Honeywell Technologies

enSuite

Parameterization and Analysis Software

Installation Instructions Parameterization and Analysis Software

ENSUITE-IA-EN u 2026-07-30

Published with enSuite V 5.2

Disclaimer

This document contains proprietary and copyrighted information of Honeywell Technologies.

The information contained herein may be used only for its intended purpose. No part of this document or its contents may be reproduced, published, or disclosed to any third party without the express permission of Elster GmbH.

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

Under no circumstances shall Elster GmbH be liable to any third party for any direct, special, incidental, or consequential damages. The information and specifications contained in this document are subject to change without notice.

Copyright © 2026 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: +49 231 937110-88+49 6134 605-0
Mail: customerfirst@honeywell.com
Website process.honeywell.com/us/en/site/elster-instromet

Technical Support:
Website: process.honeywell.com/us/en/site/elster-instromet/support

Contents

1 **Considerations and first steps** 4
1.1 What's new? 4
1.2 Download latest enSuite from Honeywell Technologies website 4
1.3 System requirements and user rights 4
2 **Installing enSuite** 6
3 **Additional device-specific installation activities** 8
3.1 Uninstalling USB device driver from a older enSuite version (only up to version 3.0) 8
3.2 LIS-200 devices – installing the infrared readout head with USB interface 8
3.3 Install gas-net support in an existing installation 9
4 **Excursus: Using data on a new computer** 10
5 **Delete enSuite data and uninstall the programm** 11
5.1 Delete data (optional) 11
5.2 Uninstalling enSuite 11
6 **Security information** 12
6.1 Security recommendations 12
6.2 Back-up data regularly 13
6.3 Evaluate log files 13
6.4 Preventing unauthorized external access 14
6.5 Security for data at rest and data in transit 16
6.5.1 Security for data at rest 16
6.5.2 Security for data in transit 16
7 **How to report a security vulnerability** 17

1 Considerations and first steps

1.1 What's new?

Details of the latest enSuite version, including new features, improvements and fixed security vulnerabilities, can be found in the change history.

The enSuite change history is available as a PDF file in the **Software Downloads** section of the Honeywell Technologies website.

process.honeywell.com/us/en/site/elster-instromet/support#software-downloads

Latest security updates only in the latest enSuite version!

To benefit from the latest cyber security measures in enSuite, always update to the latest version whenever possible.

Please note: **Security hotfixes are not (!) available for older versions!**

1.2 Download latest enSuite from Honeywell Technologies website

The Honeywell Technologies website provides the latest software releases for enSuite and the Elster Gas device series.

Download the latest enSuite version in the **Software Downloads** section and unzip it on the service PC.

process.honeywell.com/us/en/site/elster-instromet/support#software-downloads

1.3 System requirements and user rights

Minimum requirements for installation and update

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

Installation instructions also apply to updates

An update is technically equivalent to uninstalling and then reinstalling enSuite. Therefore, all installation requirements also apply to updates.

User rights

- We recommend administrator rights for installing (and uninstalling) the enSuite software.
- For operation, excecution rights for enSuite as well as read and write access to the user directory are sufficient:
  e.g., `C:\Users\<user name>`

2 Installing enSuite

The ZIP file available in the download area of the Honeywell Technologies website contains all files required to install and update the enSuite software.

> **Screenshots may differ**
>
> The illustrations shown in this manual may vary depending on the software configuration and operating system.

Steps

01 Before updating, back-up the enSuite data directories.
⇨ 6.2 Back-up data regularly (p. 13)

> **Back-up data before updating!**
>
> On first launch after an update, enSuite automatically converts its database data. Once converted, a rollback is no longer possible!
>
> To restore the previous state if required, we strongly recommend backing up your data before updating.

02 Download the latest enSuite-ZIP.
⇨ 1.2 Download latest enSuite from Honeywell Technologies website (p. 4)

03 Extract the ZIP file to a directory of your choice.

04 Navigate to the **enSuite** subdirectory within the extracted folder.

05 Launch the installer `enSuite64_[Version].exe`. The file name may vary depending on the software version.

06 Follow the instructions in the installation wizard. No special settings are required for a standard installation.

07 If you need to communicate with gas-net devices, enable the **gas-net Support** component in the **Select Components** dialog.

> **Warning: gas-net support is being discontinued**
>
> Support for gas-net is being discontinued. If you continue to use gas-net devices, the functionality remains optionally available in enSuite, but is provided without any warranty.

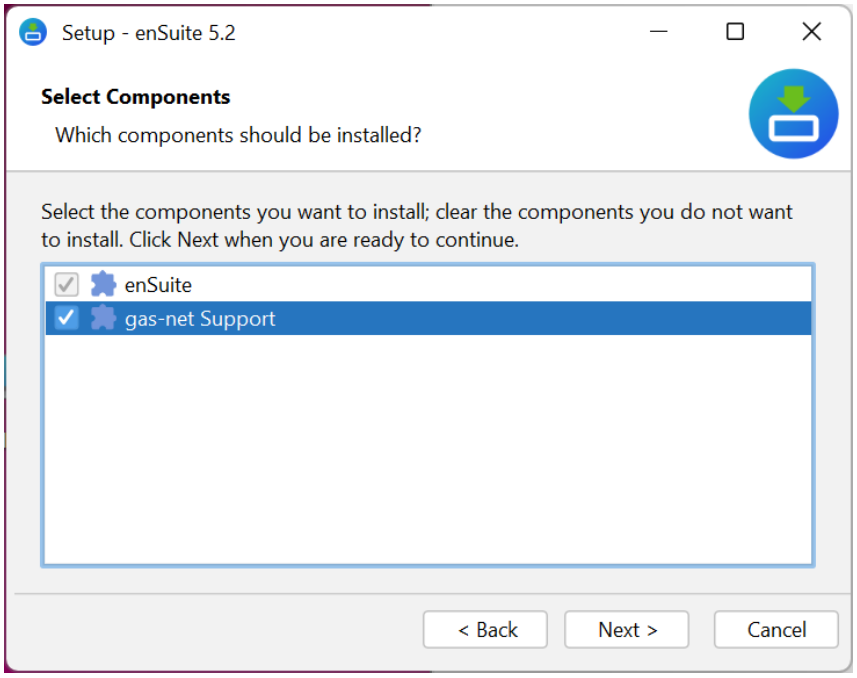


Fig. 2-1: Enable the **gas-net Support** component to communicate with gas-net devices

✓ By default, enSuite will launch automatically after installation. Alternatively, you can start enSuite using the created shortcuts.

3 Additional device-specific installation activities

Connecting to an ExMFE simulator

If you want to connect enSuite to an ExMFE simulator via a USB interface, you'll need manually install a USB device driver using an external tool.

For security reasons, we do not provide third-party tools with an enSuite release. For more information, visit:

process.honeywell.com/us/en/site/elster-instromet/support#software-downloads

3.1 Uninstalling USB device driver from a older enSuite version (only up to version 3.0)

If you are updating enSuite and a USB driver is already installed, uninstall the corresponding driver after connecting the enCore device.

01 Open the Windows **Device Manager**.

02 Locate the entry for the Elster enCore device in the device tree – typically found under the node **libUsb[-win32] devices**.
Note: If no Elster driver is listed, no deinstallation is required.

03 Right-click the device and select **Uninstall**.

04 Once the deinstallation is complete, close the **Device Manager**.

✓ The next time the device is connected, it will be listed under **USB controller** node in the **Device Manager**.

3.2 LIS-200 devices – installing the infrared readout head with USB interface

To use the Elster infrared (IR) readout head with USB interface (Elster order no. 04 115 530) to establish a connection between enSuite and a LIS-200 device (EK2x0, DL2x0), additional installation and configuration steps are required.

This procedure assumes that the optical readout head with USB interface has not yet been installed.

01 Connect the IR readout head to the PC.

✓ The **New Hardware Wizard** should start automatically.

If the PC can connect to the Microsoft® Windows™ update server, the USB driver is installed automatically.

02 If the automatic installation fails, download the USB driver manually from the Honeywell Technologies download page:
[Download driver for USB infrared optical head]

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

01 Open **Tools** – **Options** in enSuite and select the **Interfaces** tab.

02 Set the COM port for **Optical connections** according to the information displayed in the Windows **Device Manager**.

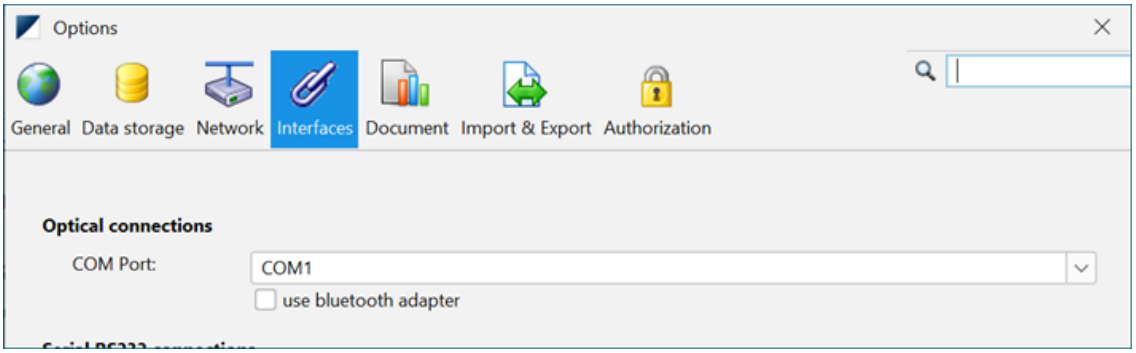


Fig. 3-1: Set the **COM port** for **Optical connections** in enSuite – example

3.3 Install gas-net support in an existing installation

Since enSuite 5.2, the **gas-net Support** component is no longer installed by default.

This section describes how to add this component to an existing enSuite installation.

01 Start the installer for the enSuite version currently in use.
⇨ 2 Installing enSuite (p. 6)

02 In the **Select Components** dialog box, enable the **gas-net Support** component.

03 Follow the remaining instructions in the installation wizard to complete the installation.

✓ The **gas-net Support** component is installed and available for communication with gas-net devices.

4 Excursus: Using data on a new computer

If you want to use data managed by enSuite on a new computer, follow these steps:

01 Open the **Help** – **About** menu item in enSuite.

✓ At the bottom of the info dialog, you'll see the path to the user directory:



Fig. 4-1: Storage location of the enSuite user directory – example

02 Exit enSuite.

03 Copy the specified user directory, e.g., to a USB stick.

04 Save the data on the new computer in the corresponding user directory.

✓ If your username on the new computer is the same, you can use the data directly – no further steps are required.

If your username has changed, adjust the new path in enSuite as follows:

01 Start enSuite on your new computer.

02 Open the menu under **Tools** – **Options** and switch to the **Data storage** tab.

03 Enter the new path to the user directory and confirm with **[OK]**.

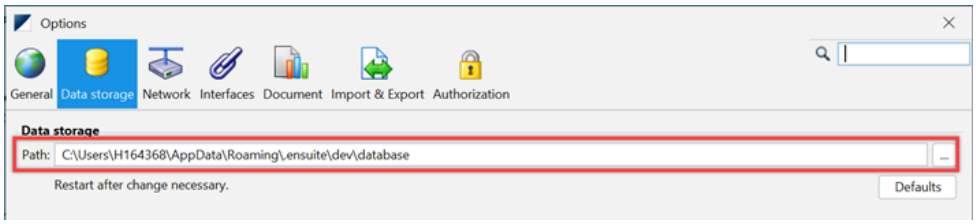
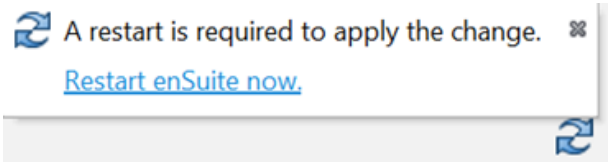


Fig. 4-2: Adjust location of the user directory – example

04 To ensure enSuite uses the updated path, restart enSuite from the bottom-right corner of the application.



5 Delete enSuite data and uninstall the programm

5.1 Delete data (*optional*)

you wish to permanently remove all user-specific data such as configurations, extracted archives, or log files – for example, for data protection reasons – please proceed as follows:

01 To identify storage locations, open the **Help** – **About** menu in enSuite.

✓ At the bottom of the dialog, you will find the paths to the user and cache directories:



Fig. 5-1: Location of the enSuite files – example

02 Exit enSuite.

03 Manually delete the specified directories usinf a file explorer.

✓ All permanent and temporary data has now been removed.

5.2 Uninstalling enSuite

Prerequisite(s)

- Administrator rights are required if enSuite was installed in the program files directory.

01 Navigate to the installation directory, e.g.,:

`C:\Program Files\Elster\enSuite[ <version>]\`

02 Run the file `uninstall.exe` and follow the instructions provided by the Windows uninstall wizard.

✓ enSuite has been completely 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\<username>`

Encrypt data storage with enSuite

The data management of enSuite includes all device parameterizations and all data read from the devices, such as archives, log data and/or reference cases, live logs or signal captures of the Q.Sonic device series.

To protect your sensitive and confidential data from unauthorized access and attackers, you can encrypt the entire enSuite data storage as of enSuite 5.0 when starting the program, if this has not already been done.

⇨ enSuite online help for more details

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:

01 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. 6-1: Storage location of the enSuite user directory – example

02 Exit enSuite.

03 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 file**

  `C:\Users\<username>\enSuite\enSuite*_Security.log`

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

  ➪ 6.5.2 Security for data in transit (p. 16)

- **up to 10 × log files**

  `C:\Users\<username>\enSuite\enSuite*0-0.html`

  ..

  `C:\Users\<username>\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**:

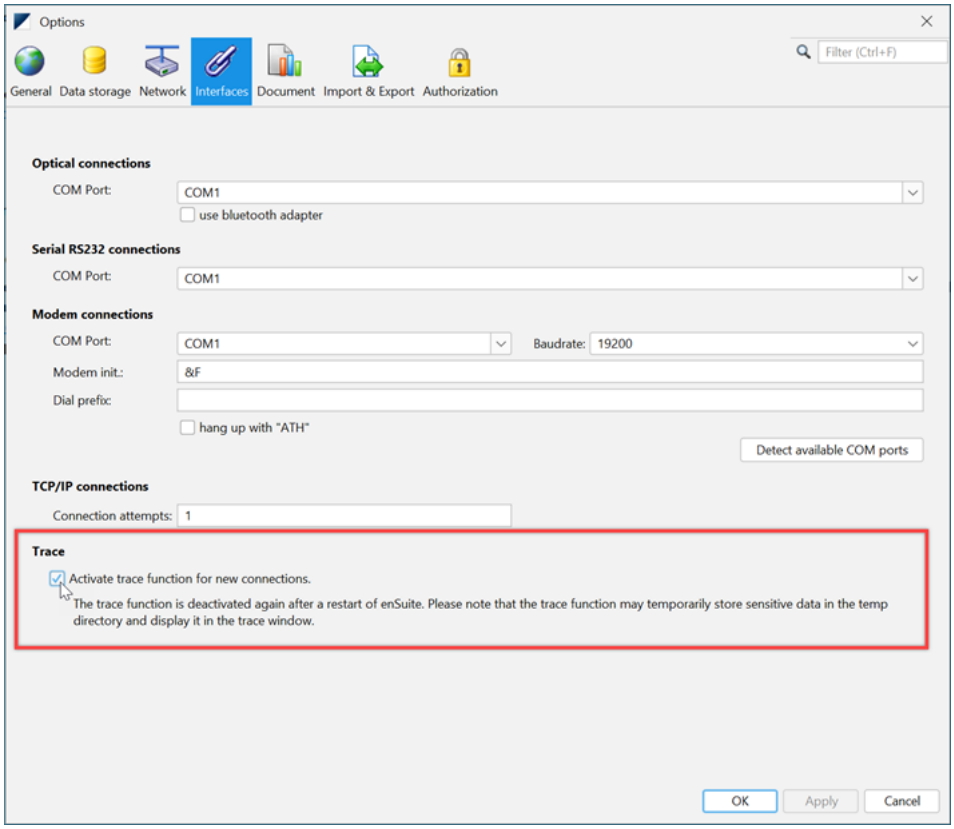


Fig. 6-2: Activate trace logs

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

`C:\Users\<username>\Temp\`

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

6.4 Preventing unauthorized external access

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. 16)

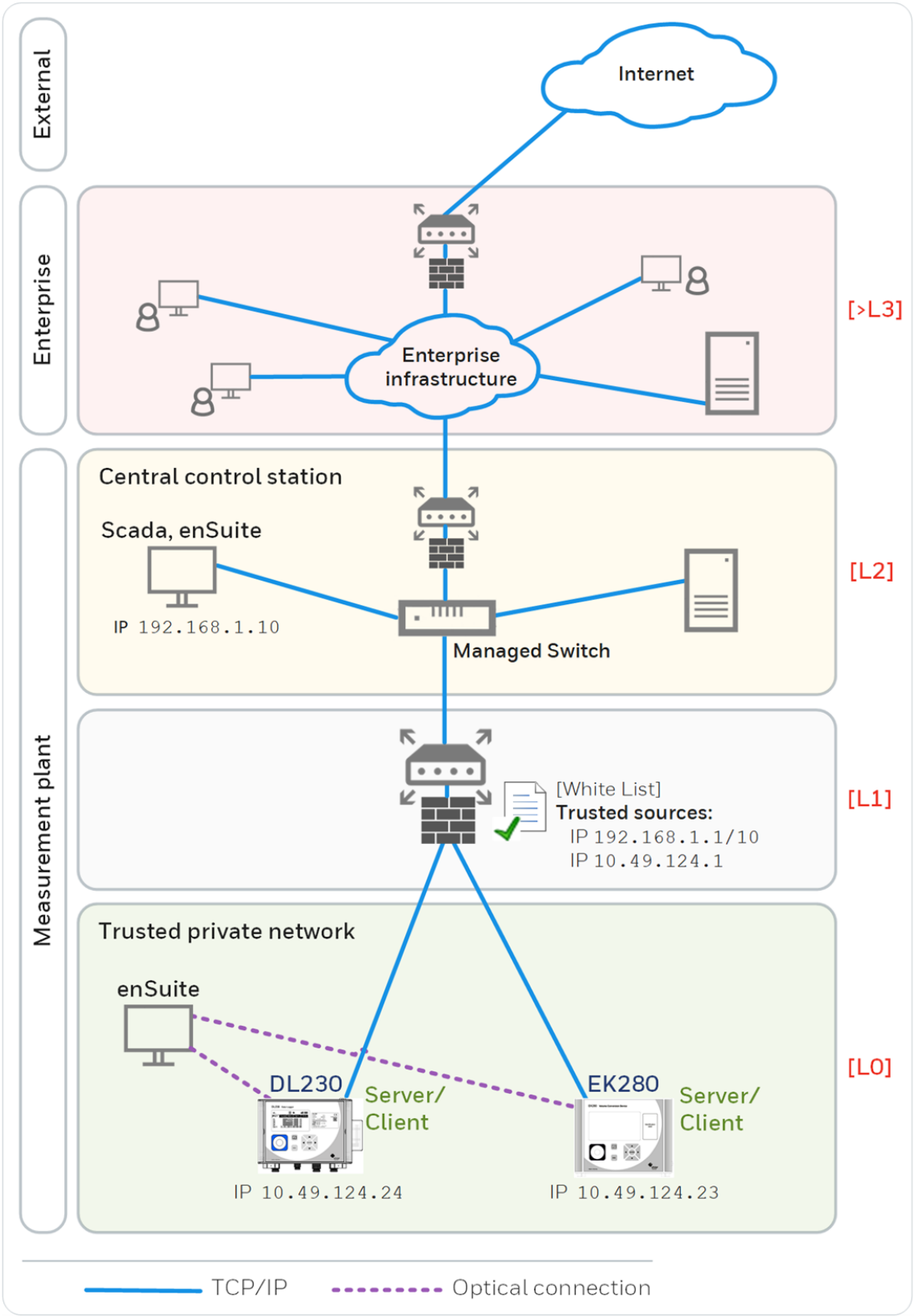


Fig. 6-3: enSuite should only be used within a secured metering system – using the example of the EK280 and DL230 device series with specification of safety zones L0 ... L4 and higher according to IEC 62443

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

6.5.1 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.

6.5.2 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.



NOTICE!

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 a defect or weakness in the software that can be exploited to compromise the operation or security of the parameterization or device software, or to gain unauthorized access to sensitive data.

Honeywell Technologies investigates all reports of security vulnerabilities affecting its products and services. For more information about the Honeywell Technologies security policy, visit:

www.honeywell.com/us/en/product-security

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

www.honeywell.com/us/en/product-security#vulnerability-reporting

To view information about current malware threats, please visit:

www.honeywell.com/us/en/news

OR

Contact your local Process Automation Customer Contact Center (CCC) or Elster Gas Technical Support.