



enSuite

Parameterization and Analysis Software

Installation Instructions

**Installation and security
measures**

Disclaimer

This document contains Honeywell proprietary information.

Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Elster GmbH.

While this information is presented in good faith and believed to be accurate, Elster GmbH disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright ©2022 Elster GmbH, Steinern Straße 19-21, 55252 Mainz-Kastel, Germany.

All rights reserved.

Contact

Elster GmbH (manufacturer)

Steinern Straße 19-21

55252 Mainz-Kastel/Germany

Phone: +49 6134 605-0

Email: info@elster.com

Website: www.elster-instromet.com

Technical Support

Website: www.elster-instromet.com

Contents

1.	Considerations and first steps	4
1.1	Is an update relevant for me?	4
1.2	Current enSuite on Elster-Instromet website	4
1.3	System requirements and user rights	4
2	Install enSuite	4
3	Additional device-specific installation activities	5
3.1	Install driver for ExMFE simulator (since enSuite 4.9.2)	5
3.2	Uninstall the USB device driver from a previous enSuite installation (up to enSuite version 3.0 only)	6
3.3	LIS-200 devices – installation of the IR readout head with USB interface	7
4	Excursus: How to use data on a new computer	7
5	Remove data and uninstall enSuite	8
5.1	Remove data (<i>optional</i>)	8
5.2	Uninstall enSuite	8
6	Security information	9
6.1	Security recommendations	9
6.2	Back-up data regularly	10
6.3	Evaluate log files	10
6.4	Preventing unauthorized access to devices from the outside	12
6.5	Security for data at rest and data in transit	13
7	How to report a security vulnerability	13

1. Considerations and first steps

1.1 Is an update relevant for me?

You can use the change history of a new enSuite version to check which device releases it will be released with and whether the new functions, improvements, bug fixes and resolved security problems are relevant for you. The change history is available on the Elster-Instromet website as a PDF file in the download area.

www.elster-instromet.com/en/ensuite

1.2 Current enSuite on Elster-Instromet website

The Elster-Instromet website contains the latest software releases for enSuite and for the Elster gas device series. Download the required enSuite version from the download area to the service computer and unpack it.

www.elster-instromet.com/en/software-downloads

1.3 System requirements and user rights

The following minimum system requirements apply for installing or updating the enSuite software:

- Microsoft® Windows™ 10 (64-bit recommended) or higher
- A graphics board with a resolution of at least 1024 × 768 pixel
- Mouse
- 10 GB free space on hard disk
- 1 GB RAM



Installation instructions apply to an update in the same way

An update is internally an uninstallation and an installation of enSuite. Therefore, all installation instructions apply to the update in the same way.

For the installation (and uninstallation) of the enSuite software, we recommend administrator rights. During enSuite operation, only the rights to execute the software as well as read/write access to the user directory (e.g. C:\documents and settings\<user name>) is required.

2 Install enSuite

The enSuite ZIP file in the download area on the Elster-Instromet homepage contains all files required to install and update the enSuite software.



The screenshots shown in this section may differ depending on the software's configuration and operating system.

Perform the following steps to install enSuite:

- Before an update, first back-up the data directories of enSuite.
⇒ [6.2 Back-up data regularly](#) (p. 10)

**Back-up data before an update!**

The first time enSuite is started after an update, it automatically converts its database data. No rollback of the data is possible after the conversion! To be able to restore the status prior to the update if required, we recommend doing a backup of your data before the update.

- ▶ Download the enSuite-ZIP from the download area of the Elster-Instromet homepage:
www.elster-instromet.com/en/ensuite
- ▶ Unpack the ZIP into a directory of your choice
- ▶ In this directory switch to the subdirectory enSuite.
- ▶ Run the file enSuite_Windows[Version].exe.



The name of this file may be different depending on the software's version.

- ▶ Follow the installation wizard - no special settings are required.
- ✓ By default, enSuite starts at the end of the installation.
Alternatively, you can start enSuite via the created shortcuts.

3 Additional device-specific installation activities

3.1 Install driver for ExMFE simulator (since enSuite 4.9.2)

If you want to establish a connection between enSuite and an ExMFE simulator via a USB interface, a manual installation of the USB device driver is required, since Windows incorrectly detects the simulators as a "Serial USB device".

We recommend using the open-source tool Zadig for the USB driver installation. The tool is certified by Akeo Consulting and does not require an installation.

The following steps describe the USB driver installation with the tool Zadig – both, the generic WinUSB driver and the tool Zadig are available in the enSuite installation folder:

**Use pre-configured Zadig from the installation folder!**

Use the Zadig version from the enSuite installation folder, as this version is preconfigured with the correct device driver.

- ▶ Open the \drivers\Zadig node in the installation directory.
- ▶ Run the file zadig_[version no.].exe with administrator rights.
- ▶ You may need to confirm the **User Account Control** (UAC) dialog.
- ✓ The tool Zadig is running.

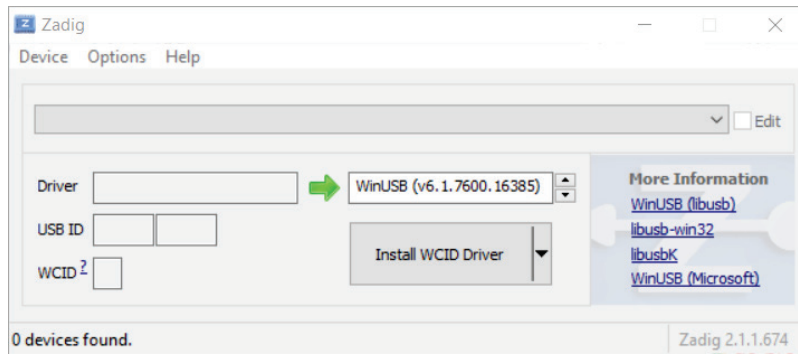


Fig. 1: Zadig after start

- ▶ From the menu select **Device – Load Preset Device**.
- ▶ Select and open the Zadig configuration file `Elster_ExMFE-Simulator.cfg`.
- ✓ The appropriate configuration for the Elster ExMFE simulator is preset.
E.g., as shown in the screenshot: the driver **WinUSB (v6.1.7600.16385)** for the USB devices with vendor ID = 1C29 and product ID for Elster ExMFE simulators = 0001 will be installed.

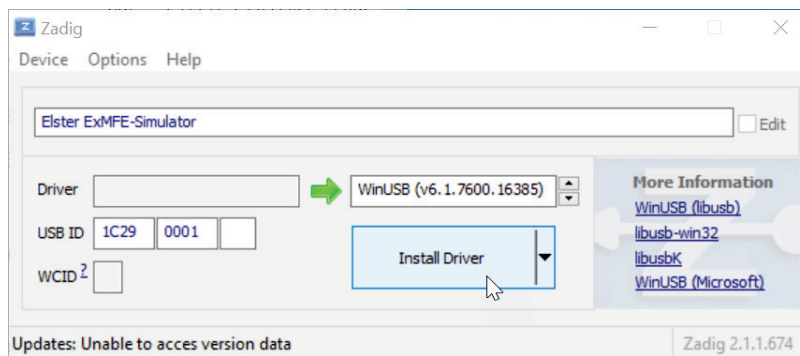


Fig. 2: Configuration for Elster ExMFE simulators

- ▶ Run the installation with **[Install Driver]** and follow the installation wizard – no special settings are required.
- ✓ The ExMFE simulator can be used with enSuite (under **Tools**).

3.2 Uninstall the USB device driver from a previous enSuite installation (up to enSuite version 3.0 only)

If you were updating enSuite and an USB driver had already been installed, uninstall the previous USB driver as soon as the enCore device is connected.

- ▶ Open the Windows Device Manager.
- ▶ Look for the Elster enCore device in the device tree – usually it is located below the node `libUsb[-win32] devices`.
Note: If no Elster driver is listed here, then no deinstallation is required.
- ▶ In the context menu select **Uninstall**.
- ▶ At the end of the deinstallation close the Windows Device Manager.
- ✓ Next time the device is connected, it will be listed below the node `Universal Serial Bus` devices in the Windows Device Manager

3.3 LIS-200 devices – installation of the IR readout head with USB interface

If the Elster IR readout head with USB interface (Elster Order No. 04 115 530) should be used under Windows to establish a connection between enSuite and a LIS-200 device (EK2x0, DL2x0), further installation and configuration activities are necessary.



The following description assumes that no installation of the Optical Readout head with USB interface has been carried out.

- ▶ Connect IR readout head with USB interface.
- ✓ The **Found New Hardware** wizard starts automatically.
If the PC can establish a connection to the Microsoft® Windows™ update server, the USB driver is installed automatically.
- ▶ If the automatic installation fails, the USB driver can alternatively be downloaded from the Elster-Instromet homepage: [Driver for Elster Opto head](#)

To be able to use the installed IR readout head, parameterize the COM port in enSuite:

- ▶ In the enSuite menu **Tools – Options** select tab **Interfaces**.
- ▶ Set the COM port for **Optical connections** according to the information in the Device Manager.

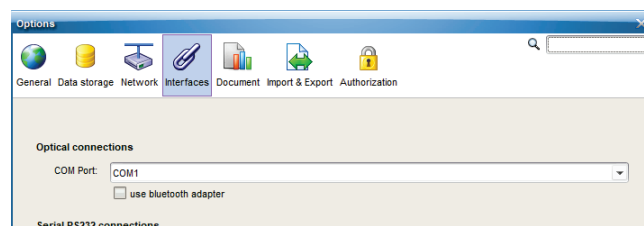


Fig. 1: Set the **COM port** for **Optical connections** in enSuite – example

4 Excursus: How to use data on a new computer

If you want to use data managed by enSuite on a new computer, proceed as follows:

- ▶ To find out where the data is stored, open the **Help – About** menu item in enSuite.
- ✓ The path to the user directory is displayed in the lower area of the info dialog:

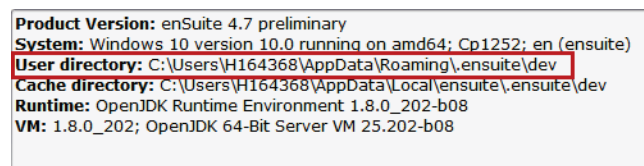


Fig. 2: Storage location of the enSuite user directory – example

- ▶ Close enSuite.
- ▶ Copy the specified directory, e.g., to a USB stick.
- ▶ Save the data in your users' directory on the new computer.
- ✓ If your user name has not changed, no further step is required. You can use the data on the new computer.

Only in case your user name has changed, set the new path in enSuite:

- ▶ Run enSuite on your new computer.
- ▶ In the enSuite menu **Tools – Options** select tab **Data storage**.
- ▶ Adapt the **Path**:

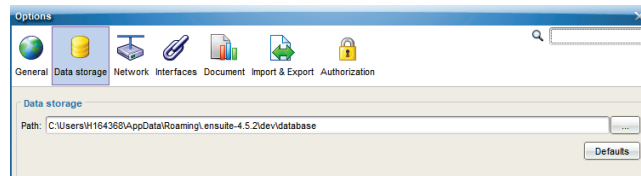


Fig. 3: Customizing the location of the user directory

- ▶ To use the adapted path restart enSuite.

5 Remove data and uninstall enSuite

5.1 Remove data (optional)

Only if you want to remove all data such as parameter settings, read out archives, log files, as they may contain sensitive data, delete the data in the user and cache directories:

- ▶ To find out the location of the data, open the menu item in enSuite **Help – About**.
- ✓ The paths to the user and cache directories are displayed in the lower area of the info dialog:

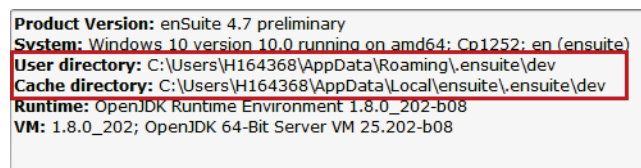


Fig. 4: Storage location of the enSuite files – example

- ▶ Close enSuite.
- ▶ Delete the specified directories.
- ✓ All permanent and temporary data are deleted.

5.2 Uninstall enSuite

Prerequisite

- You need administrator rights (if enSuite is located under Programs).
- ▶ Switch to the installation directory of enSuite, e.g.:
C:\Program Files (x86)\Elster\enSuite 4.6\
- ▶ Run `uninstall.exe` and follow the instructions in the Windows wizard.
- ✓ enSuite is removed from your computer.

6 Security information

6.1 Security recommendations



General security recommendations

- Use an antivirus program and keep it up to date.
- Activate the Windows firewall.
- Implement strict password guidelines for Windows passwords.
enSuite relies on Windows user management. Please note the following when assigning and using your password:
 - Always follow the current password guidelines when assigning passwords. Use a combination of upper and lower case letters, numbers and special characters. Protection also increases with the length of the password. A strong password consists of at least eight characters.
 - Do not share your passwords with anyone. Change your passwords regularly and whenever you suspect misuse.
- Encrypt your hard drive, e.g., with the BitLocker program from Microsoft.
- Make a backup of your user directory regularly:
C:\Users\



Encrypt data directories

enSuite stores files that may contain sensitive data in the Users directory. To protect your data from access by third parties, we recommend encrypting the directories used by enSuite:

- C:\Users\\AppData\Roaming\.enSuite,
- C:\Users\\enSuite
- additionally, when the trace function is activated:
C:\Users\\temp\

OR alternatively

- the entire users' directory:
C:\Users\

You can perform the encryption with some Windows versions using board means:

- ▶ Open the **Properties** entry in the context menu of the folder.
- ▶ On the **General** tab, click on **[Advanced]**.
- ▶ Activate the **Encrypt contents to secure data** option at the bottom of the dialog to protect data.
- ▶ Confirm with **[OK]**.



Import from and export to trusted sources only!

Ensure the following:

- Import a file into enSuite only if it comes from a trusted source.
- Provide an exported file from enSuite only to trusted sources.

6.2 Back-up data regularly

We recommend to back-up the directories in which enSuite stores its data – such as its database – on a regular basis and before every update of enSuite:

- ▶ To find out where the data is stored, open the enSuite menu item **Help – About**.
- ✓ The path to the user directory is displayed in the lower area of the **About** dialog:

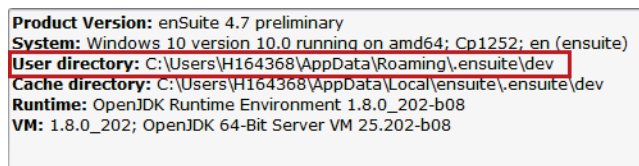


Fig. 5: Storage location of the enSuite user directory – example

- ▶ Close enSuite.
- ▶ Create a backup copy of the specified directory.

6.3 Evaluate log files

enSuite logs a large number of messages, fatal errors (exceptions) and security-relevant information in log files. enSuite stores these files in the Windows user directory:

enSuite uses different types of log files:

- 1 × security log files:

C:\Users\<user name>\enSuite\enSuite*_Security.log

Here enSuite logs permanently when an enCore device authenticates with a TLS certificate.

⇒ [Security for data in transit](#) (p. 13)

- up to 10 × log files:

C:\Users\<user name>\enSuite\enSuite*0-0.html

..

C:\Users\<user name>\enSuite\enSuite*0-9.html

Each time enSuite is started, enSuite creates a new log file. A maximum of ten log files are created, then they “rotate” so that the number does not increase excessively. The log files are overwritten one after the other (rotating log files). The file enSuite*0-0.html is the youngest, enSuite*0-9.html the oldest log file.

- Trace files (*optional*)

enSuite supports a trace function. You activate this function under **Tools – Options** on tab **Interfaces**:

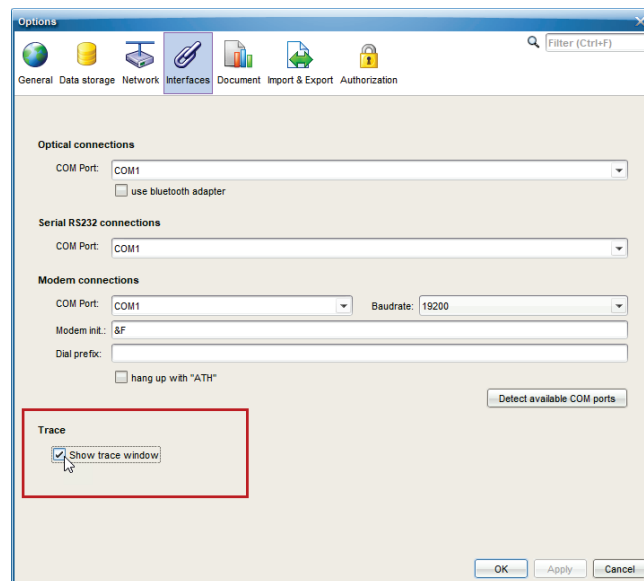


Fig. 6: Activate trace logs

As soon as you activate the function **Show trace window**, enSuite writes temporary files into the user's temp directory:

C:\Users\\temp\

The trace files can contain sensitive data. When the enSuite ends normally, the files are deleted.

6.4 Preventing unauthorized access to devices from the outside

To reduce the risk for your network, we recommend that using a firewall or other mechanisms to restrict network traffic between the “external” central billing or control system and the “internal” network of the gas metering systems.

enSuite should only be able to access a device directly within the gas measurement system where access control is guaranteed, i.e., protective measures are taken to prevent unauthorized persons from gaining physical access to the device. Direct access between enSuite and devices is established either via a USB or optical connection, depending on the device series.

We also recommend that you only allow protocols and ports that are actually used for data exchange with the external network and add them to the firewall’s whitelist, for example.

⇒ 6.5 [Security for data at rest and data in transit](#) (p. 13)

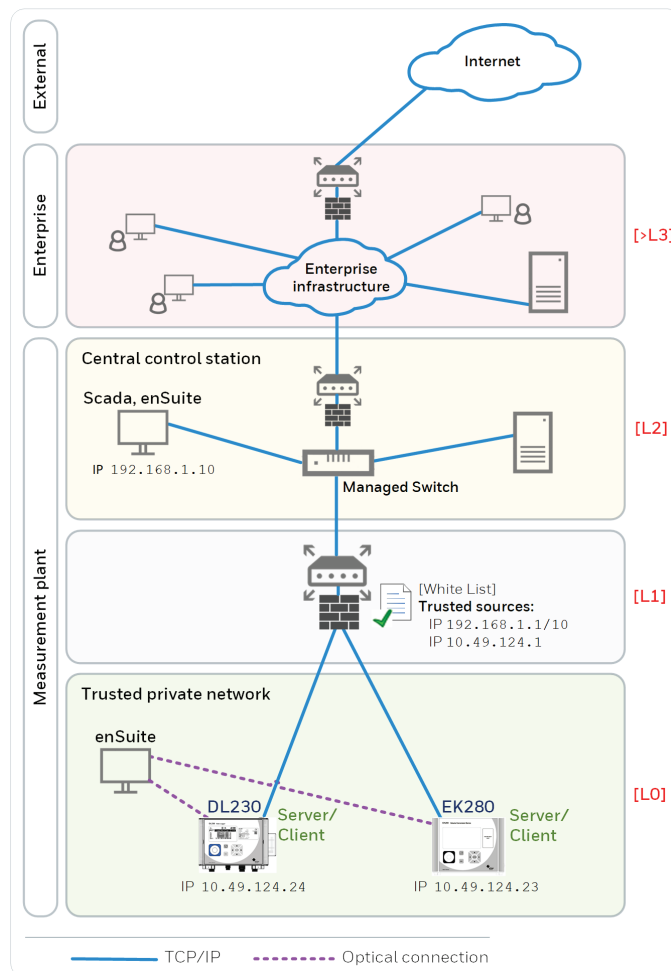


Fig. 7: enSuite should only be used within a secured metering system – using the example of the EK280 and DL230 device series with specification of safety zones L0..L4 and higher according to IEC 62443



We recommend opening safety zone L0 only for zone L1 and not for zones L2, L3 and L4.

6.5 Security for data at rest and data in transit

Security for data at rest

enSuite is the parameterization and analysis software for current Elster products in the area of flow computers, volume converters, data loggers, gas quality measuring devices and ultrasonic gas meters. The local parameterization of the devices in enSuite can also contain sensitive data. enSuite manages parameterizations unencrypted in a database in the Windows user directory.

Security for data in transit

Data in transit is the data that is transferred between an enCore device and, e.g., a control center in a public or trusted network or between enCore device and enSuite, e.g., when transferring data during parameterization of the device.

In general, protocols, such as Modbus, are managed by the devices themselves and are described in the corresponding manuals.

With enCore devices, communication between enSuite and device takes place via MMS, which is secured with TLS since enSuite 4.7 and Basic System 03–39.



Use encrypted VPN connection

We recommend using a VPN connection whenever you need a secure data connection, but no secure protocol is supported for data transmission.

In a VPN, data is transferred between two or more participants in encrypted form. For this reason, a VPN connection is recommended, for example, for mobile access to a flow computer, access to the private network or for data communication via different systems.

7 How to report a security vulnerability

A security vulnerability is defined as an error or weakness in the software that can be exploited to impair the operation or security of the parameterization or device software or to access sensitive data.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services. For details on Honeywell security policy, visit:

www.honeywell.com/product-security

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

www.honeywell.com/product-security

To view information on current malware threats please visit:

www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx

OR

Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or our technical support of Elster Gas.



“How to report a security vulnerability” in enSuite

You can find this information also in the online help in enSuite under the topic:

About enSuite – General notices – How to report a security vulnerability