SIEMENS

CIM

Operating Manual

03/2023

A5E51250518-AD

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 personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. 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 AG. 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 AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E51250518-AD
Ⓟ 03/2023 Subject to change

Preface

Purpose of the documentation

This manual describes communication interface module (CIM).

This manual supports you during the configuration, installation and operation of the communication modules.

Product names and abbreviations

- CIM or device

  In this document, the term "CIM" or "device" is also used instead of the full product name "CIM“. CIM is the abbreviation for Communication Interface Module.

Use of the device

Please observe notes marked as follows:

Note

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

Note

To prevent injury, read the manual before use.

⚠

The manual is delivered online, you can download the document from Central technical support (https://support.industry.siemens.com/cs/ww/en/).

History

Edition	Comment
09/2021	First Edition
07/2022	Added Description for UKCA certification.
11/2022	• Supported setting up SGLAN for devices from different site with CIM. • Added monitor variables in CIM web-based configuration.

Table of contents

Application and functions 1

1.1 What's new in CIM 1.1?

The features described below are only used for CIM 1.1.

New functions

CIM V1.1 provides the following new features:

- Support setting up SGLAN with CIM
  - SGLAN (Page 14) (Secured Global Local Area Network) is used for setting up virtual LAN for devices from different sites
  - Siemens CIM SGLAN Connector: application for connecting PC to SGLAN as SGLAN client
  - SGLAN page (Page 51) on CIM web-based configuration
- Monitor online variables through web-based configuration
- Allow to add extra initialization commands (Page 79) for cellular modular

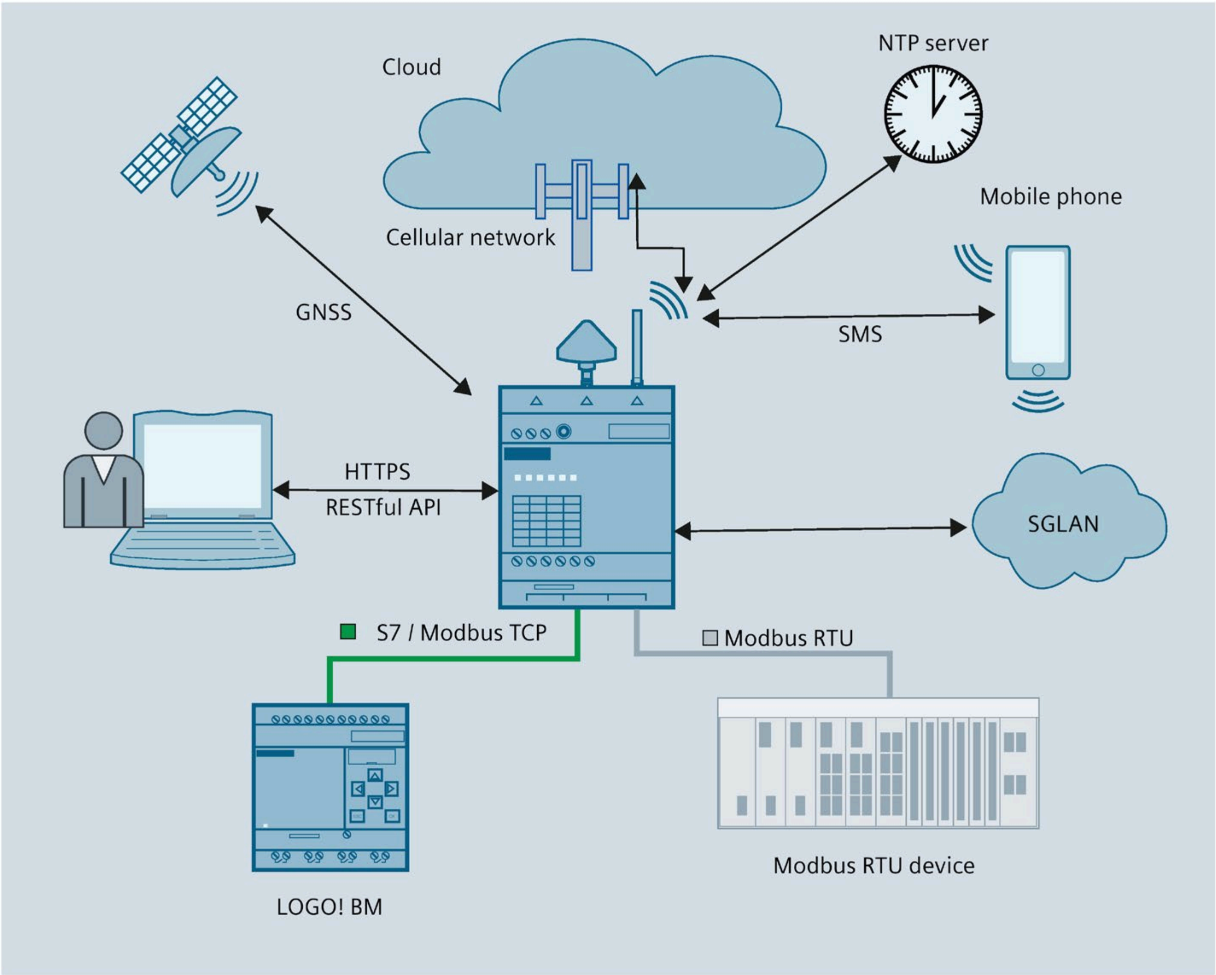
Changed functions

CIM web-based configuration:

- Add new page for monitoring online variables (Page 63)
- Add columns for monitoring and modifying in variable page (Page 57)
- Add speed, altitude of CIM in GNSS page (Page 79)
- Add IP address change notify (Page 85).

1.2 Functions

CIM provides Internet connection solution for LOGO! BM which has more and more capabilities to interact with Internet now.



General introduction

Universal Data Model (UDM)

LOGO! BM and Modbus RTU compatible devices can map their process data to UDM. UDM acts as a data center for CIM, and different protocols can exchange data through UDM.

4 ports switch

CIM can work as a LAN switch.

To ensure CIM work stably and efficiently, Siemens recommends that you should connect less than 4 devices to CIM through Ethernet switch ports.

General gateway

CIM can access the Internet with cellular module and SIM card. LOGO! BM or Modbus RTU compatible devices can access the internet by connecting to CIM.

SGLAN

Devices distributed in the same SGLAN (Secured Global Local Area Network) can communicate with each other.

Basic functions

The CIM supports the following functions:

- **Web-based configuration**

  A Web-based user interface (Web-based configuration) for the configuration of the CIM.
- **Protocol gateway**

  LOGO! BM and Modbus RTU compatible devices can communicate with CIM via S7/Modbus protocol based on the Universal Data Model (UDM).

  Application can access data through RESTful API on CIM based on UDM.
- **Data management**

  CIM can perform an action when a configured event is triggered.
  - After configured, CIM can perform an action, for example, change the data in UDM, send one or more short messages to one or more contacts.
- **Mobile cellular**

  With the CIM, you can establish a mobile data connection to a mobile cellular network.
- **GNSS position**
  - Display the position information on the web page
  - Enable/disable map the position data to UDM
- **Time Server**
  - CIM can act as an NTP server to provide time for LOGO! BM or other NTP client.
  - CIM can enable/disable mapping the time to the Universal Data Model (UDM). Then the device without NTP can get the time via multi-protocol or RESTful API.
- **Power on/off SMS**
  - CIM can send a power on/off SMS to one defined contact.
- **Certificate**
  - Owned certificate: generate and select certificate for setting up a secured web server and a SGLAN server
  - Trusted certificate: select certificate for setting up SGLAN Client

Web-based configuration

You can configure the CIM locally using a web-based configuration that can be displayed with a Web browser. The web-based configuration provides the following functions:

- Configure the LAN of CIM
- Manage the contacts

- Configure variables, messages and data bindings
- Modify and monitor variables
- Configure the multi-protocol
- Configure the cellular module
- Set the system time and synchronization of the CIM
- Configure the security functions
- Maintenance functions such as firmware update, device restart and factory reset
- Set the power on/off SMS for CIM

For more detailed information, refer to Web-based configuration (Page 43).

1.3 Requirements for use

Requirements for operation

- **Cellular module (mini PCIe)**

  To operate the CIM in its entirety, you require a cellular module that is compatible to CIM and the standard of the cellular network you are using. For more information, refer to the section Slots for SIM card and cellular module (Page 20).

- **Antenna and cables**

  Only use antennas from the accessories program for the CIM. For more information, refer to the section Antennas (Page 41).

  – Antenna for cellular

    To access the cellular network, you require an antenna that is adapted to the standard of the cellular network you are using.

  – Antenna for GNSS

    If you want to use GNSS, you require a suitable GNSS antenna.

- **Mobile data contract with SIM card**

  To use the mobile data communication via the WAN interface of the CIM, you require a contract with a suitable cellular network operator.

- **Cellular network**

  To be able to use the cellular interface, there must be a cellular network within the reach of the CIM.

- **Data contract**

  For the following data services, you require a data contract with your mobile operator:

  NTP, Cloud, HTTPS, SGLAN via cellular network

Power supply

You require a voltage source with a voltage between 12 VDC and 24 VDC that provides adequate voltage or current. For more information, refer to the section Technical specifications (Page 111).

SIM card

You require a SIM card of your mobile cellular operator.

Recommendations

Note the following recommendations for the cellular contract or for the SIM card:

- Where possible sign a cellular contract with a provider that makes all required functions available.

  To send SMS messages, the SIM card must be enabled this function and have a phone number.
- Where possible sign a fixed cellular contract and do not use prepaid cards. A flat rate for SMS and data can be recommended.

  If, however, you want to use a prepaid card note the following:
  - If your credit has been used up, the CIM does not send an automatic warning.
  - You can query your current credit with your provider.
- Where possible, use a standard SIM card without an adapter.
- If the SIM card has been assigned a PIN code, you need to enter the PIN code in the page "Cellular & GNSS -->Cellular status" of web-based configuration.
- The following access data for the cellular network must be present:
  - Access Point Name (APN)
  - Dial Number

For more information, refer to the section Cellular settings (Page 78).

Compatible cards

The card receptacle of the CIM for the SIM card is compatible with the following card formats:

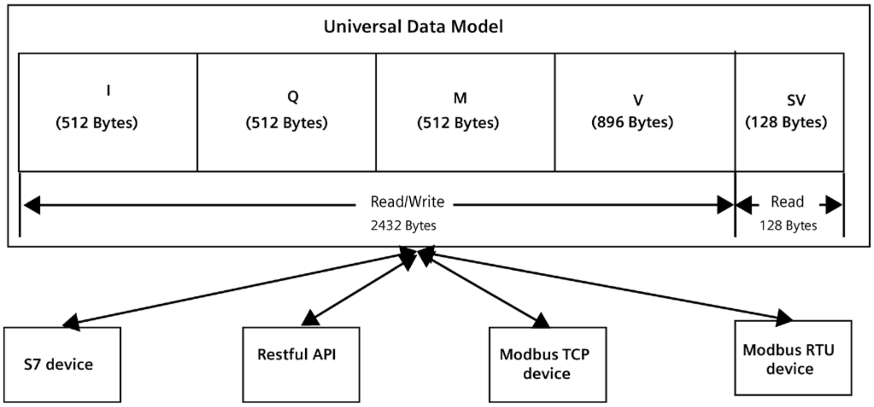
- Mini SIM card, 25 x 15 mm (ISO/IEC 7810 ID-000)

1.4 Universal Data Model

“Universal Data Model (UDM)” allows compatible PLC devices map their process data to UDM even if they use different communication protocols. UDM acts as a data center for CIM, and different protocols can exchange data through UDM.

Note

UDM uses Little Endian to store its multi-byte type data.



I, Q, M, V constructed a data model to simulate the process image in PLC.

Naming rule for the UDM address: address type + short data type + start address. No byte alignment, for example, VW3 means the word consist of Byte 3 and Byte 4 in area V.

The UDM address is case insensitive.

Data type (Short data type)	**Length**	**Value range**	I （512 Bytes）	Q （512 Bytes）	M （512 Bytes）	V (W: 896 Bytes R: 1024 Bytes)	
bool (x)	1 bit	0 ~ 1	0.0-511.7	0.0-511.7	0.0-511.7	0.0-895.7	0.0-1023.7
byte (b)	8 bit	0 ~ FF	0-511	0-511	0-511	0-895	0-1023
word (w)	16 bit	0 ~ FFFF	0-510	0-510	0-510	0-894	0-1022
double-word (dw)	32 bit	0 ~ FFFFFFFF	0-508	0-508	0-508	0-892	0-1020
long-word (lw)	64 bit	0 ~ FFFFFFFFFFFFFFFF	0-504	0-504	0-504	0-888	0-1016
short-int (si)	8 bit	-128 ~127	0-511	0-511	0-511	0-895	0-1023
int (i)	16 bit	-32768 ~ 32767	0-510	0-510	0-510	0-894	0-1022
double-int (di)	32 bit	-2147483648 ~ 2147483647	0-508	0-508	0-508	0-892	0-1020
long-int (li)	64 bit	-9223372036854775808 ~ 9223372036854775807	0-504	0-504	0-504	0-888	0-1016
Real (r)	32 bit	-3.4E38 ~ +3.4E38	0-508	0-508	0-508	0-892	0-1020
long-real (lr)	64 bit	-1.797E308 ~ +1.797E308	0-504	0-504	0-504	0-888	0-1016
short-unsigned (su)	8 bit	0 ~ 255	0-511	0-511	0-511	0-895	0-1023
unsigned (u)	16 bit	0 ~ 65535	0-510	0-510	0-510	0-894	0-1022
double - unsigned (du)	32 bit	0 ~ 4294967295	0-508	0-508	0-508	0-892	0-1020
long-unsigned (lu)	64 bit	0 ~ 18446744073709551615	0-504	0-504	0-504	0-888	0-1016

System variable

SV (System variable) is used to save some system data, such as, position, time, power state, mini PCIe module information and so on.

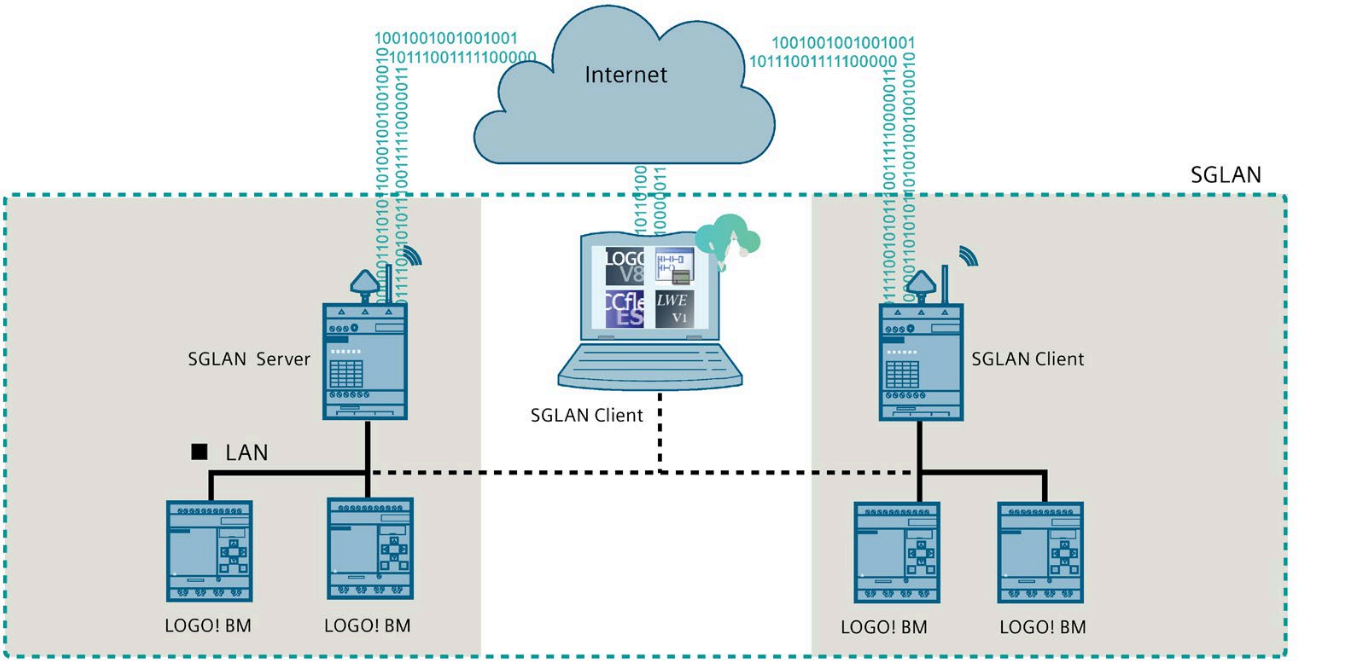
Item	Type	Size	Address	Range	Unit	comments	Sample for Restful Interface
Time							
valid flag	bool	1 bit	896.0	0 or 1		Valid flag for the time value	/pi/rest/vx896.0
UNIX timestamp	double unsigned	4 bytes	897	0 ~ 4294967295	second	Current time, seconds since 1970-1-1 00:00:00 Unit: second	/pi/rest/vdu897
year	unsigned	2 bytes	901	1970 ~ 2106	year	Current data, year	/pi/rest/vu901
month	short unsigned	1 bytes	903	1 ~12	month	Current data, month	/pi/rest/vsu903
day	short unsigned	1 bytes	904	1 ~ 31	day	Current data, month day	/pi/rest/vsu904
hour	short unsigned	1 bytes	905	0 ~ 23	hour	Current time, hour	/pi/rest/vsu905
minute	short unsigned	1 bytes	906	0 ~ 59	minute	Current time, minute	/pi/rest/vsu906
second	short unsigned	1 bytes	907	0 ~ 59	second	Current time, second	/pi/rest/vsu907
Position							
valid flag	bool	1 bit	916.0	0 or 1		Valid flag for all the position value	/pi/rest/vx916.0
latitude	short int	1 byte	917	-1 or 1		1: N; -1: S	/pi/rest/vsi917
	short unsigned	1 byte	918	0 ~ 90	degree	Latitude's degree Unit: degree	/pi/rest/vsu918
	short unsigned	1 byte	919	0 ~ 59	minute	Latitude's minute Unit: minute	/pi/rest/vsu919
	short unsigned	1 byte	920	0 ~ 59	second	Latitude's second Unit: second	/pi/rest/vsu920
	real	4 bytes	921	0 ~ 90.0	degree	Latitude's degree in float format Unit: degree	/pi/rest/vr921
longitude	short int	1 byte	925	-1 or 1		1: E; -1: W	/pi/rest/vsi925
	short unsigned	1 byte	926	0 ~ 90	degree	Longitude's degree Unit: degree	/pi/rest/vsu926
	short unsigned	1 byte	927	0 ~ 59	minute	Longitude's minute Unit: minute	/pi/rest/vsu927
	short unsigned	1 byte	928	0 ~ 59	second	Longitude's second Unit: second	/pi/rest/vsu928
	real	4 bytes	929	0 ~ 90.0	degree	Longitude's degree in float format Unit: degree	/pi/rest/vr929
altitude[1]	int	2 bytes	940	-9999 ~ 9999	m	altitude (integer part)	/pi/rest/vi940

Item	Type	Size	Ad-dress	Range	Unit	comments	Sample for Restful Interface
	short unsigned	1 byte	942	0 ~ 9	0.1 m	altitude (fractional part)	/pi/rest/vsu942
	real	4 bytes	943	-9999.9 ~ 9999.9	m	altitude in float format	/pi/rest/vr943
speed [1]	unsigned	2 bytes	933	0 ~ 9999	km/h	speed (integer part)	/pi/rest/vu933
	short unsigned	1 byte	935	0 ~ 9	0.1 km/h	speed (fractional part)	/pi/rest/vu935
	real	4 bytes	936	0 ~ 9999.9	km/h	speed in float format	/pi/rest/vu936

[1] available for CIM V1.1 and later versions.

1.5 SGLAN

SGLAN (secured global local area network) allows you to create a private network with CIM. SGLAN is the fundamental building block for your private network. Devices in the SGLAN can communicate with each other securely.



Roles in SGLAN

There are two roles in SGLAN:

- **SGLAN server**: SGLAN server is the data switch center. SGLAN server is responsible for transmitting data, authorizing connect request, dealing with login and logout request.

  Note

  Only CIM can work as SGLAN server. Each SGLAN server can connect 2 SGLAN clients maximum.

- **SGLAN client**: after joining the SGLAN, SGLAN client and devices in the same LAN with SGLAN client can communicate with other devices joined SGLAN like in a same LAN. SGLAN client can be a CIM device or PC with Siemens CIM SGLAN Connector installed.

SGLAN Page on CIM web-based configuration

You can configure the SGLAN in the web-based configuration (Page 51).

Siemens CIM SGLAN Connector

After installing Siemens CIM SGLAN connector on your host computer, you can connect to a target SGLAN server and communicate with the device in SGLAN remotely. For more information on the Siemens CIM SGLAN Connector, refer to *Siemens CIM SGLAN Connector Help*.

CIM SGLAN Connector supports the following system:

- **Windows**: Window 10

1.6 Accessories

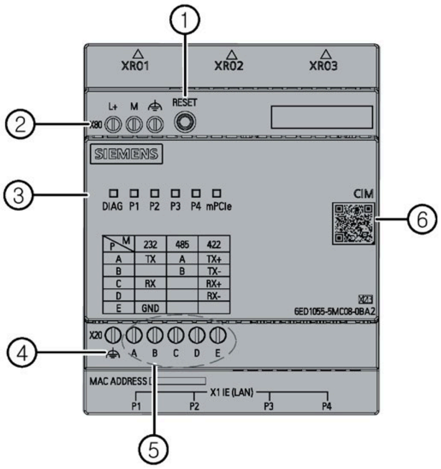
This chapter contains the scope of accessories valid at the time these operating instructions were written. The following accessories are not included in the scope of delivery and can be ordered separately.

Name	Description		Order number
Extended cable	Flexible connecting cable preassembled SIMATIC NET N-Connect/SM male/male	1 m long	6XV1875-5LH10
		2 m long	6XV1875-5LH20
		5 m long	6XV1875-5LH50
Antenna	Antenna ANT 895-6ML, active GNSS antenna		6GK5895-6ML00-0AA0
	Cylinder shaped antenna ANT 896-4ME for GSM (2G), UMTS (3G) and LTE (4G), ANT896-4ME		6GK5896-4ME00-0AA0
	IRC antenna ANT 896-4MA for GSM (2G), UMTS (3G) and LTE (4G),ANT896- 4MA		6GK5896-4MA00- 0AA3
Cellular module (mini-PCIe card)	Telit LE910C1-EU LTE CAT-1 mPCIe		
	Telit LE910C1-AP LTE CAT-1 mPCIe		
	Telit LE910C1-NF LTE CAT-1 mPCIe		
	SIM7600G-H LTE CAT-4 mPCIe		

Structure of the device 2

2.1 Appearance of the device

Front view



P \ M	232	485	422
A	TX	A	TX+
B		B	TX-
C	RX		RX+
D			RX-
E	GND		

① RESET button

② X80 (L+, M, FE) Power supply connector

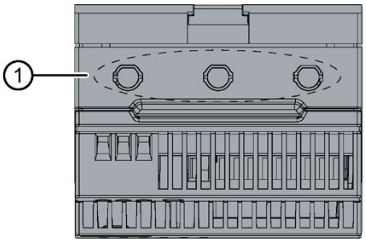
③ LED

④ FE terminal for shield cable

⑤ X20 (FE, A, B, C, D, E) Multiplex serial interface

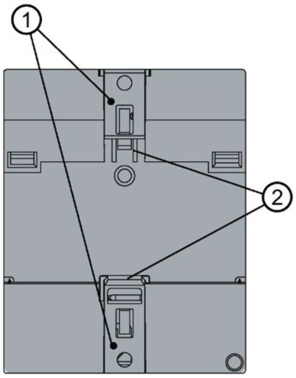
⑥ For more information about the device, scan the QR code

Top view



① Holes for RF antenna

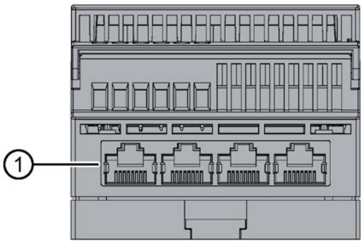
Rear view



① Mounting slides

② Mounting interlock for DIN rail

Bottom view



① 4 × RJ45 Ethernet 10/100 Mbps

2.2 LEDs to display operation

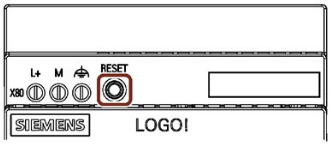
The LEDs on the CIM provide information about the operating status of the device.

Meaning of the LEDs

LED	Status	Meaning
System diagnose (DIAG)	On 🟩	The LED light is green when CIM is in RUN mode.
	On 🟧	CIM is booting or waiting for firmware update.
	Flash ☼	CIM is updating firmware.
	On 🟥	Firmware is crashed.
	Red flashing ☼	CIM is powered by capacitor.
LAN (P1, P2, P3, P4)	Flash ☼	Port is receiving or sending data across Ethernet.
	On 🟩	Port is already connected to Ethernet.
	Off □	No connection to Ethernet.
mPCIe	Off □	The cellular module is not detected.
	Flash ☼	The cellular module is initializing or registering.
	On 🟩	The cellular module has initialized and registered successfully.
	Flash ☼	The cellular module is receiving/sending data.

2.3 The "RESET" button

The RESET button allows you to recovery the module to a factory default setting.

Operator input	Function
Keep pressing for longer than 10 seconds 	Recovery the module to a default status

2.4 Slots for SIM card and cellular module

Both slots are behind the top housing.

Slot for the SIM card

Compatible cards

Mini SIM card, 25 x 15 mm (ISO/IEC 7810 ID-000)

Inserting the SIM card is described in the section Insert the SIM card (Page 37).

Slot for the cellular module

Compatible cellular modules:

	GSM/GPRS	UMTS	LTE	Certificate
Telit LE910C1-EU LTE CAT-1 mPCIe	Y	Y	Y	GCF, RED, FCC, JATE/TELEC, RCM
Telit LE910C1-AP LTE CAT-1 mPCIe		Y	Y	
Telit LE910C1-NF LTE CAT-1 mPCIe		Y	Y	
SIM7600G-H LTE CAT-4 mPCIe	Y	Y	Y	GCF, CE-RED, FCC, PTCRB, IC, Anatel, KC, NCC, JATE/TELEC, RCM, ICASA, IMDA, SRRC, CCC

Note

Applicability

The table shows the approvals that may be available. For the device itself, it is certificated as shown on the product label and package label.

Note

CIM with Telit series wireless module and SIM7600G-H LTE CAT-4 mPCIe are certified with UL, IECEx,ATEX,FM,RCM.

CE-RED: test with wireless module Telit LE910C1-EU LTE CAT-1 mPCIe and SIM7600G-H LTE CAT-4 mPCIe

UKCA-RED: test with wireless module Telit LE910C1-EU LTE CAT-1 mPCIe and SIM7600G-H LTE CAT-4 mPCIe

FCC: test with wireless module Telit LE910C1-NF LTE CAT-1 mPCIe and SIM7600G-H LTE CAT-4 mPCIe

Card errors / diagnostics

Card errors are indicated by the "mPCIe" LED.

Inserting the card

Inserting the SIM card is described in the section Installing the Cellular module (Page 39).

Security 3

3.1 Security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

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 customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/cert).

3.2 Data protection

Siemens observes the data protection guidelines, especially the requirements regarding data minimization (privacy by design). This means the following for this product: The product does not process / save any personal information, but only technical functional data (e.g. time stamps). If the user links this data to other data (e.g. shift plans) or if the user saves personal information on the same medium (e.g. hard disk) and therefore creates a personal reference in the process, the user has to ensure meeting the guidelines regarding data protection.

3.3 Important notes on using the device

The following safety notices must be adhered to when setting up and operating the device and during all associated work such as installation, connecting up or replacing devices.

NOTICE

Open Equipment

When the device is used in the area of Industrial Control Equipment in accordance with UL61010-2-201, the device is classified as "Open equipment".

Open equipment must be installed within an enclosure which protects you from hazards, including mechanical hazards, electrical shock and spread of fire.

Note

Cleaning CIM

Requirement: The supply voltages on the CIM is switched off.

If you need to clean the devices, use dry ESD cleaning cloths (observing the ESD protective measures).

Overvoltage protection

NOTICE

Protection of the external power supply

If power is supplied to the module or station over longer power cables or networks, the coupling in of strong electromagnetic pulses onto the power supply cables is possible. This can be caused, for example by lightning strikes or switching of higher loads.

The connector of the external power supply is not protected from strong electromagnetic pulses. To protect it, an external overvoltage protection module is necessary. The requirements of EN61000-4-5, surge immunity tests on power supply lines, are met only when a suitable protective element is used. A suitable device is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element.

Notices on use in hazardous areas

Note

- The equipment shall only be used in an area of pollution degree 2, as defined in IEC/EN 60664-1.
- The equipment shall be installed in an enclosure that provides a minimum ingress protection of IP 54 in accordance with IEC/EN 60079-0.
- Transient protection shall be provided that is set at a level not exceeding 140 % of the peak rated voltage value at the supply terminals to the equipment.

External power supply

- Use only an external power supply that complies with IEC/EN 61010-1 or IEC/EN 61010-2-201.
- The output voltage of the external power supply must not exceed 30 VDC.
- The output of the external power supply must be short-circuit proof.

NOTICE

Power supply

The external power supply for the CIM must meet the requirements for Safety Extra-Low Voltage (SELV).

Note the information in this section and in the installation and operating instructions from the manufacturer of the power supply.

⚠**WARNING**

The equipment is designed for operation with Safety Extra-Low Voltage (SELV).

This means that only SELV complying with IEC/EN61010-1 must be connected to the power supply terminals.

If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

⚠**WARNING**

EXPLOSION HAZARD

DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.

⚠**WARNING**

EXPLOSION HAZARD

SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.

⚠**WARNING**

When used in hazardous environments corresponding to Class I, Division 2 or Class I, Zone 2, the device must be installed in a cabinet or a suitable enclosure.

Notices on use in hazardous areas according to UL HazLoc

⚠ **WARNING**

EXPLOSION HAZARD

DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or nonhazardous locations only.

This equipment is suitable for use in Class I, Zone 2, Group IIC or non-hazardous locations only

⚠ **WARNING**

Safety notice for connectors with LAN (Local Area Network) marking

A LAN or LAN segment, with all its associated interconnected equipment, shall be entirely contained within a single low-voltage power distribution and within single building. The LAN is considered to be in an "environment A" according to IEEE802.3 or "environment 0" according IEC TR 62102, respectively.

Never make direct electrical connection to TNV-circuits (Telephone Network) or WAN (Wide Area Network).

Notes on the use

Note

Notes on protecting administrator accounts

A user with administrator rights has extensive access and manipulation options available to the system.
Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

Note

To protect LOGO!Soft Comfort from any undesired manipulation when your PC suffers malicious attacks from the Internet, Siemens strongly recommends you to install a allow list tool on the PC.

Mounting and connecting the device 4

4.1 Mounting the device

4.1.1 Mounting position

The installation should provide a dry environment for the CIM. SELV/PELV circuits are considered to provide protection against electric shock in dry locations.

The CIM installation dimensions are compliant with DIN 43880.

CIM can be snap-mounted to 35 mm DIN rails according to EN 60715 or mounted on the wall with two M4 screws.

CIM has a width of 71.5 mm.

Note

Risk to life when you touch live parts

Serious injury can result when you touch live parts.

Always switch off power before you remove or insert an expansion module.

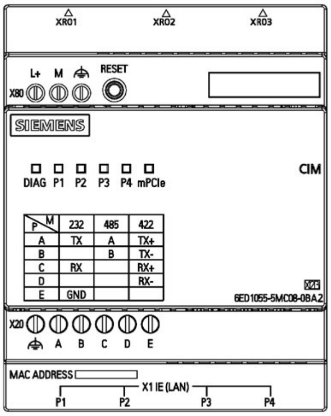
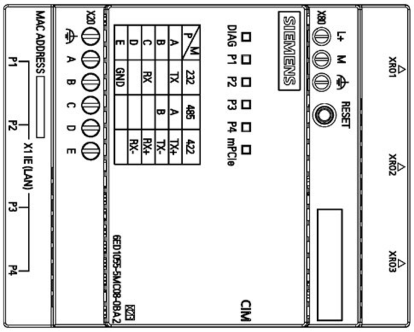
Note

The device is approved for indoor operation only.

NOTICE

Installation location - Dependency of the temperature range

The upper and lower ventilation slits of CIM cannot be covered, allowing adequate ventilation. Above and below the module, there must be a clearance of 25 mm to allow air to circulate and prevent overheating.

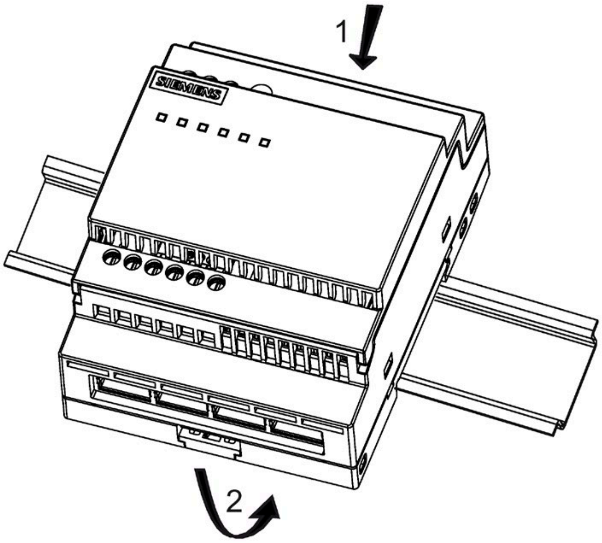
Installation position	Installation position of the CIM
Vertical installation of the CIM	
Horizontal installation of the CIM	

4.1.2 DIN rail mounting

Mounting

To mount a CIM onto a DIN rail, follow these steps:

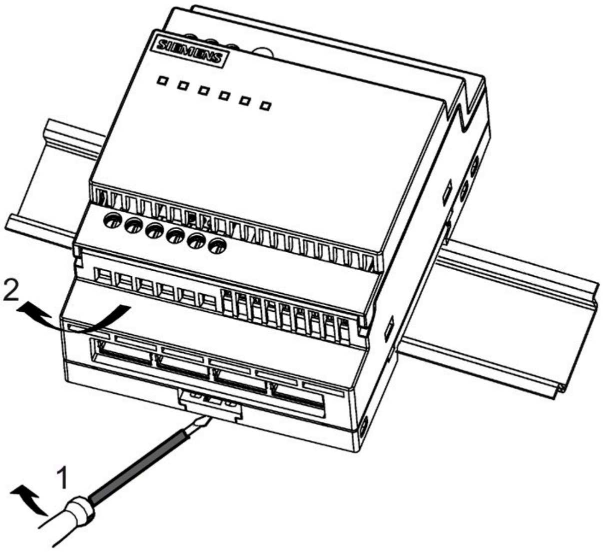
1. Hook the CIM onto the rail.
2. Push down the lower end to snap it on. The mounting interlock at the rear must engage.



Removal

To remove CIM, follow these steps:

1. Insert a screwdriver into the eyelet at the bottom of the slide interlock and move the latch downward.
2. Swing the CIM off the DIN rail.

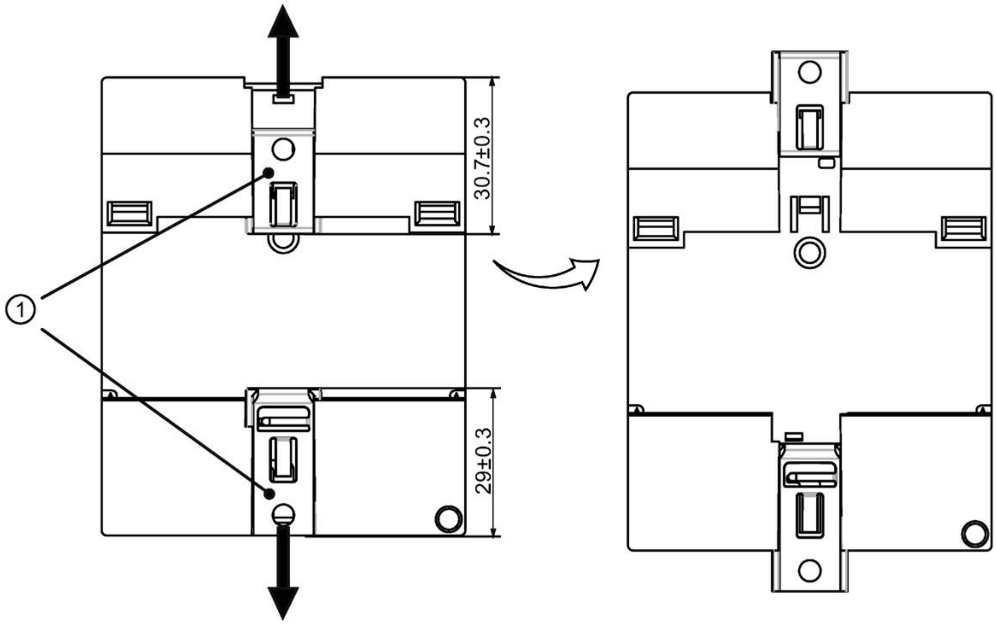


4.1.3 Wall-mounting

Wall-mounting

To mount the CIM on a wall, follow the steps below:

1. Using a screwdriver, pull the two mounting slides ① on the rear of the device towards the outside.



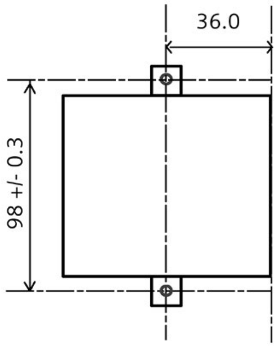
2. Feed the screws through the openings in the catches and secure the device to the wall.

Note

When you do not wall-mount CIM, always keep the mounting slides in the factory default positions, that is, within the data area given in the illustration above; otherwise, the mounting slides may deform if they are exposed to hot and humid surroundings for a long term.

Drilling template for wall-mounting

Before you can wall-mount CIM, you need to drill holes using the template shown below:



All dimensions in mm

Bore hole for M4 screw.

4.2 Connecting the device

4.2.1 Notes on connecting

WARNING

Risk of lightning strikes

A lightning flash may enter the mains cables and data transmission cables and jump to a person.

Death, serious injury and burns can be caused by lightning.

Take the following precautions:

- Disconnect the device from the power supply in good time when a thunderstorm is approaching.
- Do not touch mains cables and data transmission cables during a thunderstorm.
- Keep an enough distance from electric cables, distributors, systems, etc.

⚠ **CAUTION**

Use copper cables at connectors with terminal connections

Use copper (Cu) cables for all supply lines that are connected to the device with terminals, e.g. 24 VDC power supply cables to the 24 VDC power supply connectors.

Utiliser des câbles en cuivre sur les connexions à bornes

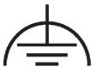
Utilisez des câbles en cuivre (Cu) pour tous les câbles d'alimentation qui sont raccordés à l'appareil par des bornes, par exemple les câbles d'alimentation 24 V CC sur le connecteur d'alimentation 24 V CC.

4.2.2 Connecting the power supply and function earth

A connected function earth discharges electrical charges from the metal enclosure.

The function earth also improves the discharge of interference generated by external power cables, signal cables or cables for I/O modules to ground.

The connection for the function earth is labeled with the following symbol:



⚠ **WARNING**

Electric shock and risk of fire

High voltage may be present in a defective device, which can cause fire or an electric shock if touched. This can result in death and serious injury.

- Connect the device to the function earth before you put it into operation.
- The function earth terminal on the device must be connected to the function earth of the control cabinet or system in which the device is installed.
- Never operate the device without function earth.
- If a device is defective, remove it from operation without delay and label it accordingly.

Note

The device should only be connected to a 12 to 24 V DC power supply which meets the requirements of safe extra low voltage (SELV) according to IEC/EN/DIN EN/UL 61010-1.

Note

The power supply must be adapted to the input data of the device, see chapter "Technical specification (Page 111)".

If there are voltage peaks on power supply lines, use a protective device in the form of a varistor (MOV) UMOV = U-rated x 1.2 (BLITZDUCTOR BVT AVD 24 (918 422) or compatible).

Note

The external bonding facility should provide effective connection of a conductor with a cross-sectional area of at least 4 mm^2.

Note

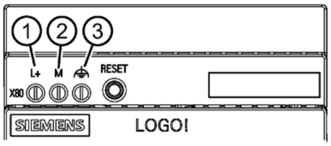
Terminal blocks do not accommodate more than one individual conductor in a clamping point.

Requirement

- You are using the supplied terminal
- A two-core cable meet the following requirements:
  - a copper (Cu) cable with cross-section of 0.75 mm^2 to 2.5 mm^2
  - rated temperature 75 °C
- A slotted screwdriver with a 3 mm blade
- Function earth with minimum cross-section of 2.5 mm^2 copper cable

Screw terminals for the power supply and function earth

1. Switch off the power supply.
2. Connect the lines to the connecting terminal with a torque of 0.8 Nm (7lb-in).



① L+ = live wire, positive pole of the DC voltage 12/24 VDC

② M = negative pole/ground of the DC voltage 12/24 VDC

③ Functional ground

- Serves to improve electromagnetic compatibility and to specify a common reference potential for all signals.
- Is achieved efficiently by a connection to the DIN rail.

Note

Power supply unit of the CIM is not electrically isolated

No electrical isolation means that the input and output circuits are not galvanically isolated.

4.2.3 Connecting the LAN interface

Connect your local area network, the PC or the BM to interface X1IE (LAN connection) of the CIM.

The interface supports autonegotiation and autocrossing. For the connection, use a patch cable with an RJ-45 plug. For the requirements and for information on grounding see below.

You will find the properties of the Ethernet interface in the technical specifications.

Requirements for the cable

Requirements for the network cable:

- Use a shielded Ethernet cable for connection to the Ethernet interface.
- To minimize electromagnetic disturbances use a pair of shielded, twisted Ethernet cables (category 5) and a shielded RJ-45 plug at both ends.

4.3 Installing expansion modules

4.3.1 Open the device

⚠ **WARNING**

Risk due to unauthorized opening and improper repairs or expansions

Improper procedure when carrying out expansions may result in substantial damage to equipment or endanger the user.

If you install or exchange system expansions and damage your device, the warranty becomes void.

⚠ **WARNING**

Malfunctions and electric shock

Improper intervention in the device endangers operational reliability and may damage the device, which may result in personal injuries and damage to the plant.

Take the following precautions:

- Always disconnect the power plug and wait until the DIAG LED goes off before you open the device.
- Close the device after every intervention.

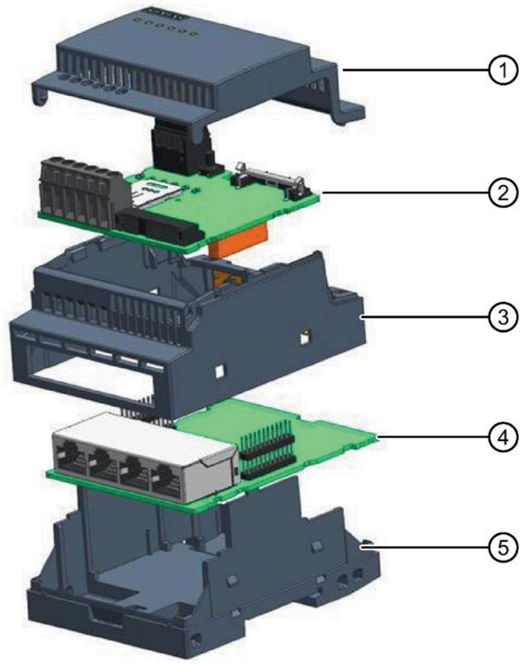
NOTICE

Electrostatic sensitive devices (ESD)

The device contains electronic components that may be destroyed by electrostatic charges. This can result in malfunctions and damage to the machine or plant.

Take corresponding precautionary measures before you open the device.

Exploded view



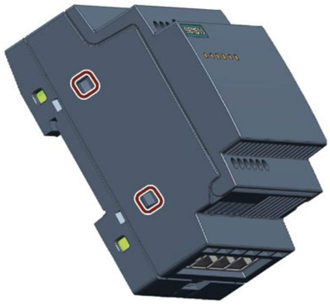
① Top housing
② Top PCBA
③ Middle housing
④ Bottom PCBA
⑤ Bottom housing

Open the middle housing

Requirements

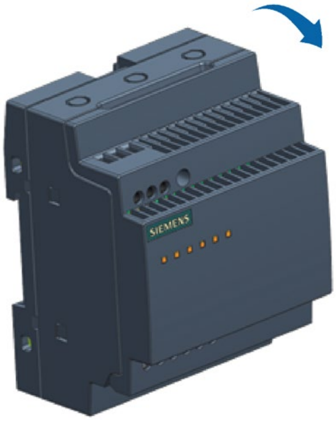
- The device is fully disconnected from the line voltage and the LED goes out, see "LEDs to display operation (Page 19)".
- All connection cables are unplugged.
- A flat-blade screwdriver

Press the marked recesses on both left and right sides of the module with a flat-blade screwdriver to loosen and then remove the middle housing.



Open the top housing

Pull the top housing in the marked direction to open the cover.



4.3.2 Installing the SMA connector

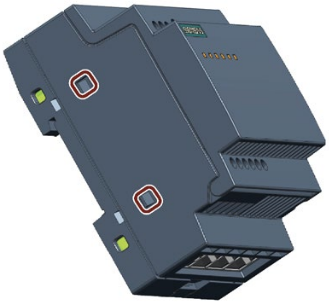
Requirement

- The device is disconnected from the power supply and the DIAG LED goes out.

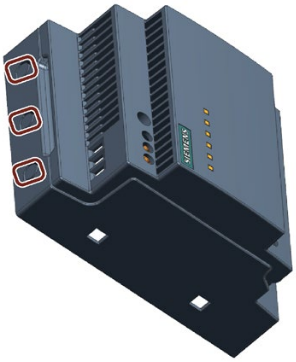
Procedure

Follow the steps to install the SMA connector.

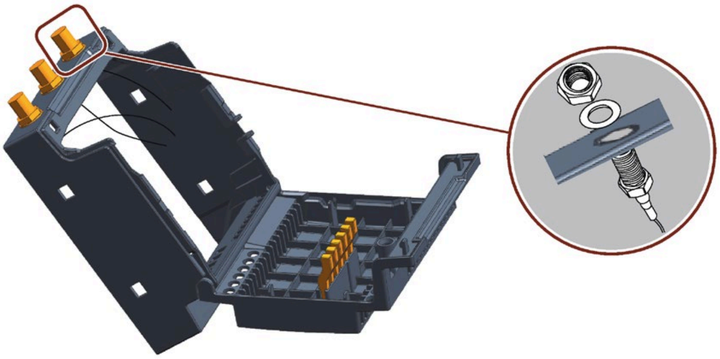
1. Press the marked recesses on both left and right sides of the module with a flat-blade screwdriver to loosen and then remove the middle housing.



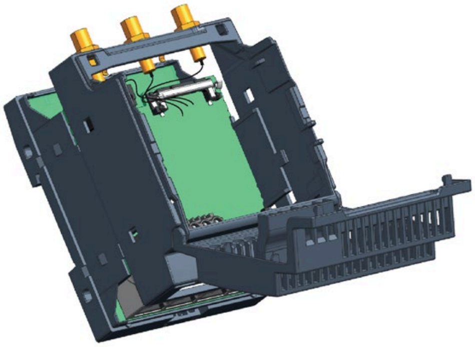
2. Remove the shelter on the middle housing.



3. Install the SMA connector as the marked order into the hole.



4. Install the middle housing back on the bottom housing. When install the middle housing, place the bottom of the SMA connectors below the top PCBA first, then adjust the position of the middle housing and install it back.



4.3.3 Insert the SIM card

Requirement

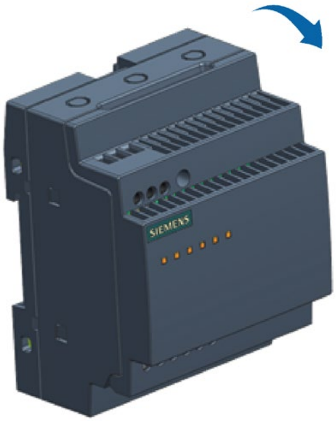
- The device is disconnected from the power supply and the DIAG LED goes out.
- The SIM card is suitable for industrial use.

  Compatible cards: Mini SIM card, 25 x 15 mm (ISO/IEC 7810 ID-000)

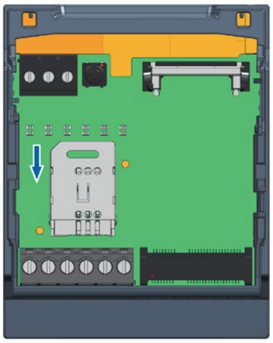
Install the SIM card

NOTICE
Inserting a SIM card If you are using the SIM card in a device installed in a system, you must observe the safety regulations for work on electrical systems. Carefully insert the SIM card into the card holder without applying excess force.

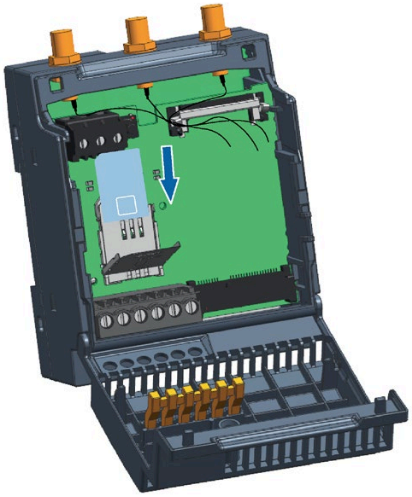
1. Pull the top housing in the marked direction to open the cover.



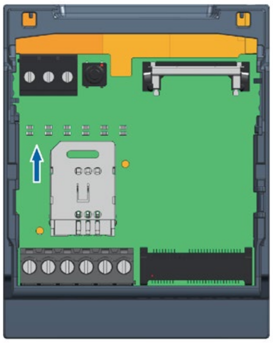
2. Unlock the card holder in the marked direction.



3. Put the SIM card in the card holder and then lock the card holder in the marked direction.



4. Lock the card holder in the marked direction.



Uninstall the SIM card

Unlock the card holder to remove the SIM card, and then lock the card holder as the default status.

4.3.4 Installing the Cellular module

Note

Power consumption

If the power consumption of the cellular module is too high, the device will be damaged.

Ambient temperature

The temperature in the housing of the device can be up to 30 °C above the maximum permissible ambient temperature of the device.

Make sure that the maximum permissible ambient temperature of the cellular module is specified accordingly.

⚠ CAUTION

Risk of burns due to hot components

The motherboard and internal components can get hot during operation. Motherboard and internal components will only cool down slowly after the device has been switched off.

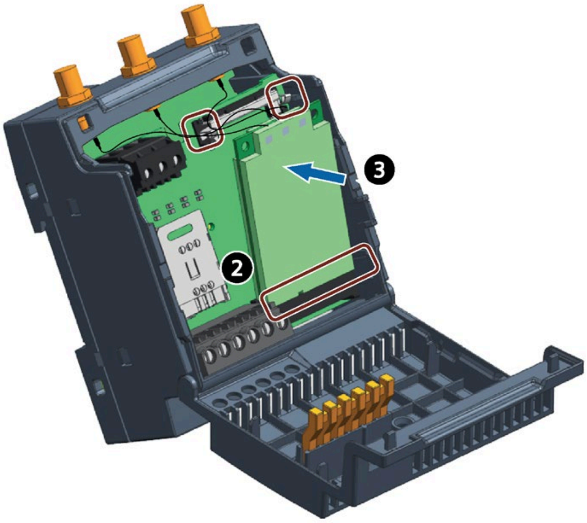
To avoid getting burned, wait a while after switching off the power supply. Be very careful when opening the enclosure and removing the motherboard.

Requirement

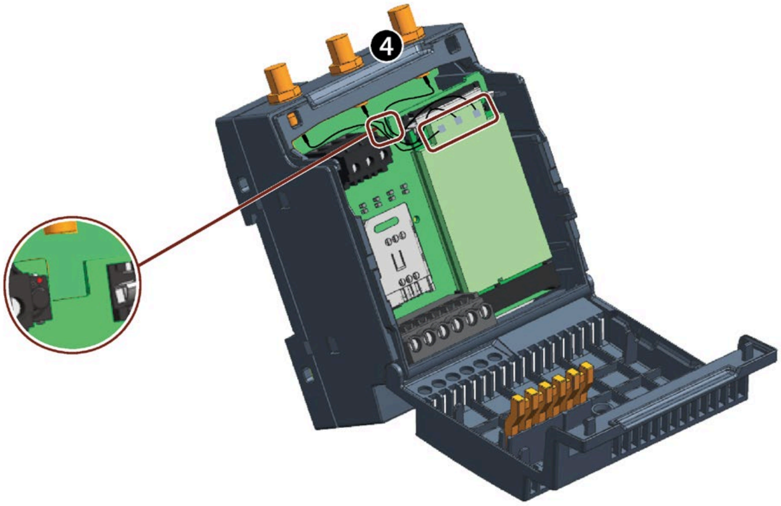
- The device is disconnected from the power supply and the DIAG LED goes out.
- A compatible cellular module (Page 20)

Install the cellular module

1. Open the top housing.
2. Insert the cellular module into the socket from the bottom side.
3. Press the cellular module in the marked direction to lock the cellular module.



4. Connect the feeder cables with the corresponding antenna connectors of the cellular module. Arrange the feed lines and make them pass from the feeder cable path to prevent interruption.
   - Cable type: SMA to U.FL
   - Cable length: 7 to 8 cm



5. Close the top housing.

Uninstall the cellular module

1. Open the top housing.
2. Disconnect the feed lines with the antenna connectors of the cellular module.
3. Pull the two lockers of the cellular module in the marked direction to loosen the cellular module.
4. Remove the cellular module and close the top housing.

4.3.5 Connecting the antenna

⚠ **WARNING**

Risk of lightning strikes when installed outdoors

If you install an antenna outside, you need to ground the antenna to protect it from lightning strikes. This work must only be carried out by qualified personnel.

NOTICE

Damage to devices due to incorrect accessories

Select the antenna suitable for your frequency band from the accessories. Other antennas could interfere with product characteristics or lead to defects.

NOTICE

Every module must be equipped with a proper antenna with the specified characteristics. The antenna must be installed with care to avoid any interference with other electronic devices and must be installed with the guarantee of a minimum 20 cm distance from a human body.

The CIM has three antenna sockets of the type SMA for connecting the antennas. The antennas must have an impedance of approx. 50 Ω.

Follow the operating instructions of the antennas used.

Supported Antenna and extended cable

Select the antenna suitable for your frequency band.

Name	MLFB	Remarks
Extended cable	6XV1875-5LH10	Flexible connecting cable preassembled SIMATIC NET N-Connect/SM male/male, 1m
	6XV1875-5LH20	Flexible connecting cable preassembled SIMATIC NET N-Connect/SM male/male, 2m
	6XV1875-5LH50	Flexible connecting cable preassembled SIMATIC NET N-Connect/SM male/male, 5m
Antenna	6GK5895-6ML00-0AA0	Antenna ANT 895-6ML, active GNSS antenna
	6GK5896-4ME00-0AA0	Cylinder shaped antenna ANT 896-4ME for GSM (2G), UMTS (3G) and LTE (4G), ANT896-4ME
	6GK5896-4MA00-0AA3	IRC antenna ANT 896-4MA for GSM (2G), UMTS (3G) and LTE (4G),ANT896-4MA

Web-based configuration 5

5.1 Security recommendations

Keep to the following Security recommendations to prevent unauthorized access to the system.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
- Check regularly for new features on the Siemens Internet pages.
  - Network security information (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html)

Physical access

Restrict physical access to the device to qualified personnel.

Passwords

- Regularly update the passwords to increase security.
- Only use passwords with a high password strength.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use one password for different users and system.

Protocols

- Only activate protocols that you require to use the system.

5.2 Downloading and installing the certificate

5.2.1 Overview

CIM has a build-in Web-based configurator which enables you to configure the CIM functions from a PC.

CIM supports HTTPS for web server communication. You need to import the LOGO! Root certificate before using HTTPS to visit CIM with browsers.

You can get the "LOGO! Root CA" in either of the following ways:

- Copy LOGO! Root CA from the DVD or LOGO!Soft Comfort installation path.
- Download LOGO! Root CA from CIM.

Copy the LOGO! Root CA

You can get the "LOGO! Root CA" in either of the following ways:

- on DVD: **Windows, Linux, or MAC→ Application"_operating system version**"→**res**

  "_operating system version" is available only for Linux and Windows.
- in LOGO!Soft Comfort installation path: The LOGO!Soft Comfort installation drive (such as C:\)→**Program Files**→**lsc**→**lsc**→**res**

Download the LOGO! Root CA from CIM

1. Set up the Ethernet communication between you PC and CIM.

   Note

   Make sure you connect to CIM within a secure network.

2. Open a web browser and enter "https://192.168.0.80".
3. Accept the risk notification and Click "Continue to visit the website".
4. Enter the password to login. The default password is "cim".

   Note

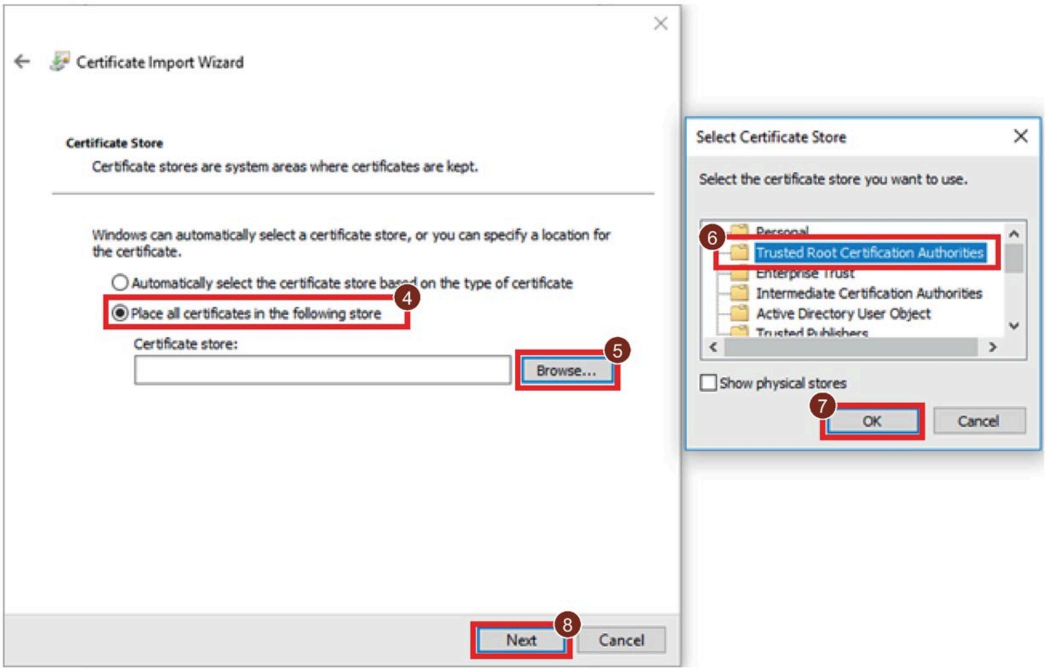
   After you log in the first time, you will be prompted to configure the power on/off SMS (Page 88) and change the default password.

5. Navigate to the **Security Setting** --> **Certificate**.
6. Select "Owned Certificates --> CIM build-in certificate".
7. Click **Download**.

5.2.2 Installing the certificate for Windows

Install the certificate for Windows

1. Double click the certificate to start the installation.
2. Check the certification information in the pop-up window, then click "Install Certificate" to continue.
3. On the certificate import Wizard welcome page, select the "Store location", then click "Next".
   - If you select “Current User”, the certificate is only valid for the current user.
   - If you select "Local Machine", the certificate is valid for all users on this PC. Only the administrator can install the certificate as "Local Machine".
4. Select the check box of ④ and click ⑤ to store the certificate.
5. Trust the certificate by selecting ⑥ in the pop-up window and then clicking ⑦.
6. Click ⑧ to continue.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Select Certificate Store

Select the certificate store you want to use.

□ Show physical stores

4
Browse...
5
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
6
7
OK
Cancel
8
Next
Cancel

7. In the "Certificate import wizard" window, click "Finish" to confirm your selection.
8. In the security warning window, click "Yes" to confirm the installation.

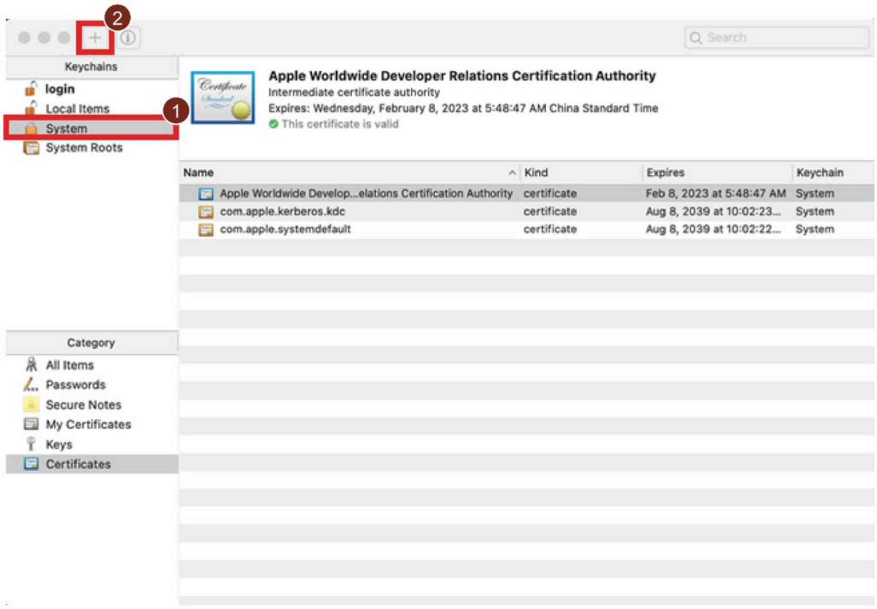
Import the certificate to Firefox

If Firefox still cannot trust the certificate after you have installed the certificate, follow the instruction from Firefox to import the certificate to Firefox under the guidance of the system administrator.

5.2.3 Installing the certificate for Mac OS

Install the certificate for MAC OS

1. Open the Keychain.
2. To add a certificate, select "system" ①, then click "+"②.



Apple Worldwide Developer Relations Certification Authority
Intermediate certificate authority
Expires: Wednesday, February 8, 2023 at 5:48:47 AM China Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
Apple Worldwide Develop...elations Certification Authority	certificate	Feb 8, 2023 at 5:48:47 AM	System
com.apple.kerberos.kdc	certificate	Aug 8, 2039 at 10:02:23...	System
com.apple.systemdefault	certificate	Aug 8, 2039 at 10:02:22...	System

3. Select the certificate of CA, then click "Open" to add it.
4. Enter the password, then Click "Modify Keychain".
5. Double-click the certificate of CA to open it.
6. Trust the certificate by clicking "Trust" and setting "Secure Sockets Layer (SSL)" as "Always trust".
7. Enter the password and confirm the modification.

5.2.4 Installing the certificate for Linux

Follow the instruction from Linux to import the certificate under the guidance of the system administrator.

5.3 Accessing web-based configuration from PC

To access the CIM Web-based configuration from a PC, follow these steps:

1. Ensure that the CIM and the PC are on a common Ethernet network or are connected directly to each other with a standard Ethernet cable.
2. Open a Web browser and enter the URL "https://ww.xx.yy.zz" corresponds to the IP address of the CIM.

Note

Make sure you do not disable cookies on your browser.

3. Enter the password.

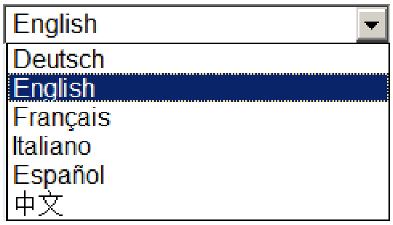
Note

The default IP address of the CIM is "https://192.168.0.80". The default password for CIM is cim.

Note

You can only log into web-based configuration with one browser at a time.

4. Select an appropriate language from the drop-down menu if needed.

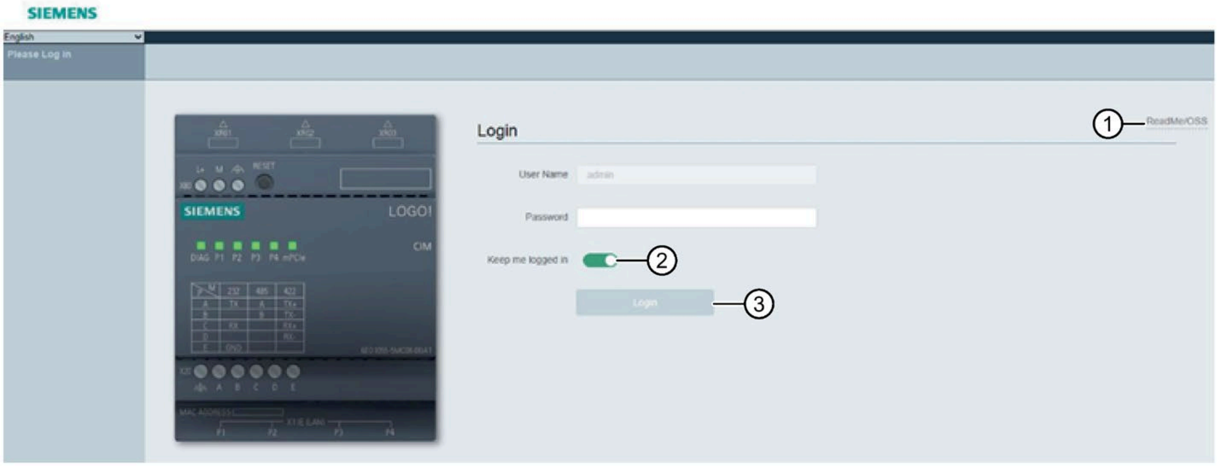


5. Click or tap "①" to view the OSS Readme.
6. Click or tap "③" to log in to the Web server.

   If you do not desire to enter the user name and password again at the next logon, you can select the "②" check box. Make sure you do not set your browser to private mode, since your browser does not record any browsing history or passwords in this mode.

   Note

   “Keep me logged in” is disabled by default and the selection will expire in 30 days.



User Name: admin

Keep me logged in: ●

Supported Web browsers

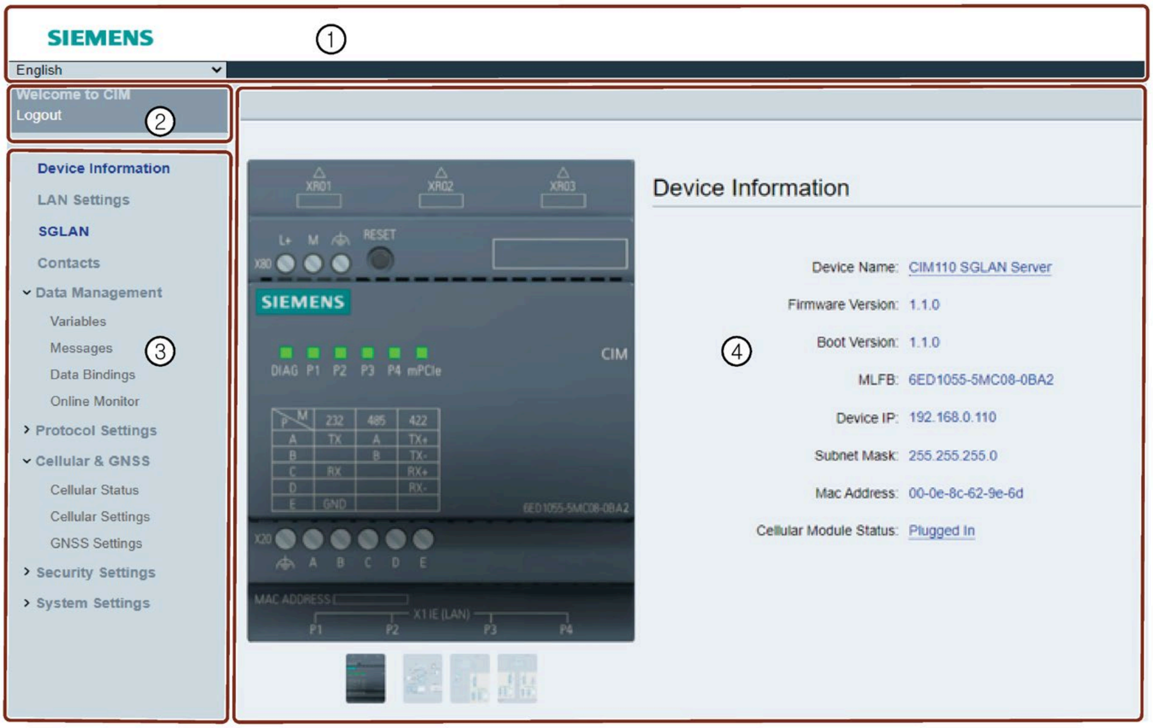
The Web server supports the following web browsers:

- Windows
  - Microsoft Internet Explorer 11.0
  - Firefox 67.0 and later versions
  - Google Chrome 63.0 and later versions
  - Edge 88.0 and later versions
- Mac OS
  - Apple Safari 12.1.2 and later versions
  - Firefox 67.0 and later versions
  - Google Chrome 63.0 and later versions
- Linux
  - Firefox 67.0 and later versions
  - Google Chrome 63.0 and later versions

5.4 Web pages

5.4.1 Layout of CIM

Once you logged in, you can see a web page appears as follows:



Device Information

Device Name: CIM110 SGLAN Server

Firmware Version: 1.1.0

Boot Version: 1.1.0

MLFB: 6ED1055-5MC08-0BA2

Device IP: 192.168.0.110

Subnet Mask: 255.255.255.0

Mac Address: 00-0e-8c-62-9e-6d

Cellular Module Status: Plugged In

① Header: selector for display language.
② Login/Logout
③ Configuration page navigator
④ Detailed information of a specific web page.

Configuration pages

The CIM includes following configuration pages:

Configuration pages	Description
Device information	Display the general information of the connected CIM
SGLAN	Set the SGLAN connection for CIM
LAN settings	Set the LAN for CIM
Contacts	Edit the contacts
Data Management	Edit the variables, messages and bindings
Protocol settings	Set the communication protocols

Configuration pages	Description
Cellular & GNSS	View and set the cellular and GNSS
Security settings	Configure the security policy
System settings	Configure the system settings

Overview of navigation/operator control and display elements

You will find the following elements in the web-based configuration pages:

Icon	Function
✎	Edit the item
🗑	Delete the item
❓	Help information

You will find the following button in the web-based configuration pages:

Icon	Function
+ Add Row	Add a new row
✓ Save Changes	Save the changes on the current page.
⊗ Discard Changes	Discard the changes on the current page.

5.4.2 Device information

The Device information page displays the general information of the connected CIM.

Parameters	Meaning
Device name	Display the device name. By clicking "Name", you can edit the CIM name.
FW version	Firmware version of CIM
Boot version	Boot version of CIM
MLFB	Order number
Device IP	IP of CIM
Subnet Mask	Mask of LAN IP
Mac address	Media Access Control Address
Cellular module	• Plugged In: cellular module is inserted into CIM and driven by CIM. • Not Plugged In: cellular module is not inserted into CIM. By clicking "Cellular module Status", you can navigate to the cellular status page.
Application scenario	An application example for CIM

5.4.3 LAN settings

This page allows you to set the IP for CIM.

If you forget the password for login, you need to reset the CIM to factory setting (Page 20) and log in with the default password.

5.4.4 SGLAN Setting

5.4.4.1 Setting up SGLAN server

This page allows you to set the CIM work as SGLAN server.

Note

To works as an SGLAN server, CIM must meet the following requirements:

- CIM can access the Internet through IPv4/IPv6
- The IPv4/IPv6 address assigned to SIM card by telecom operator can be accessed over the Internet through IPv4/IPv6
- The SIM card in CIM supports sending and receiving short message if you set up SGLAN by SMS
- The IP of the devices in SGLAN are in the same subnet and not conflict with each other

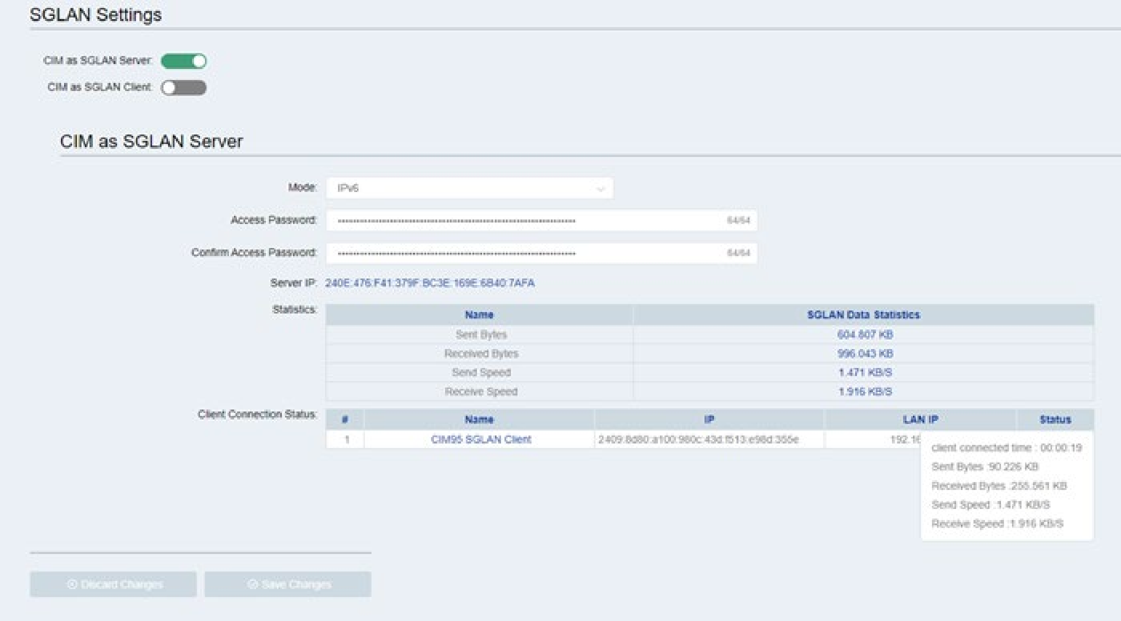
1. Enable "CIM as SGLAN Server".
2. Select the mode.

3. Set the "Access password" and confirm it in "Confirm access password".

Note

The default password for SGLAN server is “sglan”.

4. Click "Save changes".



SGLAN Settings

CIM as SGLAN Server: ●
CIM as SGLAN Client: ○

CIM as SGLAN Server

Mode: IPv6

Access Password: •• 64/64

Confirm Access Password: •• 64/64

Server IP: 240E:476:F41:379F:BC3E:169E:6B40:7AFA

Statistics:

Name	SGLAN Data Statistics
Sent Bytes	604.807 KB
Received Bytes	996.043 KB
Send Speed	1.471 KB/S
Receive Speed	1.916 KB/S

Client Connection Status:

#	Name	IP	LAN IP	Status
1	CIM95 SGLAN Client	2409:8d80:a100:980c:43d:f513:e98d:355e	192.16	

client connected time : 00:00:19
Sent Bytes :90.226 KB
Received Bytes :255.561 KB
Send Speed :1.471 KB/S
Receive Speed :1.916 KB/S

5.4.4.2 Setting up SGLAN client

This page allows you to set the CIM work as SGLAN client.

Note

To works as an SGLAN client, CIM must meet the following requirements:

- CIM can access the Internet through IPv4/IPv6
- The IPv4/IPv6 address assigned to SIM card by telecom operator can be accessed over the Internet through IPv4/IPv6
- The SIM card in CIM supports sending and receiving short message if you set up SGLAN by SMS
- The IP of the devices in SGLAN are in the same subnet and not conflict with each other

Requirement

- You get the following information of the SGLAN server: Mode, Server IP address/Phone number, access password.

Connecting to SGLAN as CIM client

To connect the SGLAN server, you need to get the mode, IP address/phone number, and access password of CIM SGLAN server.

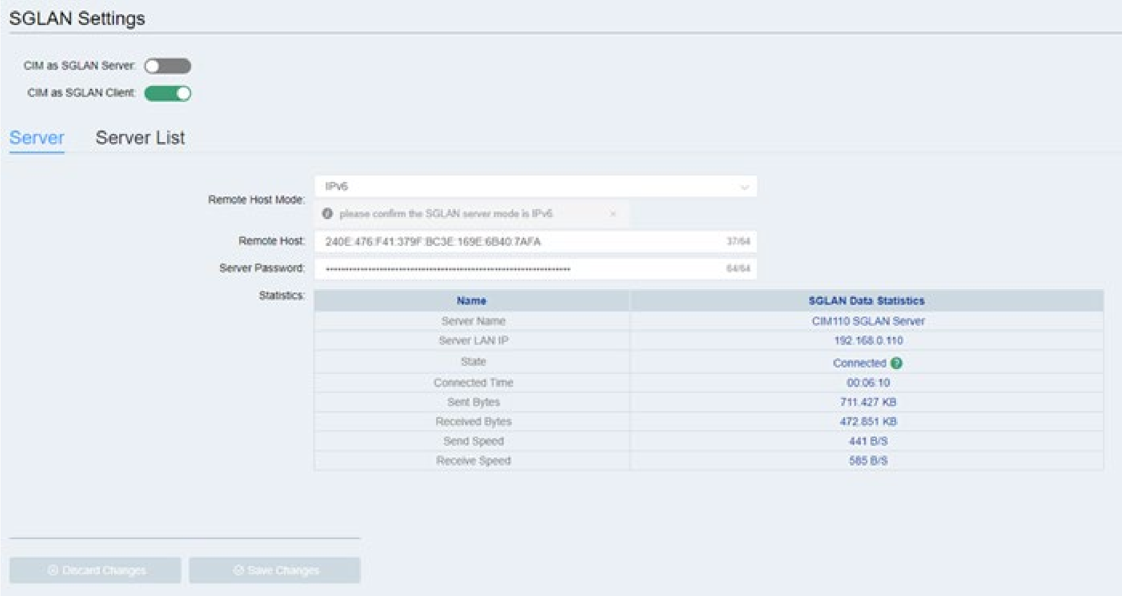
1. Enable "CIM as SGLAN Client".
2. Select the remote host mode.
3. Select "Remote Host Mode" for setting up SGLAN.
   - If you select "IPv4/IPv6", enter the server IP address of the CIM server.
   - If you select "SMS_v4/SMS_v6", enter the phone number of the CIM server.

4. Enter the access password of CIM server in the input field next to "Server Password".

Note

If you have enabled SGLAN server without changing the password, you can connect to the SGLAN server with the default password "sglan".

5. Click "Save changes".



SGLAN Settings

CIM as SGLAN Server: ○

CIM as SGLAN Client: ●

Remote Host Mode: IPv6

please confirm the SGLAN server mode is IPv6

Remote Host: 240E:476:F41:379F:BC3E:169E:6B40:7AFA 37/64

Server Password: ••• 64/64

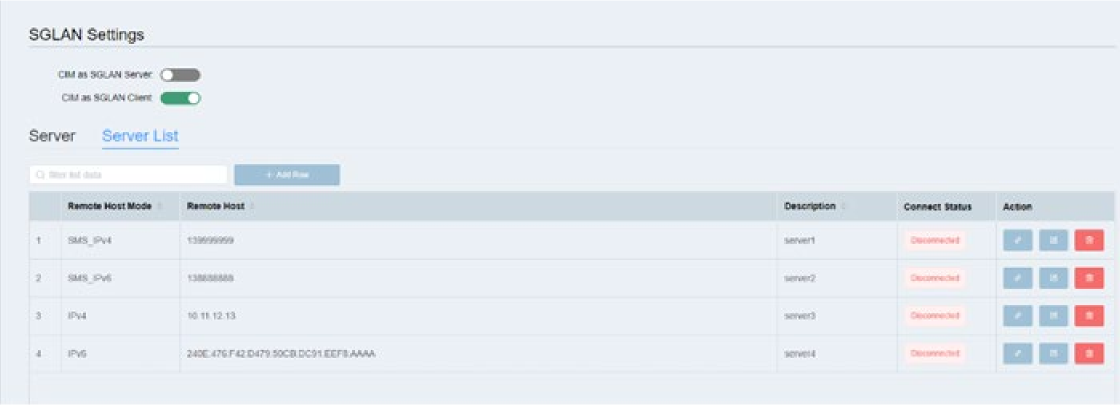
Statistics:

Name	SGLAN Data Statistics
Server Name	CIM110 SGLAN Server
Server LAN IP	192.168.0.110
State	Connected
Connected Time	00:06:10
Sent Bytes	711.427 KB
Received Bytes	472.851 KB
Send Speed	441 B/S
Receive Speed	585 B/S

Connection Status	Description
Disconnected	Not connected to SGLAN
Connecting	The SGLAN client is connecting to the SGLAN server and setting up SGLAN.
Connected	The SGLAN is setup and the SGLAN client is connected to SGLAN server.
Connect error	Failed to establish the communication between SGLAN Client and SGLAN Server
Connect timeout	Establish the communication between SGLAN Client and SGLAN Server timed out
Login fail	Login fail due to password error
Login timeout	Failed to login in within valid time
Connect break	The SGLAN is disconnected due to long-term failure of network communicate
Certificate error	Failed to verify the certificate
General error	General error

Server List

The server list allows you add SGLAN server devices you commonly used in it. You can use this server list to quickly connect to the SGLAN server.



SGLAN Settings

CIM as SGLAN Server ○
CIM as SGLAN Client ●

Server | Server List

Filter list data | + Add Row

	Remote Host Mode	Remote Host	Description	Connect Status	Action
1	SMS_IPv4	139999999	server1	Disconnected	
2	SMS_IPv6	138888888	server2	Disconnected	
3	IPv4	10.11.12.13	server3	Disconnected	
4	IPv6	240E:476:F42:D479:50CB:DC91:EEF8:AAAA	server4	Disconnected	

Create a server item

1. Click "**Add Row**" button.
2. Enter the server information. You can add maximum 64 server items at most.

   Description: description of the SGLAN server

   Remote Host Mode: remote host mode of SGLAN server

   Remote Host: IP address or phone number of SIM card of the remote host

   Server Password: password of the SGLAN server
3. Click "Save" to confirm the server information or click "Cancel" to discard the information.
4. Repeat step 1-3 to add all server items you need.

Connect the device

Click 🔗 to connect the SGLAN server.

Edit a server item

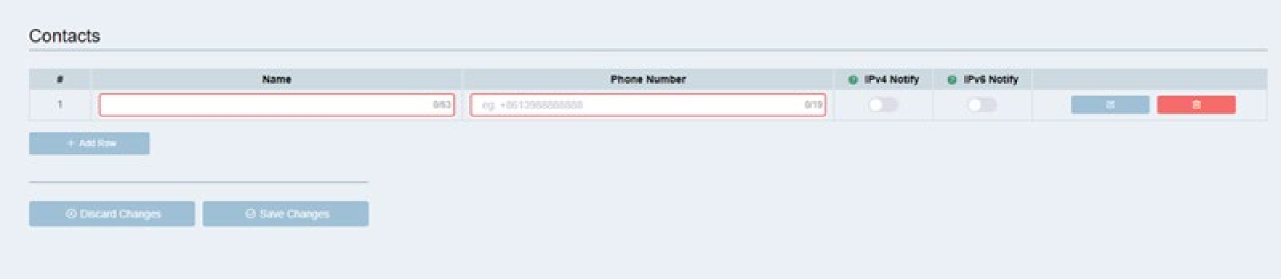
Click 📝 then enter the new value to the corresponding filed of the server item you want to change.

Delete a server item

Click 🗑 delete button next to the server item you want delete.

5.4.5 Contacts

In this table, you can configure the contacts for sending or receiving SMS messages. You can add a maximum of 16 contacts for CIM.



Contacts

#	Name	Phone Number	IPv4 Notify	IPv6 Notify	
1	0/63	eg: +8613988888888 0/19	○	○	

+ Add Row

Discard Changes   Save Changes

Add a contact

1. Click "Add Row".
2. Enter the "Name" and "Phone Number" of the contact.

   Name: A name can contain letters, numbers and special characters.

   Phone number: Phone number through which the user can be reached.

   IPv6 Notify: Notify the contact if the IP address for IPv6 is changed.

   IPv4 Notify: Notify the contact if the IP address for IPv4 is changed.

   Note

   When you enter an international number, use "+" as the exit code. For example, "+86".

   The contact name must be unique.

3. Repeat step 2 to add all the contacts as you need.
4. Click "Save Changes" to save the change or click "Discard Changes" and "Confirm" to discard the change.

Note

If the message is referred by event, action or power on/off, the message cannot be edited or deleted.

Change a contact

1. Click ✎ for the contact you want to edit, then enter the new value directly.

Delete a contact

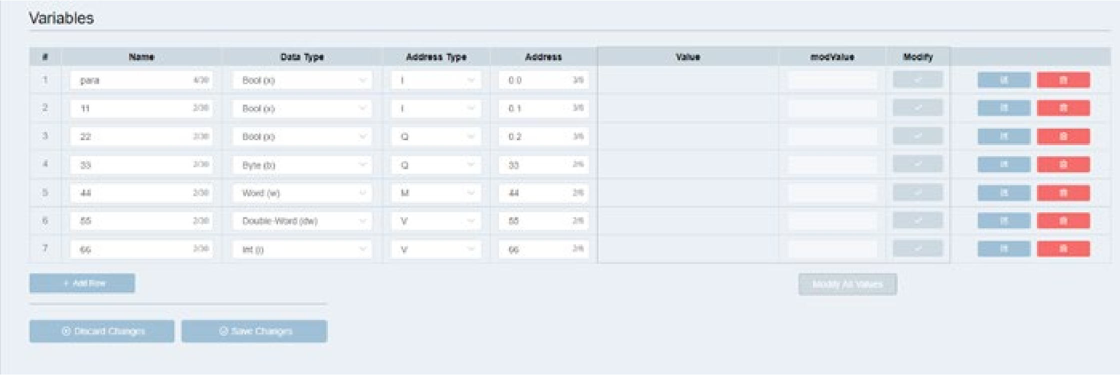
1. Click 🗑 for the contact you want to delete.

5.4.6 Data management

Data management allows you to manage the variables, messages and data bindings and monitor the online variables. The names for variables, messages, and data bindings must be unique.

5.4.6.1 Variables

The variable is defined by variable name, data type, address type and address. This chapter shows how to create and edit variables that you use to store values in CIM. You can create variables for all data type UDM permitted.



Variables

#	Name	Data Type	Address Type	Address	Value	modValue	Modify
1	para 4/30	Bool (x)	I	0.0 3/5			✓
2	11 2/30	Bool (x)	I	0.1 3/5			✓
3	22 2/30	Bool (x)	Q	0.2 3/5			✓
4	33 2/30	Byte (b)	Q	33 2/5			✓
5	44 2/30	Word (w)	M	44 2/5			✓
6	55 2/30	Double-Word (dw)	V	55 2/5			✓
7	66 2/30	Int (i)	V	66 2/5			✓

Add a variable

1. Click 'Add Row' button.
2. Enter the parameters of the variable. You can add maximum 16 variables at most.

   Name: A variable name can contain letters, numbers and special characters

   Data type: data type of the variable

   Address type: UDM address type of variable

   Address: address in the CIM
3. Repeat step 1-2 to add all variables you need.
4. You can monitor or modify the value of the variable.

   Value: the value of the parameter

   Modify value (modValue): enter the value of the parameter you want to modify

   Modify: click the check mark to modify the value of the parameter

   Modify all values: click "Modify all values" to modify the value of parameter as modValue

---

Note

If the variable is referred by an event or an action, the variable cannot be changed or deleted.

Change a variable

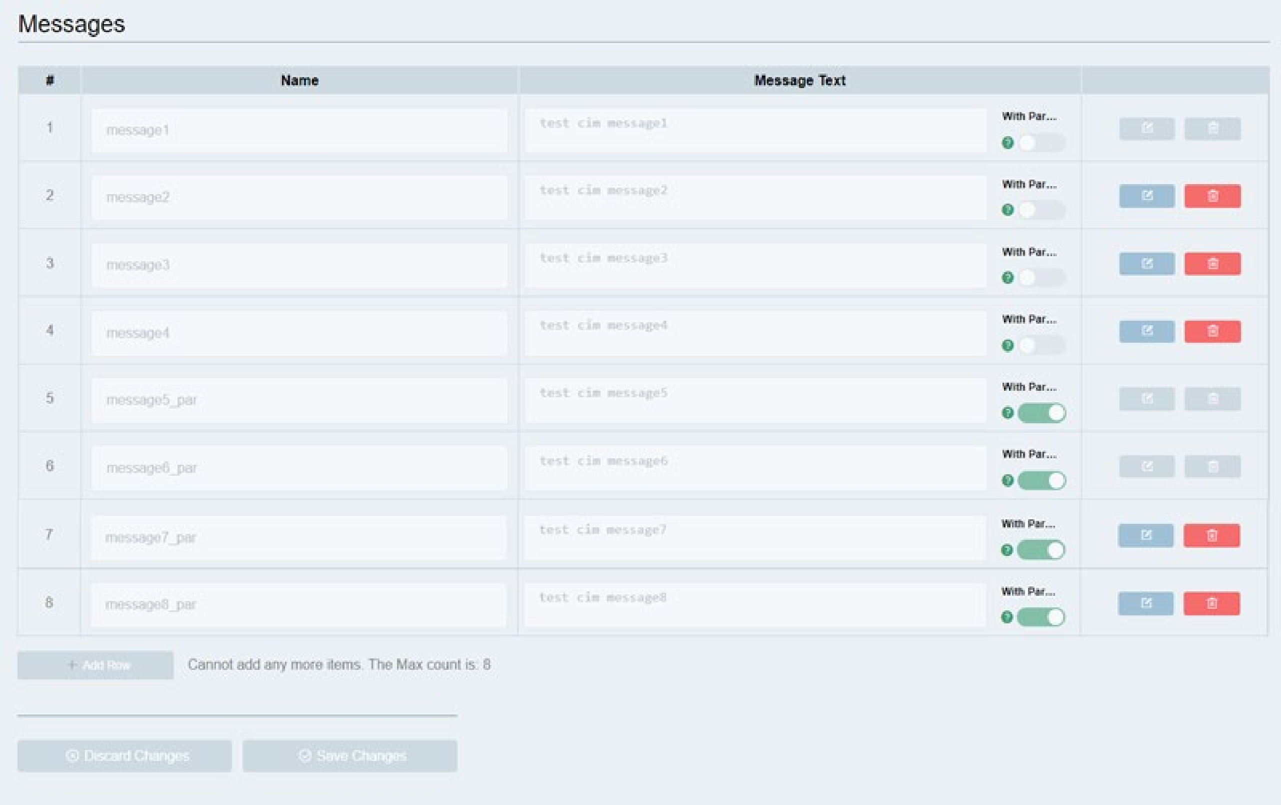
Click ✎ then enter the new value to the corresponding filed of the variable you want to change.

Delete a variable

Click 🗑 delete button next to the variable you want delete.

5.4.6.2 Messages

This page allows you add or edit a message that CIM can send and receive.



Messages

#	Name	Message Text	With Par...	
1	message1	test cim message1	○	✎ 🗑
2	message2	test cim message2	○	✎ 🗑
3	message3	test cim message3	○	✎ 🗑
4	message4	test cim message4	○	✎ 🗑
5	message5_par	test cim message5	●	✎ 🗑
6	message6_par	test cim message6	●	✎ 🗑
7	message7_par	test cim message7	●	✎ 🗑
8	message8_par	test cim message8	●	✎ 🗑

+ Add Row Cannot add any more items. The Max count is: 8

Add a message

1. Click "Add Row".
2. Enter the title and message text. You can add maximumly 8 messages. A title and message text can contain letters, numbers and special characters.

   Title: The title of the message.

   Message text: the content of the message.

3. Toggle on "With parameter" as you need.

Note

If you toggled on "with parameter", the variable value of the bind event will be added in the message CIM sends. If the parameter is in hexadecimal, 0x is also added before the value.

- Message content with parameter: message text + value of the parameter.
- Message content with parameter in hexadecimal: message text + 0x+value of the parameter.

For the allowed parameters, refer RESTful API (Page 74).

4. Repeat the steps 1-3 to add all messages you need.

Note

If the message is referred by an event or an action, the message cannot be changed or deleted.

Change a message

Click ✎ for you message you want to change, then enter the new name and message text.

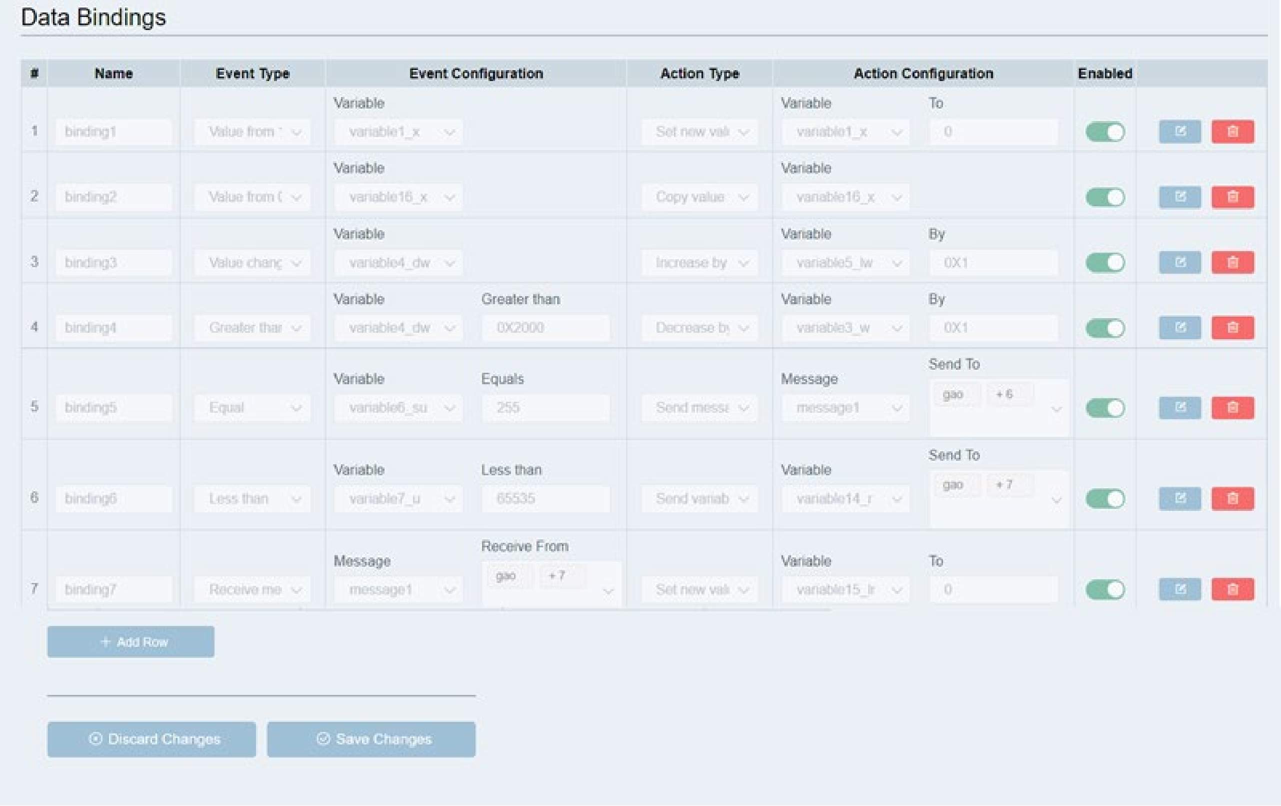
Delete a message

Click 🗑 for the message you want to delete.

5.4.6.3 Data Binding

This page allows you to bind an event to an action. Refer to Universal Data Model (Page 11) for more information.

Event is defined by you. An event can be variable change or receiving message. You can set an action CIM will take when the event you set happens.



Data Bindings

#	Name	Event Type	Event Configuration		Action Type	Action Configuration		Enabled	
1	binding1	Value from '	Variable variable1_x		Set new valı	Variable variable1_x	To 0	●	
2	binding2	Value from (	Variable variable16_x		Copy value	Variable variable16_x		●	
3	binding3	Value chang	Variable variable4_dw		Increase by	Variable variable5_lw	By 0X1	●	
4	binding4	Greater thar	Variable variable4_dw	Greater than 0X2000	Decrease by	Variable variable3_w	By 0X1	●	
5	binding5	Equal	Variable variable6_su	Equals 255	Send messa	Message message1	Send To gao +6	●	
6	binding6	Less than	Variable variable7_u	Less than 65535	Send variab	Variable variable14_r	Send To gao +7	●	
7	binding7	Receive me	Message message1	Receive From gao +7	Set new valı	Variable variable15_lr	To 0	●	

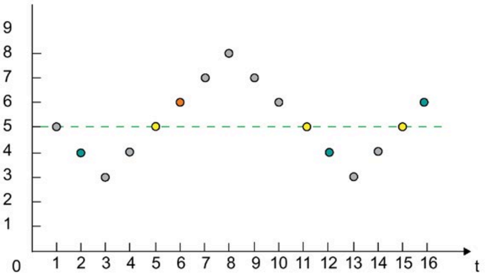
Bind data

1. Click "Add Row" to add a new row.
2. Click the "Event Type" drop-down list to choose and event.

	Event	Event source	Source restriction
1	Changes from 1 to 0	Variable	Permitted data type: bool
2	Changes from 0 to 1		
3	Value Changed		Permitted data type: all UDM permitted data type except bool.
4	Greater than		Permitted data type: all UDM permitted data type except bool. **Note**: The type and range of the reference value should be the same as event source variable.
5	Equals		
6	Less than		
7	Receives message	Message	Any message

Note

The event "Greater than" is triggered on the rising edge, while "Less than" is triggered on the falling edge.



⚪ No event triggered.

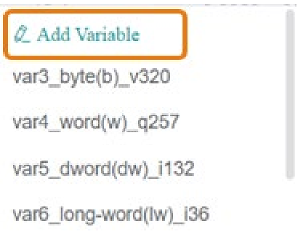
🟠 Event "Greater than 5" is triggered.

🟡 Event "Equals 5" is triggered.

🔵 Event "Less than 5" is triggered.

3. Configure the event, it can be change of a variable (Page 57) or receive Messages (Page 58) from a contact (Page 56).

   If there is no variable or message meet your requirement in the list, you can add variable or message on top of the list.



4. Set the action type.

	Action	Action source	Target restriction	Remark
1	Set new value	variable	Permitted data type: all UDM permitted data type.	
2	Copy value from event		The variable type of the action must be the same as the variable type of the source event it copied from.	If the event is "receive message" and the event source is a message without variable, then this action cannot be configured.
3	Increase by value		Permitted data type: all UDM permitted data type except bool.	• The increase or decrease value can only be positive. • If the variable reaches the maximum or minimum value of its range, the variable will not increase or decrease any more.
4	Decrease by value			
5	Send message	Message		• If the event is "receive message", this action type cannot be configured. • If the message contains a parameter, the parameter is the event parameter.
6	Send variable	Variable		• The format of the message is: variable name = value (short type) If the variable is in hexadecimal, 0x is added before the value, for example, v0.0 = 0x10(b) • If the event is "receive message" and the event source is a message without variable, then this action cannot be triggered.

5. Configure the action.
   - If the action is a variable change, you need to select a variable from the variable list and fill the new value in the input box below **To**.
   - If the action is sending a message, you need to select a message from the message list.
6. Enable the bind.

Note

If you didn't set any variable, message, or contact yet, the selectable event and action cannot display completely.

Change a data binding

Click ✎ for you data binding you want to change, then enter the new title and contact.

Delete a data binding

Click 🗑 for the data binding you want to delete.

5.4.6.4 Online Monitor

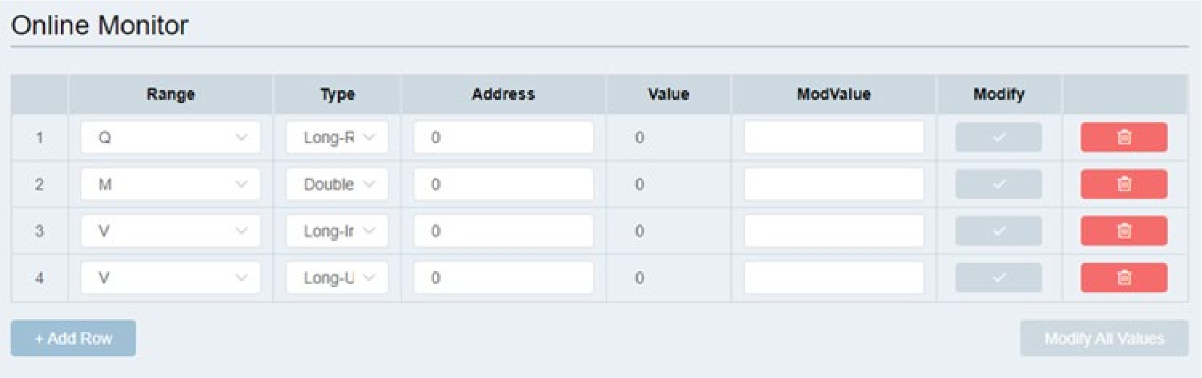
In the online UDM data table, you can monitor the UDM data through CIM web server.

Note

Online variables in the online variable page are saved in the browser

As the online variables in the online variable page are saved in the browser, you should note the following issues:

- Make sure you do not set your browser to private mode when you use CIM online monitor, since your browser does not record any browsing history in this mode.
- Variable configuration in online monitor page will not be cleared after factory resetting the CIM.
- Variable configuration in online monitor page does not exist when you change the browser or clear the data in browser.



Online Monitor

	Range	Type	Address	Value	ModValue	Modify	
1	Q	Long-R	0	0		✓	🗑
2	M	Double	0	0		✓	🗑
3	V	Long-Ir	0	0		✓	🗑
4	V	Long-U	0	0		✓	🗑

Add an online variable

1. Click 'Add Row' button.
2. Enter the parameters of the variable. You can add maximum 16 variables at most.

   Range: UDM address type of variable

   Type: data type of the variable

   Address: address in the CIM

   Value: variable value in the selected address

   ModValue: the new value you want to enter in the selected address

   Modify: Click the check mark to modify the value in the selected address
3. Repeat step 1-2 to add all variables you need.

Delete a variable

Click 🗑delete button next to the variable you want delete.

Click "Modify All values" to save all the changes.

5.4.7 Protocol Settings

5.4.7.1 Overview for multi-protocol

This page allows you to configure the following protocols: S7, Modbus TCP, Modbus RTU, RESTful API.

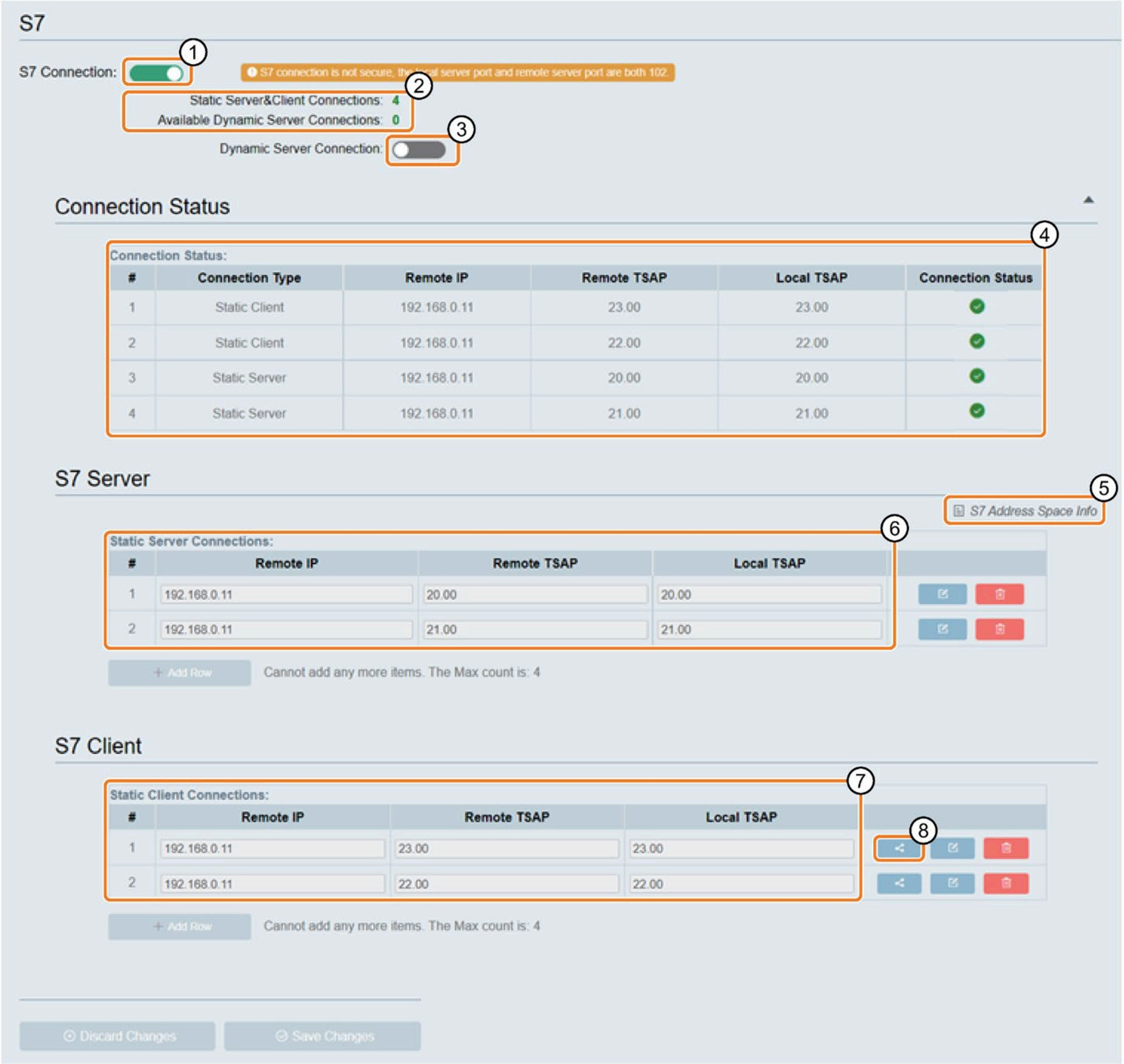
5.4.7.2 S7

This page allows you enable or disable the S7 connections, as well as check and edit the S7 connections.

CIM supports maximum four S7 connections simultaneously at most. CIM will share the connections if it acts as S7 server and S7 client at the same time.

Note

When you setup S7 communication between a remote device to CIM, make sure S7 communication is enabled in the connected remote device.



S7

S7 Connection: ●

S7 connection is not secure, the local server port and remote server port are both 102.

Static Server&Client Connections: 4
Available Dynamic Server Connections: 0

Dynamic Server Connection: ○

Connection Status

Connection Status:

#	Connection Type	Remote IP	Remote TSAP	Local TSAP	Connection Status
1	Static Client	192.168.0.11	23.00	23.00	✓
2	Static Client	192.168.0.11	22.00	22.00	✓
3	Static Server	192.168.0.11	20.00	20.00	✓
4	Static Server	192.168.0.11	21.00	21.00	✓

S7 Server

S7 Address Space Info

Static Server Connections:

#	Remote IP	Remote TSAP	Local TSAP
1	192.168.0.11	20.00	20.00
2	192.168.0.11	21.00	21.00

+ Add Row   Cannot add any more items. The Max count is: 4

S7 Client

Static Client Connections:

#	Remote IP	Remote TSAP	Local TSAP
1	192.168.0.11	23.00	23.00
2	192.168.0.11	22.00	22.00

+ Add Row   Cannot add any more items. The Max count is: 4

Discard Changes   Save Changes

① Enable or disable the S7 connection
Note: S7 connection is not secure.

② Summary of the S7 connections

③ Enable or disable the Dynamic server connection
Note: CIM support maximumly four S7 connections simultaneously. If you have set some static connections,
the number of the dynamic server connections = 4 - the number of the static connections

④ Status of current S7 connections
Click ▼ to expand the connection list or click ▲ to collapse the connection list.

⑤ Link to S7 address space information page

⑥ Here you configure the properties of the connections that CIM work as S7 server.

- Remote IP: the IP of the client that you want to connect
- Local TSAP: the TASP in CIM is 00.01 to FF.FF
- Remote TSAP: the TSAP of the client that you want to connect

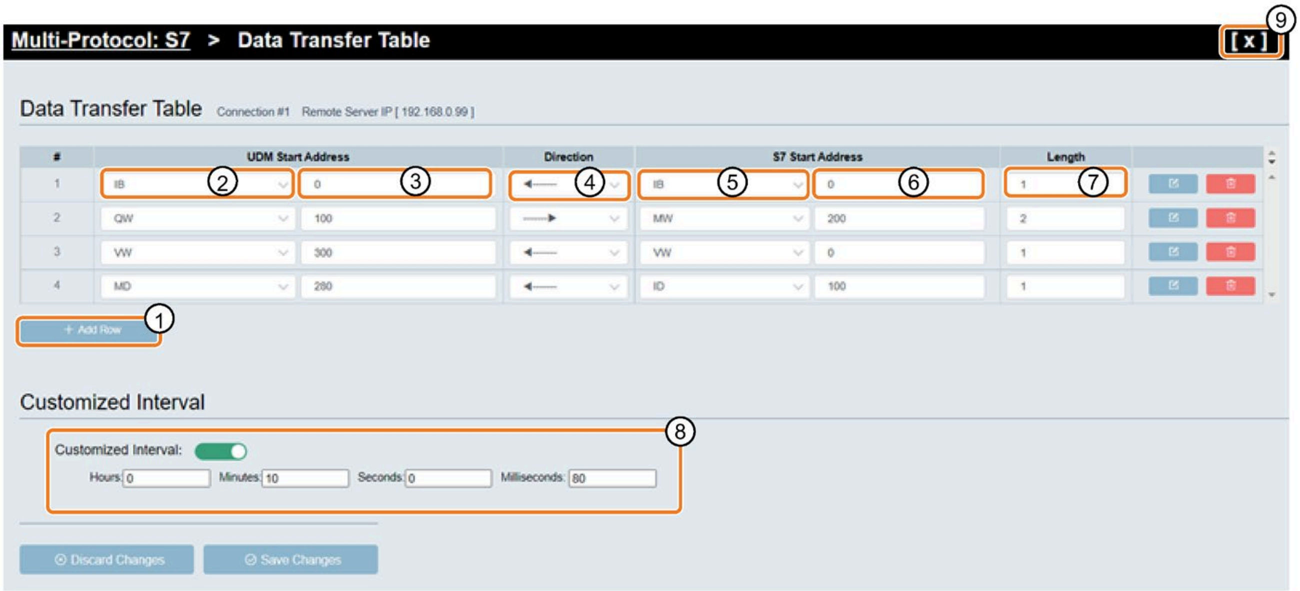
⑦ Here you configure the properties of the connections that CIM work as a S7 client

- Remote IP: the IP of the server that you want to connect
- Remote TSAP: the TSAP of the server that you want to connect
- Local TSAP: the TASP in CIM is 00.01 to FF.FF

⑧ Click to open the "Data transfer table" of the corresponding connection that CIM work as a S7 client.

Data transfer table configuration

For the connections that CIM works as S7 client, you need to configure the data transfer table:



Multi-Protocol: S7 > Data Transfer Table

Data Transfer Table Connection #1 Remote Server IP [192.168.0.99]

#	UDM Start Address		Direction	S7 Start Address		Length	
1	IB	0	◀——	IB	0	1	
2	QW	100	——▶	MW	200	2	
3	VW	300	◀——	VW	0	1	
4	MD	280	◀——	ID	100	1	

Customized Interval

Customized Interval: ●

Hours: 0 Minutes: 10 Seconds: 0 Milliseconds: 80

1. Click "Add Row".
2. Click ② to choose the UDM address type of CIM.
3. Input one address in the address field of CIM ③.
4. Click the ④ to choose data transfer directions.
5. Click ⑤ to choose S7 address type of the remote S7 server.
6. Input the S7 Start address of the remote S7 server ⑥.
7. Input the length of the Data ⑦ need to be transferred.
8. To set the time interval that CIM synchronizes the data with the server, enable "Customized Interval" and input the specified time interval ⑧.

   The default minimum transmit interval is 80 milli-second.

9. Save your changes.

10.Click ⑨ to close the Data transfer table.

Note

You can add maximum of 16 rows most.

Data transfer restrictions

The table below describes the range and local address restrictions for client connections.

Read and Write requests:

Local address (CIM)		**Remote address (S7 compatible device)**
Address Type	Range	Address Type
IB	0 to 511	IB, QB, MB, VB, Data Block
QB	0 to 511	
MB	0 to 511	
VB	0 to 1023	
IW	0 to 510	IW, QW, MW, VW, Data Block
QW	0 to 510	
MW	0 to 510	
VW	0 to 1022	
ID	0 to 508	ID, QD, MD, VD, Data Block
QD	0 to 508	
MD	0 to 508	
VD	0 to 1020	

Note

The address type is the combination of the process image name in UDM (Page 11) and data type. For example, IB means byte in memory I.

The values should follow the rule: Local address + Data length ≤ Max value of Local address type.

5.4.7.3 Modbus TCP

This page allows you enable or disable the Modbus TCP connections, configure transfer table of Modbus communication, as well as check the connection status.

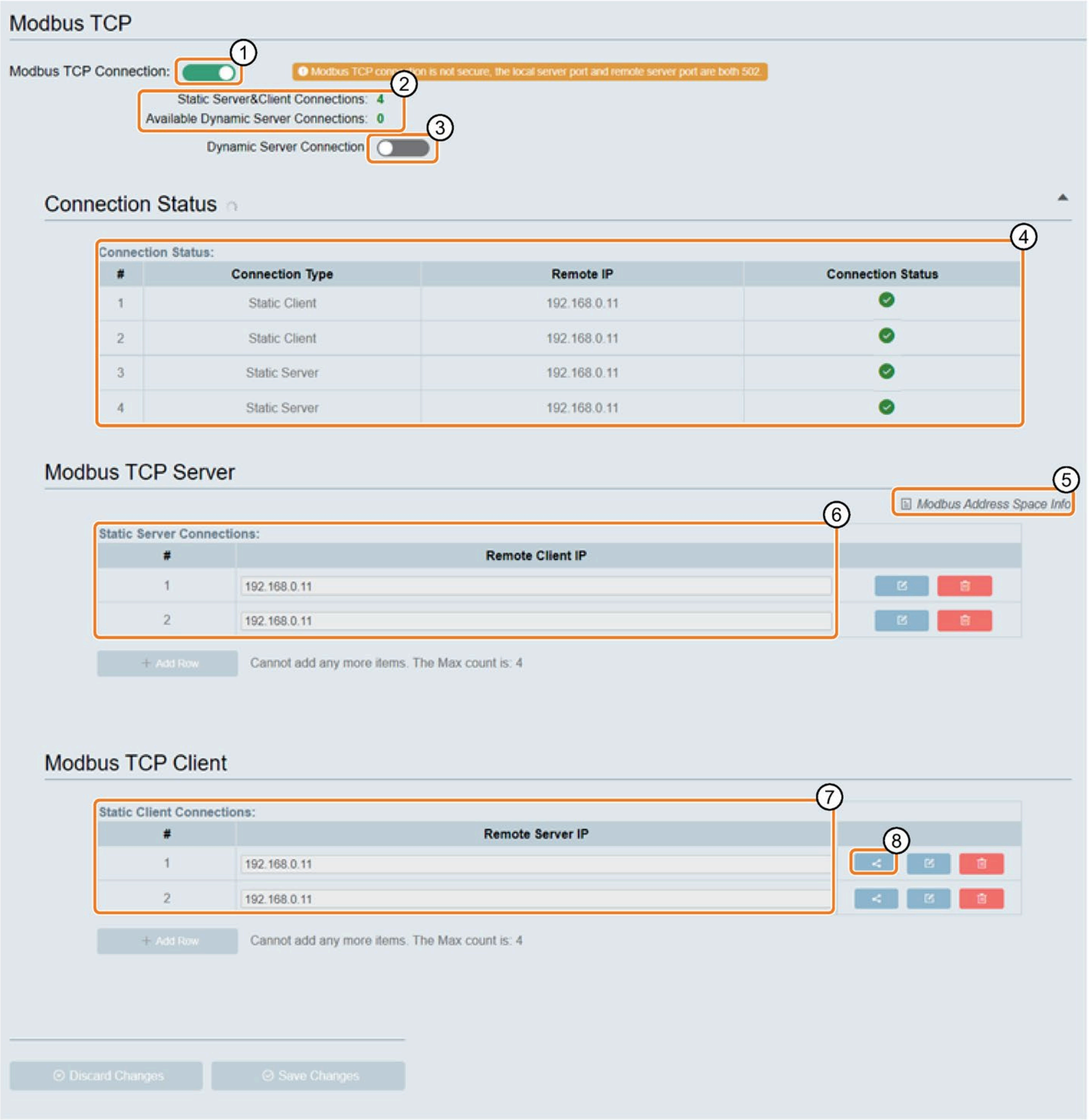
CIM support maximum four Modbus TCP connections simultaneously at most. CIM will share the connections if it acts as a Modbus TCP server, Modbus TCP client at the same time.

Note

When you set up Modbus TCP communication between two CIM, do enable S7 connection first.

Note

When you set up Modbus TCP communication between a remote device to CIM, make sure Modbus TCP communication is enabled in the connected remote device.



Modbus TCP

Modbus TCP Connection: ●

Modbus TCP connection is not secure, the local server port and remote server port are both 502.

Static Server&Client Connections: 4
Available Dynamic Server Connections: 0

Dynamic Server Connection ○

Connection Status

Connection Status:

#	Connection Type	Remote IP	Connection Status
1	Static Client	192.168.0.11	✓
2	Static Client	192.168.0.11	✓
3	Static Server	192.168.0.11	✓
4	Static Server	192.168.0.11	✓

Modbus TCP Server

Modbus Address Space Info

Static Server Connections:

#	Remote Client IP
1	192.168.0.11
2	192.168.0.11

+ Add Row   Cannot add any more items. The Max count is: 4

Modbus TCP Client

Static Client Connections:

#	Remote Server IP
1	192.168.0.11
2	192.168.0.11

+ Add Row   Cannot add any more items. The Max count is: 4

Discard Changes   Save Changes

① Enable or disable the Modbus TCP connection

Note: Modbus TCP connection is not secure.

② Summary for the Modbus TCP connection

③ Enable or disable the Dynamic server connection

Note: CIM support maximum four Modbus TCP connections simultaneously. If you have set some static connections,

the number of the dynamic server connections = 4 - the number of the static connections

④ Status of current Modbus TCP connections

⑤ Link to Modbus TCP address space information page

⑥ Here you configure the properties of the server.

- Remote IP: the IP of the client that you want to connect

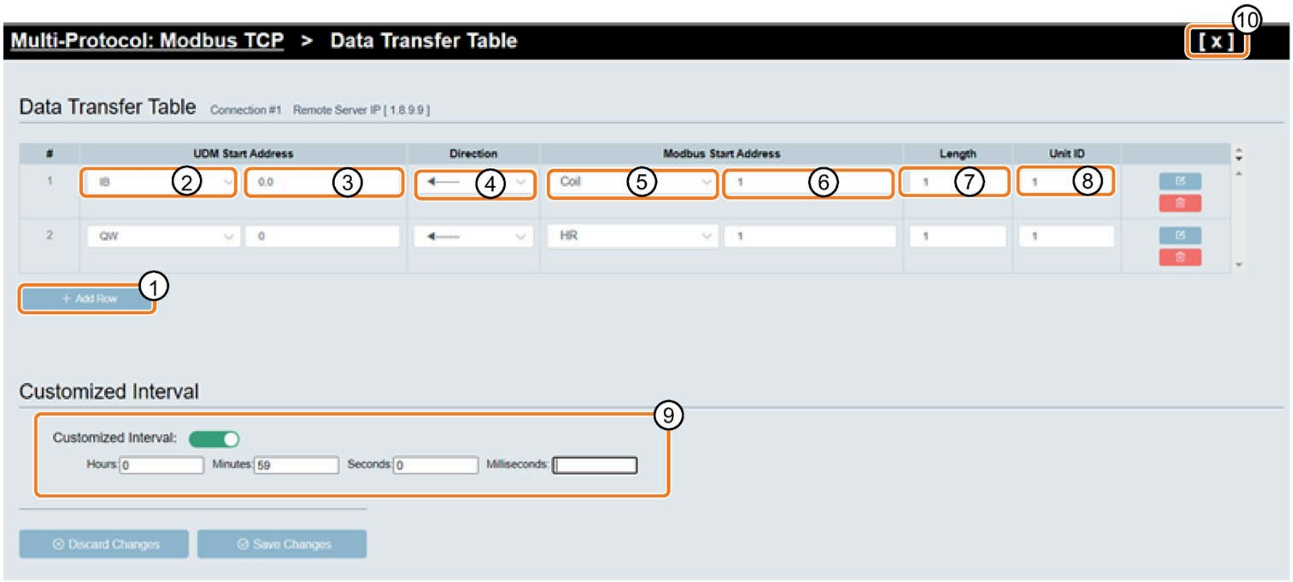
⑦ Here you configure the properties of the client.

- Remote IP: the IP of the server that you want to connect

⑧ Click to open the "Data transfer table" of the corresponding connection that CIM work as a Modbus TCP client.

Modbus TCP data transfer configuration

For the connections that CIM works as a Modbus TCP client, you need to configure the data transfer table:



Multi-Protocol: Modbus TCP > Data Transfer Table

Data Transfer Table Connection #1 Remote Server IP [1.8.9.9]

#	UDM Start Address		Direction	Modbus Start Address		Length	Unit ID
1	IB	0.0	←	Coil	1	1	1
2	QW	0	←	HR	1	1	1

Customized Interval

Customized Interval: ●

Hours: 0 Minutes: 59 Seconds: 0 Milliseconds:

1. Click ① to add a new row.
2. Click ② to choose UDM address type of CIM.
3. Input one address in the UDM start address field of CIM③.
4. Click ④ to choose data transfer directions.
5. Click ⑤ to choose Modbus address type of the remote Modbus TCP server.
6. Input the Modbus start address of the remote Modbus TCP server ⑥.
7. Input the length of the data need to be transferred ⑦.
8. Input the Unit ID ⑧.
9. To set the time interval that CIM synchronizes the data with the server, enable the customized interval and input the specified time interval ⑨.

   The default minimum transmit interval is 80 milli-second.
10. Save your changes and close the data transfer table.

Data transfer restrictions

The table below describes the range and local address restrictions for client connections.

Local address (CIM)		**Remote address (Modbus TCP compatible device)**
Address Type	Range	Address Type
IB	0.0 to 511.7	Coil Discrete Input (DI)
QB	0.0 to 511.7	
MB	0.0 to 511.7	
VB	0.0 to 1023.7	
IW	0 to 510	Holding Register (HR) Input Register (IR)
QW	0 to 510	
MW	0 to 510	
VW	0 to 1022	

Note

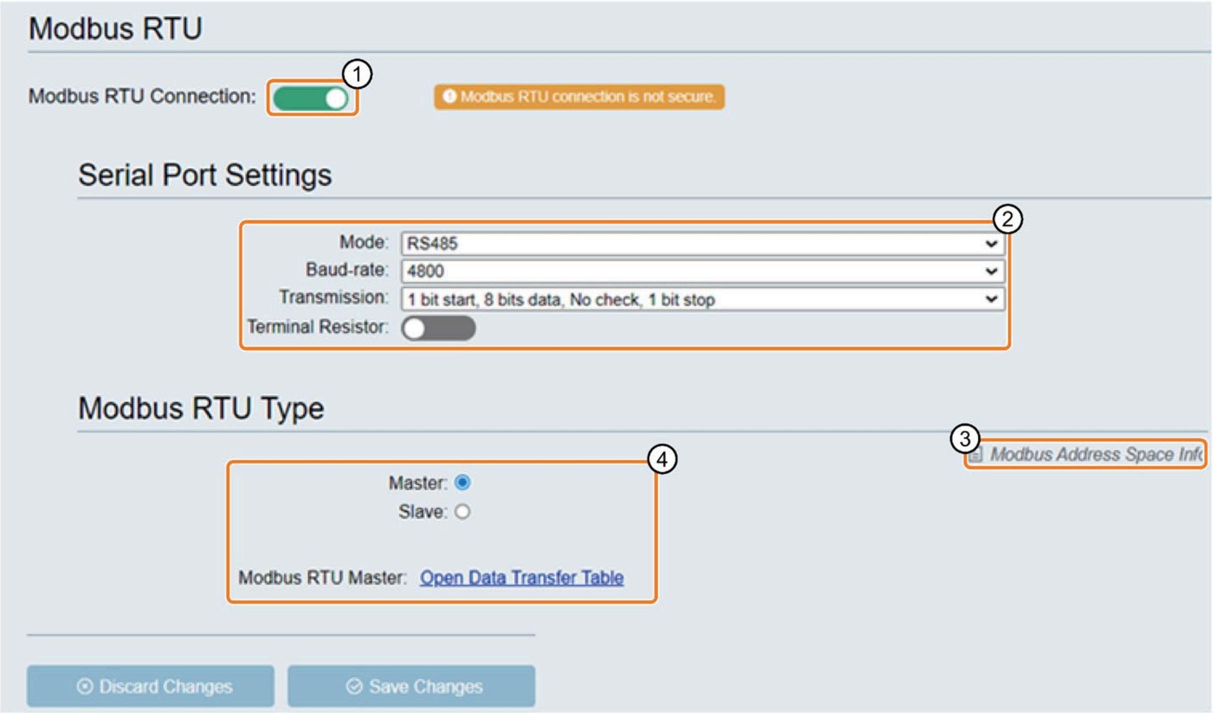
The address type is the combination of the process image name in UDM (Page 11) and data type. For example, IB means bit in memory I.

The values should follow the rule: Local address + Data length ≤ Max value of Local address type.

5.4.7.4 Modbus RTU

This page allows you enable, disable and set the Modbus RTU connection.

CIM supports only one Modbus RTU connection, either as Modbus RTU master or Modbus RTU slave.



Modbus RTU

Modbus RTU Connection: ①

Modbus RTU connection is not secure.

Serial Port Settings ②

Mode: RS485

Baud-rate: 4800

Transmission: 1 bit start, 8 bits data, No check, 1 bit stop

Terminal Resistor:

Modbus RTU Type ④

Master: ●

Slave: ○

Modbus RTU Master: Open Data Transfer Table

① Enable or disable the Modbus RTU connection
Note: Modbus RTU connection is not secure.

② Here you configure the properties of the connections of serial port.

- Mode: RS485, RS422 or RS232
- Baud-rate: set the transfer speed
- Transmission: serial port setup
- Terminal Resistor: enable or disable the embedded terminal resistor

③ Link to Modbus address space information page

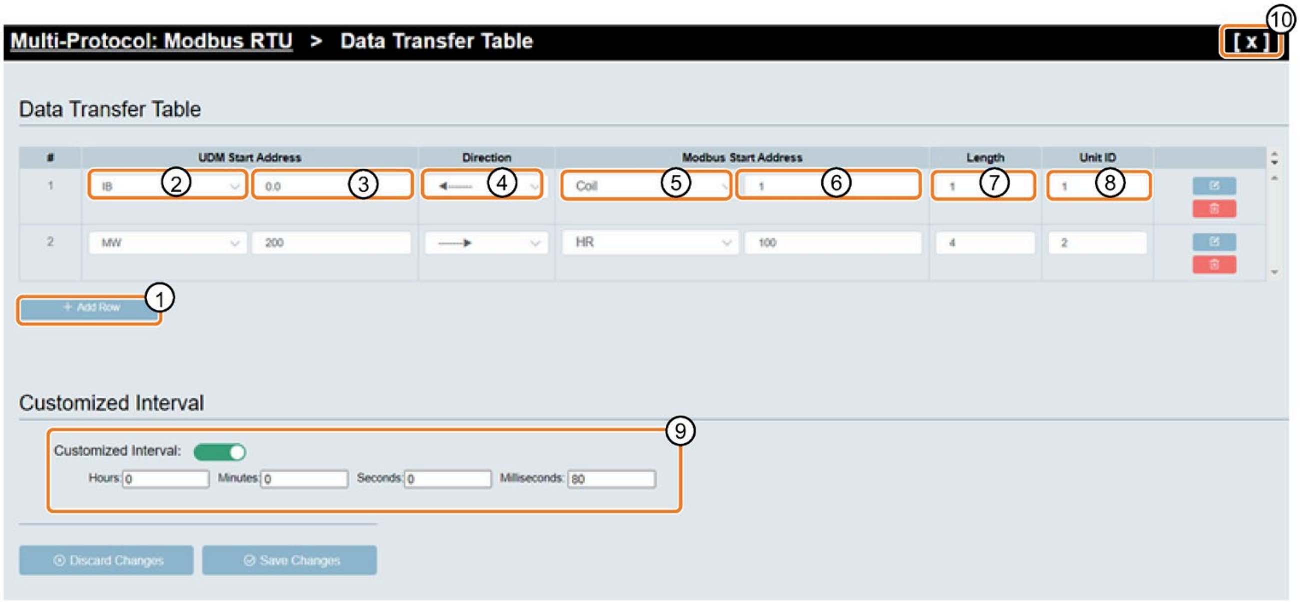
④ Here you configure the Modbus RTU Type

- If you select "Master", you need to set the "Data transfer table".
- If you select "Slave", you need to set the "Modbus RTU Slave ID".

  Range for the "Modbus RTU Slave ID": 1 to 255.

Set data transfer table

For the connections that CIM works as master, you need to set the following values in the data transfer table:



#	UDM Start Address		Direction	Modbus Start Address		Length	Unit ID
1	IB	0.0	←	Coil	1	1	1
2	MW	200	→	HR	100	4	2

Customized Interval: ●

Hours: 0 Minutes: 0 Seconds: 0 Milliseconds: 80

1. Click ① to add a new row.
2. Click ② to choose the UDM address type of CIM.
3. Input one address in the UDM start address field of CIM ③.
4. Click ④ to choose data transfer directions.
5. Click ⑤ to choose the Modbus address type of the remote Modbus RTU slave.
6. Input the Modbus start address of the remote Modbus RTU slave ⑥.
7. Input the length of the data need to be transferred ⑦.
8. Input the Unit ID of the remote Modbus RTU slave (Slave ID/Address) ⑧.
9. To set the time interval that CIM synchronizes the data with the server, select the check box and input the specified time interval ⑨.

   The default minimum transmit interval is 80 milli-second.

10.Save your changes and close the data transfer table.

Data transfer restrictions

The table below describes the range and local address restrictions for client connections.

Local address (CIM)		**Remote address (Modbus RTU compatible device)**
Address Type	Range	Address Type
IB	0.0 to 511.7	Coil Discrete Input (DI)
QB	0.0 to 511.7	
MB	0.0 to 511.7	
VB	0.0 to 1023.7	
IW	0 to 510	Holding Register (HR) Input Register (IR)
QW	0 to 510	
MW	0 to 510	
VW	0 to 1022	

Note

The address type is the combination of the address type name in UDM (Page 11) and data type. For example, IB means bit in memory I.

The values should follow the rule: Local address + Data length ≤ Max value of Local address type.

5.4.7.5 RESTful API

CIM also provides a REST interface for those users that are familiar with such technology and want to interact with CIM using an automated or programmed interface.

If the device connected to CIM supports RESTful, you can get or put data on UDM through RESTful API. For example, you can access the UDM interface by a Swagger user interface, which contains a detailed description of the classes, methods and parameters.

URI path format

```
https://[IP_address_for_cim]/pi/rest/[address_type][data_type_in_sho
rt][range]
```

Supported actions

- **get**
- **put**

  When you put a set of value to a range, separate them by ",".

Parameters

- **Address type**: i, m, v, q
- **Type**: data type of the access.
- **&**: connect multiple discrete address or address with different range or type
- **Range**: the range in the address type you want to read or write. The negative address means the position related the range end.

  Format for the range: start address~end address. If the range is not set, CIM regards you need the whole range of the address type.

  – ~end address: if the start address is not set, CIM regards the start address is the start of the range.

  – start address~: If the end address is not set, CIM regards the end address is the end of the range.

  – an address: access a single address.

  – Negative address: the address is counted from the range end.

Short data type	Data type	Length	Value range	Display	Example
x	bit	1 bit	0~1	0 or 1	1
b	byte	8 bit	0~FF	hex string	ab
w	word	16 bit	0~FFFF	hex string	aabb
dw	double-word	32 bit	0~FFFFFFFF	hex string	aabbccdd
lw	long-word	64 bit	0~FFFFFFFFFFFFFFFF	hex string	aabbccddaabbccdd
su	short-unsigned	8 bit	0~255	decimal	12
u	unsigned	16 bit	0~65535	decimal	1234
du	double-unsigned	32 bit	0~4294967295	decimal	12345678
lu	long-unsigned	64 bit	0~18446744073709551615	decimal	12345678
si	short-int	8 bit	-128~127	decimal	-12
i	int	16 bit	-32768~32767	decimal	-1234
di	double-int	32 bit	-2147483648~2147483647	decimal	-12345678
li	long-int	64 bit	-9223372036854775808 ~ 9223372036854775807	decimal	-12345678
r[1]	real	32 bit	-3.4E38 ~ +3.4E38	decimal	1234.5678
lr[1]	long-real	64 bit	-1.797E308 ~ +1.797E308	decimal	-1234.5678

[1] The significant digit for REAL and LONG REAL type cannot exceed 6.

Sample

The [address type][type][range] portion with in the examples below can be exchange with any of the allowed parameters.

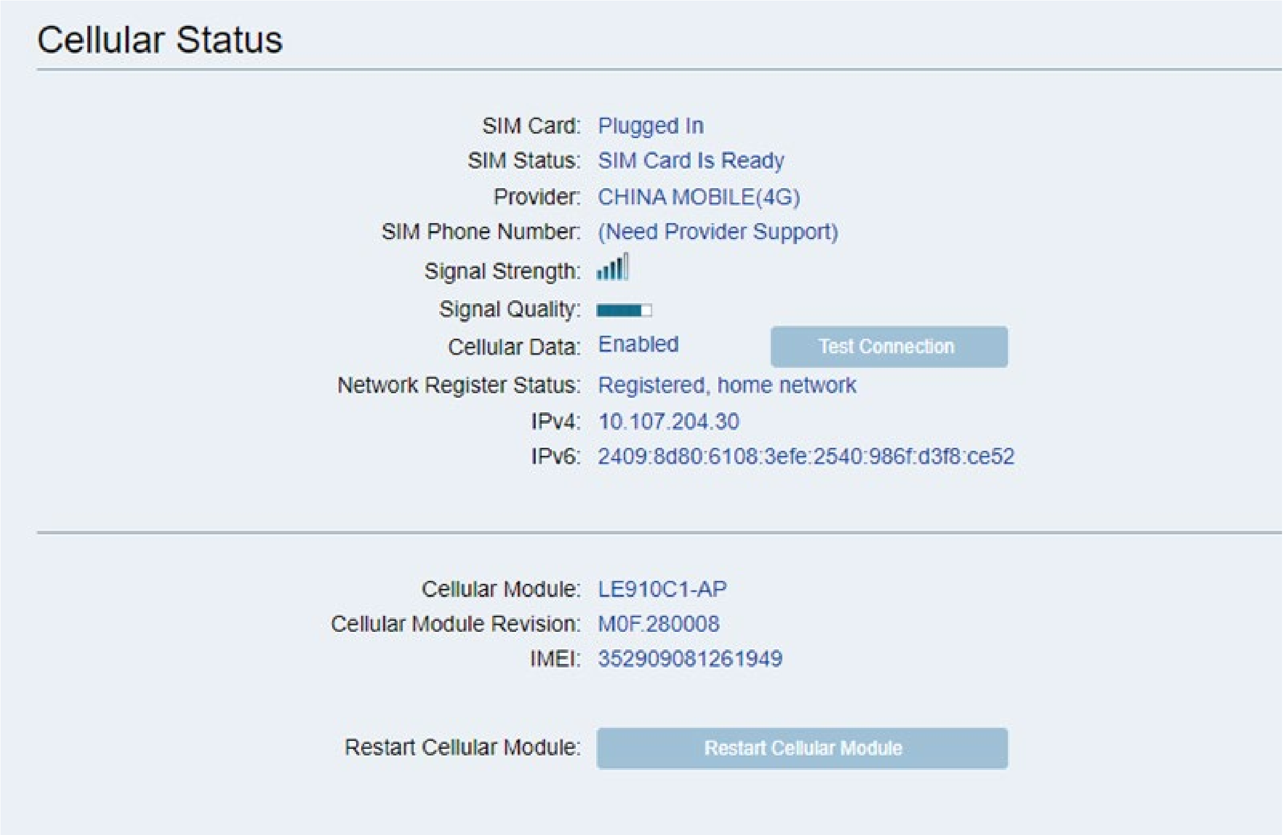
Example	Description
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3~8.7`	All bits at [5.3, 8.7] in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/i` `https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix`	All bit in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3`	A bit at 5.3 in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/ix5.3~8.7`	All bits in [5.3, 8.7] in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100`	A word at 100 in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100~200`	All words in [100, 200] in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/iw100~`	All words in [100, range_end] in range I
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qb100`	A byte at 100 in range Q
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr100`	A real at 100 in range Q
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr~100`	A real at [range start, 100] in range Q
`https://xxx.xxx.xxx.xxx:xxx/pi/rest/qr-100~-200`	All reals at [(range_size-200), (range_size-100)] in range Q
`https://xxx.xxx.xxx.xxx:xxxx/pi/rest/ix0.0&qi12`	A bit at 0.0 in range I and a bit at 12 in range Q [1]

[1] Starting from `/pi/rest/`, the length of the command should be within 500 English Characters.
Note: an wrong connector will cause the addresses cannot be recognized.

5.4.8 Cellular and GNSS

5.4.8.1 Cellular status

This page displays the current cellular network status.



Cellular Status

SIM Card: Plugged In
SIM Status: SIM Card Is Ready
Provider: CHINA MOBILE(4G)
SIM Phone Number: (Need Provider Support)
Signal Strength:
Signal Quality:
Cellular Data: Enabled
Network Register Status: Registered, home network
IPv4: 10.107.204.30
IPv6: 2409:8d80:6108:3efe:2540:986f:d3f8:ce52

Cellular Module: LE910C1-AP
Cellular Module Revision: M0F.280008
IMEI: 352909081261949

Restart Cellular Module:

Cellular status

Items	Meaning
SIM card	Plugged in / Not plugged in
SIM card status	Ready / Not Ready
Provider	Display the provider of the SIM card
SIM card number	Display the phone number of the SIM card
Signal strength	Display the level of signal strength
Signal Quality	Display the level of signal quality
Cellular data	Enabled / Disabled
Network register status	Network register status [1]
IPv4	IPv4 address
IPv6	IPv6 address
Cellular module	Cellular module type

Items	Meaning
Cellular module revision	Cellular module version
IMEI	International Mobile station Equipment Identity

[1] Register status

0 - not registered, terminal is not currently searching an new operator to register to

1 - registered, home network

2 - not registered, but terminal is currently searching an new operator to register

3 - registration denied

4 - unknown

5 - registered, roaming

Test the connection

You can test the connection of CIM to a specified destination device on Internet by the following steps:

1. Click the button "Test Connection".
2. Enter the IP address or URI, for example www.bing.com.
3. Click the "Test" button.

Note

This test is for the connection of CIM to a specified destination device, but not for the PC.

Restart cellular module

You can restart the cellular module by clicking the "Restart Cellular Module" button.

5.4.8.2 Cellular settings

This page allows you to set APN, Dial number and SMS Center number. You can get the APN, Dial number and SMS number from the SIM card provider.

Note

Siemens recommends only set these items when it is necessary.

Cellular settings

You can enable or disable the "Cellular data " in this field.

Advance setting

After enabling the advance setting, you can set the APN and Dial number for CIM:

APN: Access Point Name

Dial number: access code to the dial-up network.

SMS Center Number

You can set the SMS center number in this field.

5.4.8.3 Extra initialization commands

You can use this page to set your customized initialization commands for the cellular modular.

You can input multiple commands, each command starting with "AT" and ending with Enter. Consult the cellular module provider for detailed AT command.

5.4.8.4 GNSS settings

Current position

You can check the following information for CIM in this field:

- Latitude
- Longitude
- Speed
- Altitude
- Number and type of used satellites
- Total number of used satellites

Position settings

You can enable or disable "Map to UDM" in this field.

By clicking "Position Address Space Info", you can view the position address space information in UDM.

5.4.9 Security

5.4.9.1 Protocol

This page allows you check and manage all the protocols. You can enable/disable a protocol by toggling the switch. Except HTTPS, all other protocols are disabled by default.

Enable S7/Modbus TCP/Modbus RTU/NTP

When you enable the protocols, the settings of these protocols revert to the settings before disabling.

Disable S7/Modbus TCP/Modbus RTU/NTP

if you disabled a protocol, CIM cannot work as either a server or a client.

Note

RESTful API has no authentication

RESTful API is not safe. If you enabled the RESTful API, a device can connect to CIM by Restful API without authentication.

Only enable the RESTful API when needed.

5.4.9.2 Certificates

Before building connection with CIM, you need to select the certificate first.

- Owned certificate: generate and select certificate for setting up a secured web server and an SGLAN server
- Trusted certificate: select certificate for SGLAN client

Owned certificates

CIM provides three kinds of certificate solution for securely accessing Web configuration and setting up SGLAN server. CIM Build-in certificate is the default solution.

Certificate solution	Source	Size restricts (bytes)
CIM Build-in certificate	Signed by LOGO! Base module	1024
CIM internal certificate	Generated by CIM	1024
External certificate	Upload to CIM by you	4000

No matter which solution you select, make sure you install the certificate to your operating system or browser (Page 44) before using the Web-based configuration.

Note

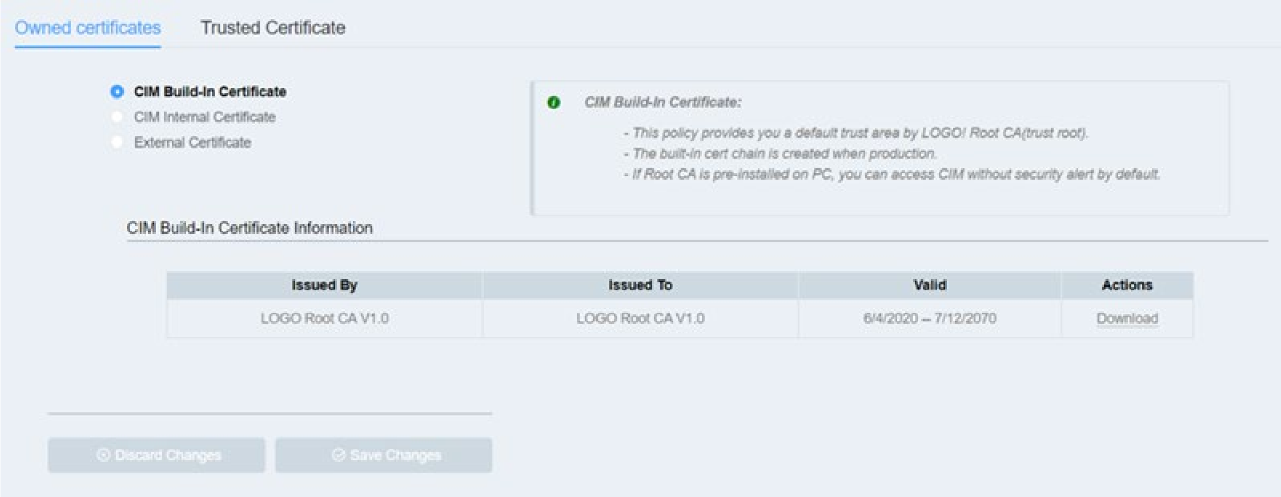
Siemens recommends you clear browser cache and restart the browser after you installed the certificate.

It takes about one minute for the certificate to take effect. Wait one minute before logging in the web-based configuration after you installed the certificate.

Download the CIM Build-in certificate

CIM Build-in certificate is created during the production.

1. Select Build-in certificate by selecting the check box next to it.
2. Click "Download" to download LOGO Root CA.



● CIM Build-In Certificate
○ CIM Internal Certificate
○ External Certificate

CIM Build-In Certificate:

- This policy provides you a default trust area by LOGO! Root CA(trust root).
- The built-in cert chain is created when production.
- If Root CA is pre-installed on PC, you can access CIM without security alert by default.

CIM Build-In Certificate Information

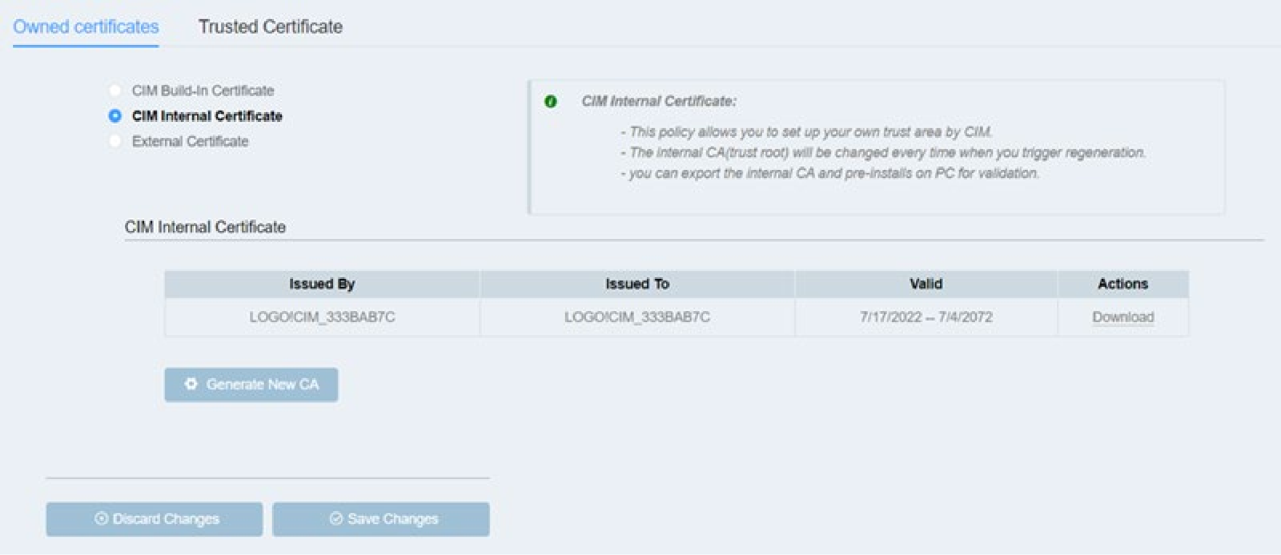
Issued By	Issued To	Valid	Actions
LOGO Root CA V1.0	LOGO Root CA V1.0	6/4/2020 – 7/12/2070	Download

Get the CIM internal certificate

CIM can generate certificate for itself.

1. Select CIM internal certificate by selecting the check box next to it.
2. Click "Generate" to generate CIM CA.

3. Click "Download" to download CIM CA.
4. Click "Save Changes" to save the change or click "Discard Changes" to discard the change.



○ CIM Build-In Certificate
● CIM Internal Certificate
○ External Certificate

CIM Internal Certificate:

- This policy allows you to set up your own trust area by CIM.
- The internal CA(trust root) will be changed every time when you trigger regeneration.
- you can export the internal CA and pre-installs on PC for validation.

CIM Internal Certificate

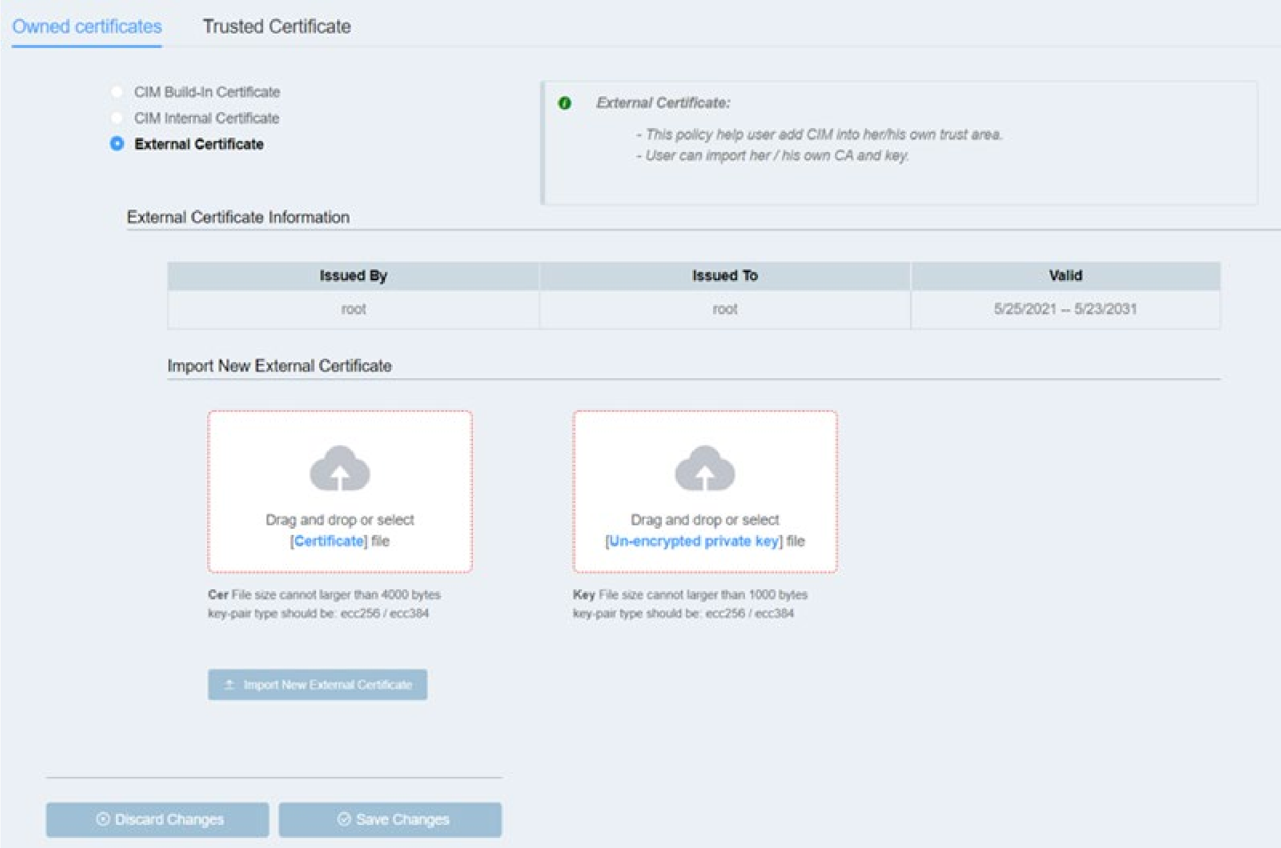
Issued By	Issued To	Valid	Actions
LOGO!CIM_333BAB7C	LOGO!CIM_333BAB7C	7/17/2022 -- 7/4/2072	Download

Upload the external CA

CIM allows you to import your own CA and key to CIM.

1. Select External certificate by selecting the check box next to it.
2. Drag and drop or select your own CA and key to the target file in the page.

3. Click "Import" to import the CA and key to CIM.
4. Click "Save Changes" to save the change or click "Discard Changes" to discard the change.



External Certificate:

- This policy help user add CIM into her/his own trust area.
- User can import her / his own CA and key.

External Certificate Information

Issued By	Issued To	Valid
root	root	5/25/2021 -- 5/23/2031

Import New External Certificate

Drag and drop or select [Certificate] file

Cer File size cannot larger than 4000 bytes
key-pair type should be: ecc256 / ecc384

Drag and drop or select [Un-encrypted private key] file

Key File size cannot larger than 1000 bytes
key-pair type should be: ecc256 / ecc384

Trusted Certificate

To build the SGLAN, you need to select the same trusted certificate in both server and client. CIM Build-in certificate is the default solution.

Note

Make sure the certificate you import to CIM client is in the validity period.

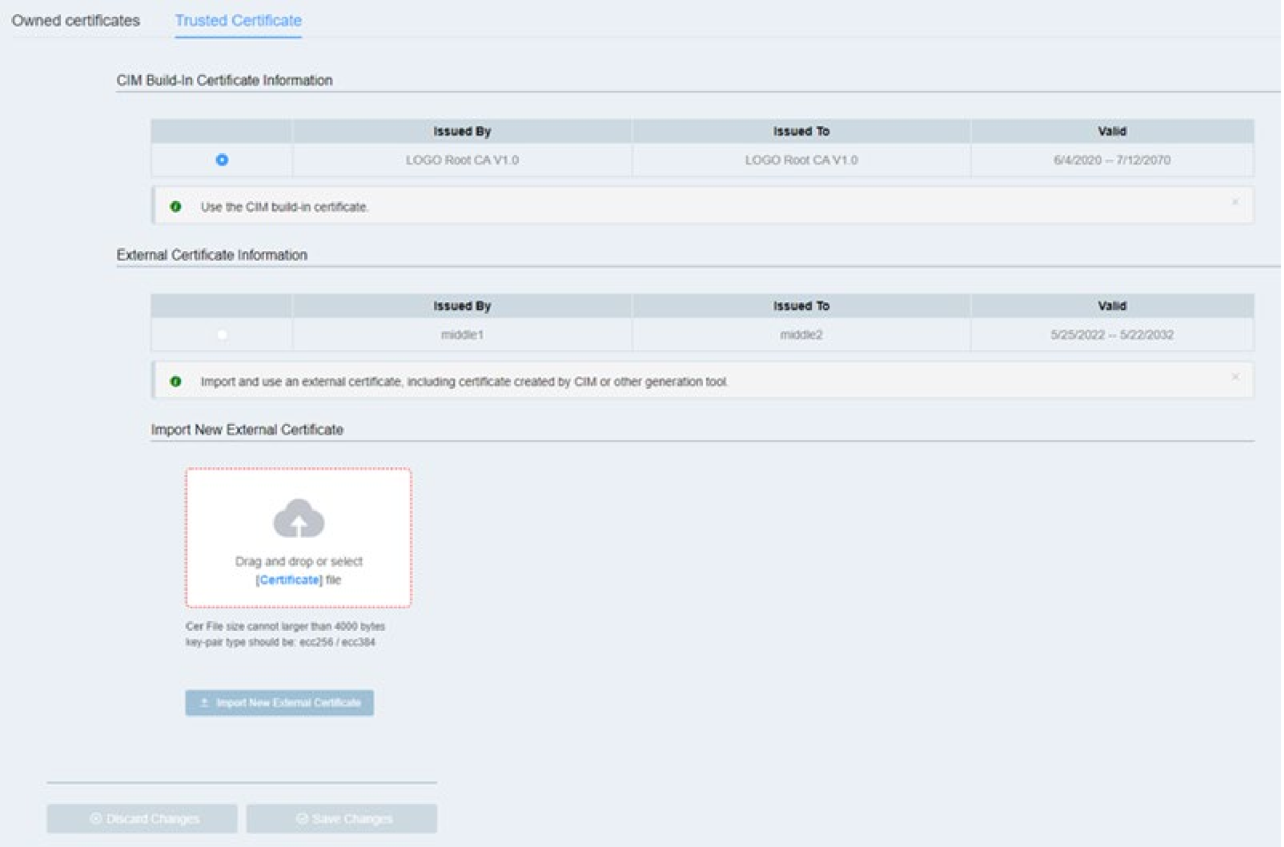
Certificate solution	Source	Size restricts (bytes)
CIM Build-in certificate	Signed by LOGO! Base module	1024
External certificate	Upload to server and client by you[1]	4000

[1] External certificate includes certificate created by CIM or other generation tool.

Import the external CA in CIM

Import external CA in CIM as follow.

1. Select External certificate by selecting the check box next to it.
2. Drag and drop or select your own CA to the target file in the page.
3. Click "Import New External Certificate" to import the CA to CIM.
4. Click "Save Changes" to save the change or click "Discard Changes" to discard the change.



CIM Build-In Certificate Information

	Issued By	Issued To	Valid
●	LOGO Root CA V1.0	LOGO Root CA V1.0	6/4/2020 -- 7/12/2070

Use the CIM build-in certificate.

External Certificate Information

	Issued By	Issued To	Valid
○	middle1	middle2	5/25/2022 -- 5/22/2032

Import and use an external certificate, including certificate created by CIM or other generation tool.

Import New External Certificate

Drag and drop or select [Certificate] file

Cer File size cannot larger than 4000 bytes
key-pair type should be: ecc256 / ecc384

Import the CA in Siemens CIM SGLAN Connector

If you connect the SGLAN with PC, select the same certificate solution from "certificate" tab in Siemens CIM SGLAN Connector first.

5.4.9.3 IP address management

If you enable this function, only contacts stored in CIM can query the IPv4/IPv6 address of SIM card through SMS. Otherwise, anyone can query the IPv4/IPv6 address of SIM card through SMS.

Get IP address by SMS

Note

Make sure your SIM card support SMS if you use SMS to query IPv4 or IPv6 address.

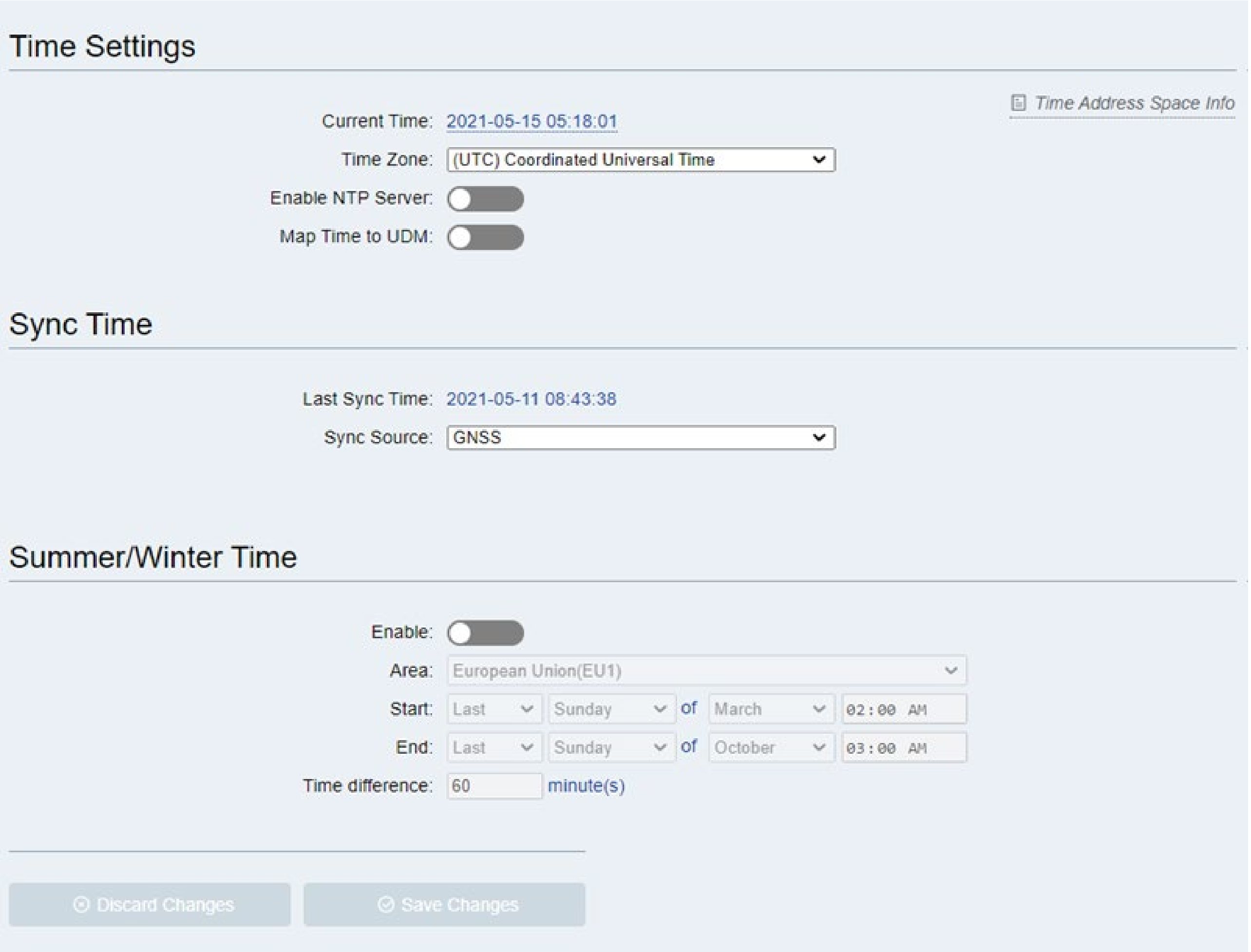
You can get the IP address by an SMS with the content "ipv6?/ipv4?" to the CIM.

Content of the SMS	Description
ipv4?	Require the IPv4 address of CIM server
ipv4#	• Respond to the "ipv4?" request • Notify the CIM client when the ipv4 address changed
ipv6?	Require the IPv6 address of CIM server
ipv6#	• Respond to the "ipv6?" request • Notify the CIM client when the ipv6 address changed

5.4.10 System settings

5.4.10.1 Time settings

This page allows you to set the time for CIM.



Time Settings

Time Address Space Info

Current Time: 2021-05-15 05:18:01

Time Zone: (UTC) Coordinated Universal Time

Enable NTP Server: ○

Map Time to UDM: ○

Sync Time

Last Sync Time: 2021-05-11 08:43:38

Sync Source: GNSS

Summer/Winter Time

Enable: ○

Area: European Union(EU1)

Start: Last Sunday of March 02:00 AM

End: Last Sunday of October 03:00 AM

Time difference: 60 minute(s)

Note

If the time you set is out of the range of the certificate defines, CIM will generate a new certificate. The page may be stuck for a few seconds during the certificate generation.

Note

If the time of CIM and PC is different more than 1 year, you will get a notice that you certificate is invalid. Set the time in web-based configuration for CIM.

Time setting

This function allows you to set the time.

- Check the current time
- Change current time by clicking the time.

Note

If you change the CIM time by clicking the time, the change will take effective immediately without clicking "Save Changes".

- Select the time zone
- Enable/disable NTP server
- Enable/disable map time to UDM

Sync Time

This function allows you synchronize CIM time with a time server.

Set GNSS as sync source

1. Select the sync source.

Set Network as sync source

1. Select the sync source.
2. Enter the IP address of the sync NTP server.
3. Click "Sync now".

Note

When you selected a sync source, CIM will sync time from the sync source periodically.

Note

Last sync time

The last sync time is the latest time CIM updated. It can be the time synchronized from NTP server or the time you set manually in time setting.

Summer/Winter Time

This function allows you to set an automatic conversion of the summer and winter time for the CIM clock:

When you enable summer/winter time conversion, you can specify a country-specific time conversion:

- EU: EU1, EU2
- UK: United Kingdom of Great Britain and Northern Ireland

- US1 / US2: United States of America
- Australia
- Tasmania
- New Zealand
- Freely adjustable: customized switchover dates and times

Time interval between software start time and software end time must be greater than time difference.

5.4.10.2 Power on/off SMS

This page allows you to set the device power on/off SMS.

1. Toggle on "Power On/Off SMS".
2. Enter the message text.
3. Select the receiver from the contact list.
4. Click "Save Changes" to save the change or click "Discard Changes" to discard the change.

5.4.10.3 Change password

This page allows you change the password for web-based configuration login.

Note

If you didn't change the password, you can log on with the default password "cim".

Siemens strongly recommend you change your default password after you first login CIM.

If you forget the password, you need to reset the CIM to factory setting (Page 20) and log on with the default password.

To change the password, you must first enter the existing password in the **Old password** text box and the new password in the two boxes for **New password** and then confirm with "Change password". The password can have a maximum of 32 characters.

5.4.10.4 System reset

This page allows you restart the connected CIM or reset the connected CIM to factory setting.

Device restart

You can press the "Device Restart" button to restart the CIM.

Note

The data in UDM will be cleared after device restart.

Factory reset

When you press the "Factory Reset" button, web-based configuration reset the connected CIM to factory setting.

Note

Before factory reset, backup the configuration data through the path **System Setting --> System Configuration Management**.

Built-in certificate (Page 80) and SMS center number (Page 78) will be kept after the factory reset.

5.4.10.5 System configuration management

This function allows you export the current CIM configuration or import a CIM configuration file to CIM.

Export configure file

1. Click the button "Export Configure File".
2. Enable or disable "Protect file with password" and set the password if you want to protect the configuration file from casual use.

Note

The following configuration will not be exported:

- IP address
- Password
- Certificate
- Key
- Clock

Import configure file

1. Click the button "Import Configure File".
2. Navigate to the folder in which you saved the configure file and select it.
3. Enter the password if the configuration file is protected.

5.4.10.6 System upgrade

This page allows you upgrade the firmware for CIM.

Prerequisites

Download the upgrade package from After sales information system (https://support.industry.siemens.com/cs/start?lc=en-US).

Upgrade the firmware

Note

- Upgrade firmware will not change any configuration. However, Siemens recommends you backup configuration data through the path **System Setting --> System Configuration Management** before the upgrading.
- In the upgrade environment, other functions of the system are stopped, such as network communication, data bindings and so on.

Follow these steps to perform an upgrade:

1. Click "Upgrade system" in the system upgrade page.
2. Navigate to the folder which you saved the upgrade package and select it.

   Note

   The upgrade package can be stored on the PC or a storage media, but not on a cell phone. Make sure the upgrade package is not stored on a cell phone.

3. Wait until the upgrade completed.

   Note

   Do not power off the device, disconnect the device or refresh the page during the upgrade. Otherwise, the upgrade may fail.

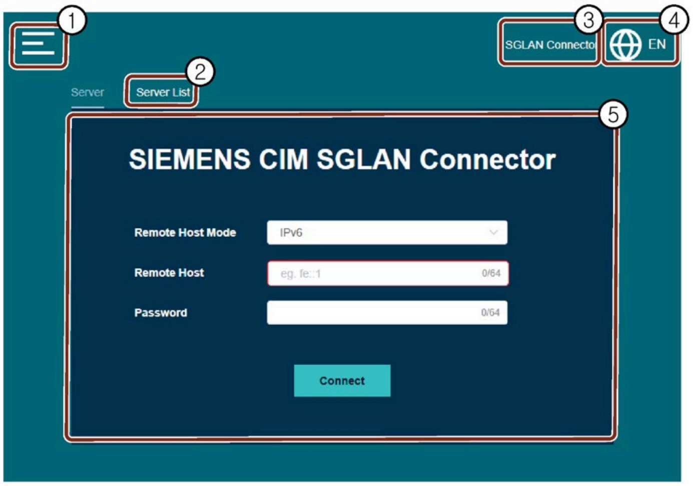
   CIM restarts to utilize the new features after the upgrade completed.

Note

If you cannot access the web server after the firmware upgrade, close and re-open the browser or clear the cash files of the browser.

6 CIM SGLAN Connector

CIM SGLAN connector provides the solution for PC connecting to SGLAN. PC can access all devices in SGLAN after connected to SGLAN server.



SIEMENS CIM SGLAN Connector

Remote Host Mode: IPv6

Remote Host: eg. fe::1 0/64

Password: 0/64

①	Menu of the CIM SGLAN Connector	
	Home page	• If you logged in, home page displays the connection status of SGLAN. • If you do not log in, home page displays the login page.
	Virtual Adapter Setting	View or set the virtual adapter
	Certificate	Select the certificate solution for connecting SGLAN server.
	Documentation	Help document
	About	Basic info about SGLAN connector
	Readme/OSS	Display the Third-Party Software Disclosure Document
②	Server list	List for remote SGLAN server
③	Connector name	Name of this connector. You can change this name by clicking the connector name.
④	Language setting	Set the display language
⑤	Main page	Information area

To connect SGLAN, perform these steps:

1. Install CIM SGLAN Connector (Page 92)
2. Select the certificate (Page 93) (If SGLAN server uses the CIM build-in certificate, skip this step)
3. Connect to SGLAN Server (Page 95)

6.1 Installation

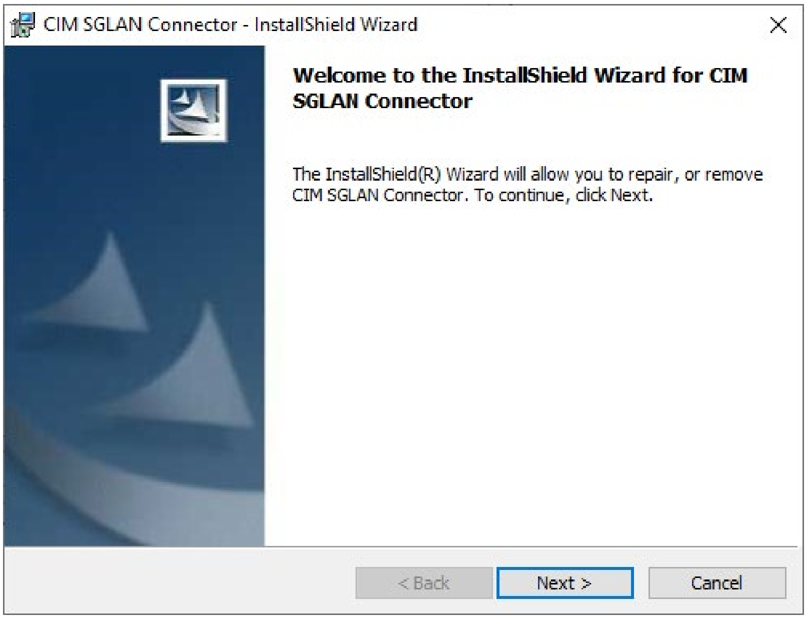
Requirements

- You have administrator privileges on your host computer with Windows 10 OS
- You have downloaded the installation package.

Procedure

To install CIM SGLAN Connector, follow these steps:

1. Double-click the file “CIMSGLANConnector_Setup_X64.exe”. The "Welcome to InstallShield wizard for CIM SGLAN Connector" dialog opens.



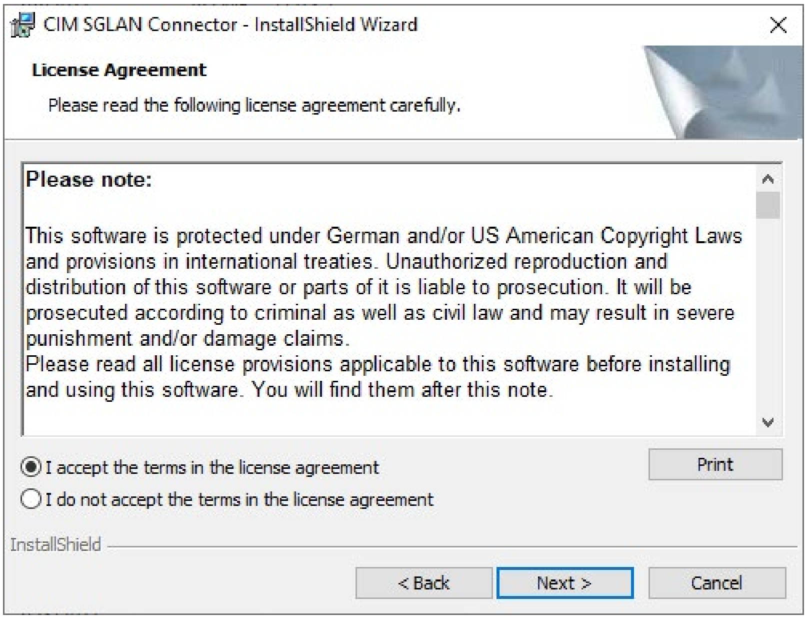
CIM SGLAN Connector - InstallShield Wizard

Welcome to the InstallShield Wizard for CIM SGLAN Connector

The InstallShield(R) Wizard will allow you to repair, or remove CIM SGLAN Connector. To continue, click Next.

2. Click "Next". The dialog for the license terms opens.

3. To continue the installation, read and accept all license agreements and click "Next".



License Agreement

Please read the following license agreement carefully.

Please note:

This software is protected under German and/or US American Copyright Laws and provisions in international treaties. Unauthorized reproduction and distribution of this software or parts of it is liable to prosecution. It will be prosecuted according to criminal as well as civil law and may result in severe punishment and/or damage claims.
Please read all license provisions applicable to this software before installing and using this software. You will find them after this note.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4. Check the costumer Information and click "Next".

   The dialog for selecting the install folder opens.

5. Click Next to install to the default folder, or click "Change" to change the install directory.
6. Click "Install" to begin the installation.
7. Click "Finish" when you get the notice that installation has finished.

6.2 Working with CIM SGLAN Connector

6.2.1 Certificate setting

Before connecting the SGLAN server, make sure you select the same trust certificate as the SGLAN server.

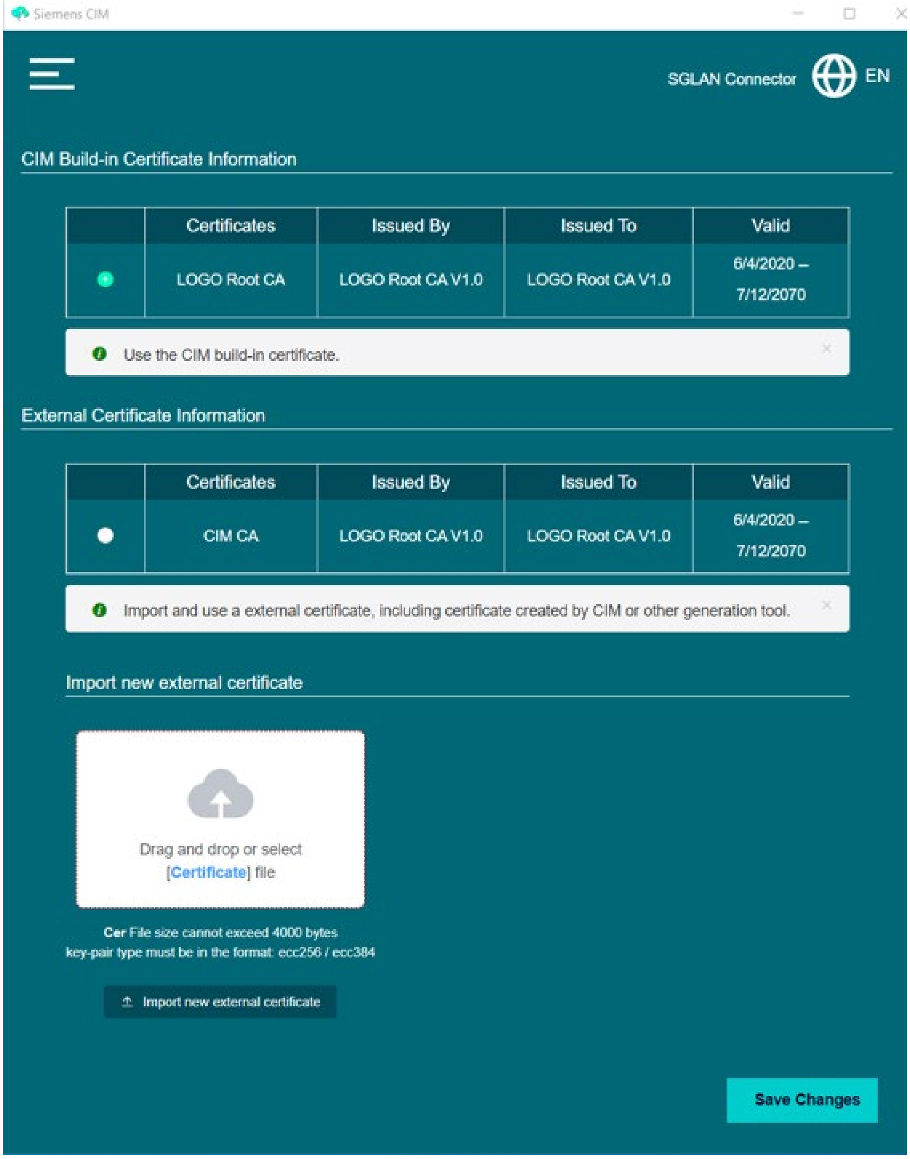
- If the SGLAN server used the CIM build-in certificate, skip this step. CIM SGLAN connector uses CIM build-in certificate by default.
- If the SGLAN server used an "CIM Internal certificate" or "External certificate", you need to upload the same certificate in SGLAN connector before connecting SGLAN server.

Import the external CA in CIM SGLAN connector

Import external CA as follow.

1. Open SGLAN connector and select "Certificate" from the menu.
2. Drag and drop or select the same CA used in server in to the blank box.

3. Click "Import New External Certificate" to import the CA.
4. Select External certificate by selecting the check box next to it.
5. Click "Save Changes" to save the change.



CIM Build-in Certificate Information

	Certificates	Issued By	Issued To	Valid
●	LOGO Root CA	LOGO Root CA V1.0	LOGO Root CA V1.0	6/4/2020 – 7/12/2070

Use the CIM build-in certificate.

External Certificate Information

	Certificates	Issued By	Issued To	Valid
○	CIM CA	LOGO Root CA V1.0	LOGO Root CA V1.0	6/4/2020 – 7/12/2070

Import and use a external certificate, including certificate created by CIM or other generation tool.

Import new external certificate

Drag and drop or select [Certificate] file

Cer File size cannot exceed 4000 bytes
key-pair type must be in the format: ecc256 / ecc384

6.2.2 Server list

The server list records all the SGLAN server devices you added. You can use this server list to quickly connect to the SGLAN server.

Create a server item

1. Click "Add Row" button.
2. Enter the server information. You can add maximum 64 server items at most.

   Description: description of the SGLAN server

   Remote Host Mode: remote host mode of SGLAN server

   Remote Host: IP address of the remote host

   Server Password: password of the SGLAN server
3. Click "Save" to confirm the server information or click "Cancel" to discard the information.
4. Repeat step 1-3 to add all server items you need.

Connect the SGLAN server

Click 🔗 to connect the SGLAN server.

Change a server item

Click ✎ then enter the new value to the corresponding filed of the server item you want to change.

Delete a server item

Click 🗑 delete button next to the server item you want delete.

6.2.3 Connecting to SGLAN server

Connect to SGLAN server

To connect the CIM SGLAN server, follow the steps:

1. Open CIM SGLAN Connector from the start menu or desktop.
2. Select the host mode the same as SGLAN server mode.
3. Enter the IP address of SGLAN server and the access password.

   Note

   If you have enabled SGLAN server without changing the password, you can connect to the SGLAN server with the default password "sglan".
4. Click "Connect".

Connect to SGLAN server stored in server list

If you stored the information of SGLAN server in the CIM SGLAN Connector, you can connect to SGLAN server as follows:

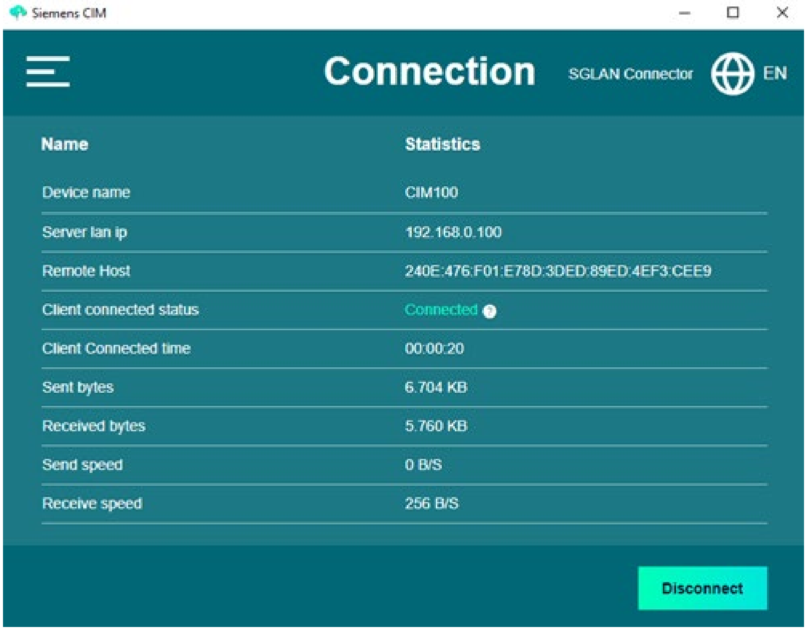
1. Open CIM SGLAN Connector from the start menu or desktop.
2. Click "Server List".
3. Select the server and click "Connect".

6.2.4 Viewing SGLAN connection

Once logged in, you can check the status of connection to SGLAN.

Operation:

- To disconnect the connection to the remote host, click "Disconnect" button by selecting "Home page" in the menu.
- To close the window, click "Close" button.



Name	Statistics
Device name	CIM100
Server lan ip	192.168.0.100
Remote Host	240E:476:F01:E78D:3DED:89ED:4EF3:CEE9
Client connected status	Connected
Client Connected time	00:00:20
Sent bytes	6.704 KB
Received bytes	5.760 KB
Send speed	0 B/S
Receive speed	256 B/S

Name	Description
State	State of connection to SGLAN server
Connected time	The amount of time spent by host computer in being connected to SGLAN server
Sent bytes	The total amount of data sent in this connection
Received bytes	The total amount of data received in this connection
Send speed	Send speed
Receive speed	Receive speed

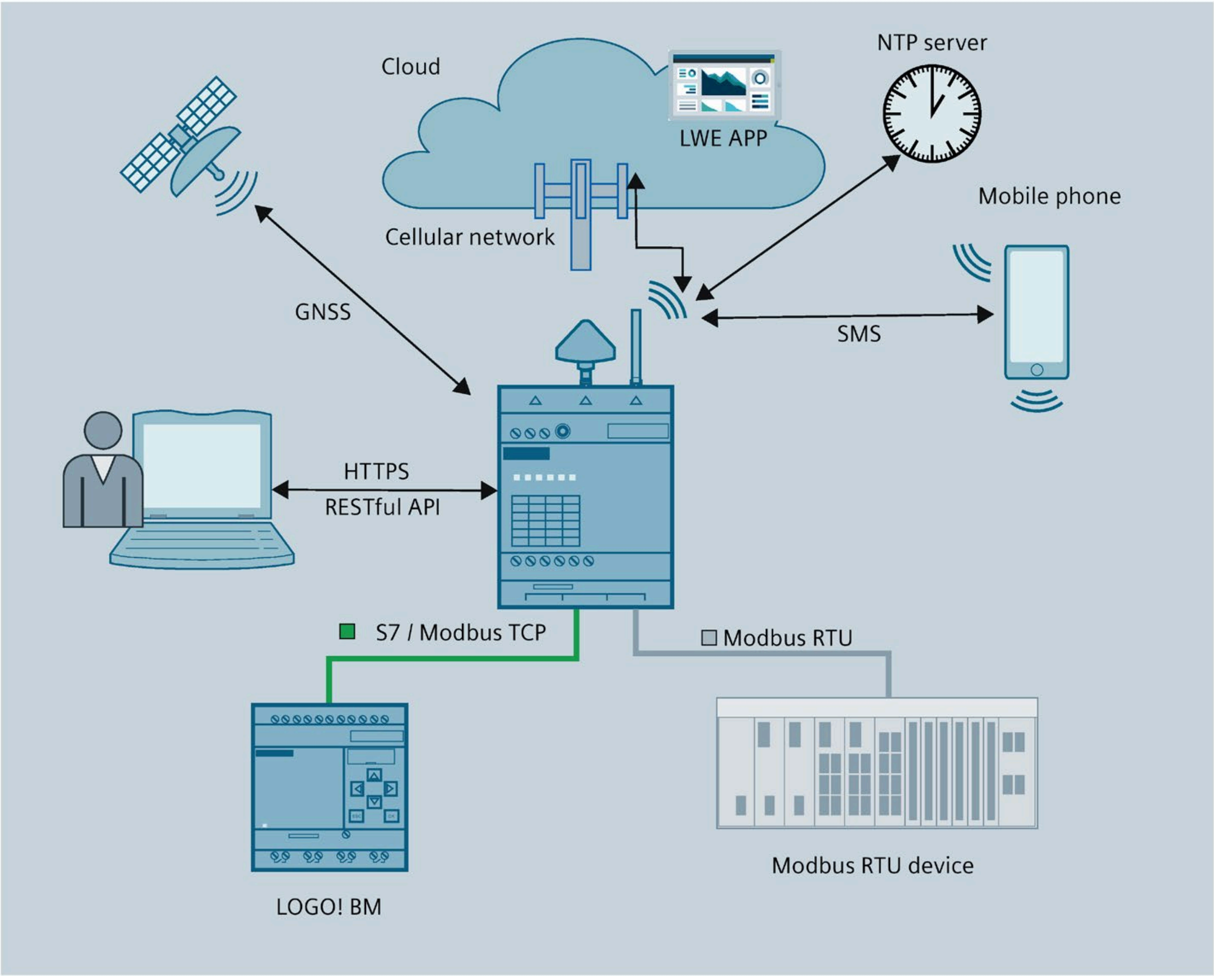
Practical example 7

7.1 Application example

7.1.1 Fill control

Requirements for a fill system

This example illustrates a fill system. We want to monitor and control the whole system anywhere through a web browser. We want to be informed with short message if the liquid level is abnormal.



Setup

We need a CIM to connect the onsite devices. The onsite devices can be LOGO! BM or Modbus RTU devices.

LWE project on AWS Could

For how to create and deploy a LWE project on AWS Cloud, refer to "LOGO! Web Editor Online Help".

Set the CIM

Requirements

- Antenna (Page 41), SMA connector (Page 36), cellular module (Page 39) and SIM card (Page 37) is installed.

Procedure

1. Downloading and installing the certificate (Page 44).
2. Accessing web-based configuration from PC (Page 47).
3. Configure the Cellular and GNSS (Page 77).
4. Set the time (Page 86).
5. Configure the connection (Page 64) of CIM to the onsite device as you need.
6. Create a variable (Page 57) for the liquid level.
7. Create a contact (Page 56) for receiving the short message.
8. Create a message (Page 58) for informing the abnormal liquid level.
9. Bind the event (Page 60) "abnormal liquid level" with an action "send message".

Set the onsite device

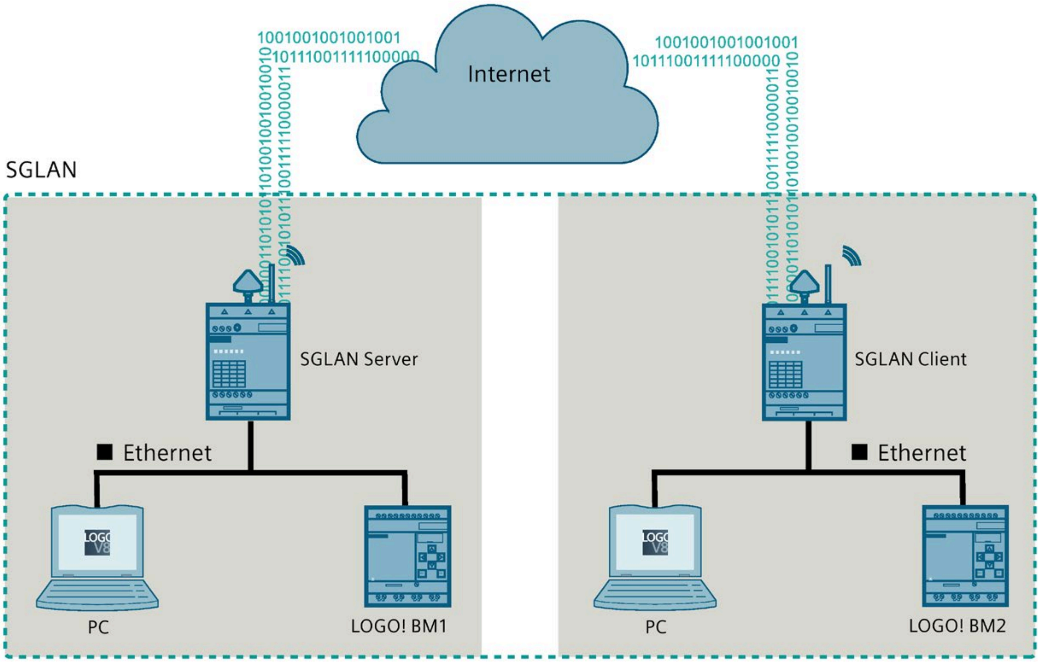
To setup the communication from CIM and the onsite device, refer to the documentation for onsite device and do the settings accordingly.

7.2 SGLAN example

7.2.1 Data exchange through SGLAN using IoT SIM cards

This example shows an SGLAN using CIM to realize data transmission between LOGO! BM devices distributed in different sites.

The sketch below illustrates how such a system works:



Requirements

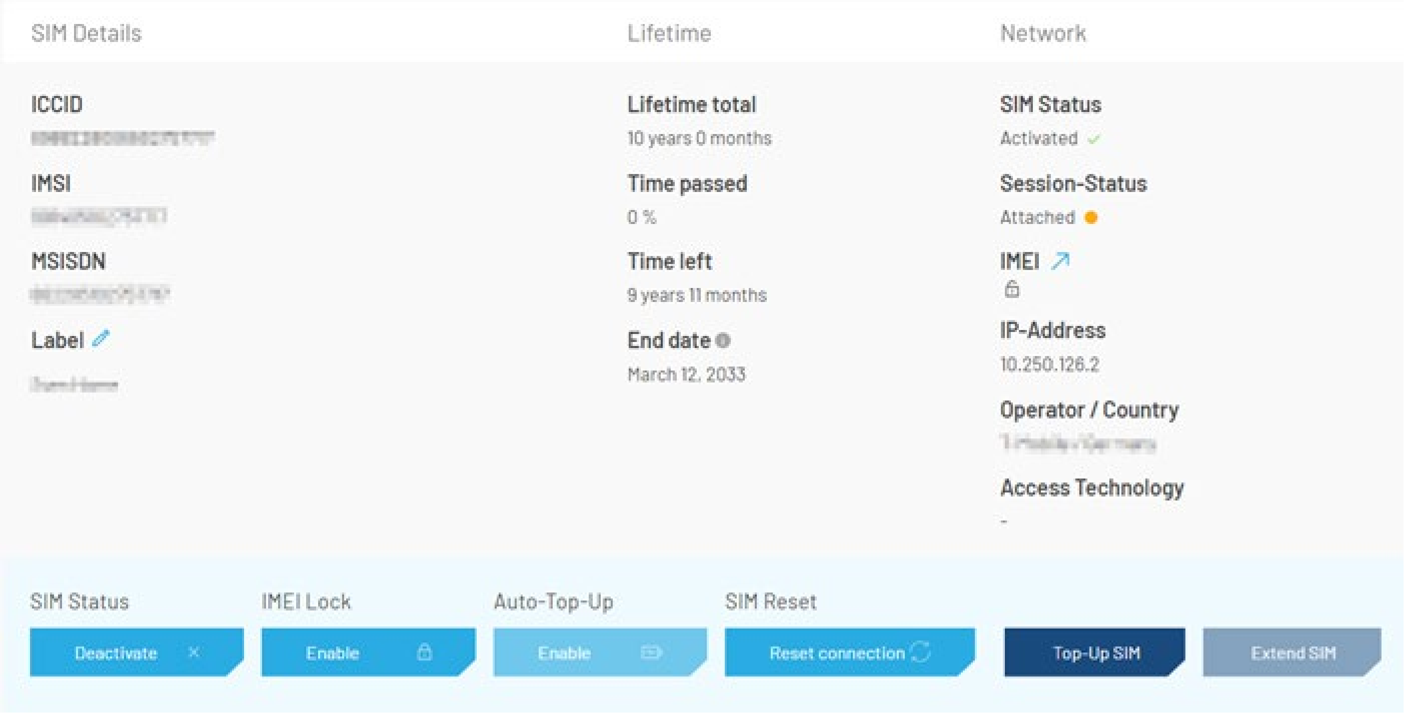
- Two IoT cards that are purchased and activated from the same SIM card operator. IoT card has fixed IPv4 address.
- All the IP of the devices in SGLAN are in the same subnet and not conflict with each other.

Note

IoT cards and devices are bound one by one. Switching devices requires the supplier to unbind and reconnect the IoT card and the device.

Note

Make sure you have activated the IoT card. The following figure shows an example of what a successful activation looks like.


SIM Details

ICCID
[redacted]

IMSI
[redacted]

MSISDN
[redacted]

Label
[redacted]

Lifetime

Lifetime total
10 years 0 months

Time passed
0 %

Time left
9 years 11 months

End date
March 12, 2033

Network

SIM Status
Activated ✓

Session-Status
Attached ●

IMEI

IP-Address
10.250.126.2

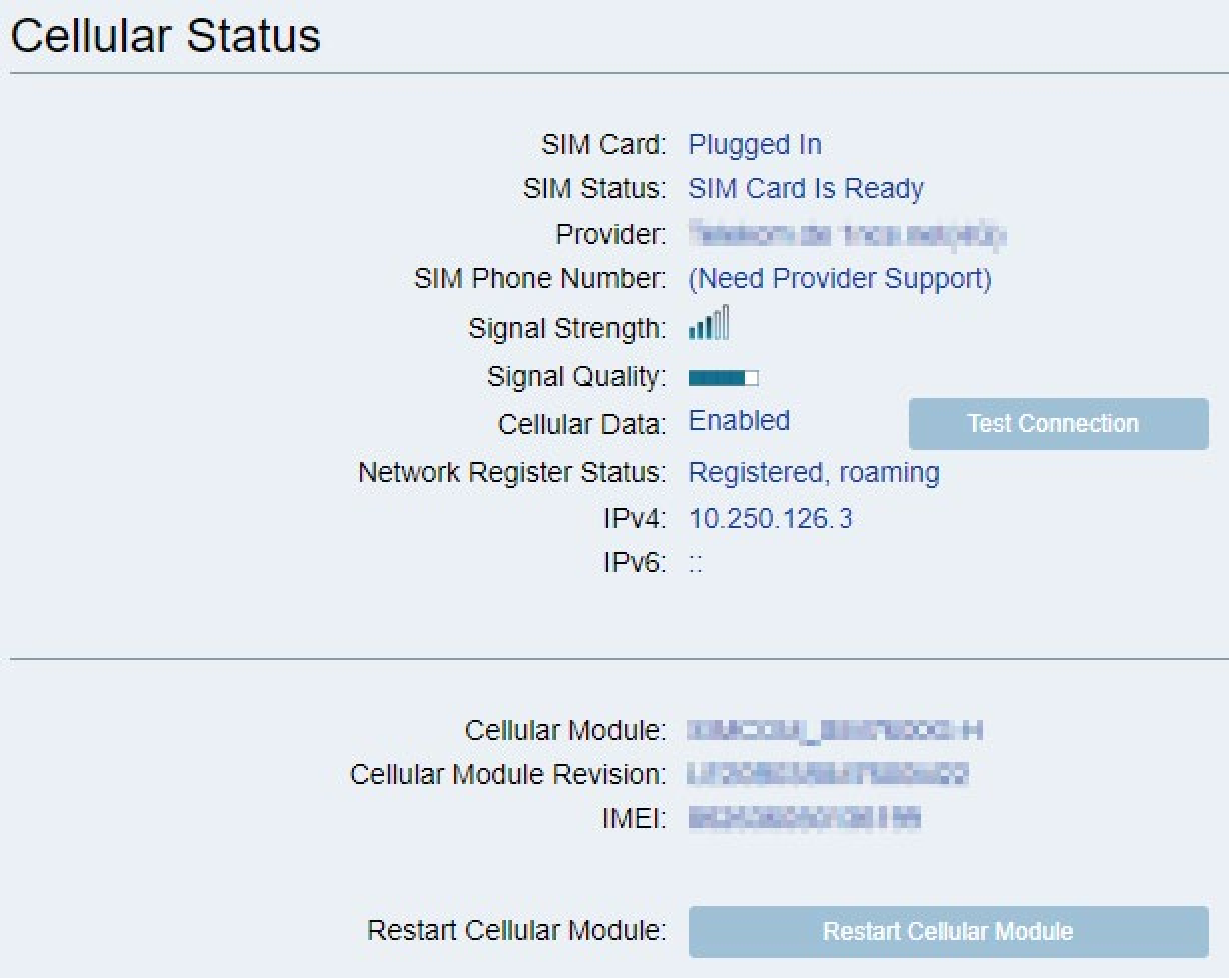
Operator / Country
[redacted]

Access Technology
-

Setting up the SGLAN server

1. Access the web-based configuration (Page 47) of CIM as SGLAN server.
2. Check the cellular status.

3. Click "Test Connection (Page 77)" to test the connection to Internet.



Cellular Status

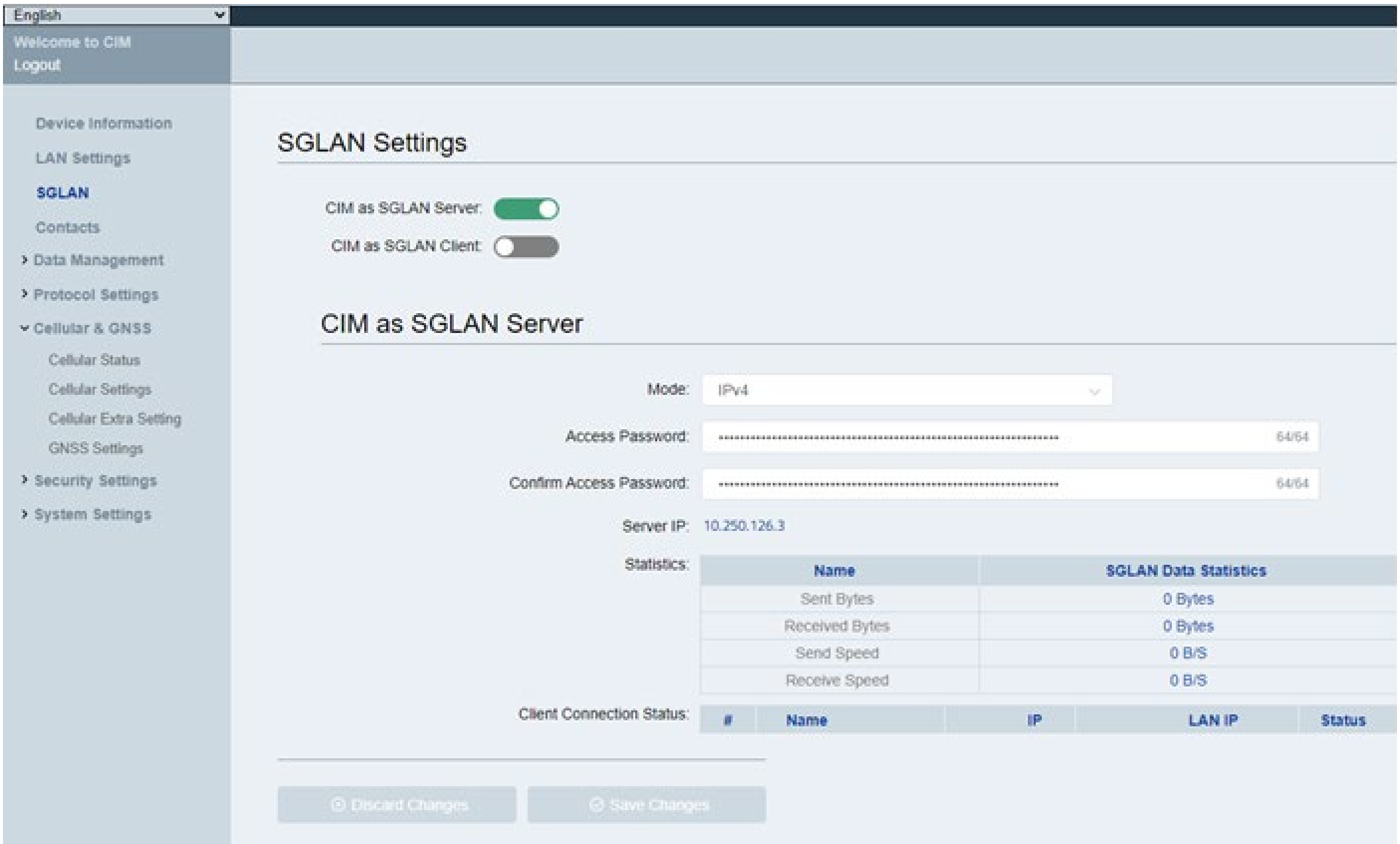
SIM Card: Plugged In
SIM Status: SIM Card Is Ready
Provider: [redacted]
SIM Phone Number: (Need Provider Support)
Signal Strength:
Signal Quality:
Cellular Data: Enabled
Network Register Status: Registered, roaming
IPv4: 10.250.126.3
IPv6: ::

Cellular Module: [redacted]
Cellular Module Revision: [redacted]
IMEI: [redacted]

Restart Cellular Module:

4. Go to the SGLAN page and enable "CIM as SGLAN Server".
5. Set the mode as IPv4.

6. Write down the Server IP address. You will need it to configure the client.
7. Set the "Access password" and confirm it in "Confirm access password". Remember the access password. You will need it to configure the client.



SGLAN Settings

CIM as SGLAN Server: ●
CIM as SGLAN Client: ○

CIM as SGLAN Server

Mode: IPv4

Access Password: •• 64/64

Confirm Access Password: •• 64/64

Server IP: 10.250.126.3

Statistics:

Name	SGLAN Data Statistics
Sent Bytes	0 Bytes
Received Bytes	0 Bytes
Send Speed	0 B/S
Receive Speed	0 B/S

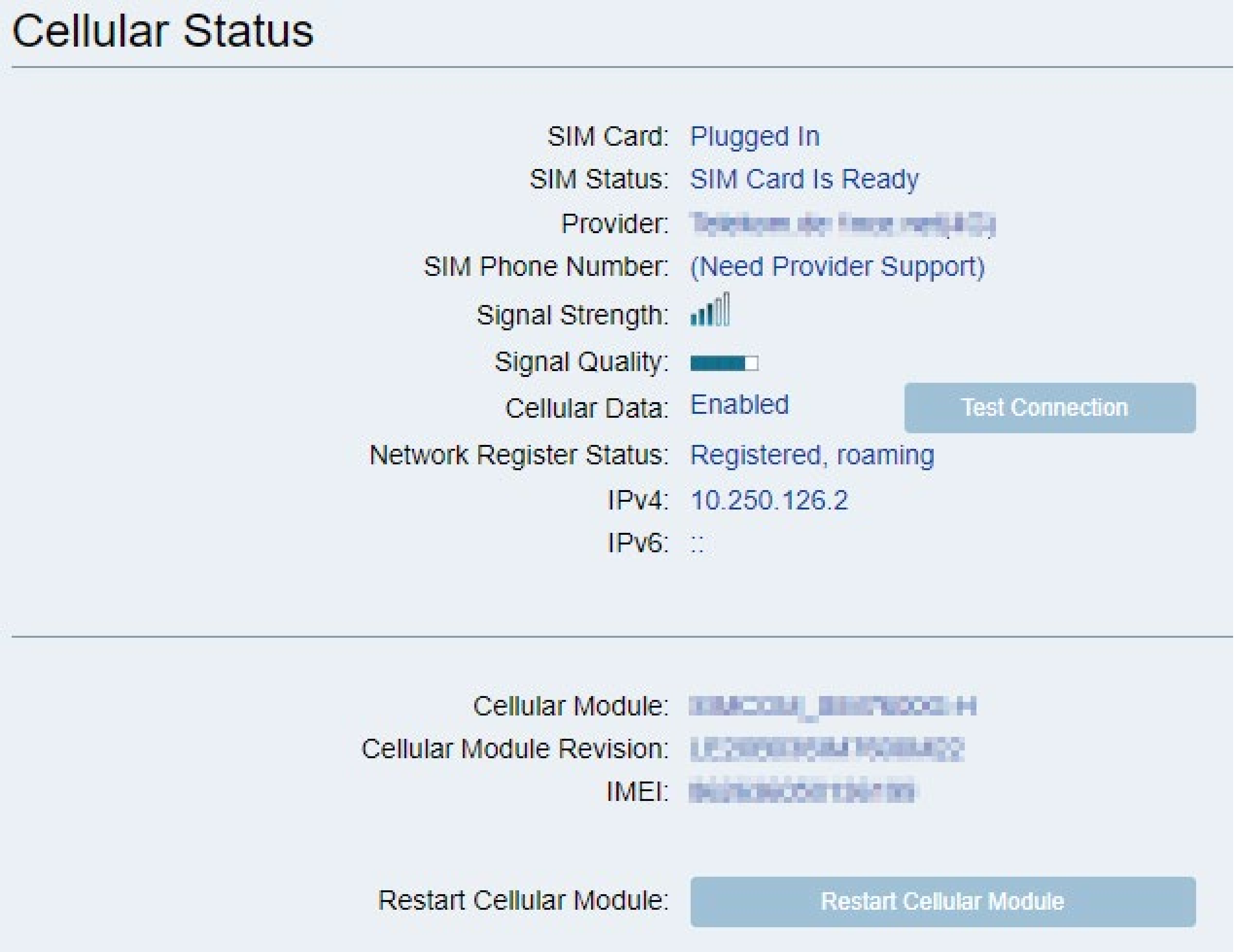
Client Connection Status:

#	Name	IP	LAN IP	Status

Setting up the SGLAN client

1. Access the web-based configuration (Page 47) of CIM as SGLAN client.
2. Check the cellular status.

3. Click "Test Connection (Page 77)" to test the connection to CIM server.



Cellular Status

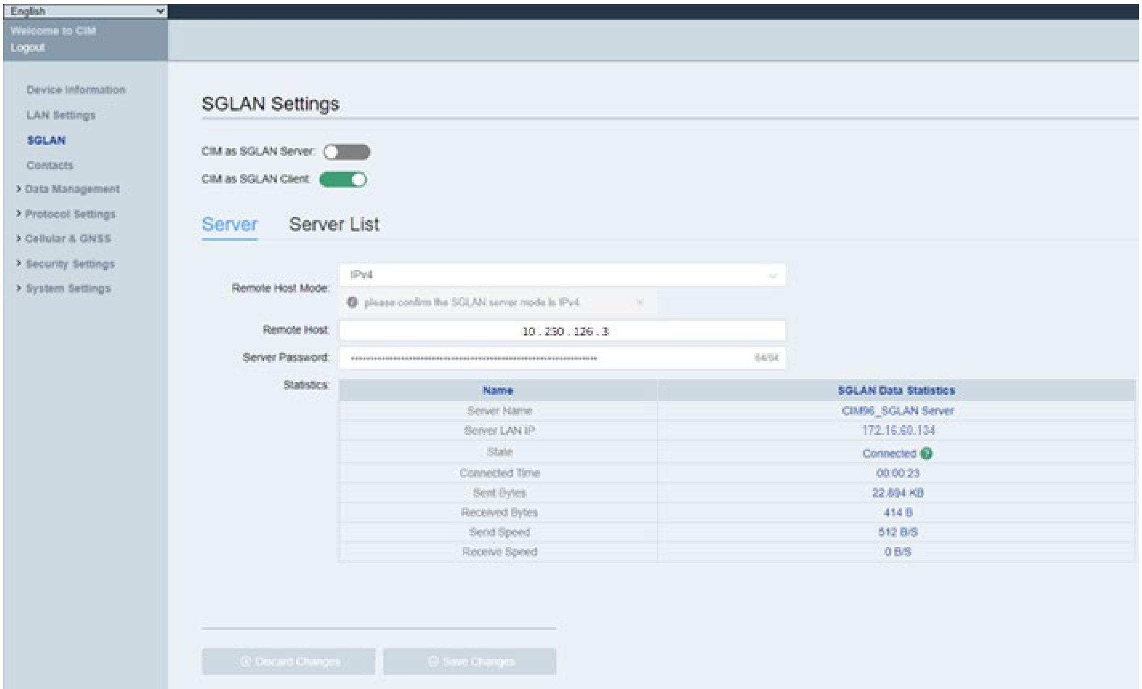
SIM Card: Plugged In
SIM Status: SIM Card Is Ready
Provider: [redacted]
SIM Phone Number: (Need Provider Support)
Signal Strength: ▂▃▅
Signal Quality: ▬
Cellular Data: Enabled
Network Register Status: Registered, roaming
IPv4: 10.250.126.2
IPv6: ::

Cellular Module: [redacted]
Cellular Module Revision: [redacted]
IMEI: [redacted]

Restart Cellular Module:

4. Go to the SGLAN page and enable "CIM as SGLAN Client".
5. Select the remote host mode as IPv4.
6. Enter the Server IPv4 address of the server in the input box next to "Remote Host".

7. Enter the access password.
8. Click "Save changes".



SGLAN Settings

CIM as SGLAN Server: ○

CIM as SGLAN Client: ●

Server | Server List

Remote Host Mode: IPv4

please confirm the SGLAN server mode is IPv4

Remote Host: 10 . 230 . 126 . 3

Server Password: ••• 64/64

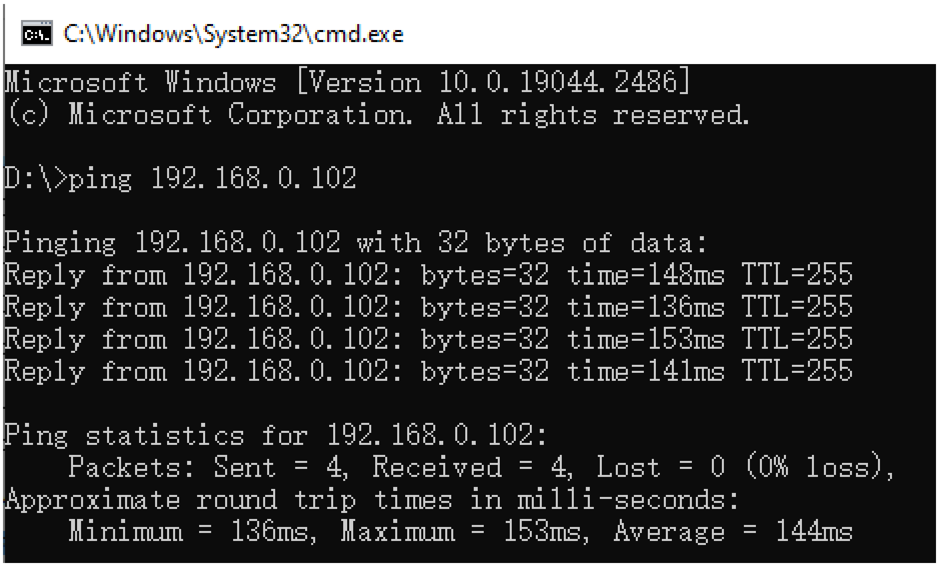
Statistics:

Name	SGLAN Data Statistics
Server Name	CIM96_SGLAN Server
Server LAN IP	172.16.60.134
State	Connected ✓
Connected Time	00:00:23
Sent Bytes	22.894 KB
Received Bytes	414 B
Send Speed	512 B/S
Receive Speed	0 B/S

7.2.2 SGLAN applications on local and remote LOGO! BM devices

Preparations

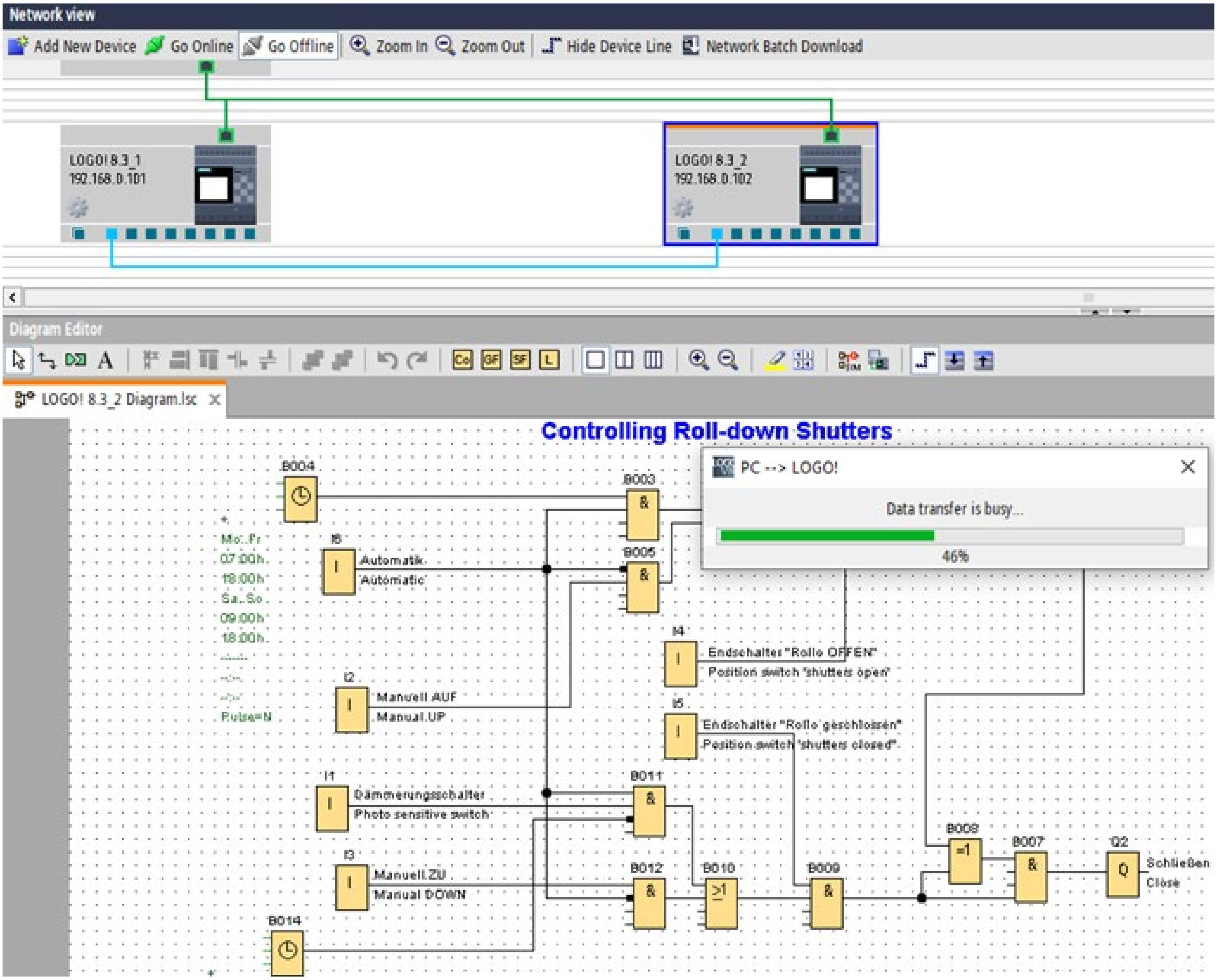
1. Connect the host PC to the CIM server with an Ethernet cable.
2. Connect the host PC to the CIM client with an Ethernet cable.



```
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

D:\>ping 192.168.0.102

Pinging 192.168.0.102 with 32 bytes of data:
Reply from 192.168.0.102: bytes=32 time=148ms TTL=255
Reply from 192.168.0.102: bytes=32 time=136ms TTL=255
Reply from 192.168.0.102: bytes=32 time=153ms TTL=255
Reply from 192.168.0.102: bytes=32 time=141ms TTL=255

Ping statistics for 192.168.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 153ms, Average = 144ms
```

Downloading program to remote LOGO! BM through SGLAN

1. Open the program with LOGO!Soft Comfort on host PC.
2. Select the client/remote LOGO! BM on Network view.
3. Click Download and select the local adapter connected to the CIM as interface. The program will be downloaded to the remote LOGO! BM.



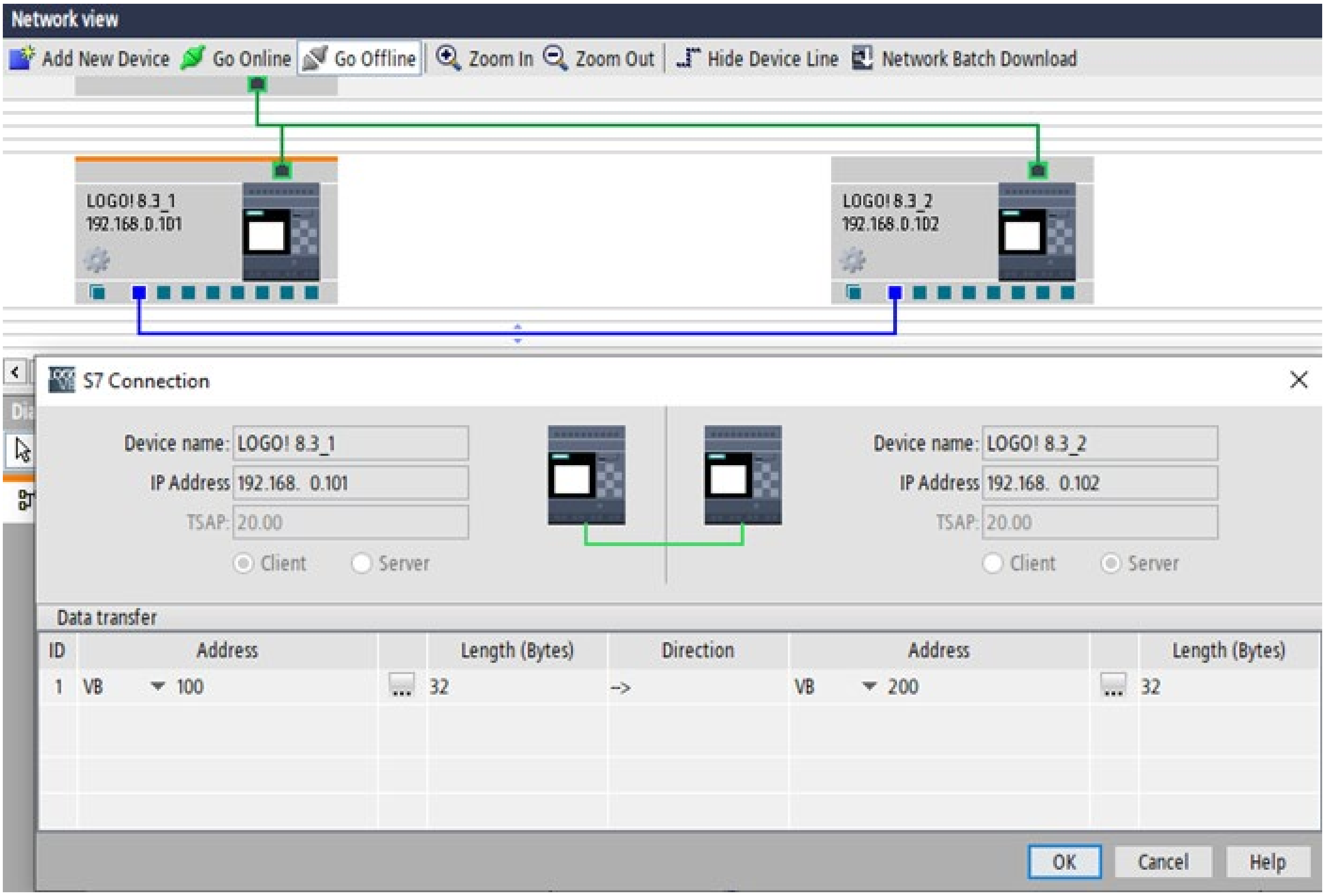
PC --> LOGO!

Data transfer is busy...

46%

Transferring data between LOGO! BM devices through SGLAN

1. Set the data transfer in S7 connection.



Device name:	LOGO! 8.3_1
IP Address	192.168. 0.101
TSAP:	20.00
● Client	○ Server

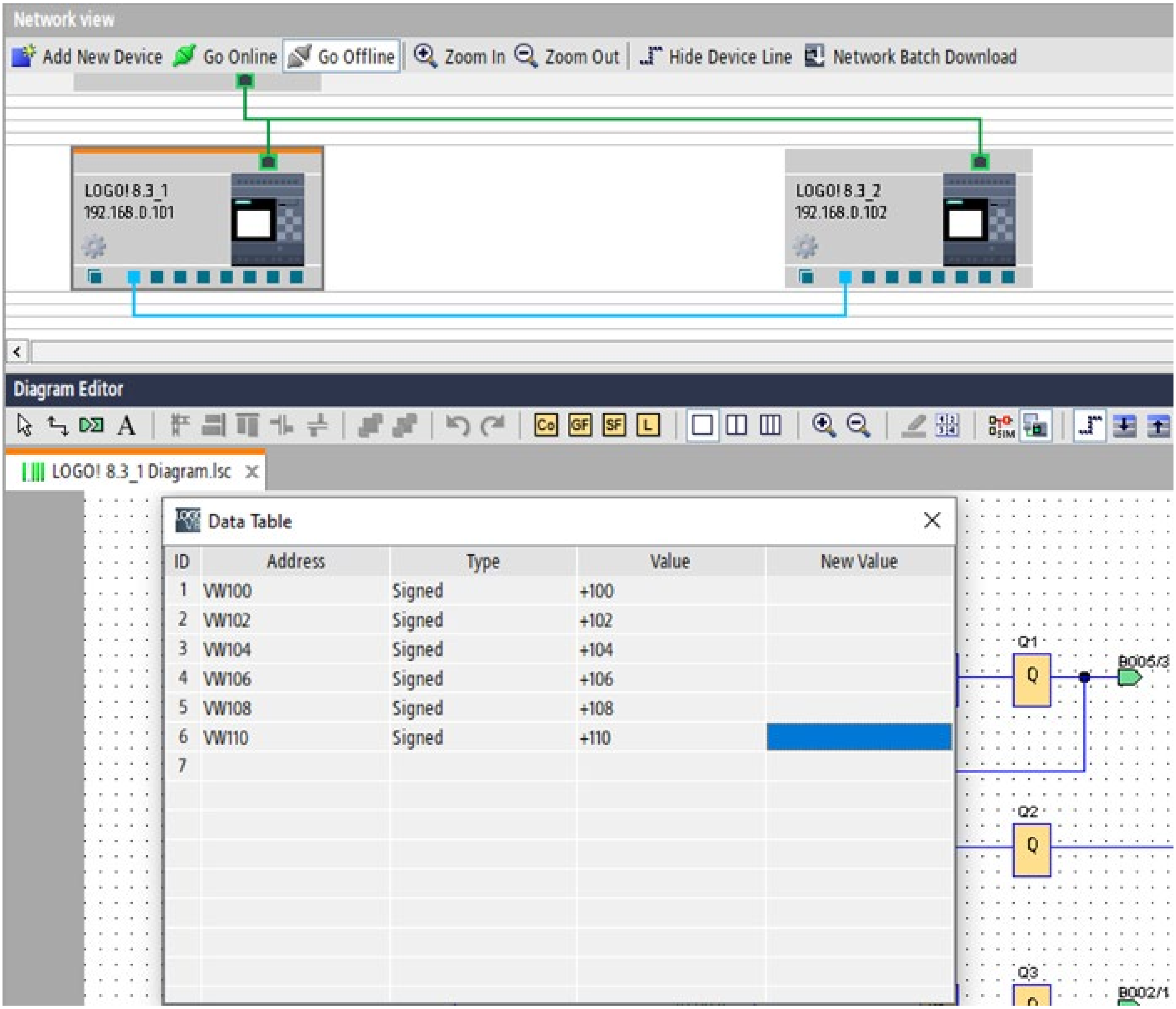
Device name:	LOGO! 8.3_2
IP Address	192.168. 0.102
TSAP:	20.00
○ Client	● Server

Data transfer

ID	Address		Length (Bytes)	Direction	Address		Length (Bytes)
1	VB ▼ 100	...	32	-->	VB ▼ 200	...	32

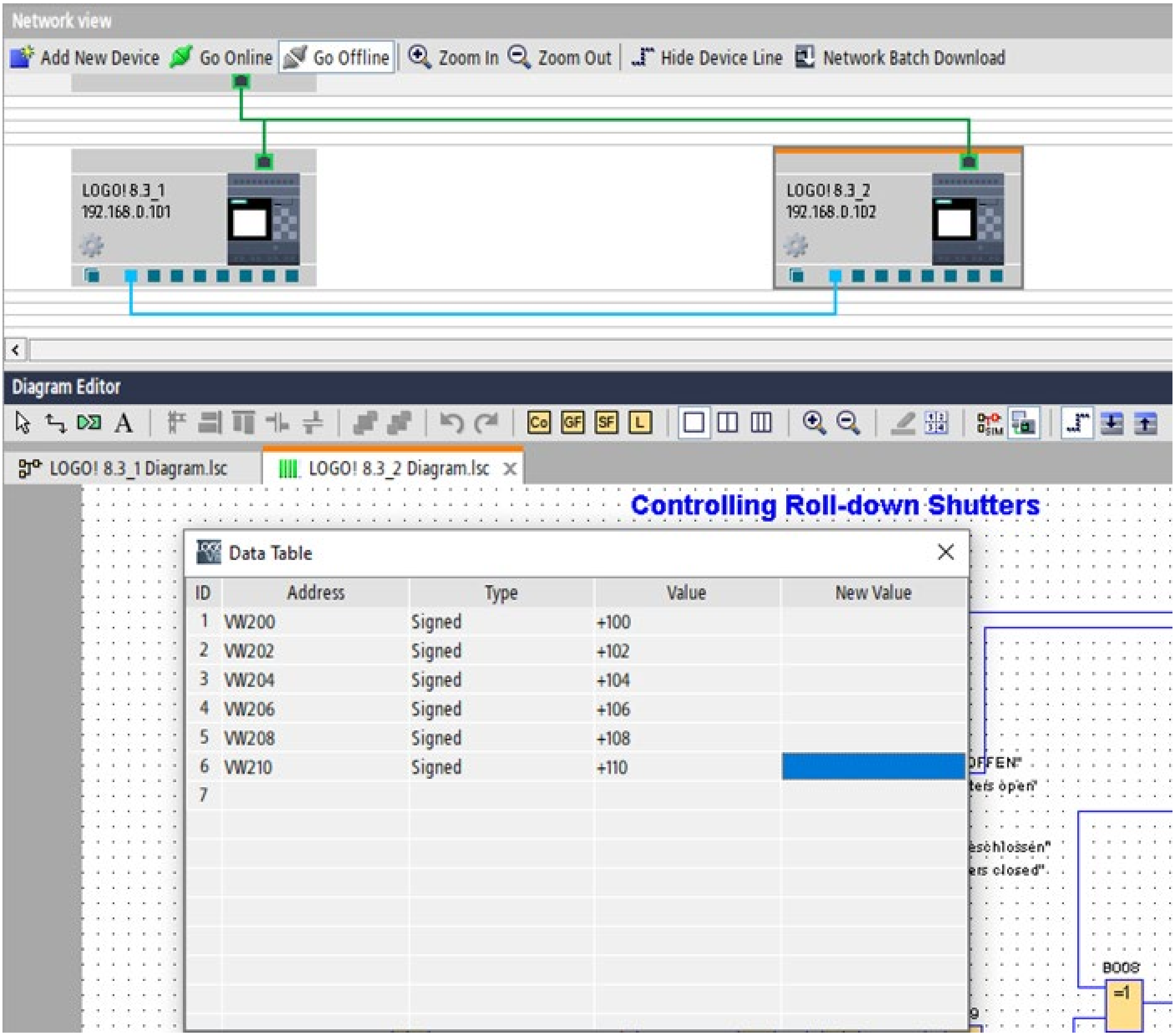
2. Click download and select the local adapter connected to the CIM as interface.
3. Select the target device in "Accessible LOGO" and click "OK".

4. Enter new values to the address on the host LOGO! BM.



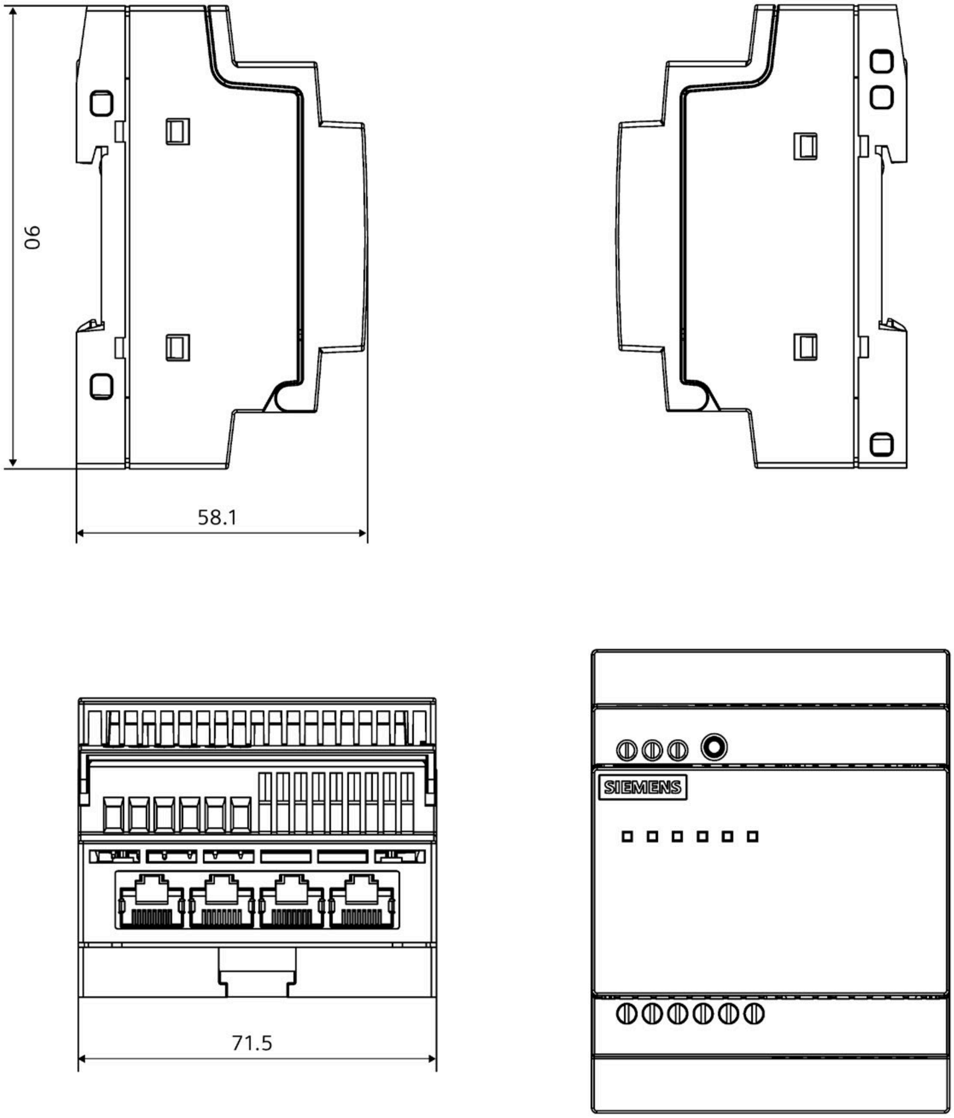
ID	Address	Type	Value	New Value
1	VW100	Signed	+100	
2	VW102	Signed	+102	
3	VW104	Signed	+104	
4	VW106	Signed	+106	
5	VW108	Signed	+108	
6	VW110	Signed	+110	
7				

5. Open the program of the remote LOGO! BM, and check if the data is transferred to it.



ID	Address	Type	Value	New Value
1	VW200	Signed	+100	
2	VW202	Signed	+102	
3	VW204	Signed	+104	
4	VW206	Signed	+106	
5	VW208	Signed	+108	
6	VW210	Signed	+110	
7				

8 Dimension drawing



All dimensions in millimeters

Technical specifications 9

9.1 Technical specification

Technical specifications - CIM		
Article numbers		
CIM	6ED1055-5MC08-0BA2	
Attachment to Industrial Ethernet		
Interface X1P1-P4 for local applications		
Quantity	4	
Design	RJ-45 jack	
Properties	10/100-Base-T, autocrossover, autonegotiation	
Transmission speed	10 / 100 Mbps	
Permitted cable lengths (Ethernet)	**(Alternative combinations per length range) ***	
0 ... 100 m	• Max. 100 m Standard Category 5 shielded twisted-pair Ethernet cable with shielded RJ45 connector.	
Electrical data		
Power supply • Power supply • Range • Design	• 12/24 V DC nominal • 10.2 to 28.8 V DC • 3-pin terminal strip, not floating	
Current consumption • At 12 V • At 24 V	• Maximum 1 A (including 4G and supercapacitor charging) • Maximum 500 mA (including 4G and supercapacitor charging)	
Effective power loss	Maximum 10.5 W	
Permitted ambient conditions		
Ambient temperature • During operation • During storage	• -20 °C to +55 °C • -40 °C to +70 °C	
Relative humidity at 25 °C	Maximum 95 %, non-condensing	
Altitude during operation	up to 3000 m	
Electromagnetic compatibility (EMC)		
Criterion	Tested in accordance with	Values
Radiated emission	EN 55011 EN 55022	Limit class B group 1 Limit class B
Electrostatic discharge	IEC 61000-4-2	±2 kV, ±4kV, ±8 kV air discharge ±6 kV contact discharge

Technical specifications - CIM		
Radiated electromagnetic field	IEC 61000-4-3	80 MHz - 1000MHz 10V/m, 80% AM (1kHz) 1,4 GHz - 6,0 GHz 3V/m, 80% AM (1kHz)
Conducted disturbance	IEC 61000-4-6	150 KHz-80 MHz 10 V, 80%AM(1 kHz)
Fast transient bursts	IEC 61000-4-4	• For power port: ±2kV,5kHz and 100kHz • For signal port: – Signal Lines<30 m: ±1 kV/5 kHz and 100 kHz – Signal Lines>30 m: ±2 kV/5 kHz and 100 kHz
Surge immunity		• ±0.5 kV line-to-line • ±1 kV line-to-earth
Design, dimensions and weight		
Design	Compact design, for DIN rail or wall mounting	
Pollution degree	IP20	
Weight	200 g	
Dimensions (W x H x D)	71.5 x 90 x 58.1 mm (without antenna sockets)	
Materials	Plastic	

9.2 Certificates and approvals

Note

Applicability

The following shows the approvals that may be available. For the device itself, it is certificated as shown on the product label and package label.

ISO 9001 certificate

The Siemens quality management system for all production processes (Development, Production, Sales and Service of Automation Products, -Systems and -Solutions) meets the requirements of ISO 9001:2015

This has been certified by DQS (the German society for the certification of quality management systems).

Certificate registration no. 001323 QM15.

Software license agreements

If the device is supplied with preinstalled software, you must observe the corresponding license agreements.

CE marking

The product meets the requirements and safety objectives of the following EC directives and it complies with the harmonized European standards (EN) for programmable logic controllers which are published in the official documentation of the European Union.

- **2014/53/EU (Radio equipment directive)**

  Directive of the European Parliament and of the Council of April 16, 2014 on the harmonization of the laws of the member states relating to placing radio equipment on the market and to cancel the directive 1999/5/EU

- **2011/65/EU (RoHS directive)**

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

Standard	**CIM**
EN 60079-0	Y
EN 60079-7	Y
EN IEC 63000	Y
EN 61010-2-201	Y
EN 62311	Y
EN 301 489-1	Y
EN 301 489-19	Y
EN 301 489-52	Y
EN 61000-6-1	Y
EN 61000-6-3	Y
EN 301 511	Y
EN 301 908-1	Y
EN 301 908-2	Y
EN 301 908-13	Y
EN 303 413	Y

Below you will find the product relevant harmonized standards according to the directives named above.

FCC and Canada

USA	
Federal Communications Commission Radio Frequency Interference Statement	This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
Shielded cables	Shielded cables must be used with this equipment to maintain compliance with FCC regulations.

USA	
Modifications	Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.
Conditions of operations	This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CANADA	
Canadian notice	This Class B digital apparatus complies with Canadian ICES-003.
Avis Canadian	Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Responsible party for Supplier's Declaration of Conformity

Siemens Industry, Inc.

Digital Factory - Factory Automation

5300 Triangle Parkway, Suite 100

Norcross, GA 30092

USA

Mail to: (amps.automation@siemens.com)

c(UL)us

Applied standards:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CAN/CSA- C22.2 No. 61010-1 (Process Control Equipment)

UL file: E472609

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: CULUS Listed E472610 IND. CONT. EQ. FOR HAZ. LOC.

Applied standards:

- UL 121201
- CSA C22.2 No. 213-17

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4
- Cl. 1, Zone 2, GP. IIC T4

UL file: E472610

Installation Instructions for cULus haz.loc.

- WARNING – Explosion Hazard – Do not disconnect while circuit is live unless area is known to be non-hazardous.
- WARNING - Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2 or Zone 2.
- This equipment is suitable for use in Class I, Division 2, Groups A, B, C, D; Class I, Zone 2, Group IIC; or non-hazardous locations.
- Antenna must be installed within the end use enclosure. Routing and remote installation (not evaluated as part of this certification) of the antenna shall be in accordance with the appropriate location regulations when installed in unclassified and/or Class I, Division 2 Hazardous Locations.

FM

Factory Mutual Research (FM) in accordance with

Approval Standard Class Number 3611, 3600, 3810

ANSI/UL61010-1, ANSI/UL 121201

CAN/CSA-C22.2 No. 0-10

CSA C22.2 No. 213

CAN/CSA-C22.2 No. 61010-1

APPROVED for use in Class I, Division 2, Group A, B, C, D T4;

Class I, Zone 2, Group IIC Tx

Installation Instructions for FM

- WARNING – Explosion Hazard – Do not disconnect while circuit is live unless area is known to be non-hazardous.
- WARNING - Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2 or Zone 2.
- This equipment is suitable for use in Class I, Division 2, Groups A, B, C, D; Class I, Zone 2, Group IIC; or non-hazardous locations.

IECEx

The CIM meet the requirements of explosion protection according to IECEx.

IECEx classification: Ex ec IIC T4 Gc

IECEx certificate: IECEx UL 22.0089X

The CIM meets the requirements of the following standards:

- IEC 60079-0, Edition 7 + Corr. 1

  Hazardous areas - Part 0: Equipment - General requirements
- IEC 60079-7, Edition 5.1

  Explosive atmospheres - Part 7: Equipment protection by increased safety «e»

Specific Conditions of Use:

- The equipment shall only be used in an area of at least pollution degree 2, as defined in IEC 60664-1.
- The equipment shall be installed in an enclosure that provides a minimum ingress protection of IP 54 in accordance with IEC 60079-0 and accessible only by the use of a tool.
- Transient protection shall be provided that is set at a level not exceeding 140 % of the peak rated voltage value at the supply terminals to the equipment.
- Antenna shall be installed within the end use enclosure. Routing and remote installation (not evaluated as part of this certification) of the antenna shall be in accordance with the appropriate location regulations when installed in unclassified and/or zone 2 Hazardous Locations.

Korea Certificate

This product meets the requirements of Korean certification.

This product satisfies the requirement of the Korean Certification (KC Mark).

CCCEx approval

The following approvals according to the following standards are valid for a device with the "CCC" marking.

- Standards:
  - GB/T 3836.1-2021 (Explosive atmospheres - Part 1: Equipment - General requirements)
  - GB/T 3836.3-2021 (Explosive atmospheres - Part 3: Equipment protection by increased safety "e")
- Approvals:
  - Ex ec IIC T4 Gc
  - -20 °C to +55 °C

Special conditions for safe operation of the devices

- The equipment shall only be used in an area of not more than pollution degree 2, as defined in GB/T 16935.1.
- The equipment shall be installed in an enclosure that provides a minimum ingress protection of IP 54 in accordance with GB/T 3836.1, and accessible only by use of a tool.

- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment.
- Antenna shall be installed within the end use enclosure. Routing and remote installation (not evaluated as part of this certification) of the antenna shall be in accordance with the appropriate location regulations when installed in unclassified and/or zone 2 Hazardous Locations.

UK Conformity Assessed marking

CIM complies with the designated British standards (BS) for programmable logic controllers published in the official consolidated list of the British Government. CIM meets the requirements and protection targets of the following regulations and related amendments:

- Regulations on the restriction of the use of certain hazardous substances in electrical and electronic equipment 2012 (RoHS).
- Radio Equipment Regulations 2017

UK Declarations of Conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg

The UK Declaration of Conformity is also available for download from the Siemens Industry Online Support website under the keyword "Declaration of Conformity".

Identification for Eurasion Customs Union

- EAC (Eurasian Conformity)
- Customs union of Russia, Belarus and Kazakhstan
- Declaration of conformity according to Technical Regulations of the Customs Union (TR CU)

RCM (Australia / New Zealand)

This product meets the requirements of AS/NZS 61000.6.3 Generic standards - Emission standard for residential, commercial and light-industrial environments.

This product meets the requirements of the standard IEC/EN 61000-6-3 Generic standards - Emission standard for residential, commercial and light-industrial environments.

Recycling and Disposal

You can fully recycle CIM due to their low-pollutant equipment. For environmentally friendly recycling and disposal of your old equipment, contact a certified electronic waste disposal company and dispose of the equipment according to the applicable regulations in your country.

WEEE label (European Union)

Disposal instructions, observe the local regulations and below Recycling and Disposal.

Technical support A

A.1 Service and support

You can find additional information and support for the products described on the Internet at the following addresses:

- Technical support (https://support.industry.siemens.com/)
- LOGO! Logic Module (https://new.siemens.com/global/en/products/automation/systems/industrial/plc/logo.html)
- Your local representative (https://www.automation.siemens.com/aspa_app)
- Industry Mall (https://mall.industry.siemens.com/)

When contacting your local representative or Technical Support, please have the following information at hand:

- MLFB of the device
- BIOS version for industrial PC or image version of the device
- Other installed hardware
- Other installed software

Tools & downloads

Please check regularly if updates and hotfixes are available for download to your device. The download area is available on the Internet at the following link:

After Sales Information (https://support.industry.siemens.com/)

A.2 Troubleshooting

This chapter provides you with tips on how to locate and/or troubleshoot problems.

Problem	Possible cause	Possible remedy
The device is not operational	No power supply	Check the power supply, the power cord and the power plug.
	Device is being operated outside the specified ambient conditions	• Check the ambient conditions. • After transport in cold weather, wait approximately 12 hours before switching on the device.

Problem	Possible cause	Possible remedy
Wrong time and/or date on the CIM	You don't set the sync time source or the sync source is not available.	Set the sync time source and make sure the source is available. • If you select GNSS as the sync source, make sure the GNSS antenna works properly. • If you select NTP server as the sync source, make sure the NTP server is available and the network works well.
LOGO! V8.3 BM cannot connect to CIM with Modbus	S7 is disabled for BM.	Enable S7 connection for BM when you build Modbus TCP with CIM.
LOGO! V8.3 BM cannot connect to AWS Cloud through CIM	CIM cannot access to the Internet. S7 is disabled for BM.	Enable S7 connection when LOGO! V8.3 BM connects to AWS Cloud through CIM.

Cellular module

When your CIM cannot send SMS or access the Internet, please log into the CIM web-based configuration and check the cellular status in **Cellular & GNSS** -> **Cellular Status**.

Item	Status	Possible Reasons	Possible remedy	Remarks
Cellular Data	Disabled	Cellular Data is disabled.	Enable the Cellular data on in the page **Cellular Settings**.	
Cellular Module	No Cellular Module	• The cellular module is not inserted correctly in CIM • CIM doesn't support the cellular module		If the "Cellular Module" displays the correct name, you need also check the "Cellular Module Revision" and whether the type of cellular module is supported in your country or region.
SIM card	Not Detected (still detecting ...)	• The SIM card is not inserted correctly in CIM		CIM does not support the Hot-plugging of SIM card or cellular module.
SIM card	Need PIN Code	The SIM card is set to require a personal identification number (PIN).	Contact the carrier of the SIM card for the PIN. Go to **Cellular & GNSS** ->**Cellular Status**, and enter the correct PIN.	Entering wrong PIN codes may block the SIM card. If the SIM card is locked, contact your provider to unlock it.
Network Register Status	Not registered	The Antenna is not connected correctly to CIM.	Check the Antenna connection.	
		Network quality is poor.		
		The SIM card account is in arrears.	Top up the account.	**Note**: If SIM card is in arrears, and you still cannot access to the Internet after topping up, restart the cellular module.

If all the items in cellular status are OK, but you still cannot send/receive SMS or access Internet, check the following cases.

Problem	Possible cause	Possible remedy
CIM cannot send/receive SMS	The SIM card account is in arrears.	Top up the account. Then go to the **Cellular status** page and press the button "Restart Cellular Module" to register again. If the SIM card still cannot be registered, try the following: • power off the CIM for more than two hours • change a CIM card or cellular module
	The SIM card is locked by your telecom provider.	Contact your provider to unlock it.
	The SMSC (Short message service center) number is not correct,	Ask your telecom provider for the SMSC number and Enter it in the following page of web-based configuration: **Cellular Settings** -> **SMS Center Number**.
	The cellular module doesn't support the provider's SMS.	
	The message encoding format is not 7-bit or UCS2 (16 bit).	
	The SIM card is not compatible with the cellular module.	Change a SIM card which is compatible with the cellular module.
Cannot access to Internet	The advanced settings (APN, dial-number) is not correct.	Contact your telecom provide and enter the APN in page: Cellular Settings -> Advanced Settings.
• It is slow to open the web-based configuration pages. • You get a load fail when opening the web-based configuration page.	• You didn't install the certificate on your operating system or browser. • There are too many cache files in the browser.	• Install the certificate on your operator control and monitoring system or browser. • Clear the cache files of the browser. • Close and re-open the browser.

A.3 SGLAN troubleshooting

Connection Status	Description	Possible cause
Connect error	Failed to establish the communication between SGLAN Client and SGLAN Server	• The SGLAN server enabled "only accept contact's request", and the SGLAN server didn’t store the SIM card number of client. • If the mode is IPv4 or IPv6: – The IP address is wrong – The IP address is inaccessible – The SGLAN client cannot access Internet • If the mode is SMS_v4 or SMS_v6: – The SIM card number is wrong – The IP address is inaccessible – The SGLAN client cannot access Internet – SGLAN server or SGLAN client cannot send or receive SMS
Cannot get reply when querying the IP address of CIM	The network quality is poor or the SMS is delayed.	Place your CIM in a place where mobile signal is strong.
Connect timeout	Establish the communication between SGLAN Client and SGLAN Server timed out	Check the 4G network quality of the SGLAN Server and SGLAN Client
Login fail	Login fail due to password error	Check the password
Login timeout	Failed to login in within valid time	Check the 4G network quality of the SGLAN Server and SGLAN Client
Connect break	The SGLAN is disconnected due to long-term failure of network communicate	Check the 4G network quality of the SGLAN Server and SGLAN Client
Certificate error	Failed to verify the certificate	• trust certificate is not the owned certificate or trust certificate of SGLAN server • the certificate is not in the valid period

Index