SIEMENS

SIMATIC

MultiFieldbus Configuration Tool (MFCT)

Configuration Manual

12/2025
A5E53511456-AC

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the application described in the catalog and the associated usage information. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Smart Infrastructure
Electrification & Automation
Mozartstr. 31 C
91052 Erlangen
GERMANY

A5E53511456-AC
Ⓟ 12/2025 Subject to change

Table of contents

Introduction

1

Purpose of this documentation

This documentation provides important information on the following topics:

- Description of the MultiFieldbus Configuration Tool (MFCT)
- Configuring and commissioning MultiFieldbus devices on fieldbuses, for example, EtherNet/IP and Modbus TCP.

The configuration manual supplements the description of the system manuals and equipment manuals of the MultiFieldbus devices.

Basic knowledge required

The following knowledge is required to understand the document:

- General knowledge of automation engineering
- Knowledge of the SIMATIC industrial automation system
- Knowledge of the use of Microsoft Windows computers
- Knowledge of PROFINET, EtherNet/IP, Modbus TCP

Scope of this documentation

This documentation is the basic documentation for the MFCT. The product documentation is based on the content of this Configuration Manual.

Conventions

The MultiFieldbus Configuration Tool is referred to in this documentation as MFCT.

This documentation contains illustrations of the MFCT user interface. The illustrations may differ in detail from the current version of the MFCT.

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Open Source Software

Open Source Software is used in the MFCT. The open-source software is provided free of charge. Siemens AG is liable for the product described, including the Open Source Software contained in it, pursuant to the conditions applicable to the product. Any and all liability is excluded:

- For use of the Open Source Software beyond the program sequence intended for the product by Siemens
- For defects caused by changes to the software

For legal reasons, Siemens AG is obliged to publish the original text of the license conditions and copyright notices from the third-party software contained in this product.
You can find the corresponding file with the above-mentioned information in the SiePortal in the section Information on third-party products, license conditions and OSS sources (https://support.industry.siemens.com/cs/ww/en/view/109773881).

1.1 Reference documents

The following list contains additional documentation that supplements this Configuration Manual:

Topic	Link to the documentation
MultiFieldbus topic page	MultiFieldbus - an overview of the most important documents and links (https://support.industry.siemens.com/cs/us/en/view/109779189)
MultiFieldbus Configuration Tool (MFCT) topic page	MultiFieldbus Configuration Tool (MFCT) (https://support.industry.siemens.com/cs/us/en/view/109773881)
SIMATIC MultiFieldbus	SIMATIC MultiFieldbus Function Manual (https://support.industry.siemens.com/cs/us/en/view/109773209)
Communications module DALI	Equipment manual SIMATIC ET 200SP ET 200SP communications module CM 1xDALI (https://support.industry.siemens.com/cs/us/en/view/109769428)
Technology module TM FAST	TM FAST Equipment Manual (https://support.industry.siemens.com/cs/us/en/view/109816087)
SIWAREX WP321	Operating instructions SIWAREX WP321 (https://support.industry.siemens.com/cs/us/en/view/109770838)
CM PtP module	CM PtP - Configurations for point-to-point connections Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59057093)
SIMATIC ET 200SP Distributed I/O System	SIMATIC ET 200SP System Manual (https://support.industry.siemens.com/cs/us/en/view/58649293)

Topic	Link to the documentation
SIMATIC S7-1500/ET 200MP Automation System	SIMATIC S7-1500/ET 200MP System Manual (https://support.industry.siemens.com/cs/us/en/view/59191792)
SIMATIC ET 200AL Distributed I/O System	SIMATIC ET 200AL System Manual (https://support.industry.siemens.com/cs/us/en/view/89254965)
SIMATIC ET 200clean	SIMATIC ET 200clean System Manual (https://support.industry.siemens.com/cs/ww/en/view/109822889)
SIMATIC ET 200eco PN Distributed I/O System	SIMATIC ET 200eco PN System Manual (https://support.industry.siemens.com/cs/us/en/view/109778292)
SIMATIC Bus links PN/MF Coupler	Installation and Operating Manual PN/MF Coupler (https://support.industry.siemens.com/cs/us/en/view/109781406)

Safety instructions

2

2.1 General security instructions

Read the security-related information provided in the corresponding system manual.

You can find cybersecurity-related information in the section Industrial cybersecurity (Page 10).

Industrial cybersecurity 3

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the relevant system manual of the devices used for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information for the MultiFieldbus Configuration Tool (MFCT).

3.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

3.2 Basic information on industrial cybersecurity

3.2.1 Definition of industrial cybersecurity

Industrial cybersecurity is generally understood to mean all measures to protect against the following threats:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability (e.g. due to the destruction of data or denial of service (DoS))

3.2.2 Objectives of industrial cybersecurity

The objectives of industrial cybersecurity are:

- Ensuring trouble-free operation of industrial systems and production processes
- Preventing threats to people and production from cybersecurity attacks
- Protection of industrial plants against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Provision of a practical and cost-effective concept for securing existing systems and devices without their own security functions
- Use of existing, open and proven industrial cybersecurity standards
- Compliance with legal requirements

An optimized and adapted security concept applies to automation and drive technology. The security measures must not impede or endanger production.

3.3 Operational application environment and security measures

3.3.1 Intended use

The MFCT is a PC-based Microsoft Windows software for commissioning and configuring MultiFieldbus devices (MF devices). MFCT uses PROFINET communication for this. You can find information on communication protocols and the port numbers used for Ethernet communication in the Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) function manual.

The software may be used only for the specific task in accordance with the relevant documentation, in particular its warning notices and security information.

Operational reliability and intended use

An MF device supports the following Ethernet-based protocols:

- PROFINET I/O (PN)
- EtherNet/IP (EIP)
- Modbus TCP (MTCP)

Communication between MFCT and an MF device does not cross network boundaries (e.g. to the customer network or the Internet).

Exception: If the IP forwarding option is enabled on devices within the system, data is forwarded to connected subnets or a configured router.

Area of application

You can use the MFCT to configure MF devices, e.g. for the following typical use cases:

- Mechanical engineering
- Tunnel applications
- Energy management

3.3.2 Requirements for the operational environment and security measures

Siemens recommends the following security measures:

- Threat and risk assessment (as part of security management)
- Network security concepts
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
  - Microsoft Windows access and protection mechanisms
- System protection
  - Consideration of security aspects in the selection of systems and components
  - Minimal assignment of rights for user management
- Access control concepts (utilizing access control systems)
  - Physical protection
  - Physical corporate security
  - Physical product security

Threat and risk assessment

Vulnerabilities and risks are identified, and countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) on the Industrial cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) website.

System protection

System protection depends heavily on the endangerment potential of the system operating entity and its infrastructure. The following measures provide extra protection against unauthorized access from external sources and through the network:

- Definition of security-specific guidelines and processes
- Consideration of security aspects in the selection of systems and components. This also relates to external service providers, commissioning and remote maintenance.
- Minimal assignment of rights for user management

Access control concepts

Physical protection

In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security

You can ensure the physical corporate security by taking the following measures:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security

You can ensure physical production security by taking the following measures, including:

- Separate access control for critical areas, such as production zones.
- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.
- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).
- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsecure on systems.

3.4 Security features of the MFCT

The MFCT does not require a setup program for installation. The application is downloaded as a zip file from the Internet and installed on the local drive by simply extracting the zip folder. The installation is now complete.

To check the integrity of the downloaded zip file, compare the checksum of the zip file to the checksum in SiePortal.

The "Standard user" role is sufficient for installing and using the MFCT in Microsoft Windows.

The MultiFieldbus Configuration Tool (MFCT) performs the following security checks itself:

- Checks the data integrity of the MFCT and the plug-ins
- Checks the files added by the user, e.g:
  - GSDML
  - GSDX
  - Project file

- Checks the preset security configuration
- Checks the signatures of the following file types:
  - exe file
  - dll files
  - gsdx containers

More information

You can find information on installing the MFCT in the section Installation (Page 26).

You can read how to compare the checksums in the following Internet article (https://support.industry.siemens.com/cs/ww/en/view/109483101).

3.5 Secure operation of the MFCT

This section describes measures recommended by Siemens to protect the MFCT and the connected devices against manipulation and unauthorized access.

Guidelines for secure operation

The following guidelines apply to the secure operation of the MFCT:

- Only use the original version that you have downloaded from the Internet. You can find the MFCT on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109773881).
  You can find information on installing the MFCT in the section Installation (Page 26).
- Do not mix files from different versions.
- Check regularly whether there are new versions of the MFCT available for download.
- Always use the latest version of the MFCT.
  You can find information on checking for updates in the section Update the MFCT installation (Page 27).

Dependencies on other software components

You can find the requirements for using the MFCT in the section System requirements (Page 24).

3.5.1 Security update notification

Setting up notification of security updates

To receive notifications about security updates, proceed as follows:

1. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home/).
2. Enter the keyword "Security" in the search engine.
3. Choose the "Search in Knowledge base" option.
4. Select your product or product group in the "Product tree" filter menu, e.g. "Automation technology > Automation systems > SIMATIC industrial automation systems > IO systems".
5. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".
6. Select the document with which you want to create notifications.

   If you would like to be informed about changes to the MultiFieldbus Configuration Tool (MFCT), for example, select the entry "MultiFieldbus Configuration Tool (MFCT)".
7. Select "Add to my favorites" using the 3 dots on the right.
8. In the following dialog, select the name and storage location for the favorite. Activate the "Notify me" option for notifications.
   Then click the "+ Add to my favorites" button.

Result: You will be notified by email each time the document is changed.

Under "mySiePortal > Lists & notifications > My notifications", you can display your notifications and delete them if necessary.

3.5.2 Hardening measures

System hardening, also simply referred to as hardening, is the secure configuration of products or systems. The aim is to close security gaps and take various measures to reduce the attack surfaces for cyberattacks.

To minimize the attack surface for a cyber attack, only activate required plug-ins in the MFCT.

3.5.3 Access control

To control access to your system, set up logical protection in addition to physical protection. For example, use the Microsoft Windows access and protection mechanisms.

To be able to install and use MFCT on the PC, the "Standard user" user role is sufficient in Microsoft Windows.

3.5.4 Notifications about security vulnerabilities (Siemens Security Advisories)

A vulnerability is a security vulnerability in information security. It can pose a threat as it provides intruders with the opportunity to access system resources and manipulate or steal data. Many vulnerabilities allow availability to be impaired.

Siemens ProductCERT

If Siemens identifies or fixes security gaps (Vulnerabilities) in the products, this will be published in the Security Advisories.

You can find the documents for SIMATIC on the following Siemens AG Web page: Siemens ProductCERT and Siemens CERT (https://new.siemens.com/global/en/products/services/cert.html?s=SIMATIC#SecurityPublications)

"SIMATIC" is preset in the "Search Security Advisories" search field. You can also enter other product names or other terms in the search field and search for them.

On this page, you can also find all the required information on how to deal with vulnerabilities:

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities
- Notifications are also possible in CSAF format
- Option to subscribe to RSS feeds and newsletters
- List of all current vulnerabilities and detailed information such as:
  - Description
  - Classification according to Common Vulnerability Scoring System (CVSS)
  - Measures
  - Availability
  - Etc.

Set up Security feeds (https://www.siemens.com/cert) to receive notifications about security-related topics.

If you suspect or have discovered a vulnerability in a Siemens product, please inform us immediately. To do this, press the "Contact" button on the CERT Services page (https://www.siemens.com/cert) and follow the instructions.

3.5.5 Data backup

Secure your configuration and parameter settings so that you can quickly restore this data if needed. Do not use the MFCT file folder for data backup. Otherwise, this will delete your backed-up data when you switch to a newer version.

3.5.6 Secure uninstallation

If you want to remove the MFCT from your PC, delete the folder in which the MFCT is stored. Also delete any additional files created in your folders, e.g. configuration and parameter settings.

Since only one zip file was extracted to install the MFCT, no further step is required to uninstall it.

Description

4

4.1 Area of application of the MFCT

The MFCT is a PC-based software for simple commissioning of MultiFieldbus devices on higher-level controllers within fieldbuses.

Main areas of application of the MFCT

The main area of application of the MFCT is in the following functions:

- Configuration of a MultiFieldbus device
- Bulk firmware update of ET 200 devices

Ethernet protocols supported by MultiFieldbus

The MultiFieldbus supports the following Ethernet protocols:

- PROFINET
- EtherNet/IP
- Modbus TCP

Additional plug-ins

You can also supplement the MFCT with the following plug-ins:

- DALI (Page 57)
  You use this plug-in to configure DALI devices.
- TM FAST (Page 80)
  You use this plug-in to create application update files for TM FAST modules or to load an application into a TM FAST module.
- SIWAREX (Page 85)
  You can use this plug-in to configure SIWAREX modules.
- PtP Event Trace (Page 91)
  You use this plug-in to do the following:
  - Read out event traces from a PtP module
  - Analyze serial communication
  - Display the current configuration of a PtP module

You can find more information on the plug-ins in the Plug-ins (Page 33) section.

4.2 Conditions for operating the MFCT

The following conditions should be met for the operation of the MFCT:

- **Commissioning:** The MF device must be connected via an Ethernet connection with 100 Mbps full duplex.
- **Network:** Only one instance of MFCT or PRONETA may be active per network.

  NOTE

  If PRONETA and MFCT are simultaneously active in the network, you must deactivate cyclic scanning in PRONETA.

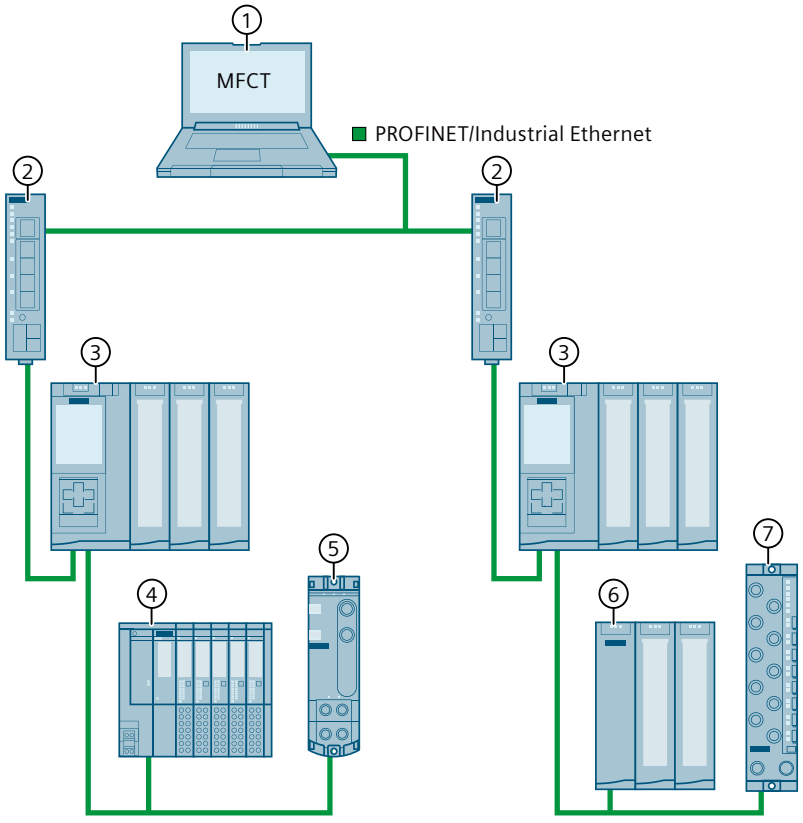
- **Fieldbus:** MFCT can only be operated on the fieldbus, not from the system network via a CPU.

4.3 Operation with multiple subnets

In the general settings of the MFCT, select which devices you would like to scan. You can find information on the individual settings in the section General settings (Page 30).

Depending on the settings selected in the MFCT, the devices must be configured accordingly in the TIA Portal. Otherwise, the MFCT cannot establish a connection to the desired devices.

The figure below shows an example of a topology with multiple subnets. The PC with installed MFCT is in a different subnet than the MF devices.



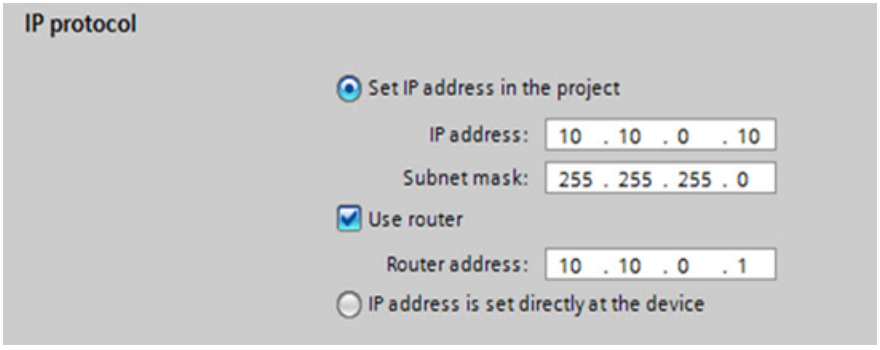
① PC with MFCT installed
② Router, e.g. SCALANCE S615
③ CPU, e.g. CPU1515-2 PN
④ MF device ET 200SP IM 155-6 MF HF
⑤ MF device ET 200AL IM 157-1 MF
⑥ MF device ET 200MP IM 155-5 MF HF
⑦ MF device ET 200eco PN

4.3.1 Recommended settings for operating the MFCT

Settings when using routers

Routers have the task of connecting IP subnets. If the MFCT is to search for MF devices in other subnets, the MFCT is first forwarded to the router. To be able to reach the devices in the other subnet, you need to enter the address of the router for each desired device.

The IP address of a device in the subnet and the IP address of the router may only be different in the places where the subnet mask contains "0".



Settings for the IPv4 forwarding configuration

If the router is connected to interface X1 of the CPU and the rest of the topology is connected to interface X2, select the "Enable IPv4 forwarding for interfaces of this PLC" check box in the TIA Portal for the CPU.

More information

You can more find information on the setting options in the TIA Portal online help, for example.

Software installation

5

In the following sections, you can find all the software information required for trouble-free operation of the MFCT.

More information

You can find more information on MFCT and the current system requirements on the Internet (https://support.industry.siemens.com/cs/us/en/view/109773881).

5.1 System requirements

5.1.1 Operating systems

To operate the MFCT, you need Microsoft Windows. Install one of the following operating systems to operate the MFCT. The installation of Microsoft .NET Framework 4.8 must be supported.

NOTE

The ability of MFCT to run on all other operating systems is not ensured. The use of any other operating system is at your own risk.

- Microsoft Windows 10 (32/64-bit)
  - Microsoft Windows 10 Home
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 (IoT) Enterprise 2016 LTSB
  - Microsoft Windows 10 (IoT) Enterprise 2019 LTSC (for IPC/PG)
  - Microsoft Windows 10 Enterprise 2021 LTSC
- Microsoft Windows 11 (32/64-bit)
  - Microsoft Windows 11 Home
  - Microsoft Windows 11 Pro
  - Microsoft Windows 11 Enterprise
- Microsoft Windows Server (32/64-bit)
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022

NOTE

Security patches from Microsoft

To ensure secure operation, make sure that the security patches from Microsoft are installed promptly.

5.1.2 Additional software components

To use the MFCT, also install the following software:

- Microsoft .NET Framework 4.8

  Use the Offline installer (https://support.microsoft.com/de-de/topic/microsoft-net-framework-4-8-offline-installer-f%C3%BCr-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0) to install it.

- The npcap-x.xx-oem.exe file from the folder "MFCT_xx.xx.xx.xx_xx.xx > Npcap > Misc"
  You can find the "Misc" folder in the unzipped folder of the MFCT.

Optional software installations:

- PG/PC Interface from the "Misc" folder
- Microsoft Visual C++ Redistributable Package (x86)

5.1.3 Security programs

To protect the software from unwanted manipulation, use the following security programs.

NOTE

Promptly perform updates available security programs.

Overview of virus scanners

The following virus scanners have been tested for compatibility with the systems:

- Trend Micro OfficeScan V12.0.6040 Service Pack 1
- Avira Security V1.1.86.3
- Trend Micro Apex One V14.0.12902

You can run these antivirus programs in the default setting.

Encryption software: BitLocker

BitLocker is a Windows security feature that protects your data by encrypting your drives. This encryption ensures that anyone attempting to access a data storage medium offline cannot read any of its contents.

5.1.4 Virtualization platforms

You have the option of operating the MFCT in a virtual machine (VM)

Use the following virtualization software:

- VMware vSphere Hypervisor ESXi ≥ 6.5
- VMware Workstation ≥ 15.5.0
- VMware Workstation Player ≥ 15.5.0
- Microsoft Hyper-V Server ≥ 2016

NOTE

Hardware certified by the manufacturer is recommended for the use of the following virtualization software:

- VMware vSphere Hypervisor ESXi
- Microsoft Hyper-V Server

Guest operating systems for virtualization software

Use the following guest operating systems within the selected virtualization software:

- Microsoft Windows 10 Pro (32/64-bit)
- Microsoft Windows 11 Pro (32/64-bit)

There could be restrictions with the online functions.

NOTE

The plant operator must ensure that sufficient system resources are provided for the guest operating systems.

5.2 Installation

The MFCT is provided as a portable application. To install the MFCT, proceed as follows:

1. Download (https://support.industry.siemens.com/cs/us/en/view/109773881) the MFCT as a zip file from the Internet.
2. To check the integrity of the downloaded zip file, compare the checksum of the zip file to the checksum in SiePortal.

   You can find instructions for comparing the checksums in the following FAQ on the online support page (https://support.industry.siemens.com/cs/ww/en/view/109483101).
3. If both checksums match, extract the downloaded zip file to a local drive on your PC.

Result: You have completed the installation. The MFCT is installed on your PC. Start the MFCT by double-clicking the "MFCT.exe" file in the extracted folder.

5.3 Update the MFCT installation

Always use the latest version of the MFCT.

To check whether a new version is available, proceed as follows:

1. Open the MFCT.
2. Open the "About" tab.
   You can find information about the installed version in the "Version information" area.
3. Click the "Check for updates" button.
   The MFCT checks whether a new version is available in SiePortal.

Result: You are notified if a new version is available. Otherwise, the MFCT indicates below the release date that your installation is up-to-date.

Optionally, you can select the "Check on startup" check box to have the MCFT automatically check for updates on each startup of the application.

More information

You can find more information on the "About" tab in the section Information on the "About" tab (Page 28).

Functions

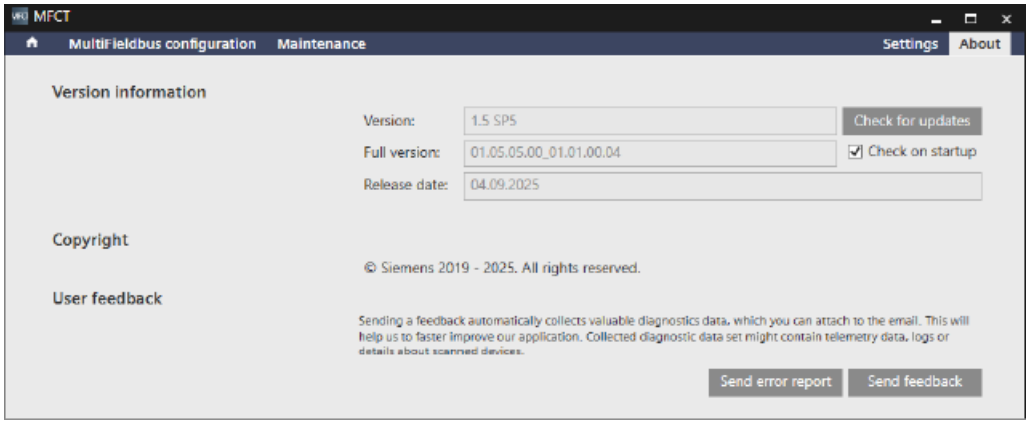
6

6.1 Information on the "About" tab

After opening the MFCT, you can find the "About" tab on the right. You can find the following information there:

- Version information
- Copyright
- User feedback

The figure below shows the contents of the "About" tab.



More information

You can learn more about version information and updates in section Update the MFCT installation (Page 27).

6.1.1 Version information

To obtain information about your installed version of the MFCT, click the "About" tab. The "Version information" area shows the following

- Version
- Full version
- Release date
- Check for updates

  You can find information on checking for updates in the section Update the MFCT installation (Page 27).

NOTE

Version of the MFCT required for operation

To ensure problem-free operation of the MFCT with an MF device, the MFCT requires at least the version required by the MF device. You can find this version in the equipment manual of the MF device used.

6.1.2 User feedback

To send error reports and feedback, click the "About" tab. The "User feedback" area offers the following options:

- Send error report:
  You can send information on collected diagnostic data.
- Send feedback:
  You can make suggestions and proposals for using the tool.

Sending an error report

To send an error report with information on collected diagnostic data, proceed as follows:

1. Select the "About" tab.
2. Click the "Send error report" button in the "User feedback" area.
   The MFCT collects diagnostic data and stores it in the MFCT installation folder under "Logs".
   The MFCT also opens a new email. The corresponding recipient is already specified in this email and the collected diagnostic data is attached as a zip file.
3. Enter additional information on the error description in the email.
4. Send the email.

Sending feedback

To make suggestions and proposals for handling the tool, proceed as follows:

1. Select the "About" tab.
2. Click the "Send feedback" button in the "User feedback" area.
   The MFCT opens a new email. The corresponding recipient is already specified in this email.
3. Enter your suggestions and proposals in the email.
4. Send the email.

6.2 Overview of the "Settings"

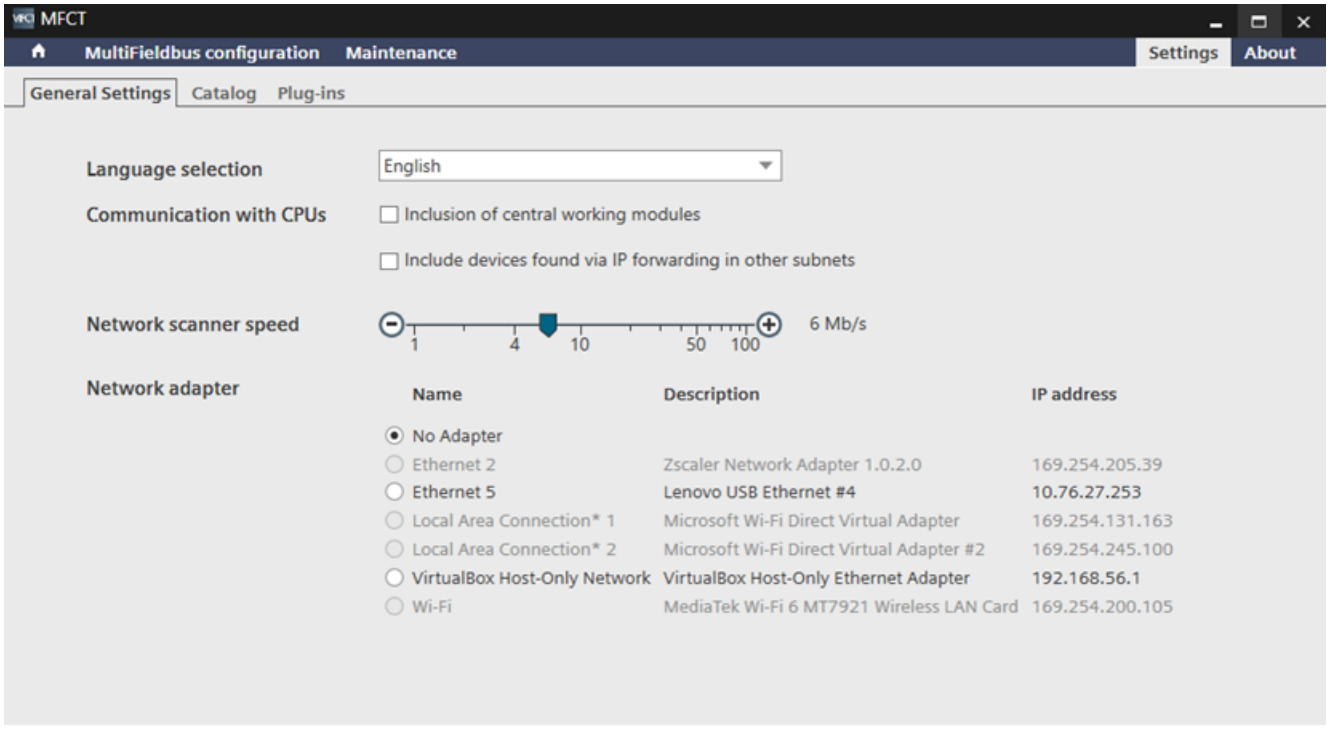
After opening the MFCT, you can find the "Settings" on the start page as an application. In an opened MFCT application, you can find the "Settings" on the right as a separate tab next to the "About" tab.

In the "Settings" tab, you have the option of configuring the basic settings of the MFCT in the following areas:

- General settings (Page 30)
- Catalog (Page 32)
- Plug-ins (Page 33)

6.2.1 General settings

The following figure shows the configuration options in the "General settings" tab:



Language selection

In the "Language selection" area, select the desired language for the user interface from the selection list. The currently supported languages are German and English.

Communication with CPUs

In the "Communication with CPUs" area, select the range in which the network scan should detect modules.

- "Inclusion of centrally working modules" check box:
  The network scan detects centrally plugged modules on a CPU.
- "Include devices found via IP forwarding in other subnets" check box:
  The network scan also detects devices in other subnets.

Network scanner speed

In the "Network scanner speed" area, select the speed at which the network is scanned.

The default setting is 6 Mbps. The highest speed that can be set is 100 Mbps.

In networks with high network load, reduce the speed of the network scanner, for example, before a firmware update. A firmware update of more than 20 devices results in a network load of approx. 3 Mbps.

Network adapter

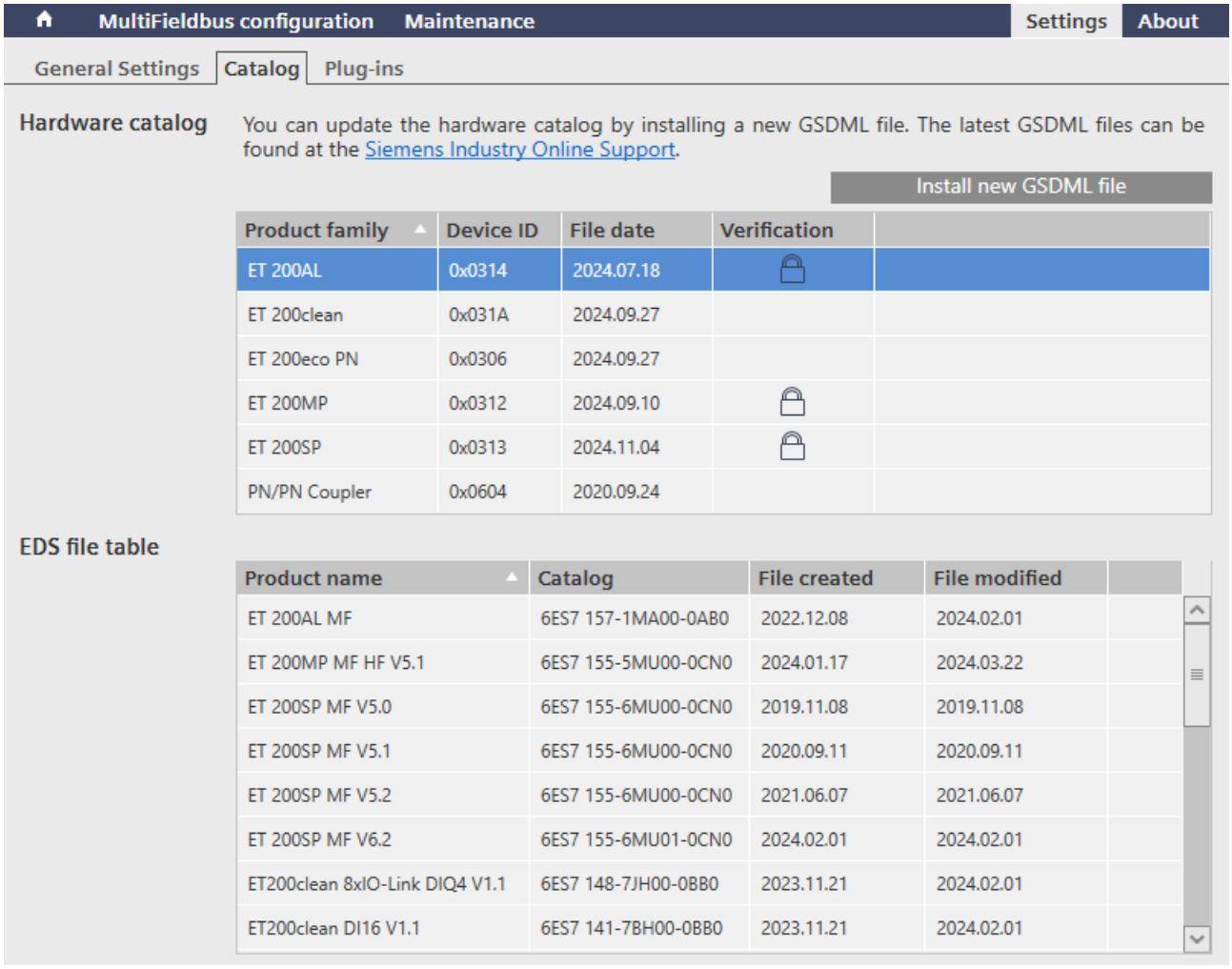
In the "Network adapter" area, you can see all available network adapters on your PC with the configured settings.

- The activated network adapters of your PC are black and can be selected.
- The deactivated network adapters of your PC are displayed grayed out.

The MFCT can only establish a connection to the devices if a network adapter is selected.

6.2.2 Catalog

The following figure shows an example of the contents of the "Catalog" tab:



Hardware catalog

You can find the currently installed GSDML files in the "Hardware catalog" area.

If the "Verification" column displays a padlock symbol, then this device originates from a GSDX-container for which the signature has been successfully verified.

To install additional GSDML files or update the GSDML files used, click the "Install new GSDML file" button.

You can find the GSDML/GSDX files used and additionally installed in the folder "MFCT_xx.xx.xx.xx_xx.xx > GSD"

EDS file table

In the "EDS file table" area, you can find the EDS files used in the MFCT.

An EDS file (Electronic Data Sheet) is an ASCII text file that contains all the relevant information of a user application. The files are used by configuration tools and controllers, for example, to integrate and configure sensors or field bus components in networks.

You can only create and configure EDS files with the MFCT (generic EDS file).

You can find the used and additionally generated EDS files in the folder "<MFCT_xx.xx.xx.xx_xx.xx > EDS".

To transfer your configuration from the MFCT project to your MF device, you need to extract the EDS file. You can find information on extracting the EDS file in the section Transfer the configuration (Page 52).

NOTE

For integration in EtherNet/IP configuration systems, use a generic EDS file according to CIP specification Vol. 1.

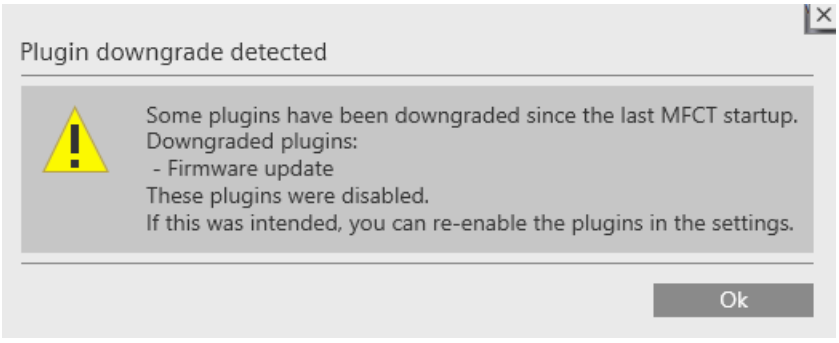
More information

You can find an overview of the most important documents and links to MultiFieldbus in the following Internet article (https://support.industry.siemens.com/cs/ww/en/view/109779189).

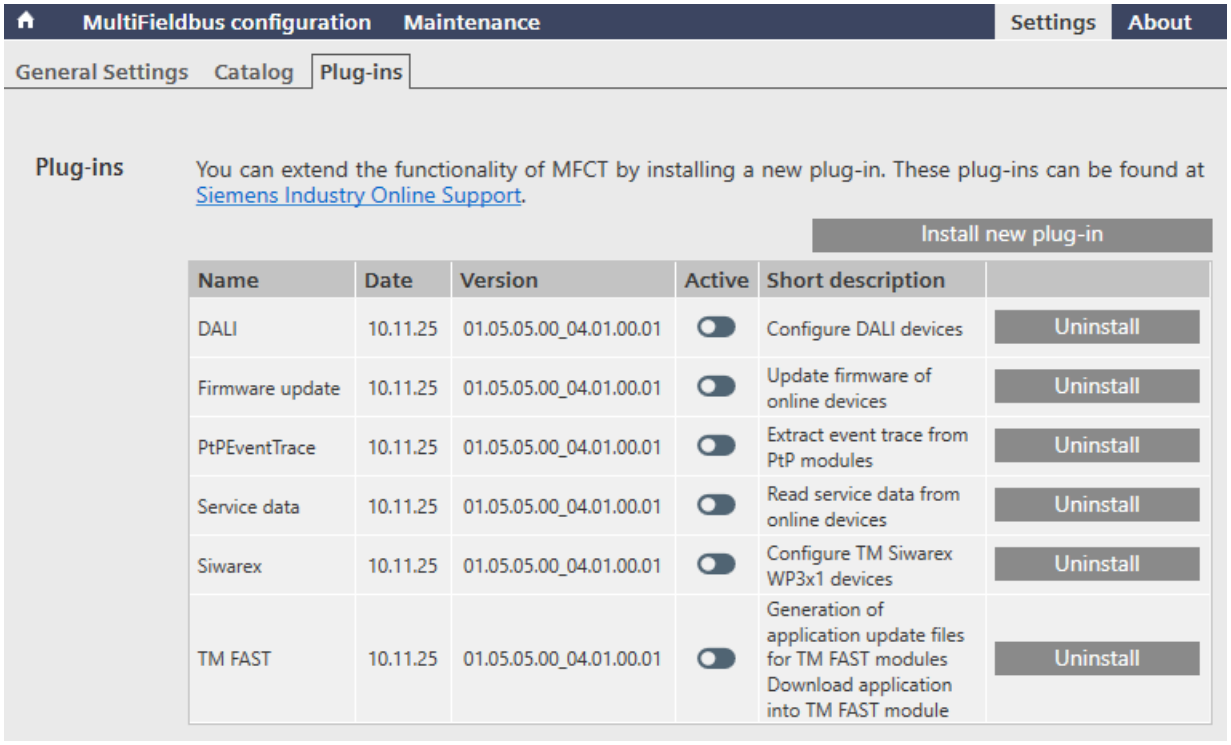
6.2.3 Plug-ins

Plug-ins supplement the MFCT with additional functions not originally supported in the main application.

On startup, the MFCT checks whether all activated plug-ins match the installed MFCT version. If a plug-in from a previous MFCT version is found, it is disabled by the MFCT.
If you want to continue working with a previous version of a plug-in, you can re-enable the plug-in on the "Plug-ins" tab. The warning is no longer displayed on the next start-up.
The MFCT displays the following warning on the start page:



In the "Plug-ins" tab, you can install, activate/deactivate and uninstall the plug-ins. The figure below shows the contents of the "Plug-ins" tab.



Installing

To install a new plug-in, click the "Install new plug-in" button.

"Active" column

You have the following options in the "Active" column:

- Activate available plug-ins: To activate the plug-in for the desired function, drag the slider to the right.
- Deactivate available plug-ins: The default setting is generally deactivated. To deactivate an activated plug-in, drag the slider to the left. The deactivation only takes effect when you restart the MFCT.

Uninstalling

To uninstall a plug-in, click the "Uninstall" button.

NOTE

Uninstalled plug-ins

If you uninstall a plug-in, the plug-in is completely removed and is no longer available to the MFCT.

If you need the uninstalled plug-in again, download the plug-in from the Siemens Industry Online Support page and reinstall the plug-in using the "Install new plug-in" button.

MultiFieldbus configuration

7

You have the following options in the "MultiFieldbus configuration" application:

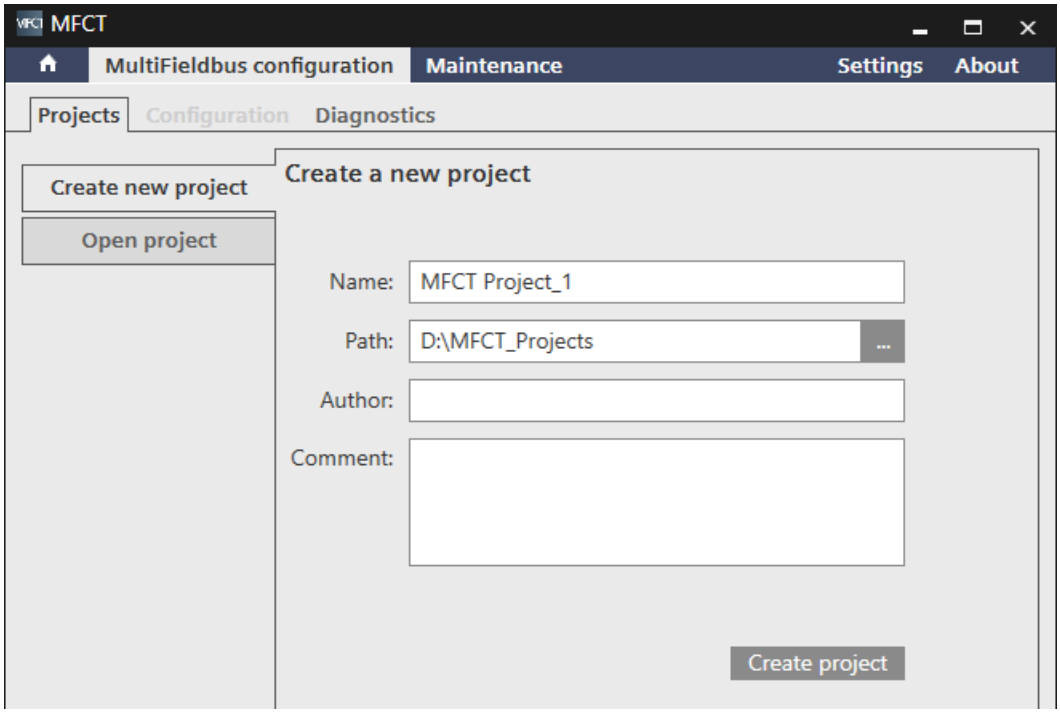
- Configure the basic settings for your MFCT project.
- Configure and assign parameters to the required MF devices for your MFCT project.
- Perform diagnostics on MF devices that can be accessed online.

After opening the MFCT, you can find the "MultiFieldbus configuration" as an application on the start page. In an application of the MFCT that is already open, you can find the MultiFieldbus configuration as a tab in the area of the button for the start screen.

7.1 Creating new MultiFieldbus project in MFCT

To create a new project in the MFCT, proceed as follows:

1. Select the "MultiFieldbus configuration" application.
2. Select the "Projects" tab.
3. Click "Create new project".
4. Assign a name for your project, e.g. MFCT Project_1.
5. Select the storage location for your MFCT project next to "Path".
6. Optionally, you can describe the project with author and comments.
7. Click "Create project".

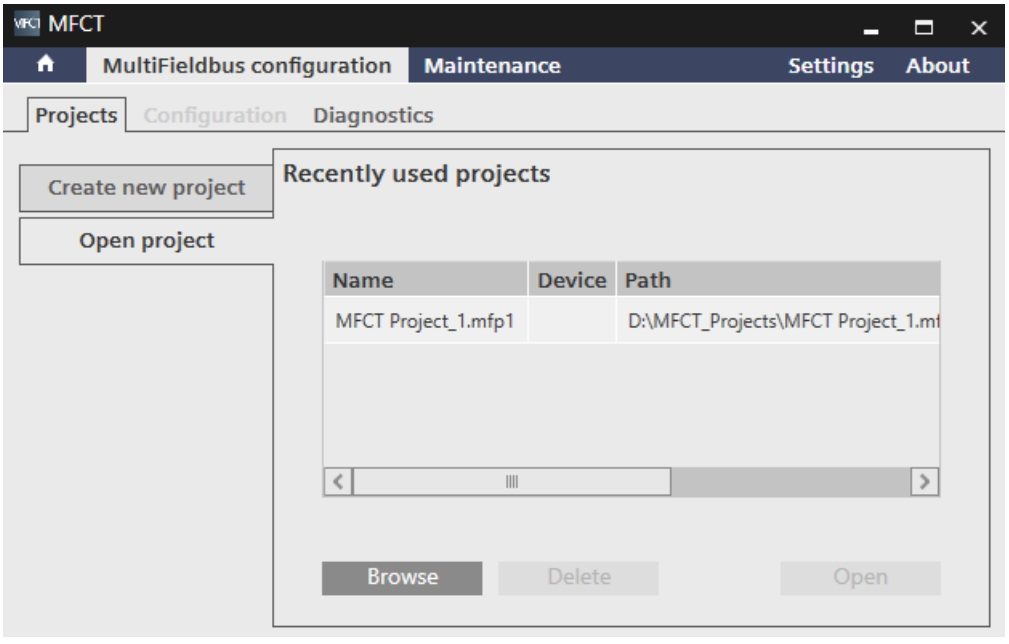


Result: MFCT creates the project under the selected path and switches to the "Configuration" (Page 38) tab for the next processing step.

7.2 Open MultiFieldbus project in MFCT

To open an existing MFCT project, proceed as follows:

1. Select the "MultiFieldbus configuration" application.
2. Select the "Projects" tab.
3. Click the "Open project" button.
   The "Recently used projects" area shows a list of the most recently used MFCT projects.
4. Select one of the following options:
   - If the list contains the desired project, click the desired project.
     To open the project, click the "Open" button or double-click the project.
   - If the list does not show the desired project, click the "Browse" button.
     Navigate to the desired project in the file explorer and select the file MFP1file.
     To open the project, click the "Open" button.



Result: MFCT opens the selected project and switches to the "Configuration" (Page 38) tab for the next processing step.

NOTE

You can use the "Delete" button to delete selected entries from the "Recently Used Projects" list. The project file itself is not deleted by this action.

7.3 Selecting a station

In the "MultiFieldbus configuration" application, you configure the devices for your project in the "Configuration" tab. To add devices to your project, you have the following options in the "Select station" area:

- Catalog:
  If the real MF device is not available or you want to configure an MF device offline.
- Network:
  If the real MF device is available online and you want to load this configuration into the MFCT project.
- Project:
  If you want to transfer MF devices from another project to this project.

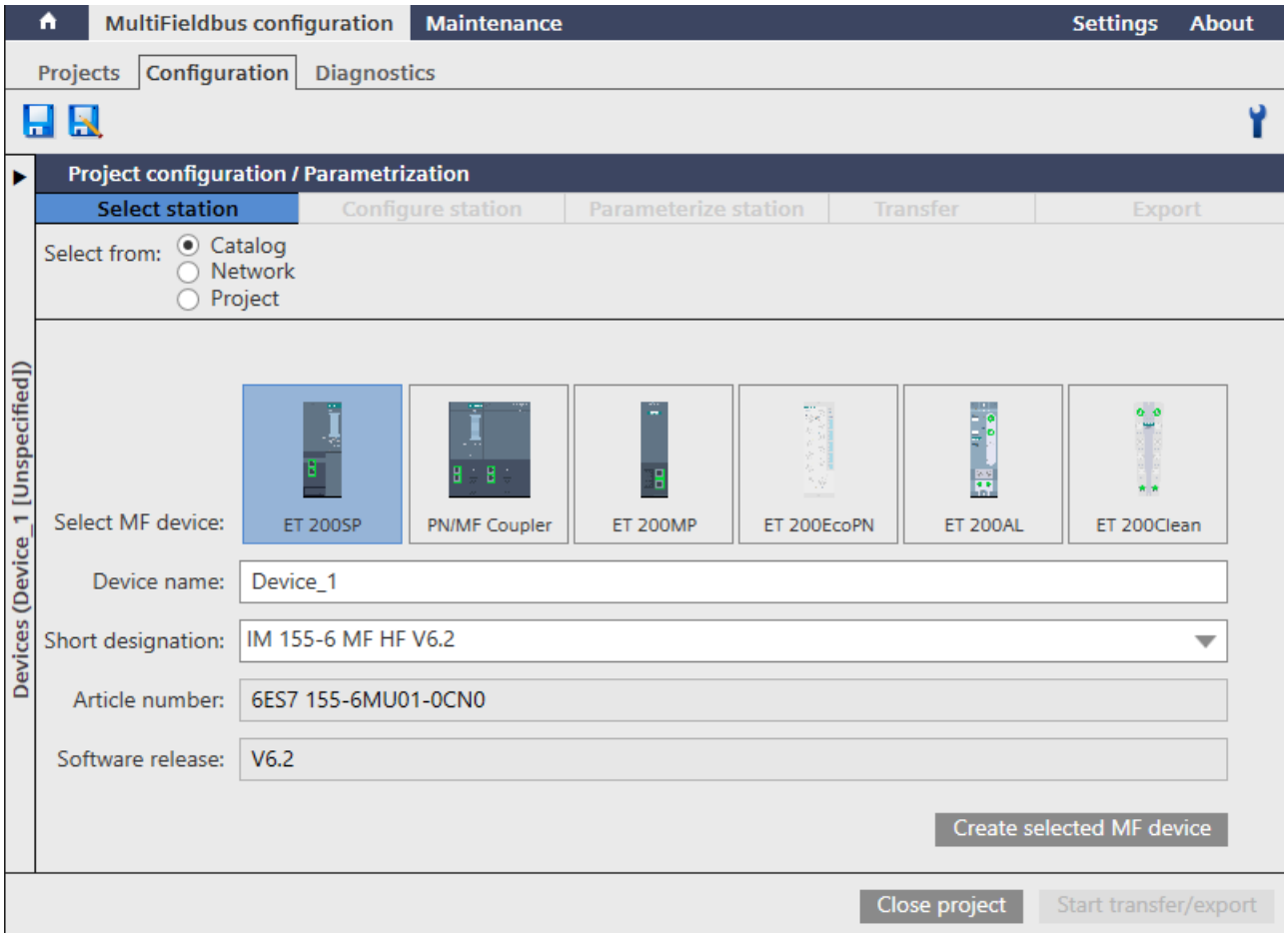
In the following sections, you can read the respective procedure for adding MF devices to your project.

Add an MF device from the catalog

To add an MF device from the catalog to your project, proceed as follows:

1. In the "Devices" area, select the "Add new device" entry.
   The MFCT creates a new device. The "Project configuration / Parameterization" area shows the other options for station selection under "Select station".
2. Select the "Catalog" option.
3. Select the product family, e.g. ET 200SP.
4. Assign a name for the MF device, e.g. Device_1.
5. Select the desired MF device from the "Short designation" selection menu.
   The "Article number" and "Software version" fields show the corresponding data.

6. Click the "Create selected MF device" button.



Result: MFCT adds the device to the project and automatically switches to the next step "Configure station" (Page 42).

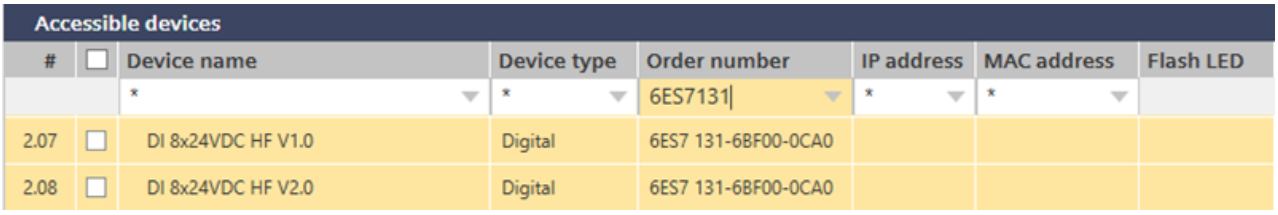
Add an MF device from the network

Requirement: The selected network adapter can access the desired MF device.

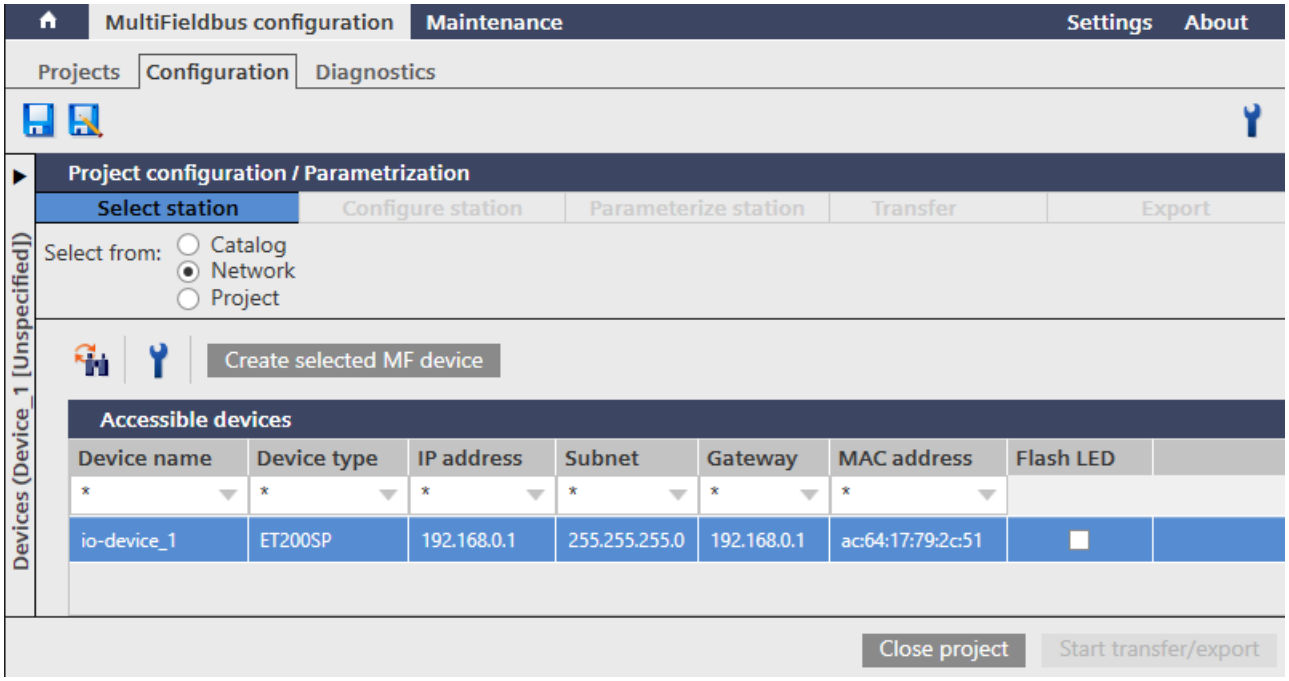
To add an MF device that can be accessed online to your project, proceed as follows:

1. In the "Devices" area, select the "Add new device" entry.
   The MFCT creates a new device. The "Project configuration / Parameterization" area shows the other options for station selection under "Select station".
2. Select the "Network" option.
3. Click the "Start scan" button.
   The MFCT searches for devices that are accessible online and displays the results in the "Accessible devices" table. Devices without MultiFieldbus support are grayed out and cannot be selected.

4. If the "Accessible devices" table does not show any results, click the "Scan settings" button .
   MFCT opens the "Scan settings (Page 97)" window to configure the settings.
5. Optional: Use the incremental search function to locate the desired MF devices. The search starts immediately after you enter the first character. The search query is refined with each additional character. The results are dynamically adapted according to your entry.



6. Select the desired MF device in the "Accessible devices" table.
7. Click "Create selected MF device".

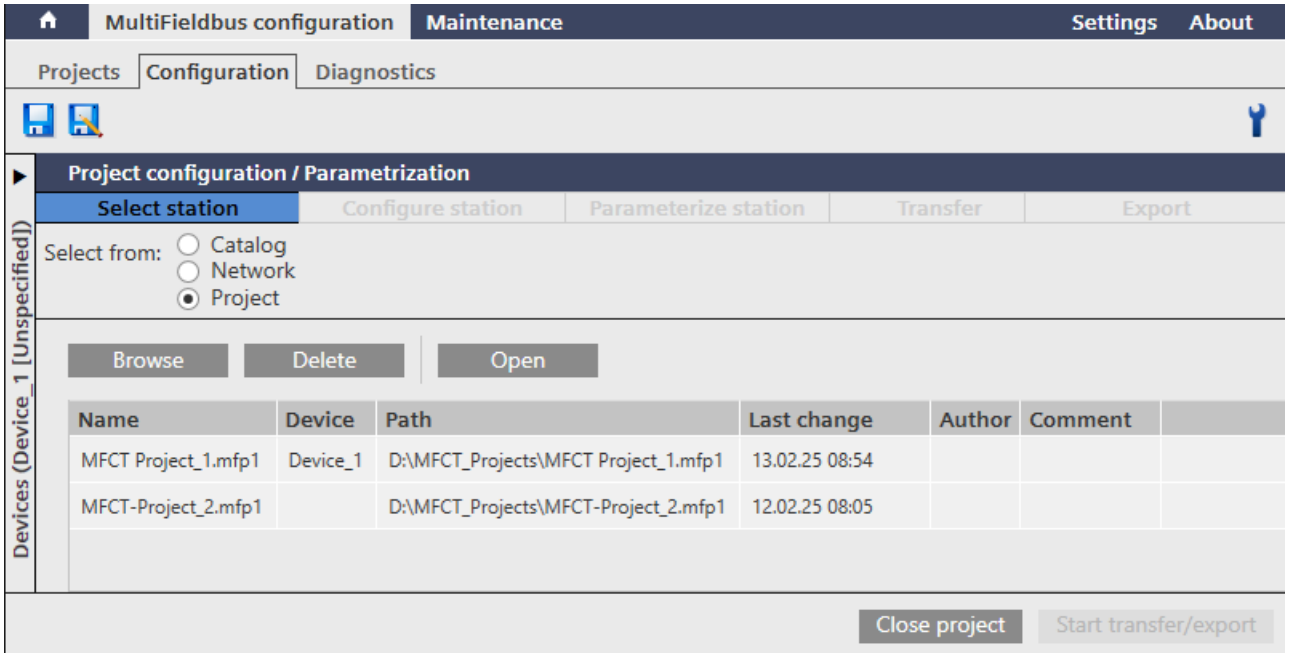


Result: MFCT reads the configuration from the MF device, transfers the configuration to the MF device added in your project and automatically switches to the next step "Configure station (Page 42)".

Add an MF device from a project

To add an MF device from another project to your project, proceed as follows:

1. In the "Devices" area, select the "Add new device" entry.
   The MFCT creates a new device. The "Project configuration / Parameterization" area shows the other options for station selection under "Select station".
2. Select the "Project" option.
   The MFCT displays a list of the most recently used MFCT projects.
3. Select one of the following options:
   - If the list contains the desired project, click the desired project.
     To open the project, click the "Open" button or double-click the project.
   - If the list does not show the desired project, click the "Browse" button.
     Navigate to the desired project in the file explorer and select the file MFP1file.
     To open the project, click the "Open" button.



Result: MFCT loads all MF devices from the selected project into your project and automatically switches to the next step "Configure station" (Page 42).

NOTE

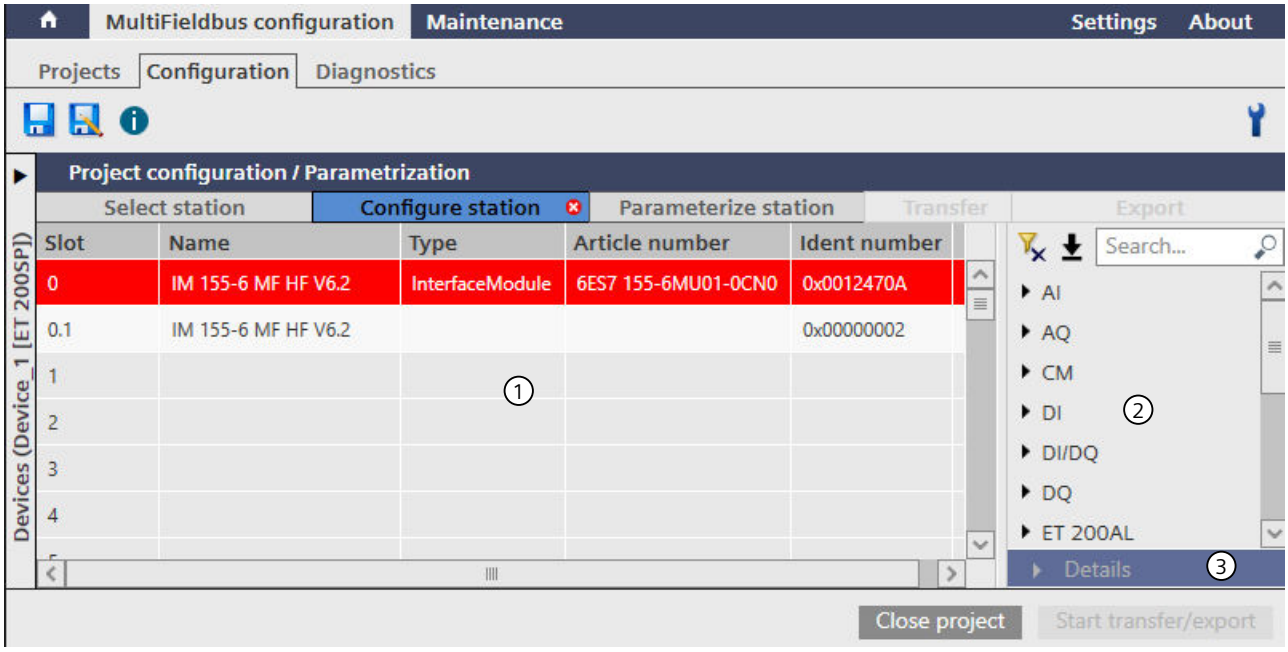
You can use the "Delete" button to delete selected entries from the "Recently Used Projects" list. The project file itself is not deleted by this action.

7.4 Configuring a station

After you have selected your required MF devices in the "Select station" area, configure your MF devices with all the required modules in the "Configure station" area.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

The following figure shows the "Configure station" area in the "Configuration" tab:



① Station setup

This area shows the structure of the MF device as a list, sorted by slots in ascending order. Incorrect configurations are displayed in red. In this example, a server module has not yet been added for the IM 155-6 MF HF interface module.

② Hardware catalog

The hardware catalog shows the modules that, based on the installed GSDML files, you can use for your MF device.

③ Details

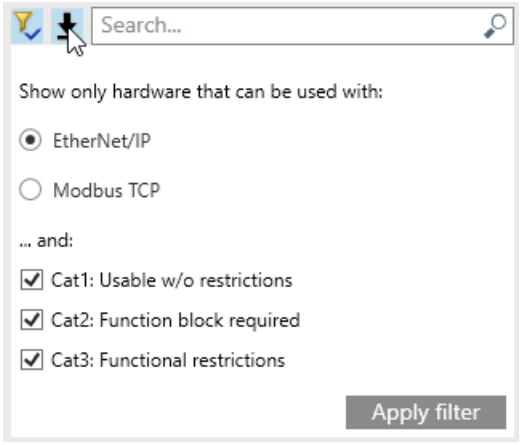
If you select a module in the hardware catalog, you can display information on the selected module and its use on fieldbuses in the "Details" area. To open the detailed view for a module from the hardware catalog, double-click the "Details" entry.

Filter function via modules of the hardware catalog

You can use the filter function to restrict the hardware catalog depending on the fieldbus and the category.

To activate the filter function, proceed as follows:

1. Open the list with the filter criteria.



2. Select the desired fieldbus.
3. Select the desired categories.
4. Activate the filter function using the "Apply filter" button.

Result: The hardware catalog only shows modules that match the filter criteria.

To disable the filter function, click the filter symbol.

Add modules

To add modules from the hardware catalog to your MF device, proceed as follows:

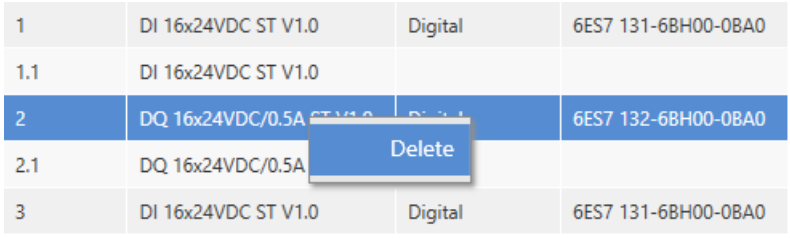
1. Navigate to the required module in the hardware catalog.
2. Select the required module version, e.g. V1.0.
3. Drag-and-drop the module to the desired slot in the station setup.
   The possible slots for the selected module are highlighted in green on the MFCT.
4. Repeat steps 1 and 2 to add further modules from the hardware catalog to your MF device.

Result: You have added the desired modules to your MF device. The corresponding submodules are automatically added for each module.

Delete modules

To delete modules on the MF device, proceed as follows:

1. Select the module to be deleted in the list view.
2. Right-click the module to be deleted.
3. Select "Delete" in the context menu.



Result: You have deleted the module.

Example configuration for a PN/MF-Coupler

The following figure shows an example of the configuration of the network page X1 of a PN/MF coupler.

1	OUT 64 Byte	Output		0x04400000
1.1	OUT 64 Byte			0x00000001
2	IN 128 Byte+DS	Input		0x00000480
2.1	IN 128 Byte+DS			0x00000001

In this example 64 bytes are written to the network page X2 and 128 bytes are read from the network page X2.

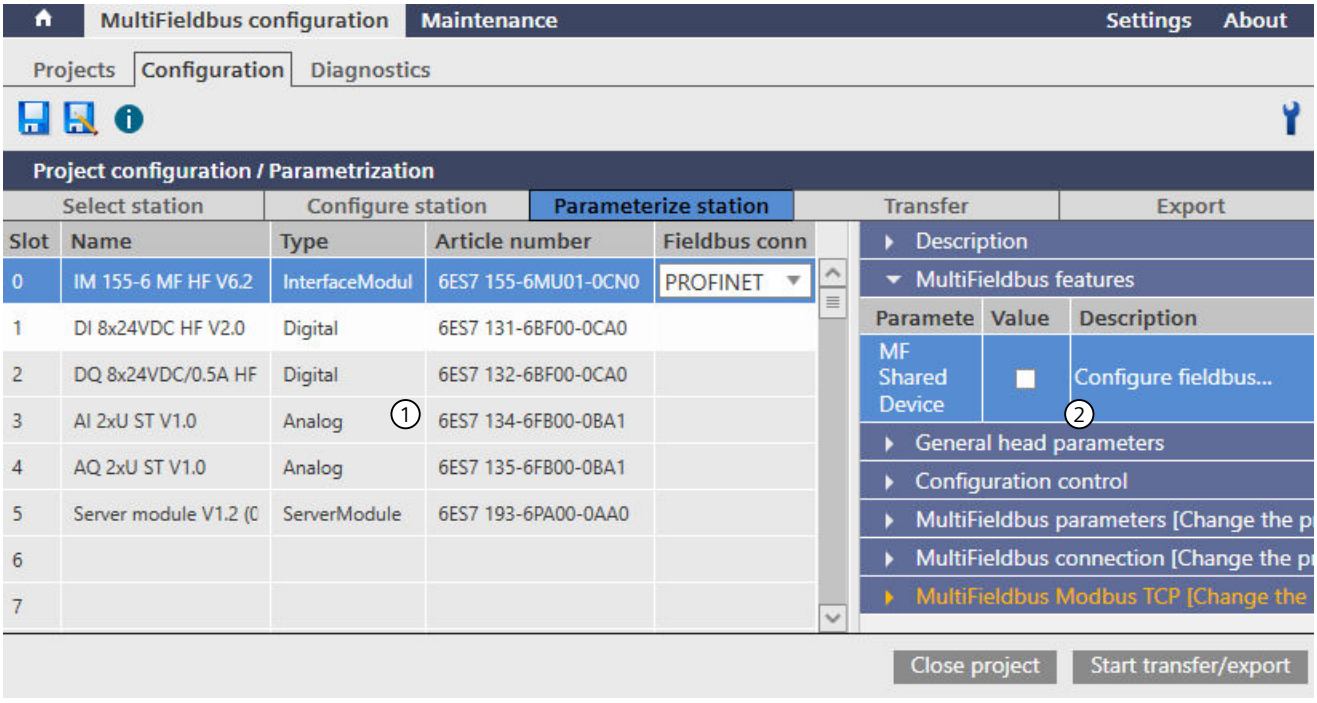
You can find information on how to use the network page X2 with STEP 7 (TIA Portal) with GSD file in the "PN/MF Coupler (https://support.industry.siemens.com/cs/ww/en/view/109781406)" installation and operating manual.

7.5 Parameterizing the station

After you have configured your MF devices with all the required modules in the "Configure station" area, configure the modules of the station in the "Parameterize station" area.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

The following figure shows the "Parameterize station" area in the "Configuration" tab:



① Station setup

This area shows the structure of the MF device as a list, sorted by slots in ascending order. In this example, the IM 155-6 MF HF interface module was configured with digital and analog modules.

② Configure the parameters of the modules

This area shows the configurable parameters for the selected module in the list view ①.

You can find information on the MultiFieldbus properties in the respective equipment manual for the module. You can find an overview in the section Reference documents (Page 7).

Procedure - Configure different fieldbuses

If an MF device supports the "MF Shared Device" function, you can configure different fieldbuses for all modules. To configure different fieldbuses for the modules of the MF device, proceed as follows:

1. In the list, select the interface module in slot 0.
   The MFCT shows the configurable parameters for the selected module.
2. Open the "MultiFieldbus properties" selection menu.
3. Activate the "MF Shared Device" option.
   The MFCT displays a selection menu next to each module in the "Fieldbus connection" column. The configured fieldbus connection of the interface module is adopted in the basic settings, e.g. PROFINET.
4. Select the fieldbus connections for the modules in the selection menus.

Project configuration / Parametrization

Select station | Configure station | **Parameterize station**

Slot	Name	Type	Article number	Fieldbus connection
0	IM 155-6 MF HF V6.2	InterfaceModule	6ES7 155-6MU01-0CN0	PROFINET
1	DI 8x24VDC HF V2.0	Digital	6ES7 131-6BF00-0CA0	ModbusTCP #0 (0x000, 0x2D0)
2	DQ 8x24VDC/0.5A HF V2.0	Digital	6ES7 132-6BF00-0CA0	EtherNet/IP #0 (0x301, 0x300)
3	AI 2xU ST V1.0	Analog	6ES7 134-6FB00-0BA1	PROFINET
4	AQ 2xU ST V1.0	Analog	6ES7 135-6FB00-0BA1	PROFINET
5	Server module V1.2 (0 bytes)	ServerModule	6ES7 193-6PA00-0AA0	PROFINET
6				

Result: You have configured different fieldbuses for the modules.

Procedure - Configure the Modbus TCP fieldbus connections

Optionally, you can configure the hold times for all Modbus TCP field bus connections as follows:

1. In the list, select the interface module in slot 0.
   The MFCT shows the configurable parameters for the selected module.
2. Edit the following values for the desired Modbus TCP fieldbus connections in the "MultiFieldbus Modbus TCP" selection menu:
   - Connection hold time:
     The default setting is 5 000 ms. You can edit the value in a range from 1 to 30 000 ms.
   - Reset hold connection:
     The default setting is 0 ms. You can edit the value in a range from 1 to 30 000 ms.

Result: You have configured the hold times for the desired Modbus TCP field bus connections.

More information

If you change the configuration from PROFINET to EtherNet/IP or Modbus TCP, a parameterization error may occur in connection with the change of BusAdapter type. You can only remedy the parameterization error with a reset to factory settings (Page 97) and reconfiguration with MFCT.

You can find information on restrictions in the equipment manuals of the MF devices used.

7.5.1 Parameterizing the I/O data alignment

In MFCT you generate and export the I/O data alignment for modules with a fieldbus connection over EtherNet/IP. The MFCT exports the generated data as a user-defined data type (User Defined Type, UDT) in an I5x file. In addition, the MFCT generates a CSV file in which byte addresses are assigned to the slots and modules.

For further processing, the user must find the required values in the UDT and insert them into a tag in the user program. Only in this way can the values be arranged in the required order. The larger the UDT is, the greater the effort will be to find the required values in the UDT.

As of MFCT version V1.5 SP5, you can configure flexible I/O data alignment for EtherNet/IP. You can configure the order of the required I/O data already in the MFCT. The MFCT generates the UDT according to your configuration. This enables you to find the required values in the UDT more quickly and avoid having to make extensive modifications in the user program of the higher-level IO controller.

The next sections provide information on the configuration options.

Selecting flexible I/O data alignment for EtherNet/IP

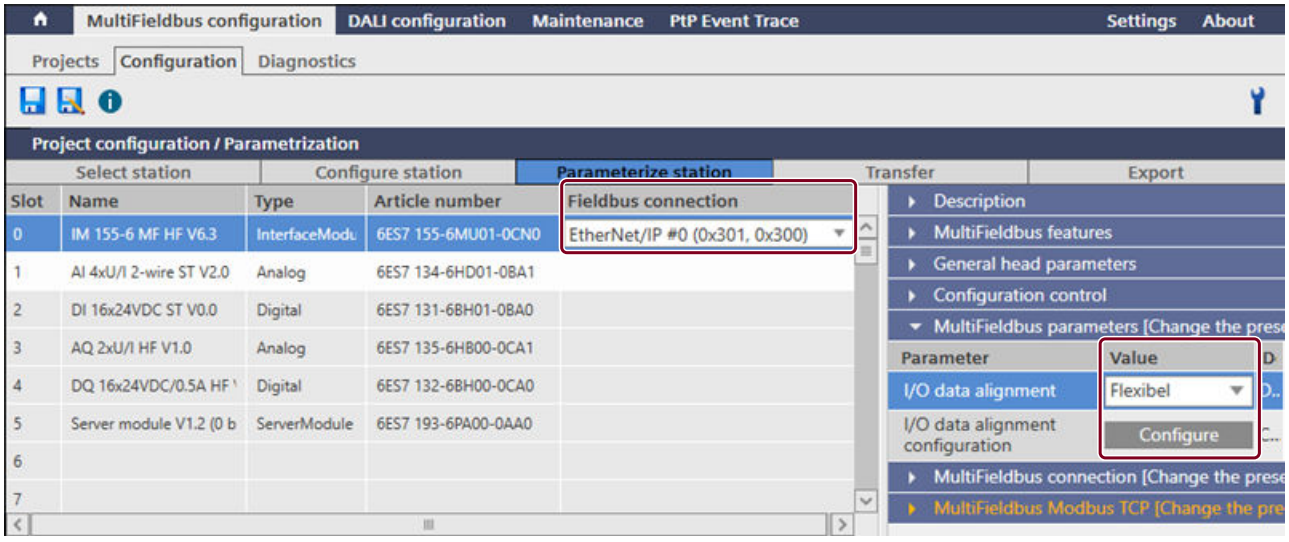
You can find the configuration options for the I/O data alignment in the module parameters of the interface module under "Parameterize station > MultiFieldbus parameters > I/O data alignment". You can choose between the following standard values in the "I/O data alignment" selection menu:

- Byte (default)
- Word

To select the flexible I/O data alignment for EtherNet/IP, proceed as follows:

1. Select the desired interface module in the "Parameterize station" area.
2. Select a fieldbus connection over EtherNet/IP.
3. Navigate in the right window to the "MultiFieldbus parameters > I/O data alignment" area.

4. Select "Flexibel" in the drop-down menu next to "I/O data alignment".
   An additional line "I/O data alignment configuration" appears below the drop-down menu.



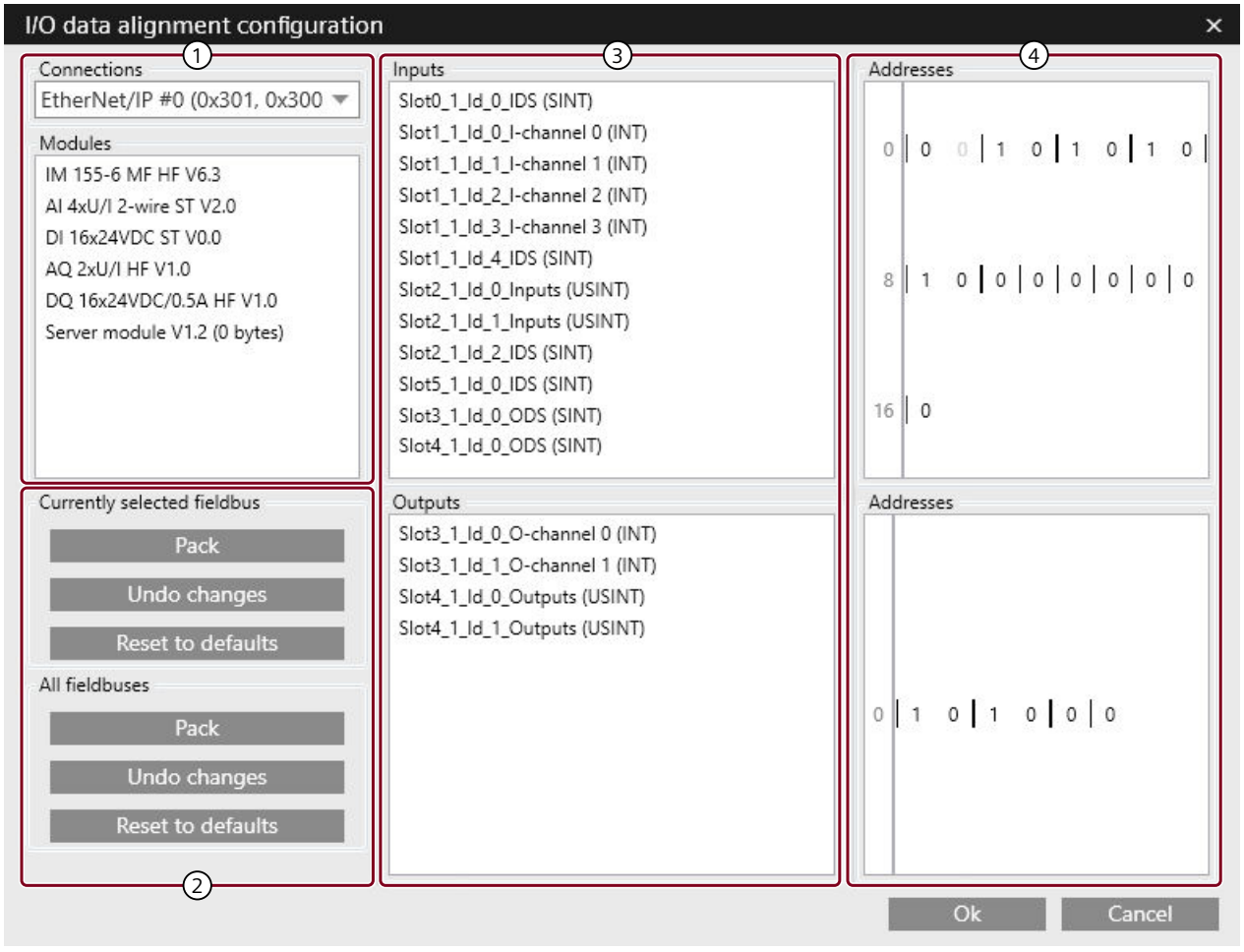
Result: You have selected a fieldbus connection over EtherNet/IP and the flexible I/O data alignment.

If you click the "Configure" button, the MFCT opens the editor for configuring the I/O data alignment.

Editor for configuring the I/O data alignment

In the "I/O data alignment configuration" editor, you configure the order of the inputs and outputs for the UDT. The next sections provide information on the various areas.

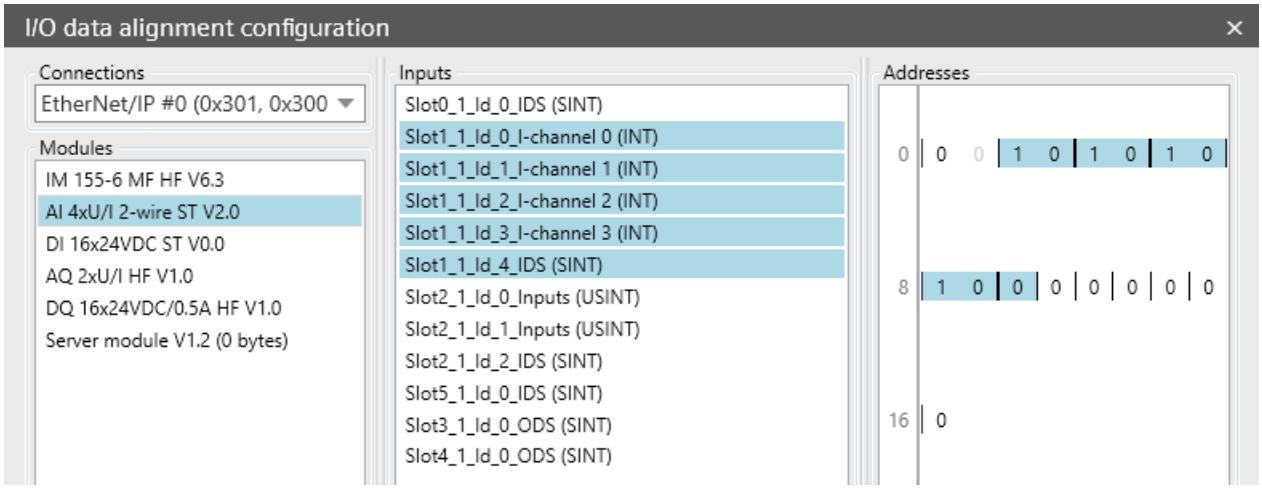
The figure below shows the "I/O data alignment configuration" editor.



① Connections and Modules

In the drop-down menu in the "Connections" area, you select the connection for which you want to configure the order of the input and output data.

In the "Modules" area, you see the modules for which the selected connection has been configured. If you select an input module, for example, then the associated data is highlighted in color in the "Inputs" and "Addresses" areas, as shown in the following figure.



② Buttons for configuration and reset

The following buttons provide configuration options that you can apply to the selected fieldbus or all fieldbuses:

- Pack:
  Arranges the data by size, starting with the largest elements. This removes padding bytes and reduces the size of the UDT.
- Undo changes:
  Resets changes.
- Reset to defaults:
  Resets the configuration to the default configuration.

③ Inputs and outputs

The "Inputs" and "Outputs" areas show all available input and output data of the selected connection.

If you select an entry in the "Inputs" or "Outputs" area, other entries belonging to the module are shown in gray.
The "Modules" and "Addresses" areas behave as follows:

- Modules:
  The module to which the selected entry belongs is highlighted in color.
- Addresses:
  The addresses belonging to the selected entry are highlighted in color. Other addresses that belong to the module are shown in gray.

④ Addresses of inputs and outputs

The "Addresses" areas show the respective address ranges of the selected input and output data. If you select an address range, this address range is highlighted in color. Other address ranges that belong to the module are shown in gray.

If you select an address range of input data, for example, then the "Modules" and "Inputs" areas behave as follows:

- Modules:
  The module to which the selected address range belongs is highlighted in color.
- Inputs:
  The entry to which the selected address range belongs is highlighted in color. Other entries that belong to the module are shown in gray.

Changing the order of input and output data

You configure the order of the input and output data for the UDT in the "Inputs" and "Outputs" areas.

To change the order of the entries, proceed as follows:

1. Left-click on the desired entry in the "Inputs" or "Outputs" area and hold down the left mouse button.
2. Drag the entry to the desired position.
   You can only move input data within the "Inputs" area. You can only move output data within the "Outputs" area.
3. Release the left mouse button.
4. Repeat steps 1 through 3 for other entries that you want to move.

Result: You have configured the order of the input and output data. The "Addresses" areas next to the "Inputs" and "Outputs" areas are automatically adjusted to reflect the changed order.

Click the "OK" button to apply the changes. The MFCT closes the "I/O data alignment configuration" editor.

7.6 Transfer the configuration

Once you have configured your station with the modules in the "Parameterize station" area, the following options are available to you:

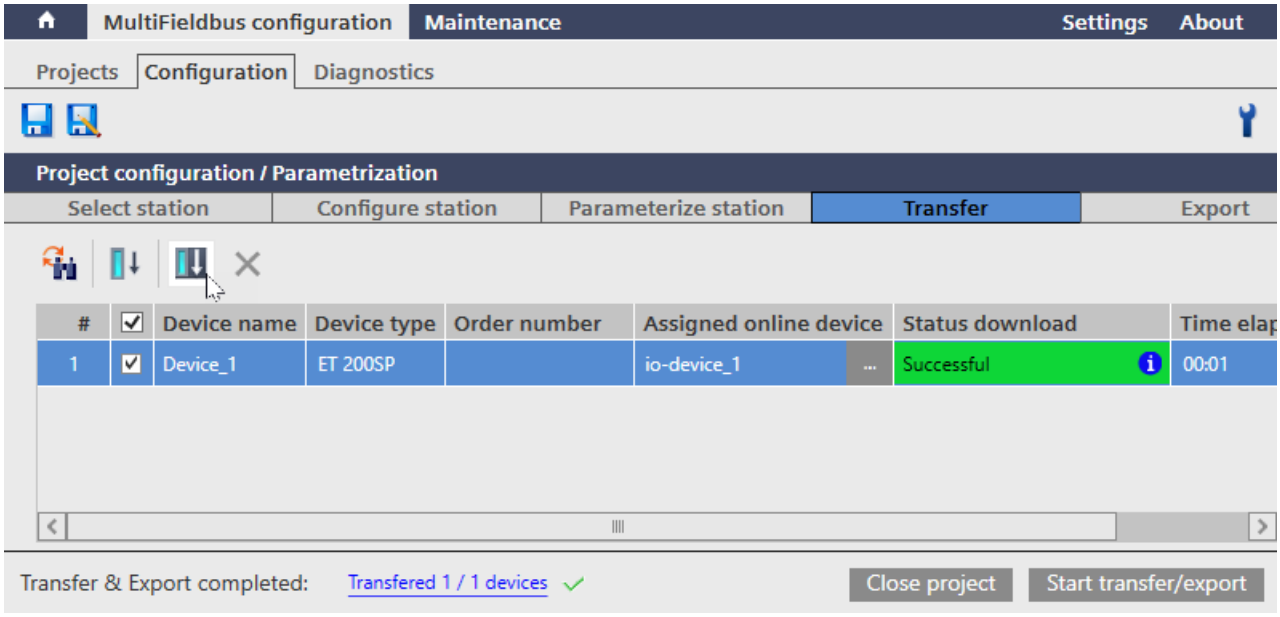
- Transfer configuration:
  You load the configuration into the MF device that can be accessed online.
- Export configuration:
  You export the configuration for use in other engineering tools. You can learn how to export the configuration in the section Exporting the configuration (Page 54).

Transfer the configuration to the MF device

To transfer the configured and parameterized station to the MF device, proceed as follows:

1. Select the "Transfer" function in the "Configuration" tab.
   The MFCT displays the configured devices as a list.
2. In the list, select the device that you want to transfer to the MF device that is accessible online.
3. In the "Assign device online" column, click the button next to the "<Select device>" entry.
   The MFCT opens another "Accessible devices" window.
4. In the "Accessible devices" window, click the"Start scan" button  .
   The MFCT shows the accessible devices for the download as a list. Devices without MultiFieldbus support cannot be selected and are shown grayed out.
5. Select an MF device from the list.
6. Click the "Assign device" button.
   The MFCT closes the "Accessible devices" window. You can see the selected device in the "Assign device online" column.

7. Click the "Start transfer of configuration" button.
   The MFCT loads the configuration into the selected MF device. You can see the progress and status in the "Download status" column.



Result: You have transferred your configuration to the MF device.

NOTE

Transferring and exporting configuration

If you click the "Start transfer of configuration" button, the configuration is transferred to the MF device.

If you click the "Start transfer/export" button, the configuration is transferred to the MF device and also exported.

Troubleshooting - Timeout during transfer to the MF device

If the transfer of the configuration to the MF device exceeds a defined time window, the MFCT shows the error as a timeout under "Download status". To correct the error, you have the following options, for example:

- Check the network accessibility of the MF device via the network adapter selected in MFCT.
- Disconnect the connection of the MF device to PROFINET I/O controllers.
- If you have selected the option "Use router for gateway" in the network parameters, check the network parameters of the device.

7.7 Exporting the configuration

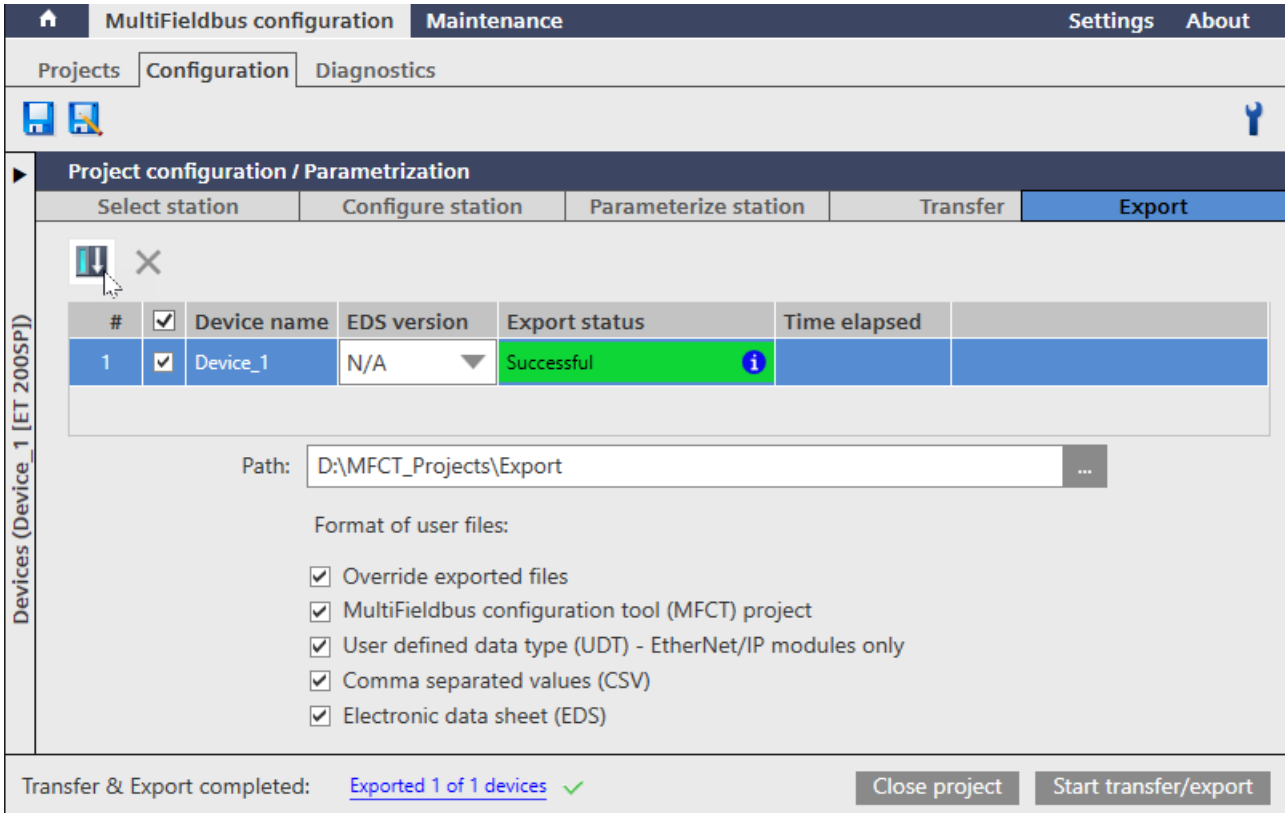
Once you have configured your station with the modules in the "Parameterize station" area, the following options are available to you:

- Export configuration:
  You export the configuration for use in other engineering tools.
- Transfer configuration:
  You load the configuration into the MF device that can be accessed online. You can learn how to export the configuration in the section Transfer the configuration (Page 52).

Exporting the configuration

To export the configured and parameterized station, proceed as follows:

1. Select the "Export" function in the "Configuration" tab.
   The MFCT displays the configured devices as a list.
2. Select the device you want to export from the list.
3. Next to "Path", select the storage location for the data to be exported.
4. Select the files to be exported in the "Format of user file" area.
5. Click the "Start configuration export" button.
   The MFCT exports the configuration to the selected storage location.



Result: You have exported your configuration to the selected storage location.

NOTE

Transferring and exporting configuration

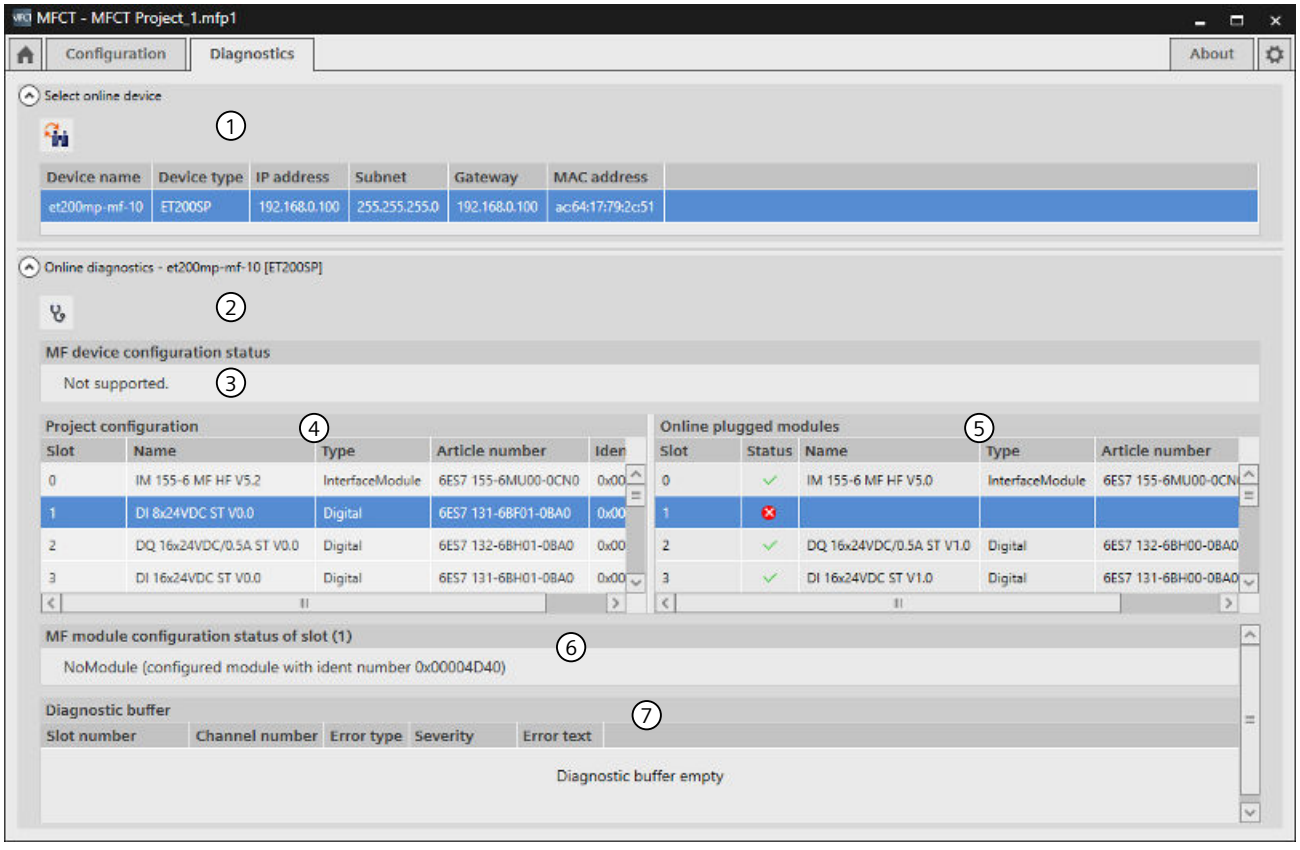
If you click the "Start configuration export" button, the configuration is exported to the selected storage location.

If you click the "Start transfer/export" button, the configuration is transferred to the MF device and also exported.

7.8 Reading diagnostics

In the "MultiFieldbus configuration" application, you can perform diagnostics on the MF devices that can be accessed online in the "Diagnostics" tab.

The following figure shows the contents of the "Diagnostics" tab:



① Selecting an online device

Use the "Start scan" button to search for the MF devices that are accessible via the preset network interface.
The MFCT shows the devices that are accessible online, from which you can select an MF device.

② Online diagnostics

Use the "Update online status" button to update the display under "Online plugged modules" ⑤.

③ MF module configuration status

The status of the configuration is displayed in the "MF module configuration status" area.

④ Project configuration

In the "Project configuration" area, you can find information on the loaded configuration of the selected MF device.

⑤ Online plugged modules

You can find information on the selected MF device in the "Online plugged modules" area. This requires that the
MF device is accessible online.

⑥ MF module configuration status of slot (x)

The "MF module configuration status of slot (x)" area shows you whether a module plugged in online matches the module in the MF project.

⑦ Diagnostic buffer

Under "Diagnostic buffer", you can see the content of the diagnostic buffer.

DALI configuration

8

The "DALI configuration" application is available as a plug-in in the MFCT. To use the "DALI configuration" application, activate the plug-in.

Once you have activated the plug-in, you can find the DALI configuration on the start page as an application. In an opened application, you can find the DALI configuration as a tab in the area of the button for the start screen.

You search the connected network for devices with DALI modules in the "DALI configuration" application. You can address, parameterize and control devices connected to the DALI modules.

As of MFCT version V1.5 SP4, you can also use expert mode without an online connection to MF devices and create or save frames.

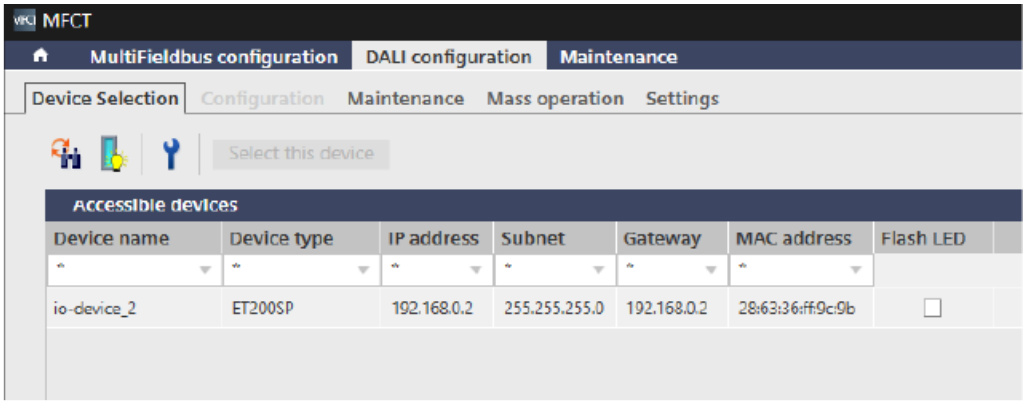
More information

You can learn how to activate a plug-in in section Plug-ins (Page 33).

You can learn how to configure frames in expert mode in section Expert mode (Page 73).

8.1 Selecting station with DALI module

You scan for ET 200 stations in which DALI modules are integrated on the "Device selection" tab.



Procedure

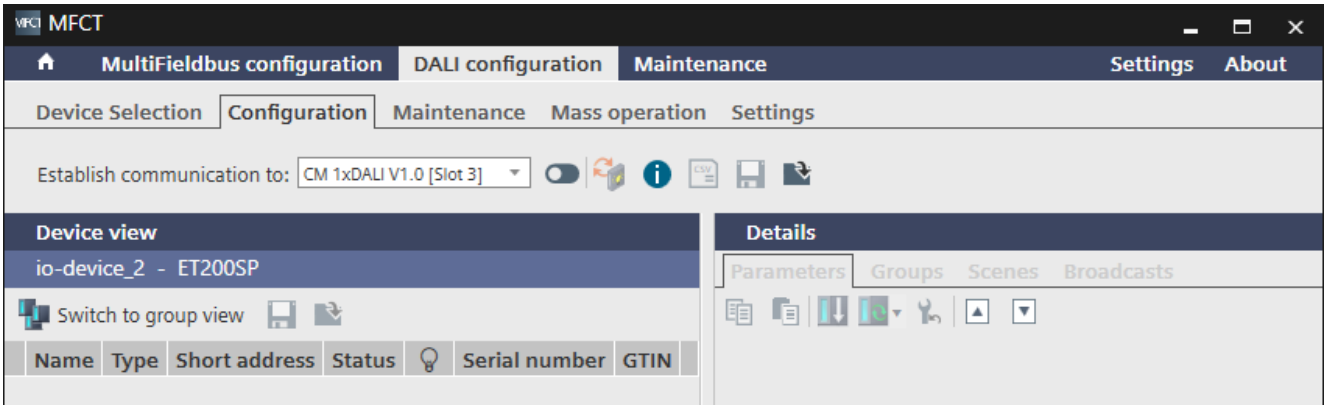
To select an accessible device, proceed as follows:

1. Click the "Start scan" button to search for accessible CPUs and ET 200SP interface modules.
2. Click the button to filter by CPUs and interface modules with an inserted DALI module.
3. Select the desired station from the list.
4. Select the station for the configuration by clicking the button Select this device or double-clicking the station.

Result: MFCT selects the desired station and opens the "Configuration" tab.

8.2 Selecting and configuring a DALI module

You select the DALI modules present in the ET 200 station and configure the connected DALI devices on the "Configuration" tab.



Procedure

To select and configure your DALI module, proceed as follows:

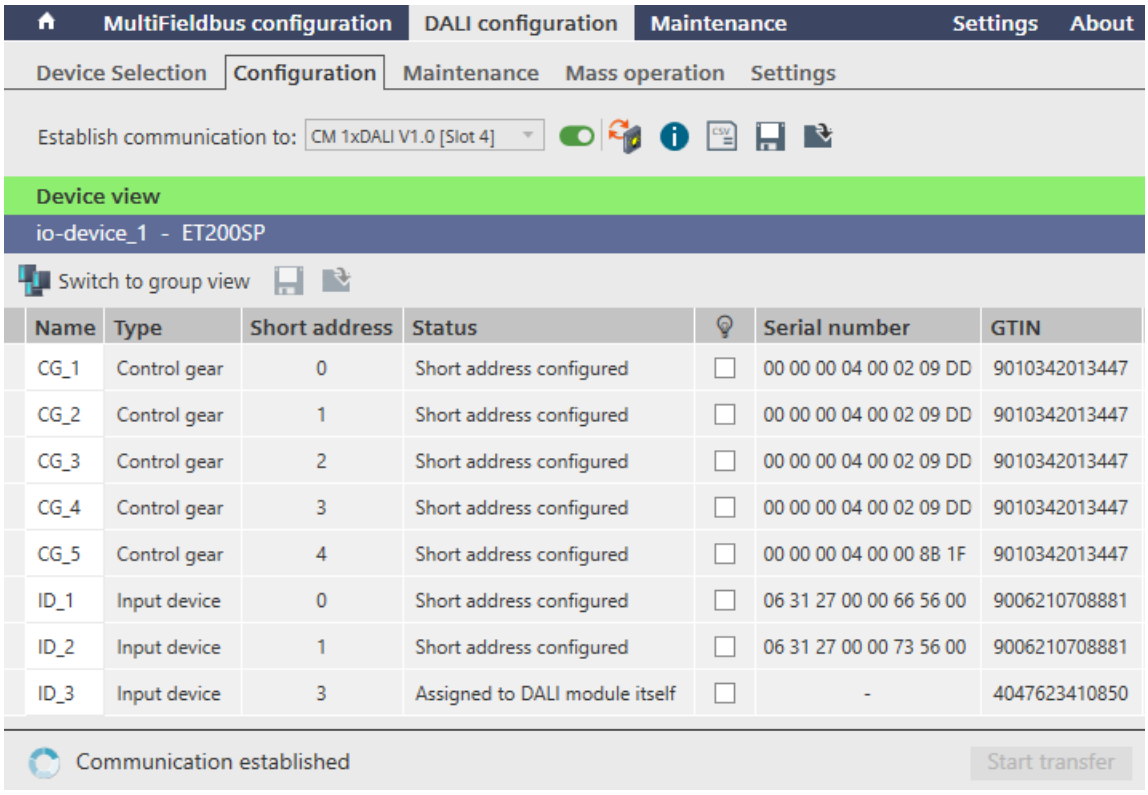
1. Select the DALI module you want to connect to in the drop-down menu .
2. Click the toggle switch "Establish communication" to establish the connection to the DALI module.
3. Beforehand, select only the required parameters in the settings (Page 78), e.g. assign short addresses automatically. The more parameters you select, the longer the scanning process will take.

NOTE

If you have selected the "Assign short addresses automatically" parameter, the unaddressed DALI devices are automatically assigned short addresses during scanning.

4. The button calls the communication status, i.e. whether you are connected to the module. When the connection is set up, start the search for the DALI devices connected to the module.

5. Click the "Start scan" button . Depending on the number of bus nodes, the process can take several minutes.



Name	Type	Short address	Status		Serial number	GTIN
CG_1	Control gear	0	Short address configured	☐	00 00 00 04 00 02 09 DD	9010342013447
CG_2	Control gear	1	Short address configured	☐	00 00 00 04 00 02 09 DD	9010342013447
CG_3	Control gear	2	Short address configured	☐	00 00 00 04 00 02 09 DD	9010342013447
CG_4	Control gear	3	Short address configured	☐	00 00 00 04 00 02 09 DD	9010342013447
CG_5	Control gear	4	Short address configured	☐	00 00 00 04 00 00 8B 1F	9010342013447
ID_1	Input device	0	Short address configured	☐	06 31 27 00 00 66 56 00	9006210708881
ID_2	Input device	1	Short address configured	☐	06 31 27 00 00 73 56 00	9006210708881
ID_3	Input device	3	Assigned to DALI module itself	☐	-	4047623410850

Result: You have read out the serial numbers and the GTIN code (Global Trade Item Number) of the connected DALI devices. For the detected DALI devices, you have the following options:

- Identify individual DALI devices using the column with the light bulb icon .
  To do so, select the check box in the row of the desired DALI device. As a result, an identification command is set on the DALI bus. Information on how a DALI device responds to this identification command can be found in the DALI device's manual.
- Change short addresses or device parameters
- Assign the DALI devices to groups

The following options are available:

- Optionally, you can export the currently displayed configuration of the devices as a *.csv file. To do this, click the "CSV" button . This allows you to document the existing configuration.
- You save and open projects with the "Save" and "Open" buttons . You can only open a saved project when there is an active connection to the CM DALI module.
- The "Status" column in the device view displays information about the bus nodes.

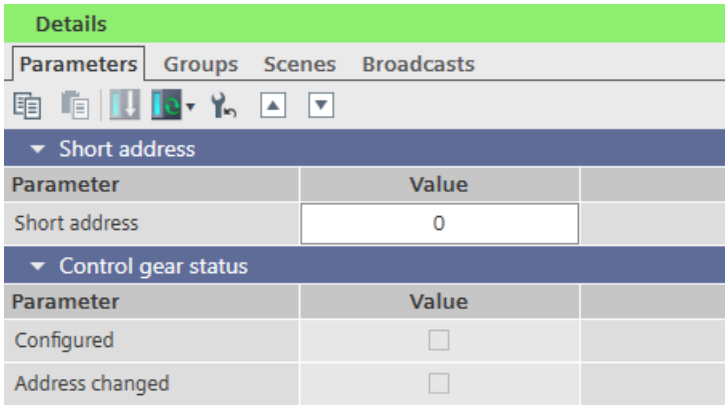
Information about the short addresses

DALI input devices and control gear have separate address ranges for short addresses. If a short address is assigned more than once within an address range, there is an address conflict. In this case, the "Status" column displays the corresponding text message.

For each DALI module, you may only assign each short address once to a DALI device or control gear connected to it. If a short address has been assigned more than once, you must reset the DALI devices involved. The next subsection explains how to reset DALI devices.

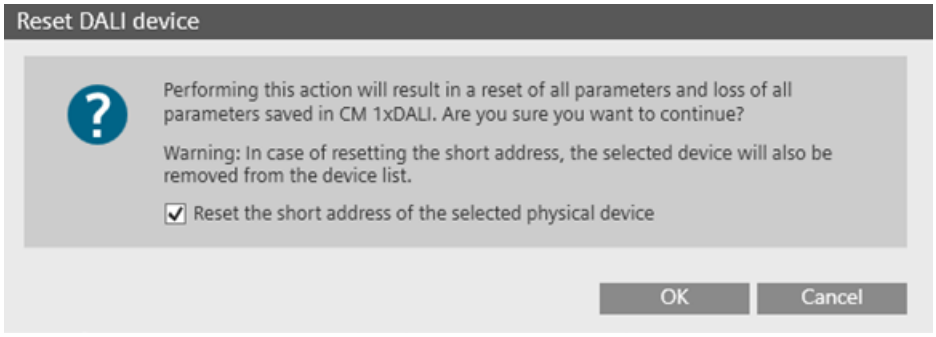
Details view

In the "Details > Parameters tab" area, you have additional options for configuring your devices.



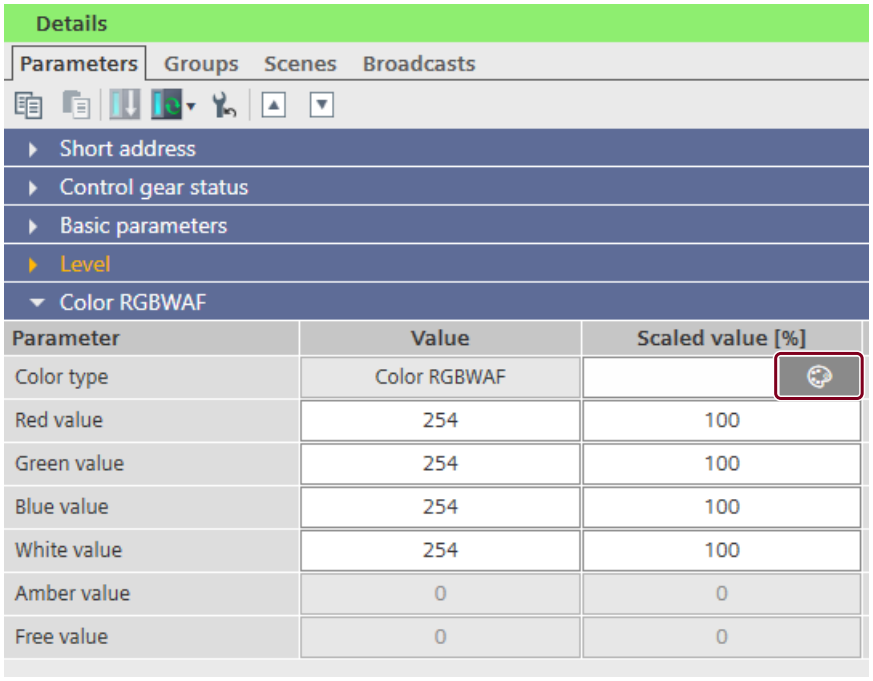
- To copy the configuration of one device and insert it into another device, use the button .
- To apply the modified parameters to the DALI device, click the button .
- In the "Details > Parameters tab" area, you can use the button to refresh the parameters of an individual device. The remaining bus nodes are not scanned again.
- To reset and/or delete a device, click the button .

  To reset only the short address of the selected device, select the "Reset the short address of the selected physical device" check box.



8.3 Making color settings

In the "Details > Parameters tab" area, click the button  to open the color picker. Select the desired color or color temperature there. The parameter fields show the appropriate values for the selected color and color temperature based on the selection.

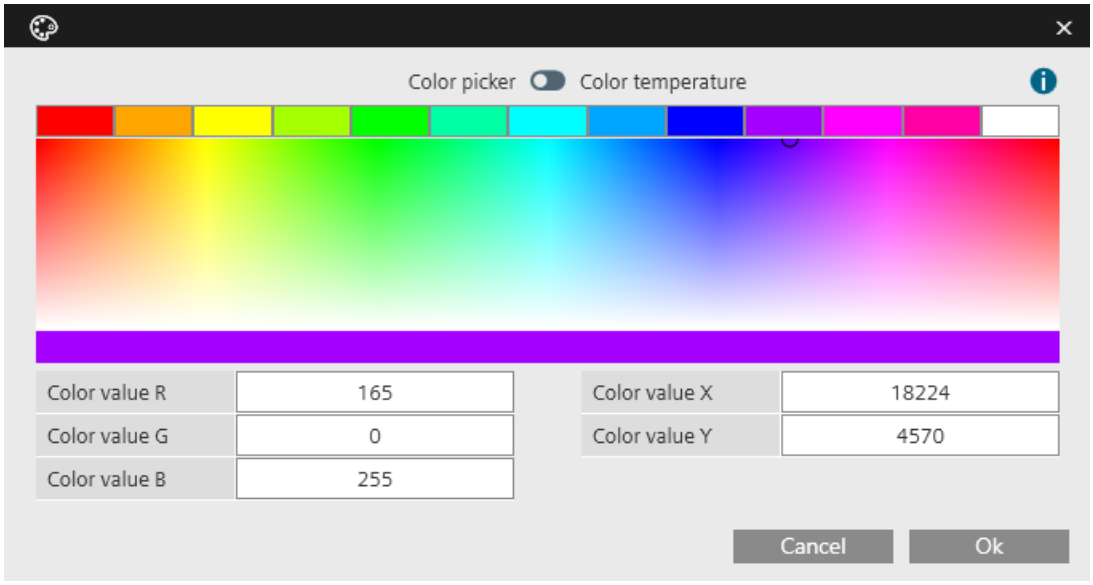


Setting the color

Depending on the control gear used, different colors are supported. The MFCT supports you in selecting a suitable color in various ways:

- Button: Select a suitable color by clicking on or in the color areas.
- Direct input:
  - Color value X/Y: X and Y coordinates for all colors
  - Color value RGBWAF: 6 values for up to 6 color components: Red, green, blue, white, amber and one free color

The following picture shows an example of a possible color selection:

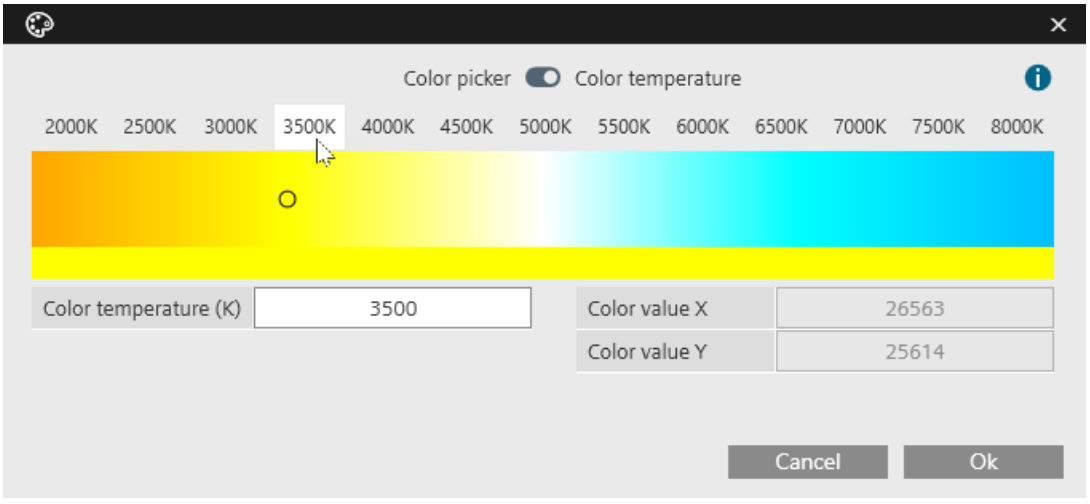


Setting the color temperature

The MFCT supports you in selecting a suitable color temperature in various ways:

- Buttons: Select a suitable value, e.g. "3500K", by clicking on the buttons.
- Direct input: Assign a value between 2000 K for warm white and 8000 K for cool white in the field next to "Color temperature (K)".

The color temperature is specified in Kelvin (K). The following figure shows an example of a color temperature of 3 500 K:



8.4 Device types

The DALI devices can be subdivided into two device types: control gear and input devices. There are different setting options for the two device types.

You can find more information in the SIMATIC ET 200SP Communication Module CM 1xDALI ST equipment manual (https://support.industry.siemens.com/cs/us/en/view/109769428).

8.4.1 Control gear

8.4.1.1 Device view

You have the following options for the control gear in the device view in the "Details" area:

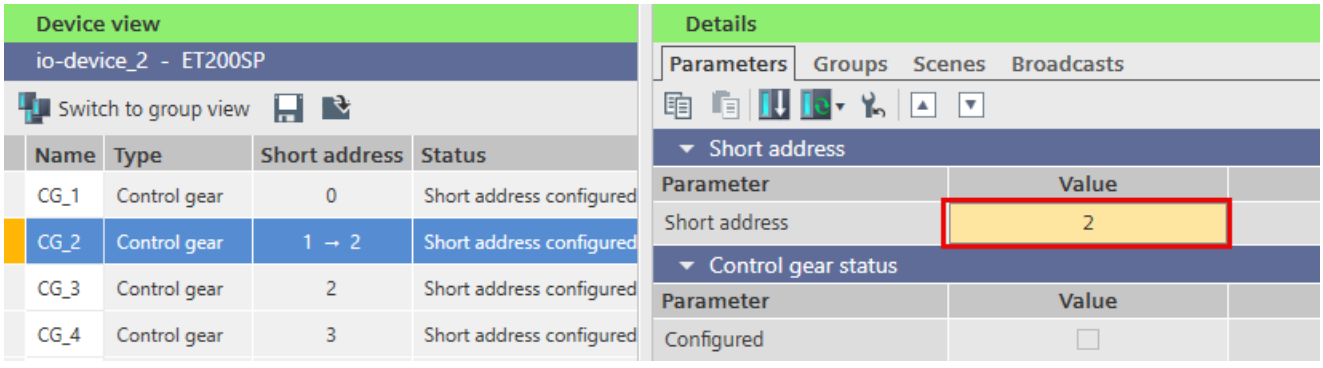
- Read out and transfer parameters
- Manage groups
- Edit scenes
- Send broadcasts

Parameters that have been changed but not yet transferred are highlighted in yellow.

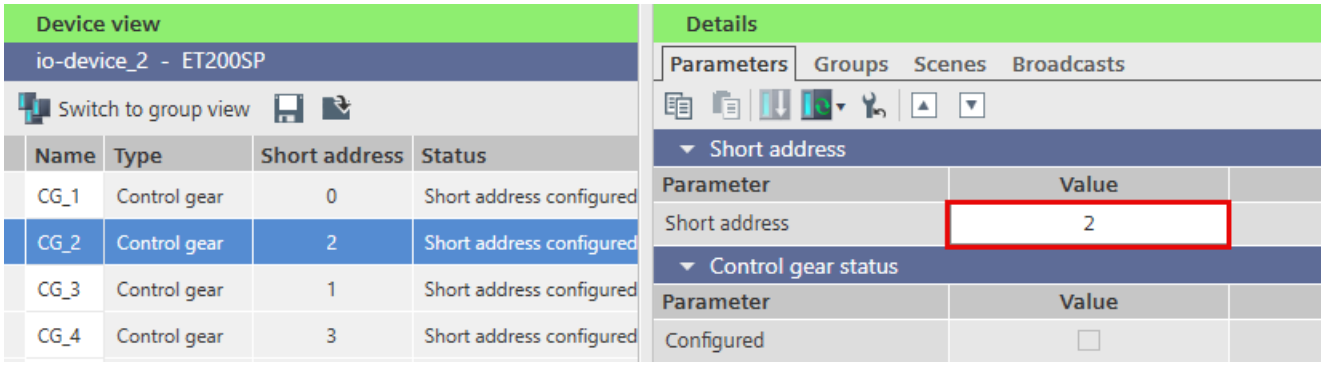
Read out and transfer parameters

You can display, change or transfer the parameters of a DALI device on the "Parameters" tab. For example, to change the short address of a DALI device, proceed as follows:

1. Select a device in the device view.
2. Change the value of the short address in the "Details > Parameters tab" area. The field with the changed value is highlighted in yellow.
3. Click the button Start transfer to transfer the changed parameters.



Result: The parameters have been successfully transferred and the result is displayed accordingly.



NOTE

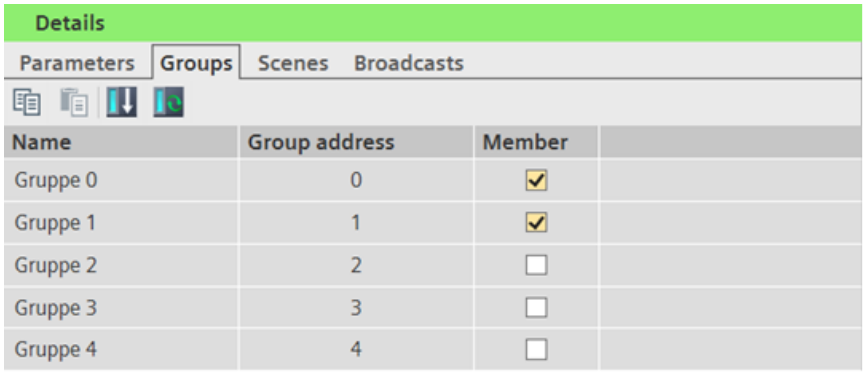
Replacing existing addresses

f the newly assigned address already exists within the address range, the addresses are replaced as follows:
The DALI device that is currently assigned this address receives the address of the device to which the new address was assigned.

Manage groups

Multiple devices can be configured and addressed simultaneously with the help of groups. To assign the devices to different groups, proceed as follows:

1. Select a device in the device view.
2. Switch to the "Details > Groups tab" area.
3. In the "Member" column, select the groups to which you want to add the selected device. In the figure below, the selected device was added as a member of groups 0 and 1.



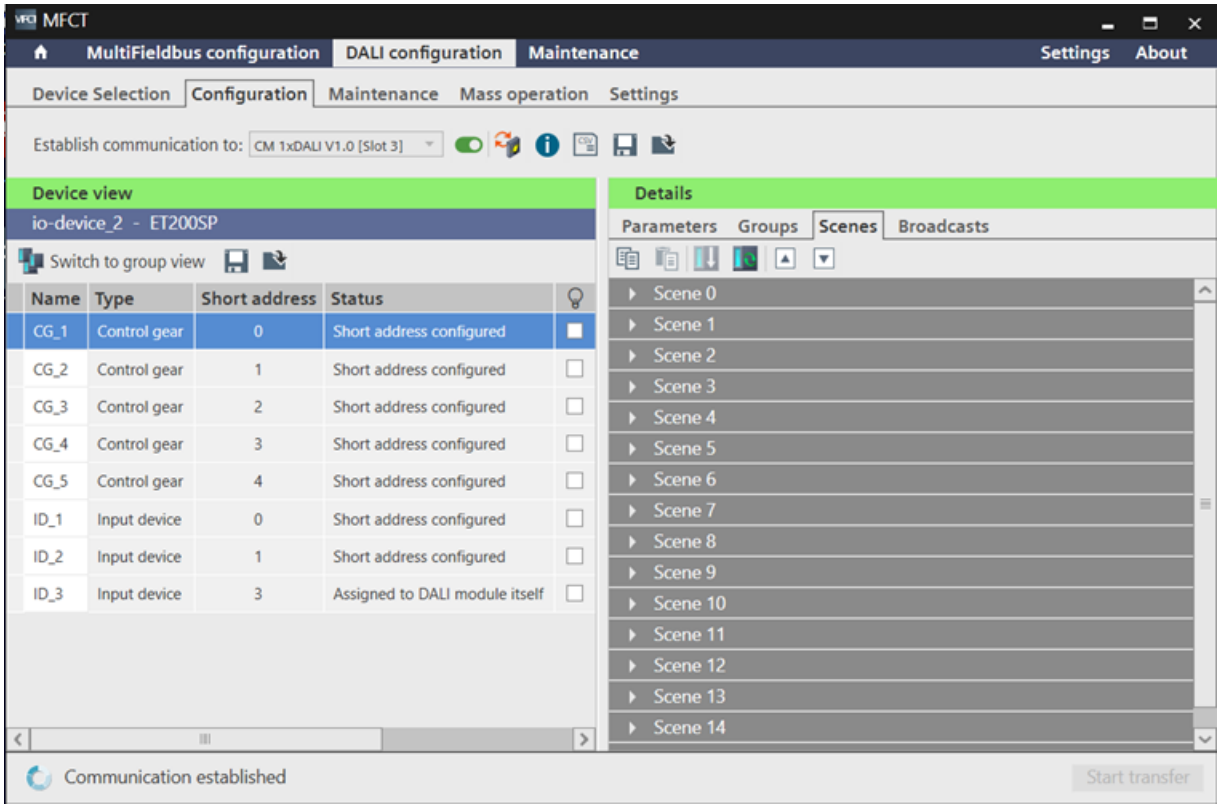
4. Click the button Start transfer to transfer the selected changes.

Edit scenes

Scenes are predefined value settings stored in the device and can be activated via a control command.

To edit the scene of a device, proceed as follows:

1. Select a device in the device view.
2. Switch to the "Details > Scenes tab" area.
3. To open the context menu, right-click in the "Scenes" area.
4. Select "Add scene".

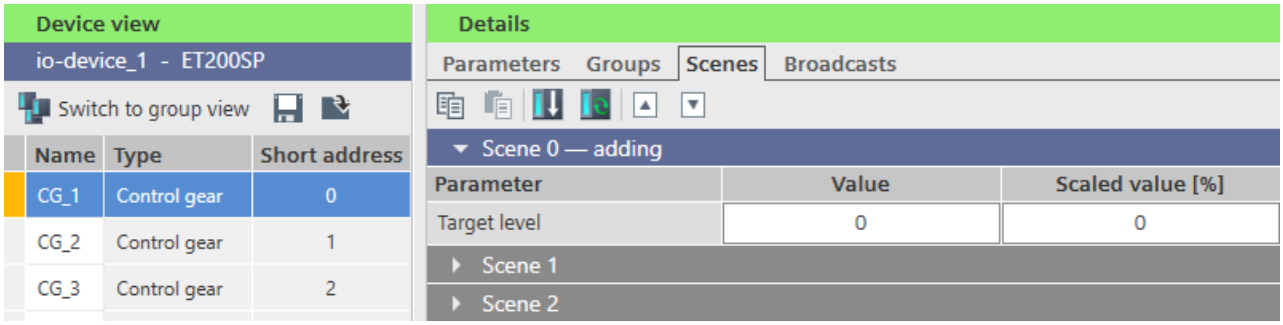


The context menu offers the following additional options

- Rename scenes
- Add all scenes
- Remove all scenes

5. For a scene stored in the device, you have the following options:
   - Activate scene
   - Remove scene

6. Optionally, you can specify the target value of the scene for the selected device.
   To do this, enter a value between 0 and 255 in the "Value" field. Depending on the type of DALI device used, you can also specify a color value for the scene.



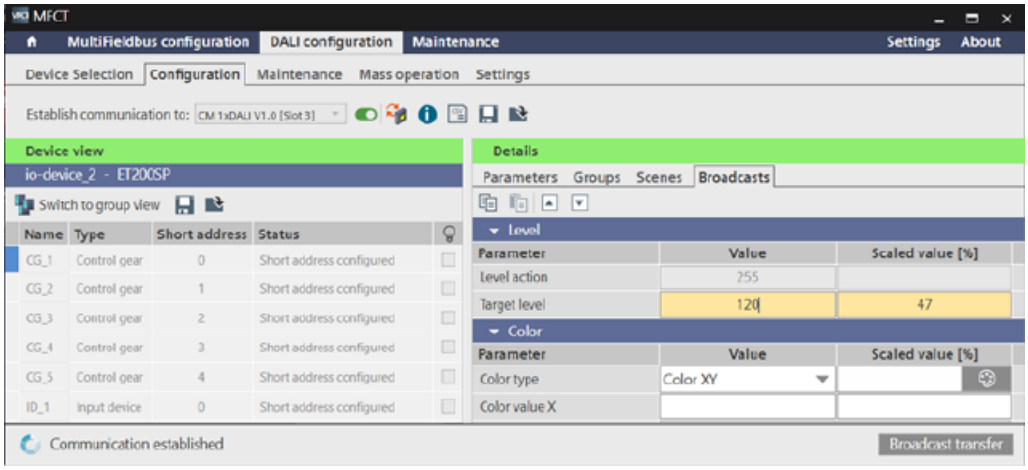
7. Click the button Start transfer to transfer the changed parameters.

Result: The parameters have been successfully transferred and the result is displayed accordingly.

Send broadcasts

To broadcast to all DALI devices, proceed as follows:

1. Select a device in the device view.
2. Switch to the area "Details > Broadcasts tab".
3. For example, change the target level in the "Value" area.
   The figure below shows an example of setting the brightness of all DALI devices on the bus to 47%:



4. Click the button "Broadcast transfer" to transfer the changed parameters.

Result: The parameters have been successfully transferred and the result is displayed accordingly.

8.4.1.2 Group view

To switch to the group view, click the "Switch to group view" button .

You have the following options for the control gear in the group view in the "Details" area:

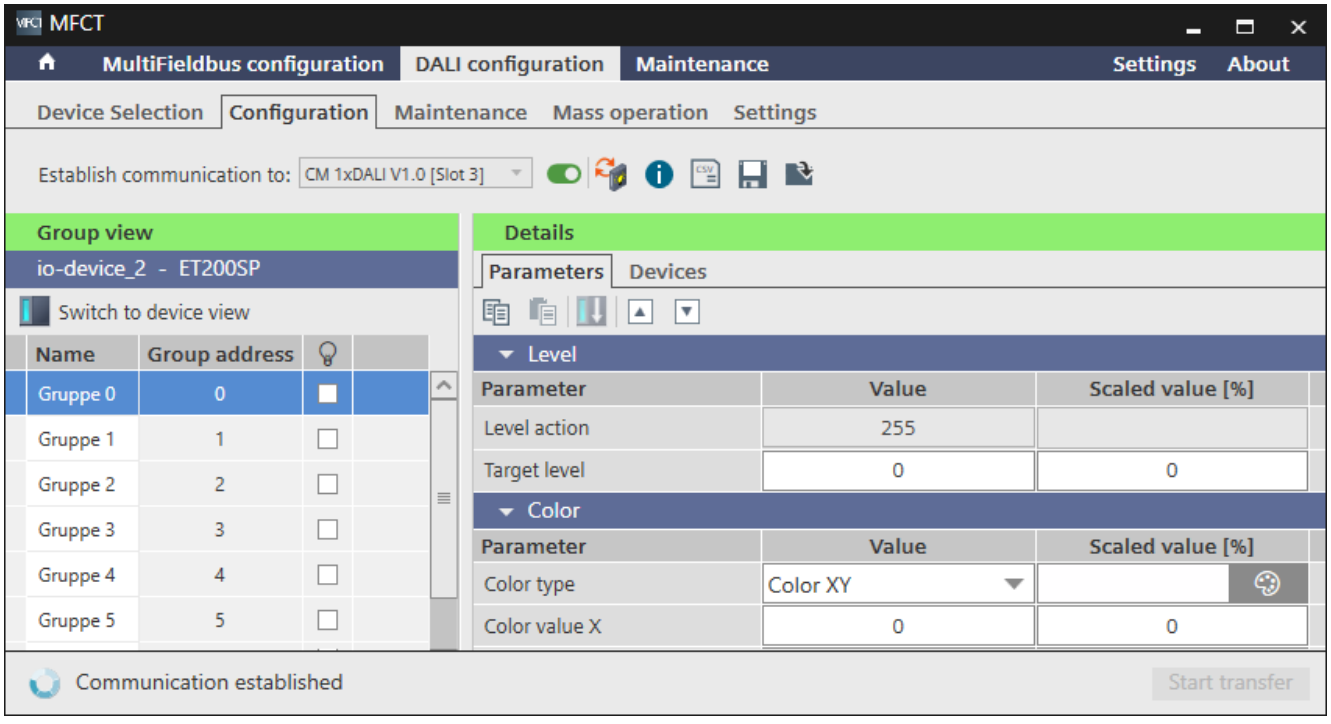
- Transfer parameters to groups
- Manage group members

Parameters that have been changed but not yet transferred are highlighted in yellow.

Transfer parameters

You can send commands to all members of a group in the "Details > Parameters tab" area.

1. Select a group in the group view.
2. Enter the required values in the "Parameters" tab.
3. Click the button Start transfer to transfer the selected changes.



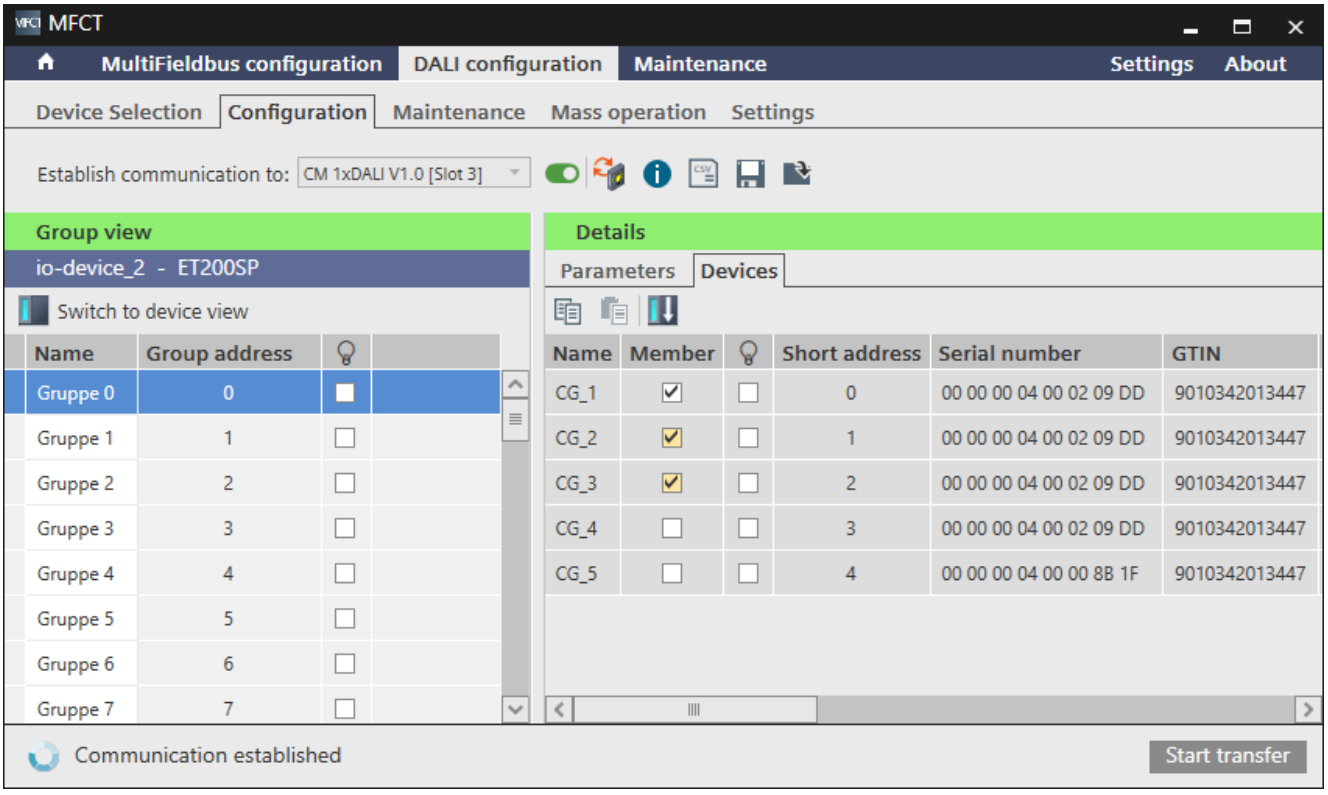
Manage group members

You have the following options in the "Details > Devices tab" area:

- Identify the individual group members. To do this, select the check box in column with the light bulb icon .
- Display, add and delete group members

For example, to add devices to a group. proceed as follows:

1. Click the desired group in the group view.
2. In the "Member" column on the "Devices" tab, select the check boxes of the devices you want to add to the group.
3. Click the button Start transfer to transfer the changed parameters.



Result: The parameters have been successfully transferred and the result is displayed accordingly.

If you want to check the result, select the check box of the corresponding group under the light bulb icon in the "Group view" section. This identifies all group members at once.

8.4.2 Input devices

DALI input devices can contain multiple instances under a single short address. The "Details" area shows a separate set of parameters for each instance. You can read out and transfer parameters.

Parameters that have been changed but not yet transferred are highlighted in yellow.

Read out and transfer parameters

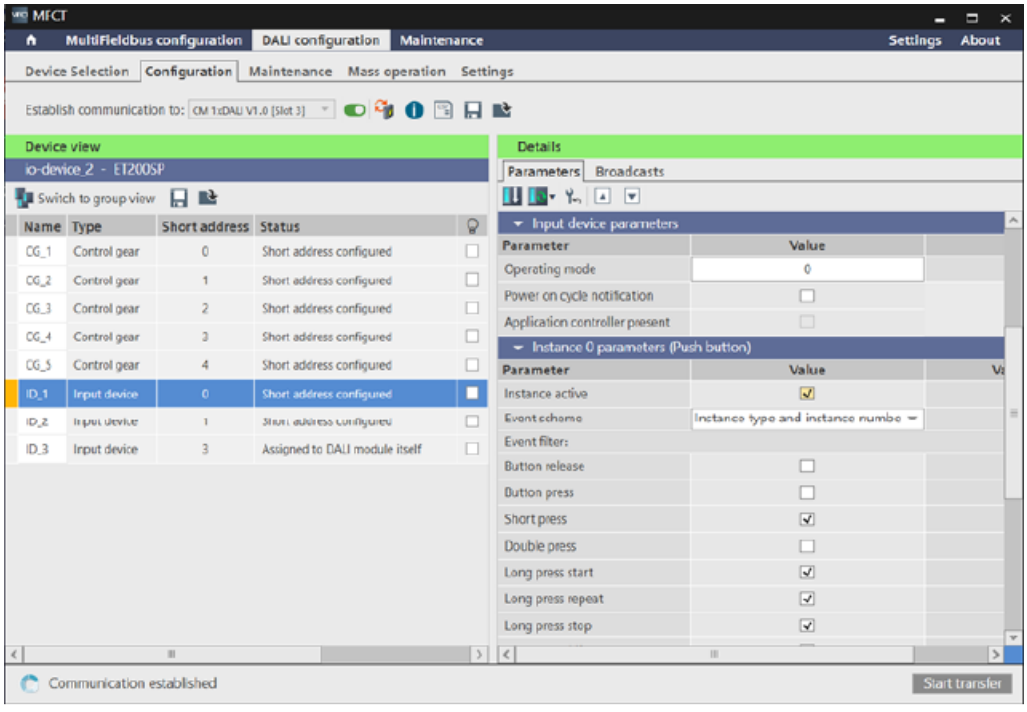
The parameters available depend on the instance type. The image below shows an example of the parameters of the "Push button" instance type.

You have the following options for the sensor instances in the "Parameters" tab:

- Activate
- Display
- Change
- Transfer

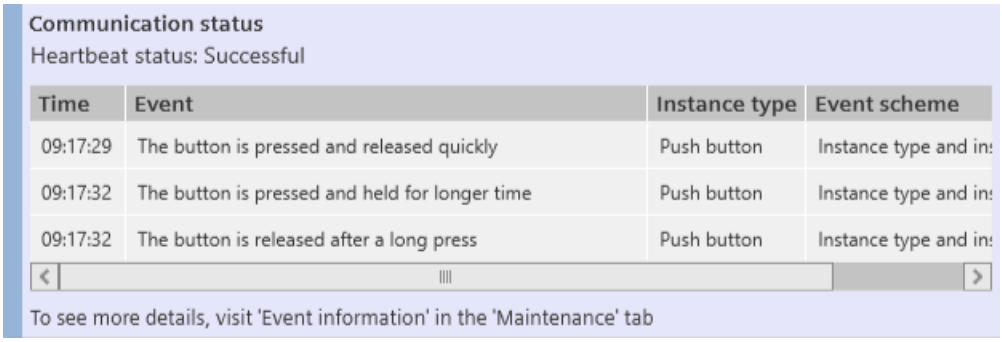
For example, to activate an instance, proceed as follows:

1. Select a device in the device view.
2. In the "Details > Parameters tab" section, open the desired instance, e.g., "Instance 0 Parameters (push button)".
3. Select the "Instance active" check box. The field with the changed value is highlighted in yellow.
4. Click the button Start transfer to transfer the changes.



Result: The changed parameters have been transferred to the selected input device.

If you want to verify the messages of the input devices, click the "Communication status" button . You then see the frames received from the CM 1xDALI module. This enables pushbutton events, for example, to be verified.



NOTE

Avoid simultaneous access attempts

An active DALI CTRL block accesses a DALI module in the user program of a CPU. At the same time, you want to access a DALI module with the MFCT. If the CPU is already communicating with the DALI module, the event is not displayed by the MFCT. The reason for this is that only the communication partner that first communicates with the DALI module after the message occurs receives the data. Either the CPU or the MFCT.

8.5 Maintenance

You can implement and process various commands with the DALI module on the "Maintenance" tab.

The sections below provide information on the following:

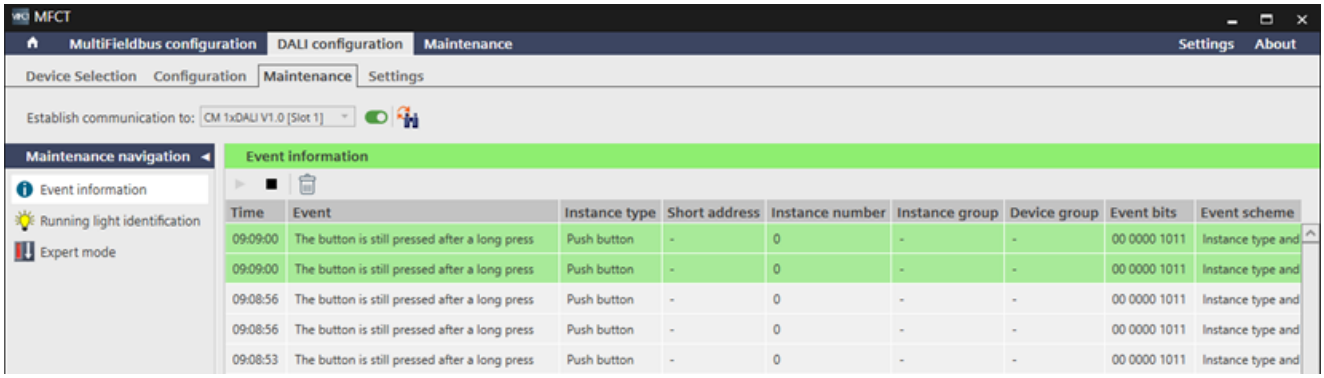
- Event information (Page 71)
- Running light identification (Page 72)
- Expert mode (Page 73)

8.5.1 Event information

Input devices compliant with the DALI-2 standard can actively report events on the DALI bus. These events are received by the CM 1xDALI and can be recorded by the control unit or the MFCT.

You control the function with the Start/Stop commands ▶ ■. You clear the window by clicking the button 🗑.

The following figure shows an example of received events on the DALI bus.



NOTE

Avoid simultaneous access attempts

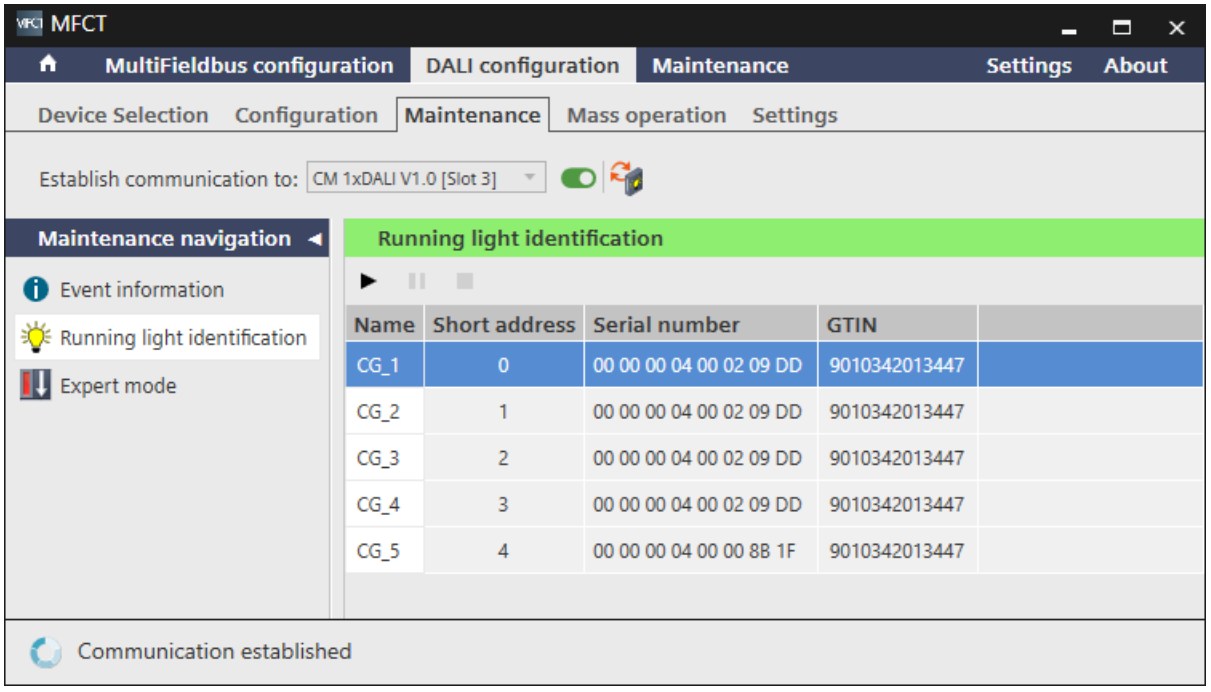
An active DALI CTRL block accesses a DALI module in the user program of a CPU. At the same time, you want to access a DALI module with the MFCT. If the CPU is already communicating with the DALI module, the event is not displayed by the MFCT. The reason for this is that only the communication partner that first communicates with the DALI module after the message occurs receives the data. Either the CPU or the MFCT.

8.5.2 Running light identification

With the running light identification, you start a running light to identify the individual devices. For this purpose, the dimming values of the individual lights are set to 0 and then switched on one after another. After the running light function, the lights are returned to their original dimming value.
This makes it easy to check the arrangement of the short addresses once commissioning is complete. You can also monitor the progress of the running light identification in the list of existing short addresses.

You control the function using the Start, Pause and Stop buttons ▶ ⏸ ■.

You configure the duration and speed of the identification, for example, on the "Settings" tab. You can find more information in section Settings (Page 78).



8.5.3 Expert mode

Expert mode is a function in the "Maintenance" area of the DALI configuration and offers options, such as:

- Direct access to the DALI bus with free single frames
- Creation and sending of specific frame sequences

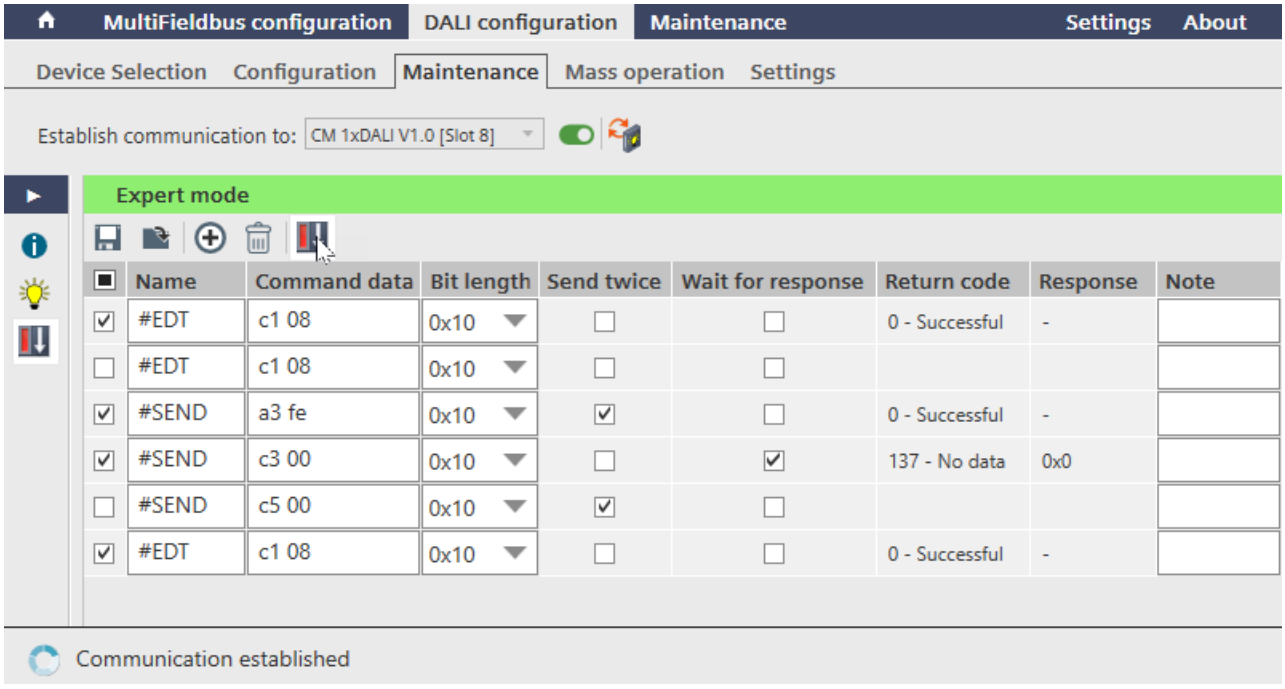
Requirement
For MFCT versions up to V1.5 SP3: You must be connected online to the DALI module.
As of MFCT version V1.5 SP4: You can also use expert mode without a connected DALI module and create or save frames.

Procedure - Creating and sending command data

To create and send a sequence of frames with command data in expert mode, proceed as follows:

1. Use the "Plus" and "Recycle bin"  buttons to add entries or remove all entries.
   Use the "Save" and "Open" buttons  to load a preconfigured sequence of frames or to save the sequence you created.
2. In the first table column, select which frames you want to send to the DALI bus.
3. In the selection menu, select the bit length in each entry to be sent.
4. Edit the command data in each frame to be sent.
5. Optional:
   - To send the command twice, select the "Send twice" option.
     Some configuration commands for DALI require repetition of the frame for successful execution.
   - To wait for the response from a device connected to the DALI bus, select the "Wait for response" option.
     A received response is shown in the corresponding row in the "Response" column.
   - Enter a meaningful name in the "Name" column and a note for the entries in the "Note" column.

6. Click the "Download" button .
   The transfer to the DALI bus starts and the created list is processed.



Result: You have configured the command data and transferred it to the DALI bus. The columns "Return code" and "Response" show the results of each row.

NOTE

Avoid simultaneous access attempts

An active DALI CTRL block accesses a DALI module in the user program of a CPU. At the same time, you want to access a DALI module with the MFCT. If the CPU is already communicating with the DALI module, the event is not displayed by the MFCT. The reason for this is that only the communication partner that first communicates with the DALI module after the message occurs receives the data. Either the CPU or the MFCT.

More information

You will find additional information on how to construct the command frames in the IEC 62386 standard and in the DALI device's manual.

8.6 Mass operation

As of MFCT version V1.5 SP4, the "DALI configuration" application includes the mass operation function. The mass operation feature allows you to edit multiple DALI devices across several DALI modules at the same time. The individual DALI modules may also be distributed across different ET 200SP stations.

In the mass operation, you search the network for devices that are accessible online and then select the desired DALI modules. This MFCT scans the selected DALI modules and automatically assigns short addresses to the connected devices. You can change the automatically assigned short addresses in the results list as required and reassign them to the connected devices of all DALI modules.

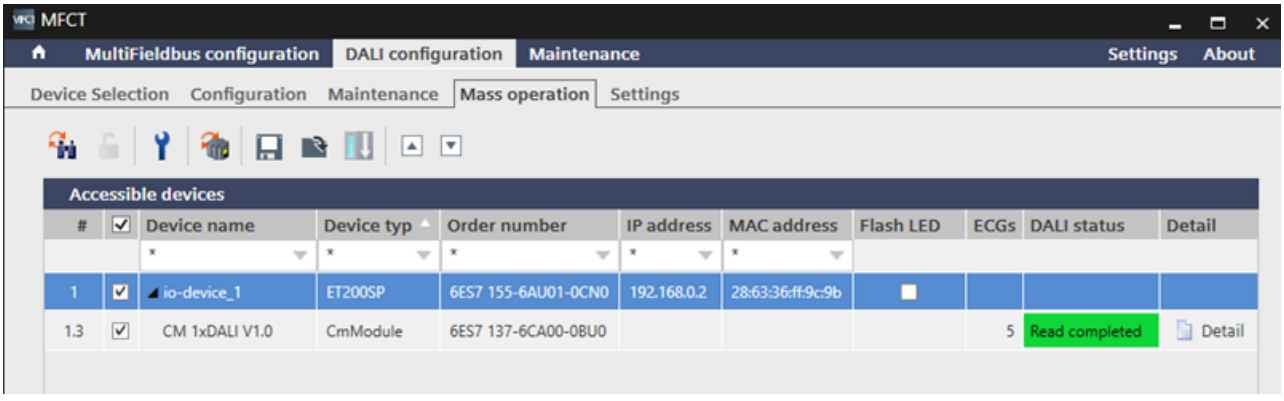
You can also export and save the results list locally as a CSV file. In the CSV file, you can assign pre-defined short addresses to the DALI devices based on the serial numbers or assign the DALI devices to a group. When editing the CSV file, you do not need a connection to the DALI modules.
If you are connected to the DALI modules, you can load the edited CSV file in the MFCT and load the changes into all the desired DALI devices.

You can find the mass operation as a tab in the "DALI configuration" application.

Procedure - Starting the mass scan

To start the mass scan for online-accessible DALI modules, proceed as follows:

1. Select the "Settings" tab in the "DALI configuration" application.
   The MFCT shows the settings for the DALI scan.
2. Select only the settings required for the DALI scan in order to keep the duration of the scan to a minimum.
   You can find information in section Settings (Page 78).
3. Select the "Mass operation" tab in the "DALI configuration" application.
4. Click the "Start scan" button .
   The MFCT shows the online-accessible devices as a list under "Accessible devices".
5. Select the desired DALI modules for the mass operation from the list.
6. Click the "Start mass scan" button .
   The MFCT scans the selected DALI modules and automatically assigns short addresses to the connected DALI devices. The "DALI status" column shows the progress for the respective DALI module.



Result: You have scanned the desired DALI modules. The "DALI status" column shows the progress as "Read completed" next to the modules. In the "Detail" column, you can find a list of the results of all DALI modules and the connected DALI devices for further processing.

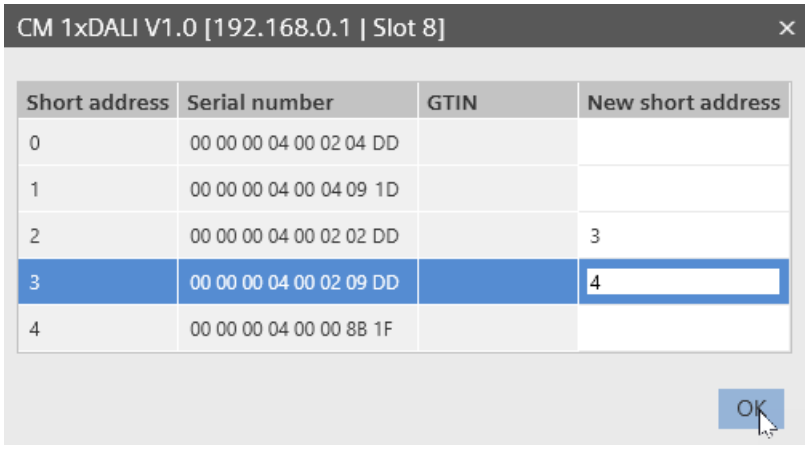
Procedure - Configuring short addresses online

Requirements:

- You have scanned the desired DALI modules.
- The "Detail" column shows a list of the results of the mass scan.

To configure the automatically assigned short addresses online, proceed as follows:

1. Click the list in the "Detail" column.
   The MFCT opens the list in a new window. The list shows the automatically assigned short address next to each serial number of the DALI device.
   – If you also want to read out the GTIN code, you must first enable the corresponding option in the Settings (Page 78).
2. Assign the desired short address to the devices in the "New short address" column.



3. Click the "OK" button.
   The MFCT closes the list and shows in the "DALI status" column that parameters have been changed.
4. Click the "Load changed parameters into the devices" button.
   The MFCT automatically loads the newly assigned short addresses into the DALI devices.

Result: You have changed the automatically assigned short addresses and loaded them into the DALI devices.

Procedure - Saving results list locally and configuring offline

Requirements:

- You have scanned the desired DALI modules.
- The "Detail" column shows a list of the results of the mass scan.

To save the results list locally, proceed as follows:

1. Click the "Save" button.
   The MFCT opens the "Save as" window.
2. Select the storage location for the file in Explorer.
3. Assign a name for the file.
4. Select the file type CSV.
5. Click "Save".

Intermediate result: You have saved the results list locally as a CSV file.

To configure the short addresses offline, proceed as follows:

1. Open the CSV file.
   The CSV file shows all the information about the DALI modules and the DALI devices connected to them.
2. Assign a new short address to the devices in the "New short address" column.
3. Save the changes to the CSV file.

Result: You have configured the short addresses offline in the CSV file.

Procedure - Loading results list as CSV file

Requirements:

- You have saved the results list locally on your PC as a CSV file and configured the short addresses.
- The MFCT is open and shows the "Mass operation" function in the "DALI configuration" application.

To upload the CSV file with the changes, proceed as follows:

1. Click the "Open" button.
   The MFCT opens the "Open" window.
2. Select the CSV file to be opened.
3. Click the "Open" button.
   The MFCT closes the "Open" window and loads the results list.

Intermediate result: You have loaded a results list as a CSV file.
Optionally, you can open the configuration again in the "Data" column and change the short addresses in the "New short address" column. If you have changed short addresses and close the list, the MFCT shows in the "DALI status" column that parameters have been changed.

To load the changed short addresses into the DALI devices, proceed as follows:

1. Click the "Load changed parameters into the devices" button.
   The MFCT automatically loads the newly assigned short addresses into the DALI devices.

Result: You have loaded the changed short addresses into the DALI devices.

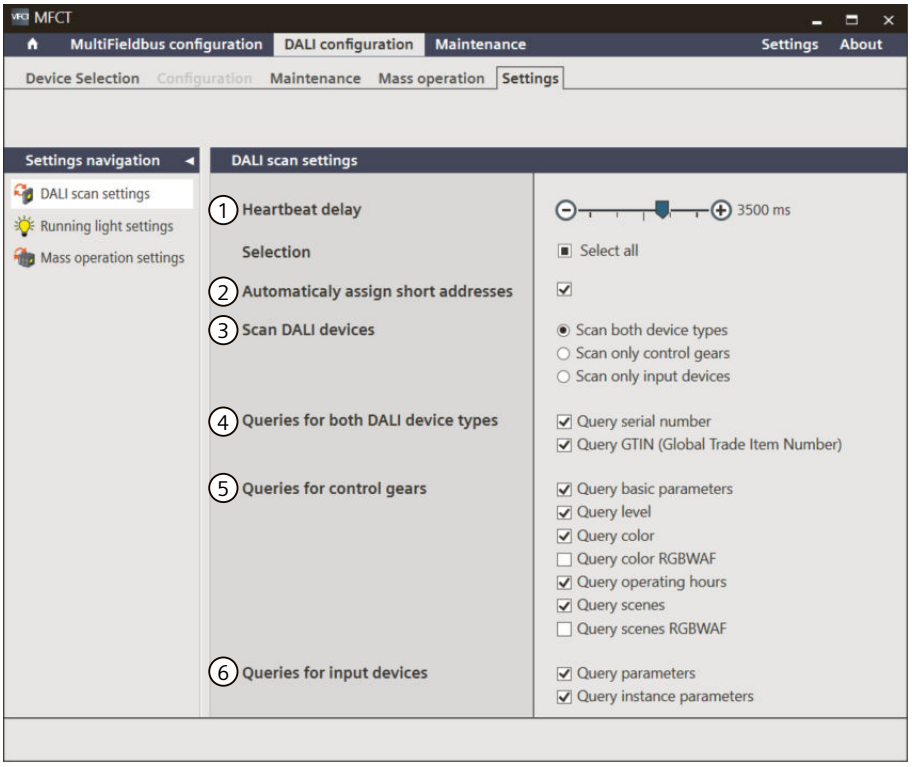
8.7 Settings

You can make various modifications to the following on the "Settings" tab:

- Basic configuration of the DALI scan
- Configuration of the running light for identification
- Parallel processing for the mass operation

Basic configuration of the DALI scan

Select the entry "DALI scan settings" in the "Settings navigation" column.



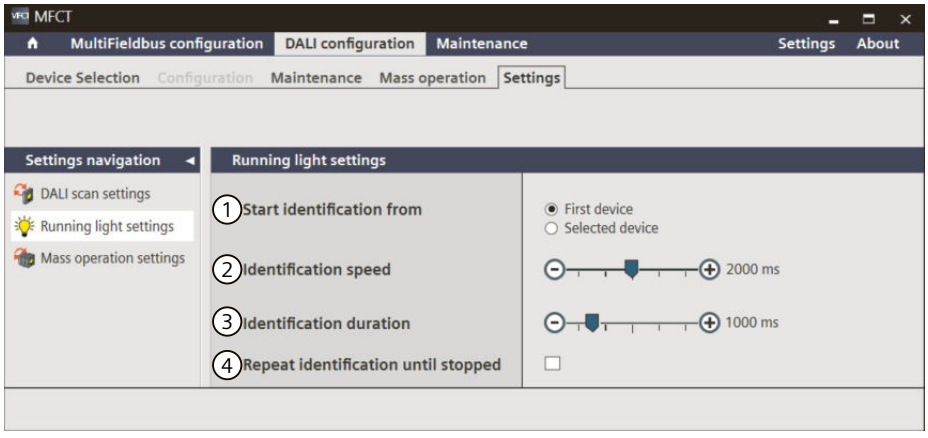
①	Heartbeat delay	Setting for the maximum time between two DALI frames to maintain communication.
②	Automatically assign short addresses	Specifies whether unaddressed devices on the DALI bus are automatically assigned an address.
③	Scan DALI devices	Specifies whether the MFCT should scan for control gear, input devices or all types on the bus.
④	Queries for both DALI device types	Specifies whether the GTIN code (Global Trade Item Number) and/or serial number should be queried for each device.
⑤	Queries for control gear	Specifies the parameters to be read out from the control gear.
⑥	Queries for input devices	Specifies the parameters queried for the input devices.

NOTE

A multiple selection is possible for items 4 to 6.
The more parameters that are queried, the longer the scan will take.

Configuration of the running light for identification

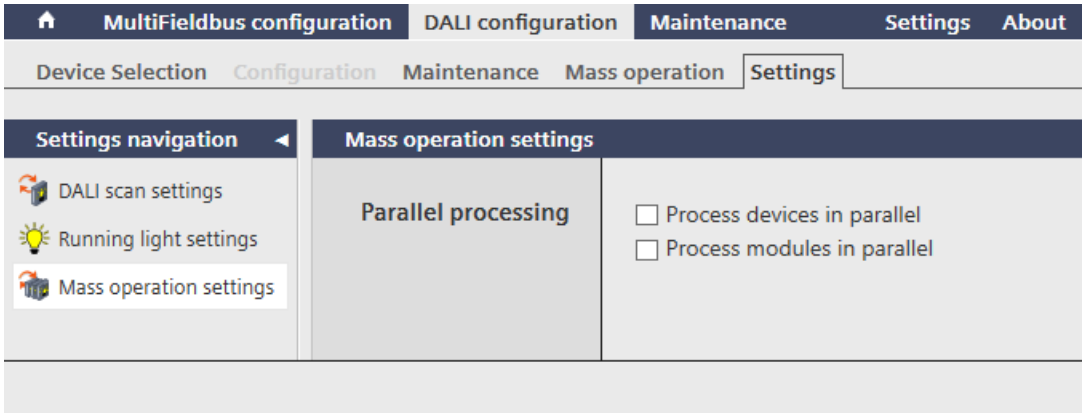
Select the entry "Running light settings" in the "Settings navigation" column.



①	Start identification from	Specifies where the identification should start: • Selected device • Lowest address on the bus
②	Identification speed	Changeover time from one connected lamp to the next.
③	Identification duration	How long each controlled lamp should be lit.
④	Repeat identification until stopped	Activates the identification in an endless loop until manually stopped.

Parallel processing for the mass operation

Select the entry "Mass operation settings" in the "Settings navigation" column. You can activate parallel processing for devices and/or modules.



TM FAST

9

The TM FAST application is available as a plug-in in the MFCT. To use the TM FAST application, activate the plug-in.

Once you have activated the plug-in, you can find the TM FAST on the start page as an application. In an opened application, you can find the TM FAST as a tab in the area of the button for the start screen.

You can generate the following in the TM FAST application:

- A UPD file (**Upd**ate file)
- A DB file (**D**ata**b**lock file)

In this case, you use the UPD file to load the TM FAST application. You perform loading using the MFCT or the TIA Portal.

You use the DB file in STEP 7 (TIA Portal) to write the user logic from the user program of the CPU to a TM FAST module.

More information

You can learn how to activate a plug-in in section Plug-ins (Page 33).

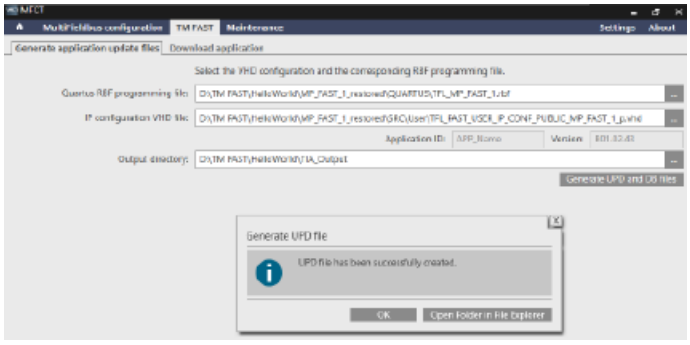
You can get detailed information on the TM FAST module in the technology module TM FAST equipment manual (https://support.industry.siemens.com/cs/us/en/view/109816087).

You can find an application example for handling DB files in the following Internet entry (https://support.industry.siemens.com/cs/ww/en/view/109823442). This application example shows how to load and activate a TM FAST application from a SIMATIC CPU to the TM FAST module. This enables you to replace a module without additional tools such as TIA Portal or the MFCT.

9.1 Generating UPD and DB files

To generate UPD or DB files with the TM FAST application, proceed as follows:

1. Generate the Raw Binary File *.rbf and the VHD file *.vhd from the development environment for programming the FPGA application logic (Quartus® Prime Software).
2. Select the path to your RBF file in the "Quartus RBF programming file" field.
3. Select the path to your VHD file in the "IP configuration VHD file" field.
4. Select the folder in which the generated files are to be stored in the "Output directory" field.
5. After successful creation of the UPD and DB files, the following dialog is displayed as confirmation.



The result is that you will find the following files in the selected output directory:

- 6ES7 554-1AA00-0AB0 APP_Name_UserLogic_B01.02.43.upd
- APP_Name.db

You need the UPD file to load the user program created in Quartus® Prime using the MFCT or the TIA Portal.

More information

The DB file can be imported into STEP 7 (TIA Portal) as an external source and interconnected with the function block "CheckUserlogicdata". More information can be found in the following Internet entry (https://support.industry.siemens.com/cs/us/en/view/109817062).

9.2 Download UPD files

Transferring UPD file to a TM FAST module

You can transfer the UPD file to a TM FAST module on the tab "Download application > Device view area". To do so, proceed as follows:

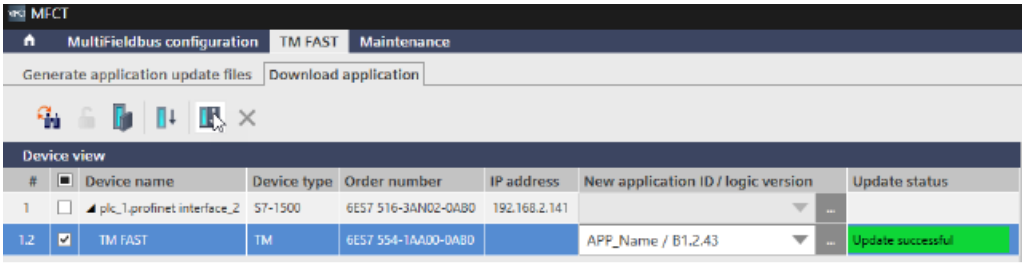
1. Click the "Start scan" button to display all accessible devices of the preset network interface.

NOTE

To find all modules in the central configuration, select the "Inclusion of central working modules" check box under "Communication with CPUs" in the general settings.

You can find more information in section General settings (Page 30).

2. Click the button to sort by devices with TM FAST modules.
3. In the "New application ID/logic version" column, select the TM FAST user logic (*.upd) for the update.
4. Click the button to start the download.



Result: You have started the download of the UPD file. You can see the progress of the update in the "Update status" column.

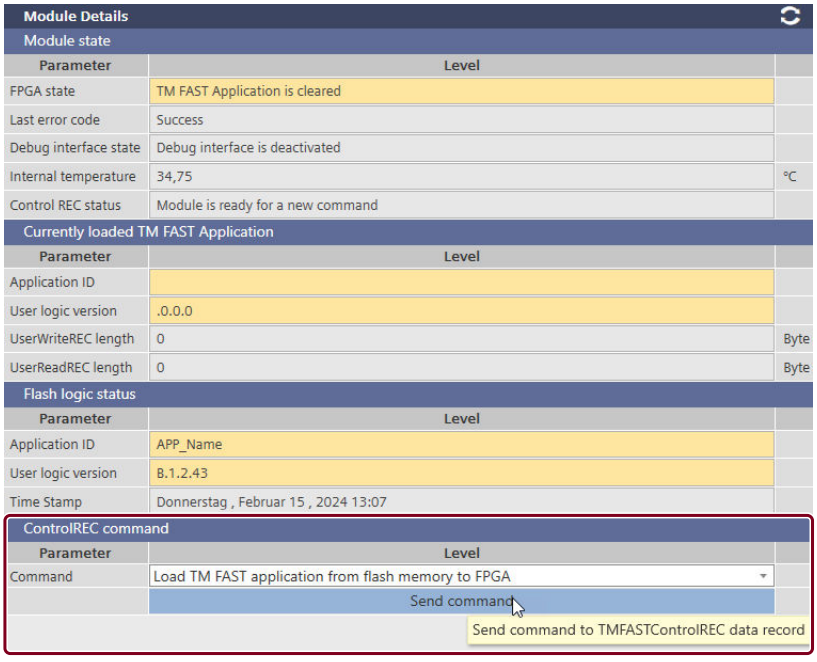
Loading and activating the application

In the "Module details" area, you see that the new TM FAST user logic has been loaded into the flash memory:

- Application ID: "APP_Name"
- User logic version: "B1.2.43".

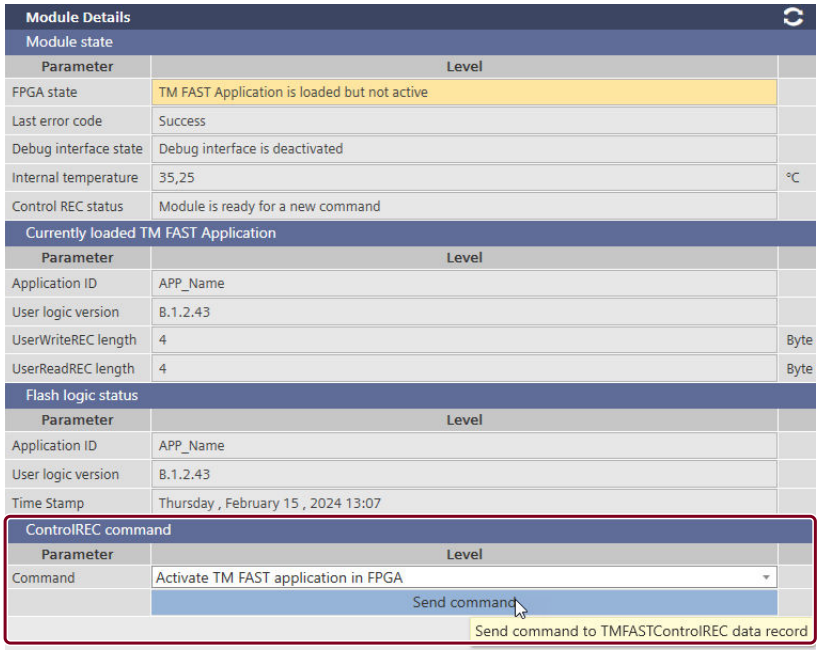
To load the application into the FPGA and activate it, proceed as follows:

1. Select the command "Load TM FAST application from flash memory to FPGA" in the "ControlREC command" area.
2. Click the "Send command" button.

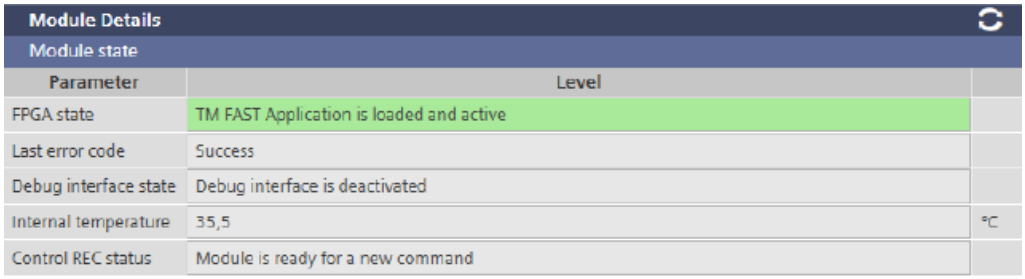


3. Select the command "Activate TM FAST application in FPGA" in the "ControlREC command" area.

4. Click the "Send command" button.



Upon successful activation, you will get the following message:



5. Enable the following parameters in the hardware configuration of the module:
   - Load TM FAST application during startup
   - Always activate TM FAST application

Result: You have loaded the application to FPGA and activated it. The application starts up automatically after a restart.

SIWAREX

10

The "SIWAREX" application is available as a plug-in in the MFCT. To use the "SIWAREX" application, activate the plug-in.

Once you have activated the plug-in, you can find SIWAREX on the start page as an application. In an opened application, you can find SIWAREX as a tab in the area of the button for the start screen.

You search the connected network for TM SIWAREX WP3x1 modules in the "SIWAREX" application. You have the following options for the found modules:

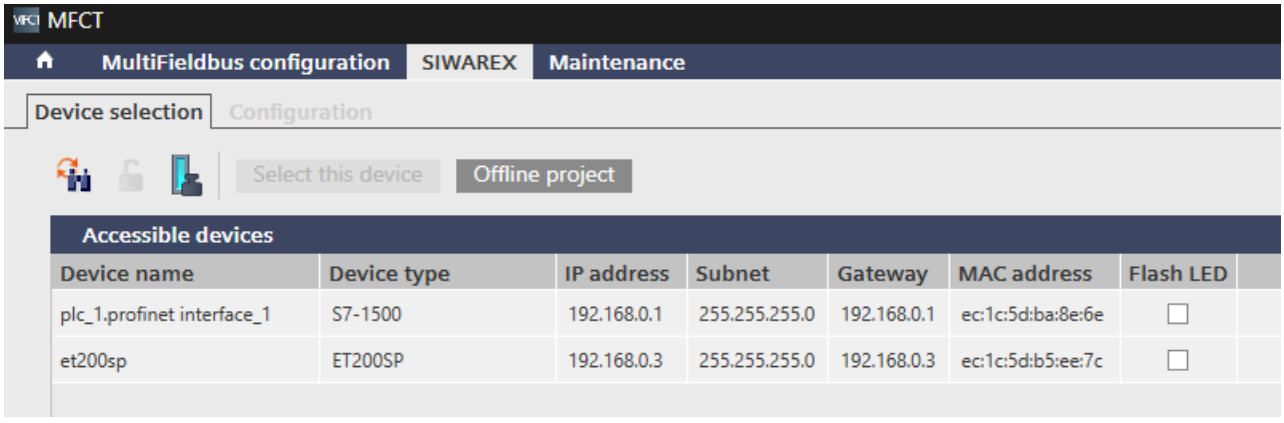
- Edit parameters
- Read, write or monitor data records

You can learn how to activate a plug-in in section Plug-ins (Page 33).

10.1 Scanning for SIWAREX assemblies

You scan for devices with connected SIWAREX modules on the "Device selection" tab. To do so, proceed as follows:

1. Click the "Start scan" button to search for accessible devices.



2. Optional: Click the "Set filter" button to show only the devices with connected SIWAREX WP3x1 modules.
3. Select the desired device in the selection list.
   If the ET 200SP station has multiple SIWAREX modules but you only want to select one of them, click its check box.

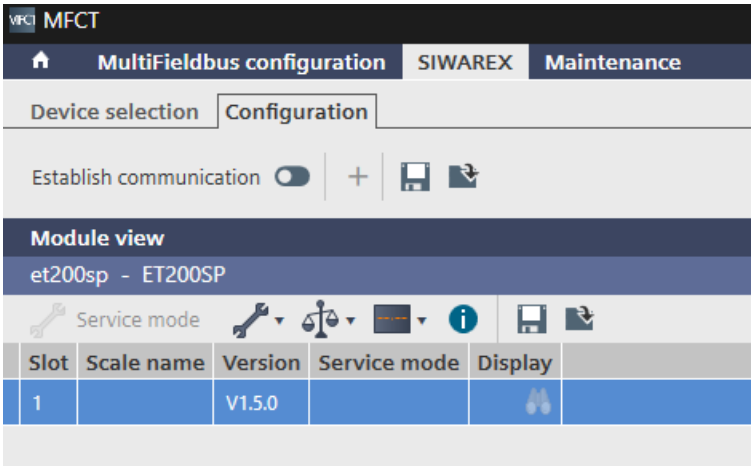
Result: You have scanned the network and selected the desired device. When you click the button Select this device, the station view opens.

Editing data offline

If you want to open and read backup files without an online connection, click the button Offline project. You can also prepare and store the parameters offline and transfer them to the modules later.

10.2 Setting up communication in the station view

You establish the communication with the SIWAREX module on the "Configuration" tab.

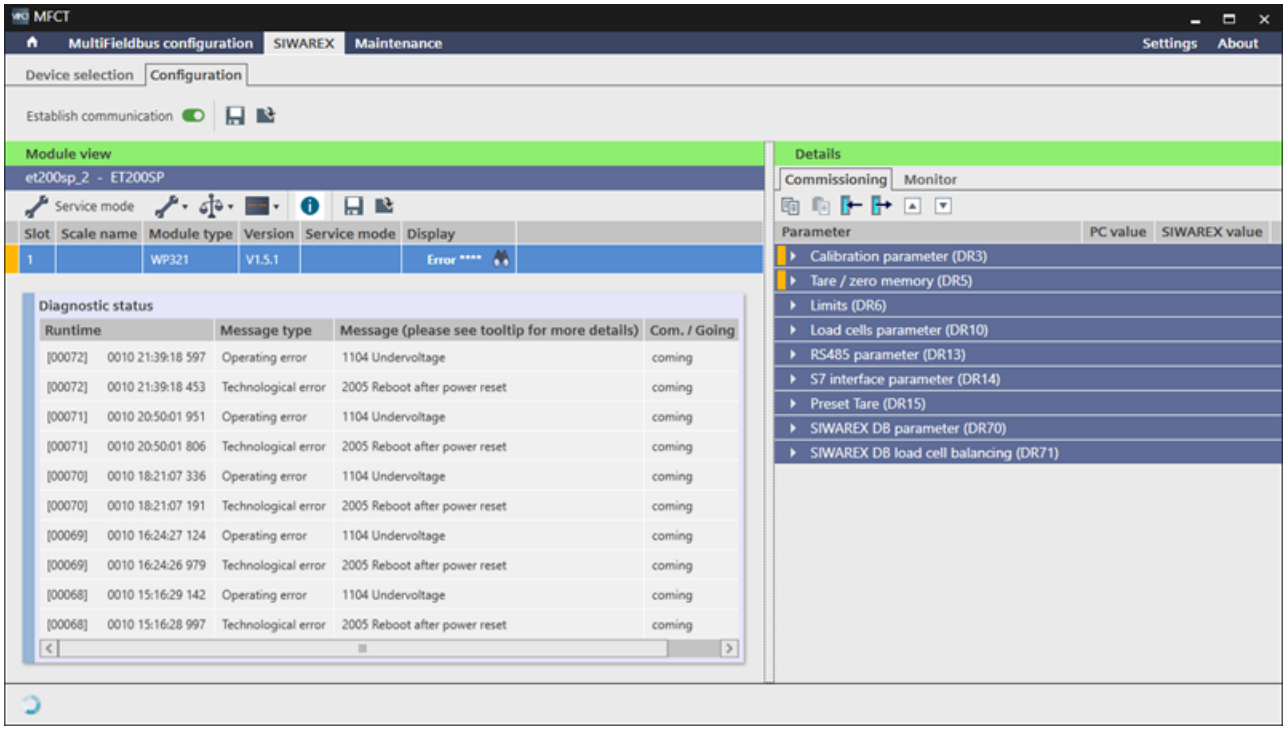


To establish the communication between the MFCT and the SIWAREX module, click the button Establish communication in the station view.

Result: The module view displays a list of all WP3x1 modules in the station.

10.3 Working in the station view

You can make different configurations on the "Configuration" tab. The figure below shows an example of the two areas "Module view" and "Details". You can find a detailed explanation of the icons in the following table.



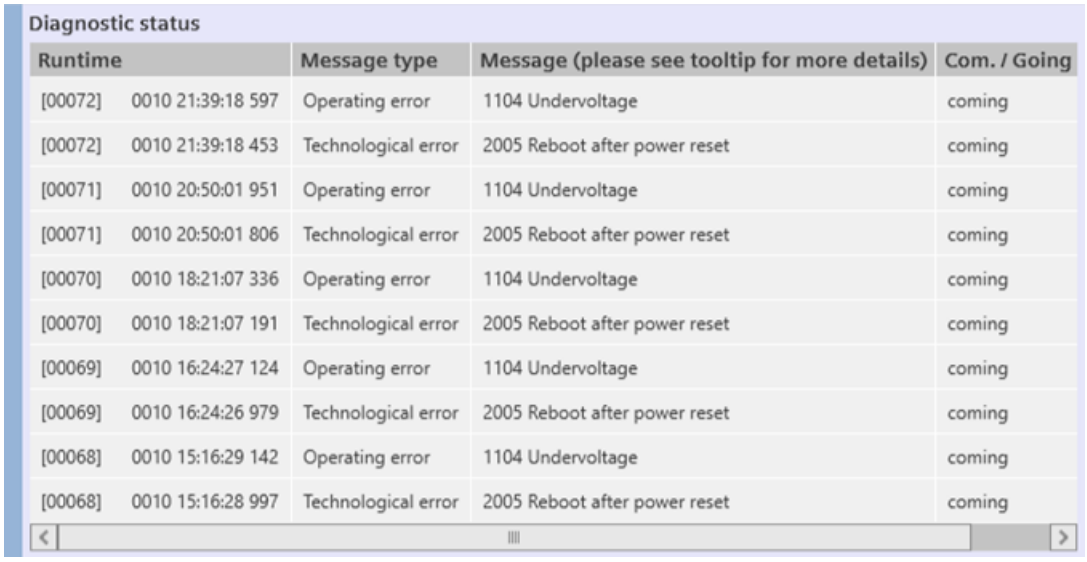
"Module view" area

	"Configuration" area: Create backup of the currently selected module. "Module view" area: Open/store configurations within the station.
	Activate/deactivate service mode.
	Execute service commands
	Execute scale commands
	Execute display commands
	Show diagnostics status Click the button to open the error buffer of the module.

Area "Details > Commissioning tab"

	Send data records from the MFCT to the module. You can only click the button if the PC values and the SIWAREX values are different from each other.
	Read in data records from the module to the MFCT.
	Open pop-up window with a strongly magnified weight display.

You see the error buffer of the module in the "Diagnostic status" display.



More information

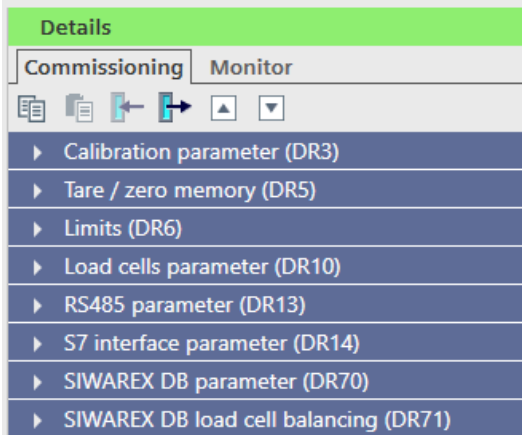
You can find more information on the commands and parameters in the respective equipment manuals.

- TM SIWAREX WP321 (https://support.industry.siemens.com/cs/ww/en/view/109770838)
- TM SIWAREX WP341 (https://support.industry.siemens.com/cs/ww/en/view/109813264)
- TM SIWAREX WP351 (https://support.industry.siemens.com/cs/ww/en/view/109825886)

10.4 Commissioning and monitoring

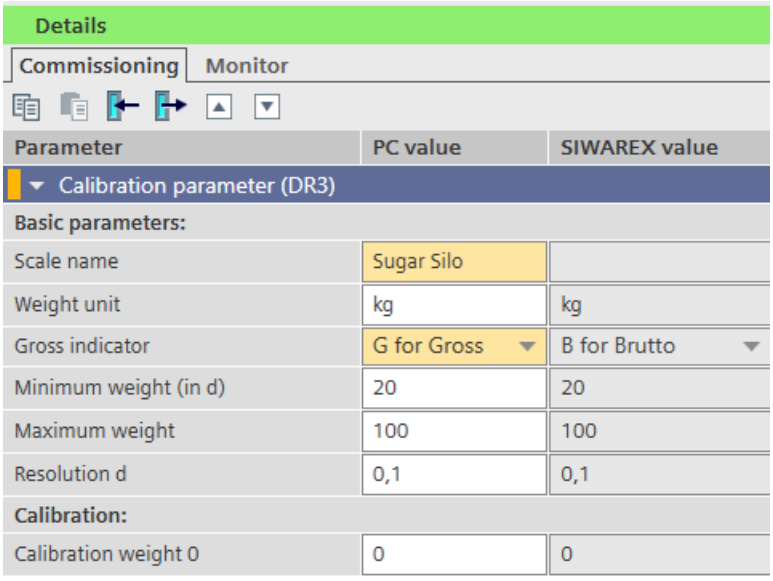
Commissioning

In the "Details > Commissioning tab" area, you can view the module's data records and edit their parameters.



To change, for example, the adjustment parameters in data record 3 (DR3) of the SIWAREX WP321 module, proceed as follows:

1. Click the button to read all data records from the WP321 module into the MFCT.
2. Change the desired parameters.
   Parameters that have been changed but not yet transferred are highlighted in yellow.



3. Click the button to write all data records from the MFCT to the WP321 module.

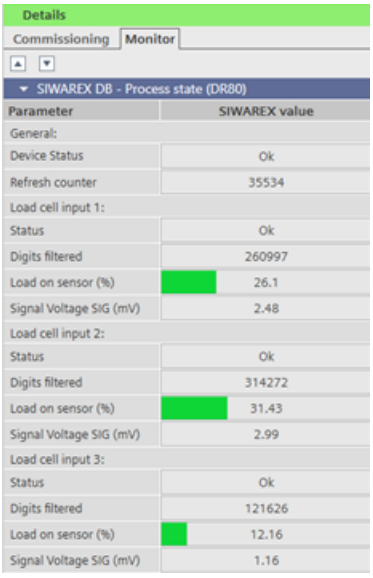
Result: The changed parameters have been transferred to the WP321 module.

You can expand or collapse all parameters by clicking the button .

A right-click in the "Parameters" area opens a context menu with further options for managing data records.

Monitoring

You can read-access and monitor all process data on the "Monitor" tab.



PtP Event Trace

11

The PTP Event Trace application is available as a plug-in in the MFCT. To use the "PtP Event Trace" application, activate the plug-in.

Once you have activated the plug-in, you can find PtP Event Trace on the start page as an application. In an opened application, you can find PtP Event Trace as a tab in the area of the button for the start screen.

You have the following options with the PtP Event Trace plug-in in combination with a SIMATIC CM PtP module:

- Read Event Traces
- Analyze serial communication
- Display the current configuration

More information

You can learn how to activate a plug-in in the section Plug-ins (Page 33).

You can find more information on the CM PtP module in the CM PtP (https://support.industry.siemens.com/cs/ww/en/view/109793681) equipment manual.

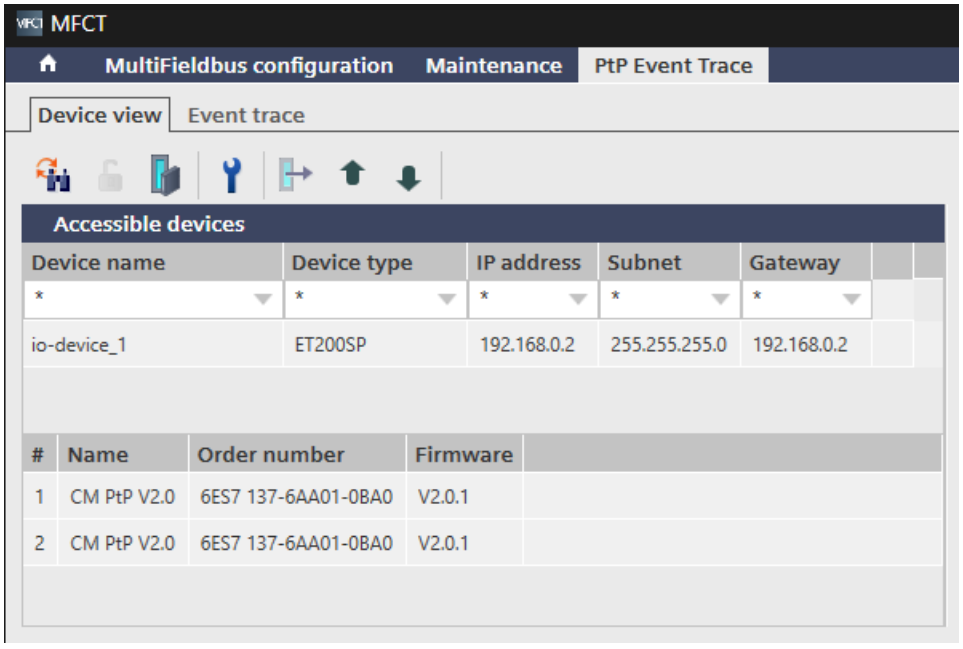
You can find more information on the configuration in the CM PtP - Configurations for point-to-point connections (https://support.industry.siemens.com/cs/ww/en/view/59057093) Function Manual.

11.1 Selecting a station with CM PtP module

You scan for stations with integrated CM PtP modules and can read out the traces of the modules on the "Device view" tab.

This offers you the following options:

- Analyze serial communication data
- Display the configuration of the serial interface



Procedure

To read out the trace from a CM PtP module, proceed as follows:

1. Click the "Start scan" button to scan for accessible devices.
2. Click the button to display only the devices with a CM PtP module.
3. To read out the trace from a CM PtP module:
   - Select the station
   - Select the CM PtP module
   - Click the button .

Result: The "Module details" tab shows the parameters of the CM PtP module.

Module details

Identification & Maintenance

Parameter	Value
Order number	6ES7 137-6AA01-0BA0
Serial number	S C-T7A10N7P2025
Firmware version	V2.0.1
Plant designation	
Location identifier	
Installation date	
Additional information	
Slot	1

Port configuration

Parameter	Value	
Specification of the operating mode	RS232C	
Receive line initial state	Keine	
Protocol	Freeport/Modbus	
Modbus CRC active	False	
Transmission rate	9600	bits/s

Importing/exporting trace files

To export a trace file, proceed as follows:

1. Read the trace of the selected module.
2. Click the "Export trace file" button .
3. Save the file in a location of your choice.

Result: You have saved the file in *.json format.

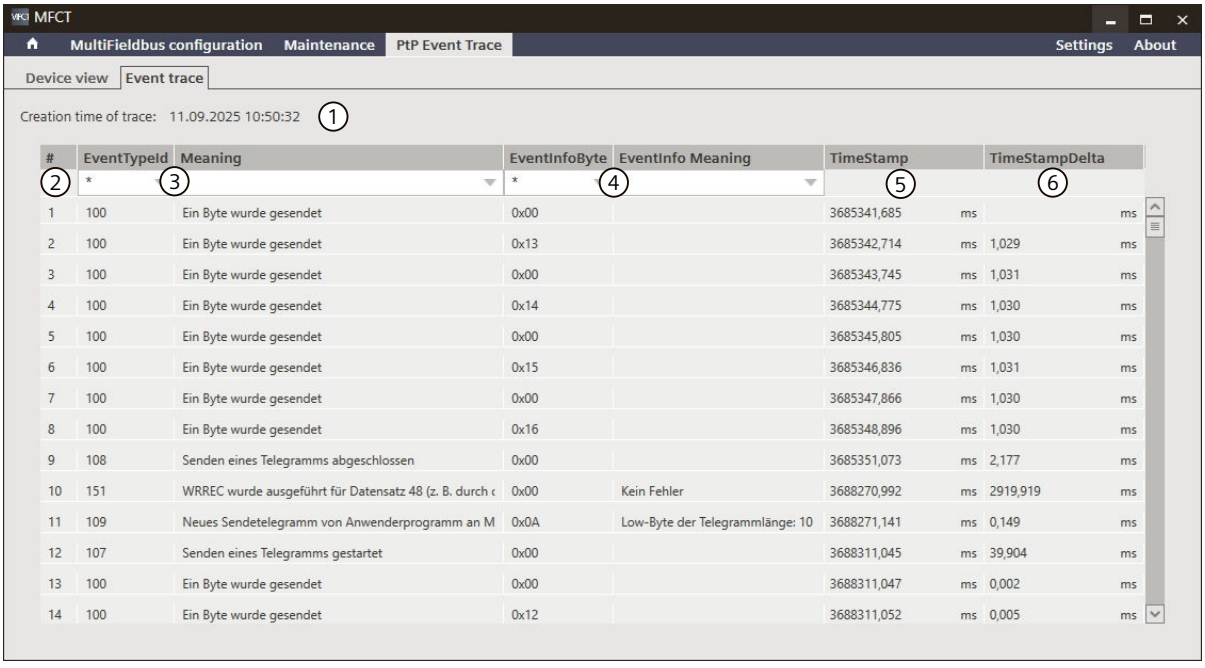
To import a trace file, proceed as follows:

1. Click the "Import trace file" button .
2. Select the desired file in *.json format.

Result: The "Module details" tab shows the saved parameters.

11.2 Analyzing a trace

The "PtP Event Trace" tab shows a table with the trace data.



#	EventTypeId	Meaning	EventInfoByte	EventInfo Meaning	TimeStamp	TimeStampDelta
1	100	Ein Byte wurde gesendet	0x00		3685341,685 ms	ms
2	100	Ein Byte wurde gesendet	0x13		3685342,714 ms	1,029 ms
3	100	Ein Byte wurde gesendet	0x00		3685343,745 ms	1,031 ms
4	100	Ein Byte wurde gesendet	0x14		3685344,775 ms	1,030 ms
5	100	Ein Byte wurde gesendet	0x00		3685345,805 ms	1,030 ms
6	100	Ein Byte wurde gesendet	0x15		3685346,836 ms	1,031 ms
7	100	Ein Byte wurde gesendet	0x00		3685347,866 ms	1,030 ms
8	100	Ein Byte wurde gesendet	0x16		3685348,896 ms	1,030 ms
9	108	Senden eines Telegramms abgeschlossen	0x00		3685351,073 ms	2,177 ms
10	151	WRREC wurde ausgeführt für Datensatz 48 (z. B. durch (	0x00	Kein Fehler	3688270,992 ms	2919,919 ms
11	109	Neues Sendetelegramm von Anwenderprogramm an M	0x0A	Low-Byte der Telegrammlänge: 10	3688271,141 ms	0,149 ms
12	107	Senden eines Telegramms gestartet	0x00		3688311,045 ms	39,904 ms
13	100	Ein Byte wurde gesendet	0x00		3688311,047 ms	0,002 ms
14	100	Ein Byte wurde gesendet	0x12		3688311,052 ms	0,005 ms

①	Creation time of the trace	Creation time with the date and time of the CPU.
②	#	Consecutive numbering of the entries.
③	EventType and meaning	Type of event as a decimal number (EventType) and text (meaning).
④	EventInfoByte and EventInfo meaning	Additional event information as a hexadecimal number (EventInfoByte) and text (EventInfo meaning).
⑤	Time stamp	Relative time stamp of the event in milliseconds, for time analysis between the individual events.
⑥	Time stamp delta	Time difference between two consecutive events. If the table has been filtered, the time difference from the previous event is displayed.

More information

A complete list of all possible events can be found in the "CM PtP - Configurations for point-to-point connections" Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59057093).

12 Maintenance

You have the following options in the "Maintenance" tab:

- Assign parameters (Page 97)
- Read service data (Page 98)
- Firmware update (Page 98)

After opening the MFCT, you can find "Maintenance" on the start page as an application. In an opened MFCT application, you can find "Maintenance" as a separate tab.

12.1 "Assign parameters" tab

You have the following options in the "Assign parameters" tab:

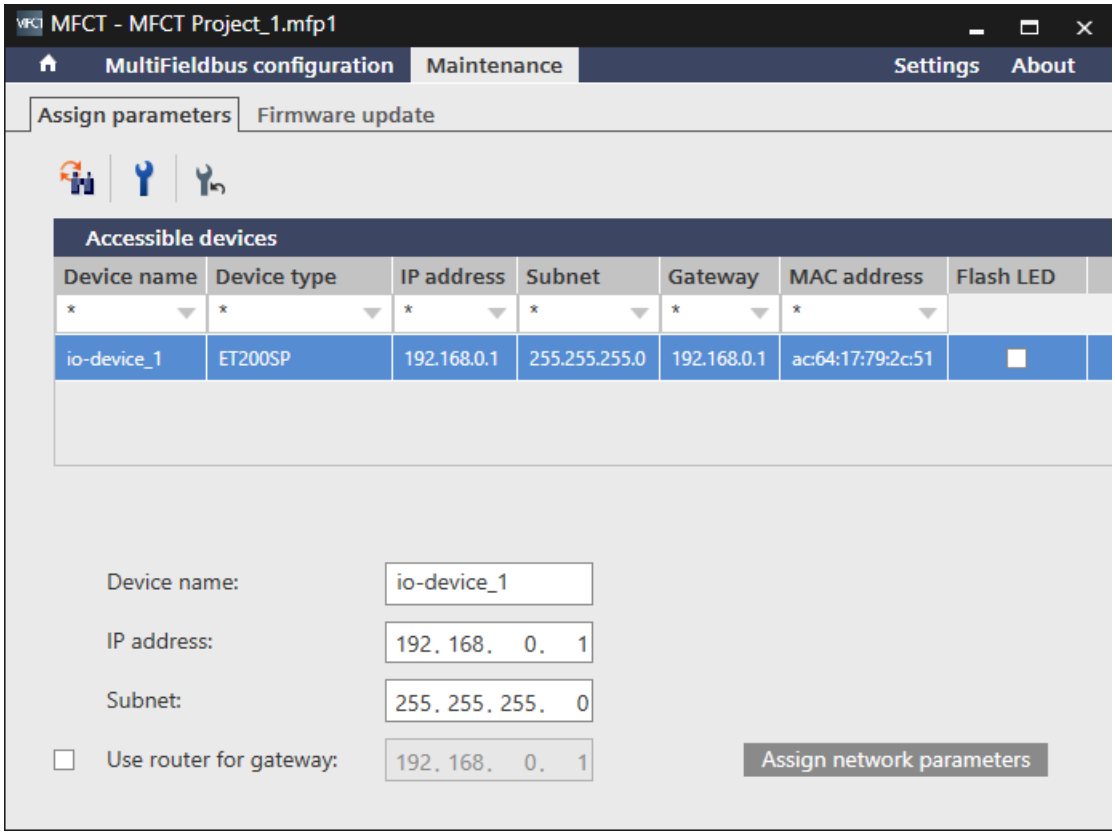
- Assign network parameters (Page 97)
- Resetting to factory settings (Page 97)
- Defining scan settings (Page 97)

Procedure for displaying all accessible online devices

To display all accessible online devices, proceed as follows:

1. Click "Start scan" .

   The following figure shows the contents of the "Assign parameters" tab:



2. Select the desired device.
3. To more easily locate the selected device, you have the option of making the LEDs of the device flash. To do so, select the check box in the "Flash LED" column.

You have found your desired device and can now carry out the steps described below.

12.1.1 Assigning network parameters

Requirement: You have opened the view with your selected device.

To assign the network parameters for MF devices, proceed as follows:

1. In the lower area, you can find the device name, the IP address and the subnet in which the selected device is located. If necessary, change this information.
2. If you are using a gateway, select the "Use router for gateway" check box.
3. Enter the address of the router.
4. To complete the entries, click the "Assign network parameters" button.

You will receive a message that the assignment of the network parameters was successful.

12.1.2 Resetting to factory settings

Requirement: You have opened the view with your selected device.

To reset a device to factory settings, click the "Reset network parameters" button .

After a positive answer to the confirmation prompt, the network parameters are reset to the factory settings.

12.1.3 Defining scan settings

To define the scan settings, proceed as follows:

1. Click the "Scan settings" button .
2. In the "Scan range" selection menu, select the area you want to scan:
   - All devices
   - Devices in the IP address range
   - Devices with specific IP address
   - Use the grid filter for network scans
3. Use the "Communication with CPUs" check boxes to select the following options:
   - Inclusion of centrally working modules
   - Include devices found via IP forwarding in other subnets
4. Confirm the selection with the "OK" button.

You have made and completed the settings for the scan.

12.2 "Read service data" tab

Requirement

The ET 200 station supports this function.

Procedure

To read out and save provided service data, proceed as follows:

1. Click "Start scan" .
2. Select the desired device.
3. To locate the selected device, you have the option of making the LEDs of the device flash. To do so, select the check box in the "Flash LED" column.
4. Enter the path under which you want to save the service data in the "Service data output path" text box at the bottom.
5. Click the "Start" button.

You will receive a message that the reading of the service data has been successfully completed.

12.3 "Firmware update" tab

The firmware update allows you to load or activate new firmware in multiple devices in parallel during operation. The devices continue to run without interruption.

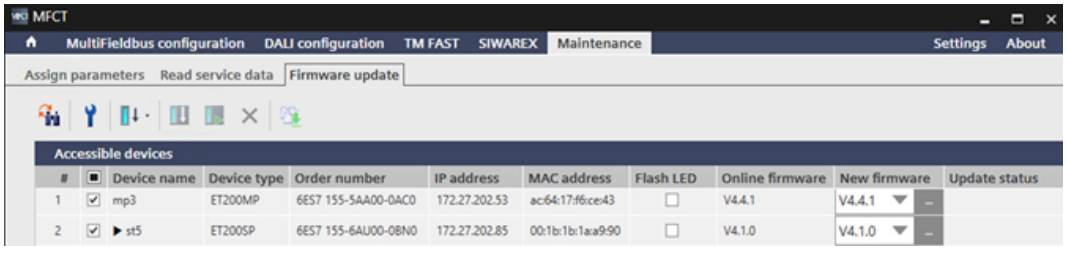
You have the following options in the "Firmware update" tab:

- Settings for firmware update (Page 99)
- Update firmware (Page 103)
- Activate firmware (Page 106)

Procedure to display all accessible online devices

To display all accessible online devices, proceed as follows:

1. Click the "Start scan" button .
   The following figure shows a section of the contents of the "Firmware update" tab:

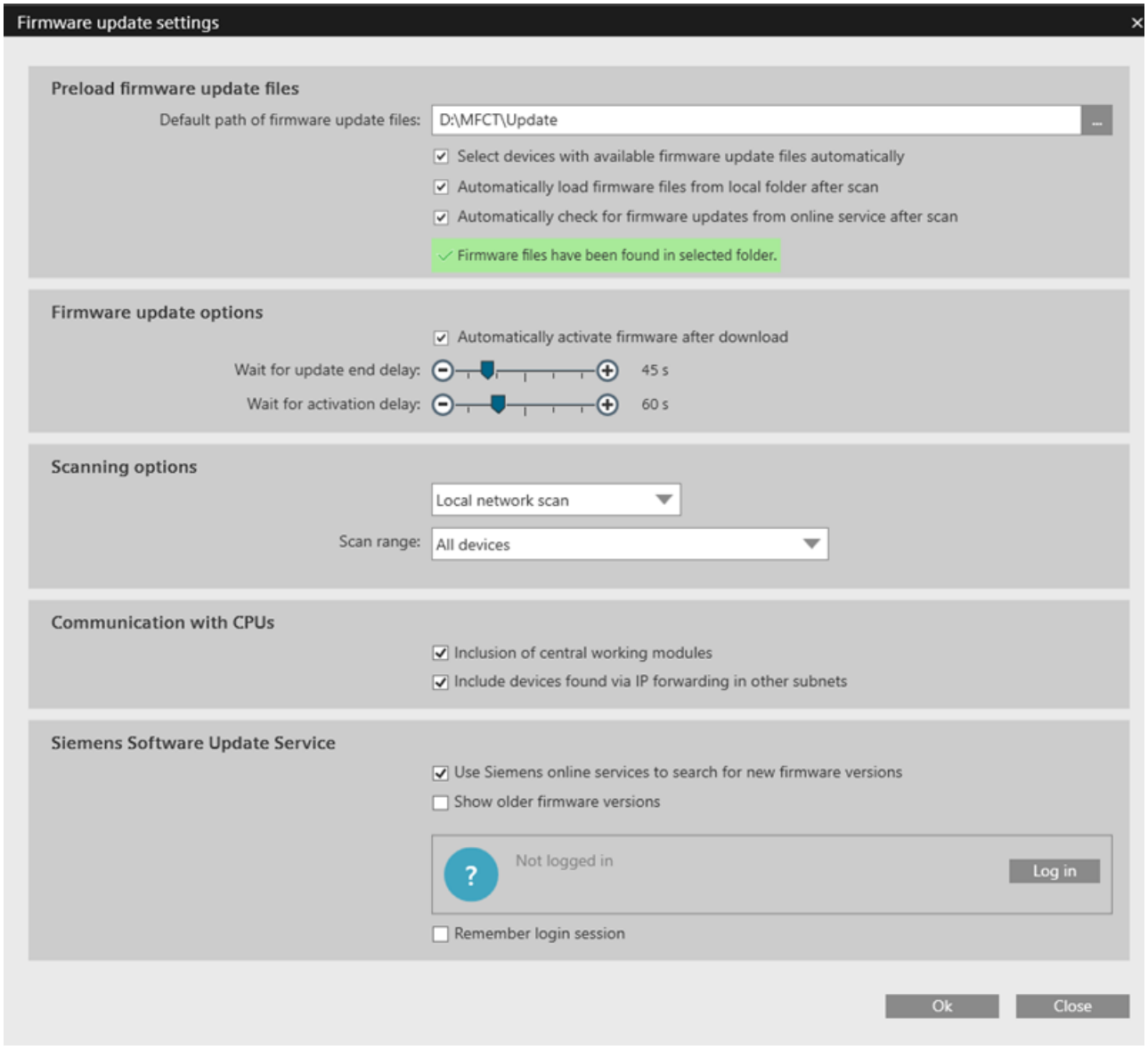


You have found your devices and can now carry out the steps described below.

12.3.1 Settings for firmware update

To make the settings for the firmware update, proceed as follows:

1. Click .
   The following figure shows the contents of the "Firmware update settings" window:



In the "Firmware update settings" window that opens, you can now make the settings explained below.

Preload the firmware update file

In the "Preload firmware update file" area, you can find the "Default path of firmware update file" text box. Here, you specify the storage path for the firmware update file.

When the "Select devices with available firmware update files automatically" check box is selected, all devices in the network for which the following criteria are met are automatically identified:

- a suitable firmware update file is available, and
- an update is possible or required, e.g. because the current firmware is out of date.

With the following options, you determine which firmware files the MFCT should display during updates:

- After the scan, automatically load firmware files from the local directory:
  The MFCT displays the locally stored firmware files in the selection menu during updates.
- After the scan, automatically check for firmware updates from the online service:
  The MFCT displays the firmware files provided by the Siemens Software Update Service in the selection menu during updates.
  This option is only available if the "Use Siemens online services to search for new firmware versions" option is enabled in the "Siemens Software Update Service" area.

Firmware update options

To activate the new firmware **directly after loading**, select the "Automatically activate firmware after download" check box. This option must be enabled in order for the two options below it to take effect.

- "Wait for update end delay": Specifies the delay time between the sending of the update file and the confirmation by the module that it received it.
  This prevents an unwanted cancellation of the download to the device.
- "Wait for activation delay": After the successful download, the MFCT waits the set amount of time before activating the firmware and restarting the device.

You can find information on the delay times in the respective equipment manual of the module. The times must be adjusted to the module with the longest delay time.

Scanning options

In the "Scanning options" area, you can determine whether the scan if to be run locally or whether subnets are also to be included.

You can find the further procedure in the section Set scanning options (Page 102).

Communication with CPUs

In the "Communication with CPUs" area, select the range in which the network scan should detect modules.

- "Inclusion of centrally working modules" check box:
  The network scan detects centrally plugged modules on a CPU.
- "Include devices found via IP forwarding in other subnets" check box:
  The network scan also detects devices in other subnets.

Siemens Software Update Service

If this section is not shown, this service is currently unavailable.

The Siemens Software Update Service is an automated service that ensures that your SIMATIC software is always up to date.

To use the service, you must register with the Siemens Software Update Service. After successfully registering, click the "Log in" button to connect your MFCT to the Siemens Software Update Service.

Select the "Use Siemens online services to search for new firmware versions" check box to allow the MFCT to search for available firmware files using the Siemens Software Update Service.

If you select the "Show older firmware versions" option, the Siemens Software Update Service will also display previous firmware files for the modules.

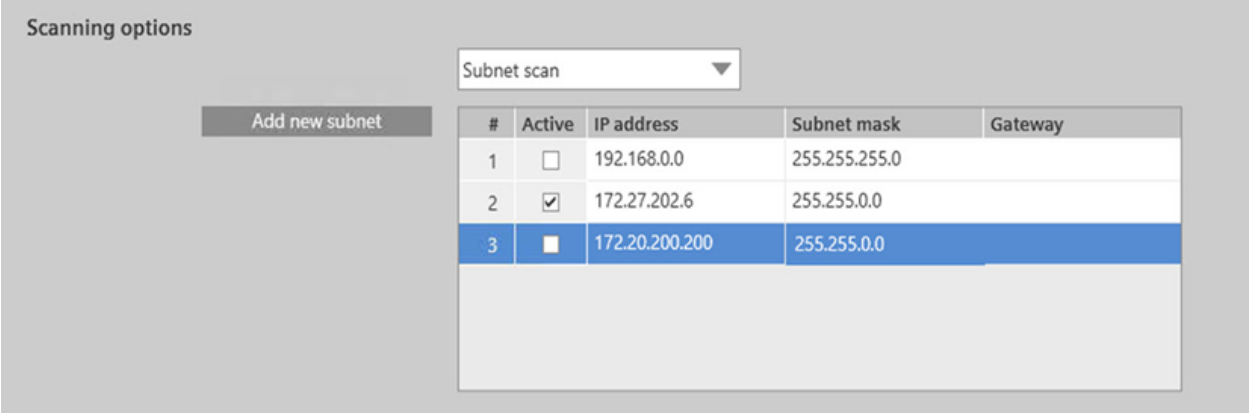
Select the "Remember login session" option to save your login credentials. If you are already logged in and you enable the option, you will be logged out of the Siemens Software Update Service and will need to log in again once.

12.3.1.1 Setting scanning options

To set the scan options, proceed as follows:

1. In the "Scan options" drop-down list, select the area you want to scan:
   - Local network scan: update the firmware in the local network
   - Subnet scan: update the firmware in multiple subnets

     The following figure shows an example of the three subnets found:



2. Enter the following details for each subnet:
   - IP address
   - Subnet mask
   - Address for the gateway
3. To create a new subnet and add it to the list, click the "Add new subnet" button.
4. To complete the entries, click the "OK" button.

You have made and completed the settings for the scan options.

12.3.2 Updating firmware

NOTE

We recommend that you do not connect directly with the device which you want to update. The activation of the new firmware can lead to a loss of the scanned devices due to a brief interruption of the network connection at the network adapter.

Procedure - Checking for updates

To check whether firmware updates are available for your devices, proceed as follows:

1. Click "Start scan" .
   All devices are displayed.
2. Optional: Use the incremental search function to locate the desired MF devices and modules. The search starts immediately after you enter the first character. The search query is refined with each additional character. The results are dynamically adapted according to your entry.

Accessible devices

#		Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware
		*	*	6ES7131	*	*		*	
2.07	☐	DI 8x24VDC HF V1.0	Digital	6ES7 131-6BF00-0CA0				V1.0.0	
2.08	☐	DI 8x24VDC HF V2.0	Digital	6ES7 131-6BF00-0CA0				V2.0.3	

3. Click the "Check for updates" button.
   The MFCT opens the selection menu with the available options for searching for firmware updates.
4. Select one of the following options in the shortcut menu:
   - Check for all updates:
     The MFCT searches online and locally for firmware updates.
   - Check for online updates:
     The MFCT searches the Siemens Software Update Service for firmware updates.
   - Check for local updates:
     The MFCT searches locally for firmware updates in the path you selected in the firmware update settings.

NOTE

Separation of the plant network and the Internet

To search online for firmware updates, your PG/PC must have an Internet connection. If it is not possible to connect to both the plant network and the Internet at the same time, proceed as follows:

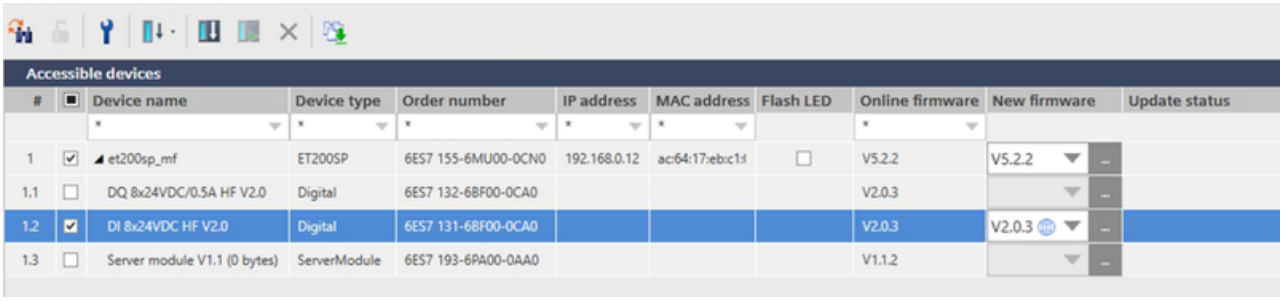
1. After the scanning process, disconnect the plant network from your PG/PC.
2. Connect to the Internet.

Result: You have started the check for current firmware files.
The MFCT searches for available firmware updates based on your selection. The following subsections explain how to select firmware updates and load them onto the devices.

Procedure – Selecting and downloading the firmware file

Once the MFCT has finished checking for firmware updates, proceed as follows:

1. Navigate to the "New firmware" column.
2. In the selection menu, choose which firmware file you want to use for each device. Firmware files that are available online are indicated by the Internet icon V2.0.3 in the MFCT.



Intermediate result: You have selected the desired firmware file for all the required devices.

If you want to use firmware files that are available online but you are not connected to your plant network, click the "Download all online firmware" button. The MFCT downloads the selected firmware files and saves them in the path you specified in the firmware update settings. The "Update status" column shows the current progress.

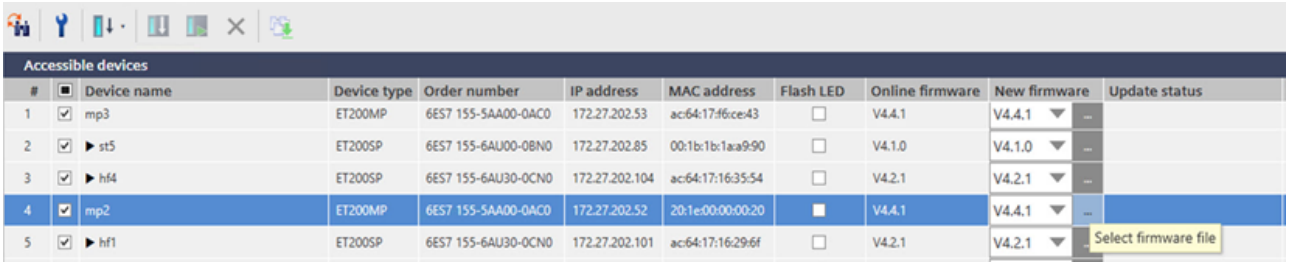
The downloaded firmware files are then displayed in the device selection menus just like locally stored firmware files.

Procedure - Loading firmware to the devices

To load the firmware on the devices, proceed as follows:

1. Optional: Reconnect your plant network to the PG/PC where the firmware updates are stored.
2. Set the appropriate firmware file for each device.

   Recommendation: If you are using a STEP 7 firmware update file, select the file: header.upd.



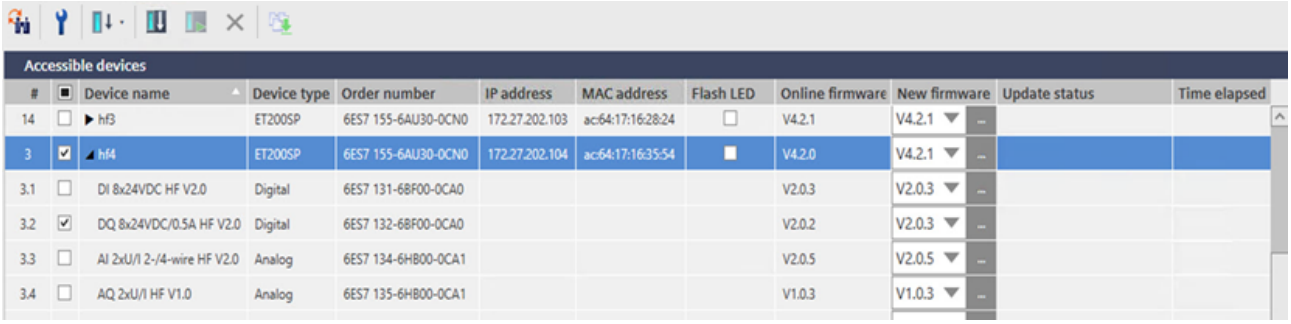
#	Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware	Update status
1	mp3	ET200MP	6ES7 155-5AA00-0AC0	172.27.202.53	ac:64:17:f6:ce:43		V4.4.1	V4.4.1	
2	▶ st5	ET200SP	6ES7 155-6AU00-0BN0	172.27.202.85	00:1b:1b:1a:a9:90		V4.1.0	V4.1.0	
3	▶ hf4	ET200SP	6ES7 155-6AU30-0CN0	172.27.202.104	ac:64:17:16:35:54		V4.2.1	V4.2.1	
4	mp2	ET200MP	6ES7 155-5AA00-0AC0	172.27.202.52	20:1e:00:00:00:20		V4.4.1	V4.4.1	
5	▶ hf1	ET200SP	6ES7 155-6AU30-0CN0	172.27.202.101	ac:64:17:16:29:6f		V4.2.1	V4.2.1	

NOTE

Select a directory, which contains subdirectories with firmware files.

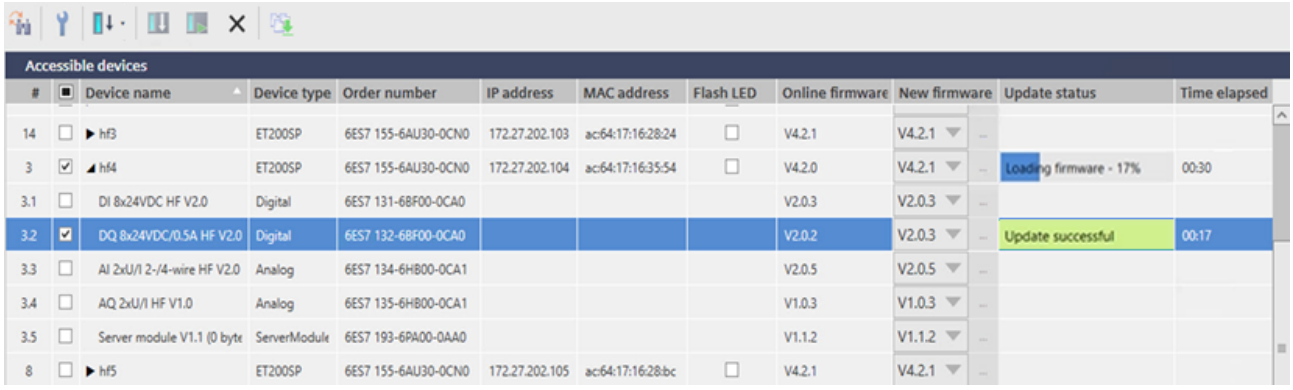
If you select large directories, entire hard disks (for example C:\) or directories on network drives, the corresponding access can take very long or MFCT can no longer react.

3. Select the devices to be updated.



#	Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware	Update status	Time elapsed
14	▶ hf3	ET200SP	6ES7 155-6AU30-0CN0	172.27.202.103	ac:64:17:16:28:24		V4.2.1	V4.2.1		
3	◢ hf4	ET200SP	6ES7 155-6AU30-0CN0	172.27.202.104	ac:64:17:16:35:54		V4.2.0	V4.2.1		
3.1	DI 8x24VDC HF V2.0	Digital	6ES7 131-6BF00-0CA0				V2.0.3	V2.0.3		
3.2	DQ 8x24VDC/0.5A HF V2.0	Digital	6ES7 132-6BF00-0CA0				V2.0.2	V2.0.3		
3.3	AI 2xU/I 2-/4-wire HF V2.0	Analog	6ES7 134-6HB00-0CA1				V2.0.5	V2.0.5		
3.4	AQ 2xU/I HF V1.0	Analog	6ES7 135-6HB00-0CA1				V1.0.3	V1.0.3		

4. To start the firmware update for the selected devices, click the "Update firmware" button .
   The update can be canceled at any time using the "Cancel" button .



NOTE

If you cancel the update of the firmware in the "Initialization" or "Waiting" phase, it takes some minutes until the MF devices are ready again and you can restart the update.

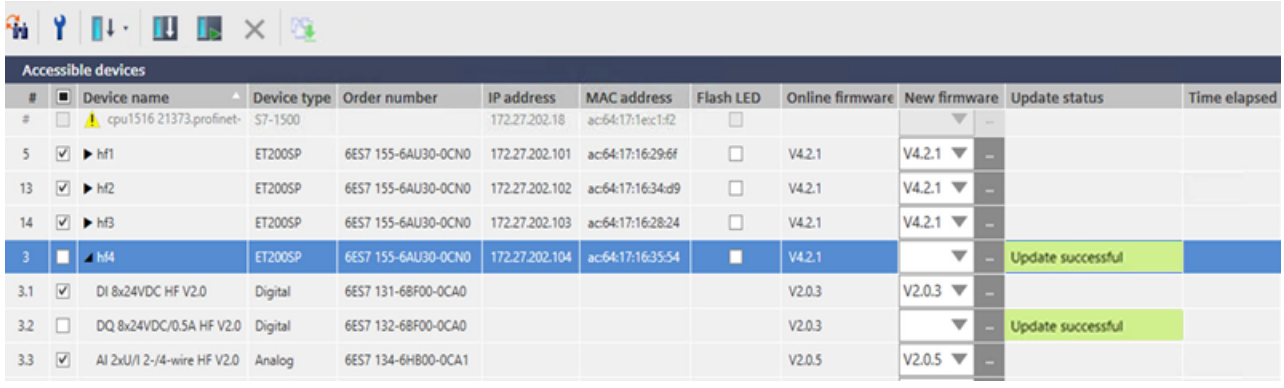
12.3.3 Activating the firmware

The new firmware is not active yet once the firmware update has been successfully performed. You can activate the firmware on the device later.

Procedure

To activate the firmware, proceed as follows:

1. Click the "Start scan" button . You can recognize devices with updated firmware that has not been activated yet in the device table by scanning again.
2. Select the devices whose firmware you want to activate.



3. Click the "Activate firmware" button . This activates the firmware of the selected devices one after the other.
4. If activation fails, scan the network again.

Once activation is complete, all selected devices should have the latest firmware version.

Glossary

Automation system

Programmable logic controller for the open-loop and closed-loop control of process chains in the process engineering industry and in manufacturing technology. The automation system consists of different components and integrated system functions according to the automation task.

Bus

Joint transmission path to which all devices in a fieldbus system are connected.

Configuration

Systematic arrangement of the individual modules (configuration).

CPU

The **C**entral **P**rocessing **U**nit (CPU) contains the operating system and executes the user program. The user program is located on the SIMATIC memory card and is processed in the work memory of the CPU. The PROFINET interfaces on the CPU allow simultaneous communication with PROFINET devices, PROFINET controllers, HMI devices and PGs/PCs.

Data block

Data blocks (DBs) are data areas in the user program that contain user data. Available data blocks:

- Global data blocks that you can access from all code blocks.
- Instance data blocks that are assigned to a specific FB call.

Device names

Each IO device must have a unique device name. This is required to allow the IO controller to communicate with an IO device. Advantage: Device names are easier to manage than complex IP addresses.

In its delivery state, an IO device has no device name. A device name must be assigned using the PG/PC before an IO device can be addressed by an IO controller. Example: For transmission of the configuration data (e.g. the IP address) during startup or for exchanging user data in cyclic mode.

Diagnostic buffer

The diagnostic buffer is a battery-backed memory area in the CPU where diagnostics events are stored in their order of occurrence.

Diagnostics

Monitoring functions include:

- Detection, localization and classification of errors, faults and alarms.
- Display and further evaluation of errors, faults and alarms.

They run automatically while the system is in operation. This increases the availability of systems by reducing commissioning times and downtimes.

Distributed I/O system

System with I/O modules that are configured on a distributed basis, at a large distance from the CPU controlling them.

DP

Distributed I/O

EDS

An electronic data sheet or also an EDS file is an ASCII text file that contains all the relevant information about a user application.

EtherNet/IP

EtherNet/IP (EtherNet Industrial Protocol) is a real-time Ethernet that is mainly used in automation technology. Alongside PROFINET and Modbus/TCP, EtherNet/IP is an Ethernet-based fieldbus.

Firmware of the CPU

In SIMATIC, a distinction is made between the firmware of the CPU and user programs.

The firmware is a software embedded in electronic devices. The firmware is permanently connected to the hardware in functional terms. It is usually saved in a flash memory, such as EPROM, EEPROM or ROM, and cannot be replaced by the user or only with special tools or functions.

User program: You can find more information in the "User program" glossary entry.

Firmware update

You update the module firmware with a firmware update. A firmware update is, for example, run for new functions of a CPU or an interface module.

GSD file

As a Generic Station Description, this file contains all the properties of a PROFINET or PROFIBUS device that are necessary for its configuration.

GSDML file

As Generic Station Description Markup Language, this file is an XML-based extension of a GSD file and contains additional information on the device configuration.

GSDX file

A GSDX file can contain one or more GSD files, together with associated files and a verified manufacturer signature.

Host-based Intrusion Detection System

Host-based Intrusion Detection System (HIDS) is a network security tool that monitors network traffic and devices for suspicious activity or violations of security policy.

I/O module

Device of the distributed I/O that is used as an interface between the controller and the process.

I5x file

I5x is the file format for a global library. An I5x file is used to store and manage standardized and reusable components, such as UDTs.

Interface module

Module in the distributed I/O system. The interface module connects the distributed I/O system to the CPUs (IO controllers) via a fieldbus, and prepares the data of the I/O modules.

MF

Multi**F**eldbus

The MultiFieldbus sits at the boundary between controllers and field devices and supports several Ethernet protocols.

Modbus TCP

Modbus/TCP is a protocol for communication between devices in a network that is based on the Modbus protocol and the TCP/IP protocol.

Operating system

Software that allows the use and operation of a computer. The operating system manages resources such as memory, input and output devices and controls the execution of programs.

PROFINET

PROcess **FI**eld **NET**work, open Industrial Ethernet standard that continues PROFIBUS and Industrial Ethernet. A cross-manufacturer communication, automation, and engineering model defined by PROFIBUS International e.V. as an automation standard.

PROFINET IO

Communication concept for the realization of modular, distributed applications within the scope of PROFINET.

PROFINET IO controller

Device used to address connected IO devices (for example distributed I/O systems). The IO controller exchanges input and output signals with assigned IO devices. The IO controller is often the CPU on which the user program is running.

PROFINET IO device

Distributed field device that can be assigned to one or more IO controllers. Examples: Distributed I/O system, valve terminals, frequency converters, switches

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning.

Restart

A warm restart deletes all non-retentive bit memory and resets non-retentive DB contents to the initial values from load memory. Retentive bit memory and retentive DB contents are retained. Program execution begins at the call of the first startup OB. A restart is triggered with POWER OFF/POWER ON of the CPU supply voltage.

Security

Generic term for all the measures taken to protect against:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability due to the destruction of data

TIA Portal

Totally **I**ntegrated **A**utomation Portal

The TIA Portal is the key to the full performance capability of Totally Integrated Automation. The software optimizes operating, machine and process sequences.

UDT

A **u**ser-**d**efined **t**ype (UDT) is a user-defined data type in which several associated tags are grouped. UDTs are used to logically structure complex data.

User program

In SIMATIC, a distinction is made between user programs and the firmware of the CPU.

The user program contains all instructions, declarations and data that control a system or process. The user program is assigned to the redundant system. Structuring into smaller unit is supported.

Firmware: You can find more information in the "Firmware of the CPU" glossary entry.

Index

T

U

V