Honeywell

Flow Computer

Device Series enCore FC

FC1, MC1

Manual
Configuring the Device with enSuite

Contact

Elster GmbH (manufacturer)

Steinern Straße 19-21

55252 Mainz-Kastel/Germany

Phone: +49 6134 605-0

Email: **customerfirst@honeywell.com**

Website: **process.honeywell.com/us/en/site/elster-instromet**

Technical Support Flow Computers and Gas Analyzers

Phone: +49 231 937110-88

Support request: **process.honeywell.com/us/en/site/elster-instromet/support**

Website: **process.honeywell.com/us/en/site/elster-instromet**

Contents

1 About these instructions

The enCore FC manual has a modular design. To get an overview of the enCore/enSuite concept, the structure of the manual, safety and risk instructions and the text labeling, refer to ⇨ the "Operating Instructions" of the enCore FC.

The present volume describes the configuration of the device software and the parameterization of the enCore Flow Computer device series (called enCore FC in the following text).

> **enSuite and the enCore FC device series**
>
> enSuite is the configuration and analysis software for Honeywell Elster devices in the field of flow computers, data loggers, gas analyzers and ultrasonic flow meters. enSuite offers tools for configuration, parameterization, diagnosis, software download as well as other service purposes, and supports all activities required for the commissioning and maintenance of these devices.
>
> This volume focuses on the enCore FC series. Under this name all enCore devices are summarized, which are used as industrial process computers for certain tasks in the gas and liquid measurement. These include, for example, the enCore MC1 signalling and monitoring unit and the enCore FC1 Flow Computer. Which functions a device supports in detail depends on its device type and is described in detail in the online help.

This volume is intended for specialist personnel who are responsible for the service activities of the following tasks after the successful assembly of the device and installation of the current enSuite version on PC:

- adaptation of device parameterization
- Software download
- other service activities

The illustrations in these instructions serve to depict the facts that are being explained, and therefore deviate depending on the configuration of device and enSuite.

> **Saving documentation on the service PC**
>
> This volume of the enCore FC manual is delivered in electronic form. We recommend saving the document on the PC intended for service activities so that it is available at all times.
>
> You can download all volumes of the enCore FC manual in PDF format from our Docuthek. The manuals are updated regularly.
>
> **www.docuthek.com**

2 Device series enCore FC

2.1 Hardware

The device types of the enCore FC series are based on the enCore platform.

The enCore FC is housed in a 19" casing and is available in two different mounting widths (1/3 mounting width or 1/2 mounting width).

The operating and display elements (touchscreen, various keys for operation, status LEDs), the USB port and the security switch are all located on the front.

The rear provides several slots for process boards. The maximum number of boards depends on the casing width (maximum of four process boards for 1/3 mounting width, and maximum seven process boards for 1/2 mounting width).

The following board types are currently available:

- ExMFE5 Ex-input board
- MFE7 input board
- MFE11 input board
- MFA8 output board
- MSER4 digital process board
- ESER4 digital process board

The configuration of the board equipment is variable. Each process board type can in principle be installed in as many board slots as you like. Restrictions only apply to MSER4 and ESER4 boards (there may be no more than either 1 MSER4 or 1 ESER4 board in board slot 4 for 1/3 mounting width, and up to 2 MSER4 and/or ESER4 boards in board slots 6 and 7 for 1/2 mounting width).

Further information on the process boards and additional serial interfaces on the CPU board can be found in the "Operating Instructions" of the enCore FC.

2.2   Software

The device software of each enCore product consists of the following:

- the Basic System that contains different basic functionalities
  (SFBs = System Function Blocks)

and

- several so-called Application Function Blocks (AFBs)

The Basic System is responsible for all basic functionalities (such as the I/O coupling or connection to digital protocol interfaces). Thus, the Basic System is a key component of the software for all enCore devices.

However, an AFB is a single application-specific functionality that can be added or removed via the parameterization. The AFB arrangement is variable; most AFBs can also be used several times.

Which AFBs are necessary for a device or which AFBs can be used as an option depends on the individual device type. The following table lists the use of AFBs for each device type, which are supported in the Basic System version 03-41-A:

AFBs	enCore FC1	enCore MC1
DSfG	✓	✓
Event Administration	(✓)	✓
Flow Conversion	✓	–
G260	–	✓
Gas Prover	(✓)	–
Gas Quality	✓	–
IEC60870	(✓)	✓
Liquid Prover	(✓)	–
Liquid Quality	(✓)	–
Liquids Flow Conversion	(✓)	–

AFBs	enCore FC1	enCore MC1
Mass Conversion	(✓)	–
Modbus	✓	✓
Postprocessing	✓	✓
Notification	✓	✓
Orifice	(✓)	–
Peer2Peer	(✓)	–
Printer	✓	(✓)
Simulation	✓	✓
Soft PLC	✓	✓
Station	✓	✓
Table Z	✓	–
User Archives	✓	✓

Table 2-1: AFBs for enCore device types (in alphabetical order)

Legend:

✓   AFB is included in the delivery status of the device software.

(✓)   AFB is not included in every configuration in the delivery status of the device software, but can be added via the software configuration of enSuite.
Optional AFBs may be subject to a charge. Extra buyable AFBs are marked with this sign in enSuite:
⇨ Please contact your local Honeywell Support team for further details.

−   AFB is not available for this type of device.

Example

- enCore FC1
  The most important AFBs for the FC1 flow computer are the Gas Quality and Flow Conversion AFBs. The main task of the Gas Quality AFB is to calculate the gas characteristics required for conversion purposes from the gas composition (in due consideration of the measurement conditions). The main task of the Flow Conversion AFB is the creation and management of various counters for volume at measurement conditions, volume at base conditions and for energy and mass.

- enCore MC1
  The main tasks of the MC1 are monitoring and control processes in the field of industrial gas measurement. It solves his special tasks with the help of AFBs. For example, one task of the G260 AFB is monitoring the compliance with the maximum concentrations of gas companion substances, as classified in the DVGW work sheet G 260 ("DVGW Arbeitsblatt 260").

3 Starting and configuring enSuite

This section requires both the assembly and installation of the enCore device as well as the installation of enSuite software on the computer to have been completed already. [1]

The basic working steps, which are always necessary when dealing with enCore devices and the associated enSuite PC software, are described here. It is therefore recommended that you read through this section in full before handling the device for the first time.

3.1 Starting enSuite; the first steps

You usually start enSuite █ under Windows via the desktop or the start menu.

The language used by enSuite can be changed via the options dialog (**Tools – Options**, tab **General**).

> 📖 **Online help**
>
> You can also activate the general online help via the menu item **Help – ❓ Show online help**. Open the context-sensitive help directly from the desired branch in the parameterization window with **[F1]**.

3.1.1 Navigation window with actions

The upper half of the navigation window is designed with a fixed data structure, just like an application-oriented file manager. The top hierarchy levels include the aforementioned levels **Devices** and **Connections**.

---

[1] ⇨ "Operating Instructions" of the enCore FC (⇨ 4.2.4 Current manuals available in Docuthek, p. 49) and ⇨ enSuite installation instructions (⇨ 4.2.3 Use compatible enSuite version, p. 49)

The view of the data structure in the navigation window can be changed; by default, you only see the currently selected branch. You can navigate to a lower level by double clicking, or a higher level by pressing the 📁 button.

The navigation window is normally located on the left-hand edge of the screen. It can be hidden so that a greater working area is available. The navigation window is then displayed once again after clicking on the 🧭 **Navigation** button on the left-hand edge of the enSuite window. If you simply move over the button using the cursor, the navigation window is temporarily displayed. You lock the navigation window with the box in the upper right corner of the window.

The lower half of the navigation window shows which actions are executable in the current context. If, for example, an unconnected device is highlighted, then only the actions **New parameterization** and **Connect** are executable. If a currently connected device is highlighted, then the entries **Disconnect** and **Readout parameterization**, along with several other actions which are only possible in the event of an active data connection, are possible here instead of **Connect**. All possible actions are also provided in the context menu on the device (right mouse click).

By clicking on one of the actions, it is then started and opened in a new editing window.

3.2   Establish connection to the enCore device

A data connection between computer and device can be established either directly via a USB cable or via TCP/IP computer network.

The communication between enCore device and enSuite is carried out via MMS and is secured via TLS since Basic System V 03-39. The enCore device uses a self-signed certificate to authenticate itself to enSuite every time an MMS connection is established. The certificate is normally created once when the enCore device is put into operation and is announced to enSuite during the first MMS connection.

3.2.1   Connect enCore device locally via USB

Prerequisite

- USB cable type A to B (included in delivery)

► Connect service PC and enCore device using the USB cable provided.
The USB interface is located at the bottom left of the front of the device
(🖳).

🖳 Since Windows 10, enSuite can communicate with the enCore device
via USB without driver installation.

> **❗ Important notice:**
> **Change the Windows USB energy saving settings for USB connections between notebooks and enCore devices**
>
> Since in particular mobile devices are designed to use as little energy as possible, communication problems can occur when data is connected between notebooks and enCore devices via USB.
> Therefore, we recommend deactivating the USB energy saving settings for battery and mains operation under Windows:
>
> ► Open the Windows **Control Panel**.
> ► Make sure that for **View** either option **Small icons** or **Large icons** is selected.
> ► Open the **Power Options**.
> ► Click on the actions **Change when the computer sleeps** – **Change advances power settings**.
> ► In dialog **Power Options** open node **USB settings** – **USB selective suspend setting** and deactivate the following settings:
>
>   - **On battery**
>   - **Plugged in**

3.2.2   Connect the enCore device via TCP/IP

Prerequisites

- Device is mounted in an accessible computer network.
- cable type according to Category 5 (Cat 5)

► Connect the service PC and enCore device with a CAT 5 cable, e.g., via a network.
The network interface is located on the rear of the device in the top right-hand corner (LAN).

3.2.3   Establish a connection to the enCore device

To establish a data connection to a service PC and one or more devices, ...

► ... select one of the following options in enSuite:

Symbol	Action	Description
	Search device (alternatively press the [F3] key)	Searches for all accessible devices and establishes the connection. All devices which were unknown up until now are entered in the enSuite database. This option is recommended for all initial connections established with one or more devices.
	Connect	Establishes the connection to a specific device. The device must be contained already in the enSuite database and selected in the navigation window under the **Devices** branch (identification via serial number).

Table 3-1: Establish a connection

✓ In both cases, a dialog to select the connection path appears once the option is activated.
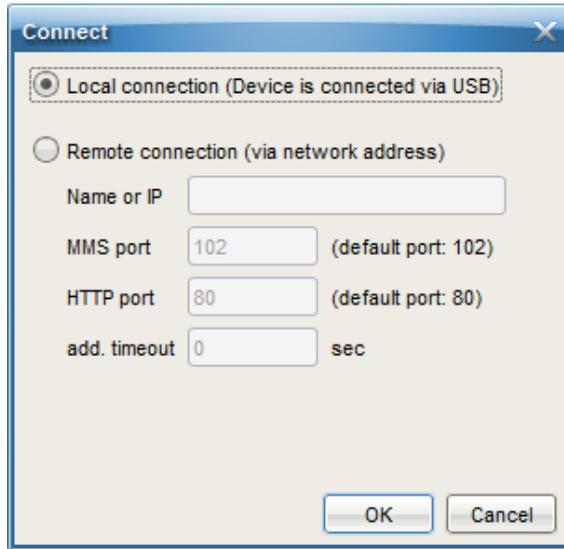

Fig. 3-1: This dialog appears with action **Connect** – example

► To establish a USB connection, select **Local connection**;
to establish a TCP-IP connection, select **Remote connection** – in this case, the network name or IP address of the enCore device is required, adjust the default ports if necessary.

► Confirm with **[OK]**.

✓ (Since Basic System V 03-39) The enCore device tries to authenticate itself with its self-signed TLS certificate.
Only in case the certificate is unknown to enSuite, enSuite will display the certificate for validation. This is the case the first time the device is connected, or the device authenticates itself with a new certificate.
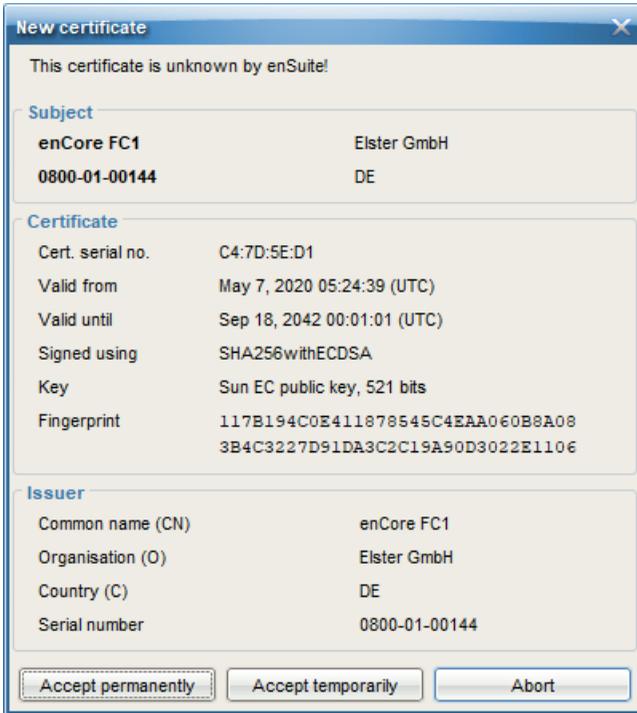
Fig. 3-2: Certificate is still unknown – example first connection establishment

► Check the validity of the certificate. You have the following options:

- Check certificate on site directly on the device:

  – Open the certificate information via the 🏠 basic display of the device:

  ℹ️ **Info – <device serial no.>**, **Certificate**

  – Compare fingerprint and subject information from enSuite and device.

- Check certificate remotely:

  Without a connection to the device, you have no way to compare the fingerprint. Therefore, ...

  – first check the information about the device in the section **Subject** of the dialog.

- – If the information is correct, the next step is to establish a temporary connection to the device.
  (⇨ next action)

► You now have the following options:

- • If you trust the certificate (for example, because the fingerprint matches), select **[Accept permanently]**.

  In this case, enSuite saves the certificate in the database. Each time a connection is established, enSuite compares the received certificate (in the background) with the saved one. As long as both certificates match, enSuite trusts this connection and establishes the connection. Only if the device's certificate changes, e.g., because a user has newly created the certificate, will enSuite display the new certificate information. You can also view the previous certificate information here.

- • If you are unsure whether you trust the connection (e.g., because you are not on-site), select **[Accept temporarily]**.

  The current MMS connection will remain, but enSuite will not save the certificate in the database. The next time a connection is established, a security query will appear again.

- • If you do not trust the certificate, select **[Cancel]**.

  In this case, the MMS connection is interrupted.

✓ As soon as the connection is established, you can readout and parameterize the device etc.

To compare the fingerprint of the certificate when accessed remotely, ...

► ... since a temporary connection exists, call the **Remote operation panel** action.

► Open the certificate information from the 🏠 basic display of the device:
  ℹ **Info – <device serial no.>**, **certificate**

► In enSuite, open the output window via **Window – Output**.

✓ Here all transferred certificates are linked with the time stamp of the transfer.

► Open the corresponding certificate with **Show certificate**.

► Compare fingerprint and subject information of enSuite and device with each other.

► If both match, you can permanently save the certificate in enSuite by reconnecting to the device and **[Permanently accept]** the certificate.

In the enSuite navigation window, all devices with serial numbers which are contained in the database are listed under the **Devices** branch.

> **Device ID**
>
> The individual devices are identified in the enSuite database via their serial numbers. In addition, it is possible to append an individual name to the serial number (highlight device, select **Properties** in the context menu and enter the name).

With respect to devices for which a connection has currently been requested but has not yet been established, the device symbol is marked under the **Devices** branch with a yellow dot ●. The device symbol is then marked with a green dot ● during the data connection.

In addition, all devices for which a connection has been established during the current enSuite session are listed under the **Connections** branch. These entries are retained until enSuite is closed, even if the respective connection is disconnected.

3.3   Disconnecting the device

There are two further options available to disconnect data connections:

Symbol	Action	Description
	Disconnect from all devices (alternatively press the [F4] key)	Terminates all active connections.

Symbol	Action	Description
![disconnect symbol]	**Disconnect**	Terminates the connection to the device which is selected in the navigation window (identification via serial number).

Table 3-2: Disconnect

3.4 Parameterization: terms

3.4.1 Product and device parameterizations

Two different types of parameterization are provided in the enSuite database:

A **Product parameterization** belongs to an enCore product class (e.g., enCore FC1) and may be used as a template when creating a parameterization for a specific device. By using **File – New** ▢, you can then create a new product parameterization.

A **Device parameterization** belongs to a specific device with a fixed serial number. A device parameterization can only be transferred to the device with the matching serial number.

A device parameterization may be obtained, for example, when reading an existing parameterization from a device (⇨ 3.4.3 Edit parameterization: sensitive data (🛡), p. 21). Alternatively, you can create a completely new device parameterization (either based on a product parameterization or without a template) for a specific device in the enSuite database after selecting the action **New parameterization** from the context menu of a selected device.

You can save a device parameterization as a product parameterization so that it is available as a template for parameterizations for other devices.

3.4.2   Offline and online parameterization

By using the term **Offline parameterization**, reference is made to parameterization in the following steps:

1. Editing or creating a device parameterization ("offline", i.e., without data connection to the device).

2. Transfer of device parameterization to the device with the matching serial number.

Online parameterization means that the content of certain parameters is changed directly during an existing data connection to the device.

The following table outlines the differences between offline and online parameterization:

Offline parameterization	Online parameterization
Editing the device parameterization without being connected to the device. The parameterization is transferred to the device in a second step.	Changing of parameter contents during an existing data connection to the device.
The options available for editing the parameterization are in principle available. Whether a parameterization can be accepted or not after installation is decided by the device whilst taking into account the access rights of the logged in user and the condition of the security switch.	It is necessary to log in to the device to start editing. Only changes that the logged in user is allowed to make are possible. In addition, the condition of the security switch is taken into account.
The edited device parameterization must be saved in the enSuite database prior to being transferred.	The saving of the edited parameterization as a device parameterization in enSuite is optional.
Changes of the AFB configuration possible.	No changes of the AFB configuration possible.

Offline parameterization	Online parameterization
In addition to changing parameter *content*, changes of the parameter *structure* are also possible (e.g., by activating functionalities or adding process boards).	Only the content of parameters which already exist may be changed.
Restart of the device necessary to activate all changes in one step.	No restart of the device necessary. Changes active instantly.

Table 3-3: Offline vs. online parameterization

3.4.3 Edit parameterization: sensitive data (🛡)

enCore parameterizations may contain sensitive data like SIM PIN, E-Mail credentials etc. To prevent unauthorized persons from gaining access to this information, since Basic System V 03-39 sensitive data is stored encrypted on the SD card and are under special protection.

> ❗ **User-defined displays show sensitive data without login!**
>
> Note that sensitive data is displayed in user-defined displays up to Basic System version 03-38 and can be viewed by third parties without authentication.

Characteristics of sensitive data

- Parameters with sensitive data are marked in enSuite with a protective shield, as shown in the screenshot **Username** and **Password** of the Notification AFB.

Reading parameterizations:

- The enCore device transfers the sensitive data of a parameterization only with a login via **<Username>** and **<Password>**.

- Special case: When logging in with the security switch open and **<Username>** (**Authorization mode**: **Security switch**), i.e., without entering a password, the sensitive data remains empty.

Changing sensitive data:

- Sensitive data can only be transferred to the enCore device after authentication with **<Username>** and **<Password>**.

- In Suite, you can only change sensitive data if the **Keep** setting checkbox is disabled. In expert mode, this setting is available in the context menu of the parameter. You can only change this setting for offline parameterizations.
  Note: In the **Keep** setting the value is used, which is already stored in the device.

- The audit trail of the device logs the change of sensitive data only with timestamp and user name. Old and new values are not documented.

Export and dispatch of parameterizations:

- In enSuite you have the option to remove the sensitive data of a parameterization before export or dispatch.

3.5   Readout parameterization

Prerequisites

- An active data connection is established to the device.

- To readout sensitive data, you need the user authorization **Change general system settings**.

How to proceed

► Highlight the device in question in the navigation window either under the **Devices** branch or under the **Connections** branch.

► Select the action **Readout parameterization** in the lower section of the navigation window.

► Make the following settings in the **Save As** dialog – the dialog varies depending on the parameterized authentication mode, login status and position of the security switch.
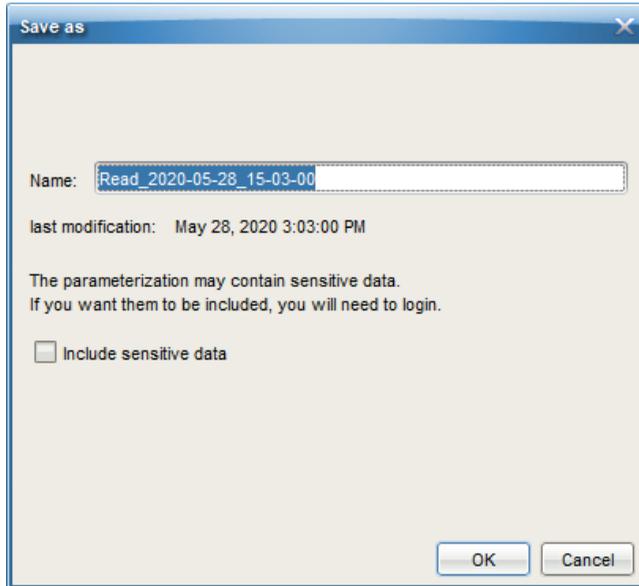

Fig. 3-3: Settings for reading out a parameterization – example

• Enter a file name in the Save as field name. The read parameterization is then stored under this name under the **Devices – <Serial Number/Name> – Parameterizations** branch.

• (Since Basic System V 03-39)
To readout a parametrization with sensitive data, select the check box **Include sensitive data**.
In the default setting (check box deactivated), sensitive data in the readout parameterization is deleted. This is useful, for example, if you want to pass on a parameterization to a third party.
⇨ 3.4.3 Edit parameterization: sensitive data (🛡) (p. 21)

► If you readout the parameterization **Including sensitive data**, authentication is required.
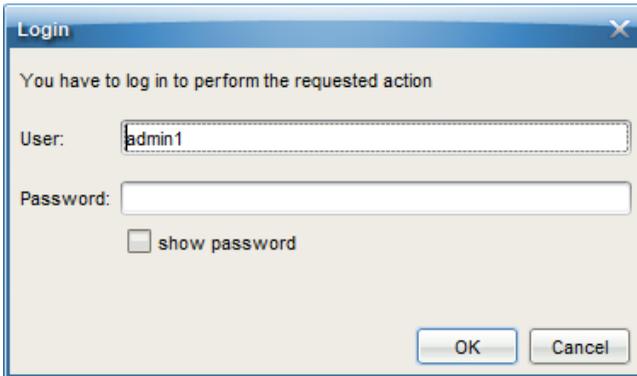
3.6   Offline Parameterization

3.6.1   Select basis of device parameterization

There are two alternatives available to create a device parameterization offline.

To change an existing device parameterization offline, ...

► ... open an existing device parameterization by double-clicking.
► Edit the device parameterization.
  ⇨ 3.6.3 AFB configuration (p. 27)
► Save the device parameterization 🖫.

> **❗ Parameterization is saved under old name**
>
> Note that the device parameterization is saved under the old name, i.e., the original file is overwritten.

OR

To create a new device parameterization offline, ...

►   ... highlight the device.
►   Select the action **New parameterization**. You can select a product
      parameterization as a template for this purpose.
►   Edit the device parameterization.
      ⇨ 3.6.3 AFB configuration (p. 27)
►   Save the device parameterization 💾 using a suitable name.
✓   enSuite opens the parameterization window to edit the device
      parameterization.

> 📖   Several parameterization windows may also be opened in
> different tabs. You can distinguish them by the tab label – the
> parameterization name is stated here (saved name or
> identification of the device for new parameterizations and
> parameterizations which have not yet been saved).

3.6.2   Select approval

For devices, which are intended to be used in legal metrology, the approval
specifies which parameters are legally relevant. The editing of such
parameters must be specifically protected or logged.

> 📖   There are two different types of access rights for legally relevant
> parameters:
>
> 🔒 Can only be changed if the sealable security switch is open.
>
> 📖 Can also be changed if the security switch is closed, provided
> the fiscal audit trail is not yet full. The change is logged in the
> fiscal audit trail.

If the device is operated in accordance with an approval, the para-
meterization needs to meet valid conditions as follows:

•   The access rights for legally relevant parameters must be set in line
      with the approval.

- The software versions of the fiscal software components must comply with the approval.

To ensure compliance with these conditions, please proceed as follows, ...

► ... select the approval to be applied in the **Configuration** tab.

✓ All parameters and parameter branches whose official access rights (i.e., 🔒 or 📖) deviate from the selected approval are now labeled in bold orange. A blue label indicates that official access rights have been newly added.

► To set the access rights of the legally relevant parameters in conformity with the selected approval, click on **[Make compliant]**.

✓ The orange labeling is replaced by a blue one as the changes have not yet been saved.

► Check the listing of AFBs in the **Configuration** tab whether an AFB is still labeled in bold orange.

✓ If this is the case, a software version was selected for this AFB that does not comply with the approval.

► Select the correct software version that complies with the approval.

> **Marking of AFB software versions**
>
> The font color with which an AFB is listed in the AFB list has the following meaning:
>
> - Font color black
>   AFB version conforms to approval.
>
> - Font color orange
>   AFB version does not conform to approval.
>
> - Font color red
>   AFB version is not compatible with the current Basic System.

► Click the **[Commit changes]**.

► Save the parameterization 💾.

✓ The blue labeling of parameters and parameter paths then disappears.

> 📖 **Approval file within the device**
>
> A special official approval file contained in the device's software determines which approval should apply for the device. It is possible to replace the approval file in the device via software configuration (⇨ 4 Software configuration/software update, p. 47).

During operation, the device checks whether the official access rights and the fiscal software component versions match the requirements of the approval file in the device. The selection in enSuite is used solely for support purposes during parameterization.

> 📖 **Approval: Check within device**
>
> On the device itself, you can see an identifying string for the approval file in the Info display, such as `FC1_NMI_2013`. If both the official access rights of the parameterization as well as the legally relevant AFBs versions are in line with the approval file, then this text is black; the text is **red** in the event of any deviations.
>
> If you activate the hyperlink Approval, a display is then evoked which contains detailed information on the approval.

Security switch and fiscal audit trail may also be used for devices that are not to be operated in accordance with an official approval. In such cases, there are prepared unofficial "approval" files `<device type>_Standard_<date>`), including a file without any official access rights whatsoever (`none`).

3.6.3   AFB configuration

In expert mode you can see the current parameter structure tree on the left-hand part of the parameterization window. The root is for the device. The first sublevel consists of AFBs that are currently included. The Basic System is always included in the device software; however, AFBs may be grouped, added or deleted.

If the tree root (i.e., the device name) is highlighted, you will see all available AFBs for the device in the **Configuration** tab. Of each AFB, both the version and the number of instances already used in the parameterization are stated there.

Generally speaking, the AFB composition can be freely configured. Restrictions result from the resources already in use. Most AFBs can be used several times.

Here's how to edit the AFB composition:

Adding an AFB

► Highlight it in the right-hand part of the window in the **Configuration** tab and click on **Add AFB**.
► Check the font color of the newly added AFB in the parameter window:

- font color **orange**
  The AFB does not conform to the approval.
  Click **[Make compliant]** again.
  ⇨ 3.6.2 Select approval (p. 25)

- font color **blue**
  The changes are compliant, but not yet saved.

Deleting an AFB

► Highlight the AFB in the parameter tree.
► In the context menu select the action **Delete AFB**.
✓ If an AFB is deleted, it may happen that the parameterization is no longer valid. In this case, all parameter folders and parameters that contain invalid references to the deleted AFB are marked in **red**.

> **Grouping of AFBs**
>
> With respect to parameterizations with many AFBs, it is re-commended that functionally related AFBs are grouped together

in the parameterization. This not only simplifies the parameteri-
zation, but it also means that the AFBs grouped in such a way are
also shifted to a separate folder in the device display.

Example

An FC1 is used for conversion purposes in a dual-stream
application. In addition to the Basic System, the device contains
one Gas quality AFB and one Flow Conversion AFB for
each stream. It is recommended that AFBs belonging to a stream
are grouped (e.g., into *Stream 1* and *Stream 2* groups).

To create an AFB group, highlight one of the associated AFBs
and enter the name of the group in the context menu under **Move
to group**.
This procedure can be repeated for all AFBs that ought to belong
to this group. AFBs with the same structure name belong to the
same group.
Alternatively, an AFB can also be dragged into an existing group
using drag-and-drop.

3.6.4 Restricting options available for editing in due consideration of access rights

In addition to the official access rights, a user authorization is also required
to change parameters. The user must log in as a member of a user group by
entering a password. An administrator can in principle make any changes,
however the conditions of the applicable approval must be taken into
account, e.g., it may be necessary to open the security switch.
⇨

In addition to the administrator groups, individual user groups which only
allow access to part of the parameters may also be set up as well. Further
information on user management can be found in the Basic System
description.
⇨ „Basic System with SFBs" of the enCore FC

Virtual login

Which parameters a user is allowed to change depends on the user group that he/she belongs to and, potentially, whether it is allowed to open the security switch or not.

For offline parameterization, enSuite offers the option to restrict the editing possibilities so that only changes can be made that an individual user is actually permitted to make. This is referred to as a **virtual login**.

Here's how to proceed:

► Highlight the parameter tree root (**<device name>**) in the parameter window.

► On the **Configuration** tab activate **Use virtual login** and enter the user name.

✓ All parameters that may not be edited by this user are no longer editable.
Parameters that cannot be edited are marked in the parameter lists with grey text and with the symbol ⊘.

► In addition, to be able to no longer edit all parameters under security switch, deactivate the check box **Assume open security switch**.

► To hide all parameters that cannot be edited, select the check box **Show enabled parameters only**.

► To manage access rights for user groups at parameter level, select the **Edit user rights** check box.

✓ At parameter level, the **Rights** column is expanded to allow you to grant or revoke access rights to user groups.

3.6.5   Edit parameterization: methods

The methods for editing the parameterization are explained in this section. The parameterization is edited in the parameterization window of enSuite.

> **Parameterization window:**
> **Navigation in AFB and parameter structure**
>
> The left-hand part of the parameterization window contains the parameter tree. The top level shows the device name; in the subordinate level, you can see the Basic System, the AFBs (possibly in groups) and node **Displays**.
>
> The tree levels can be opened by clicking on the prefix +. If the selected level contains parameters, you can view and edit these parameters on the right-hand side of the window.

In the **Parameters** tab, the parameters of the individual parameter branches are listed in table format and offered for editing.

For more complex functionalities, there is sometimes a more convenient editing dialog in a separate tab.

> You can sometimes select operating modes or add or remove functions in the **Parameters** tab as well.
>
> *Examples*
>
> - Converting the operating mode of a process board channel, e.g., for changing a digital input from "not used" to HF or LF pulse input or message input.
>
> - Adding an ultrasonic gas meter which is connected to the enCore FC via network (**Basic System – I/O – LAN: Ultrasonic gas meters**).
>
> New functions or changed operating modes require additional parameters which are then made available for editing in a new

> subordinate branch. Any such structural changes to a
> parameterization are only possible using offline parameterization.

The tabular listing of parameters in the parameter window has several columns.

The name of the parameter (**Parameter name** column) depends on the selected language.

You can see the current value of the parameter in the **Value** column; here, changes can be made.

You can distinguish between different types of parameters:

- Selection of one of several options
  Example: Selection of one of several calculation methods

- Name
  Entry of character string for identification purposes
  Example: Name of a temperature sensor, e.g., serial number

- Constant Entry of numerical constant
  Example: Constant **Qmax** as a limit value for the monitoring of gas flow

- Import value
  Assignment of an export value (result of another functionality)
  Examples:

  – Assignment of conversion factor to calculate volumes at base conditions in Flow Conversion AFB

  – Assignment of the time event 🎯 **Every hour** of the Time Service as a trigger for the formation if hourly averages in the Postprocessing AFB.

The function blocks of the enCore software provide results which can be further processed by other function blocks. These results are called **Export values**.

> **Value window – Export values**
>
> There is a value window with a tab for export values in the parameterization interface of enSuite. All export values are sorted here according to function blocks and made available in a tree. The structure here is identical to the parameter tree structure in the parameterization window.
>
> The value window is normally located on the right-hand corner of the screen. It can be hidden so that a greater working area is available. The value window is then displayed once again after clicking on the **[Values]** button on the right-hand edge of the enSuite window. If you simply move over the button using the cursor, the value window is temporarily displayed.

The export value name is derived from the tree structure.

Examples

The measurement of a pressure sensor, which is connected to the current input of the first process board, is provided by the Basic system I/O SFB. This export value is called:
Basic System.I/O.board 1.P+P-.Measured value

The export values in the value window are identified by a symbol. This symbol shows at a glance to which physical quantity the value belongs, e.g.:

Symbol	Physical quantity
	temperature
	pressure (absolute or gauge)
	volume (volume at base conditions, volume at measurement conditions)
	energy

Symbol	Physical quantity
🔥	heating value

Table 3-4: Examples of symbols of physical quantities

If a parameter is an import value, i.e., the assignment of an export value is expected, then, within the corresponding **Value** field, the symbol for the physical quantity is shown on the left-hand side and the drag-and-drop sign 🖱 on the right-hand side.

> 📖 **Parameters: Assignment of import values**
>
> The assignment of an export value to an import parameter only works if the physical quantity is matching.
>
> You can assign a value by dragging onto the parameter from the value window using drag-and-drop. A stop sign ⊘ appears if any such assignment is not possible (e.g., because the physical quantity is not matching).
>
> Alternatively, you can expand the selection list directly at the parameter value and select the desired value. However, this list contains all export values that match the physical quantity. For more complex parameterizations, the drag-and-drop method is therefore clearer. If possible, enSuite also adjusts the unit for some imports, e.g., in the `Postprocessing AFB` after the measured value inputs.

There are parameters for which either the use of a constant or an import value is possible. For certain parameters, it is also possible to select the option **Not used**, e.g., for unavailable input values or to disable a monitoring routine (by choosing **Not used** for a limit value).

In addition, there is another parameter type for which the option **Automatic** is preset or selectable. The values of such parameters are numerical constants or texts that can be automatically determined by the device. Typically, this is either information supplied by a connected measurement device via digital protocol or determined internally.

Example

A gas meter connected via encoder protocol also provides its identification data (type plate) via the digital meter protocol. These data can be transferred to the device parameterization as automatic parameters during runtime of the device. They are thus available as information for further use – for example for display on the device or for printing a data book.

📖 **Parameters: Switching the parameter type**

The possibility of switching the parameter type (import value or constant or not used) depends on the respective parameter. If several options are possible, you can open a context menu by right clicking on the parameter name. You can select the desired option here.

Alongside the **Name** and **Value** of a parameter, the associated physical unit is displayed in the **Unit** column for values that correspond to a particular physical quantity. Under normal circumstances, the default unit is used for the physical quantity in question. This is highlighted in the display with an asterisk *.

📖 **Change units**

If you click on the unit of a parameter in the **Unit** column, a list then opens in which you can select another unit if required.

The default units for specific physical quantities can also be edited. This is carried out centrally under **Basic System – Unit Service – Default units**.

You can find out more information on the Unit Service SFB in the ⇨ Online Help.

3.6.6   Edit parameterization: practical tips

This section briefly describes an appropriate order of steps for creating or editing a device parameterization for the enCore FC.

1. Configure AFB composition or grouping of AFBs
    ⇨ 3.6.3 AFB configuration (p. 27)

2. Set up process board equipment
    Specify in the **Basic System – I/O – I/O boards** parameter branch which process boards are placed in the individual board slots.

> 🛈 **Mapping process board assembly in enSuite**
>
> Ensure that the process board arrangement in the parameterization corresponds exactly to the process board configuration in the device.

3. Process boards: Parameterization of input channels
    Parameterize the measurement devices that are connected to the analog and digital channels of the input boards.
    The operating mode typically needs to be selected initially for the respective channel of the input board (under **Basic System – I/O – I/O boards – <Board name> – <Channel name>**). The associated parameters can then be edited.

4. Process boards: Define protocol channels
    Both the CPU and certain process boards provide digital protocol channels. These are intended for the connection of measurement devices via digital protocol or for communication via Modbus (in conjunction with the `Modbus AFB`).
    There are also analog input boards that support the connection of measurement devices via HART protocol as an alternative to the current input operating mode.

    Only the basic communication parameters are specified when defining a protocol channel.

5. Parameterization of intelligent measurement devices
The term "Intelligent measurement devices" refers to all measurement devices that are connected via digital protocol. Typical examples include PGCs, measurement devices via HART protocol or ultrasonic gas meters.

Intelligent measuring devices that are not connected to the enCore FC device via TCP/IP can be parameterized in the **Basic System – I/O** boards parameter branch, directly on the corresponding protocol input channel.

Measurement devices that you connect via the network and TCP/IP, are parameterized in parameter branch **Basic System – I/O – LAN: GBH measurement devices** or **LAN: Ultrasonic gas meters**.

6. Parameterization of AFBs/SFBs

    – In certain AFBs and SFBs there is an option to define **Pre-processing** operations to implement a multi-level substitute value strategy in the event of errors, either for redundant measurements and/or for fixed substitute values.
    The **Pre-processings** parameter branch is found, for example, in the `Gas quality AFB`. It is recommended here that a pre-processing operation is defined both for pressure and temperature (as well as for gas quality if this is measured).

    – Assign the desired export value to each required input value of the AFB or SFB. This export value is typically provided by another SFB or AFB. You must take care to ensure that the source of the value is correct.

    – Check or edit all options and constants. For certain constants, such usage can also be switched off via the context menu by choosing **Not used**.

    – Activate and parameterize any desired additional functions (e.g.: gas meter correction in `Flow Conversion AFB`).

> **Context-specific online help**
>
> You can activate the associated online help to find out information regarding the importance/meaning of individual functionalities and parameters. Simply highlight the parameter or parameter tree and press **[F1]**.

3.6.7   Save the edited parameterization

Once you have made all desired amendments, simply save the parameterization 💾.

> **Modified or invalid parameters are highlighted**
>
> During editing, enSuite uses color-based signs to identify the status. If the parameter label is **blue**, this means that the parameter was edited but the change has not yet been saved. Any superordinate branches are also blue at the same time.
>
> A **red** parameter label indicates that changes have been made and the parameterization is not yet valid. The parameterization can be saved, but it cannot be transferred to a device.

3.6.8   Transfer parameterization to device

Only saved device parameterizations can be transferred, and only to the device with the matching serial number.

► Establish the data connection to the device.
► Highlight the desired device parameterization in the data structure of the navigation window.
► Select the action **Transfer parameterization to device**.

► Log in to the login dialog.
(further details on user management ⇨ "Basic System with SFBs" of the enCore FC)

✓ After successful login, the transfer of the parameterization to the device starts.

▭ After successful transmission, the device restarts automatically.
OR
If the parameterization cannot be successfully transferred to the device, an error message is displayed. In this case, the device does not restart and the old parameterization is still used.

> 📖 **Parameterization with secured parameters under the protection of the security switch**
>
> A parameterization can*not* be transferred to the device if it contains changed parameters that are under the protection of the security switch and the security switch is closed, or if an attempt is made to change sensitive data with the **Authorization mode** set to **Security switch** and the security switch being open (i.e., no password required).
>
> In this case, the message **Transfer of parameterization into device failed** is displayed. The device does not restart and the old parameterization is still in use.

3.7   Online parameterization

Online parameterization means that the parameterization contained in the device is edited directly.

To change a parameterization online, ...

► ... establish the data connection to the device.
► Highlight the device in question in the navigation window either under the **Devices** branch or under the **Connections** branch.
► Select the entry **Online parameterization** in the lower section of the navigation window.

► Log in with your username and password using the login dialog that appears.

✓ The parameterization is read; the parameterization window then opens for editing purposes.

The editing methods are in principle the same as for the offline editing of a parameterization, albeit with the following restrictions:

- No changes may be made to the AFB composition.

- No changes may be made to the parameter structure.

- Only parameter changes that the logged in user is permitted to carry out may be made.

  The following applies additionally in the event the security switch is closed:

  Parameters labeled as 🔒 cannot be changed, parameters labeled as 📓 may only be changed provided the fiscal audit trail is not full. Non-editable parameters are listed in gray in the parameter lists and are labeled with the symbol 🚫.

► Activate the **Transfer parameterization to device** button 📥.

📖 **Meaning of highlighted parameters**

A parameter label highlighted in **green** indicates that the parameter was edited but the change has not yet been transferred to the device. Any superordinate branches are also **green** at the same time.

Once the transfer is completed, the parameter label is **blue**. This indicates that the transfer was completed but the edited para-meterization has not yet been saved in enSuite.

► You can save 💾 the edited parameterization in enSuite to back up the current status.

3.8 Remote access to the enCore device

The so-called remote operation panel refers to a function that enables the remote control of enCore devices with your service computer. The remote operation panel is a copy of the local operation panel and is displayed in enSuite. As soon as you open the remote operation panel, enSuite displays the virtual front of the device type. You can operate the displayed keys, actions or hyperlinks with the mouse and the virtual keyboard.

This remote access is possible via Ethernet and USB connection.

Starting with Basic System V 03-39, the implementation of the remote operation panel meets higher requirements for data security and privacy. From that version on:

- The remote operation panel uses a TLS secured MMS connection. The unsecure HTTP protocol is no longer supported, which means the remote operation panel can no longer be viewed in a browser of the service computer.

- Only one remote access is possible at the same time.

- As soon as you open the remote operation panel, the local display shows a lock screen, hiding your operation from users looking at the device. In enSuite you can grant the view or even the operation control to the local user at the device.
  This may be reasonable e.g., if our technical support from remote and you at the device shall be able to see the device's display at the same time.

- As soon as the user at the device with granted control opens the virtual keyboard for input, enSuite shows a lock screen to hide the input.
  To prevent local users from accidentally blocking the remote operation the virtual keyboard will be closed automatically after one minute without input.

- When a remote operation panel is active, the local user can cancel the remote access at any time by pressing left and right function key simultaneously.

Starting the remote operation panel in enSuite

Prerequisite

- An active data connection is established to the device.

► Select the device in the enSuite navigation window.

► Call the **Remote operation panel** action in the lower part of the navigation window.

✓ enSuite displays the remote operation panel on a tab with the following information:

Fig. 3-4: Remote operation panal tab

❶ Exit the remote operation panel by closing the tab with **×**.

❷ **<Device type>** and **<serial number>** of the connected device

❸ 2 toggle buttons:
Use the upper button to grant or revoke the view of the actual display content for the local user:

👁 Current status:
The local user sees a lock screen and the device cannot be operated locally.

Action:
You grant the view for the local user. Using the lower button, you can also grant local user operation.

👁 Current status:
The local user sees the device's display – the same what is shown on the remote operation panel.

Action:
You revoke the view for the local user, a lock screen will be displayed on the device. This also cancels granted local control. No user interaction is possible at the device.

The second toggle button grants operating control to the local user. This button is only enabled if local view is active:

⌨ Current status:
The local user cannot operate the device.

Action: Allow user interaction for the local user.

🖱 Current status:
The local user can operate the device.

Action: revoke the right to operate the device locally.

❹ Device's status bar (⇨ below)

■   On the device, the local user sees the lock screen:
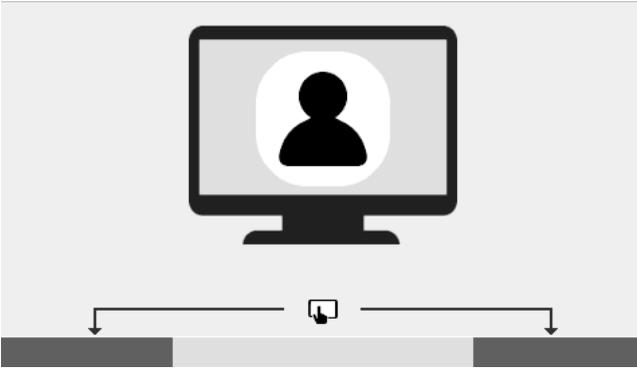
Fig. 3-5: The device displays this lock screen when remote operation is active

Information in the device's status bar – all these situations imply that the
remote operation panel is active:

(no icon)   A lock screen is displayed, hiding the actual device
            display. No operation is possible – except the
            simultaneous press of left and right function key,
            used to cancel the remote access.

👁   The local user sees the actual display content and
            can operate the device.

👁   The local user sees the actual display content, but
            the device is operated from remote.

👁   The remote user sees a lock screen because the
            local input is active and shall be hidden for the
            remote user.

ℹ   **When view is granted to the local user, remote keyboard
    entry is visible for the local user on the device's display!**

    Please note that your input via remote operation panel can be
    observed on the device's display. Please revoke view before
    entering sensitive data, e.g., your user password, with: 👁

> **Local keyboard entry is never visible on the remote operation panel**
>
> As soon as the virtual keyboard is activated on the device the remote operating panel shows this lock screen:
>
>
> Fig. 3-6: Lock screen shown on remote operation panel (enSuite) during local keyboard entry
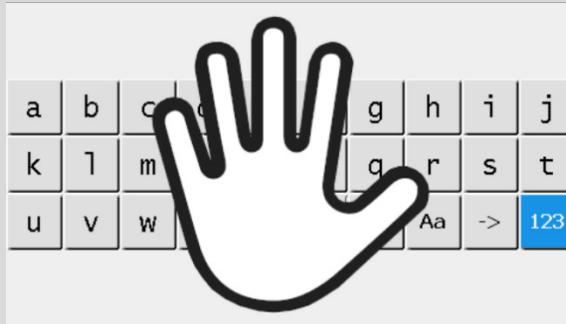
Closing the remote operation in enSuite

► You can terminate the remote operation by closing the corresponding window.

✓ The window is closed, the remote operation is terminated, and the device will accept a new remote operation connection.

> **Mechanisms that terminate the remote operation**
>
> Only one remote operation connection per device is possible at the same time. To prevent inadvertent locking of the device, e.g., for another remote operation, the device supports the following mechanisms:
>
> - The remote operation panel will be closed automatically if there was no user interaction for 5 minutes. This timeout duration is fixed and cannot be changed.

- Closing enSuite or closing the connection to the device will also close the remote operation panel.
- At the device, a local user can cancel the remote operation at any time by pressing both left and right function keys simultaneously.
  (There are arrows on the lock screen pointing to the function keys.)

4 Software configuration/software update

4.1 About this section

This section[2] describes how to update the software of enCore FC devices, the special case of bugfix software, possible requirements and steps after the update.

4.1.1 What is a software update for enCore devices?

Since the device software consists of different modules, the software update works individually for each module.[3] enSuite ensures the compatibility of the software modules.

These software modules include the Basic System (with its SFBs), all available AFBs as well as the approval file for devices in legal metrology, which defines the official access rights.

Structure of the version information for software modules

The version information for software modules is structured as follows, for example:
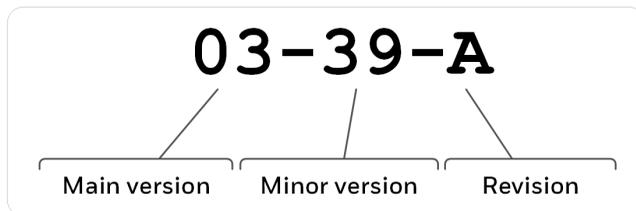
Fig. 4-1: Structure of version information – example V 03-39-A

---

[2] You can download this sections as a separate update guide from the download area of the Honeywell website. ⇨ 4.2.2 Current software on Elster-Instromet website (p. 48)

[3] In special cases, there may be a requirement to downgrade to older software modules. In this case, it is possible to exchange more recent versions for older ones.

- Main version (two-digit number)
  The main version changes only in case of major structural changes to the Basic System. It is the same for all software modules within a device.

- Minor version (two-digit number)
  The minor version is typically increased in new developments and indicates that the parameter structure has changed. It may vary between the modules.

- Revision (letter)
  The revision letter changes for small changes such as bug fixes. For AFBs, the revision is also adjusted as soon as the minor version of the Basic System is increased.

4.2 Considerations and first steps

4.2.1 Is an update relevant for me?

You can use the change history of a new software version to check whether the new functions, improvements, bug fixes and resolved security problems are relevant for your enCore device. The change history is available for software releases on the Honeywell website since 2020 as a PDF file in the download area of the respective device type.

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

4.2.2 Download current software from Honeywell website

The Honeywell website contains the latest software releases for the Elster Gas device series. Download the required enCore FC version from the download area to the service PC and unzip it.

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

4.2.3   Use compatible enSuite version

In most cases, a new enSuite version is required for a device release – only in case of a bug fix software, no new enSuite is required. The current enSuite is available in the download area of the Honeywell website.

process.honeywell.com/us/en/site/elster-instromet/support #software-downloads, section **enSuite**

Use the enSuite change history on this website to check which enSuite version is compatible with the current device version.

If necessary, download the enSuite version and update the existing installation.

4.2.4   Current manuals available in Docuthek

Elster Gas provides the latest user documentation such as manuals, certificates, data sheets, technical information for various device types in the Docuthek. The documents are updated regularly.

www.docuthek.com

Use the device type as search term, e.g., enCore FC1.

> **Check PDF after download**
>
> You can use SHA-1 checksum information to verify the file integrity of a PDF after download with an appropriate tool.
>
> The nominal value of the SHA-1 checksum for a PDF can be found in the Docuthek in the detailed information in the remarks section, or - if you download the PDF from the Honeywell website – in brackets next to the download link.

> **Which manuals are relevant for earlier device software versions?**
>
> Only the latest manuals are available in the Docuthek. If you are using an older software version, you can look up the corresponding manuals for each version since 2020 in the change history on the Honeywell website.
> ⇨ 4.2.2 Download current software from Honeywell website (p. 48)

4.2.5   Required access rights

The exchange of legally relevant and operational (i.e., not legally relevant) software modules may be restricted by special access rights and may, for example, require opening the security switch.
⇨ "Basic System with SFBs" of the FC manual

In the following use cases, a distinction is made between the use cases "legally relevant update" and "operational update" as examples and listed with the minimum required rights.

Use case 1: legally relevant update:
Update legally relevant software and approval file.

OR

Update or install selected legally relevant software modules.

Primary actor(s)

service technicians with additional qualification as metrology

expert [4]
OR
service technician plus metrology expert

Goals

−   open security switch if necessary

−   change software (operational, legally relevant)

−   change approval file

Minimal erforderliche Rechte

−   on system level:
    Update non-fiscal firmware, Update fiscal firmware, Update approval file

−   on parameter level:
    AFBs and/or individual parameters can be under the protection of the security switch

Minimum required rights

Administrator profile (*no adjustment required*)

---

[4] How an update of legally relevant software may be performed is determined by the applicable legal regulations and country-specific relevant standards and may vary from country to country.
In Germany, for example, changing legally relevant software is protected by the security switch. Here, the security switch may only be opened if either a fiscal verification officer or a test center manager is present. A service technician can also be authorized as test center manager (additional qualification).

Use case 2: operational update
Update operational software.
OR
Update or install selected operational software modules.

Main actor(s)

> service technician

Goals

> −   change software (operational)
> −   open security switch if necessary [5]

Minimum required rights

> −   on system level:
>   **Update non-fiscal firmware**
>
> −   on parameter level:
>   AFBs and/or individual parameters can be under protection of the
>   security switch

Benutzerprofile in enSuite

> **Administrator profile (*no adjustment required*)**
>
> OR
>
> **User profile 1..5:**
>   Parameterize minimum required rights

---

[5] The replacement of legally relevant and/or operational (i.e., not legally relevant) software modules may be under the protection of the security switch. These settings can be found in the parameterization in branch **Basis System – Users** on the **Special user rights** tab.

4.3 Update device software

4.3.1 Steps in a nutshell

Perform all steps one after the other, if necessary:

4.3.2 Preparations

(1) Open security switch

Background

The exchange of legally relevant and operational (i.e., not legally relevant) software modules can be under the protection of the security switch and is therefore only possible when the security switch is open.

When opening the security switch, observe the legal requirements of the respective country.

Procedure on the device

► Open the security switch.

(2) Readout archives

Background

To avoid data gaps in the archives as much as possible, readout the archives from the enCore device immediately before the update:

Procedure in enSuite

► Connect enSuite to the enCore device.
► In the lower area of the navigation window, select the action **Readout archives**.
► Save the archives under the desired name.

(3) Readout parameterization

Background

As soon as the version numbers of the software modules differ in the version number (and not only in the version letter), the current parameterization – hereinafter referred to as original parameterization – is no longer compatible after the update. In this case, readout the original parameterization from the device. It can be easily converted in enSuite and transferred to the device after the update.

Procedure in enSuite

► Connect enSuite to the enCore device again if necessary.
► In the lower area of the navigation window, select the action **Readout parameterization**.
► Save the data under the desired name.

(4) Special case: bugfix software

Background

The special thing about a bugfix software is that typically only one AFB is published. With this AFB only the revision letter is increased. No suitable enSuite is published, which means that your enSuite installation does not know the new device software. To enable the transfer of a bugfix software to the enCore device, you have to explicitly allow this installation in enSuite.

Allow installation of a bugfix software in enSuite

► Open the menu item **Extras – Options** in enSuite.

► Activate the **Allow bugfix installation** checkbox.
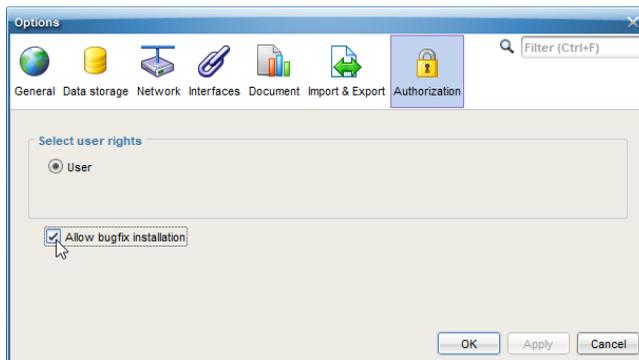
✓ As soon as you confirm the setting with **[OK]**, software modules with a revision change can be transferred to the enCore device.

4.3.3   Update software modules

> 📖 **Activate chargeable AFBs**
>
> If you want to unlock chargeable AFBs in the device, first transfer
> the resource ticket with the unlocked AFBs to the device.
>
> ⇨

Prerequisites

- Data connection to the device exists.
- Required access rights are granted, if necessary, the security
  switch is open.

► In the Navigation pane, highlight the device in either the **Devices** or the
  Connections folder.

► Select the action **Software configuration**.

✓ The **Configure software** window lists in a table (**1**) all software
  modules that are currently contained in the device with version
  information in the **Current** column.
  In addition, the column **Fiscal** informs whether a module is legally
  relevant.
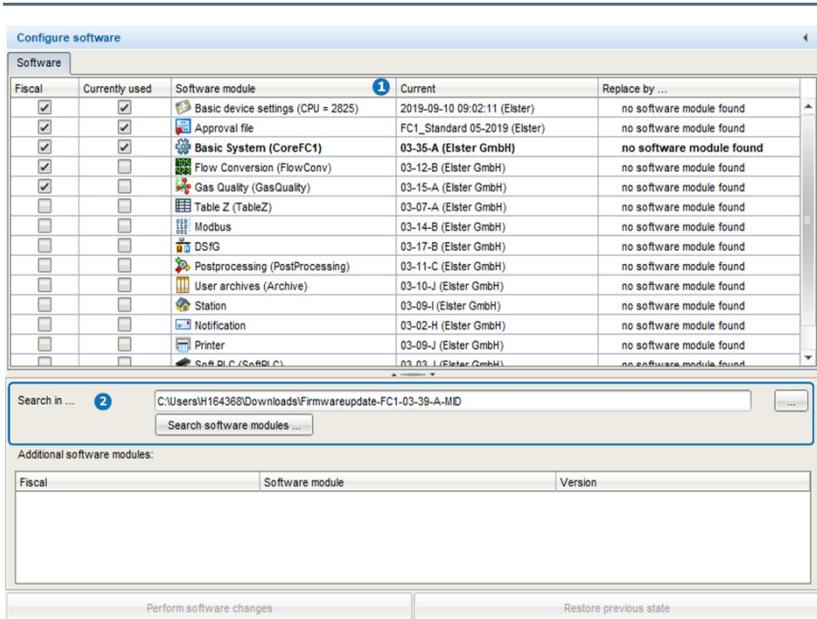
Fig. 4-2: Current software modules in the device (**1**) – example FC1 V 03-35-A

To search for the current software (**2**), …

► … under **Search in...** enter the directory with the unpacked software.

> 📖 **Activate chargeable AFBs**
>
> If you want to unlock chargeable AFBs in the device, first transfer the resource ticket with the unlocked AFBs to the device.
>
> ⇨ 4.4 Excursus: Activate chargeable AFBs in the device (p. 63)

► Click on the button **[Search software modules...]**.
✓ The specified directory is searched for other software versions:
  - In the **Replace by...** column, newer module versions are highlighted in bold and **green** and preselected for an update by default.
    The text **do not replace** is displayed if there is no newer version for a module.
  - The **Additional software modules** (**3**) show up if not in the device by default.

Fig. 4-3: Possibly newer versions in searched software – example FC1 V 03-35-A

► In columns **Replace by...** and **Version**, define one of the actions for each module:

- update **<version>**. (*default*)

- to keep a module version in the device:
  Select the entry **do not replace**.

- to delete module version in the device:
  Select the entry **remove**.

🛈 **Explicitly select approval file**

Note that approval files do not have a version but are identified by their name. If a current approval with a new approval file must be taken into account, select it explicitly.

To transfer the selected software to the device, …

► … click on the button **[Perform software changes]**.

▣ To transfer the selected software to the device:

- The process is aborted if the security switch is closed, and a change of the software configuration is prohibited in this case.

- The login dialog appears when …

  - … the security switch is open.

  - … the security switch is closed, and the action is permitted with the security switch being closed.

If the action is allowed, …

► …log in with username and password.

✓ If authentication is successful, enSuite lists the modified modules before transmission.

► To transfer the modified software to the device, confirm this dialog.

▣ After successful transmission, the device restarts automatically with an empty basic parameterization (without AFBs).

► If necessary, check on the device in the **Info – Software status** display whether the parameterization conforms to the approval file contained in the device.

   ⇨ info Approval: Check within device (p. 27)

4.3.4 Check conformity with approval (only for devices in legal metrology)

An identifying code for the approval file, such as `FC1_NMI_2013`, is shown on the device in the **Info – Software-status** display. If both, the legally relevant access rights of the parameterization and the versions of the legally relevant software modules, are conform to the approval file, this text is black, but in case of deviations the text is marked **red**.

With the hyperlink **<abbreviation of the approval file>** you will receive detailed information about the approval.

4.3.5   Check update

To ensure that the desired software modules have been transferred to the device, compare the version numbers in enSuite (**Configure software** window) with the version numbers of the device.

►   To view the version numbers of the software modules in the device, change to the home display at FC1 if necessary.

►   Open 🛈 **Info – <u>Software status</u> – <<u>Basic System or name of legally relevant AFBs</u>>**.

🖼   Here (among other things) the Basic System and the used AFBs are listed with their version number.

Info	Software status			07:57:34
1 EXAMPLES	2.0.7	📕	L4209B03	
2 MFE7	1.0.9	📄	6A251F79	
Basic System	03-35-A	📄	54C6F663	
Gas Quality	03-15-A	📕	328F0321	
Flow Conversion	03-12-B	📕	06CBE582	
Station	03-09-I		AA74484F	
Postprocessing	03-11-C		707C2479	
User archives	03-10-J		3DFF4EF0	
Modbus	03-14-B		7BD2343E	
⬅		🔒💻		🏠

Fig. 4-4: Basic System and AFBs with version number – example

4.3.6   Tasks following the update

(1) Convert original parameterization (*optional*)

Background

If the versions of the Basic System in the device and the parameterization no longer match after the software update, the original parameterization is no longer compatible with the new software but can be easily converted.

Procedure in enSuite

To make the original parameterization compatible with newer software modules, …

► … open the original parameterization that you have just readout of the device for editing.
► In the parameter window, select the root of the parameter tree with the device name.
✓ The **Configuration** tab shows the parameterizable software modules, i.e., the Basic System and all AFBs used in the parameterization with version information.
► Select the new version for the Basic System in the **Version** column. enSuite searches for the versions of the AFBs that match the Basic System and highlights them in **green**.
► Click on **[Commit changes]**.
► Check the parameterization of the changed modules for new para-meters and edit the parameterization, if necessary. It is also possible that individual AFBs are marked **red**. In this case the parameterization is invalid and must be reworked.
► Save the device parameterization and close the parameterization window.
▨ The converted device parameterization can now be transferred to the device.

(2) Transfer (converted) parameterization to the device

Optionally you can transfer a new or converted parameterization to the device.[6]

Procedure in brief

► Establish a data connection to the device with enSuite.
► Select the action **Transfer parameterization to device**.
► Authenticate yourself in the login dialog.

---

[6] ⇨ 3.6.7 Save the edited parameterization (p 38)

✓   After successful login, the transmission starts.

▫   After successful transmission, the device restarts automatically.

(3) Close security switch

Procedure on the device

►   Close and seal the security switch if necessary.

4.4 Excursus: Activate chargeable AFBs in the device

Background

Since software version 03-38, the enCore FC device series supports additional, chargeable AFBs. Fee-based AFBs are typically not included in the delivery state of the device software. As soon as you have purchased a chargeable AFB, you will receive a new resource ticket with the basic device settings for your device, in which the purchased AFBs are activated. To unlock chargeable AFBs, first transfer only the basic device settings to your device.

In enSuite chargeable AFBs are marked with this symbol 🗂️.

> 📖 **Purchase chargeable AFBs from the Honeywell Sales Team**
>
> Contact your Honeywell Sales Team to purchase a chargeable AFB. The following information is required to create a new `Basic device settings.SDM2` for your device:
>
> - customer/name
> - AFB name, such as `Notification AFB`
> - year of manufacture
> - serial number of the device (e.g. 7ELS962522xxxx)
> - device type (e.g. enCore FC1)
> - CPU serial number (4 digits)
>
> Serial number, device type and CPU serial number can be found in the **Info** display of the device.

Transferring a resource ticket to the device

► Establish a data connection to the device with enSuite.
► Call up **Software configuration** in the action menu.
► In the software configuration with **[...]** you specify the path to the current resource ticket.
► Confirm with **[Search software modules...]**.
✓ In column **Replace by...** the new basic device settings of the resource ticket are detected and the text **do not replace** is displayed.
► Select the new version of the **Basic device settings**.

Software

Fiscal	Currently used	Software module	Current	Replace by ...
☑	☑	🐾 Basic device settings (CPU = 2825)	2019-09-10 09:02:11 (Elster)	do not replace
☐	☑	📄 Approval file	FC1_Standard 05-2019 (Elster GmbH)	do not replace
☑	☑	⚙ Basic System (CoreFC1)	03-39-A (Elster GmbH)	2020-06-08 13:32:37 (DEMO)
☑	☐	🔲 Flow Conversion (FlowConv)	03-13-B (Elster GmbH)	no software module found
☑	☐	📊 Gas Quality (GasQuality)	03-15-D (Elster GmbH)	no software module found

► Transfer the new basic device settings to the device with **[Perform software changes]**.
► Follow the dialog guidance of enSuite.
🔲 After the successful transfer of the new basic device settings, the device restarts.
► (Optional) To view the list of enabled AFBs, switch to the **Info** display on the device:

Info	0800-01-00144	08:54:40

Certificate   Delete certificate

Device type   enCore FC1
CPU Serial number 2825

Access allowed for optional AFBs
   Event Administration   IEC60870

⇐   ⌂
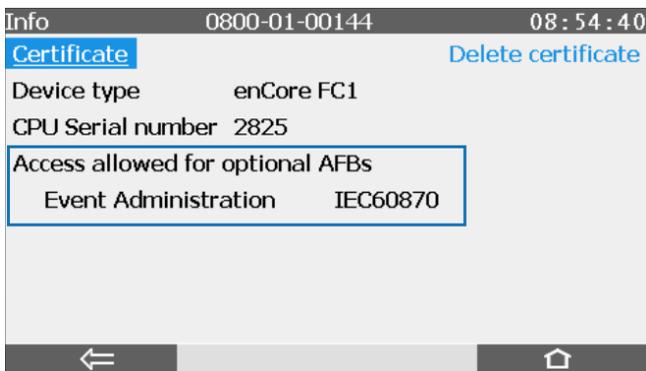
Fig. 4-5: **Info** display with enabled AFBs – example

5 FAQ

5.1 USB connection problems after waking up the notebook

Prerequisite

You use a Windows notebook to establish a USB connection between enSuite and enCore device.

Problem

As soon as the notebook wakes up from sleep mode, it may happen that Windows no longer recognizes the USB device correctly and cannot restore the USB connection between enSuite and enCore device.

Workaround

As soon as you unplug the USB connection cable from the notebook and plug it in again, the USB hardware recognition under Windows starts. As soon as Windows recognizes the USB device, you can establish a connection between enSuite and the enCore device again.

It is not necessary to restart the notebook.

6 Index