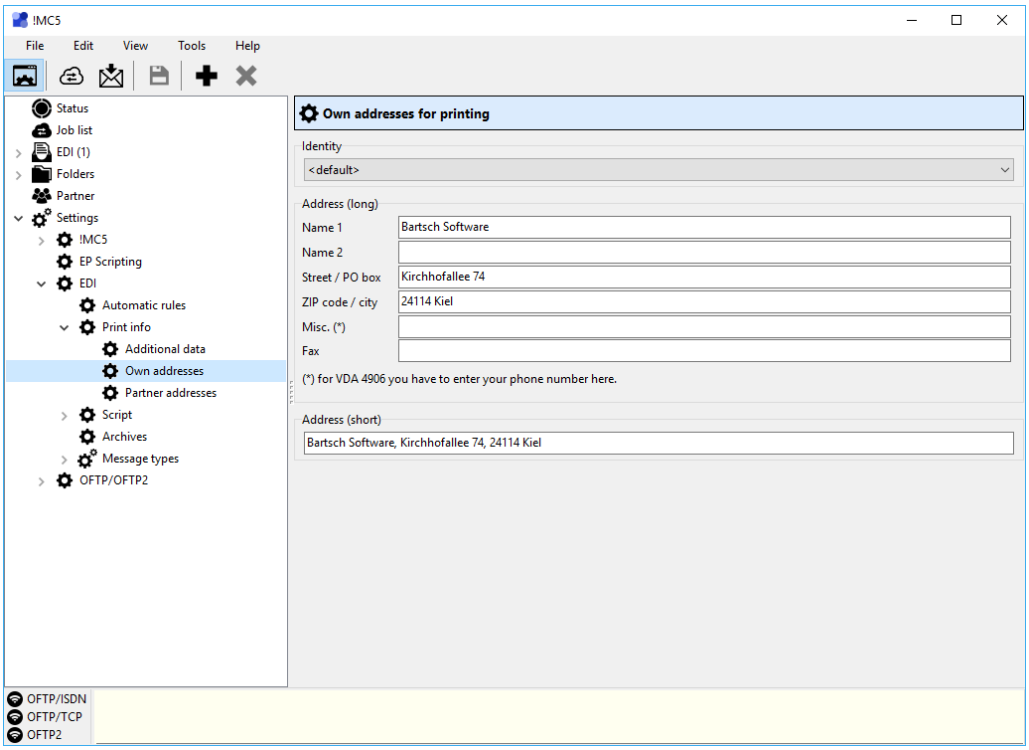
### 5.3.2.3 Print info

#### 5.3.2.3.1 Additional data




The additional data entered here is used for printing of some messages type formats, e.g. VDA 4902 transport labels. The data can be entered manually or by defining data base associations in FlatFile definitions to automatically capture data while reading a FlatFile.

### 5.3.2.3.2 Own addresses




Your own addresses are needed when printing of some message types.

## Identity

For printing on or more different identities can be used. By using print rules some message types can use different identities based on message content when being printed (see Print rules). The following functions are available:

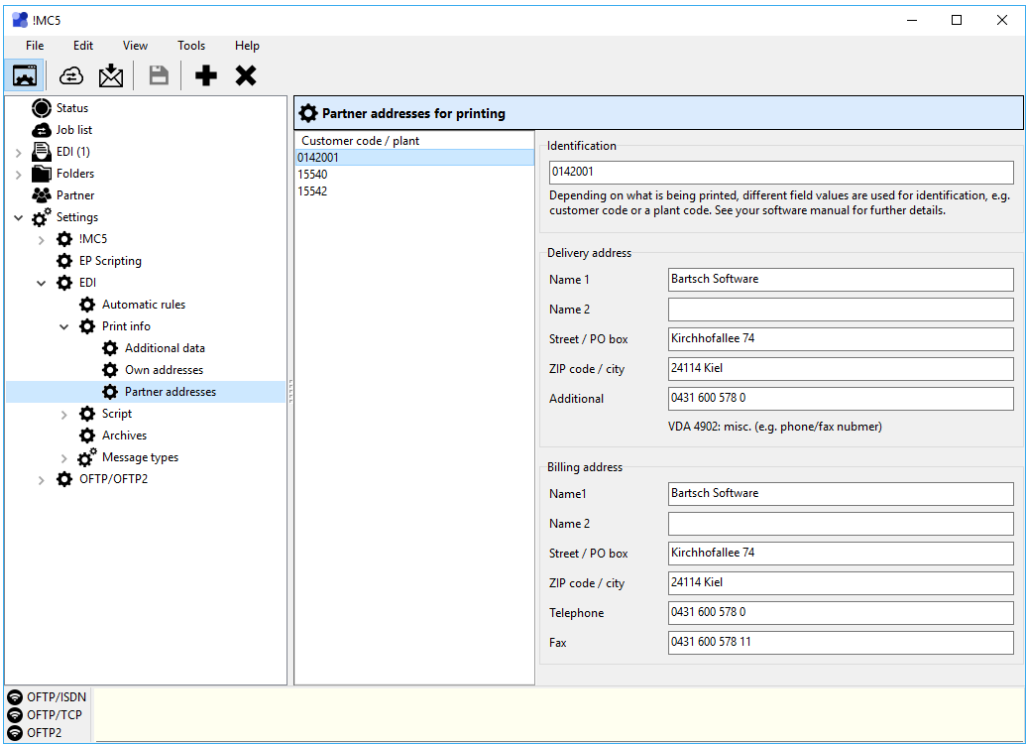
***Add new identitiy*** - Add an additional identity.

***Delete selected identity*** - Delete the selected identitiy. The identity *<default>* can not be deleted.

## Address (long) / Addresse (short)

Company info used for the selected identity. The information will be used when printing messages using e.g. VDA4902, VDA4906, VDA4912 or VDA4922 standards.

### 5.3.2.3.3 Partner addresses



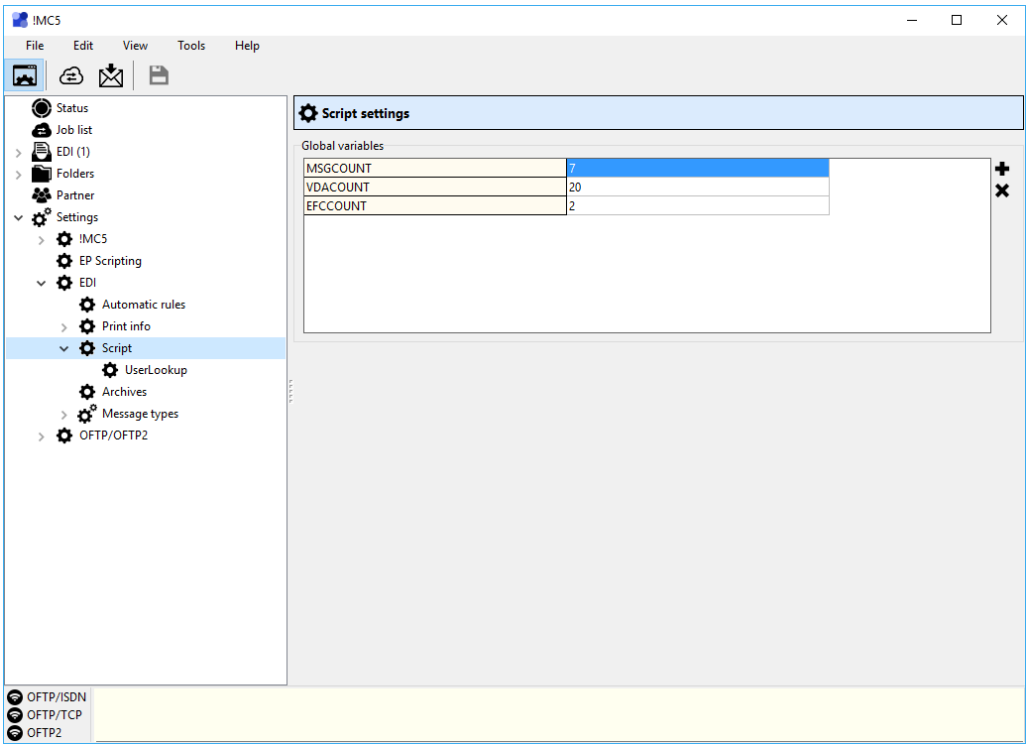

Partner addresses are used for printing of some VDA message type formats. Which addresses are used when printing and which fields are used for identification of the address is described in the references of the messages types. In most cases the customer number of the message is used for identification.

The following functions are available:

***Add new entry*** - Add a new partner address.

***Delete selected entry*** - Delete the selected address.

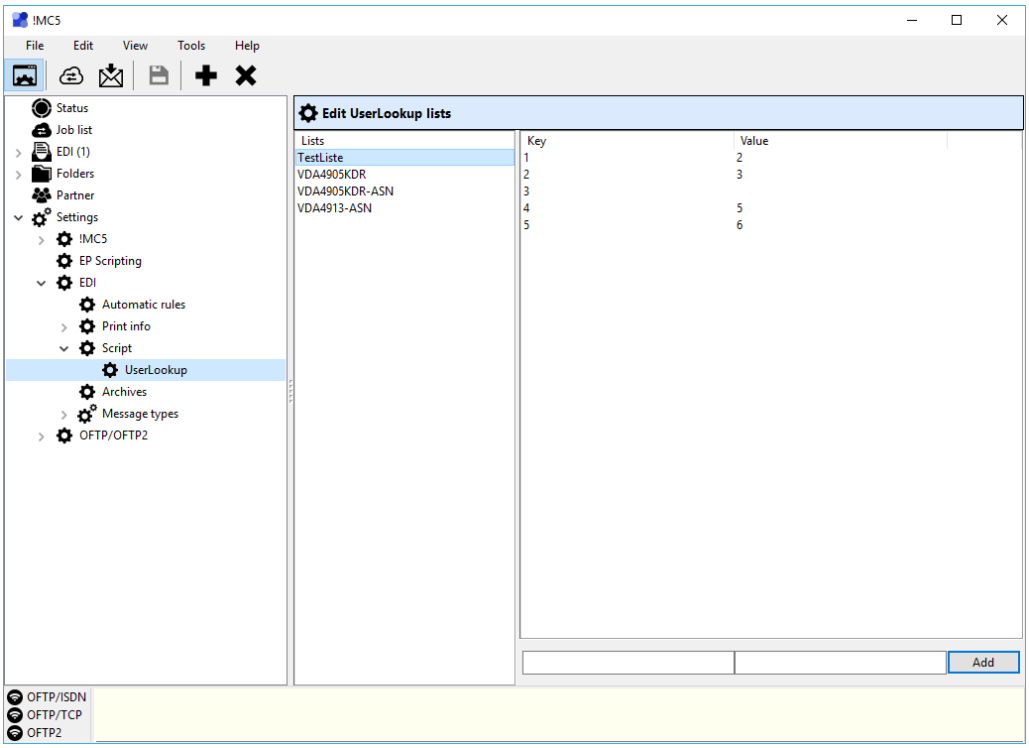
### 5.3.2.4 Script




## Global variables

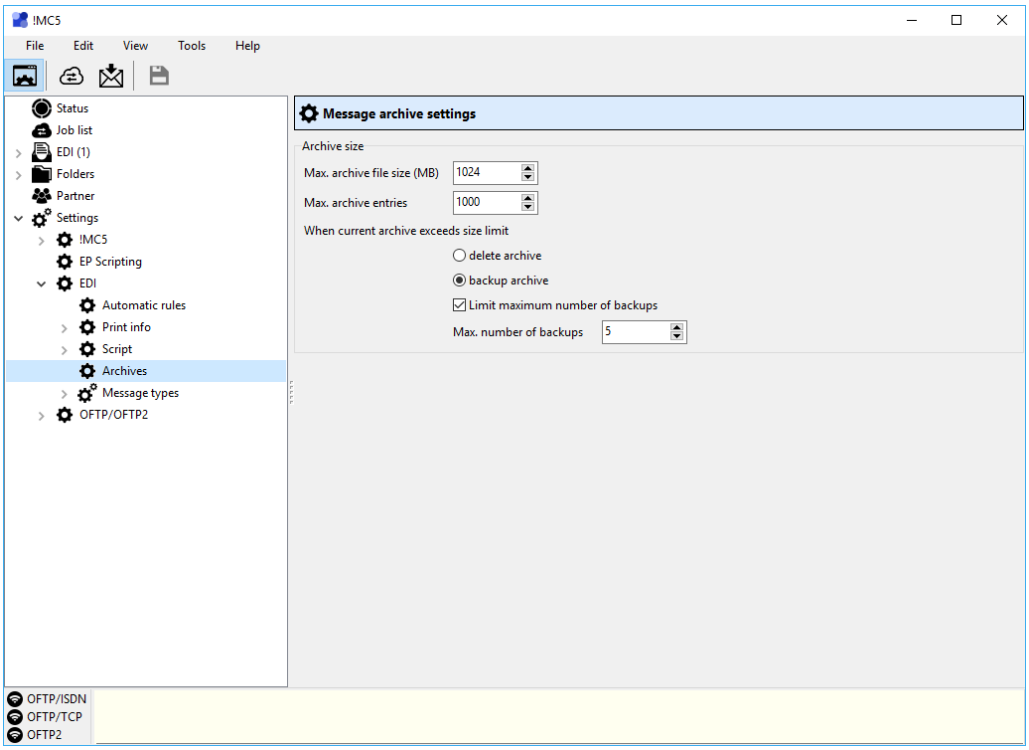
This list shows all known global script variables. Global variables keep their values between conversions. Here, new variables can be added and existing ones deleted. When adding a new variable an initial value can be specified. It is not necessary to add a new global variable here before it can be used in a conversion script, only to specify an initial value. Each variable declared using the key word *registry* will be treated as global variable. If not already found it will get an initial value of *0*.

### 5.3.2.4.1 UserLookup




Here you can edit UserLookup tables which can be used during conversions by using the UserLoopup function in the script.

### 5.3.2.5 Archives




## Archive size

All processed EDI messages are stored in an internal database. To prevent the data base to become too large and thus reduces system performance, !MC5 creates backups of the database when it hits one of the specified size limits.

**Max. database size in MB**
Maximum size of the message database in megabyte.

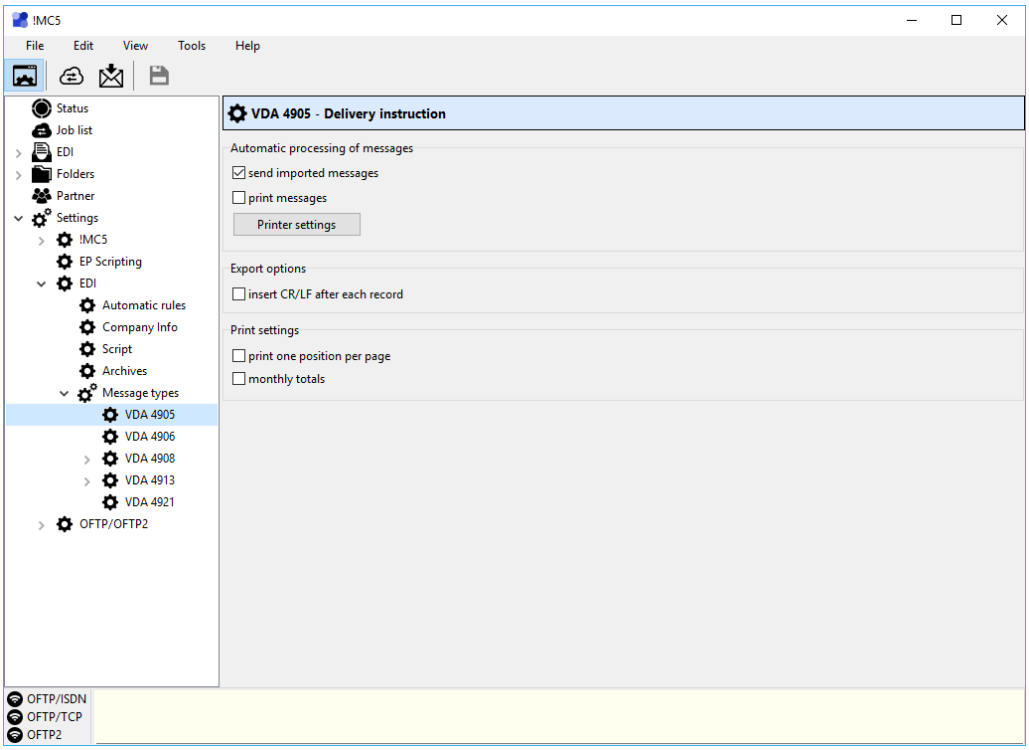
**Max. number of entries**
Maximum size of database in stored messages.

**When current archive exceeds size limit**
Select what happens, if the current Archive exceeds one of the size limits. *Delete archive* deletes the existing one and creates a new archive. All messages contained in the old database will be lost! B*ackup archive* will backup the existing archive and then create a new one. Backed up archives are accessible using the *EDI / Archives* page in the main !MC5 window.

**Limit maximum number of backups**
If this option is enabled, the maximum number of archive backups will be limited to the value specified in *Max. number of backups*. When the maximum number of backups is reached, the oldest backup will be replaced. Use this option e.g. if only limited disc space is available.

**Max. number of backups**
Defines how many archive backups will be created before the oldest backup gets replaced.

### 5.3.2.6 Message types




Default processing options for incoming and outgoing messages can be defined for each registered message type. Automatic processing rules can override these settings. The available settings can differ for each message type. Common processing for all types are the following:

## Message processing

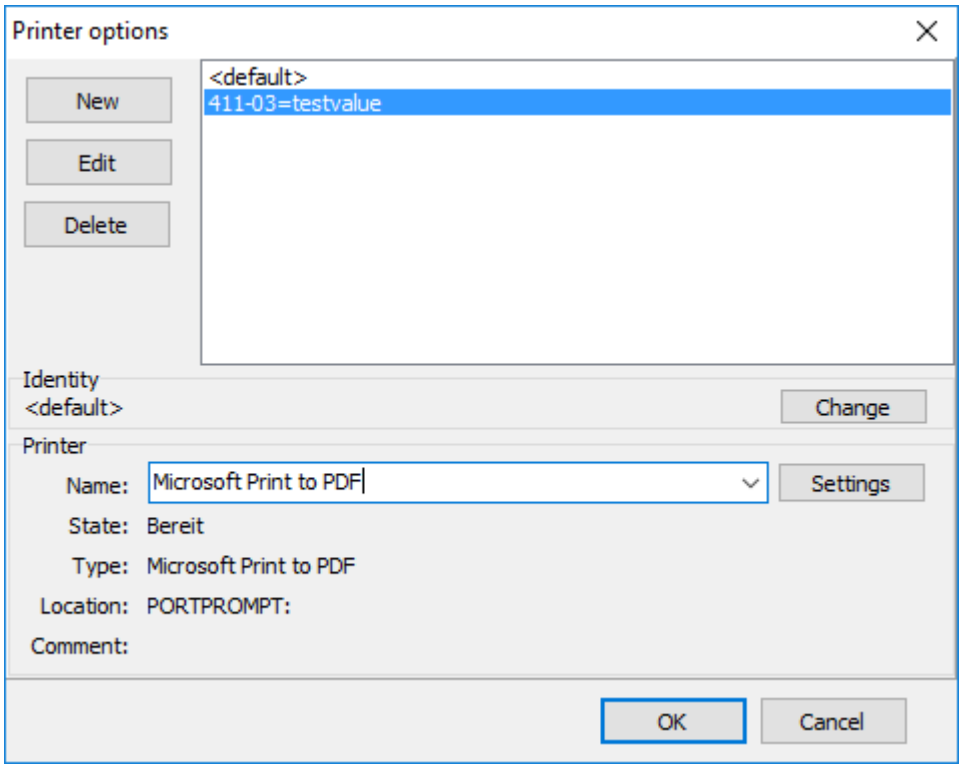
**send imported messages**
Imported messages (imported using automatic processing) will automatically get sent to respective partner.

**print messages**
Incoming and outgoing messages will be printed automatically to the printer selected using the Printer options.

**Printer settings**
Select which printer, format and settings will be used for printing. These settings will only apply to the selected message type. For each message type different settings can be chosen, e.g. printing different message types to different printers.

### 5.3.2.6.1 Print rules

Using print rules messages of certain types can be printed to different printers depending on message contents. For example messages sent to the different plants of one partner can get printed to printers in different departments before being sent.




The print rule <*default*> is the default rule and can not be deleted. This rule will get used if a message matches no other rule or no other rule is specified. For each rule different printer, printer settings and identity (see Company info) can be used. Selecting a rule shows the selected settings.

Clicking *New* adds a new rule. First the field of the specific message that has to be checked for a certain value, then the value which that field has to contain for the rule to apply must get entered. Clicking *Edit* allows to edit the selected rule. *Delete* deletes the selected rule.

**Content based identity selection**

If the field value of a print rule matches the name of a identity (see *Own addresses*) that identity will be used for printing. **The name of the identity has to exactly match the field value**, else the default identity will be used.

### 5.3.2.6.2 VDA 4906

#### Used addresses

**Own address**

| Field | Content / Format |
|---|---|
| Field 8 (Company) | Name 1 |
| Field 9 (Name/Dept.) | Name 2 |
| Field 10 (Phone) | Misc. |
| Field 11 (Fax) | Fax |
| Field 12 (Address) | Street / PO box<br>Zip code / city |

**Partner address (Invoice address)**

| Field | Key | Content / Format |
|---|---|---|
| Field 15 (Company) | Customer code (811-3) | Name 1 |
| Field 16 (Name/Dept.) | Customer code (811-3) | Name 2 |
| Field 17 (Phone) | Customer code (811-3) | Phone |
| Field 18 (Fax) | Customer code (811-3) | Fax |
| Field 19 (Address) | Customer code (811-3) | Street / PO box<br>Zip code / city |

### 5.3.2.6.3 VDA 4908

#### Used addresses

If the key from field 821-4 was found in the partner addresses:

**Own address**

| Field | Content / Format |
|---|---|
| Customer | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Supplier | Field 821-4 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

If the key from field 821-3 was found in the partner addresses:

**Own address**

| Field | Content / Format |
|---|---|
| Supplier | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Customer | Field 821-3 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

### 5.3.2.6.4 VDA 4913

#### 5.3.2.6.4.1 VDA 4902

## Used addresses

**Own address**

| Field | Content / Format |
|---|---|
| Field 4 | Address, short |
| Field 17 | Name 1, Street / PO box, Zip code / city |

**Partner address**

***Default***

| Field | Key | Content / Format |
|---|---|---|
| Field 1 (Recipient) | Field 711-3 | Name 1<br>Zip code / city |

***Field 2 / Use long address of recipient***

| Field | Key | Content / Format |
|---|---|---|
| Field 1 (Recipient) | Field 711-3 | Name 1<br>Name 2<br>Zip code / city |
| Field 2 (Recipient continued) | Field 711-3 | Street / PO box<br>Misc. |

***KLT label***

| Field | Key | Content / Format |
|---|---|---|
| Field 1 (Recipient) | Field 711-3 | Name 2<br>Zip code / city |

#### 5.3.2.6.4.2 VDA 4912

### Used addresses

**Own address**

| Field | Content / Format |
|---|---|
| Supplier address | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Customer address | Field 711-3 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

#### 5.3.2.6.4.3 Control protocol

### Used addresses

If the key from field 711-3 was found in the partner addresses:

**Own address**

| Field | Content / Format |
|---|---|
| Customer | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Supplier | Field 711-3 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

If the key from field 711-4 was found in the partner addresses:

**Own address**

| Field | Content / Format |
|---|---|
| Supplier | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Customer | Field 711-4 | Name 1<br>Name 2<br>Street / PO box<br>Zip coed / city<br>Misc. |

#### 5.3.2.6.4.4 M.A.N. JIS

### Used addresses

**Own address**

| Field | Content / Format |
|---|---|
| Field 6 (Sender) | Address, short |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Field 4 (Receiver) | Field 711-3 | Name 1<br>Zip code / city |

#### 5.3.2.6.4.5 VDA 4922

### Used addresses

**Own address**

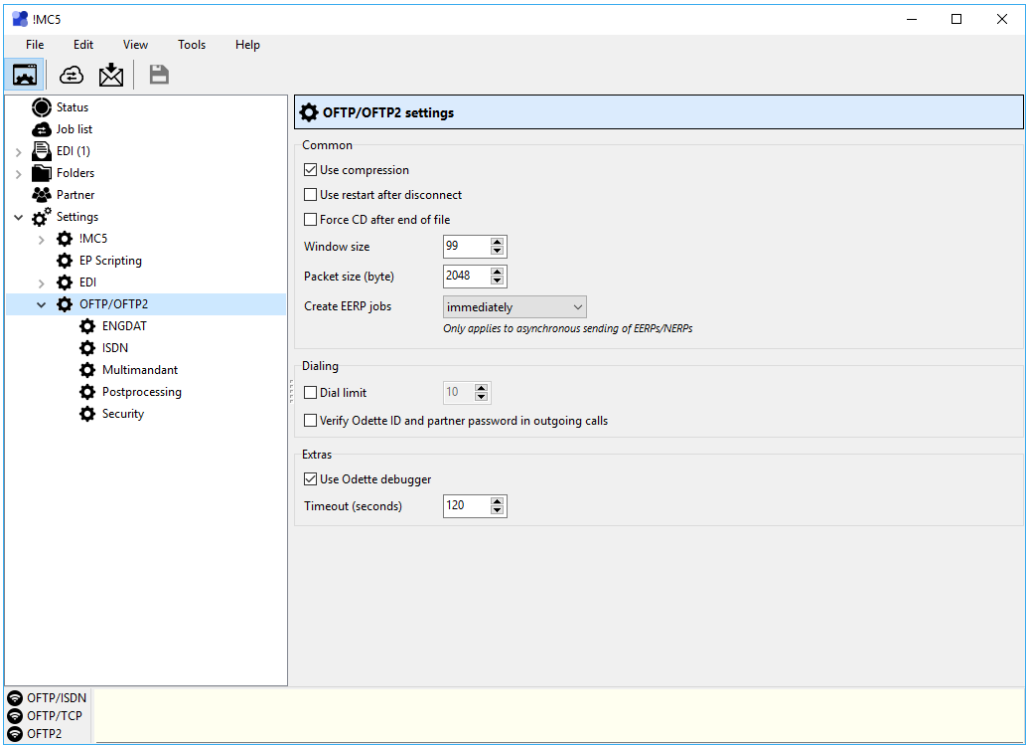
| Field | Content / Format |
|---|---|
| Field 1 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |

**Partner address**

| Field | Key | Content / Format |
|---|---|---|
| Field 9 | Field 712-13 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city<br>Misc. |
| Field 14 | Field 713-5, or if empty: Field 713-11 | Name 1<br>Name 2<br>Street / PO box<br>Zip code / city |

### 5.3.3 OFTP / OFTP2

*(OFTP and/or OFTP2 module only)*




## Common

**Use compression**
If enabled data will get compress during transmission. The compression used is part of the OFTP norm which is not as efficient as other compression methods like used for gzip or zip, so it can't replace those for large files.

**Use restart after disconnect**
If activated !MC5 will, in case of a disconnect during a transmission, try to resume the data transmission at the point when the disconnect occurred, so already transmitted data has not to be retransmitted. For this to work resuming has to be supported by the partner software.

**Force CD after end of file**
Some OFTP implementations don't handle the change direction (CD) command as specified in the OFTP norm. If receiving of multiple files from a partner doesn't work as expected this might be the cause. Activate this option tot try to "fix" such an issue.

**Window size**
The window size determines the amount of data packages !MC5 can send without waiting for a receipt of the communication partner. Only change the default value of 15 if explicitly needed by the partner.

**Packet size**
The size in byte of a single data package wich can be sent or received in one block. The default value is 2000 byte and it should only be changed if explicitly needed by the partner.

**Create EERP jobs**
By default EERPs (End to End Responses) will get immediately after a file is received. Some communication partners require a delayed transmission of EERPs. If so, you can set a delay using this setting. This setting only applies to cases, in which EERPS/NERPs are sent using a new connection, e.g. if any postprocessing of the received files is need. If files are not postprocessed, EERPs/NERPs are always sent directly using the same connection.

## Dialing

**Dial limit**
The number times !MC5 retries to connect to a partner if the connection could not be established. This value applies to each transmission job.

**Verify Odette-ID and password of partner in outgoing calls**
When this option is activated the partners received Odette ID and password are compared to those specified in the partner settings on outgoing connections. If they don't match, the connection will be refused. If the option is deactivated, ID and password are only compared on incoming connections.

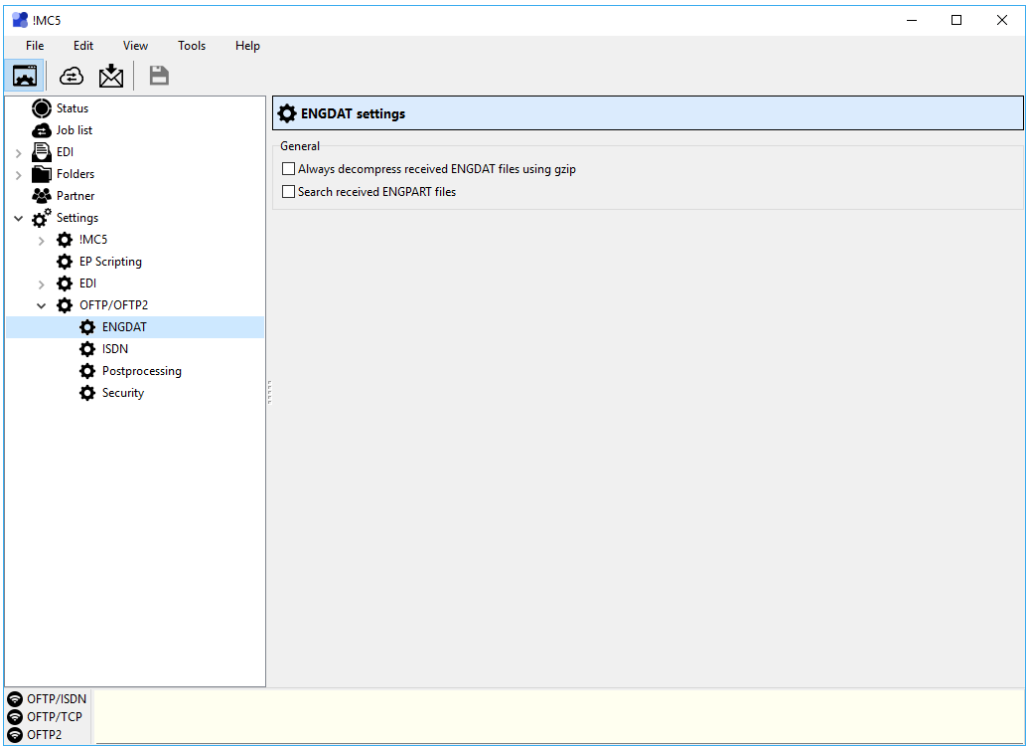
## Extras

**Use Odette debugger**
Activates detailed logging of each data transmission into the log files *DebugISDN.txt*, *DebugTCPIP.txt* or *DebugTLS.txt.* Only commands and no transmitted data will get logged.

**Time-Out**
The OFTP norm specifies a time out of two minutes, a relatively high value due to the early use of Datex-P for data transmission. For ISDN and TCP/IP connections this value can get reduced.

### 5.3.3.1 ENGDAT

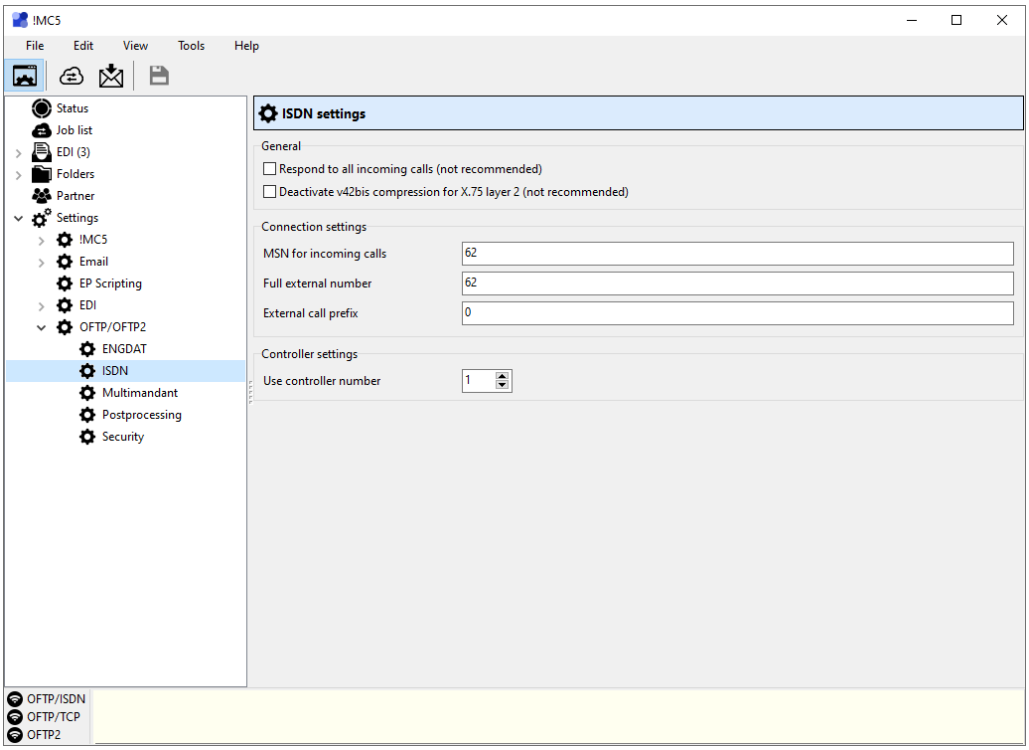
(*ENGDAT add-on only*)




**Always decompress received ENGDAT file with GZip**
The VDA recommendation is to compress all ENGDAT files using GZip. The compressed files are usually marked as such inside the ENGDAT abstract file. Activating this option !MC5 always tries to decompress all received ENGDAT files regardless.

**Search received EngPart files** *(EngPart add-on only)*
EngPart files are sent using the ENGDAT format. By activating this option received ENGDAT files will get scanned by the EngPart add-on for EngPart information. Received EngPart information will be displayed in the EngPart main window.

### 5.3.3.2 ISDN




## General

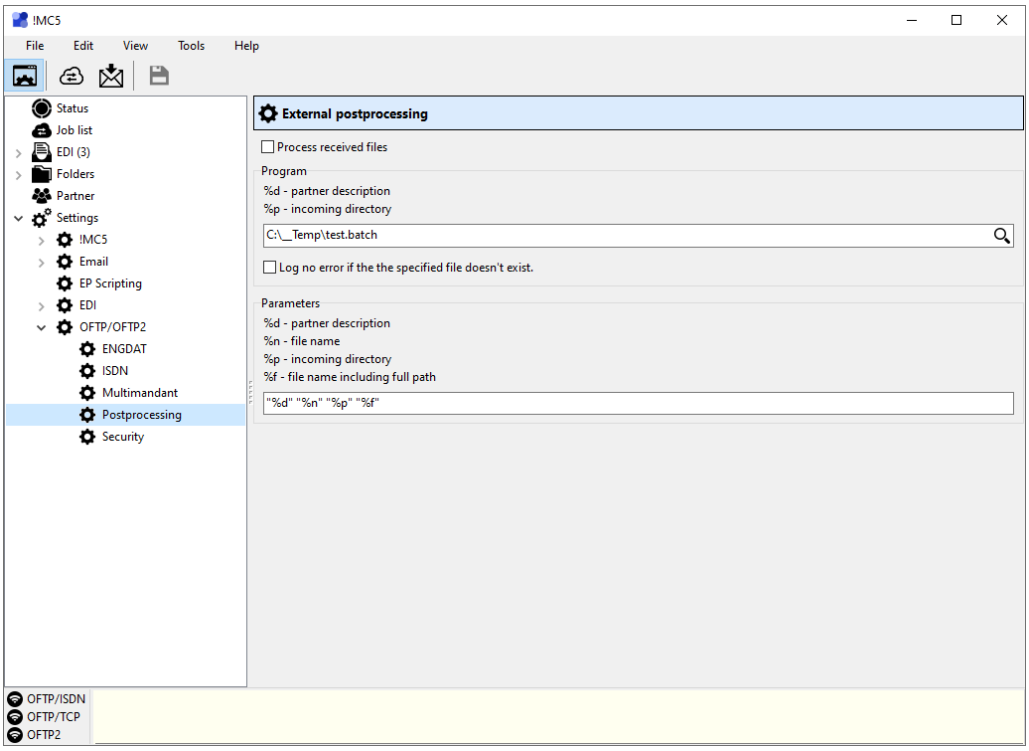
**Respond to all incoming calls (not recommended)**
**Be very careful to activate this option!** By default, !MC5 only responds to incoming calls to the ISDN number entered during setup. Activating this option will result in !MC5 responding to **all** incoming calls regardless of the destination number. This can prevent usage of any other service on the same ISDN line!

**Deactivate v42bis compression for X.75 layer 2 (not recommended)**
OFTP uses the X.75 protocol which supports v42bis compression of data. By default the usage of compression gets negotiated upon connection establishment so there is no need to deactivate this option. Some CAPI implementations don't support v42bis compression or use a incompatible implementation. Deactivating compression can fix connection errors in such cases.

### 5.3.3.3 Postprocessing

*(OFTP and OFTP2 modules only)*

Postprocessing allows the execution of external applications or scripts upon receiving of files passing certain parameters to the external program. A common way for global post-processing is using Windows Batch Scripts (files with extension *.bat*). For further reading about Windows Batch Scripting refer to the FAQ section Links.




**Process received files**
If activated the application or script stated under *Program* will get executed with the parameters stated under *Parameter*. Any place holders will get replaced by the corrsponding values of the received files.

## Program

Must contain the application or script to be executed. The following place holders can be used:

- %p = Path to the incoming directory in which the received files are saved.
- %d = Partner name as used in partner management.

**Log no error if the specified file doesn't exists.**
Before executing the post processing command !MC5 checks, if the file to be called exists. Depending on used placeholders this might not be the case. If the file doesn't exists and this option is enabled, no error will be logged. This is useful if a placeholder is used in the commands path or name and not the file doesn't exist for all partners.

## Parameter

Can contain optional parameters for the application or script. The following place holders can be used:

- %p = Path to the incoming directory in which the received files are saved.
- %d = Partner name as used in partner management.

- %n = Local file name of the received file.
- %f = Local file name of the received file including full path.

For security reasons the file name can only be used as a parameter to prevent execution of received files.

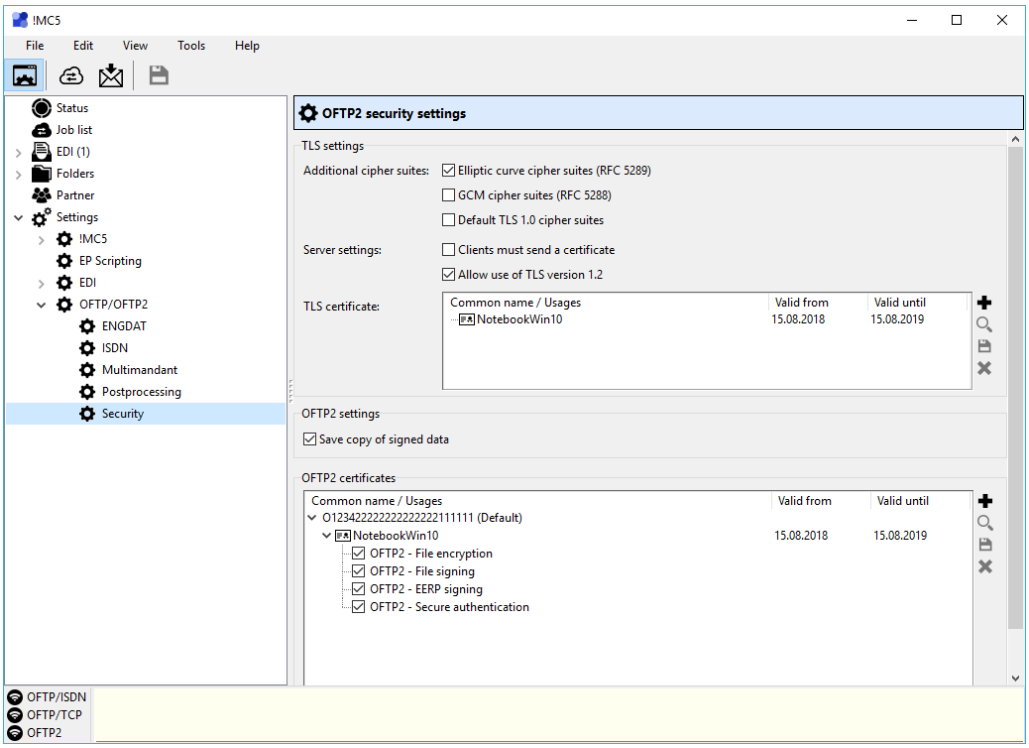
## Example

Program: *%p\cmd\processing.bat*
Parameter: *%d %f*

Upon receiving of files the batch file processing.bat, located in the sub fold cmd of the incoming directory will get called. Additionally the partner name and the file name including the full file path of the received file will be passed to the batch script, which in turn can use those parameters to e.g. copy the received file to another location, based on the partner from which it was received.

If the application/script stated under Program isn't found processing continues without any error messages.

### 5.3.3.4 Security




**OFTP2 secutiry settings with licensed add-on Multimandant**

## TLS settings

**Additional cipher suites**
Enable the use of additional cipher suites for TLS connections. Depending on the OFTP2 software your partners use, it may be necessary to enable additional cipher suites.

The following cipher suites are always used for TLS connections:

- DH_RSA_3DES_SHA1
- DH_RSA_AES128_SHA1
- DH_RSA_AES256_SHA1
- DH_RSA_AES128_SHA256
- DHE_RSA_AES128_SHA256
- DH_RSA_AES256_SHA256
- DHE_RSA_AES256_SHA256
- DHE_DSS_AES256_SHA256

Usage of the following cipher suites is optional:

***Elliptic curve cipher suites (RFC 5289)***

- ECDHE_RSA_AES128_SHA256
- ECDHE_RSA_AES256_SHA384
- ECDHE_RSA_AES128_GCM_SHA256
- ECDHE_RSA_AES256_GCM_SHA384
- ECDH_RSA_AES128_GCM_SHA256
- ECDH_RSA_AES256_GCM_SHA384

***GCM cipher suites (RFC 5288)***

- RSA_AES128_GCM_SHA256
- RSA_AES256_GCM_SHA384

- DHE_RSA_AES128_GCM_SHA256
- DHE_RSA_AES256_GCM_SHA384
- DH_RSA_AES128_GCM_SHA256
- DH_RSA_AES256_GCM_SHA384

***Default TLS 1.0 cipher suites***
- RSA_AES128_SHA256
- RSA_AES128_SHA1
- RSA_AES256_SHA1
- RSA_3DES_SHA1
- DHE_RSA_AES256_SHA1
- DHE_RSA_AES128_SHA1
- DHE_RSA_3DES_SHA1

**Clients must send a certificate**
If active !MC5 requires clients to transmit a certificate upon incoming TLS connections. Only if the transmitted certificate is present in the partner database the connection will be accepted. This option assures only known partners can connect.

**Allow use of TLS version 1.2**
This option allows incoming connections to use TLS version 1.2, if supported by both sides. When deactivated version 1.2 will not be used when negotiating the TLS version. This can be necessary as some OFTP2 softwares use faulty TLS implementations causing errors while protocol negotiation.

## OFTP2 settings

**Save copy of signed data**
If this option is activated and singed files are sent to a partner, a copy of the signed data is saved into the subfolder *Signed* in the partners outgoing directory.

## TLS/OFTP2 certificates

In order to use OFTP2 at least one certificate for *TLS authentication* has to be selected. Depending on used OFTP2 features (adjustable by partner) additional certificates or certificate usages are necessary. One certificate can be used for all usages or different certificates for different usages.

# FAQ

# 6 FAQ

## 6.1 General

### 6.1.1 Windows File Virtualization

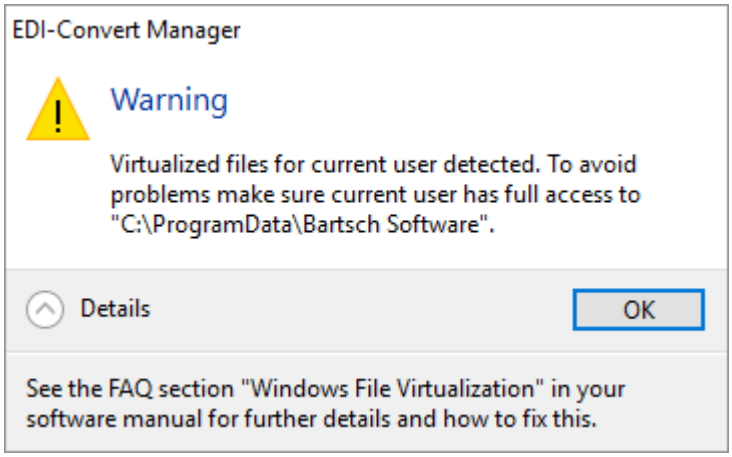
#### Windows File Virtualization

(*only applies when using Windows Vista/Server 2009 or newer*)
!MC5 stores all its data files in a subfolder inside windows' common appdata folder (typically *C:\ProgramData\Bartsch Software\MC5*). During the installation this folder is created and full access is granted for all users, to make sure all users use the same configuration, conversion files, message archives, and so on. The common appdata folder is monitored Windows' file virtualization. When a user lacking the required rights tries to write to this folder Windows File Virtualization steps in. Instead of denying access, the file get written to the users virtual store (and subsequently read from it, when accessed by the same user). As a result different users see e.g. different versions of a conversion, configuration or database file. When using !MC5 with different users (e.g. when using the add on *Windows Service*) this can cause all sorts of trouble.

Windows File Virtualization should not be deactivated and is in effect while UAC is enabled. **Disabling UAC is not recommended!** Instead make sure all (required) users have full access to !MC5s data folder. As already mentioned, file permissions are set accordingly during setup but might be changed when migrating to another machine or due to security considerations.

Also, if any files got virtualized, those have to be moved to their original destination. Be careful when doing so and **only replace those original files with their virtualized counterparts if you are sure, the virtualized one is newer!**

!MC5s default data folder is (typically) located at: *C:\ProgramData\Bartsch Software\MC5* (ProgramData is a hidden folder)
Windows Virtual Store is (typically) located at: *C:\Users\UserName\AppData\Local\VirtualStore* (AppData is a hidden folder)




When starting !MC5 the program tests if the folder *C:\Users\UserName\AppData\Local\VirtualStore\ProgramData\Bartsch Software* exists. If so, it displays a warning. To remove that warning, delete the folder (but only after applying the steps mentioned above!).

## 6.2 Modules and Addons

### 6.2.1 Windows Service

#### How can I check, if the Windows Service is running?

If the add-on Windows Service is licensed and the service is installed, the protocol analyser can be used to monitor the Windows Service status. When starting the protocol analyser the program will display an icon in the task bars system tray which refelcts the current state (see Windows Service Monitor). The Windows task manager can also be used to check, if the service is running: The processes *mc5serv.exe as well as mc5.exe* have to be running after closing the !MC5 GUI. If only the service (*mc5serv.exe*) but not !MC5 (*mc5.exe*) is running, check the protocols for error messages.

#### !MC5 seems to regularly freeze when running as service.

If files are still being received, but are processed by the EDI module only after starting the GUI, the reason for this might be the default printer fallback (see General EDI settings). Check the protocols for corresponting messages (e.g. "*Printer [...] not found. Trying to use default printer.*"). By default the service is started using the SYSTEM user account. This account might not have access to the same printers as other, "normal" users (especially network printers might not be available). If so, when printing during automatic processing !MC5 tries to use the Windows default printer instead. If the default printer is the "*Microsoft XPS Document Writer*" or "*Microsoft Print to PDF*" or any other virtual printer, that creates a file, printing will open a save dialog and the program waits for user input. Until that dialog is closed the program seems to be frozen, but the dialog might not be visible, as !MC5 is started in the background.
To fix this issue either make sure, all used printers are available under the user account, which is used to run the windows service, change the user account, which is used to run the service and/or deactivate the *default printer fallback* option.

## 6.3 Network

### 6.3.1 TCP/IP errors

#### 0 - The operation completed successfully

The error 0 isn't an actual error: The partner disconnected the TCP connection. If !MC5 displays this error in most cases the reason is one of the following two:

1. If the error occurs while establishing a connection to an OFTP2 partner most likely an error occurred on the partners side while establishing the encrypted TLS connection and the partners system disconnects without any error messages (some implementations regard any error message regarding the encrypted connection as potential security risk). The cause for this can be an invalid certificate or no common cipher suites. Validate that your own certificate is present and valid in *Settings / OFTP2 / Security*. There you can also activate the usage of additional cipher suites. For more information about the settings see Reference / Settings / OFTP / OFTP2 / Security.

2. If the error occurs after successfully connecting to the partner, e.g. after all files have been transmitted, it is highly likely your partner is using an OPFT software using a faulty OFTP protocol implementation. For a protocol conform disconnect both parties have to negotiate disconnect on OFTP level. Only afterwards the TCP connection might be disconnected. Some OFTP/OFTP2 software implementations violate the protocol and disconnect too early. !MC5 displays this as error as the software can't distinguish between an intentional disconnect and a real error.

#### 10053 - Software caused connection abort

This error occurs, if the connection get aborted within the local network, e.g. if the remote host didn't acknowledge sent TCP packets. Usually this means, network traffic gets blocked somewhere between the local computer and the remote host.
A common cause for this error are anti virus software of software firewalls. Turn off all respective software or change it's configuration so, that network traffic is allowed.
If the problem persists, the local network configuration can be the cause. Check for firewalls and their configuration in the local network and configure then so, that connections to the remote host are allowed. You can use the Windows Command Prompt to try to *ping* the remote host. If the ping fails the remote host is blocked somewhere and using *tracert* might help you find out where.