SIEMENS

SIMATIC NET

Industrial Ethernet - CloudConnect SIMATIC CC7

Operating Instructions

SIMATIC CloudConnect 712 (6GK1411-1AC00)
SIMATIC CloudConnect 716 (6GK1411-5AC00)

09/2023
C79000-G8976-C503-10

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

C79000-G8976-C503-10
Ⓟ 09/2023 Subject to change

Preface

CAUTION

To prevent injury, read the manual before use.

Products

This document contains information on the following products:

SIMATIC CC712 / SIMATIC CC716
Hardware product version 1
Firmware version V2.3
Gateway for connection of a SIMATIC S7, SIMATIC S7Plus, OPC UA, or Modbus station to a cloud system, OPC UA server for SIMATIC S7 data

Figure 1 SIMATIC CC716

The MAC address of the device is located below the socket for the power supply. You will find the article number on the device front.

You will find the hardware product version on the right side of the device as placeholder "X". "X 2 3 4", for example, indicates hardware product version 1.

Validity

This manual is valid for the following products:

Product name	Article number	Functions
SIMATIC CloudConnect 712	6GK1411-1AC00	Connection of 1 process station over Ethernet
SIMATIC CloudConnect 716	6GK1411-5AC00	Connection of up to 7 process stations In addition: 1 digital input, 1 digital output, PROFIBUS DP connection

Individual paragraphs or sections that are only valid for the CC716 are labelled with the short form of the device.
Example: "PROFIBUS (CC716)"

Purpose of the manual

This manual describes the properties of the modules and shows application examples. It supports you when installing, connecting up and commissioning the modules.

The required configuration steps are described. You will also find instructions for operation and information about the diagnostics options.

Required experience

To install, commission and operate the module, you require experience in the following areas:

- Data transfer via Ethernet / Internet / PROFIBUS
- Cloud systems, MQTT
- OPC UA
- Automation engineering

Terminology: Names and abbreviations

The following terms and abbreviations are used in this document:

- **CC712**
  Short form for the gateway SIMATIC CloudConnect 712
- **CC716**
  Short form for the gateway SIMATIC CloudConnect 716
- **Device / Gateway / Module**
  Designations for the two products "SIMATIC CC712" and "SIMATIC CC716"
  If content in the manual applies to only one of the two device variants, this will be explicitly pointed out.
- **Station**
  Process station (SIMATIC S7 / SIMATIC S7Plus / OPC UA station using OPC UA client / Modbus)
- **WBM**
  Web Based Management
  Web pages of the device for configuration and diagnostics data
- **API**
  Application Programming Interface
  HTTP-based AP interface for configuring the WBM

- **DB**
  Data block of a SIMATIC CPU
- **SiOME**
  Siemens OPC UA Modeling Editor
  The free "Siemens OPC UA Modeling Editor" tool supports you in defining your own OPC UA information models or mapping existing Companion Specifications.
  Link: (https://support.industry.siemens.com/cs/ww/en/view/109755133)

New in this release

- Support of S7Plus stations

Replaced edition

Edition 06/2023

Current edition of the manual and application example on the Internet

You can find the current version of this manual on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/25621/man)

You can find an application example here:
Link: (https://support.industry.siemens.com/cs/ww/en/view/109766675)

Cross references

In this document there are cross references to other sections.

To be able to return to the initial page after jumping to a cross reference, some PDF readers support the command <Alt>+<left arrow>.

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

You will find the license conditions as a loadable file on the WBM pages of the device. You will find the description of opening and loading license conditions in section User data for the first login to the WBM (Page 68).

You can find the file with the license conditions for open source software under the following name:

- OSS_CloudConnect_99.html

Cybersecurity notes

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrialcybersecurity.html).

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

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html).

Device defective

If a fault develops, please send the device to your Siemens representative for repair. Repairs on-site are not possible.

Recycling and disposal

The product is low in pollutants, can be recycled and meets the requirements of the WEEE directive 2012/19/EU "Waste Electrical and Electronic Equipment".

Do not dispose of the product at public disposal sites. For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact.

Keep to the local regulations.

You will find information on returning the product on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/view/109479891)

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary on the Internet at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/view/50305045)

Training, Service & Support

You will find information on training, service and support in the multilanguage document "DC_support_99.pdf" on the Internet pages of Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/en/view/38652101)

Table of contents

Security recommendations

1

NOTICE
Information security Connect to the device and change the default password for the factory-set user "admin" before you operate the device.

To harden the device against security threats and prevent unauthorized access to the device and/or network, observe the following security recommendations.

General

- Check the configuration and ambient conditions of the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products.
- Check regularly for security updates of the products and use them.
- Check regularly for new features on the Siemens Internet pages.
  - Here you will find information on industrial security:
    Link: (http://www.siemens.com/industrialsecurity)
  - You can find a selection of documentation on the topic of network security here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)
- Keep the software up to date. Always use the latest software version of the device. Information regarding product news and new software versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/25621/pm)
- If Siemens detects and resolves security incidents in the products, this is published in Security Advisories. You can find the documents for CC7 on the following Siemens AG web page:
  Link: (https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications)

- The gateway has two interfaces for network separation and implementation of the cell protection concept:
  - Process interface (P2)
    The interface (P2) is used for connecting to the subnet of the process stations and accessing the WBM of the module for configuring. This network is considered an internal, protected network.
  - Cloud interface (P1)
    The interface (P1) is used for connecting to the Internet or to a router over which the broker or the network with external OPC UA clients can be reached. This network is considered an external network. The gateway to unprotected networks such as the Internet must be protected by means of a separate firewall.

  When the internal and external network are disconnected, an attacker cannot access internal data. Access from the cloud interface (P1) to devices in the internal network at the process interface (P2) is not possible via IP routing. IP routing is not supported.
- It is also possible to operate the process stations and the cloud broker in the same subnet. In this case, the cloud broker and the process stations are all in the internal, protected network. This use case is intended for self-administered brokers and should not be used for external cloud systems on the Internet such as Insights Hub, MindSphere, AWS, Azure, etc.
  For this purpose, the option "Cloud interface in the same network" is offered in the section Interface configuration (Page 74). When the option is enabled, the unused interface P1 is disabled and access to the gateway via this unused interface is prevented.
- Use a firewall to connect the internal, protected network to external networks and configure it with restrictive rules.
- No product liability will be accepted for operation in a non-secure infrastructure.
- For data transmission via a non-secure network, use additional security components that provide an encrypted VPN tunnel (IPsec, OpenVPN).
- Terminate connections correctly (e.g. logout in WBM).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.

Physical access

Restrict physical access to devices to qualified personnel because the plug-in data medium can contain sensitive data.

Security functions of the product

- Think about the services with which you want to enable access to the process stations via public networks.
- This product must not be operated on unprotected/trustworthy networks (e.g. the Internet) without additional upstream protective devices.
- Use the options for security settings in the configuration of the product:
  - Activate the security functions of the product and the devices involved.
  - Use secure protocol variants (see below).

- The configuration files can be saved with and without user details, passwords, certificates and private keys. Configuration files that contain sensitive user data are always stored encrypted. A password can also be optionally assigned to prevent unauthorized use.
  Make sure that the configuration files outside the device are suitably protected. You can store the files at a safe location and transfer them via secure communications channels.
- Use a central logging server to log changes and access operations. Operate your logging server within the protected network area and check the logging information regularly.
- If you require communication with devices that use processes for encrypted communication that are no longer recommended due to known vulnerabilities, you can enable or disable legacy cipher support as required, refer to section MQTT configuration (Page 110) or HTTP profiles (Page 113).

Authentication and users

Note

Accessibility risk - Risk of data loss

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings which completely removes all configuration data.

- Replace the default passwords for all user accounts before you use the device.
- Define rules for the use of devices and assignment of passwords. Follow current recommendations on defining strong passwords, e.g. by the Federal Office for Information Security (Link: (https://www.bsi.bund.de)).
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use one password for different users and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- A password must be changed if it is known or suspected to be known by unauthorized persons.

Certificates and keys

- There is a preset SSL/TLS certificate for access to the WBM. Replace this certificate with a user-generated, high-quality certificate with key.
  Use a certificate signed by a reliable external or internal certification authority.
- Use a certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.

- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Protocols

Secure and insecure protocols

- Avoid or disable non-secure protocols and services, for example HTTP or NTP.
  These protocols are available for historical reasons, but not intended for secure applications.
  Use non-secure protocols on the device with caution.
- Only activate protocols that you require to use the system.
- Check whether use of the following protocols and services is necessary:
  - Syslog
  - DHCP options 66/67
  - S7
- Use secure protocols when access to the device is not secured by physical protection measures.
  - The NTP protocol provides a secure alternative with NTP (secure).
  - The HTTP protocol provides a secure alternative with HTTPS.
  - An S7Plus station with TLS offers a secure alternative to the unencrypted S7 station.
  - An OPC UA station with active encryption offers a secure alternative to the unencrypted S7 station.
- Restrict the services and protocols available to the outside to a minimum.
- If you require non-secure protocols and services, operate them only within a protected network area.

Decommissioning

- Decommission the device properly to prevent unauthorized persons from accessing confidential data in the device memory.
- To do this, restore the device to the factory settings. Also restore the factory settings on the storage medium.

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

1.1 Ports

Server ports

The following table provides you with an overview of the open ports on this device.

- **Protocol / function**
  Protocols that the device supports.
- **Port number (protocol)**
  Port number assigned to the protocol.
- **Default of the port**
  - Open
    The port is open at the start of the configuration.
  - Closed
    The port is closed at the start of the configuration.
- **Port configurable**
  Specifies whether the port number can be set in the WBM.
- **Authentication**
  Specifies whether authentication of the communication partner takes place or whether authentication can be configured.
- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption can be configured.

Protocol / function	Port number (protocol)	Default of the port	Port configurable	Authentication	Encryption
HTTP [1) 2)]	80 (TCP)	Open	Yes	No	No
HTTPS [2)]	443 (TCP)	Open	Yes	Yes	Yes
OPC UA server port	4840 (TCP)	Closed	Yes	Yes, when security is enabled.	Yes, configurable

1) Is rerouted to HTTPS in the factory settings.

2) Protocol can only be used at the process interface (P2) in the factory settings.

Client ports

Make sure that you open port 443 in your configuration PC (HTTPS) as well as the required client ports of the services used in the respective firewall in the subnet of the cloud in intermediary routers/gateways.

This can be:

- Broker port
  - MQTT unsecured: 1883 (TCP)
  - MQTT via TLS: 8883 (TCP)
  - HTTP: 80 (TCP)
  - HTTPS: 443 (TCP)

  The port numbers can be set in the WBM.
- OPC UA client / 4840 (TCP)
  The port number can be set in WBM.
- NTP / 123 (UDP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- Syslog / 514 (UDP)
  The port number can be set in WBM.
- Modbus/TCP / 502 (TCP)
  The port number can be set in WBM.
- S7 / 102 (TCP)
- S7Plus / 102 (TCP)

Planned operating environment

2

2.1 Application

Applications of the gateway

The CC712 and CC716 gateways are designed for connection of process stations in protected automation cells to internal or external cloud systems via MQTT or HTTP and/or the connection of external OPC UA clients.
You can find supported process stations, cloud systems and OPC UA functions in the following subsection.
You can protect the automation cells to the outside through the firewall functionality of a SCALANCE S, for example.
You can find specific configuration examples of the automation cells to be connected, including system sketches, in the section Configuration examples (Page 21).

2.2 Functions and communication services

Process stations

The gateway can communicate with the following process stations and their supported products:

- SIMATIC S7-1200/1500/ET200SP
  S7Plus communication via:
  - Ethernet
- SIMATIC S7-300/400/1200/1500/ET200SP/LOGO!
  S7 communication via:
  - Ethernet
  - PROFIBUS/MPI (CC716)
- Modbus controllers
  Communication via Ethernet (Modbus/TCP)
- OPC UA Station
  Communication via Ethernet and integrated OPC UA client

Protocols for the cloud connection

The gateway supports the following protocols for communication with a cloud broker or cloud server:

- MQTT
  According to OASIS standard version 3.1 / 3.1.1 / 5.0
- HTTP
  HTTP/1.0 and HTTP/1.1 versions, optionally via TLS

Supported cloud systems

The gateway supports the connection to cloud systems that support a broker functionality with the above-mentioned requirements and the functions described below.

The cloud access ("Cloud profile") of the gateway is adapted to communication with the following cloud systems and supports the listed services and functions:

- Insights Hub (Siemens)
  Service: MindConnect IoT Extension
  Function: Publisher
- AWS (Amazon)
  Service: IoT Core
  Function: Publisher and Subscriber
- Azure (Microsoft)
  Service: IoT Hub
  Function: Publisher and Subscriber
- IBM Cloud (IBM)
  Service: Watson IoT Platform
  Function: Publisher and Subscriber
- Other Cloud
  Profile for another cloud system
  Function: Publisher and Subscriber

OPC UA server for process data

The gateway can be used as OPC UA server for transferring process data. The gateway reads process data from a connected process station and makes it available to one or more OPC UA clients as an OPC UA server.

The server function can be enabled or disabled in the configuration.

The OPC UA server supports the following functions:

- Reading and writing variables
- Monitoring variables (MonitoredItems) using Subscriptions
- Hierarchical browsing of addresses

The OPC UA server is implemented based on the "Micro Embedded Device 2017 Server Profile" of the OPC Foundation. For details, see:
Link: (https://profiles.opcfoundation.org/profile/1659)

The OPC UA server supports the functions relevant for this profile from the following specifications:

- IEC/TR 62541-1 (08-2012) OPC Unified Architecture - Part 1: Overview and Concepts
- IEC/TR 62541-2 (02-2009) OPC Unified Architecture - Part 2: Security Model
  For the supported security profiles, refer to the section OPC UA Security (Page 94).
- IEC 62541-3 (08-2012) OPC Unified Architecture - Part 3: Address Space Model
  For the supported data types, refer to the section Data points (Page 136).
- IEC 62541-4 (08-2012) OPC Unified Architecture - Part 4: Services
- IEC 62541-5 (08-2012) OPC Unified Architecture - Part 5: Information Model
- IEC 62541-6 (08-2012) OPC Unified Architecture - Part 6: Mappings
- IEC 62541-7 (09-2010) OPC Unified Architecture - Part 7: Profiles

Configuration using the WBM

You configure the gateway parameters in Web Based Management (WBM). The WBM consists of Web pages stored in the gateway. From a configuration PC you connect to the WBM of the gateway via HTTPS. You can only reach the WBM via the process interface (P2) in the factory settings.

2.3 Configuration examples

Below you will find examples of possible configurations with the "CloudConnect 7" gateway:

Connecting process stations

In the configurations shown, the gateway reads process data from one or more S7 stations and transfers them via MQTT to a cloud broker and/or makes the data available to OPC UA clients via the OPC UA server.

The process stations in the automation cell are connected to the process interface (P2) of the gateway. The cloud broker is connected to the cloud interface (P1) via a SCALANCE S/M.

A Modbus station or an OPC UA server, for example the automation device of a third-party manufacturer, can also be connected to a cloud broker for data transfer.

- When it is connected to a SIMATIC S7, the gateway communicates using an S7 connection. Alternatively, S7 stations with OPC UA servers, e.g. a CPU1500 or a CPU1200 as of FW 4.0, can also communicate via an OPC UA connection. The gateway is the OPC UA client here. Data from the S7 station with activated "Optimized block access" option can also be accessed via OPC UA.
  Alternatively, stations such as a CPU1500 or a CPU1200 can communicate via an S7Plus connection. Data from the station with activated "Optimized block access" option can also be accessed via S7Plus.
- When it is connected to a Modbus station, the gateway communicates using Modbus/TCP.
- When connected to an OPC UA server, the gateway communicates with the process station as an OPC UA client.

Configuring a CC712

The process station is a SIMATIC S7-300 in this example.

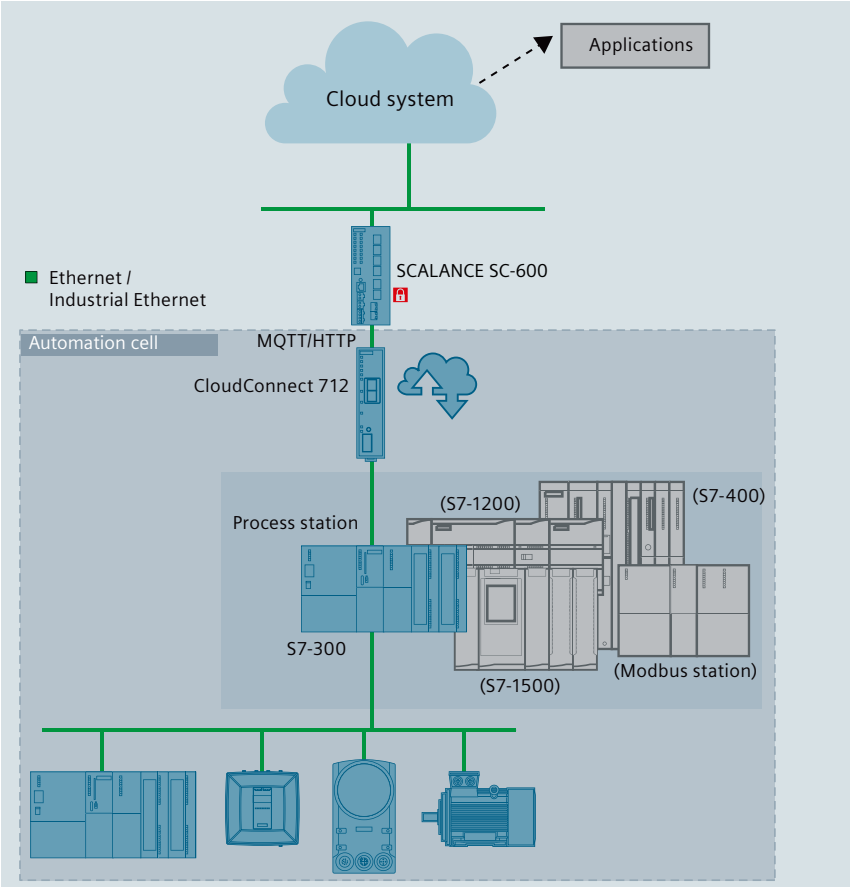


Figure 2-1 CloudConnect 712: Connection of a station to the cloud

Configuring a CC716

You can connect up to 7 stations over Ethernet or PROFIBUS using the CC716 gateway. The gateway transfers the data to a cloud broker using MQTT.

In the example shown, an S7-300 is connected via Ethernet, an S7-1200 and an S7-400 via PROFIBUS and an S7-1500 via OPC UA.

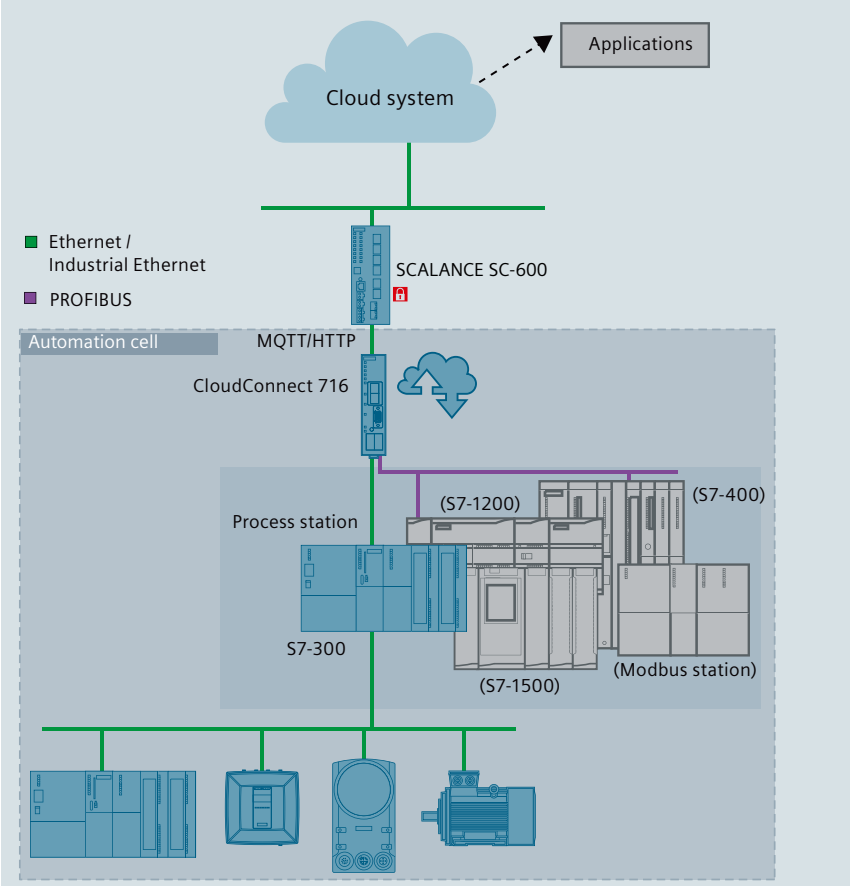


Figure 2-2 CloudConnect 716: Connection of stations to the cloud

Connection of process stations to external OPC UA clients

Configuring a CC712

In the configuration shown, the CC712 gateway transfers process data of an S7 station over OPC UA to a central control room or one or more OPC UA clients.

The gateway reads process data from the S7 station and, as OPC UA server, makes it available to one or more OPC UA clients.

The process stations in the automation cell are connected to the process interface (P2) of the gateway.
The control center or the OPC UA clients are connected to the cloud interface (P1) via a SCALANCE S/M.

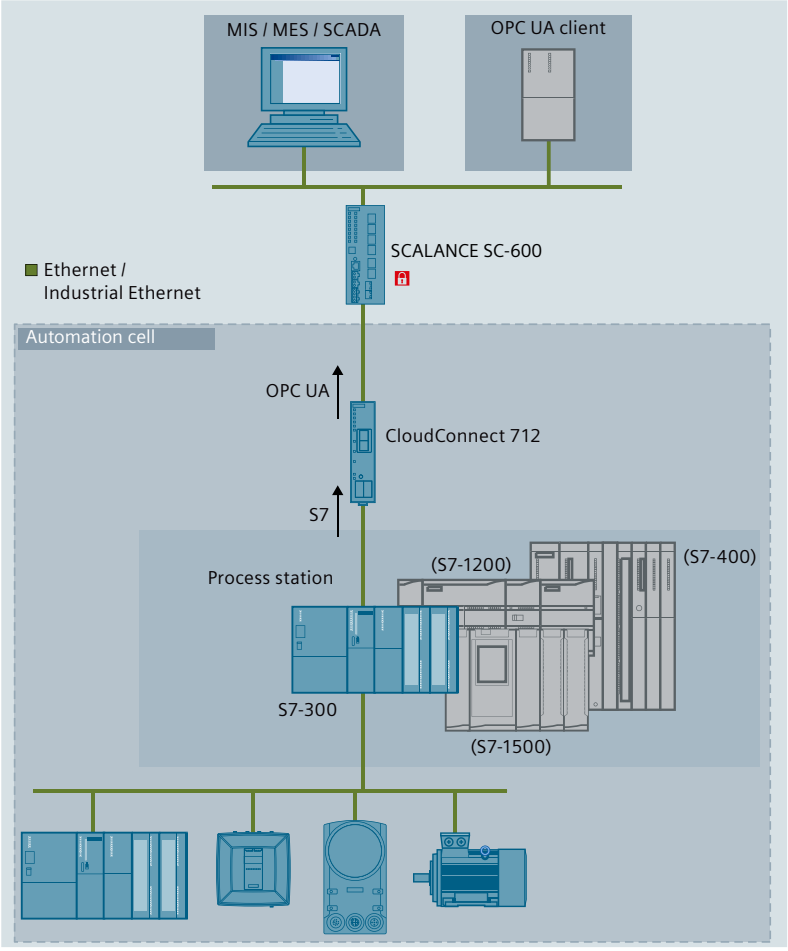


Figure 2-3 CloudConnect 712: Connection of a station to OPC UA clients

Via the CC716 gateway, the following stations can be connected via Ethernet or PROFIBUS and the data can be exchanged with the external OPC UA clients.

- Up to 7 SIMATIC S7 stations and OPC UA stations
- Up to 10 Modbus stations in addition

Overview of functions 3

3.1 Other services and properties

Other services and properties

- **IP configuration**
  - The gateway supports IP addresses according to IPv4 and IPv6. For details, see section Ethernet (Page 74).
  - Address assignment:
    The IP address, the subnet mask and the address of the default router can be set in the configuration.
  - DHCP: As an alternative, the IP address can be obtained at every interface independently from a DHCP server.
  - DNS: DNS servers can be optionally set up to resolve the host names of communication partners.
- **Time-of-day synchronization over Industrial Ethernet**
  Time-of-day synchronization of the gateway can be configured according to the following NTP method (Network Time Protocol):
  - NTP
  - NTP (secure)

  For more information, refer to the section System time (Page 154).
- **CLP (Exchangeable storage medium)**
  The gateway can save the configuration data on a CLP. The CLP is an external storage medium and does not ship with the product.
  For information on the CLP slot, see section CLP Slot (Page 39).
  For information on the functions of the CLP, see section Using a CLP (Page 56).
  For ordering data of the available CLPs, see appendix CLPs (Page 187).
- **Diagnostics**
  With the following means and methods, you can obtain the diagnostics data of the gateway:
  - LEDs
  - Web diagnostics

  You will find more information on diagnostics in the section Diagnostics (Page 167).

3.2 Configuration limits - communication

The gateway supports the following maximum quantity structure.

Connection resources over the process interface

- **Number of connections via S7Plus protocol**
  - CC712: Max. 1 S7Plus connection with an S7Plus station via Ethernet
  - CC716: Max. 7 S7Plus connections with S7Plus stations via Ethernet
- **Number of connections via S7 protocol**
  - CC712: Max. 1 S7 connection with an S7 station via Ethernet
  - CC716: Max. 7 S7 connections with S7 stations via Ethernet or PROFIBUS
- **Number of connections via OPC UA client**
  - CC712: Max. 1 OPC UA client connection to an external OPC UA server
  - CC716: Max. 7 OPC UA client connections to external OPC UA servers
- **Number of connections via Modbus/TCP**
  Max. 10 connections to Modbus stations
- **Number of connections to the configuration PC**
  Max. 2 HTTPS connections

Maximum number of connections

S7/S7Plus connections and OPC UA client connections are counted together. The maximum number is:

- CC712: 1 connection
- CC716: 7 connections

Number of process data

Note

For S7Plus stations, the max. number of available data points depends on the CPU type used

CC7 works exclusively on a subscription basis with S7Plus stations. If the maximum configuration limit is exceeded and the CPU therefore cannot process the subscription, no changeover to Polling takes place. When the subscription fails, all data points of the S7Plus station with quality "BAD" are transferred and a diagnostics message is created.

- **Variables in the data area of S7, S7Plus or OPC UA stations**
  - CC712: Max. 500 variables in total
  - CC716: Max. 3500 variables in total
    You can create multiple stations that represent the same physical device. This increases the amount of process data that can be read from this device. You configure the stations from which the process data is read in the section Process access (Page 81).
- **Variables per S7, S7Plus or OPC UA stations**
  Max. 500 variables
- **Arrays per S7, S7Plus / OPC UA client station**
  Max. 100 arrays

- **Strings per S7, S7Plus / OPC UA client station**
  Max. 100 strings
- **Variables in the data area of Modbus stations**
  Max. 100 variables per Modbus station

Connections over the Cloud interface

- **Number of connections to a cloud profile**
  Max. 3 active cloud profiles
- **Number of connections of the integrated OPC UA server to external OPC UA clients**
  Max. 10 simultaneous sessions with OPC UA clients

OPC UA server

As OPC UA server, the gateway supports the following quantity structure.

- **Number of variables**
  - CC712: Total of max. 1500 variables; 500 for S7/S7Plus/OPC + 10 * 100 for Modbus
  - CC716: Total of max. 4500 variables; 7 * 500 for S7/S7Plus/OPC + 10 * 100 for Modbus
- **Number of supported subscriptions**
  Max. 5 subscriptions per session
  In total maximum of 50 subscriptions at the same time
- **Number of items per subscription**
  Max. 1000 variables per subscription
  Max. 4500 variables over all subscriptions

3.3 Range of functions of the WBM

Web Based Management (WBM)

You configure the gateway using its Web Based Management (WBM). The WBM consists of Web pages that can be called up in the Web browser of a connected PC. From your PC you connect to the WBM via HTTPS. In addition, via the HTTP-based AP interface, you can access the WBM of the gateway and configure API requests with it. For more information, see section API (Page 67).

For information on the Web browsers that can be used on the PC, see section Scope of delivery and requirements (Page 28).

Access to the WBM

To call the WBM, you need to establish a connection between the PC and the gateway via LAN, see section Establishing a connection to the WBM (Page 67).

Overview of the functions of the WBM

The WBM provides the following functions:

- **User management**
  In the open WBM, you specify the user name and the password for the "Administrator" role. You can only access the WBM and make changes with this administrator information. You can add up to six additional users and assign them to the desired role. Users with the "GUEST" role can only access diagnostics data without making changes to the configuration.
- **Configuration**
  Using the WBM, configure the following function areas:
  - Basic functions such as the time of day or IP address
  - Connection of the process station
  - Connection to the higher-level network (cloud, OPC clients)
  - Communication functions
- **Maintenance and diagnostic functions**
  - Diagnostics
  - Loading and storing the configuration data
  - Downloading new firmware versions

Reusing the configuration file

The configuration data you create in the WBM is saved in the gateway. If you have plugged in a CLP, the configuration data of the gateway is also written to the CLP after clicking the "Apply" button.

If you are using multiple gateways with partially identical configuration data, you can export the configuration file of a gateway and download it to additional gateways where you can adapt it as needed.

3.4 Scope of delivery and requirements

Scope of delivery

The following positions ship with the gateway:

- Gateway "CloudConnect 7"
- Terminal block for power supply of the gateway
- Terminal block for the digital input and the digital output (CC716)

Required accessories

The following accessories (which do not ship with the product) are required for gateway operation:

- Power supply
  You need a 24 V DC external voltage source.
- PC
  To configure the gateway, you need a configuration PC with suitable Web browser (see below).
- LAN cable
  For the connection of the configuration PC to the X2 LAN interface of the gateway, you need a Cat 5 or higher ITP cable.
- Cable for the process connections
  To connect the process station(s) with the gateway, you need the appropriate LAN or PROFIBUS cable.

Communication partner

- **Process access**
  For process access you need a station in productive operation, alternatively:
  - S7 station
  - OPC UA station with OPC UA server
  - Modbus station
- **Cloud access / External OPC clients**
  - For cloud access, you need the access set up to a cloud broker.
  - You need at least one configured OPC UA client to connect external OPC UA clients.

  If you use a service on the Internet as cloud system, you need to protect the automation cell to the outside with additional security components (e.g. SCALANCE S/M).

Requirements in the S7 stations

⚠ WARNING

Writing values to outputs

When referencing to outputs with write access, note that the values are written immediately to the outputs of the CPU without first being processed by the user program.

Writing values has a direct influence on the process.

The following requirements need to be met in your STEP 7 project or in the connected S7 stations.

- Variables / symbols
  For access to the process data by referencing to variables of the CPU, variables or symbols must be created in the relevant CPU.
  Write access via the MQTT Subscriber function of the gateway is only possible in DB variables of the CPU.
  STEP 7 Professional: The "Optimized block access" option must be disabled for DBs and access via an S7 connection. The option need not be disabled for access via the OPC UA server of the CPU or an S7Plus connection.
  The variables of the CPU must be marked as follows for use by OPC UA services (options selected):
  - "Accessible from HMI/OPC UA"
  - "Writable from HMI/OPC UA"
    Required for write access

  For further details, see section Data points (Page 136).
- OPC UA: Components of the identifier
  During configuration, note that the following names are used as part of the identifier in the NodeID of a variable:
  - CPU name
  - Name of the DB variable
- CPU 1200/1500 via S7 connection
  - Read protection cannot be configured under "Protection & Security" in the CPU.
  - Access via PUT/GET must be configured under "Protection & Security" in the CPU.
- CPU 300/400 via S7 connection
  Read protection cannot be configured under "Protection" in the CPU.
- CP 300/400 via S7 connection
  The following requirements must be met on the CP for access to the station via a CP:
  - When "IP access protection" is configured, the IP address of the gateway must be configured with the right "A".
- CP 1200 via S7 connection
  For access to the station via a telecontrol CP, S7 communication must be enabled on the CP under "Communication types".

Web browser for the configuration PC

For access to the WBM of the gateway, the configuration PC needs one of the following Web browsers.

- Apple Safari
- Firefox Quantum
- Google Chrome
- Microsoft Edge

The Web browser must accept cookies. The application uses a cookie.

JavaScript must be enabled in your Web browser.

Recommendation: Use the latest available version of the Web browser.

Optional

- CLP
  Exchangeable storage medium for storing configuration data
- NTP server - can be reached over interface P1 / P2
- DHCP server - can be reached over interface P1 / P2
- DNS server - can be reached over interface P1 / P2

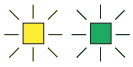
LEDs, Connectors, Buttons, CLP

4

4.1 LEDs

The LEDs on the front show the states of the module.

The LED symbols in the table below correspond to the following states of the LEDs:

LED symbol			
LED status	OFF	ON (steady light) *	Flashing

* : Part flashes yellow and part lit green

Meaning of the LED displays

LED name (colors)	**LED pattern**	**Meaning / Module status**
Power (green)	**Power supply**	
		Power OFF
		Shut down
		Power ON
Device Connection (green / yellow)	**Connection to process stations**	
		No process station configured
		Shut down
		Existing connection to all configured process stations
		No communication with at least one process station. Possible causes: • Connection establishment active • Incorrect configuration
		Stop of communication via: • WBM: "Maintenance > Communication / Restart" • CC716: Digital input
Cloud Connection (green / yellow)	**Connection to Cloud**	
		No connection to cloud server configured
		Shut down
		Existing connection to all configured cloud servers
		No communication with at least one cloud server. Possible causes: • Connection establishment active • Cloud server not ready • Incorrect configuration

LED name (colors)	LED pattern	Meaning / Module status
Diagnosis (green / yellow)	**Diagnostics**	
	☐	No error
		Shut down
		Diagnostic message regarding NTP or DHCP available, see WBM "Maintenance > Diagnostics".
		Reset is initiated (button pressed during startup).
	■	Reset is executed (button can be released).
	■	No configuration, module has the factory settings
P1 / P2 (green / yellow)	**Connection to Ethernet at interface P1 or P2**	
	☐	No Ethernet connection
	■	Existing Ethernet connection
	■	Existing connection with data traffic
LEDs only on CC716		
MPI/DP (green / yellow)	**Connection to PROFIBUS/MPI**	
	☐	No connection to PROFIBUS/MPI configured
		No communication with PROFIBUS/MPI. Possible causes: • Wire break, short circuit • Incorrect configuration, e.g. wrong transmission speed • Stop of communication
	■	Established connection to PROFIBUS/MPI
DI (yellow)	**Digital input**	
	■	Digital input ON (1)
	☐	Digital input OFF (0)
DO (yellow)	**Digital output**	
	■	Digital output ON (1)
	☐	Digital output OFF (0)

4.2 Connections

4.2.1 Ethernet interfaces P1/P2

Ethernet interfaces

The gateway has two Ethernet interfaces according to Gigabit standard IEEE 802.3ab, designed as RJ45 socket.

- P1
  Cloud interface for connecting a cloud broker and external OPC clients
- P2
  Process interface for connecting the stations of the automation plant

Note

Connection to subnets

The two Ethernet interfaces are not designed as a switch, but are intended for connection to different networks.

If the connection to the cloud is in the same subnet as the process connection, disable the cloud interface P1 in the configuration. This physically switches off the interface.

You can find the properties of the Ethernet interfaces in section Technical specifications (Page 175).

4.2.2 PROFIBUS/MPI interface (CC716)

9-pin D-sub socket (MPI/DP)

The PROFIBUS/MPI connection is a 9-pin D-sub socket and operates according to the RS-485 standard.

You also have the option of connecting to optical PROFIBUS networks via an Optical Bus Terminal OBT or an Optical Link Module OLM.

You can find the properties of the PROFIBUS interface in section Technical specifications (Page 175).

4.2.3 Digital Input / Output (CC716)

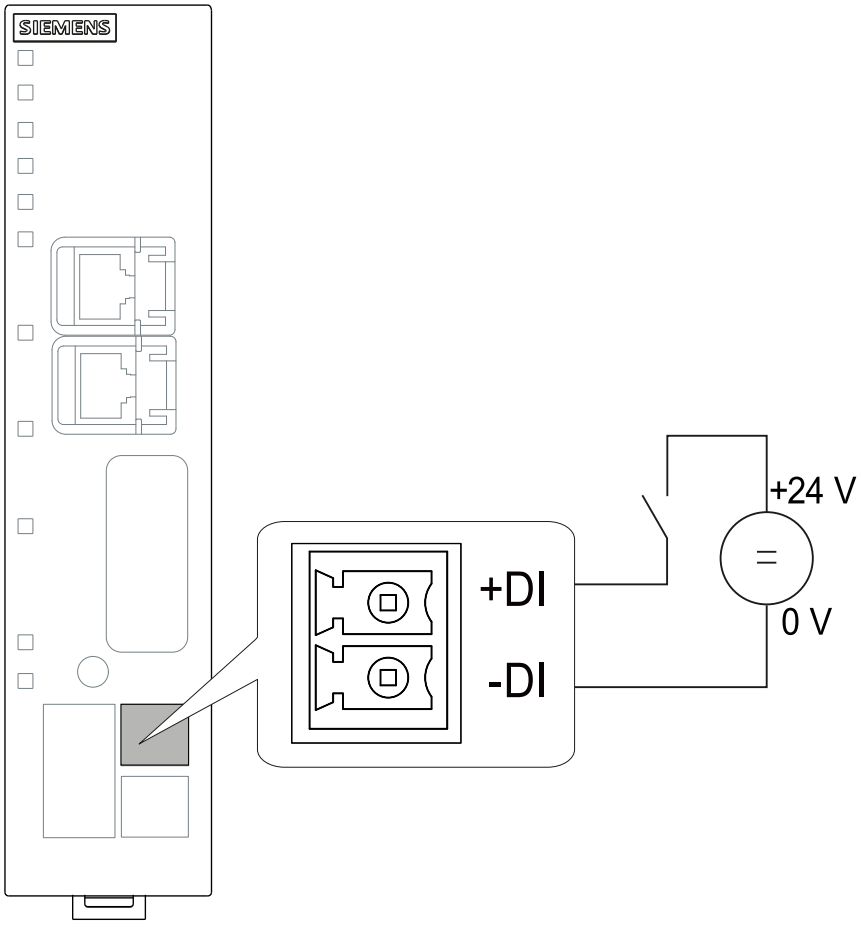
The CC716 gateway has a digital input and a digital output. They can be used as follows:

- Digital input
  The input can be used alternatively as a trigger for the following functions:
  - External trigger for transferring data points
  - Stop/start trigger for process communication
- Digital output
  The output is a switch and can be used to generate a status signal:
  - Connection status to the cloud

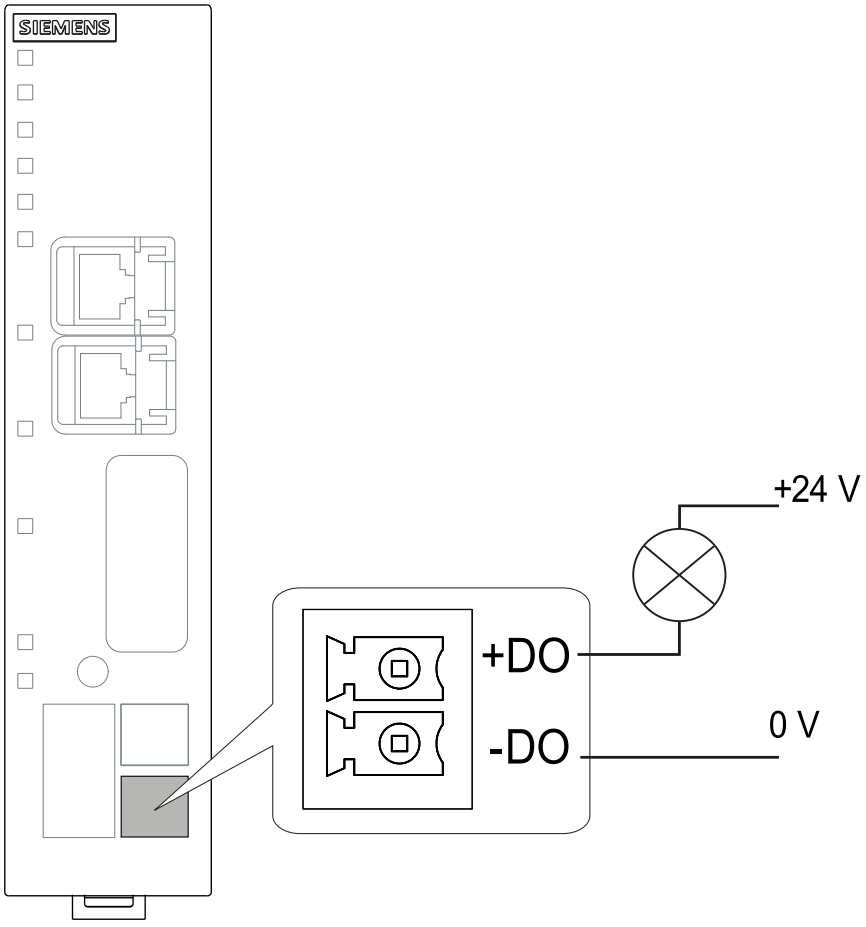
The functions are configurable, see section DI/DO (CC716) (Page 80).

For information on allocation of the terminal blocks, see section Connecting (Page 50).

Digital input



Digital output



The output is a switch that switches the signal at +DO to -DO.

4.2.4 External power supply

External power supply

The connector (socket) for the external 24 V DC power supply is located on the front of the gateway. The external power supply is redundant (optional use).

The power supply is connected to the gateway with the supplied 5-pin plug-in terminal block.

The connection has a mechanical reverse polarity protection. The terminal block is designed so that it can only be inserted in one position into the socket of the gateway.

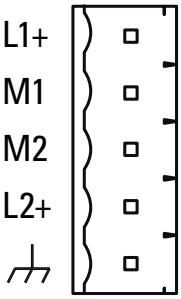


Figure 4-1 Socket of the external power supply

For information on allocation of the socket and for the connection, see section Connecting (Page 50).

You will find further data on the power supply in section Technical specifications (Page 175).

4.3 The button "SET"

Functions of the button

WARNING

EXPLOSION HAZARD

Do not press the button if there is a potentially explosive atmosphere.

The "SET" button has the following functions:

- **Resetting to factory settings**

  Note

  Configuration data is deleted

  By resetting to factory settings, the gateway is reset to the status as it was delivered from the factory. This deletes all the configured settings.

  The data on an optional CLP are deleted as well.

  For the precise effects of resetting, refer to the section Restarting and resetting (Page 172).

Pressing the button

Duration of pressing the button (seconds)	Function and operation
≥ 5 s	**Resetting to factory settings** 1. Turn off the power supply. 2. Switch the power supply on again while pressing the button. Hold down the button for at least 5 seconds during startup. Reset is prepared while the "Diagnosis" LED flashes. 3. Release the button when the LED stops flashing. While the LED lights up with a green steady light, the gateway performs the reset. Once reset is complete, the gateway performs a restart and can be reached using the default IP address set at the factory.

4.4 CLP Slot

The slot for an optional CLP is located on the back of the module.

For information on inserting and removing the CLP, see section Using a CLP (Page 56).

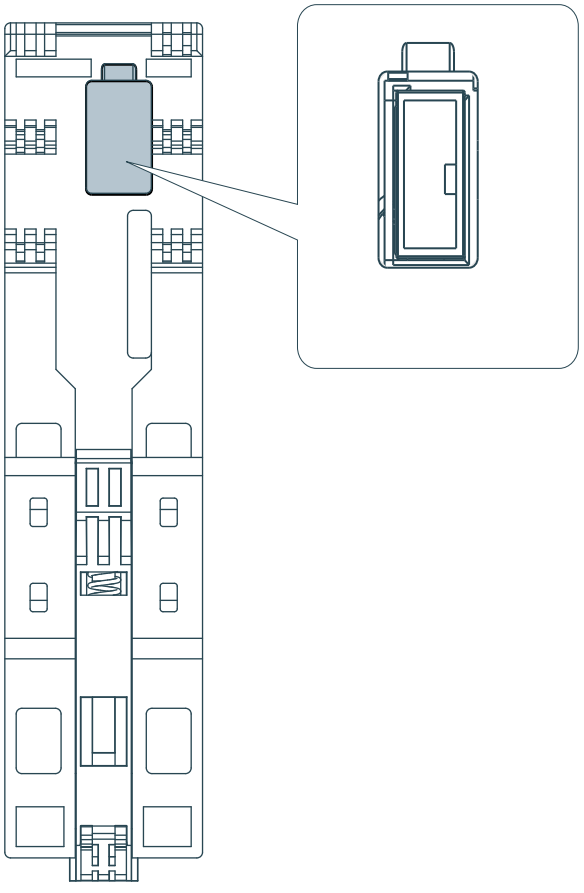


Figure 4-2 Slot for optional CLP on the back of the device

Installation, wiring, commissioning, removal 5

5.1 Important notes on using the device

Safety notices on the use of the device

Note the following safety notices when setting up and operating the device and during all associated work such as installation, connecting up or replacing the device.

WARNING

If the device is installed in a cabinet, the inner temperature of the cabinet corresponds to the ambient temperature of the device.

5.1.1 Notes on use in hazardous areas

WARNING

EXPLOSION HAZARD

DO NOT OPEN WHEN ENERGIZED.

WARNING

EXPLOSION HAZARD

Replacing components may impair suitability for Class 1, Division 2 or Zone 2.

WARNING

The device may only be operated in an environment with pollution degree 1 or 2 as described in EN/IEC 60664-1, GB/T 16935.1.

WARNING

EXPLOSION HAZARD

Do not connect or disconnect cables to or from the device when a flammable or combustible atmosphere is present.

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.

WARNING

If a device is operated in an ambient temperature of more than 60 to 70 °C, the temperature of the device housing may be higher than 70 °C. The device must therefore be installed so that it is only accessible to service personnel or users that are aware of the reason for restricted access and the required safety measures at an ambient temperature higher than 60 °C.

5.1.2 Notices for use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex

WARNING

Requirements for the cabinet

To comply with EU Directive 2014/34 EU (ATEX 114), UK Regulation SI 2016/1107 or the conditions of IECEx or CCC-Ex, the housing or cabinet must meet the requirements of at least IP54 (according to EN/IEC 60529, GB/T 4208) in compliance with EN IEC/IEC 60079-7, GB 3836.8.

WARNING

Cable

If the cable or conduit entry point exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 50 °C, only use cables with admitted maximum operating temperature of at least 80 °C.

WARNING

Suitable cables at high ambient temperatures in hazardous area

At an ambient temperature of ≥ 60 °C, use heat-resistant cables designed for an ambient temperature at least 20 °C higher. The cable entries used on the enclosure must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB 3836.1.

WARNING

Transient overvoltages

Take measures to prevent transient overvoltages of more than 40% of the rated voltage (or more than 119 V). This is the case if you only operate devices with SELV (safety extra-low voltage).

WARNING

EXPLOSION HAZARD

Do not press the SET button if there is a potentially explosive atmosphere.

5.1.3 General notices on use in hazardous areas according to UL HazLoc / FM

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

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

WARNING

EXPLOSION HAZARD

You may only connect or disconnect cables carrying electricity when the power supply is switched off or when the device is in an area without inflammable gas concentrations.

WARNING

EXPLOSION HAZARD

The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

WARNING

Wall mounting is only permitted if the requirements for the housing, the installation regulations, the clearance and separating regulations for the control cabinets or housings are adhered to. The control cabinet cover or housing must be secured so that it can only be opened with a tool. An appropriate strain-relief assembly for the cable must be used.

⚠ WARNING

Substitution of components may impair suitability for Division 2.

5.2 Installation

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

- Before mounting the device, always ensure that there is no visible damage to the device.
- Mount the device using suitable tools. Observe the information in the respective section about mounting.

⚠ WARNING

Open equipment

The device is "open equipment" acc. to the standard UL 61010-2-201. To fulfill requirements for safe operation with regard to mechanical stability, flame retardation, stability, and protection against contact, the following alternative types of installation are specified:

- Installation in a suitable cabinet.
- Installation in a suitable enclosure.
- Installation in a suitably equipped, enclosed control room.

Note

You must not install the device on a wall in hazardous areas.

⚠ WARNING

Wall mounting outside of the control cabinet or housing does not fulfill the requirements of the FM approval.

⚠ WARNING

Cable temperatures

If the cable or housing socket exceeds 70 °C or the branching point of the cables exceeds 60 °C, special precautions must be taken. If the equipment is operated in an ambient environment in excess of 40 °C, only use cables with permitted maximum operating temperature of at least 80 °C.

NOTICE
Install and remove the device only when the power is off. Switch off the power supply of the device before you install or remove the device. Installing and removing devices with the power supply on can lead to damage to the devices and to loss of data.

Installation options

You have the following options to install the gateway:

- Wall mounting
- Mounting on the following rail types (rack):
  - DIN rail
  - S7-1500 standard rail
  - S7-300 standard rail

  You can find suitable standard rails in the Siemens accessories program for automation technology, for example:
  35 mm standard mounting rail for 19" cabinets, article numbers 6ES5710-8MA11
- Mounting on pedestal
  You can use the SCALANCE M pedestal 6GK5898-8MD00 for table mounting (does not ship with the product).

Installation location

NOTICE
Installation location - Dependency of the temperature range Note the dependency of the permitted temperature range of the installation location. • Horizontal installation of the rack (DIN rail) means a vertical position of the modules. • Vertical installation of the rack (DIN rail) means a horizontal position of the modules. You will find the permitted temperature ranges in the section Technical specifications (Page 175).

Installation of the rack	Installation position of the modules
Horizontal installation of the rack	
Vertical installation of the rack	

Minimum clearances

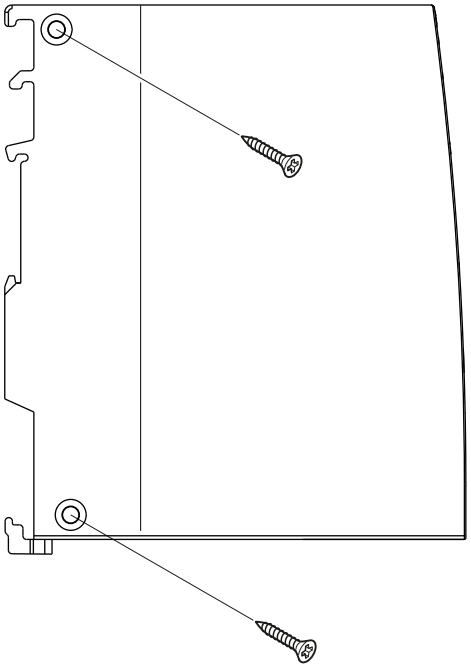
Mount the device so that its upper and lower ventilation slits are not covered, allowing adequate ventilation as protection from overheating.

Keep to the following minimum clearances for the circulation of air when the rack is installed horizontally:

- Above the device: At least 33 mm
- Below the device: At least 25 mm

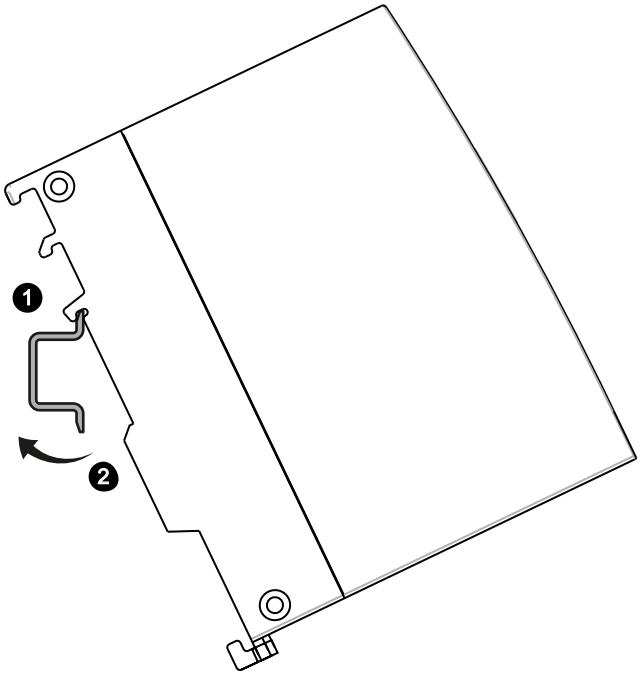
Wall mounting

1. Prepare the drill holes for wall mounting. For the dimensions, refer to the section "Dimension drawings (Page 185)".
2. Secure the device to the wall with two screws (4 mm).



Installation on a DIN rail

1. Insert the device with the respective guide ① into the standard rail:
   - Top guide for S7-1500 standard rail
   - Center guide for S7-300 standard rail
   - Bottom guide for DIN rail
2. Tilt the device to the back until the mounting rail release audibly locks in place ②.



3. Ground the mounting rail.

NOTICE
Grounding For reasons of electrical safety, the DIN rail must be connected to the protective conductor system (PE) of the electrical system.

Note

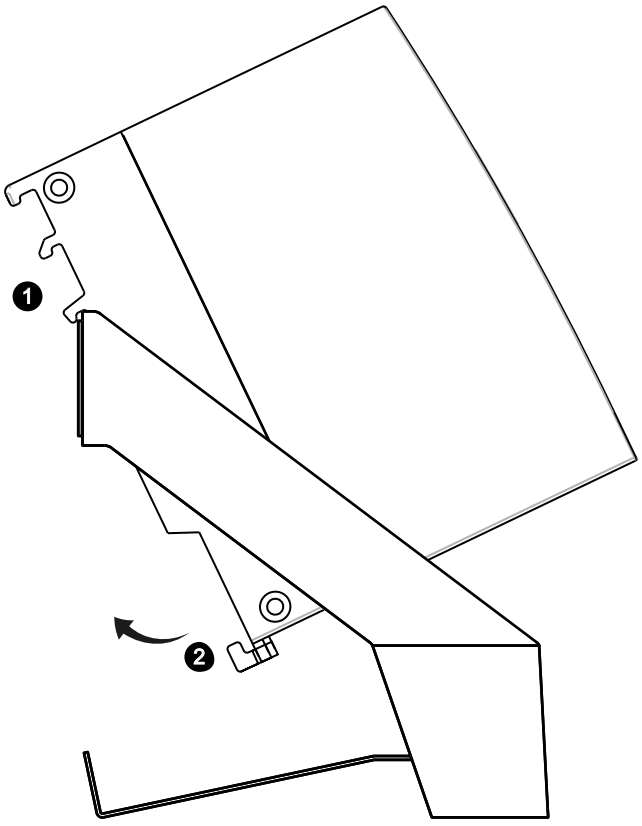
Protecting the modules from slipping on the DIN rail

If you install the modules in an area with mechanical load, use suitable clamping devices at both ends of the device group to secure the modules on the DIN rail, e.g. Siemens and retainer 8WA1808.

The end retainers prevent the modules separating under mechanical load.

Mounting on pedestal

1. Insert the device with the bottom housing guide on the top edge of the pedestal ①.
2. Press the device against the pedestal until the mounting rail release audibly locks in place ②.



Uninstalling

Follow the steps below to remove the device from the rail:

1. Turn off the supply voltage of the device.
2. Pull the power supply plug and the cables of the communication networks.
3. Pull down the mounting rail release on the rear of the device.
4. Tilt the device out of the standard rail.

5.3 Connecting

⚠ WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

- Only use connectors that meet the requirements of the relevant type of protection.
- If necessary, tighten the connector screw connections, device fastening screws, grounding screws, etc. according to the specified torques.
- Close unused cable openings for electrical connections.
- Check the cables for a tight fit after installation.

⚠ WARNING

Unprotected cable ends

There is a risk of explosion due to unprotected cable ends in hazardous areas.

- Protect unused cable ends according to IEC/EN 60079-14.

⚠ WARNING

Lack of equipotential bonding

If there is no equipotential bonding in hazardous areas, there is a risk of explosion due to equalizing current or ignition sparks.

- Ensure that equipotential bonding is available for the device.

⚠ WARNING

Improper installation of shielded cables

There is a risk of explosion due to equalizing currents between the hazardous area and the non-hazardous area.

- Ground shielded cables that cross hazardous areas at one end only.
- Lay a potential equalization conductor when grounding at both ends.

⚠ WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

- When connecting intrinsically safe and non-intrinsically safe circuits, ensure that the galvanic isolation is performed properly in compliance with local regulations (e.g. IEC 60079-14).
- Observe the device approvals applicable for your country.

⚠ WARNING

Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS)

The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS).

This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

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

NOTICE

Suitable fusing for the power supply cables (corresponds to "Limited Energy")

The current on the terminal must not exceed 3 A. Use a fuse for the power supply that protects against currents > 3 A.

The fuse has to be designed for protection of DC power supply circuits as well as for the following requirements.

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for DC (min. 60 V / max. 3 A)
  - Breaking current min. 10 kA
  - UL/CSA listet (UL 248-1 / CSA 22.2 No. 248.1)
  - Classes R, J, L, T or CC
- In other areas:
  - Suitable for DC (min. 60 V / max. 3 A)
  - Breaking current min. 10 kA
  - Approved for power supply circuits (branch circuits) according to local regulations (e.g. IEC 60127-1, EN 60947-1)
  - Breaking characteristics: B or C circuit breakers and fuses

If the properties of the supplying current source are known, the following fuse is also possible:

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for DC (min. 60 V / max. 3 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval in accordance with UL 1077 or CSA C22.2 No. 235
- In other areas, the fuse must meet the following requirements:
  - Suitable for DC (min. 60 V / max. 3 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to IEC/EN 60934
  - Breaking characteristics: Max. 120 s at 2 x I_n

You do not need a fuse for the power supply cable if you use a voltage source according to NEC Class 2 or a power supply from the range of accessories, see appendix Power supply (Page 187).

Recommendation: Use the power supply of a process station if this is in the vicinity of the gateway.

Note

Protective ground

A PELV circuit contains a connection to protective ground. Without a connection to protective ground, or in case there is a fault in the connection to the protective ground, the voltage for the circuit is not stabilized.

NOTICE
Fuses for the cables of the digital output (corresponds to "Limited Energy") The current on the terminal must not exceed 1 A. Use a fuse for the power supply that protects against currents > 1 A. The fuse has to be designed for protection of DC power supply circuits as well as for the following requirements. • In areas subject to the NEC or CEC, the fuse must meet the following requirements: – Suitable for DC (min. 60 V / max. 1 A) – Breaking current min. 10 kA – UL/CSA listet (UL 248-1 / CSA 22.2 No. 248.1) – Classes R, J, L, T or CC • In other areas: – Suitable for DC (min. 60 V / max. 1 A) – Breaking current min. 10 kA – Approved for power supply circuits (branch circuits) according to local regulations (e.g. IEC 60127-1, EN 60947-1) – Breaking characteristics: B or C circuit breakers and fuses

The following fusing is also possible for the digital output:

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for DC (min. 60 V / max. 1 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to UL 1077 or CSA C22.2 No. 235
- In other areas, the fuse must meet the following requirements:
  - Suitable for DC (min. 60 V / max. 1 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to IEC/EN 60934
  - Breaking characteristics: max. 120s at 2 x I_n

Order of the work

NOTICE
Connection only with power off Only connect the device with the power switched off. The device can be disconnected from the power supply with the terminal block.

Requirement: The device is mounted.

1. Connect the external power supply to the terminal block of the device.
   Use functional earthing (see below) to ground the gateway.
2. Connect the cables of the two Ethernet networks to the interfaces of the device.
   See the note in section Ethernet interfaces P1/P2 (Page 35).
3. CC716:
   Connect the gateway on the RS485 socket to PROFIBUS via a plug-in cable.

NOTICE
Contacting the shield of the cable on the connector The shield of the cable must be contacted. To do this, strip the insulation from the end of the cable and connect the shield to functional earth.

4. CC716:
   If necessary, connect the cable for the digital input/output to the terminal block of the device.
   – Always wire the digital input and output in pairs.
   – The maximum permitted cable length is 30 m.

   For information on the position of the terminals, see section Digital Input / Output (CC716) (Page 36).
5. Turn the power supply on only after the device has been completely wired and connected.

The further procedure is described in the section Commissioning (Page 55).

Terminal blocks for digital input/output and power supply

The plug-in terminal blocks for the sockets have mechanical reverse polarity protection.

You can find additional technical details in the section Technical specifications (Page 175).

Digital input/output (CC716)

Table 5-1 Assignment of the sockets for the digital input (DI) and digital output (DQ)

Terminal	Assignment
DI+	DC 24 V
DI- (ground)	-
DO+	Max. 24 V DC / max. 1 A
DO-	-

Power supply

Note

The power supply unit of the device is not electrically isolated.

Use only copper cables for the power supply.

Table 5-2 Pin assignment of the socket for the power supply

Terminal	Assignment
L1+	DC 24 V
M1	Reference ground
M2	Ground reference for redundant connection (optional)
L2+	24 V DC for redundant connection (optional)
⏚	Functional earth

5.4 Commissioning

5.4.1 Commissioning

Commissioning

1. After connecting the power supply to the gateway, switch on the power supply.
2. Connect the configuration PC to the gateway for configuration, refer to the section Establishing a connection to the WBM (Page 67).

If you want to use a CLP, turn off the power supply before you start configuring, insert the CLP and turn on the power supply again.

To make it easier to commission multiple gateways, see section Configuration (Page 164).

Requirements for operation

At least the following requirements apply to operating the gateway:

- Configuration of the device
- At least one running process station
- A configured cloud service or external OPC UA client on the internal OPC UA server
- Connecting the gateway to the networks of the communication partners

Applying the configuration data during commissioning

For information on the buttons of the WBM, see section General functions of the WBM (Page 63).

The "**Save**" button

Confirm all your entries by clicking the "Save" button. This causes the settings to be stored in the buffer, but not yet applied by the device. This prevents inconsistent changes from being loaded to the Runtime system when the WBM page is changed.

The "Apply" button

All saved configuration data is applied to the Runtime system by clicking on the "Apply" symbol.

5.4.2 Using a CLP

Exchangeable storage medium CLP

The gateway can be operated with an exchangeable CLP. The configuration data can be stored on this exchangeable medium and this is retained if there is a power failure.

This removable medium simplifies the replacement of the gateway. By simply exchanging the plug, all data can be transferred without having to be configured again.

The CLP is supplied with power by the gateway. The CLP retains all data permanently when the power is turned off.

Note

Using brand-new CLPs

If you are using a brand-new CLP, follow the steps below:

1. Insert the CLP into the turned-off gateway.
2. Switch on the power of the gateway.
3. Format the CLP.
   See section Configuration (Page 164) for more on this.

Clicking the "Apply" button automatically writes the configuration data of the gateway to the CLP.

Startup of the gateway with configuration file on CLP

If a configuration file is stored on the CLP and you plug the CLP into a gateway, this configuration is overwritten by clicking the "Apply" button.

By inserting a CLP with valid configuration data into a brand-new gateway or a gateway that was reset to factory settings, you can cause the gateway to start up with the configuration file saved on the CLP.

Function

The configuration of the gateway is automatically saved on the CLP when you apply the configuration in the WBM.

A device with the CLP plugged in only uses the configuration data on the CLP during startup if it has been reset to the factory settings. This is, however, only possible when the data was written by a compatible device type.

This allows fast and simple replacement of the basic device. If a device is replaced, the CLP is taken from the failed device and inserted in the replacement. As soon as it starts up, the replacement automatically applies the same device configuration as the failed device.

Inserting the CLP and startup behavior

Note

Insert and remove only when power is off

The CLP may be inserted or removed only when the power is off!

The slot for the CLP is located on the back of the device, see section CLP Slot (Page 39).

To insert the CLP, follow these steps:

1. Turn off the power to the gateway.
2. Insert the CLP in the slot.
   The CLP can only be inserted in one position.
3. Switch on the voltage again.
   The behavior of the gateway depends on the state of the gateway and the CLP:

- Gateway is reset to factory settings (e.g. brand new)
  - CLP unformatted (factory state) or previously used in a different device type:
    Gateway starts up without configuration data, CLP remains unformatted.
  - CLP formatted by a compatible gateway CLP without configuration data
    Gateway starts up without configuration data.
  - CLP formatted by a compatible gateway - CLP with valid configuration data:
    Gateway starts with the configuration data of the CLP.
- Gateway with internally stored configuration data
  - CLP unformatted (factory state) or previously used in a different device type:
    Gateway starts with internal configuration, CLP remains unformatted.
  - CLP formatted by a compatible gateway CLP without configuration data
    The gateway starts up with internal configuration data. By changing and applying the configuration, it is written to the CLP.
  - CLP formatted by a compatible gateway - CLP with valid configuration data:
    The gateway starts up with internal configuration data. By changing and applying the configuration, it is written to the CLP.

Removing the CLP

1. Turn off the power to the device.
2. Insert a screwdriver between the front edge of the CLP and the slot and remove the CLP.

Diagnostics

Malfunctions of the CLP are signaled by diagnostic messages.

5.5 Disassembly

⚠ WARNING

Improper disassembly

Improper disassembly may result in a risk of explosion in hazardous areas.

For proper disassembly, observe the following:

- Before starting work, ensure that the electricity is switched off.
- Secure remaining connections so that no damage can occur as a result of disassembly if the system is accidentally started up.

5.6 Maintenance and cleaning

⚠ CAUTION

Hot surfaces

Risk of burns during maintenance work on parts with a surface temperature above 70 °C (158 °F).

- Take appropriate protective measures, for example, wear protective gloves.
- Once maintenance work is complete, restore the touch protection measures.

⚠ WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.

⚠ WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories and original spare parts.
- Observe all relevant installation and safety instructions described in the manuals for the device or supplied with the accessories or spare parts.

⚠ WARNING

Cleaning the housing

- **In hazardous areas**
  Only clean the outer parts of the housing with a damp, but not wet, cloth.
- **In non-hazardous areas**
  Only clean the outer parts of the housing with a dry cloth.

Do not use any liquids or solvents.

Configuration 6

HTTPS connection over the process interface

For security reasons, you can only establish a connection to the WBM via the process interface of the gateway from your PC in the factory settings.

Note

Ensure that the PC and gateway are located in a protected network.

The cloud interface is blocked for access to the WBM in the factory settings. On the "Maintenance" > "HTTP Server" page, the interface for WBM operation can be activated.

6.1 Overview of the WBM pages

Opening the WBM pages

All page titles that you need for navigation through the WBM are located at the top of each WBM page.

Open a WBM page by clicking the page title.

The WBM tabs

The following list provides an overview of the WBM pages and their functions.

- Info (Page 70)
  - Info
  - Communication
  - System monitoring
  - Network

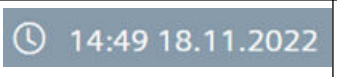
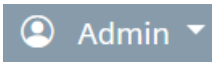
  These pages provides an overview of important status and configuration data of the gateway.
- Interface configuration (Page 74)
  - Configuration of the gateway Ethernet interfaces
  - Configuration of the PROFIBUS / MPI interface (CC716)
  - Configuration of the digital input/output (CC716)

- Process access (Page 81)
  - Configuration of S7 station (S7 Ethernet / S7 PROFIBUS/MPI (CC716))
  - S7Plus station configuration
  - Configuration of Modbus station
  - Configuration of OPC UA station
- OPC UA server (Page 92)
  - Configuring the OPC UA server
  - Configuration and administration of the XML Nodeset
  - Configuration and management of events
- Cloud configuration (Page 106)
  - Configuring the MQTT settings
  - Configuring the HTTP settings
  - Publisher: Configuring the topics/groups and the payload format and assigning the data points
  - Subscriber: Configuring the topics/groups and assigning the data points
- Data points (Page 135)
  - Configuring the data points of the process stations
- Maintenance (Page 153)
  - Managing the web server settings
  - Time-of-day synchronization / setting the time
  - Creating and managing certificates
  - User management
  - Firmware update
  - Backing up and restoring the configuration
  - Process communication, restart
  - Diagnostic messages
  - Exporting logging data

6.2 General functions of the WBM

Symbols in the toolbar

You can reach the following functions using the displays and symbols in the toolbar:

Symbol	Function
	Time and date of the runtime system
	Profile: Edit the user profile Language: Switching the WBM language Log off: Ends the connection to the WBM.
	Apply All saved data is applied to the Runtime system.
	Opens the online help of the WBM.
	Shows the number of active sessions.

Menu bar

The menu bar shows the tabs of the WBM over which you reach the different pages of the WBM.

When you minimize your browser window, the display of the tabs disappears and the following symbol is displayed:

Symbol	Function
	Shows the tab titles as navigation with a minimized browser window.

Input boxes with filter

Input boxes as shown below have a filter function. If you enter a character or a character string and click on the filter icon, all existing elements containing this character string are displayed. You can use the following placeholders when filtering:

- %
  The percent sign serves as a placeholder for any character string.
- _
  The underscore serves as a placeholder for exactly one character.

If you wish to use the percent sign or the underscore as a character and not as a placeholder, place a backslash "\" in front of the character.

You find these input boxes in the assignment of data points to topics, for example.

Figure 6-1 Empty input box with cursor

Save

Confirm all your entries by clicking the "Save" button. Your settings are thus saved to the buffer.

The saved configuration data is not applied by the device yet by saving. This prevents inconsistent changes from being loaded to the Runtime system when the WBM page is changed.

Application to the runtime system 

All saved configuration data is applied to the Runtime system by clicking on the "Apply" symbol.

Incorrect entries in the configuration

The input boxes of the WBM are checked during input for faulty content and consistency. Notes are output for boxes with detected errors during saving. The settings can only be saved after the error has been corrected.

Grayed out fields cannot be edited.

6.3 Permitted characters and parameter lengths

6.3.1 Permitted characters and parameter lengths

When configuring user data, passwords, device parameters etc., ASCII character sets are often specified. Below you will find ASCII character sets with their hexadecimal code and the corresponding character.

Standard characters

- **0x30 .. 0x39**
  0 1 2 3 4 5 6 7 8 9
- **0x41 .. 0x5A**
  A B C D E F G H I J KL M N O P Q R S T U V W X Y Z
- **0x61 .. 0x7A**
  a b c d e f g h i j k l m n o p q r s t u v w x y z

Special characters

- **0x21 .. 0x2F**
  ! " # $ % & ' ( ) * + , - . /
- **0x3A .. 0x40**
  : ; < = > ? @
- **0x5B .. 0x60**
  [\ ] ^ _ `
- **0x7B .. 0x7E**
  { | } ~

Special characters ≥ 0x80

- **0x80, 0xA3, 0x8A, 0x9A, 0x8E, 0x9E, 0xB5**
  € £ Š š Ž ž µ
- **0xC0 .. 0xFF**
  À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

Note

Character limit

Input fields have a defined maximum string size, e.g. 1024 bytes. On input, the bytes are counted, not the characters. This means that you can save the following values, for example, depending on the data type.

Data types:

- 1024 ASCII characters
- 1024 x byte data
- 512 x special symbols according to UTF-8
- or a mix of different data types with a total size of up to 1024 bytes.

Table 6-1 **Characters and formats of the strings that can be entered in the WBM**

Parameter	String min.	String max.	**Permitted characters / format**
Name, Topic	1	1024	**Standard characters** **0x20 spaces** / + - _ . : ; @
Hostname	0	255	According to the rules for DNS names with a combination of: • 0x2D .. 0x2E • 0x30 .. 0x39 (no numbers alone) • 0x41 .. 0x5A • 0x61 .. 0x7A
User name (user, OPC, Cloud)	2	1024	All the characters listed above
Password (user, OPC, Cloud, Zertifikat, privater Schlüssel)	0	1024	All the characters listed above
OPC Server / Client			
Application URI	1	1024	**Standard characters** / + - _ . : ; @
Application name	1	1024	**Standard characters** / + - _ . : ; @
URL path (optional)	1	1024	**Standard characters** & / = ? # - _
Namespace URI	0	1024	**Standard characters** / + - _ . : ; @

Name of the root directory	0	1024	**Standard characters** / + - _ . : ; @
Node ID of the root directory	0	1024	**Standard characters** / + - _ . : ; @
Cloud connection			
Client ID	1	254	All the characters listed above
Topic prefix	0	1024	All the characters listed above
Topic suffix	0	1024	All the characters listed above
Last will topic	1	65535	All the characters listed above
Last will / testament	0	65535	All the characters listed above
Device Name	0	1024	All the characters listed above
Device type	0	1024	All the characters listed above
Payload templates			
Version	0	2	**0x30 .. 0x39**
Zertifikate			
Organization name (O)	0	64	**Standard characters** / + - _ . : , ; @
Organizational unit (OU)	0	64	**Standard characters** / + - _ . : , ; @
Town (L)	0	128	**Standard characters** / + - _ . : , ; @
State (ST)	0	128	**Standard characters** / + - _ . : , ; @
Country (C)	0	2	Two-letter country code (according to ISO 3166)
Common name (CN)	0	64	**Standard characters** / + - _ . : , ; @
Domain component (DC)	0	16	**Standard characters** / + - _ . : , ; @
URI	0	1024	According to the rules for DNS names with a combination of: • 0x2D .. 0x2E • 0x30 .. 0x39 (no numbers alone) • 0x41 .. 0x5A • 0x61 .. 0x7A

DNS name	0	255	According to the rules for DNS names with a combination of: • 0x2D .. 0x2E • 0x30 .. 0x39 (no numbers alone) • 0x41 .. 0x5A • 0x61 .. 0x7A
E-Mail	3	254	The e-mail address has the following structure: Part1@Part2.Part3 Part 1@: Standard characters + special characters (< 0x80; only one "@" character is allowed) Part 2+3: Standard characters

6.4 Calling the WBM

6.4.1 API

The API server of the gateway is permanently active.

The gateway can be configured and diagnosed automatically via the HTTP-based interface.

You can find more information on configuring the WBM of the gateway with the API interface in the "SIMATIC CC7 API server" Getting Started. See Link: (https://support.industry.siemens.com/cs/ww/en/ps/25621/man)

6.4.2 Establishing a connection to the WBM

Requirements

You can only establish a connection between a PC and the gateway via HTTPS.

You can establish a connection over the P2 interface of the gateway.

The condition for access to the gateway is that the PC is located in the same subnet and that the gateway can be reached.

First connection setup with preset IPv4 address

Use the following preset IPv4 address of the gateway during the first connection setup:

- P2 interface address: 192.168.0.55 / 24

Note

IP address of the CP

By default, the DHCP client of the gateway is disabled. Make sure that the PC has a fixed IP address during the first connection setup and that it is located in the same subnet as the connected interface of the gateway.

When using a DHCP server you do not need to specify the addressing on the PC to be connected. When it is connected to the network, the PC is assigned an address.

Connection to the Web server of the gateway

Follow the steps below to connect the PC to the Web server of the gateway:

1. Open the Web browser.
2. Enter the IP address of the gateway in the address line of the Web browser:
   – https://<Address>

   If you access via HTTP, the address is automatically diverted to HTTPS.
   With HTTPS connections when you log in, a warning can appear that the Web page is not secure or that the certificate is not trustworthy. If you are sure that you have entered the correct address, ignore the message. If necessary add the connection to the exceptions (depending on the Web browser).

When the connection setup is successful, the logon window of the WBM opens.

6.4.3 User data for the first login to the WBM

HTTPS connection

Only HTTPS connections are supported.

You can establish a connection between a PC and the WBM of the device.

Changing standard user data

After establishing a connection between the PC and the device, the WBM opens with the login page.

Note

Changing standard user data

For security reasons, the factory set user data (user name, password) of the standard user must be changed when you log in the first time, see section User (Page 159).

Standard user data for the first login to the WBM is preassigned by the system:

User data	Default values set in the factory
User name	admin
Password	admin

An administrator can be set up with all available rights for operation of the WBM.

6.4.4 Logging in

Logging in

After establishing a connection between the PC and the device, the WBM opens with the login page.

Note

Entering the wrong user name or password

After entering an incorrect user name or password three times, a lockout period of one minute begins. Only after the lockout time has expired can you try to log in again.

- **User name**
  Enter the user name here.
- **Password**
  Enter the password here.
- **Logging in**
  Click the button to set up the connection to the WBM.

When you log in for the first time, you are prompted to change the default user data. You can find the rules for password assignment in the section User (Page 159).

Open Source Software and links to additional information

You can find the following links at the bottom of the login page:

- **Online help**
  Opens the online help of the WBM.
- **Open Source Software**
  Opens the license conditions document for the open source software.
  If necessary, you can save the document on your PC.
- **Siemens Industry Online Support**
  Opens the page of the gateway in the Internet portal of Siemens Industry Online Support.

6.4.5 Log out

Manual logout via the WBM

To log out of the WBM, click on the user in the toolbar and select the "Log out" option in the drop-down list.

The connection to the device is terminated. All changes to the configuration data not saved previously are lost.

Automatic logout after timeout

After the set timeout has elapsed (default 600 seconds) without saving or changing the WBM page, you are logged out and disconnected from the WBM. In this case, you must log in again.

6.5 Info

The page provides an overview of important status and configuration data of the device.

Status

- **Operating state**
  Operating state of the device
- **Process communication**
  Shows the status of the communication with the process stations.
- **System runtime (dd-hh-mm-ss)**
  Time since the last startup (dd-hh-mm-ss)
- **Serial number**
  Serial number of the device
- **Article number**
  Article number of the device
- **Hardware product version**
  Hardware product version of the device
- **U-Boot version**
  Current U-Boot version for the firmware bootloader
- **Firmware version**
  Current firmware version of the device
- **CLP**
  Shows whether a CLP is currently inserted.
- **Application checksum**
  Checksum for the current firmware version

- **Configuration checksum**
  Checksum for the current configuration of the CC7
- **Power supply**
  Shows whether the module is supplied via socket L1+, L2+ or both.

Process interface (P2)

The parameter group displays the current address data of the P2 interface.

- **MAC address**
- **IPv4 / IPv6**
  Address parameters, Default router

Cloud interface (P1)

The parameter group displays the current address data of the P1 interface.

- **MAC address**
- **IPv4 / IPv6**
  Address parameters, Default router

DNS

- **Hostname**
  Shows the local host name.
- **DNS server**
  The parameter group shows the addresses of up to two DNS servers that are either configured or assigned via DHCP.

6.5.1 Communication

On this page you obtain an overview of all configured process stations, the cloud connection and the OPC UA server.

Update

Here you set whether and in which cycle the WBM updates the displayed diagnostic messages.

Process communication

Shows the status of the communication with the process stations.

- **Protocol**
  Shows the protocol of the process station (S7 Ethernet, S7+ Ethernet, S7 PROFIBUS / MPI, OPC UA, Modbus / TCP, MQTT, HTTP).
- **Name**
  Shows the configured station name.

- **Address**
  - With S7 Ethernet: Display of the configured IP address and TSAP
  - With S7Plus Ethernet: Display of the configured IP address
  - With S7 PROFIBUS / MPI: Display of the configured PROFIBUS / MPI address and TSAP
  - With OPC UA client and Modbus: Display of the configured IP address and the port number
  - Only with OPC UA: Display of the security policy being used
- **Connection**
  Uses a symbol to show the connection status to the station:
  - ?: No information received yet, page refresh required, no data point assigned
  - Two green arrows: Station connected
  - Rotating orange arrow: Connection establishment
- **Polling cycle**
  Shows the average duration of the last 100 read cycles for each S7 Ethernet, S7 PROFIBUS and Modbus station. The duration can be compared with the configured cycle time.
  No time "--" is displayed:
  - If 100 values have not yet been determined
  - With OPC UA client stations
  - With S7Plus stations

Cloud communication

Shows the status of the communication with the active cloud profile.

- **Address**
  - Display of the configured IP address and the port number
- **Connection**
  Uses a symbol to show the connection status to the cloud:
  - ?: No information received yet, page refresh required
  - Two green arrows: Station connected
  - Rotating orange arrow: Connection establishment

OPC UA server

- **Security Policies**
  All permitted policies of the server.
- **Address**
  All addresses of the OPC UA server.
- **Sessions**
  Number of OPC UA clients connected to the server. When you click on the field, the IP addresses / port / security profiles of the connected clients are shown.

Read errors/Write errors

The fields are grayed out when there is no connection. As soon as a connection has been set up, the read and write errors are being collected and displayed.

- Green: no error
- Yellow: There is at least one error

For quicker diagnostics, the error type (e.g. BadTypeMismatch) can be read out via the drop-down list.

The read and write errors are reset at each restart or with save and confirm.

6.5.2 System monitoring

This page provides an overview of CPU utilization and memory load.

Update

Here you set whether and in which cycle the WBM updates the displayed diagnostic messages**.**

Tasks

6.5.3 Network

On this page you obtain an overview of the open ports and the connections of the module.

Update

Here you set whether and in which cycle the WBM updates the displayed diagnostic messages**.**

Open ports

Shows the status of the communication with the process stations.

- **Application**
  Specifies the type of the CC7 service.
- **Transport**
  UDP or TCP
- **Address**
  IP address and port number
- **Status**
  Listen: The port is open and waiting for the connection.
  Connected: The connection is established.

6.6 Interface configuration

6.6.1 Ethernet

In this tab, you configure the address data of the Ethernet interfaces of the device.

Note

Changes to settings relating to P1/P2 or host name

If you make changes to the settings relating to the P1/P2 interfaces or the host name, the internal network service may be restarted. You then need to log in to the WBM again or call the page again.

Interface and factory default addresses

You configure the following interfaces on the web page:

- Process interface (P2)
  The interface (P2) is used for connecting to the subnet of the process stations and accessing the WBM of the module for configuring.
- Cloud interface (P1)
  The interface (P1) is used for connecting to the Internet or to a router over which the broker or the network with external OPC UA clients can be reached.

The device supports IPv4 and IPv6 addresses.

The following address data is preset in the factory:

Table 6-2 Preset address data

	Address data preset in the factory	
	Process interface (P2)	**Cloud interface (P1)**
IPv4 address	192.168.0.55	192.168.121.55
IPv6 address	-	-
Subnet mask	255.255.255.0	255.255.255.0

Process interface (P2) / Cloud interface (P1)

Note

No address check / configuration rules

The address bands are not checked automatically.

Make sure that the subnets of the two interfaces are not the same.

Configuration of link local, multicast and broadcast addresses is not allowed for the IPv6 address.

You configure both interfaces separately.

The following parameters apply to both interfaces.

- **IPv4 / IPv6**
  - **Active**
    Activation of the respective IPv4 or IPv6 address

Note

No reachability when IP address data of the process interface is applied

The IP parameters of the process interface must match the settings of the IP address data of your PC.

- **IP address via DHCP**
  Enable the option if you want to obtain the address data of the selected interface from a DHCP server.
  When the option is enabled, the address data boxes are grayed out, and the values obtained from the DHCP server are displayed.

Note

DHCP server

To use the function, a DHCP server must be located in the subnet.

- **IP address**
  Shows the default or last configured IP address. The actual IP address is displayed on the "Info" start page.
  During the initial configuration: Assign the IP address of the respective interface or activate addressing by a DHCP server.
- **Subnet mask (only IPv4)**
  Shows the preset, last configured or the last subnet mask to be obtained from the DHCP server.
  During the initial configuration: Assign the subnet mask of the respective interface.
- **Prefix length** (only IPv6)
  Shows the IPv6 prefix that is preset, most recently configured or obtained from the DHCP server.
  During the initial configuration: Assign the prefix to the respective interface.
  Range of values: 0...128
  Default setting: 64
- **Default router**
  Shows the configured IP address of the router being used or the one last obtained with DHCP.
  During the initial configuration: Assign the IP address of the router.
- **Hostname**
  With enabled DHCP client function, the configured host name is transferred to the DHCP server using the DHCP option 12.
  Default: cc7-device

DNS server

- **DNS server**
  You have the option of configuring the IP addresses of up to two DNS servers.
  With an activated DHCP server, the related IP addresses of the DNS server are displayed.
  If no DNS server is used, the address box is empty.

Routing Table

This is where you define via which routes can be used for data exchange between the different subnets but cannot be reached via the default router.

You can enter up to 20 static routes.

- **Create**
  Another route can be created. You are forwarded to a separate page.
- **Delete**
  The selected table row is deleted.
- **Active**
  Activation and deactivation of defined routes
- **Destination Address**
  Enter the IP address and associated subnet mask of the destination that can be reached via this route. Use the CIDR notation, for example, 192.168.28.0/24 or 120.12.0.0/16.
- **Gateway Address**
  Enter the IP address of the gateway via which this network address is reachable.
- **Interface**
  Specify whether the route can be reached via interface P1 or P2.

6.6.2 PROFIBUS / MPI (CC716)

In this tab, you configure the address data of the PROFIBUS interface and the bus parameters for the network connection of the gateway.

During manual configuration ("Automatic configuration" disabled), take into account address assignment due to existing bus nodes, the transmission speed set on the bus, and the profile of the connected PROFIBUS network.

PROFIBUS configuration

- **Address**
  Unique PROFIBUS/MPI address of the gateway in the bus system
  Range of values: 0...126
  Note:
  You configure the address of the gateway communication partner in the tab "Process access > Station configuration".
- **Automatic configuration**
  - Option enabled
    The gateway reads all relevant configuration data from the connected PROFIBUS network. The following parameters are hidden for the configuration.
  - Option disabled
    You configure the PROFIBUS parameters yourself.
- **Transmission speed**
  Transmission speed on the bus, value range - depending on the profile:
  9.6 kbps, 19.2 kbps, 45.45 kbps, 93.75 kbps, 187.5 kbps, 500 kbps, 1.5 Mbps, 3 Mbps, 6 Mbps, 12 Mbps
  With the "Universal" profile, max. 1.5 Mbps
- **Highest address**
  Highest possible PROFIBUS address of a node in the PROFIBUS bus system
  Range of values: 1...126

- **Profile**
  Here you can specify the method (algorithm) with which the bus parameters important for PROFIBUS operation should be calculated. The various methods are optimally adapted to the respective operating mode of the subnet and result in stable network operation.
  - Standard/DP
    The DP profile is suitable for using the DP protocol. For a homogenous DP network with maximum one Class 1 DP master and no other DP masters (additional PG is possible). The standard profile is suitable for multi-protocol and multi-master operation with fast bus nodes, for example, all SIMATIC NET S7 PROFIBUS CPs.
  - Universal
    For operation with stations that cannot be operated in the DP or Standard categories. This option can only be selected with a transmission speed ≤ 1.5 Mbps.
  - User-defined
    In this setting, you can configure some of the bus parameters.
    This profile should only be selected by trained specialists. Only change the default values if you are familiar with the configuration of the bus profile for PROFIBUS.
- **Number of masters / Number of slaves**
  When using the "Standard/DP" and "Universal" profiles, you can specify the number of masters and slaves in the network in these two text boxes. The number of masters and slaves is used for calculating the bus parameters in the network.
  Permissible value ranges for these profiles:
  - Number of masters: 0..126
  - Number of slaves: 0..126

  If you are using the "User defined" profile, the two text boxes are disabled. In this case, the boxes have a fixed presetting:
  - Number of masters: 1
  - Number of slaves: 126

Bus Parameters

The parameters (see table) that describe the properties of the PROFIBUS subnet are mostly preset:

- The bus parameters are fixed or are calculated from them with the use of the "Standard/DP" "Universal" profiles.
- If you are using the "User-defined" profile, you can configure some of the bus parameters.

Note

Configuring the bus parameters

We recommend applying the values already set in the connected PROFIBUS network for the bus parameters.

Bus parameter	Value range [1] (default) [2]	Meaning [3]
Tslot	815/995...16383 [1] (100...3000)	Slot time [t_Bit] The slot time specifies the maximum length of time the sender will wait for a response from an addressed partner. For the calculation, the following parameters which have an effect on the bus hardware are used as basis: • Cable length: 1...1100 m • Number of repeaters: 0...10
Max. Tsdr	76...1023 [1] (55...980)	Maximum protocol processing time [t_Bit] The maximum protocol processing time specifies the maximum time allowed for the responding station to answer. Max. Tsdr must be less than the slot time.
Min. Tsdr	11...75 [1] (11...150)	Minimum protocol processing time [t_Bit] The minimum protocol processing time specifies the minimum amount of time after which the responding station can answer.
Tset	1...255 [1] (1...240)	Trigger time [t_Bit] The trigger time is the time that can elapse in the station between receiving a data frame and reacting to it.
Tqui	0...10 [1] (0...9)	Modulator quiet time [t_Bit] The modulator quiet time is the time that a sending station needs to switch from send to receive after frame end.
GAP Factor	1...100 [1] (10...1000)	The gap update factor specifies how many token round trips occur before a new active station can be included in the logical token ring.
Retry limit	1...15 [1] (1...10)	This parameter specifies the maximum number of attempts (frame repetitions) allowed to access a station.
Tid2	55...980 Calculated value	Idle time 2 [t_Bit] Idle time 2 defines the minimum amount of time after sending an unacknowledged frame after which a sending station can send the next frame.
Trdy	11...150 Calculated value	Ready time [t_Bit] The ready time specifies the minimum amount of time after which a sending station can receive a response frame.
Tid1	37...515 Calculated value	Idle time 1 [t_Bit] Idle time 1 defines the minimum amount of time after receiving an answer after which a sending station can send the next frame.
Ttr	256...16777960 [1] (0...49888)	Target Rotation Time [t_Bit] The target rotation time is the maximum length of time available for a token round trip. During this time, all active stations (DP master etc.) are in possession of the token once. The difference between the target rotation time and the actual token holding time of a station determines the length of time remaining for the other active stations (PG, additional DP masters etc.) to send frames. Recommendation for the value: 5000 * "Highest PROFIBUS address"
Ttr (ms)	Calculated value	Target Rotation Time [milliseconds], calculated from "Ttr".

[1] Value can only be defined under Profile "User-defined"; value range depending on transmission speed.

[2] Default: Values depending on the profile and transmission speed.

[3] The parameter values are specified in t_Bit. Exception: Ttr (ms)

Bit time (t_Bit)

The bit time is the time that elapses when sending a bit. It is calculated from the reciprocal value of the transmission speed.

Using the "Bit time" unit has the advantage that the bus parameters can be specified independently of the transmission speed used.

To calculate the time in milliseconds from the number of bit time units, use the following formula:

$$\text{Time (ms)} = \frac{\text{Number of bit-time units}}{\text{Transmission speed (kbps)}}$$

6.6.3 DI/DO (CC716)

You set the function of the digital input and output for the CC716 here.

If you do not need the input or output, select the "No function" option.

Digital Input

Configuration

The input can be disabled or used alternatively as a trigger for the following functions:

- **No function**
  The input is disabled.
- **Use as data point trigger**
  - 1 → 0
    A falling edge at the input triggers the transfer of the topics with the assigned data points once with the 1 → 0 trigger condition.
  - 0 → 1
    A rising edge at the input triggers the transmission of the topics with the assigned data points with the trigger condition 0 → 1 once.
- **Control process communication**
  The process communication is only started after a restart/after the configuration is applied if the input has a logical 1.
  When there is a restart/the configuration is applied with a logical 0 at the input, process communication is stopped.
  An edge change at the input causes the following:
  - 1 → 0: Stop
    With a negative edge at the input, communication with all process stations is stopped.
  - 0 → 1: start
    With a positive edge at the input, communication with all process stations is started.

Digital output

Configuration

The output can be disabled or used alternatively as a display for the following functions:

- **No function**
  The output is disabled.
- **Connection to the cloud**
  The output signal shows the following:
  - 0: disconnected
    The output signal 0 indicates that the connection of the gateway to at least one active cloud profile has been terminated.
  - 1: connected
    The output signal 1 indicates that the connection of the gateway to all active cloud profiles has been established.

6.7 Process access

You get to an overview page of the respective station type via the drop-down list.

- S7 stations
- S7Plus stations
- Modbus stations
- OPC UA stations

The overview page shows a list of the created stations and their properties.

The displayed properties can be edited directly on the overview page.

Create

The button leads to a new page on which all parameters of the new station can be set. Clicking the "Save" button applies the settings and the new station appears in the table on the overview page.

Delete

By clicking the button, the selected station is deleted.

Note

Accidental deletion

If you accidentally delete a station, you cannot undo the deletion.

6.7.1 S7 stations

6.7.1.1 S7 Ethernet

The gateway and the SIMATIC S7 station communicate over S7 connections. The connection type is TCP. The gateway is the active partner during connection setup.

Requirements:

- PUT/GET communication must be activated in the S7 CPU.
- STEP 7: The "Optimized access" option must be deactivated for data blocks of the CPU that are accessed by the gateway via an S7 connection.

You do not necessarily have to create a connection at the station end for the gateway to communicate with the S7 station. The CPU reserves connection resources to unspecified partners.

If you nevertheless want to create fixed connections, disable the "Active communication establishment" option in the connection properties of the CPU. In this case, write down the TSAP of the connection assigned by STEP 7 for each station.

Parameters:

- **Active**
  A connection is only established to active stations. At least one data point with a destination must be assigned to the station.
- **Name**
  Enter a name for the profile.
- **Controller family**
  Select the controller family of the connected station from the drop-down list:
  - S7-1200/1500
  - S7-300/400
  - LOGO!
- **IP address**
  IP address of the station interface (CPU or CP)

- **Standard TSAPs**
  When the option is enabled, the device uses the standard TSAPs for its local TSAP and the remote TSAP (S7 CPU). The standard settings for the remote TSAP are intended for the case that you have not configured a connection to the gateway in the STEP 7 project.
  TSAPs are entered as hexadecimal values. For an S7-300/400, the TSAP references the rack, the slot and the type of CPU connection resource.
  Examples for an S7-300 CPU:

  – TSAP: 11.02
    Rack 0, slot 2, connection resource 11

  – TSAP: 03.02
    Rack 0, slot 2, connection resource 03
    Connection configured at one end (Local end point "One-way") Connection partner "unspecified"; the gateway as connection partner is not configured.
    A connection resource for a connection configured at one end with unspecified partner has the value 03.
    A connection resource for a connection configured at both ends with unspecified partner has the range of values 0x10...0xDF.
    Recommendation for station configuration:
    Use the configuration 0/0 or 0/1 for the rack/slot.

  The following standard TSAP IDs are used:

  – Local TSAP of the gateway: 01.01

  – Remote TSAP of the controller family:
    - S7-1200/1500: 02.01
    - S7-300/400: 03.02
    - LOGO!: 20.00

  Disable the option if the remote TSAPs do not match the preset standard TSAPs. In this case, configure the TSAP that is assigned in the STEP 7 project.

- **Local TSAP**
  Range of values: 01.01 ... 7E.7E
  We recommend using the default TSAP (01.01).

- **Remote TSAP**
  Enter the TSAP of the S7 connection assigned in STEP 7 at the station end if you have configured a connection with an unspecified partner in the CPU for the gateway.
  When using a configured unspecified connection, disable the "Active connection establishment" option in STEP 7.

- **Polling cycle (ms)**
  Cycle time in milliseconds in which the gateway reads the data from the station.
  Range of values: 50...100 000 000
  Note: If you transfer large volumes of data, the actual cycle time may be longer than configured.

6.7.1.2 S7 PROFIBUS / MPI

Only for CC716

The gateway and the SIMATIC S7 station communicate over S7 PROFIBUS connections. The gateway is the active station.

Requirements:

The same requirements apply as described in section "S7 Ethernet" above.

Parameters:

- **PROFIBUS / MPI address**
  PROFIBUS address of the S7 station (gateway communication partner)
- **Controller family**
  Select the controller family of the connected station from the drop-down list:
  - S7-300
  - S7-400
  - S7-1200
  - S7-1500
- **Standard TSAPs**
  When the option is enabled, the device uses the standard TSAPs for its local TSAP and the remote TSAP (S7 CPU). The standard settings for the remote TSAP are intended for the case that you have not configured a connection to the gateway in the STEP 7 project.
  TSAPs are entered as hexadecimal values. For an S7-300/400, the TSAP references the rack, the slot and the type of CPU connection resource.
  Examples for an S7-300 CPU:
  - TSAP: 11.02
    Rack 0, slot 2, connection resource 11
  - TSAP: 03.02
    Rack 0, slot 2, connection resource 03
    Connection configured at one end (Local end point "One-way") Connection partner "unspecified"; the gateway as connection partner is not configured.
    A connection resource for a connection configured at one end with unspecified partner has the value 03.
    A connection resource for a connection configured at both ends with unspecified partner has the range of values 0x10...0xDF.

  The following standard TSAP IDs are used:
  - Local TSAP of the gateway: 01.01
  - Remote TSAP of the controller family:
    - S7-1200/1500: 01.01
    - S7-300: 03.02
    - S7-400: 03.03

  Disable the option if the remote TSAPs do not match the preset standard TSAPs. In this case, configure the TSAP that is assigned in the STEP 7 project.
- **Local TSAP**
  Range of values: 01.01 ... 7E.7E
  We recommend using the default TSAP (01.01).

- **Remote TSAP**
  Enter the TSAP of the S7 connection assigned in STEP 7 at the station end if you have configured a connection with an unspecified partner in the CPU for the gateway.
- **Polling cycle (ms)**
  Cycle time in milliseconds in which the gateway reads the data from the station.
  Range of values: 50...1 000 000 00
  Note: If you transfer large volumes of data, the actual cycle time may be longer than configured.

You configure the transmission speed and the other network parameters in the tab "Interface configuration > PROFIBUS".

6.7.2 S7Plus stations

6.7.2.1 S7Plus Ethernet

The gateway and the SIMATIC S7Plus station communicate over the Siemens communication library IOMS. The connection type is TCP. The gateway is the active partner during connection setup.

The gateway can communicate with S7-1200, S7-1500, S7-1500 Software Controllers and ET200SP devices and offers the following functionality:

- Receipt of spontaneous data from the PLC by using subscriptions
- Support of all access levels (from "No protection" to "Complete protection")
- Optimized data access

The gateway reads the configured data points exclusively via subscriptions from the S7Plus station.

Note

The maximum number of variables within the subscription is limited by the hardware used.

Parameters:

- **Active**
  A connection is only established to active stations. At least one data point with a destination must be assigned to the station.
- **Name**
  Enter a name for the profile.
- **IP address**
  IP address of the station interface

- **TLS**
  - Option enabled
    The data is transferred using the secure TLS method.
  - Option disabled
    The data is transferred unencrypted.

  Requirement for a TLS connection:
  - TIA Portal as of V17
  - S7-1500 firmware as of V2.9
  - S7-1200 firmware as of V4.5
- **Disable certificate validation**
  With this option, you disable the validation of the partner certificate.
  If this option is enabled, the client generally allows communication even if the certificate validation criteria are not met or if the server certificate is not in the list of trusted servers.
  If this option is disabled, the station checks the certificates of its partners.
- **Trusted servers**
  You can add a server certificate via the "Add" symbol. Select the suitable server certificate from the global certificate store via the drop-down list.
- **Password**
  Password of the communication partner for the selected protection level.
- **Keepalive interval (s)**
  Assign a value for monitoring the connection to the S7Plus station (seconds). If no further data for transfer is pending within the configured time after the data is sent, the device sends a keepalive frame to the S7Plus station.
  Permitted range: 0...255
  If you enter 0, the function is disabled.
  Default setting: 20 s
- **Min. subscription interval (ms)**
  Range of values: 100...10000
  Default setting: 100 ms

6.7.3 Modbus stations

The gateway and the Modbus station communicate over Modbus/TCP connections. The gateway is the active partner during connection setup.

Parameters:

- **RTU number**
  RTU number of the Modbus slave
  Range of values: 1...254
- **IP address**
  Address of the station interface.
  IPv4, IPv6

- **Port number**
  Port number of the interface of the station. Default: 502
  Range of values for Modbus station: 1...65535
- **Connection establishment attempts**
  Maximum number of attempts to establish a connection to a station.
  After reaching the configured number of attempts, no additional connection attempts are made until the gateway is restarted.
  Range of values: -1...32767
  With "-1" the number of connection attempts is unlimited.
- **Polling interval (ms)**
  Cycle time in milliseconds in which the gateway reads the data from the station.
  Range of values: 50...65535

  Note

  Time delay with larger amounts of data

  If you transfer large volumes of data, the actual cycle time may be longer than configured.

- **Connection establishment delay (ms)**
  Wait time (seconds) before a new connection attempt is made when the station cannot be reached or the connection is terminated.
  A wait time makes sense, for example, to wait for short-term network faults to be removed or restart of a station.
  Range of values: 1000...100000
- **Timeout (ms)**
  If the gateway does not receive a response from the station within the configured time (milliseconds), the connection is aborted and evaluated as faulty. The settings within the "Retries" and "Max. number of faulty responses" parameters determine whether the request is sent again.
  Range of values: 100...65535
- **Max. number of faulty responses**
  Maximum number of outstanding or faulty station responses across all data points.
  When reaching the maximum number, the gateway considers the station to be faulty and terminates the connection. When a connection is terminated, the gateway tries to re-establish the connection.
  Range of values: 1...32

- **Retries**
  Maximum number of retries of the station request per data point.
  If the gateway receives no response or a faulty response from the station during a timeout, the request of the individual data point is repeated until a change to the next data point takes place.
  The number of requests is limited by the retries set in the "Max. number of faulty responses" parameter. When the value set there is reached, an attempt is then made to re-establish the connection.
  Range of values: 0...10
- **Endianness**
  The setting only has effects on data types that consist of more than one word.
  You use this option to specify the order in which the data of the station read word by word is saved.
  - Big Endian
    The higher word 1 is saved first. (Modbus standard)
  - Little Endian
    The lower word 0 is saved first.

6.7.4 OPC UA stations

OPC UA stations

Parameters:

- **Active**
  A connection is only established to active stations. At least one data point must be assigned to the station.
- **Station name**
  To create a new station, enter a unique name in the text box.
- **Application URI**
  Unique URI of the station with the following default components:
  <Scheme (protocol)>:<Authority (station)>:<Path>
  Default:
  - urn:cc7-device:Siemens:OPCStation1@cc7-device
- **Application name**
  Name of the OPC UA application of the gateway. The application name is required to display the station at the server.
  Default:
  - OPCStation1@cc7-device
- **Server address**
  Set the IPv4/IPv6 address or the DNS name of the OPC UA server to which the station is to connect.

- **Port number**
  You can change the port number of the station here. As default port number 4840 is used, the standard TCP port for the OPC UA binary protocol. Permitted port numbers are as follows:
  – 1...65535
- **URL path**
  Optionally enter a URL path within the server address of the OPC UA client.
- **Service call timeout (ms)**
  Enter the required time in milliseconds. If there are no service calls to the lower-level OPC UA server after this period of time, the service calls are automatically interrupted.
  Range of values: 1000...60000
- **Connection timeout (ms)**
  Enter the required time in milliseconds. If no connection to the lower-level OPC UA server is established after this period of time, the connection is automatically terminated.
  Range of values: 1000...60000
- **Watchdog time (ms)**
  Enter the required time in milliseconds. If a connection fails, this is the time interval between connection checks or attempts to reconnect.
  Range of values: 1000...600000
- **Watchdog timeout (ms)**
  Enter the required time in milliseconds. If the connection to the lower-level OPC UA server is not successfully checked after this time, the check is automatically aborted.
  Range of values: 1000...60000
- **Discover**
  When using "Discover", a connection is established with the server address and port number specified above. If an OPC UA server is found, the application name, the application UI and the discovery URLs of the OPC UA server are displayed.
  Clicking on one of the discovery URLs displays the available endpoints of the OPC UA server connection. If one of the available endpoints with the desired encryption is selected and accepted with "Save", this security policy is set and the OPC UA server certificate is automatically saved, an optional URL path is set and the selected IP address is set.
  Note that an OPC UA client certificate must first be created or imported before an endpoint ! = None - None can be saved.

Note

Update interval of the data

The OPC UA client works with subscriptions instead of polling. This allows the load on the CPU side to be reduced as much as possible while still increasing the actuality of the data in the gateway. This is why it is not necessary to specify the polling cycle as is the case with S7 or Modbus stations.

6.7.4.1 OPC UA Security

OPC UA security

You can select certificates and keys from the global certificate store or create a self-signed certificate. After saving, the certificate and the private key are automatically entered in the appropriate fields. For information on managing certificates and keys, see section Certificate management (Page 156).

- **Security Policy**
  Select the required option in the table.
  The station supports the following options of the "SecurityPolicy":
  - None (not recommended)
  - Basic128Rsa15 (not recommended)
    Signing and 128-bit encryption
  - Basic256 (not recommended)
    Signing and 256-bit encryption
  - Basic256Sha256 (SecurityPolicy [B])
    Signing and 256-bit encryption (SHA-256)
  - Aes128_Sha256_RsaOaep
    Signing and 256-bit encryption
  - Aes256_Sha256_RsaPss
    Signing and 256-bit encryption

  The supplementary Conformance Units (Signing / Encryption) mean:
  - Sign
    The station only allows communication with signed frames.
  - Sign and encrypt
    The station only allows communication with signed and encrypted frames.
- **Trusted servers**
  - **No certificate validation**
    With this option you disable the validation of the partner certificates.
    If this option is enabled, the client generally allows communication even if the certificate validation criteria mentioned below are not met or if the server certificate is not available in the list of trusted servers.
    If this option is disabled, the station checks the certificates of its partners, except when "SecurityPolicy - None" is selected.
    For information on the check mechanisms, refer to the "Certificate validation" section below.
  - **Import server certificate**
    With this option, client certificates can be selected from the global certificate store.

Certificate validation

If the "No certificate validation" option is disabled, the UA server of the station checks the certificates of its communication partners, except if "SecurityPolicy - None" is configured.

If a partner certificate is invalid or is not trustworthy, communication is aborted. Communication is aborted in the following cases:

- The IP address of the communications partner is not identical to the IP address in its certificate.
- The use stored in the certificate (OPC UA client/server) differs from the function (OPC UA client/server) of the communications partner.
- The current time of the station is beyond the period of validity for the partner certificate.

Requirements for connection setup

The following requirements must be met to set up a connection regardless of the certificate validation:

- The application URI sent by the requesting station must match the URI of the station's server application.
- If the partner certificate is not trustworthy, the station must have stored at least one self-signed certificate of the partner.
- At least one authentication option is enabled (see below).

Partner certificates issued by multiple CAs (certificate chains) are not supported by the station.

6.7.4.2 User authentication

Use the option to set the access authorization of the OPC UA station:

- **Anonymous access**
  If you enable the option, the user name and password are grayed out. The station can access the OPC UA data without authentication.
- **Authentication via user name and password**
  If you activate the option, the text boxes for the user of the OPC UA station open. The station can only access the OPC UA data with user authentication.
- **User name**
  User name of the communication partner
- **Password**
  Password of the communication partner

The user data must be configured on the respective server.

6.8 OPC UA server

6.8.1 Configuration

Requirements

CPU variables

The process data that the gateway makes available to the OPC UA services originate from the connected process stations. The permissible memory areas of the different station types and the supported data types are described in section Data points (Page 136).

The data point names assigned during data point configuration are included in the NodeID of an item as part of the identifier, see section Properties of the OPC UA server (Page 96).

Note:
Where possible, read variables in data blocks block by block per DB to achieve a higher speed.

Security settings: Server certificate

If you enable the OPC UA server of the gateway, you must create or import a self-signed server certificate.

OPC UA server

- **Enable OPC UA server**
  Select the option to enable the OPC UA server function of the gateway.
- **Application URI**
  Unique OPC UA server URI of the gateway with the following preset components:
  <Scheme (Protocol)>:<Authority (Server)>:<Path>
  Default:
  - urn:cc7-device:Siemens:OpcUaServer@cc7-device

  The protocol part (urn) must not be changed; the other components can be configured.
- **Application name**
  Name of the OPC UA application of the gateway. The application name is required for display of the OPC UA server at the clients.
  Default:
  - OpcUaServer@cc7-device
- **Interface**
  Select the interface via which the OPC UA server is accessed:
  - All
  - Process interface (P2)
  - Cloud interface (P1)

- **Host name** (optional)
  Optional text box for a host name that can be used instead of the IP address of the UA endpoint of the gateway.
  If you do not want to use a host name, leave the box empty.
- **Port number**
  Here, you can change the port number of the server application. As default port number 4840 is used, the standard TCP port for the OPC UA binary protocol.
  Permitted port numbers are as follows: 1024...65535
- **URL path** (optional)
  Optionally enter a URL path within the server address of the OPC UA server.

Node manager

- **Locale ID**
  Enter a Locale ID for the OPC UA server, e.g. en-US.
  The ID is required when a string is mapped to a LocalizedText for Nodeset.
- **Namespace URI**
  Enter the address (Namespace URI) of the destination server.
  Default setting: urn:Siemens:OpcUaServer:CC7
- **Name of root directory**
  Enter a name for the directory.
  Default setting: CC7
- **Node ID of root directory**
  Change the NodeID of the CC7 folder;
  Default: ns=2;s=CC7; comprised of the namespace index of the active node manager (2) and a String identifier with the name of the root directory (CC7).
- **Min. publishing interval (ms)**
  Here you set the minimum publishing interval that the server application of the gateway should support. Lower values requested by OPC UA clients are not taken into account.
  The OPC UA server provides the clients with the UA data in the cycle of the publishing interval.
  Range of values: 100...10000 ms
  Default setting: 500 ms
- **Min. sampling interval (ms)**
  Here you set the minimum sampling interval that the server application of the gateway should support. Lower values requested by OPC UA clients are not taken into account.
  The OPC UA server of the gateway samples its internal process image with the sampling interval.
  You specify reading from the station with the polling cycle, see section Process access (Page 81).
  The default is suitable for most applications. A smaller sampling interval can be selected for reading fewer data points when the polling cycle is configured with a smaller value as well.
  Range of values: 100...10000 ms
  Default setting: 500 ms

6.8.1.1 OPC UA Security

Security mechanisms

The gateway supports the following security profiles in accordance with the OPC UA specification:

- **SecurityPolicy**
  It determines the signing and encryption of the transferred data.
- **UserToken**
  Enables authentication using certificates.
- **Authentication of the communications partners with user name and password**
  See section Authentication (Page 95) for more on this.

For information on the OPC UA profiles of the OPC Foundation, see:
Profiles (https://apps.opcfoundation.org/ProfileReporting)

- **Self-signed certificate**
  Click the "Create" button to create a self-signed certificate. Required fields are filled out with the necessary parameters. After saving, the certificate and the private key are automatically entered in the following fields and saved in the global certificate store.
- **Server certificate**
  Select a server certificate from the global certificate store via the drop-down list.
- **Private key**
  Select a private server key from the global certificate store via the drop-down list.
- **No certificate validation**
  With this option you disable the validation of the partner certificates.
  When this option is enabled, the gateway generally permits communication even if the criteria of the certificate validation listed below are not met or when the client certificate is not included in the list of trusted clients.
  When the option is disabled, the gateway validates the certificates of its partners, except if "SecurityPolicy - None" is selected.
  For information on the check mechanisms, refer to the "Certificate validation" section below.
- **Trusted clients**
  With this option, you can select client certificates from the global certificate store.

Certificate validation

The UA server of the gateway checks the certificates of its communication partners when the "No certificate validation" option is disabled, except if "SecurityPolicy - None" is configured.

If a partner certificate is invalid or is not trustworthy, communication is aborted.
Communication is aborted in the following cases:

- The IP address of the communications partner is not identical to the IP address in its certificate.
- The use stored in the certificate (OPC UA client/server) differs from the function (OPC UA client/server) of the communications partner.
- The current time on the gateway is outside the period of validity of the partner certificate.

Requirements for connection setup

The following requirements must be met to set up a connection regardless of the certificate validation:

- The application URI sent by the requesting client must match the URI of the server application of the gateway.
- If the partner certificate is not trustworthy, the gateway must at least have stored a self-signed certificate of the partner.
- At least one authentication option is enabled (see below).

The gateway does not support partner certificates that were issued by multiple CAs (certificate chains).

6.8.1.2 Authentication

User authentication

You use the two options to set the access authorization of the communication partners (clients) to the OPC UA data of the gateway. Select one or both (parallel operation possible) options.

- **Enable anonymous access**
  Clients can access the OPC UA data without user authentication when this option is activated.
- **Authentication via user name and password**
  Clients can only access the OPC UA data with user authentication when this function is activated.
- **Add user**
  With enabled "Authentication via user name and password" option, you use this button to open the text boxes for a new user.
- **User name**
  User name of the communication partner
- **Password**
  Password of the communication partner

The user data must be configured for the respective client.

Protection against brute force attacks

- **Number of failed login attempts**
  Number of failed login attempts until the IP address is locked.
  Range of values: 1...100
  Default setting: 3
- **Monitoring time of failed login attempts (s)**
  Period of time in which the configured number of failed attempts is monitored.
  Range of values: 1...3600
  Default setting: 60 s
- **Block time (s)**
  Duration for which the WBM is locked for the IP address.
  Range of values: 1...3600
  Default setting: 60 s

6.8.1.3 Properties of the OPC UA server

Identification and addressing

The following addressing and identification features of the OPC UA server of the gateway apply.

- Application name, Application URI, Server URL, Port number of the application:
  - See section Configuration (Page 92).
- Namespace of the gateway data points:
  - CC7
- Namespace URI:
  - urn:Siemens:OpcUaServer:CC7
- NodeID - Identifier:
  The identifier of the NodeIDs of the data points of the "CC7" namespace is formed by the server application of the gateway from the name of the CPU and perhaps the data block, and the structure and the data point name:
  - *<CPU name>.<DB name>__<Data point name>*
- Supported sampling intervals
  100, 250, 500, 1000, 2000, 5000, 10000 ms

Subscriptions

For the number of subscriptions supported by the gateway as OPC UA server for MonitoredItems, see section Configuration limits - communication (Page 25).

The data management of the subscriptions is stored in the RAM of the gateway.

If there is power down, all data and connection information of subscriptions is lost.
After restarting the server, the client needs to re-establish the connection and set up the subscriptions again.

Deadband

When monitoring items in the "DataChangeFilter", the OPC UA server of the gateway uses the filter "AbsoluteDeadband".

6.8.2 Nodeset

Nodeset files

The OPC Foundation has specified a standard format based on XML for writing information models. This means a client can receive the information model of an OPC UA server beforehand, or information models can be loaded to an OPC UA server. A file in this format is called a "Nodeset file" because it describes an information model as a set of nodes.

All variables, regardless of the source (process stations), have a defined value and a defined NodeID.

Creating an OPC UA export file

You can create Nodeset files either manually or with OPC-compliant software.

Siemens offers the following software to create Nodeset files:

- With STEP 7 (TIA Portal) you can export the standard SIMATIC information model to an OPC UA XML file (Nodeset file); including all PLC tags, NodeIDs and methods that you have enabled for OPC UA.
- As of SiOME V2.7.2, CC7-specific XML files can be created and these XML files can be imported into CC7 as of V2.2.
  The XML files contain:
  - Definition of the S7 / S7-PB process stations
  - Definition of data points
  - Mapping of data points with the elements of OPC UA nodeset

  After the XML file is imported from SiOME, the OPC UA server can be used with the desired nodeset files and data points.
  You can find a description of the creation of XML files on the SiOME SIOS pages or in the SiOME manual:
  Link: (https://support.industry.siemens.com/cs/ww/en/view/109755133)

Import OPC UA Nodeset

During import, the process variables and the variables in the loaded Nodeset file are being mapped. Thus, the CC7 presents the preferred standardized OPC UA values on its own OPC UA server and not its own structure.

- **Nodeset file**
  - Click the "Browse" button.
    The browser for browsing your PC file system opens.
  - Select the desired XML file and click "Open".
    The file name is displayed in the output field of the WBM.
  - If you want to use the file, click "Upload".
  - If the wrong file is selected, click the "Delete" symbol.
- **Active**
  If enabled, CC7 uses the structure and data of the loaded nodeset file and not its own process data.
- **Parsing**
  Parsing takes place automatically when a new nodeset file is loaded.
  Result: The nodeset file is read and the user interface of the WBM is split into two areas:
  - On the left, you can see the loaded nodeset file with the associated variables. You can browse individual folders or variables.
  - On the right, all process stations of the CC7 are listed. In the folders of the process station, all data points that are assigned to the destination "OPC" are displayed.

Import SiOME OPC UA nodeset

If you import an XML file with the "Cloud Connect 7" layout from SiOME, a specific import page is displayed.

After the import, the file name is displayed and the following information is shown under "Nodeset file generator":

- **Product**
  SiOME
- **Edition**
  SiOME edition used.
- **Version**
  SiOME version used.
- **Hash**
  Unique checksum of the XML file.

"S7 stations" table

The "S7 stations" table contains an overview of the process stations and data points from the XML file.

Each station is shown as individual list entry.

- **Name**
  Name of the station from the XML file.
- **Address**
  Address of the station from the XML file.
- **TSAP**
  TSAPs of the station from the XML file.
- **Polling cycle (ms)**
  Configured polling cycle for the station.
- **Data points**
  Number of data points configured in XML for the station.
- **Error**
  Number of errors found when parsing the station definition.

Import

The following happens when you click "Import":

- The named stations are created
- Existing stations are deleted
- The data points are created and mapped with the defined SiOME nodeset

CC7 can thus be used directly as desired OPC UA server with the desired data.

The XML can then be used/edited and mapped like an OPC UA nodeset in the past.

6.8.2.1 Mapping

Mapping variables

During mapping, the process data of the CC7 stations is assigned to the variables of the nodeset file. A variable of the CC7 station can be assigned to multiple variables of the nodeset file.

To that end, drag the data points of the CC7 stations in the right area to the corresponding Nodeset XML variables in the left area.

Result:

- An assigned variable is marked in bold in the nodeset file followed by the corresponding CC7 data point.
- The number of links is shown on the CC7 page behind the assigned variable.
- The full NodeID is shown in the tooltip if you move over the data point name with the mouse.
- With the black cross icon behind the data point, you can remove the connection again.
- Any data points of the XML that are not assigned are transferred with the QualityCode "BadNotImplemented" to the CC7 OPC UA server.

6.8.2.2 Casting

Converting variables (Casting)

When assigning the variables to the OPC UA XML data points, it is possible to convert the access and/or the data type of the CC7 process tags.

CC7 data points with the OPC authorization "ReadWrite" can be converted into XML data points "Read", "Write" and "ReadWrite".

However, it is not possible to convert a CC7 variable "Read" into an XML variable "ReadWrite".

OPC UA XML data points	**CC7 process tags**		
Access right	Read	Write	ReadWrite
Read	x	-	x
Write	-	x	x
ReadWrite	-	-	x

Overview by OPC UA data types

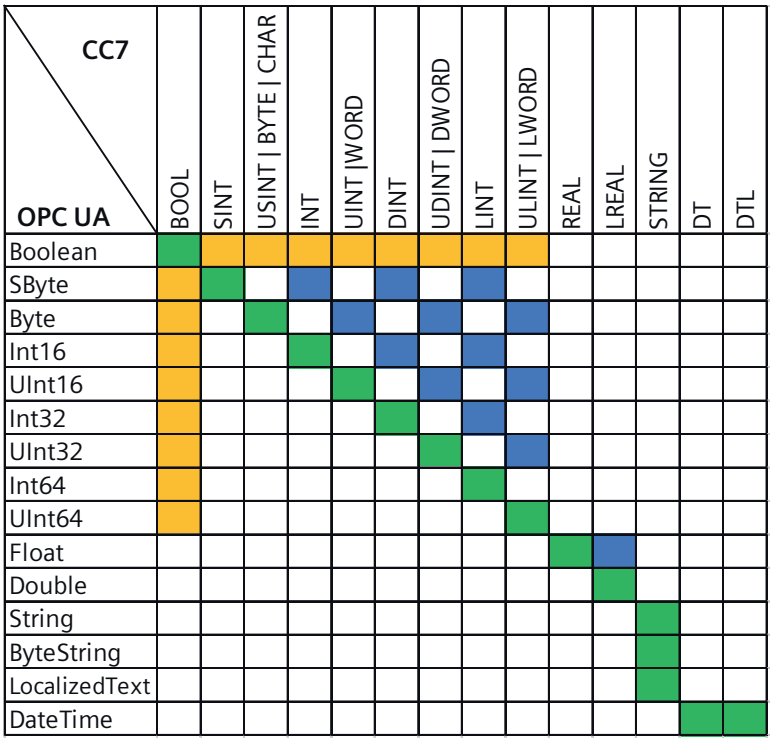
The graphics below provide an overview of which incoming and outgoing data types of the CC7 process tags can be converted into which incoming and outgoing OPC UA XML data points, depending on the OPC access right. The fields have the following meaning:

Field	**Description**
CC7	CC7 process tags
OPC UA	OPC UA XML data points / Nodeset
	Assignment by data types
	Conversion of data types For "ReadWrite", the data types must match exactly, upcasting or downcasting as with "Read" or "Write" is not possible.
	The variable can be assigned to an XML Bool variable. In this case, the following values of the process station correspond to the following XML Bool variables on the OPC UA server: Value "0" corresponds to the value "false" Value "!= 0" corresponds to the value "true"
	Conversion of strings Each data point can be converted into a string and thus shown as a string.

XML data "Read"

CC7 / OPC UA	BOOL	SINT	USINT | BYTE | CHAR	INT	UINT |WORD	DINT	UDINT | DWORD	LINT	ULINT | LWORD	REAL	LREAL	STRING	DT	DTL
Boolean	■	■	■	■	■	■	■	■	■					
SByte	■	■												
Byte	■		■											
Int16	■	■		■										
UInt16	■		■		■									
Int32	■	■		■		■								
UInt32	■		■		■		■							
Int64	■	■		■		■		■						
UInt64	■		■		■		■		■					
Float										■				
Double										■	■			
String	■	■	■	■	■	■	■	■	■	■	■	■	■	■
ByteString	■	■	■	■	■	■	■	■	■	■	■	■	■	■
LocalizedText	■	■	■	■	■	■	■	■	■	■	■	■	■	■
DateTime													■	■

XML data "Write"



CC7 / OPC UA	BOOL	SINT	USINT | BYTE | CHAR	INT	UINT |WORD	DINT	UDINT | DWORD	LINT	ULINT | LWORD	REAL	LREAL	STRING	DT	DTL
Boolean	■													
SByte		■		■		■		■						
Byte			■		■		■		■					
Int16				■		■		■						
UInt16					■		■		■					
Int32						■		■						
UInt32							■		■					
Int64								■						
UInt64									■					
Float										■	■			
Double											■			
String												■		
ByteString												■		
LocalizedText												■		
DateTime													■	■

XML data "ReadWrite"

CC7 / OPC UA	BOOL	SINT	USINT | BYTE | CHAR	INT	UINT |WORD	DINT	UDINT | DWORD	LINT	ULINT | LWORD	REAL	LREAL	STRING	DT	DTL
Boolean	■													
SByte		■												
Byte			■											
Int16				■										
UInt16					■									
Int32						■								
UInt32							■							
Int64								■						
UInt64									■					
Float										■				
Double											■			
String												■		
ByteString												■		
LocalizedText												■		
DateTime													■	■

6.8.3 Events

This section describes how you configure the "CC7 OPC UA server" as "Event subscription server". The configuration was implemented according to:

Link: (https://profiles.opcfoundation.org/profile/1483)

Requirement for user-defined events

A nodeset file is uploaded under "OPC UA server" > "Nodeset".

The two predefined events "BaseEventType" and "SystemEventType" can be used without an uploaded nodeset file.

6.8.3.1 Import

The OPC "EventTypes" from the uploaded nodeset file are filtered and shown as browsable.

1. Select the desired "Event Types" with <Ctrl> + left mouse button.
2. Click "Import".
   Result: The selected "Event Types" are transferred to the "Event types" tab.

6.8.3.2 Event types

Overview of the imported event types.

- **Delete**
  All selected event types are deleted.
- **NodeID**
  Display of the NodeID of the imported event type.
- **Name**
  Display of the imported event type.

6.8.3.3 Events

The overview page lists the created events and their properties.

You can edit the displayed properties directly on the overview page.

- **Create**
  Clicking the button opens a new page on which you set the parameters of the new event. Clicking the "Save" button applies the settings and the new event appears in the table on the overview page.
- **Delete**
  Clicking the button deletes the selected event.

Parameters

- **Event type**
  Select the desired event type via the drop-down list.
- **Name**
  Enter a name for the event.
- **NodeID of the source**
  Define the NodeID of the source for the OPC event.
  Default: "i=2253"
- **NodeName of the source**
  Define a node name of the source for the OPC event.
  Default: "Server"

- **Message**
  Define a desired message for the event.
- **Severity**
  Define the severity of the event.
  Range of values: 1 ... 65535

Severity	Range of values
HIGH	801 ... 1000
MEDIUM HIGH	601 ... 800
MEDIUM	401 ... 600
MEDIUM LOW	201 ... 400
LOW	1 ... 200

You will find more information on the page:
Link: (https://reference.opcfoundation.org/v104/Core/docs/Part5/6.4.2)

6.8.3.4 Data point assignment

In this tab, you assign the configured data points to a previously created event. Data points can be linked with multiple events.

Data point assignment

All configured events are shown on the left, and all configured OPC data points of the selected station are shown on the right.
Assignment is performed using drag-and-drop. Select the data points and drag them to the desired topic, keeping the left mouse button pressed.

To ensure that the event is triggered correctly, assign a suitable trigger to the data points used in the data point configuration. Alternatively, use the quality change of a data point as trigger.

Individual assignment

Assign each data point in the data point table individually to an event.
For assignment rules, refer to the *"Read" XML data* table in section Casting (Page 100).

The number of links is shown on the CC7 page behind the assigned variable. You can remove the connection again with the black cross icon behind the data point.

Event trigger

An event trigger is automatically created for each event, which you can also use to trigger the event. Because the event trigger is not linked to any fixed data type, you can assign it to all data points.

6.9 Cloud configuration

6.9.1 Notes on data structuring and configuration

WARNING

Writing values to outputs

When referencing to outputs with write access, note that the values are written immediately to the outputs of the CPU without first being processed by the user program.

Writing values has a direct influence on the process.

Data structures

Depending on the cloud provider, the data is structured differently for transfer to the broker:

- AWS / Azure / IBM Cloud
  - Topics
    A topic is the channel for the transfer of values of one or more data points.
    You can create several topics.
    No groups can be configured.
- MindConnect IoT Extension (outdated) / Other cloud
  - Groups
    A group can contain one or multiple data points.
    You can create one or more groups.
  - Topic
    You can assign different topics to the groups.
    MindConnect IoT Extension: In the default setting, the groups are assigned to the standard topic "s/us" of the MindConnect IoT Extension.

Structure of the topic names

Because the requirements on the format of the topics can be different depending on the receiver (broker, cloud), a topic name is made up of different parts.

Prefix and suffix generally apply to all topics.

Prefix and suffix are not relevant for groups.

Structure of the topic names:

- **Prefix**
  The prefix of the name is an addressing and structuring string.
- **Topic name**
  - For the cloud provider MindConnect IoT Extension, the topic name "s/us" is a fixed name.
  - For all other cloud providers, the topic names can be configured.
    By inserting multiple name components separated by forward slashes (/), you can create hierarchy levels for later evaluation by the subscriber.
- **Suffix**
  The suffix of the name is a format string.

Name assignment for topics and groups

Because the topic or group names are incorporated in the data management structure of the broker, later assignment and evaluation of the published data is facilitated if the names refer to the process data of the stations.

Example:

You would like to name a group or topic "Motor5" and assign the name "Station1" to the station. In this case, the following entry, for example, would be suitable for the topic name or group name:

Station1/Motor5

Configuration rules

Observe the following rules for configuration:

- Topic name
  The name of a topic must be unique within a cloud application.
  This applies to all participating publishers and subscribers.
- Data point name
  The name of a data point must be unique within a topic.

Note

Consistency check of parameters for Publisher and Subscriber

If the gateway as a subscriber receives data from a publisher during runtime, the subscriber checks the following parameters supplied by the publisher in the user data for each value received:

- Topic name
- Data point name
- Data type

If these three parameters of the publisher are identical with the parameters configured in the subscriber and if the quality code of the message is "GOOD", the subscriber writes the received data into the data block of its CPU.

If these three publisher parameters do not match the parameters configured in the subscriber, the subscriber discards the data.

The station name of a publisher is not evaluated by the gateway as a subscriber.

Recommendations for configuration

When transferring data in a hierarchically structured system, it is generally advisable to name the components according to this hierarchical structure.

Example for the name of a data point to be transferred:
"Plant_1/Unit_1/Aggregate_1/DB_1_Signal_1".

For access to the process data of an S7 station, the gateway can directly access inputs and outputs or tags of the CPU.

Within a cloud application, individual publishers can publish data for multiple subscribers. Individual subscribers can subscribe to data from multiple publishers.

For better clarity of the data and to reduce the possibility of identical names, the following procedure is recommended for configuration:

- Data point name / DB number
  Use the number of the data block (DB) that the data point accesses as part of the data point name.
- Publisher
  Integrate the station name as part of the data point name, for example, as prefix. This will result in unique data point names.
- Subscriber
  Create a separate DB for each publisher in the assigned CPU.

Configuration error - Diagnostic messages

If you experience different behavior than expected after commissioning the gateway, use the diagnostic messages of the gateway that you can find in the WBM under "Maintenance > Diagnostics".

6.9.2 Profile

The settings that you configure for the cloud access of the gateway are stored in a profile. This will make it easier to use the device for different scenarios. Individual settings for different scenarios can thus be summarized in different profiles without the need to change the configuration when you switch the cloud.

For the preset cloud providers, certain parameters are already stored according to the different requirements of the respective cloud.

Via the tabs, you switch between the overview page of the MQTT profiles and the HTTP profiles. All saved profiles are shown in the overview table. You can edit the displayed information directly on the overview page.

Add/edit profile

Create at least one profile in which you save your settings for cloud access. You can create up to 10 profiles.

Settings

- **Active**
  Enables the selected profile for use in productive operation.
- **Name**
  Enter a name for the profile.
- **Cloud provider**
  Select your service provider.
  Selecting the cloud provider also affects the parameters of the topic configuration; see also section Publish groups (Page 114).
  By selecting the cloud provider, you determine whether topics or groups are configured for the data transmission:
  - AWS / Azure / IBM Cloud
    You can create several topics. A topic can contain multiple data points.
  - MindConnect IoT Extension
    You can create several groups. A group can contain multiple data points.
    A group corresponds to the "Series" structure feature in the IoT Extension.
    In the default setting, all groups are assigned to the preset standard topic "s/us".

    Note

    Name change of the assigned topic "s/us"

    If you give a different name to the assigned topic in the configuration, note that it may not be possible for the data to be evaluated by the IoT Extension.

  - Other Cloud
    You can create several groups. A group can contain multiple data points.
    In the default setting, all groups are assigned to a topic. You can also assign different groups to different topics.
    If you do not wish to use groups, create only a standard group and delete the entry "<GROUP_NAME>" in the payload editor.

You configure access of the device to the cloud in the additional tabs of this page.

6.9.2.1 MQTT configuration

Add MQTT profile

- **Active**
  Enable the profile for use in productive operation.
- **Name**
  Enter a name for the profile.
- **Cloud provider**
  Select a cloud provider from the drop-down list.
- **Address**
  Enter the IP address or the host name of the broker.
  This information is provided by your service provider.
- **Port number**
  Enter the port number name of the broker.

MQTT security

- **TLS**
  - Option enabled
    The data is transferred using the secure TLS method. The default port for encrypted transmission is 8883.
  - Option disabled
    The data is transferred unencrypted. The default port for unencrypted transmission is 1883.
- **TLS version**
  From the drop-down list, select the TLS protocol version you wish to use that is also supported by the broker.
- **Only use secure ciphers**
  Here you can allow communication with devices that use processes for encrypted communication that are no longer recommended due to known vulnerabilities.
  - Option enabled
    Enables communication only with devices that support recommended encryption methods (secure ciphers).
  - Option disabled
    Enables communication also with devices that support encryption methods that are no longer recommended (legacy ciphers).
- **Client certificate**
  Select a suitable certificate from the global certificate store via the drop-down list**.**
- **Client private key**
  Select the suitable private key from the global certificate store via the drop-down list.
- **Server certificates**
  You can add a server certificate via the Add symbol. Select the suitable server certificate from the global certificate store via the drop-down list.

- **Authentication via user name and password**
  - Select the option if you want to use a connection setup with authentication. Authentication takes place via user name and password.
  - When the option is disabled, the connection is established anonymously.
- **User name**
  Enter the user name that was assigned by your service provider or that you defined.
- **Password**
  Enter the password assigned by your service provider or that you defined.

MQTT settings

- **MQTT version**
  Select the protocol version you are using.
- **Client ID**
  Enter the client ID of the device that was assigned by your service provider or that you defined.
- **Clean session**
  - When the option is enabled, the session information is deleted when the connection is terminated.
  - When the option is disabled, the session information is retained when the connection is terminated.
- **Keepalive interval (s)**
  Assign a value for monitoring the connection to the broker (seconds). If no further data for transfer to the broker is pending within the configured time after the data is sent, the device sends a keepalive frame to the broker.
  Permitted range: 0 or 5...65535
  With 0 (zero), the maximum value (65535 seconds) is used.
  Default setting: 10
- **Topic prefix**
  Assign an optional prefix in front of the topic name.
  By using identical prefix components, you can group different topics in topic levels.
  The prefix can also contain components that are necessary for the recipient of the topic as component of the topic name.
- **Topic suffix**
  Assign an optional suffix after the topic name.
  By using identical suffix components, you can earmark different topics for the same recipient.
  The suffix can also contain components that are necessary for the recipient.

Last will / testament

- **Last will / testament**
  - When the option is enabled, the functions "Last will" and "Testament" are released.
  - When the option is disabled, the use of both functions is disabled.

  The functions have the following meaning:

  - Last will
    If the connection between device and broker is terminated, a message can be sent to the subscribers.
    As soon as the broker (server) detects that the connection to the device (client) was terminated, it sends a message (testament) to all subscribers that have registered for this topic on the broker.
  - Testament
    The testament is the content of the message that is sent to the subscribers registered on the broker for this topic when the connection is terminated.
    The testament message is saved on the broker.
- **Last will topic**
  Enter the name of the topic that transfers the testament here.
  You configure the additional parameters of the topic in the topic editor, see section Publish groups (Page 114).
- **Testament**
  Here you enter the content of the message to be transferred.
  Max. number of characters: 65535
- **QoS - Last will**
  From the drop-down list, select the Quality of Service with which the Last will topic is transferred.
  - QoS 0 / QoS 1 / QoS 2

  For information on the meaning of the three options, see section Publish groups (Page 114).
- **Retain- Last will**
  - If the option is enabled, the testament is sent with the "Retain" flag to the broker.
    The testament is enabled for permanent storage in the broker.
    If the connection between the device and the broker is terminated, the broker publishes the testament for each registered subscriber.
    If a subscriber does not have a connection to the broker when the connection between device and broker is terminated, the "testament" for the subscriber is lost. When the connection to the broker is reestablished, the subscriber first receives the "testament" with the "Retain" flag.
    For more information on the flag "Retain", refer to section Publish groups (Page 114).
  - If the option is disabled, the testament is not stored permanently in the broker.

Device parameters

The parameter group is only relevant for the connection to MindConnect IoT Extension. The fields can only be edited if MindConnect IoT Extension is selected as cloud provider.

After the establishment of a connection between the device and MindConnect IoT Extension, the two parameters are used for the identification of your device and for the exchange of key material during the Onboarding process.

- **Device name**
  Assign the name under which the device is registered for the Onboarding process.
  The Device name is displayed in MindConnect IoT Extension at the following location:
  Device > Device profile > "NAME"
- **Device type**
  The parameter is required in MindConnect IoT Extension to determine the device type. Enter the following string:
  - c8y_MQTTDevice

  The Device type is displayed in MindConnect IoT Extension at the following location:
  Device > Device profile > "Type"

You can find additional information on setting up the IoT Extension on the Internet at:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/25621)

6.9.2.2 HTTP profiles

Add HTTP profile

- **HTTP active**
  Enable the profile for use for productive operation.
- **Name**
  Enter a name for the profile.
- **Cloud provider**
  Select a cloud provider from the drop-down list.
- **Address**
  Enter the IP address or the host name of the server.
- **HTTP port**
  Enter the port number of the server.

TLS

- **TLS**
  - Option enabled
    The data is transferred using the secure TLS protocol. The default port for encrypted transmission is 443.
  - Option disabled
    The data is transferred unencrypted. The default port for unencrypted transmission is 80.
- **TLS version**
  From the drop-down list, select the TLS protocol version you wish to use that is also supported by the server.

- **Only use secure ciphers**
  Here you can allow communication with devices that use processes for encrypted communication that are no longer recommended due to known vulnerabilities.
  - Option enabled
    Enables communication only with devices that support recommended encryption methods (Secure Ciphers).
  - Option disabled
    Enables communication also with devices that support encryption methods that are no longer recommended (Legacy-Cipher).
- **Certificate**
  Select a certificate from the global certificate store via the drop-down list.
- **Private key**
  Select a key from the global certificate store via the drop-down list.
- **Trusted server**
  You can add a server certificate via the Add symbol. Select a trusted server via the drop-down list.

HTTP settings

- **HTTP version**
  Select the required protocol version.
- **Target path prefix**
- **Target path suffix**

6.9.3 Publisher

Overview

In this tab, you create the topics or groups for transfer to the broker/HTTP server for all enabled profiles. For configuration of the profile, refer to the section Profile (Page 109).

You can find information on structuring the data in topics or groups for different cloud providers and on configuring the topic names in section Notes on data structuring and configuration (Page 106).

6.9.3.1 Publish groups

Add topic / Add group

- **Select profile**
  Select one of the previously created profiles from the drop-down list.

All configured groups/topics for the selected topic are displayed.

- **Add**
  A new editable topic is added to the table.
  Maximum number of publish and subscriber topics or groups
  CC712: 500
  CC716: 3500
- **Copy**
  The selected topics are copied and added to the table again.
- **Delete**
  All selected topics are deleted.

Topic/group table

You can see the created topics or groups in the table and configure their properties.

You can sort the display alphabetically by name or topic by clicking on the icon next to the name in the table header.

- **Name**
  The names of the configured groups are displayed.
- **Topic**
  - ⇒ Validity: MindConnect IoT Extension
    The preset topic name "s/us" is inserted.
    Use this default name when connecting to Insights Hub via IoT Extension.
    Adapt the name when connecting to another cloud according to the cloud provider's specifications.
  - ⇒ Validity: AWS / Azure / IBM Cloud / Other cloud
    Enter the name of the topic.
  - Validity: HTTP
    Specify the part of the URL following <server name>:<port>.

  The configured name with all components is shown in the tooltip if you move over the topic with the mouse.

- **QoS**
  Only when profile "MQTT" is selected.
  You use the "Quality of Service" parameter to specify the transfer performance of the messages for this topic:
  - QoS 0
    Transfer no more than once
    The device sends the topic once to the broker. The device does not expect an acknowledgment. If the topic is not received by the broker, it is lost.
  - QoS 1
    Transfer at least once
    The device sends the topic to the broker until it receives a PUBACK packet as acknowledgment from the broker.
  - QoS 2
    Transfer exactly once
    The device sends the topic and waits until it receives the two-step acknowledgment from the broker as specified.
    This version represents the highest level of quality, but it is also associated with the highest administrative burden for the client as well as the server.

  When a connection is aborted, the data frames are buffered for QoS 1 and QoS 2. See also the section "Connection abort" below.
- **Retain**
  Only when profile "MQTT" is selected.
  From topics/groups with the "Retain" flag, the broker always saves the last message.
  When a subscriber subscribes to a new topic or when the connection with a subscriber returns after being terminated, the broker sends the last message on each topic with Retain flag to the subscriber.
  You can set the Retain flag for all or for individual topics/groups (option enabled in single row).
  The higher-level check box activates the function for all topics/groups of the table.
  Please note:
  If you want to revoke the sending of the last message by the broker to newly connected subscribers after starting productive operation, you cannot accomplish this by retroactively disabling the Retain flag on the topic. The broker will still send the last valid message of the publisher to newly connected subscribers. To prevent the broker from sending these messages, send an empty message (0 bytes) to the broker, for example.

- **Payload format**
  Shows the currently selected payload format.
  You use the first button to open the Payload editor to specify the format of the transferred payload. For a description, see section Payload format (Page 120).
  Use the second button to open the payload preview to check and display the specified payload with the desired format. If a new payload format is select, the page with the publish groups must be saved first. Only then is the preview adapted to the newly selected format.

  Note

  Payload format of older firmware versions cannot be changed

  A payload format of older firmware versions is displayed as obsolete. Although it is still supported by the current firmware version for runtime, it cannot be changed without changing to a current format.

  Future firmware versions will no longer support obsolete formats and a corresponding configuration can then no longer be loaded.

- **Verb**
  Only when profile "HTTP" is selected.
  Select one of the HTTP methods: POST, PUT, PATCH, DELETE

- **HTTP header**
  Only when profile "HTTP" is selected.
  Append the HTTP header required by the HTTP server.
  For sending payload data in JSON format, for example, the "Content-Type" HTTP header should be supplemented by the value "application/json".
  The module supplements the "Content-Length" HTTP header internally.

- **Trigger**
  You use the triggers to specify the conditions that initiate the transfer of the value saved in the device to the broker.
  One trigger can be selected per topic. The following trigger classes can be configured:
  Time trigger
  - Cyclic
    The value of the data point is transferred cyclically. Range of values:
    100 .. 100 000 000 ms
    1 .. 100 000 s
    1 .. 1666 min
    1 .. 27 h
  - Once daily
    The value is transferred once a day at the configured time.
  - Once weekly
    The value is transferred once a week.
  - Once monthly
    The value is transferred once a month.
    If a month has fewer days than the day specified in the configuration, the value of the data point is transferred at the end of the month.

  Input trigger
  - Digital Input
    Only appears in the drop-down list when the digital input was defined as trigger in the interface configuration, see section DI/DO (CC716) (Page 80).
    Transfer once upon edge change at the digital input.
    Alternatively with edge change 1 → 0 or 0 → 1
  - Cloud connection
    Transfer upon edge change of the cloud connection status.
- **Message buffering**
  In the event of a connection loss between the gateway and the cloud server, the gateway stores incoming messages in its message store up to the number entered in the "Message buffering" field. The total size of the message store can be distributed to the individual topics or groups. When the setting is saved, the system checks whether the configured number for this topic or group still fits in the message store. The required message memory space also depends on the number of data points assigned to the topic and/or group and their maximum data width. The collection of values also has an effect on the required space in the message memory.
  The message memory works chronologically, i.e. the oldest messages are sent first (FIFO principle). As soon as the configured buffer locations for a topic or group are full, the oldest message is overwritten.

- **Collect**
  Collects values that are triggered due to fulfilled trigger conditions (value or time trigger). As soon as the specified number of values has been reached, they are collected in a message and sent to the broker.
  Alternatively, the collected values can be displayed in the payload as follows:
  - As Array, separated by commas in a list.
  - As collected individual values, each with quality status and time stamp. Use the `TIME_SERIES` code key within the payload format for this purpose.
- **Delete**
  By clicking the button, the topics of the selected rows are deleted. If no rows are selected, you are asked whether you want to delete all topics.

Note

Delete

Note that if you accidentally delete a topic or a group, you cannot undo the deletion.

Data point assignment

On this page, you assign the configured data points to a previously created topic or a group. For a description, see section Data point assignment (Page 131).

You assign the transferred payload to the topics in the data point configuration.

6.9.3.2 Publish settings

Recommendations for configuration

- **Select profile**
  Select one of the previously created profiles from the drop-down list.
- **Time stamp format**
  Setting for the format in which the `PUBLISH_TIMESTAMP` and `SOURCE_TIMESTAMP` placeholders of the topics are transferred.
  - **ISO 8601 String**
    Specification in format 2021-10-26T10:35:06.248716825+00:00
  - **Unix time**
    Specification as Unix value, e.g. 1635238284.356
  - **Custom**
    Definition of a user-defined time stamp format. The format is entered in the text box below

- **Time stamp string**
  Text box for entering a user-defined time stamp. Only possible when the "Custom" time stamp format is selected.
  The following placeholders can be used:
  Link: (https://cplusplus.com/reference/ctime/strftime/)
  The following placeholders are defined in addition:

Placeholder	Appearance
{{ms}}	Second portion with three decimal places (milli-seconds)
{{us}}	Second portion with six decimal places (micro-seconds)
{{ns}}	Second portion with nine decimal places (nano-seconds)

  When "ISO 8601 String" is selected, the text box is grayed out and set with the format "%FT%T.{{ns}}+00:00"

- **Quality code format**
  Setting for the format and value with which the `QUALITY_CODE` placeholder is to be transferred.
  Defaults are:
  Good = String "GOOD"
  Bad = String "BAD"

- **Boolean value format**
  Setting for the format and value with which the `VALUE` placeholder is to be transferred for BOOL variables.
  Defaults are:
  True = Integer 1
  False = Integer 0

Note

Check user-defined payload formats after a firmware update

After the firmware update, the status ""GOOD"" is output instead of "GOOD", as was previously the case, for user-defined payload formats that use the "`{{QUALITY_CODE}}`" placeholder.

Check whether the user-defined payload formats have the correct JSON syntax after the update and adapt it if necessary.

When using the CloudConnect 7 templates for the payload formats, the data is converted and can be used without any adaptations.

6.9.3.3 Payload format

Because different cloud systems expect different payload formats, you must adapt the format to the requirements of the processing systems.

On this page, you will find syntax templates. You can select the appropriate one and adapt it to the requirements of the cloud system, if needed. You change the code in the "Payload format" text box.

Automatic data point assignment to the payload format

If the code meets the requirements, do not change it. Thus, all data points assigned to the topic/group are always prepared according to the selected template before sending. This means that if you remove already assigned data points from this topic/group or assign further data points, the payload always contains the finally assigned data points.

Manual data point assignment to the payload format

If you change the payload format in the text box, the dialog selects the "User defined" template. This defines the content and format of the payload and the gateway does not change this format or the assignment of the data points afterwards. Not even if you remove data points already assigned from the topic or group or assign additional data points to the topic. Explicit references to data points that are not assigned to the topic or group are shown as empty strings in the payload.

The UTF-8 character encoding is used for formatting the payload.

Payload templates

The most important information is listed here and can be edited directly. For the respective explanations of the parameters, the following pages are available when new stations are created.

- **Add**
  Redirects to a new page on which payload templates can be created.
- **Delete**
  The selected rows payload templates are deleted. Default profiles managed by CC7 cannot be deleted.

Syntax templates

The following templates are available:

- **Add**
  Own payload templates can be created via the "Add" icon.
- **JSON generic v2 / JSON specific v2**
  - The syntax of the JSON format according to ECMA-404 and ISO/IEC 21778:2017 is used.
  - The values are not used as string but as native data types and, therefore, can transfer data points of the type "Array".
- **JSON generic v3 / JSON specific v3**
  - The syntax of the JSON format according to ECMA-404 and ISO/IEC 21778:2017 is used.
  - The values are not used as string but as native data types and, therefore, can transfer data points of the type "Array".
  - When the "Collect" option is enabled, all data points are transferred together in a topic over the "TIME_SERIES" loop.

  All templates are suitable for connection to:
  - AWS (Amazon) / IoT Core
  - Azure (Microsoft) / IoT Hub
  - IBM Cloud (IBM) / Watson IoT Platform

- **XML generic v1 / XML specific v1**
  Templates for the connection to cloud services that expect the XML format.
- **CSV generic v1**
  Template for the connection to Insights Hub (Siemens) / MindConnect IoT Extension

Payload editor

You use the "Payload format" button to open the payload editor.

- **Template for payload format**
  By default, the "Payload format" text box displays the "JSON generic v2" format.
  You can select one of the syntax templates described above from the drop-down list. After selecting a syntax template, you can click the pencil icon to switch to user-defined editing.
- **Payload format**
  In the text box, you can change the payload format to be used or create the format according to your own requirements.
  When a syntax template is selected (see above), the syntax of the template selected above is displayed and used.

  Note

  Settings for the payload format

  - If you change the "Template for payload format" (for example, from "User defined" to "JSON specific"), a manually adjusted payload format is lost. However, you can also use it to restore the automatic data point assignment to the payload format.
  - The payload format must not contain more than 65,535 bytes of UTF-8 text, otherwise it cannot be adopted.

- **Add quotation marks around values automatically**
  Option can only be adapted with the syntax template "User-defined". For all other syntax templates, the option is set according to the selection.
  When enabled, a string is automatically set around the value {{VALUE}}, if necessary, for data points of the type "String" and "DateTime".

- **Escape sequences**
  Escape sequences which adapt the code according to the protocol used can be used to convert certain special characters.
  Special characters can occur within the following name components, for example:
  - Station name
  - Topic name
  - Group name

  The following escape sequences are available to the application for selection:
  - JSON
    Standard JSON escape sequences
  - XML
    Standard XML escape sequences
  - CSV
    Standard CSV escape sequences

  When an option is selected, the respective special characters are converted into escape sequences at the publisher.
  At the subscriber, the escape sequences are converted in the reverse direction.
  For information on the escape sequences used with the JSON format, see appendix JSON escape sequences (Page 189).
- **Use this payload format for all topics**
  When the option is enabled, the payload format displayed in the text box is applied to all groups or topics to be published.
  After saving, the check mark for the option is removed from the topic editor.
  Please note:
  If changes are made later, the changes are only applied to the relevant topic or group and not to all topics or groups when you press "Apply".
- **Cancel**
  The payload editor is closed without saving the changes made.
- **Save**
  The changes made in the payload editor are saved and the payload editor is closed.

Payload preview

The preview shows how the configured payload of the selected topic, filled with example values, will be sent to the broker.

The display is limited to 65535 characters.

- **Export**
  The entire payload format can be downloaded for analysis as a "cc_plrender.txt" file (even if there are more than 65535 characters).
- **Close**
  The payload preview is closed.

Payload format - JSON generic v3

All data points assigned to the topic are mapped to the payload using a loop construct with the specified properties and formatting.

```
{"Timestamp":"{{PUBLISH_TIMESTAMP}}","DataItems":
[{{#DATA_POINT_ARRAY}}
{"Variable":"{{NAME}}","Type":"{{TYPE}}","TimeSeries":
[{{#TIME_SERIES}}{"Value":{{VALUE}},"QualityCode":
{{QUALITY_CODE}},"SourceTimestamp":"{{SOURCE_TIMESTAMP}}"}
{{^LAST_ITEM}},{{/LAST_ITEM}}{{/TIME_SERIES}}]}{{^LAST_DATA_POINT}},
{{/LAST_DATA_POINT}}{{/DATA_POINT_ARRAY}}]}
```

Use cases:

- Simple JSON payload format with many data points and the highest possible performance with the lowest possible data volume.
- Support for data points of the type "Array".
- Support of the "Collect" function.

Payload format - JSON generic v2

All data points assigned to the topic are mapped to the payload using a loop construct with the specified properties and formatting.

```
{"Timestamp":"{{PUBLISH_TIMESTAMP}}","DataItems":
[{{#DATA_POINT_ARRAY}}
{"Variable":"{{NAME}}","Type":"{{TYPE}}","Value":
{{VALUE}},"QualityCode":{{QUALITY_CODE}}}{{^LAST_DATA_POINT}},{{/
LAST_DATA_POINT}}{{/DATA_POINT_ARRAY}}]}
```

Use cases:

- Simple JSON payload format with many data points and the highest possible performance with the lowest possible data volume.
- Support for data points of the type "Array".

Payload format - JSON specific v3

If this format is selected, all assigned data points are listed individually with their available properties. Example for 3 data points of the "ST1" station with the names "DP1", "DP2" and "DP3":

```
{
 "Timestamp": "{{PUBLISH_TIMESTAMP}}",
 "DataItems":
 [
 {
 "Variable":"{{ST1.DP1.NAME}}",
 "Type":"{{ST1.DP1.TYPE}}",
 "TimeSeries":
```

```
[{{#ST1.DP1.TIME_SERIES}}
{
"Value":{{VALUE}},
"QualityCode":{{QUALITY_CODE}},
"SourceTimestamp":"{{SOURCE_TIMESTAMP}}"
}{{^LAST_ITEM}},{{/LAST_ITEM}}
{{/ST1.DP1.TIME_SERIES}}]
},
{
"Variable":"{{ST1.DP2.NAME}}",
"Type":"{{ST1.DP2.TYPE}}",
"TimeSeries":
[{{#ST1.DP2.TIME_SERIES}}
{
"Value":{{VALUE}},
"QualityCode":"{{QUALITY_CODE}}",
"SourceTimestamp":"{{SOURCE_TIMESTAMP}}"
}{{^LAST_ITEM}},{{/LAST_ITEM}}
{{/ST1.DP2.TIME_SERIES}}]
},
{
"Variable":"{{ST1.DP3.NAME}}",
"Type":"{{ST1.DP3.TYPE}}",
"TimeSeries":
[{{#ST1.DP3.TIME_SERIES}}
{
"Value":{{VALUE}},
"QualityCode":"{{QUALITY_CODE}}",
"SourceTimestamp":"{{SOURCE_TIMESTAMP}}"
}{{^LAST_ITEM}},{{/LAST_ITEM}}
{{/ST1.DP3.TIME_SERIES}}]
}
]
}
```

Switching from "JSON specific" to "User-defined"

Each data point can be individually formatted and displayed with selected properties in the payload. Unneeded properties of individual data points can simply be erased. Additional (e.g. static) content can be added. The properties of selected data points can also be referenced multiple times. The references to the data points must always be placed within the square bracket "DataItems" [...].

Use cases:

- Complex JSON payload format with few data points.
- Support for data points of the type "Array".
- Support of the "Collect" function

Payload format - JSON specific v2

If this format is selected, all assigned data points are listed individually with their available properties. Example for 3 data points of the "ST1" station with the names "DP1", "DP2" and "DP3":

```
{
 "Timestamp": "{{PUBLISH_TIMESTAMP}}",
 "DataItems":
 [
  {
   "Variable": "{{ST1.DP1.NAME}}",
   "Type": "{{ST1.DP1.TYPE}}",
   "Value": {{ST1.DP1.VALUE}},
   "QualityCode": {{ST1.DP1.QUALITY_CODE}},
   "StationName": "{{ST1.DP1.STATION_NAME}}",
   "Timestamp": "{{ST1.DP1.SOURCE_TIMESTAMP}}"
  },
  {
   "Variable": "{{ST1.DP2.NAME}}",
   "Type": "{{ST1.DP2.TYPE}}",
   "Value": {{ST1.DP2.VALUE}},
   "QualityCode": {{ST1.DP2.QUALITY_CODE}},
   "StationName": "{{ST1.DP2.STATION_NAME}}",
   "Timestamp": "{{ST1.DP2.SOURCE_TIMESTAMP}}"
  },
  {
   "Variable": "{{ST1.DP3.NAME}}",
   "Type": "{{S1.DP3.TYPE}}",
   "Value": {{ST1.DP3.VALUE}},
```

```
   "QualityCode": {{ST1.DP3.QUALITY_CODE}},
   "StationName": "{{ST1.DP3.STATION_NAME}}",
   "Timestamp": "{{ST1.DP3.SOURCE_TIMESTAMP}}"
  }
 ]
}
```

Switching from "JSON specific" to "User-defined"

Each data point can be individually formatted and displayed with selected properties in the payload. Unneeded properties of individual data points can simply be erased. Additional (e.g. static) content can be added. The properties of selected data points can also be referenced multiple times. The references to the data points must always be placed within the square bracket "DataItems" [...].

Use cases:

- Complex JSON payload format with few data points.
- Support for data points of the type "Array".

Payload format - XML generic

All data points assigned to the topic are mapped to the payload using a loop construct with the specified properties and formatting.

```
<?xml version="1.0" encoding="UTF-8"?
><root><Timestamp>{{PUBLISH_TIMESTAMP}}</
Timestamp><DataItems>{{#DATA_POINT_ARRAY}}<DataItem><Variable>{{NAME
}}</Variable><Type>{{TYPE}}</Type><Value>{{VALUE}}</
Value><QualityCode>{{QUALITY_CODE}}</QualityCode></DataItem>{{/
DATA_POINT_ARRAY}}</DataItems></root>
```

Use cases:

- Simple XML payload format with many data points and the highest possible performance at the lowest possible data volume.

Payload format: XML specific

If this format is selected, all assigned data points are listed individually with their available properties. Example for 3 data points of the "ST1" station with the names "DP1", "DP2" and "DP3":

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
 <Timestamp>{{PUBLISH_TIMESTAMP}}</Timestamp>
 <DataItems>
  <DataItem>
   <Var>{{ST1.DP1.NAME}}</Var>
   <Type>{{ST1.DP1.TYPE}}</Type>
```

```
    <Value>{{ST1.DP1.VALUE}}</Value>
    <QualityCode>{{ST1.DP1.QUALITY_CODE}}</QualityCode>
    <StationName>{{ST1.DP1.STATION_NAME}}</StationName>
    <Timestamp>{{ST1.DP1.SOURCE_TIMESTAMP}}</Timestamp>
   </DataItem>
   <DataItem>
    <Var>{{ST1.DP2.NAME}}</Var>
    <Type>{{ST1.DP2.TYPE}}</Type>
    <Value>{{ST1.DP2.VALUE}}</Value>
    <QualityCode>{{ST1.DP2.QUALITY_CODE}}</QualityCode>
    <StationName>{{ST1.DP2.STATION_NAME}}</StationName>
    <Timestamp>{{ST1.DP2.SOURCE_TIMESTAMP}}</Timestamp>
   </DataItem>
   <DataItem>
    <Var>{{ST1.DP3.NAME}}</Var>
    <Type>{{ST1.DP3.TYPE}}</Type>
    <Value>{{ST1.DP3.VALUE}}</Value>
    <QualityCode>{{ST1.DP3.QUALITY_CODE}}</QualityCode>
    <StationName>{{ST1.DP3.STATION_NAME}}</StationName>
    <Timestamp>{{ST1.DP3.SOURCE_TIMESTAMP}}</Timestamp>
   </DataItem>
  </DataItems>
</root>
```

Switching from "XML specific" to "User defined"

Each data point can be individually formatted and displayed with selected properties in the payload. Unneeded properties of individual data points can simply be erased. Additional (e.g. static) content can be added. The properties of selected data points can also be referenced multiple times. The references to the data points must always be placed within the XML bracket <DataItems> ... </DataItems>.

Use cases:

- Complex XML payload format with rather few data points.
- Special adaptation of the payload to third-party specifications.

Payload format - MindConnect IoT Extension

```
{{#DATA_POINT_ARRAY}}200,{{NAME}},{{GROUP}},{{VALUE}},
{{ADDITIONAL_ATTRIBUTE}},{{PUBLISH_TIMESTAMP}}\n{{/
DATA_POINT_ARRAY}}
```

Code: Syntax and meaning

Description of the syntax

The description of the individual keys is structured as follows:

- **Name**
  `<Syntax>`
  Meaning

Code key

The code for formatting the payload can consist of the following keys listed below.

If you want to use not only the keys for the transfer of payload but also want to add text, you can add the text in front of or after a key.

The code of the formatted payload can contain the following keys depending on the format.

- **Time stamp**
  `{{PUBLISH_TIMESTAMP}}`
  Time of the publication
  - Example for coding the time stamp with added text "sent at":
    Syntax: "`sent at {{PUBLISH_TIMESTAMP}}`"
    Results in string: "`sent at 2019-04-20T13:58:16.192313634+00:00`"
- **Start and end of the loop over all assigned data points**
  `{{#DATA_POINT_ARRAY}}`
  `{{/DATA_POINT_ARRAY}}`
- **Start and end of the loop over all collected values**
  `{{#TIME_SERIES}}`
  `{{/TIME_SERIES}}`
- **200**
  `200`
  Function code (MindConnect IoT Extension)
- **Station**

  Note

  Correct naming of the station/variable

  Direct referencing by means of {{Station.Variable.xxx}} with user-defined payload can only be used with stations or variables in which there is no period in the name. If there is a period, the values are no longer replaced correctly.

  `{{STATION_NAME}} /`
  `{{Station.Variable.STATION_NAME}}`
  Station name of the data point
  Configuration only for publisher
- **Data point / Variable**
  `{{NAME}} /`
  `{{Station.Variable.NAME}}`
  Name of the data point

- **Group**
  `{{GROUP}} /`
  `{{Station.Variable.GROUP}}`
  Group name
- **Value**
  `{{VALUE}} /`
  `{{Station.Variable.VALUE}}`
  Value of the data point
  If the "Collect" function is enabled and the payload format does not contain a TIME_SERIES loop, the collected values within the payload are displayed in a list, separated by commas.
- **Attribute**
  `{{ADDITIONAL_ATTRIBUTE}} /`
  `{{Station.Variable.ADDITIONAL_ATTRIBUTE}}`
  Additional attribute, which can be configured manually for each individual data point (mandatory for MindConnect IoT Extension, otherwise optional).
- **QualityCode**
  `{{QUALITY_CODE}} /`
  `{{Station.Variable.QUALITY_CODE}}`
  Quality status of the value
  If the "Collect" function is enabled and the payload format does not contain a TIME_SERIES loop, the overall quality status corresponds to that of all collected values. This means that the overall quality status "GOOD" is only reached when each individual value has this status.
  For the meaning, see section Publish groups (Page 114).
- **Data type**
  `{{TYPE}} /`
  `{{Station.Variable.TYPE}}`
  Data type alias: Data type of the data point output by the device in the payload
  For the output of the data types, see section Data points (Page 136).
- **Last data point** (in the generic variant only)
  `{{#LAST_DATA_POINT}} /`
  `{{/LAST_DATA_POINT}}`
  Last data point
- **All except the last data point** (in the generic variant only)
  `{{^LAST_DATA_POINT}} /`
  `{{/LAST_DATA_POINT}}`
  All data points except the last data point
- **All except the last data point of the TIME_SERIES**
  `{{^LAST_ITEM}} /`
  `{{/LAST_ITEM}}`
  "True" for the last item of a TIME_SERIES
- **Source time stamp**
  `{{SOURCE_TIMESTAMP}} /`
  `{{Station.Variable.SOURCE_TIMESTAMP}}`
  Time of the last reception from the source station.

Example for transferred payload based on the unchanged "JSON generic" template

Below you will find an example of the transferred payload of a topic.

The topic contains three variables of an S7 station for the data points "DP1", "DP2" and "DP3".

The value of the "DataItems" key is an array with the objects of the three variables.

```
{ "Timestamp": "2019-05-03T09:13:46.000000000+00:00",
"DataItems": [ { "Variable":"DP1", "Type":"BOOL", "Value":"0",
"QualityCode":"GOOD" }, { "Variable":"DP2", "Type":"DOUBLE_FLOAT",
"Value":"0.496043966059748", "QualityCode":"GOOD" },
{ "Variable":"DP3", "Type":"S7_STRING", "Value":"Abcd99vE",
"QualityCode":"GOOD" } ] }
```

6.9.3.4 Data point assignment

In this tab, you assign the configured data points to a previously created topic or a group. Data points can be linked with multiple topics/groups of multiple cloud profiles.

Requirement

Before you assign data points to topics or groups, you need to create the data points, see section Data points (Page 136). You also specify the data point name, data type and the other parameters there.

Data point assignment

All configured topics or groups of the selected profile can be seen on the left. On the right, all configured cloud data points of the selected station are visible.

The assignment works via drag-and-drop. Select the data points and drag them to the desired topic, keeping the left mouse button pressed.

Multiple selection of data points is possible with Ctrl + left mouse click.

- **Select station**
  Select the desired cloud profile and the desired station via the drop-down list.
  The data point table lists all data points that are configured in the stations selected above and have "Write" or "Read/Write" access.
  You can assign the data points to the topics / groups individually or as a bundle.
  Individual assignment:
  Assign each data point in the data point table individually to a topic or a group.
  Bundled assignment:
  Before you make the bundled assignment, select all data points in the table that you want to assign to a topic.
  Assign the data points to a topic with the mouse by means of Drag&Drop.
  To assign all data points of a station to a topic at the same time, assign the higher-level station object to a topic with the mouse by means of Drag&Drop. You are asked whether you want to assign all lower-level data points to the topic.
  The number of assigned data points is displayed per topic or group.
  The assigned data points can be viewed using the button of the topic and the assignment can be deleted.

See also

Payload format (Page 120)

Process access (Page 81)

6.9.4 Subscriber

Validity

⇒ Valid for MQTT profiles with the cloud providers: AWS / Azure / IBM Cloud / Other Cloud

In this tab, you create the topics for the subscriber function of the gateway under the enabled profile.

6.9.4.1 Configuring topics

Add topic

- **Select profile**
  From the drop-down list, select one of the configured cloud profiles.
  All configured groups/topics for the selected topic are displayed.
- **Add**
  A new editable topic is added to the table.
  Maximum number of publish and subscriber topics or groups
  CC712: 500
  CC716: 3500
- **Copy**
  The selected topics are copied and added to the table again.
- **Delete**
  All selected topics are deleted.
- **Name**
  Enter the name of the group that you want to create in the text box.
  The name is the essential part for identifying a group.
- **Topic**
  Enter the name of the topic in the text box. You can change the name later in the topic table below.
  The name of a topic must be unique within a cloud application.

Subscribe group configuration

The "Payload format" output box specifies the syntax that is expected and required of the received subscribed messages. Take this into account when configuring the relevant publisher.

When a message is received with a payload format that does not correspond exactly to this syntax, the message is discarded and the gateway generates a diagnostic message.

You can find the diagnostic messages in the WBM under "Maintenance > Diagnostics".

6.9.4.2 Payload format

Payload format

Use the JSON Payload format from the template for communication between the publisher and subscriber:

```
{
   "Timestamp": "PUBLISH_TIMESTAMP",
   "DataItems":
   [
      {
         "Variable": "{{Var1.NAME}}",
         "Type": "{{Var1.TYPE}}",
         "Value": {{Var1.VALUE}},
         "QualityCode": "{{Var1.QUALITY_CODE}}"
      },
      {
         "Variable": "{{Var2.NAME}}",
         "Type": "{{Var2.TYPE}}",
         "Value": {{Var2.VALUE}},
         "QualityCode": "{{Var2.QUALITY_CODE}}"
      },
...

{
         "Variable": "{{VarN.NAME}}",
         "Type": "{{VarN.TYPE}}",
         "Value": {{VarN.VALUE}},
         "QualityCode": "{{VarN.QUALITY_CODE}}"
      },
   ]
}
```

The time stamp is optional. It is not evaluated in the payload format.

Payload example

You will find an example of the expected syntax with different data types by clicking on the button.

Topic table

You can see the created topics in the table and configure their "Quality of Service" parameters.

You can sort the display alphabetically by topic name by clicking on the icon next to the name in the table header.

- **Topic**
  If necessary, you can change the name of the topic here.
- **QoS**
  You use the "Quality of Service" parameter of the topic to specify the transfer behavior of the messages between the broker and subscriber of the gateway:
  - QoS 0
    Transfer no more than once
    The broker sends the topic once to the gateway. The broker does not expect an acknowledgment. If the topic is not received by the gateway, it is lost.
  - QoS 1
    Transfer at least once
    The broker sends the topic to the gateway until it receives a PUBACK packet as acknowledgment from the gateway.
  - QoS 2
    Transfer exactly once
    The broker sends the topic and waits until it receives the two-step acknowledgment from the gateway as specified.

  When a connection is aborted, the data frames are buffered in the broker for QoS 1 and QoS 2. If a lower QoS value is configured at the subscriber of the gateway than at the publisher, the lower value applies to the communication between broker and subscriber.
- **Delete**
  By clicking the button, the topic of the respective row is deleted.

Note

Delete

Note that if you accidentally delete a topic, you cannot undo the deletion.

6.9.4.3 Data point assignment

Data point assignment

All configured topics or groups of the selected profile can be seen on the left. On the right, all configured cloud data points of the selected station are visible.

The assignment works via drag-and-drop. Select the data points and drag them to the desired topic, keeping the left mouse button pressed.

Multiple selection of data points is possible with Ctrl + left mouse click.

- **Select station**
  Select the desired cloud profile and the desired station via the drop-down list.
  The data point table lists all data points that are configured in the stations selected above and have "Write" or "Read/Write" access.
  You can assign the data points to the topics / groups individually or as a bundle.
  Individual assignment:
  Assign each data point in the data point table individually to a topic or a group.
  Bundled assignment:
  Before you make the bundled assignment, select all data points in the table that you want to assign to a topic.
  Assign the data points to a topic with the mouse by means of Drag&Drop.
  To assign all data points of a station to a topic at the same time, assign the higher-level station object to a topic with the mouse by means of Drag&Drop. You are asked whether you want to assign all lower-level data points to the topic.
  The number of assigned data points is displayed per topic or group.
  The assigned data points can be viewed using the button of the topic and the assignment can be deleted.

6.10 Data points

6.10.1 Transmission time and transferred data

Note

Requirements for the transfer (Cloud)

The following conditions must be met to transfer a value:

- The data point is assigned to a topic in the configuration.
- At least one trigger condition is met.

Time of the data transfer and quantity of the transmitted data

Triggering the data transfer is different for the two target systems:

- **Cloud**
  The transfer time is controlled via trigger, refer to the section Data points (Page 136) and section Publisher (Page 114).
  You specify the time when the values of data points are transferred to the broker for each data point and for each topic with the "Trigger".
  The following data is transferred together to the broker:
  - AWS / Azure / IBM Cloud
    Transmission of the values of all data points of the assigned topic
  - MindConnect IoT Extension / Other Cloud
    Transfer of the values of all data points of the assigned group

  Transfer takes place as soon as the value of a data point is pending for transfer or, with enabled "Sammeln" function, the conditions for collecting the data are met.
  For all value triggers, note that the data of a topic or a group is transferred as long as the trigger condition is met. This has effects on the transferred data volume.
- **OPC UA**
  The OPC UA server of the gateway executes the read and write jobs of the OPC UA clients. For OPC UA clients with subscriptions, the values are sent from the server according to the settings in the section Configuration (Page 92) under "Min. publishing interval (ms)" and "Min. polling interval (ms)". The trigger for this is a value change or a change of the QualityCode.

6.10.2 Data points

Data point configuration

In this tab, you define the data points as data sources or data destinations for the transmission, station by station.

For S7 stations, you can also export the variable information of the CPU via a source file from STEP 7 and import it as basis for the data point configuration, see S7 import (Page 146).

Follow these steps for S7Plus stations:

- Set up a connection to the station with "S7Plus browse" and import the data points; see S7Plus browse (Page 150).

For OPC UA client stations, you can proceed as follows:

- Export the variable information of the server to an XML source file and import it as basis for the data points, see OPC UA import (Page 152).
- Set up a connection to the OPC server with "OPC UA browse" and import the data points, see OPC UA browsing (Page 151).

Note

Deletion of configured data points during import

When importing variables from STEP 7 files, you can select whether previously configured data points should be deleted.

After importing variables from STEP 7 files, you can also manually configure more data points.

A data point in the gateway can alternatively be configured for one of the two target systems (Cloud / OPC UA).

However, multiple data points can be created for different target systems with reference to the same address in the station.

- **Select station**
  Select a station from the drop-down list whose data points you want to configure for the transfer. The drop-down list contains all stations that were configured under "Process access", see section Process access (Page 81).
  If data points are already configured for a station, these are displayed in the table below when selecting the station. You can change the data later.
- **Add data point** (for all stations except S7Plus)
  Creates the row for a new data point in the table.
  Alternative:

- **Copy**
  You can also create new data points by copying existing data points.
  To do so, select one or more data points using the check boxes (see below) and click the "Copy" button.
  Then adjust the properties of the copied data points.
- **Multi-editing**
  You use this button to open the "Data point configuration" dialog. You can set specific parameters for all or previously selected data points in one editing step in the dialog.
  Select multiple data points for this function using the check box in the selection column (left) of the data point table.
  You can set the following parameters for multiple data points in the dialog:
  - Target
  - Access
  - Trigger
  - Quality change

  For the meaning of the parameters, see below.
  Multi-editing is practical especially when you are importing large volumes of data points which are to receive the same values for the specified parameters.
  After configuring the specified parameters in the "Data point configuration" dialog, select one of the two options in the "Set for" parameter and click "Save".
  - **Set for selected**
    Assigns the parameter values to those data points that you selected before opening the dialog.
  - **Set for all**
    Assigns the parameter values to all data points of the data point table.

Selection of data points using the selection column

Using the check boxes in the selection column on the left in the table, you can select individual data points for copying, deleting and multi-editing.

You can sort the data points in the table columns to facilitate selection.

You use the top check box in the table header to select all data points of the table.

Deleting data points

Note

Delete

You cannot undo deleting a data point.

You can delete multiple data points by selecting them using the selection column (left) and then clicking on the "Delete" button above the table.

If you have not selected a data point and click the "Delete" button, you can delete all data points.

Data point table

Configure the parameters of the data points in the table and save them. You can correct or delete incorrect data points in the table.

The parameters are different depending on the transfer protocol of the data points. The list below contains all parameters that can be configured for S7 and Modbus/TCP.

- **Selection column**
  By using the check boxes in the left-hand column, you can select all, individual or multiple rows for multi-editing, copying or deleting.
- **Target**
  Select the target system you wish to use for the respective data point.
  - **-**
    No target system is assigned to the data point. Data is not being read or transferred.

    Note

    No connection without assigned data points

    If no data points are assigned to a target, no connection to the respective station is established.
  - Cloud
  - OPC UA
- **Name**
  Assign a unique name to the data point.
- **Type**
  Configured data point of the data area of the data point to be read
  You can find the data types supported in the table of data types below.
- **Operand area** (S7 stations only)
  The following operand areas of the CPU are available for S7:
  - I - Input
  - M - Memory
  - Q - Output
  - DB - Data block
- **Function code** (Modbus stations only)
  The following areas (tables) of the station memory area are available for selection with Modbus/TCP:
  - 1: Read Coil
  - 2: Read Discret Input
  - 3: Read Holding Registers
  - 4: Read Input Registers
  - 5: Write Single Coil
  - 6: Write Single Holding Registers
  - 16: Write Multiple Holding Registers

- **DB number** (S7 stations only)
  Number of the S7 CPU DB
  Make sure that the number matches the actually configured number of the data block.
- **Offset / Address** (only S7 and Modbus stations)
  For S7 stations
  Address of the operand depending on the data area. Enter the value as a decimal number:
  - Address (input, memory, output, DB)
    Information for Bool operands in <Byte.bit>. E.g.: 0.6
    Information for operands ≥ byte in <bytes>. E.g.: 3
  - Offset of the operand for the start address of the operand area (coil, tab)
    Information in <bytes>. E.g.: 12

  For Modbus stations
  Specifies the location of the register from which reading or writing takes place.
- **NodeID** (OPC UA stations only)
  ID of the node for unique identification of the object at the OPC UA server.
- **Array dimension** (S7, S7Plus and OPC UA stations only)
  The array size.
  - An empty entry means that the variable is not an array.
  - One-dimensional array: Input of the number whose size equals that of the array.
    For variables of the type "Bool", only arrays with a dimension are supported.
  - Multi-dimensional arrays: Input of numbers separated by comma.
    Max. three dimensions are supported.
- **Length** (S7, S7Plus and Modbus stations only)
  Number of characters for the "String" and "C_String" data type (S7/S7Plus station: 1 .. 254, Modbus station: 64)
- **Access**
  The option specifies access of the communication partners to the gateway data.
  - **Read**
    Only read access is permitted.
  - **Read/write**
    Read and write access is permitted.
  - **Write**
    Write access is permitted.

- **Trigger**
  You use the triggers to specify the conditions that initiate the transfer of the value saved in the device to the broker. You can select one trigger per data point.
  Select the type for the value trigger using the drop-down list and add the respective values:
  - Change
    The value is transferred as soon as it changes compared to the value that was read in before.
  - Range outside
    The value is transferred as soon as it is outside the configured area.
  - Range inside
    The value is transferred as soon as it is inside the configured area.
  - Threshold HIGH
    The value is transferred as soon as it exceeds the configured value.
  - Threshold LOW
    The value is transferred as soon as it drops below the configured value.

  Note:
  - The ranges of values of the value triggers depend on the data type of the data point.
  - The range of values of the station data point is converted to the range of values of the device data point.

- **Quality change**
  With this parameter, you specify the transfer behavior of the messages of all topics or groups:
  - Enabled
    Transfer on change of "QualityCode" (Good → Bad or Bad → Good)
    As soon as the quality of a data point changes, the topic is transferred.
  - Disabled
    No transfer on change of the "QualityCode".
- **Attribute**
  The attribute is included in the payload as `{{ADDITIONAL_ATTRIBUTE}}` / `{{Station.Variable.ADDITIONAL_ATTRIBUTE}}`, see section Payload format (Page 120).
  Enter the attribute according to the requirements of the cloud provider:
  - AWS / Azure / IBM Cloud / Other cloud: Optional
    If no attribute is demanded or required, leave the box empty.
  - IoT Extension: Mandatory

  With a connection to IoT Extension, the attribute is interpreted as a label of the physical units of the respective data point. The standard units are:
  - C = Temperature in degrees Celsius
  - P = Pressure in bars
  - mm = Length in millimeters
  - km/h = Speed in km/h
  - m/s2 = Acceleration in m/s^2
  - % = Size in percent
  - %RH = Relative humidity in percent
  - A = Current in amperes
  - V = Voltage in volts
  - W = Power in watts
  - kWh = Energy in kilowatt hours
  - VAh = Apparent energy in volt ampere hours
  - dBm = Transmit power in decibel-milliwatts (logarithmic ratio)
  - lux = Illuminance in lux (lm/m^2)

  Other compound units of the SI system can also be specified, for example:
  m/h, m/s, m, km, mW, kW, mWh, mA, VArh

Trigger

You can combine two triggers for each data point:

- One trigger with the value of the data point.
- One time trigger or input trigger at the topic to which the data point is assigned.

When two triggers are configured, the transfer is initiated as soon as one of the two trigger conditions is met.

Additional restrictions can result from the trigger types supported by the individual data types; see "Data types" table below.

Transfer and QualityCode

The "QualityCode" quality status of a data point is also transferred with the payload. The status indicates the validity of the value.

The status is set by the gateway as publisher and has the following value range:

- GOOD
  The value is valid.
- BAD
  The value of the variable is not valid or not current. Possible causes:
  - CPU in STOP
  - Value not current
  - Error while reading the variable

The value of the status has the following effect on the transmission:

- Publisher → Cloud
  Publishing of messages of the gateway as publisher is independent of the value of the status.
- Cloud → Subscriber
  Receiving of messages by the gateway as subscriber is independent of the value of the status. However, when a message with the status "BAD" is received, the value is not written to the process station by the gateway as subscriber.

Connection abort and QualityCode

The behavior for a connection abort is as follows:

- **Connection abort between station and gateway**
  - During the connection abort
    The gateway sends the topic with empty strings for the values and the QualityCode "Bad".
  - Recurring connection
    When the trigger condition is met, the gateway sends the topic with the current values and the QualityCode "Good".
- **Connection abort between gateway and cloud**
  - During the connection abort - cable pulled at the gateway or cloud server cannot be reached.
    The gateway is not sending data. Depending on which value you have entered for the individual topics or groups for "Message buffering", the data is buffered in the gateway with its current value and quality code.
  - Recurring connection
    The gateway first sends the buffered messages. Afterwards, the current values are sent after the trigger conditions are triggered.

Data types

Not every data type supports all trigger types. The following tables list the configurable data types and specify the supported trigger types for each data type.

Table 6-3 **Data types for S7/S7Plus station**

S7/S7Plus station			Data type in the target system		Supported triggers		Suitable for array
Data type	**Bit width**	**Operand area**	**OPC server**	**MQTT/HTTP**	**Time**	**Value**	**(max. 100 arrays per station)**
BOOL	1	I, Q, M, DB	Boolean	BOOL	x	x	x [7]
CHAR	8	I, Q, M, DB	Byte	CHAR	x	x	x
SINT [2]	8	I, Q, M, DB	SByte	INT8	x	x	x
INT	16	I, Q, M, DB	Int16	INT16	x	x	x
DINT	32	I, Q, M, DB	Int32	INT32	x	x	x
LINT [1]	64	I, Q, M, DB	Int64	INT64	x	x	x
USINT [2]	8	I, Q, M, DB	Byte	UINT8	x	x	x
UINT [2]	16	I, Q, M, DB	UInt16	UINT16	x	x	x
UDINT [2]	32	I, Q, M, DB	UInt32	UINT32	x	x	x
ULINT [1]	64	I, Q, M, DB	UInt64	UINT64	x	x	x
BYTE	8	I, Q, M, DB	Byte	UINT8	x	x	x
WORD	16	I, Q, M, DB	UInt16	UINT16	x	x	x
DWORD	32	I, Q, M, DB	UInt32	UINT32	x	x	x
LWORD [1]	64	I, Q, M, DB	UInt64	UINT64	x	x	x
REAL	32	I, Q, M, DB	Float	SINGLE_FLOAT	x	x	x
LREAL [2]	64	I, Q, M, DB	Double	DOU-BLE_FLOAT	x	x	x
DATE_AND_TIME [3]	64	DB	DateTime	S7_DT [5]	x	-	-
DTL [2]	96	DB	DateTime [4]	S7_DTL [5]	x	-	-
STRING	2..256 bytes	DB	String	STRING	x	-	x
CSTRING [6]	0..254 bytes	DB	String	STRING, C_STRING	x	-	x

[1] S7-1500 only

[2] S7-1200/1500 only

[3] S7-300/400/1500 only

[4] The accuracy of the DTL (1 ns, 10^{-9} seconds) is restricted to 100 ns (10^{-7} seconds) for OPC DateTime.

[5] Formatting according to ISO 8601, e.g. "2020-03-31T08:25:59.1234+02:00".

[6] Only valid for S7 stations. An array of the type "CHAR" or individual directly consecutive data points of the type "CHAR" can be defined as "CSTRING". The length of the string is composed of the number of individual CHAR elements. The data point is represented as string in both target systems. For correct processing in a subscriber topic, the "C_STRING" data type must be received.

[7] Only one-dimensional arrays of the type "Bool" are supported. Multi-dimensional arrays of the type "Bool" cannot be configured and are not offered during the import.

Table 6-4 **Data types for Modbus client**

Modbus client			Data type in the target system		Supported triggers		Suitable for array
Data type	**Bit width**	**Memory area** [1]	**OPC server**	**MQTT/ HTTP**	**Time**	**Value**	
BOOL	1	Coil, Discrete Input	Boolean	BOOL	**x**	**x**	-
UINT16	16	Holding Register, Input Register	UInt16	UINT16	**x**	**x**	-
UINT32	32	Holding Register, Input Register	UInt32	UINT32	**x**	**x**	-
FLOAT	32	Holding Register, Input Register	Float	SINGLE_FLOAT	**x**	**x**	-
STRING	64 bytes	Holding Register, Input Register	String	STRING	**x**	-	-

[1] Write access is not supported for "Discrete Inputs" and "Input Register".

Modbus data types

The Modbus standard only recognizes 1-bit and 16-bit data objects. The extended data types are transmitted as 2 or 4 consecutive 16-bit data objects.

When using other data types in the device and in downstream applications, you must map and interpret the data read from the station in a user-specific manner.

Table 6-5 **Data types for OPC stations**

OPC server		Data type in the target system		Supported triggers		Suitable for array
Data type	**Bit width**	**OPC server**	**MQTT/HTTP**	**Time**	**Value**	**(max. 100 arrays per station)**
Boolean	1	Boolean	BOOL	**x**	**x** (value 0 only)	**x**
SByte	8	SByte	INT8	**x**	**x**	**x**
Int16	16	Int16	INT16	**x**	**x**	**x**
Int32	32	Int32	INT32	**x**	**x**	**x**
Int64	64	Int64	INT64	**x**	**x**	**x**
Byte	8	Byte	UINT8	**x**	**x**	**x**
UInt16	16	UInt16	UINT16	**x**	**x**	**x**
UInt32	32	UInt32	UINT32	**x**	**x**	**x**
UInt64	64	UInt64	UINT64	**x**	**x**	**x**
Float	32	Float	SINGLE_FLOAT	**x**	**x**	**x**
Double	64	Double	DOUBLE_FLOAT	**x**	**x**	**x**
DateTime	64	DateTime	DTL [3]	**x**	-	-

OPC server		Data type in the target system		Supported triggers		Suitable for array (max. 100 arrays per station)
Data type	**Bit width**	**OPC server**	**MQTT/HTTP**	**Time**	**Value**	
String [1]	0..256 bytes	String	STRING	**x**	-	**x**
S7_DATE_AND_TIME [2]	8 bytes	DateTime	DT-STRING (ISO 8601)	**x**	-	-

[1] If the string exceeds 256 bytes in the OPC Server, the string cannot be read by the OPC UA client and the QualityCode changes to BAD.

[2] An S7-1500 maps the internal data type DATE_AND_TIME as byte array with length of 8 in its OPC UA server. This array can be interpreted by the OPC UA client of the CC7 as S7-DATE_AND_TIME variable and forwarded to the target system with the date/time value.

[3] Formatting according to ISO 8601, e.g. "2020-03-31T08:25:59.1234+02:00".

Restrictions for MindConnect IoT Extension

The following data is not supported:

- Time stamp
- With S7-LINT / S7-ULINT:
  Integers from 2^{63} to 2^{64}

The following data types are only supported when they are transferred as event:

- Bool
- String

6.10.3 S7 import

In addition to manual data point configuration, you can import the variable information using a file exported from STEP 7 for S7 stations.

When importing variables from STEP 7 files, you can select whether or not previously configured data points are to be deleted or not.

After importing variables from STEP 7 files, you can also manually configure more data points.

Observe the following limits for the import:

- Maximum number of variables per file: 5000
- Maximum number of variables per station: 500
  The value also applies to the import of multiple files.

Requirement: Creating CPU variables in STEP 7

As a prerequisite for using the function, you need to have created variables or symbols in the respective CPU in your STEP 7 project.

- STEP 7 Professional (TIA Portal)
  - DB variables
    The "Optimized block access" option must be disabled in DBs.
  - PLC tags
- STEP 7 V5.6
  - DB variables
  - Symbols

Export from STEP 7

In the STEP 7 project, export the variables into an export file.

Recommendation: Give the export files meaningful names from which the station type, station name and possibly the DB number can be derived.

The following file formats are supported: *.db, *.awl, *.sdf, *.xml, *.dif, *.asc

- **STEP 7 Professional (TIA Portal)**
  DB variables
  - Select the DB.
  - Click on the shortcut menu "Generate source from blocks > Selected blocks only".
  - Select the file type "DB files (*.db)" and click "Save".

  PLC tags
  - Open the tag table
  - Click on the "Export" icon above the tag table.
  - Select the relevant options in the following "Export" dialog.
  - Save the PLC tags in one of the following file formats: *.xml, *.sdf

  UDT
  - Select the PLC data type UDT.
  - Click the "Generate source from blocks > Including dependent blocks" shortcut menu so that the program code of the dependent blocks and referenced PLC data types is also saved in the external source file.
  - Select the file type "DB files (*.db)" and click "Save".
- **STEP 7 V5.6**
  DB variables
  - In SIMATIC Manager, open the DB in the block directory of the CPU.
  - Click on "File > Generate source" in the block editor.
  - In the "New" dialog, select the sources of the CPU, assign a name for the file under "Object name" and click on OK.
  - In the next dialog "Generate source", move the DB(s) to the "Blocks selected" box using the arrow symbol.
    Select the "Absolute" option and click on OK.
  - Close the block window.
  - In SIMATIC Manager, in the source directory of the CPU, select the newly generated source and click on the shortcut menu "Export source".
  - In the "Export source" dialog, select the desired target directory in the PC file system.
  - Select the file type "STL source (*.awl)" and click "Save".

  Symbols
  - Select the S7 program of the CPU in SIMATIC Manager.
  - Open the symbol table.
  - Click on the menu "Table > Export".
  - Save the symbol table in one of the following file formats: *.SDF, *.ASC, *.DIF

  UDT
  - In SIMATIC Manager, open the DB in the block directory of the CPU.

- Click on "File > Generate source" in the block editor.
- In the "New" dialog, select the sources of the CPU, assign a name for the file under "Object name" and click on OK.
- In the next dialog "Generate source", move the DB(s) to the "Blocks selected" box using the arrow symbol.
  Enable the "Include referenced blocks" option and click on OK.
- Close the block window.
- In SIMATIC Manager, in the source directory of the CPU, select the newly generated source and click on the shortcut menu "Export source".
- In the "Export source" dialog, select the desired target directory in the PC file system.
- Select the file type "STL source (*.awl)" and click "Save".

Import variables

1. Save the file exported from STEP 7 with the variable information in the file system of your PC.
2. Open the WBM tab "Data points > S7 import".
3. With multiple stations, select the desired station.
4. Click "Browse", select the desired STEP 7 file and click on "Open".
   The file name is displayed in the WBM.
5. Select the required option for "Import arrays as single elements". If enabled, arrays are imported as single elements. If disabled, arrays are imported as a single data point.

   Note

   Importing Struct arrays

   Struct arrays are always imported as single elements. The "Import arrays as single elements" option relates to arrays of supported data points within the Struct array.

6. If you want to use the file, click "Import source file".
   If you want to import multiple files, repeat the operation "Browse" > "Import source file".
   After a source file is imported from a DB, the following columns are first shown in a table:
   - Name
   - DB number
     Only this box can be edited.
7. If you do want to cancel the import, click "Delete". The file and the variables that have already been imported are deleted.

8. Assign the DB number according to the STEP 7 configuration and click "Save".
   This does not yet apply the data to the data point list of the application.
   After the DB number is assigned or a source file is imported from a variable list, the variables are displayed in a table with the following columns.
   - Selection column
     Used to select data points for partial transfer into the application.
   - Name
     The data point name is formed from the following two components and applied later:
     - DB variable: <DB name>__<Variable name>
     - PLC tag/symbol: <Symbol name>
   - Operand area, DB number, address, type, length, array dimensions
     The relevant data pertaining to the contents of the source file is displayed.

   The "Delete" button removes the selected data points. If no data points are selected, you are asked whether you want to delete all data points.
9. If you want to adapt values of individual data points before the import, make the changes and confirm the change with "Save".
10. Transfer the variables into the application.
    - If you want to transfer all variables of the table, select all variables at the same time by selecting the check box in the table header and clicking "Import".
      You are asked in a dialog whether you want to delete all existing data points:
      - Select "Yes" to delete all existing data points before the import.
      - Select "No" if the data points should be imported in addition to the existing ones.
    - If you only want to use some of the imported variables, select the affected variables using the check box (left column) in the respective table row and click on "Import".

    The applied variables are deleted from the table.
11. Then go to the WBM tab "Data points", check the applied variables and click "Save".

You can continue editing the applied variables in the "Data points" tab.

6.10.4 S7Plus browse

- **Select station**
  Select one of the created stations to display the settings.

Browse S7Plus address space

- **Address**
  The IPv4 address of the S7Plus station is displayed.
- **TLS**
  The option selected for the station is displayed.

Perform S7Plus browse

1. Select the desired station via "Select station".
2. Click the "Connect" button.
3. Confirm the message that the connection to the server was successful.
   Result: The selected station with the associated variables is displayed. In addition, the following information is displayed after successful connection:
   - SPS version
   - Maximum number of subscriber data points
   - Maximum size of all data points of the station

You can browse individual folders or variables and import variables.

Import variables

Select individual variables or entire folders and click "Import". To select an entire folder, you need to open it once. The variables are transferred to the "Data points" WBM tab and can be edited there.

Note

Only create S7Plus data points using "S7Plus browse"

Due to the internal data structure, it is not possible to create S7Plus data points on the Data points page. S7Plus data points can only be created via the S7Plus browse functionality.

6.10.5 OPC UA browsing

- **Select station**
  Select one of the created stations to display the settings.

Browse OPC UA address space

- **Server address (IPv4) / (IPv6) / DNS name**
  The IPv4 or, if applicable, the IPv6 address or the DNS name of the station is displayed.
- **Security Policy**
  The option selected for the station is displayed.
- **Connect**
  You connect to the server using the button.
  On successful connection, this row is hidden and the OPC UA Nodeset tree is displayed instead.
- **Only show supported variables**
  Displayed when a successful connection to the station is established. When enabled, all invalid data points that are not supported are hidden.
- **Import**
  During the import, the selected variables are transferred to the application.

Browse OPC UA

1. Select the desired station via "Select station".
2. Click the "Connect" button.
3. Confirm the message that the connection to the server was successful.
   Result: The selected station with the associated variables is displayed. The "Display only supported variables" option can also be selected.
   You can browse individual folders or variables and import variables.

Import variables

Select individual variables or entire folders and click "Import". To select an entire folder, you need to open it once. The variables are transferred to the "Data points" WBM tab and can be edited there.

6.10.6 OPC UA import

Import OPC UA Nodeset

- **Select station**
  Select one of the created stations to display the settings.
- **Nodeset XML**
  Click the "Browse" button.
  The browser for browsing your PC file system opens.
  Select the desired XML file and click "Open".
  The file name is displayed in the output field of the WBM.
  If you want to use the file, click "Import" and confirm with "OK".
  The import process is shown by a progress bar.
  If you want to import multiple files, repeat the operation "Browse" > "Import".
  Result: The "Only show supported variables" option can be selected.
  If you do not want to use the file, click "Delete".
- **Upload**
  The upload transfers the selected Nodeset XML file to the application.
- **Only show supported variables**
  Is displayed when a Nodeset XML file was successfully loaded. When enabled, all invalid data points that are not supported are hidden.

OPC UA import

You can navigate offline through the individual folders or variables and import variables.

- **Import variables**
  Select an individual variable or a folder. To select a folder, it needs to be open.
  Click "Import".
  Result: The variables are transferred to the "Data points" WBM tab and can be edited there.

6.11 Maintenance

6.11.1 HTTP server

Settings for the web server are made in this tab.

HTTP server settings

- **Interface**
  Select the interface via which access to the WBM takes place.
  Options:
  - Process interface (P2)
  - Cloud interface (P1)
  - All
- **HTTP active**
  When this option is enabled, unencrypted access to the WBM using HTTP is possible. The option is disabled in the default setting.
- **HTTP port**
  Setting of the HTTP port. Default setting: 80
- **Redirect HTTP to HTTPS**
  When this option is enabled, access via HTTP is forwarded directly to HTTPS. The status code of forwarding can be set below.
- **Redirect status**
  Choose whether the status code "301 Moved Permanently" or "308 Permanent Redirect" is used when forwarding from HTTP to HTTPS requests.

HTTP security

- **HTTPS active**
  When this option is enabled, encrypted access to the WBM via HTTPS takes place. The option is enabled in the default setting.
- **HTTPS port**
  Setting of the HTTPS port. Default: 443

  Note

  Certificates for HTTPS communication

  The application contains a certificate issued by Siemens for HTTPS communication with the WBM.

  To increase security, you also have the option to import your own server certificate and a private key.

- **Web server certificate**
  Select a web server certificate. The Siemens factory certificate is preset with the "Standard" selection.

- **Web server private key**
- Selection of the web server key file. The Siemens factory certificate key is preset with the "Standard" selection.

Protection against brute force attacks

- **Number of failed login attempts**
  Number of failed login attempts until the IP address is locked.
  Range of values: 1...100
  Default setting: 3
- **Monitoring time of failed login attempts (s)**
  Period of time in which the configured number of failed attempts is monitored.
  Range of values: 1...3600
  Default setting: 60 s
- **Block time (s)**
  Duration for which the WBM is locked for the IP address.
  Range of values: 1...3600
  Default setting: 60 s

6.11.2 System time

In these tabs, you set the time or configure the time-of-day synchronization of the gateway.

Note

Configured NTP server must be reachable on startup of the module

If you have configured an NTP server, make sure that it can be reached during restart of the module. If the configured NTP server cannot be reached, the module will not start.

Time-of-day format and time stamps

The device keeps the time internally as UTC. The local time configured in the WBM is displayed with time zone and optional consideration of daylight saving / standard time.

The time stamps of the transferred data are transferred in UTC format (48 bits).

Synchronization method

You can synchronize the time of day manually or via NTP (Network Time Protocol).

Note

Time-of-day synchronization

For applications that require time-of-day synchronization, you should synchronize the time of day of the device. If you do not synchronize the time of day regularly, there may be deviations of several seconds each day between the device and its communication partners.

NTP configuration

- **Active**
  Enable the option if the time of day is to be synchronized via NTP.
  When this option is disabled, you can set the time of day of the device manually.
- **NTP server address**
  Enter the address of the NTP server as IPv4/IPv6 address or as DNS name.
- **Port number**
  Setting of the port via which the NTP server is reached. Default: 123
- **Synchronization cycle (s)**
  Specifies the cycle of the time-of-day queries to the NTP server.
  Range of values in seconds: 16..1024
- **NTP (secure)**
  When this option is enabled, the time is synchronized with the secure method NTP (secure).
  NTP (secure) uses authentication by means of symmetrical keys.

Parameters for the NTP (secure) method

- **Key ID**
  Key ID of the NTP server. Numeric value.
  Range of values: 1..65534
- **Key**
  Enter the NTP key in the selected format.
  Permitted key length:
  - ASCII: 5..20
  - Hexadecimal: 10-40
- **Key format**
  Specify the format in which you enter the key:
  - ASCII
  - HEX (hexadecimal)
- **Hash algorithm**
  Select alternatively:
  - SHA-1
  - MD5
  - AES128
  - AES256

Time zone

- **Time zone**
  In NTP mode, it is generally UTC (Universal Time Coordinated) that is transferred. This corresponds to GMT (Greenwich Mean Time).
  The time offset from UTC can be set by configuring the local time zone.

Daylight saving time (DLS)

- **Active**
  When this option is enabled, the system time is changed to daylight saving time, i.e. one hour is added.
  If disabled, the current system time is not changed.
- **Starts on**
  Select when daylight saving time should be enabled.
- **Ends on**
  Select when daylight saving time should be disabled.

System time

Manual setting of date and time

Note

Time does not continue to run when no voltage is applied

If you switch off the power supply to the gateway, the manually set time will not continue to run during the power-off period.

The text boxes for date and time are only active with disabled time-of-day synchronization via NTP.

- **Date**
  Enter the current date manually in the specified format or use the calendar that opens when you click in the input box:
  – DD.MM.YYYY
- **Time**
  Enter the current time of day manually in the specified format:
  – hh:mm:ss
- **Save**
  The device applies the saved time data when you click this button.

6.11.3 Certificate management

All certificates and private keys are managed on this page.

Switch between the overview of certificates and private keys via the tabs. The saved certificates and keys are shown in the overview table. You can filter the display via the table row.

Certificate details

The table shows the details of the saved certificates with the following parameters:

- **File name**
  Name of the certificate file is displayed.
- **Issuer**
  Information on the applicant of the certificate (CN, OU, O, L, S, C)
- **Valid from**
  Start date of the period of validity of the certificate
- **Valid to**
  End date of the period of validity of the certificate
- **Fingerprint**
  Fingerprint (Digest) of the certification data
- **Download**
  The certificate is saved on the PC.

Certificates

- **Create**
  When you click on the button, you are forwarded to a page on which you can create a new certificate.
- **Upload**
  Load existing certificates and client keys into the certificate store.
  The requirement for importing certificates and keys is that the corresponding files are saved on your PC.
  The following types of certificate files are supported: *.pem, *.crt, *.cer, *.crl
  The following types of key files are supported: *.pem
  - Click the "Choose file" button.
    A browser opens to search the content of your PC file system.
    Select the file saved on your PC.
  - Then click "Import" to download the certificate.

  The file name is displayed after importing a file.
- **Delete**
  You click this button to delete the respective certificate and key files from the certificate store.

Creating a certificate

- **File name**
  Assign a name for the file.
- **Format**
  Select a format from the drop-down list.
- **Algorithm**
  Select the required algorithm from the drop-down list.
- **Length of the private key (bits)**
  Select the key length from the drop-down list.

- **Elliptic Curve Cryptography (ECC)**
  Select the desired elliptic curve from the drop-down list.
- **Password of private key (optional)**
  Optionally, assign a password for the private key.
- **Validity (days)**
  Specify the number of days for which the certificate will be valid. Range of values: 1..3650.
- **Signature algorithm**
  Select a signature algorithm from the drop-down list.
- **Organization name (O)**
- **Organizational unit (OU)**
- **Town (L)**
- **State (ST)**
- **Country (C)**
- **Common name (CN)**
- **Domain component (DC)**

Subject alternative name (SAN)

- **URI**
- **DNS name**
  You can enter multiple DNS names, separated by a comma.
- **IP address**
  You can enter multiple IP addresses, separated by a comma.
- **E-mail**

Private keys

- **Upload**
  Load existing private keys into the certificate store.
  Requirement for import: The key is saved on your PC.
  - Click the "Choose file" button.
    A browser opens to search the content of your PC file system.
    Select the file saved on your PC.
  - Then click "Import" to download the key.

  The file name is displayed after importing a file.
  - Assign a password for the key.
- **Delete**
  Deletes selected keys.

6.11.4 User management

6.11.4.1 Password rules

In this tab, you can define the rules for password creation for each user group.

- **User group**
  Select the user group for which you want to define password rules.
- **Min. password length**
  Define the minimum length of the password. Default: 8 characters
- **Maximum password length**
  Define the maximum length of the password. Default: 1024 characters
- **At least 1 lowercase letter**
  Select the check box to apply this rule.
- **At least 1 uppercase letter**
  Select the check box to apply this rule.
- **At least 1 number**
  Select the check box to apply this rule.
- **At least 1 special character**
  Select the check box to apply this rule. The password must contain one of the following special characters (ASCII 0x21..0x7E):
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- **Force password reset**
  Select the check box to reset all user passwords when you change the password rules.
  Users with the "ADMIN" role need to enter a new password on the next login.
  Users with the "GUEST" role are disabled until a user with the "ADMIN" role assigns the "GUEST" a new password.

6.11.4.2 User

Note

Loss of user data

Note changed or newly assigned user names and passwords.

When you lose the user data of the administrator, you no longer have access to the WBM.

When losing the login data, you only have access to the WBM by resetting the device to the factory settings. This is associated with a loss of data.

For the preset standard user data for initial login, see section User data for the first login to the WBM (Page 68).

Permitted length of the user name: 4...64 characters

Note

Changing the password

For security reasons, the user name and password preset at the factory must be changed at the first login.

Overview

All created users are displayed in the table on the overview page.

You can filter and sort using the first row in the table.

Some of the displayed properties can be edited directly on the overview page.

Password rules

Newly assigned user passwords must meet the following requirements:

- Minimum length: 8 characters
- At least 1 lowercase letter
- At least 1 uppercase letter
- At least 1 number
- At least one of the following special characters (ASCII 0x21..0x7E):
  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Roles and rights

SuperUser

The SuperUser is the first user on the module. It is in the "ADMIN" group by default and cannot be regrouped or deleted. There is exactly one SuperUser.

You can add up to six additional users with the roles "ADMIN" or "GUEST".

ADMIN

Users with the "ADMIN" role have the rights to change all data that is accessible in the WBM.

GUEST

Users with the role "GUEST" only have access to the diagnostics data and cannot make changes to the configuration.

Add user

Click the "Create" button to create a new user.

- **Active**
  Only active users can establish a connection to the WBM. There must always be one active user with administrator rights.
- **User group**
  Assign the "ADMIN" or "GUEST" role to the user. The selected role can no longer be changed later.
- **New user name**
  Enter the user name of the new user.
- **Repeat user name**
  To confirm, repeat the user name entered above.
- **New password**
  Enter the password for the new user.
- **Repeat password**
  Repeat the password entered above.
- **Language**
  Select the default language of the WBM for the user.
- **First name**
  Optionally, enter the first name of the user.
- **Last name**
  Optionally, enter the last name of the user.

Editing user data

Note

Applying changed user data

Changed user data is applied immediately after it has been saved.

After the user data is changed, it must be used for the next login.

Click on the icon in the "Edit" table column to edit the user data.

Parameters:

- **Active**
  Only active users can establish a connection to the WBM.
- **SuperUser**
  Shows whether the user is an administrator.
- **User group**
  Shows which role is assigned to the user. The user group cannot be changed.
- **User name**
  Display of the current user name

- **Current password**
  Enter the current password before you make any changes to the user name or password.
- **New user name**
  Enter a new user name to change it.
- **Repeat user name**
  To confirm a new user name, repeat the user name entered above.
- **New password**
  Enter a new password to change the password.
- **Repeat password**
  Repeat the new password.
- **Language**
  Select the default language of the WBM for the user.
- **First name**
  Optionally, change the first name of the user.
- **Last name**
  Optionally, change the last name of the user.

6.11.4.3 User groups

In this tab, you can define for each user group the period of inactivity after which the running session ends and the user is logged out.

- **Session lifetime**
  Select the period of inactivity after which the running session is automatically ended.
  - 10 min
  - 30 min
  - 1 hour
  - 1 day
  - 1 week

  Default: 10 min.

6.11.5 Firmware

You can find the current firmware version of the device on the WBM page Info (Page 70).

If a new firmware version is available, you can download the firmware file from the PC to the gateway via this WBM page.

For new firmware files for the gateway, refer to the section Loading new firmware (Page 171).

Note

Digitally signed and encrypted firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Firmware update

- **Firmware file**
  After selecting a firmware file stored on the PC using the "Search" button, the file name is displayed here.
- **Browse**
  Searches the file system of the PC for a firmware file saved there that is intended to be loaded on the gateway.
  Firmware files have the file format *.upd.
  After selecting the file, the name of the selected file is displayed but the firmware is not used yet.
- **Load on device**
  By clicking the button, you download the selected firmware file to the gateway.
  The ongoing update process is indicated in the WBM by a progress bar.

After the update is complete, the gateway automatically reboots. After the restart you will need to log in again. Check whether the loaded firmware version is displayed on the home page under "Info" > "Status".

Note

Firmware update

Note that updating the firmware can take a while.

- **No input during activation**
  During activation until the gateway restarts, the WBM is not locked.
  Do not change the WBM page during this time.
- **No switch off of the gateway**
  Do not switch off the gateway during activation of the firmware. This avoids the occurrence of inconsistent statuses.
- **Automatic adoption of stored configuration changes**
  Configuration changes already saved but not yet adopted are automatically applied on restart after a firmware update.

6.11.6 Backup and restore

6.11.6.1 Configuration

In this tab, you can save the configuration data of the gateway in a configuration file and load it again.

Configuration files have the names "CC712<Date and Time>.cfg" or "CC712<Date and Time>.cfgp" or "CC716...".

You cannot edit encrypted configuration files (*.cfgp). If encrypted parts are changed, the configuration file is rejected when you try to download it.

You can manually edit encrypted configuration files (*.cfg). If invalid changes are made, e.g. formal errors, the configuration file is rejected when you try to load it.

Saving the configuration file on the PC is useful in the following cases:

- You want to use the configuration data of the gateway for another gateway.
- You want to use multiple gateways with similar configuration data.
- In case of replacement

You download the configuration data from the PC to another gateway and reconfigure only the parameters that are different, if necessary.

You can also allow an inserted CLP to be formatted by the gateway.

Export configuration

Note

Options for exporting a configuration

You have the following options when exporting a configuration:

- **Without user data and PKI**
  This file with the *.cfg file extension only contains the device configuration with the configured connections and data points. This file is suitable for transferring the configuration to other gateways, since certificates and keys usually have to be adapted.
- **With user data and PKI**
  This file with the *.cfgp file extension contains the device configuration with the configured connections and data points as well as all user data, passwords, certificates and, if necessary, the corresponding private keys. With this file, another gateway can take over all settings, e.g. when replacing parts, and immediately resume operation.

Note

Automatic backup

If you do not wish an existing configuration of CloudConnect to be converted on a firmware update, the configuration is automatically saved as backup and can be downloaded. You can send this backup to Support in urgent cases.

In this case, CC7 starts with factory settings and default user data.

- **Password** (optional)
  The configuration file is stored encrypted. Additionally, you can secure the configuration file against unauthorized use by entering a password (8-64 characters). The configuration file can only be reloaded by entering this password.
- **Export**
  Saves the configuration currently used by the gateway with the selected options to a configuration file on the PC.

Downloading a configuration

- **Legacy configuration (before V2.0)**
  You can load a backup configuration file of V1.9 with this option. With legacy configurations of earlier firmware versions, the import can fail.
- **Password (optional)**
  If a password was specified when the configuration file was saved, this password must also be specified again when loading this configuration file.
- **Configuration file**
  After a configuration file saved on the PC is selected with the "Browse" button, the file name is displayed here.
- **Select file**
  Searches the file system of the PC for a configuration file saved there that is intended to be loaded on the gateway.
- **Load on device**
  Downloads the configuration file shown under "File" to the gateway.

Note

Applying the configuration data

The user data of a loaded configuration file of the type "cfgp" is applied directly and used by the gateway on the next user login, even if the remaining configuration has not yet been applied on the CC7.

The configuration data of the loaded configuration file is applied with a click on the "Apply" button and used by the gateway on the next user login.

Note

Saved certificates

When a configuration file of the type "cfg" is loaded, all existing certificates are retained in the certificate store.

When a configuration file of the type "cfgp"" is loaded, the existing certificates are overwritten by the certificates from the loaded configuration file.

6.11.6.2 CLP

In this tab, you obtain information about the CLP. You can also format a brand new CLP or one previously used by another device. The formatting deletes the existing data on the CLP.

- **Status**
  Shows whether a CLP is inserted and whether the format is known.
- **File system**
- Shows where in the file system. EXT4
- **Memory capacity**
  Memory size of the CLP in bytes.
- **Used memory**
  Used memory in bytes.
- **Information**
  Display of general information stored on the CLP.
- **Save**
  Click "Save" to save the current configuration on the CLP.
- **Format**
  The inserted CLP is formatted after you click the "Format" button.
  When the formatting process is complete, a message is displayed in the WBM. Do not switch off the gateway before the message appears.

6.11.7 Communication / Restart

Process communication / Restart

On this page, you can stop or start the communication between gateway and process stations and initiate a restart of the application.

With each command, a message is output by the system and the displayed status is updated.

Process communication

The current status is displayed under "Status".

- **Stop**
  Click the button to stop communication.
  The labeling of the button changes.
- **Start**
  Click the button to restart communication.

Restart

- **Restart**
  Click the button to initiate a restart of the application.

Reset to factory settings

By clicking the button, you reset all data of the application to the factory settings.

The MAC addresses of the interfaces are not deleted by the reset.

After the reset, the application performs a restart.

Note

Data loss due to reset

Before you reset, note the effects of the reset described below.

- All configuration data, certificates, keys and user data are deleted by the reset.
  The data on an optional CLP are deleted as well.
- By resetting the IP parameters at the respective interface, the application can no longer be reached using the previously configured address data.
  The application can be reached at the factory set IP address of the respective interface. For information on the preset IP parameters, see section Restarting and resetting (Page 172).

Operating system

- **Restart**
  Click the button to fully restart CC7.
- **Shut down**
  Click the button to fully shut down CC7.
  All LEDs except for the LAN LEDs of P1 and P2 are disabled. The CC7 can now be disconnected from the power.
  The CC7 will only restart when the power has been disconnected and reconnected once.

6.11.8 Diagnostics

Diagnostic messages

This page contains diagnostics messages for internal events and errors.

- **Update**
  Here you set whether and in which cycle the WBM updates the displayed diagnostic messages.

The entries contain a time stamp and the message text.

- Notifications (NOTIFICATION) are displayed in bold.
- Errors are displayed in red.
- Notes are displayed in blue.
- Warnings are displayed in yellow.

Examples of events:

- Startup

- Establishment/termination of a communications connection

- Change to the configuration

6.11.9 Logging

6.11.9.1 Logging

Use of logging

By using the logging functions in log files, you can export important events to a file.

- **Export**
  Click the button to export the respective file to the PC file system.

The exported files are displayed in the footer of the WBM. You can open the files from the PC file system or directly from the WBM tab.

See also

Syslog messages (Page 191)

6.11.9.2 Export log files

- **Trace**
  During runtime, information about important events is automatically saved. This data contains information on the configuration, active procedures and error situations.
  You should only use logging of events if you have problems with the application that you cannot solve yourself.
  Using the "Export" button, you can save this data in a "*.enc" logging file.
  The information in this unreadable file is encrypted and can only be read by Siemens Industry Online Support. Send the log file back to your contact at Siemens Industry Online Support.
- **Security messages**
  You can save the security events in a *.log file.
- **Diagnostic messages**
  Here you can save the diagnostic messages of the device in a compressed archive "diagnostic.tqz".
  Unzip the *.tqz archive and the following extracted *.tar archive. You can find the diagnostic messages in a *.log file.
- **Network analysis**
  Only users with the "ADMIN" role can perform network analysis.
  The results of the network analysis are saved in up to four files.
  You should only use the network analysis if you have problems with the application that you cannot solve yourself.
  Using the "Export" button, you can save this data in a "*.enc" logging file.
  The information in this unreadable file is encrypted and can only be read by Siemens Industry Online Support. Send the log file back to your contact at Siemens Industry Online Support.
- **PROFIBUS/MPI (CC716)**
  Using the "Export" button, users with the "ADMIN" role can save this data in a "profibus.bin" logging file.

6.11.9.3 Record data traffic

To diagnose network problems, you can enable recording of the data traffic on the CC7. You can export the results and send them as encrypted file to the Siemens Industry Online Support for analysis.

The parameters can be combined and left blank.

- **Enable**
  Enable the option to start the recording.
  The recording is automatically ended when the module is restarted. The recording continues with "Save" and "Apply".
- **Network interface**
  Select the network interface whose sent or received data traffic is being recorded.
- **Host**
  Select the direction and the IP address to be recorded.
- **Port**
  Select the direction and the port number.
- **Protocol**
  Select the required protocol.

6.11.9.4 Security events

The gateway outputs Syslog messages according to RFC 5424 / RFC 5426. The messages are based on IEC 62443-3-3.

When the address data of a Syslog server is input, the gateway sends the messages to the server.

If you do not have a Syslog server, leave the server address free.

- **Active**
  When enabled, all security events are sent to the configured Syslog server.
- **Server address**
  Enter the IP address of the Syslog servers.
- **Server port**
  You can change the default server port 514 (UDP).

You will find a description of the Syslog messages in the appendix Syslog messages (Page 191).

Diagnostics and maintenance 7

7.1 Diagnostics options

The following diagnostics options are available:

LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 33).

Web Based Management (WBM)

To do this, you need to connect your PC to the gateway.

On the following WBM pages you obtain information on the status of the gateway:

- You will find general information on the status of the gateway on the start page of the WBM, compare to section Info (Page 70).
- You will find the diagnostics messages on the diagnostics page of the WBM, refer to the section Diagnostics (Page 167).
  When important events occur, the gateway writes diagnostic messages to the diagnostics buffer.

7.2 Loading new firmware

You can find the current firmware version of the device on the WBM page Info (Page 70).

New firmware versions

If a new firmware version is available for the module, you will find this on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/25621/dl)

Save the firmware file on the configuration PC.

Downloading new firmware files

You load a new firmware file from the configuration PC on the gateway via the WBM.

You will find the description in the section Firmware (Page 162).

7.3 Restarting and resetting

Functions and execution

The following functions are available for resetting:

- **Restart**
  The configuration data is retained.
  The gateway performs a restart.
  You can perform the function via:
  - WBM: "Maintenance > Communication / Restart"
- **Reset to factory settings**
  The configuration data is deleted.
  The data on an optional CLP are deleted as well.
  The gateway performs a restart.
  You can perform the function via:
  - "SET" button
    To operate the button, refer to the section The button "SET" (Page 38).
  - WBM: "Maintenance > Communication / Restart"

Restart

The gateway ends productive operation, restarts automatically and takes up productive operation again with the existing configuration data.

Resetting to factory settings: Effect

Note

Data is deleted

With the resetting to factory settings, all configuration data and process data on the gateway is deleted.

With a reset to factory settings, the gateway can only be reached over the factory default address data.

- **Deleted data**
  The following data is deleted in the gateway by resetting to factory settings:
  - Addresses of the LAN interfaces configured by the user
    They are reset to the factory default address data.
  - All other configuration data of the gateway
  - All process data in the memory of the gateway
  - User names and passwords
  - All imported certificates
  - Diagnostics buffer

  The following data is also deleted:
  - All data on an inserted CLP
- **Data not deleted**
  The following data is not deleted by resetting to factory settings:
  - MAC address of the LAN interfaces

Restart after reset

- The gateway starts up without configuration data.
- The DHCP client function is disabled.

The gateway can only be reached over the default address data, refer to the section Establishing a connection to the WBM (Page 67).

7.4 Device replacement in the event of a fault

Device defective

If a fault develops, please send the device to your Siemens representative for repair. Repairs on-site are not possible.

Replacing the gateway

⚠ WARNING

Before replacement

- Before replacing the gateway, read the safety notices in the section Important notes on using the device (Page 41).
- While working on the device make sure that the power supply is turned off.

When replacing the gateway follow the steps described in the section Installation (Page 44).

Transfer of the configuration data to the new gateway

If you have previously saved the configuration data of the gateway in a configuration file on a PC or a CLP, you can download the data to the gateway after connecting the PC to the gateway or after starting, refer to the section Configuration (Page 164).

Technical specifications

8

8.1 Technical specifications - CloudConnect 712

Technical specifications - CloudConnect 712		
Article number	6GK1411-1AC00	
Attachment to Industrial Ethernet		
Quantity	2 x gigabit interface (P1, P2)	
Design	RJ-45 jack, galvanically isolated	
Properties		
• Standard	• 1000BASE-T, IEEE 802.3ab	
• Transmission speeds	• 10 / 100 / 1000 Mbps	
• Other properties	• Half duplex/full duplex, autocrossover, autonegotiation, autosensing	
Power supply		
Design	Socket including 5-pin terminal block with reverse polarity protection	
Power supply	• Type of voltage	• 24 V DC
	• Permitted low limit	• 19.2 V
	• Permitted high limit	• 28.8 V
Terminal block	(Power supply)	
Clamping screw	M2	
	Screwdriver blade:	0.4 x 2.5 (DIN 5264)
Tightening torque	0.2...0.25 Nm	
Connectable cable cross-sections	• Without wire end ferrule	• 0.5...2.5 mm^2 / AWG 20...12
	• With wire end ferrule	• 0.5....1.5 mm^2 / AWG 20 .. 16
Further electrical data		
Current consumption (typical)	200 mA	
Effective power loss (typical)	4.8 W	
Overvoltage category according to IEC / EN 60664-1	Category II	
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally	0 °C ... +60 °C
	During operation with the rack installed vertically	0 °C ... +50 °C
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 60 % at 25 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3	
	• SO_2	• < 0.5 ppm
	• H_2S	• < 0.1 ppm

Technical specifications - CloudConnect 712	
Design, dimensions and weight	
Module format	Compact module S7-1500
Degree of protection	IP20
Weight	300 g
Dimensions (W x H x D)	35 x 147 x 127 mm
Mounting type	• 35 mm DIN rail mounting • S7-300 standard rail mounting • S7-1500 standard rail mounting • Wall mounting

For further data, refer to section Planned operating environment (Page 19).

8.2 Technical specifications - CloudConnect 716

Technical specifications - CloudConnect 716		
Article number	6GK1411-5AC00	
Attachment to Industrial Ethernet		
Quantity	2 x gigabit interface (P1, P2)	
Design	RJ-45 jack, galvanically isolated	
Properties		
• Standard	• 1000BASE-T, IEEE 802.3ab	
• Transmission speeds	• 10 / 100 / 1000 Mbps	
• Other properties	• Half duplex/full duplex, autocrossover, autonegotiation, autosensing	
Connection to PROFIBUS		
Quantity	1 x PROFIBUS/MPI interface (MPI/DP)	
Design and standard	9-pin D-sub socket, RS-485	
Transmission speeds	9.6 kbps, 19.2 kbps, 45.45 kbps, 93.75 kbps, 187.5 kbps, 500 kbps, 1.5 Mbps, 3 Mbps, 6 Mbps, 12 Mbps	
Maximum current consumption on the PROFIBUS interface when connecting network components (for example, optical network components)	15 mA at 5 V (only for bus termination) *	
Power supply		
Design	Socket including 5-pin terminal block with reverse polarity protection	
Power supply	• Type of voltage	• 24 V DC
	• Permitted low limit	• 19.2 V
	• Permitted high limit	• 28.8 V
Cable cross-section connectable to the terminal block	• Without wire end ferrule	• 0.2 .. 2.5 mm^2 / AWG 24 .. 13
	• With wire end ferrule	• 0.25 .. 1.5 mm^2 / AWG 24 .. 16
	• With TWIN wire end ferrule	• 0.5 .. 1.0 mm^2 / AWG 20 .. 17

Technical specifications - CloudConnect 716		
Further electrical data		
Current consumption (typical)	250 mA	
Effective power loss (typical)	6 W	
Overvoltage category according to IEC / EN 60664-1	Category II	
Digital input		
Quantity	1 x terminal block (DI)	
Design	2-pin	
Voltage	Rated voltage 24 V DC Safety Extra Low Voltage (SELV) • For state "1": 13 to 30 V DC • For state "0": -30 to 3 V DC	
Other properties	• Maximum input current 8 mA • Maximum cable length < 30 m Cables should be routed in pairs • Input isolated from electronics • Minimum pulse length: 100 ms	
Digital output		
Quantity	1 x terminal block (DO)	
Design	Switch, 2-pole	
Voltage	Rated voltage 24 V DC Safety Extra Low Voltage (SELV)	
Other properties	• Internal, not current-limited • Maximum current-carrying capacity 1 A • Maximum cable length < 30 m Cables should be routed in pairs • Output isolated from electronics	
Terminal blocks (power supply, digital input, digital output)		
Clamping screw	M2	
	Screwdriver blade:	0.4 x 2.5 (DIN 5264)
Tightening torque	0.2...0.25 Nm	
Connectable cable cross-sections	• Without wire end ferrule	• 0.5...2.5 mm^2 / AWG 20...12
	• With wire end ferrule	• 0.5....1.5 mm^2 / AWG 20 .. 16
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally	0 °C ... +60 °C
	During operation with the rack installed vertically	0 °C ... +50 °C
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 60 % at 25 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3	
	• SO_2	• < 0.5 ppm
	• H_2S	• < 0.1 ppm

Technical specifications - CloudConnect 716	
Design, dimensions and weight	
Module format	Compact module S7-1500
Degree of protection	IP20
Weight	400 g
Dimensions (W x H x D)	35 x 147 x 127 mm
Mounting type	• 35 mm DIN rail mounting • S7-300 standard rail mounting • S7-1500 standard rail mounting • Wall mounting

***** The current load due to an external consumer connected between VP (pin 6) and DGND (pin 5) must not exceed a maximum of 15 mA (short-circuit proof) for bus termination.

For further data, refer to section Planned operating environment (Page 19).

Approvals

9

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/25621/cert))

You can view the considered standards in the respective certificate which is available on the Internet at the address listed above.

Address for declarations of conformity

The EU and the UK declarations of conformity are available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
P.O. Box 48 48
90026 Nuremberg
Germany

EC declaration of conformity

The product meets the requirements and safety objectives of the following EU 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.

- **2014/34/EU (ATEX explosion protection directive)**
  Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356
- **2014/30/EU (EMC)**
  EMC directive of the European Parliament and of the Council of February 26, 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, pages. 79-106
- **2011/65/EU (RoHS)**
  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

UK Declaration of Conformity

Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

The product meets the requirements of the following directives:

- UKEX Regulations
  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.
- EMC Regulations
  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.
- RoHS Regulations
  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX, IECEx, UKEX and CCC Ex certification

Observe the information in the "Use of subassemblies/modules in a Zone 2 Hazardous Area" document, which you will find here:

- On the documentation DVD supplied with the product, under:
  "All documents" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- On the Internet at the following address:
  Link: (Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013))

The conditions must be met for safe usage of the product according to the section Notices for use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 42).

The product meets the explosion protection requirements outlined below.

II 3G Ex ec IIC T4 Gc

- DEKRA 18ATEX0027 X
- DEKRA 21UKEX0003 X
- IECEx DEK 18.0019X

Importer UK:
Siemens plc,
Manchester
M20 2UR
(Ex na IIC T4 Gc, not on the nameplate)

The product meets the requirements of the standards:

EN/IEC 60079-7, GB 3836.8

EN IEC/IEC 60079-0, GB 3836.1

You can find the standards involved in the currently valid certificates.

EMC

The product meets the requirements of the following directives:

- EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive)
- EMC Regulations SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

Applied standards:

- EN 61000-6-2
  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN 61000-6-4
  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

RoHS

The product meets the requirements of the following directives:

- EU directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.
- SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

Applied standard: EN IEC 63000

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)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E 85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

Applied standards:

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta: Refer to the temperature class on the type plate of the CP

Report / UL file: E223122 (NRAG, NRAG7)

Note the conditions for the safe deployment of the product according to the section General notices on use in hazardous areas according to UL HazLoc / FM (Page 43).

Note

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

CSA

CSA Certification Mark Canadian Standard Association (CSA) nach Standard C 22.2 No. 142:

- Certification Record 063533–C-000

FM

Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

You will find the temperature class on the type plate on the module.

Australia - RCM

The product meets the requirements of the AS/NZS 2064 standards (Class A).

Canada

This class A digital device meets the requirements of the Canadian standard ICES-003.

AVIS CANADIEN

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Note that in terms of the emission of interference, this device corresponds to limit class A. This device can be used in all areas except for residential environments.

Current approvals

SIMATIC NET products are regularly submitted to the relevant authorities and approval centers for approvals relating to specific markets and applications.

If you require a list of the current approvals for individual devices, consult your Siemens contact or check the Internet pages of Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15248/cert)

Dimension drawings

10

All dimensions in the dimension drawings are in millimeters.

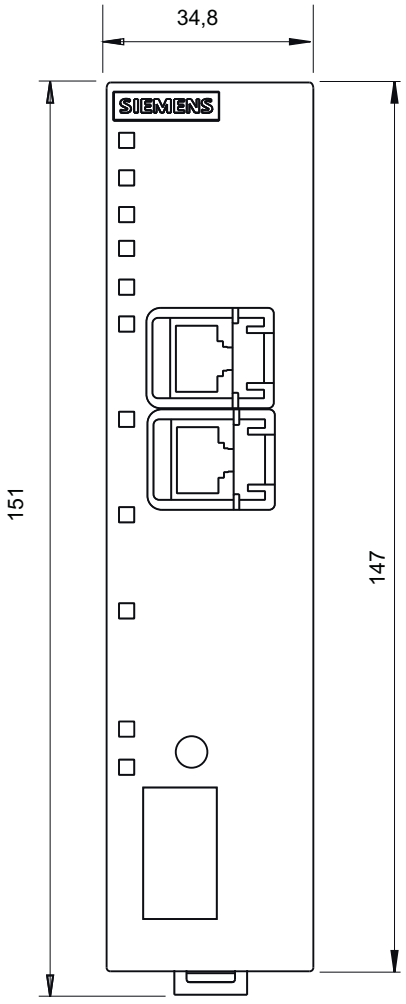


Figure 10-1 Front view

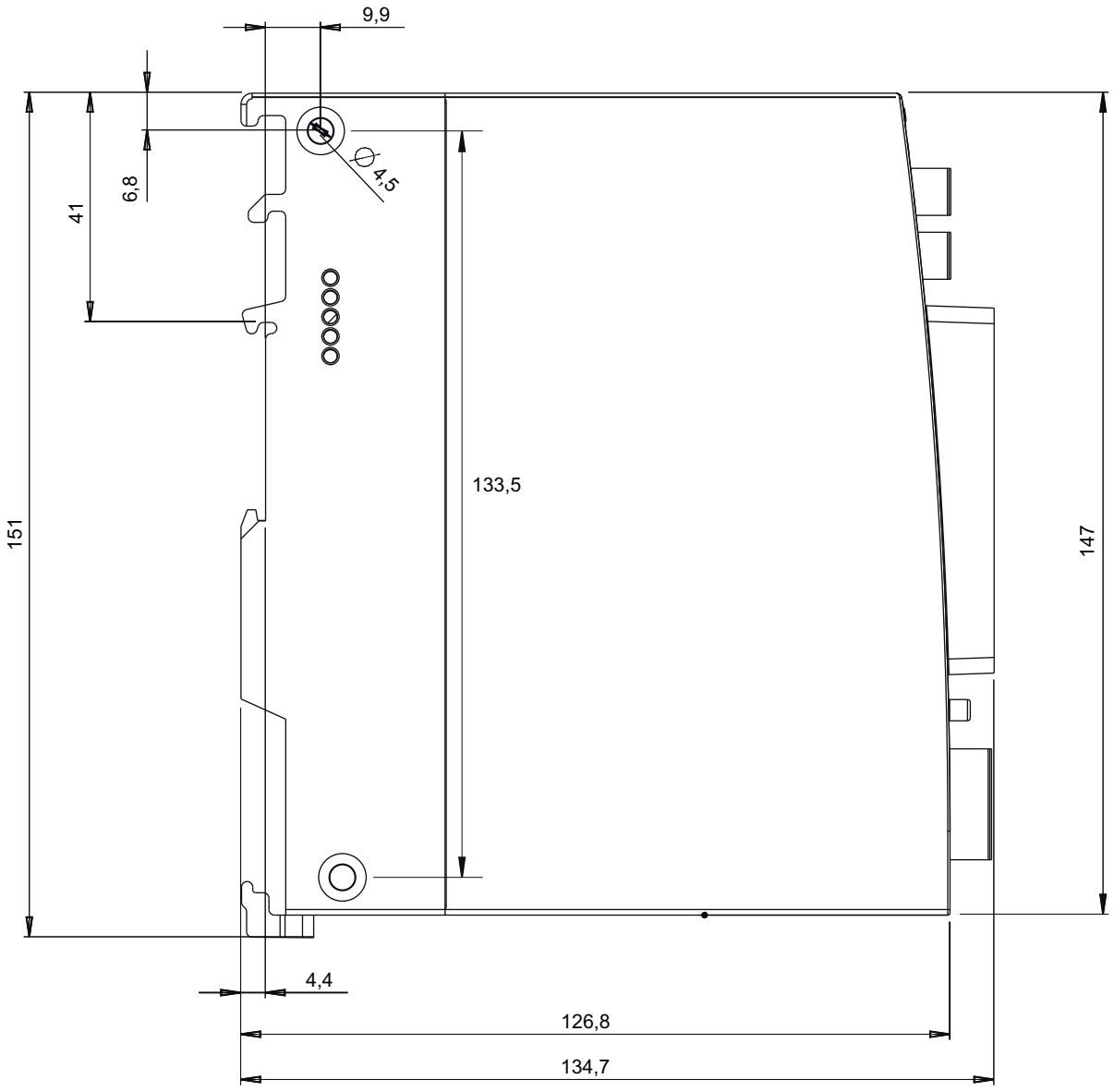


Figure 10-2 Side view

Accessories

A

You will find details and ordering data for the products of the accessories program in the Siemens Industry Mall, see:
Link: (https://mall.industry.siemens.com)

A.1 Power supply

Power supplies for the gateway

Excerpt from the Siemens program for power supplies SITOP and S7-1500:

- SITOP PSU100C
  24 V / 0.6 A stabilized power supply, input: AC 120/230 V, output: DC 24 V / 0.6 A
  Article number: 6EP1331-5BA00
- SIMATIC PM 1507 24 V / 3 A
  Stabilized power supply for SIMATIC S7-1500, input: AC 120/230 V, output: DC 24 V / 3 A
  Article number: 6EP1332-4BA00
- SIMATIC PM 1507 24 V / 8 A
  Stabilized power supply for SIMATIC S7-1500, input: AC 120/230 V, output: DC 24 V / 8 A
  Article number: 6EP1333-4BA00

A.2 CLPs

Usable CLPs

The device can be operated with a CLP, an exchangeable storage medium for storage of configuration data. A CLP does not ship with the device.

The following CLPs are available:

- SCALANCE CLP 2GB
  Article number: 6GK1900-0UB00-0AA0
  Exchangeable storage medium for easy device replacement
- SCALANCE CLP 32GB
  Article number: 6GK1900-0UB40-0AA0
  Exchangeable storage medium for easy device replacement
- SCALANCE CLP EEC 2GB
  Article number: 6GK1900-0UQ00-0AA0
  Exchangeable storage medium with painted circuit boards for easy device replacement

Escape sequences

B

B.1 JSON escape sequences

JSON escape sequences

When the JSON format is used for the user data, the following characters are converted into escape sequences in the Publisher:

For the subscriber, the escape sequences are converted into the reverse direction.

To transfer the user data, see section Payload format (Page 120).

Characters	JSON escape sequence	Note
\n	\\n	New line *
\r	\\r	Line break *
\t	\\t	Tab *
\"	\\"	Quotation marks
\\	\\\\	Double backslash
\u0000	\\u0000	
\u0001	\\u0001	
\u0002	\\u0002	
\u0003	\\u0003	
\u0004	\\u0004	
\u0005	\\u0005	
\u0006	\\u0006	
\u0007	\\u0007	
\b	\\u0008	
\t	\\u0009	
\n	\\u000A	
\u000b	\\u000B	
\f"	\\u000C	
\r	\\u000D	
\\u000e	\\u000E	
\u000f	\\u000f	
\u0010	\\u0010	
\u0011	\\u0011	
\u0012	\\u0012	
\u0013	\\u0013	
\u0014	\\u0014	
\u0015	\\u0015	
\u0016	\\u0016	
\u0017	\\u0017	

Characters	JSON escape sequence	Note
\u0018	\\u0018	
\u0019	\\u0019	
\u001a	\\u001a	
\u001b	\\u001b	
\u001c	\\u001c	
\u001d	\\u001d	
\u001e	\\u001e	
\u001f	\\u001f	
\u007F	\\u007F	

***** Not configurable in STEP 7 as name component

Syslog messages

C

Security events

The gateway outputs Syslog messages according to RFC 5424. The messages are based on IEC 62443-3-3.

C.1 Structure of the messages

C.1.1 Structure of the Syslog messages

Syslog messages record changes in device states as status information. Syslog messages according to RFC 5424 or RFC 5426 are output by devices and transferred to a server via the set UDP port (standard: 514). The Syslog server collects the information of the devices and informs you about these events.

The Syslog protocol prescribes a fixed sequence and structure of the possible parameters. Syslog messages according to RFC5424 have the following structure:

Part / Parameter	Explanation
HEADER	
PRI	Priority of the Syslog message, divided into: • Severity (Severity) Possible values: – 0 Emergency – 1 Alert – 2 Critical – 3 Error – 4 Warning – 5 Notice – 6 Information – 7 Debug • Facility (Origin) Possible values, e.g.: Sub-system, service, user
VERSION	Version number of the Syslog specification
TIMESTAMP	Time stamp of the device as local time including time zone and correction for daylight saving/standard time Format: YYYY-MM-DDThh:mm:ss.msmsmsms+xx:yy Example: 2010-01-01T02:03:15.0003+02:00

Part / Parameter	Explanation
HOSTNAME	Identifies the source device by either: • FQDN • IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX • IPv6 address according to RFC4291 Section 2.2 • Host name "-" is output if information is missing. In the product: The configured IPv4 address of the process interface P2
APP-NAME	Device or application from which the message originates. "-" is output if information is missing. In the product: "-"
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing. In the product: "-"
MSGID	ID to identify the message. "-" is output if information is missing. In the product: "-"
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on system time with the two parameters "tzKnown" and "isSynced". Example: [timeQuality tzKnown="0" isSynced="0"] • tzKnown This parameter specifies whether the time zone is known in the source device. – 1 = known – 0 = unknown • isSynced This parameter specifies whether the source device is synchronized with a reliable external time source, e.g. via NTP. – 1 = synchronized – 0 = not synchronized
MSG	
MESSAGE	Message text as ASCII string (English)

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in the RFCs:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

C.1.2 Variables in Syslog messages

The variables are displayed in the section "Syslog messages" in the field "Message text" within curly brackets {variable}.

The output messages can contain the following variables:

Variable	Description	Format	Possible values or example
{IP address}	IPv4 address according to RFC1035 IPv6 address according to RFC4291 Section 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{FQHN}	Fully Qualified Host Name: Completely specified host name; specification as domain (FQDN) or as IP address.	FQDN: host1.com IPv4: %d.%d.%d.%d	server1 192.168.1.105
{Protocol}	Layer 4 protocol or service used that generated the event.	%s	UDP | TCP | WBM | PB | OPC
{User name}	String (without spaces) that identifies the authenticated user by his or her name.	%s	<Admin>
{Time minute} {Timeout}	Number of minutes	%d	1
{Time second}	Number of seconds	%d	600
{Failed login count}	Number of failed login attempts	%d	3
{Max sessions}	Maximum number of sessions	%d	2
{Version}	Name of the version (without spaces)	%s	V1.2.6
{Config detail}	String to identify the WBM session.	%s	ELXsKPKGzx-Fey7ap92bqBbbU7ux-tazb7QCEaptnpZDG-oaO05XK5l6UpbF1HUTFV2

C.2 Syslog messages

The gateway outputs the following SYSLOG messages, sorted by classes:

C.2.1 Process communication status

SE_COMMUNICATION_STARTED_(protocol)

Message text	{Protocol}: User {User name} started the process communication.
Example	Console: User Admin started the process communication.
Explanation	The user has started the process communication.
Severity	Notice
Facility	local0
Standard	-

SE_COMMUNICATION_STOPPED_(protocol)

Message text	{Protocol}: User {User name} stopped the process communication.
Example	Console: User Admin stopped the process communication.
Explanation	The user has stopped the process communication.
Severity	Notice
Facility	local0
Standard	-

C.2.2 IACS User identification and authentication

SE_NETWORK_SUCCESSFUL_LOGON_(protocol)

Message text	{Protocol}: User {User name} logged in from {IP address}.
Example	Console: User Admin logged in from 192.168.0.1.
Explanation	Login with valid login information
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

SE_NETWORK_UNSUCCESSFUL_LOGON_(protocol)

Message text	{Protocol}: User {User name} failed to log in from {IP address}.
Example	Console: User Admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or password specified during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

SE_LOGOFF (protocol)

Message text	{Protocol}: User {User name} logged out from {IP address}.
Example	Console: User Admin logged out from 192.168.0.1.
Explanation	Session ended with user logout.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

SE_DEFAULT_USER_AUTHENTICATION_USED (protocol)

Message text	{Protocol}: Default user {User name} logged in from {IP address}.
Example	Console: Default user <user name> logged in from 192.168.0.1.
Explanation	Default user has logged in via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

C.2.3 Account management

SE_ACCESS_PWD_CHANGED_(protocol)_(own password)

Message text	{Protocol}: User {User name} has changed the password.
Example	Console: User admin has changed the password.
Explanation	User has changed own password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

SE_ACCOUNT_NAME_CHANGE_(protocol)_(user)

Message text	{Protocol}: Default user account was changed to {User name}.
Example	Console: Default user account was changed to <new user>.
Explanation	The default account was changed.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

SE_USER_ACCOUNT_CREATED_(protocol)

Message text	{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.
Example	WBM: User "ADMIN" created user-account "User1" with role "GUEST".
Explanation	The administrator created a new user "User1" with the role "GUEST".
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

SE_USER_ACCOUNT_CHANGED_(protocol)

Message text	{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.
Example	WBM: User "ADMIN" changed user-account "User1" with role "GUEST".
Explanation	The administrator changed the existing user account "User1" with the role "GUEST".
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

SE_USER_ACCOUNT_DELETED_(protocol)

Message text	{Protocol}: User {User name} deleted user-account {Destination user name}.
Example	WBM: User "ADMIN" deleted user-account "User1".
Explanation	The administrator deleted the existing user account "User1".
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

C.2.4 Unsuccessful login attempts

SE_ACCOUNT_LOCKED_TEMP_(protocol)_(User)

Message text	{Protocol}: User {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Example	Console: User Admin account is locked for 1 minutes after 3 unsuccessful login attempts.
Explanation	After too many failed login attempts, the corresponding user account is locked for a specific time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

C.2.5 Remote session termination

SE_RAS_SESSION_TERMINATED_INACTIVITY_(protocol)

Message text	{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.
Example	WBM: Remote session o1cs3jjKy... was closed after 600 seconds of inactivity.
Explanation	The session was closed after a period of inactivity.
Severity	Notice

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.6

C.2.6 Concurrent session control

SE_ACCESS_DENIED_NUMBER_OF_CONCURRENT_SESS_(protocol)

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM: The maximum number of 2 concurrent login session exceeded.
Explanation	The maximum number of simultaneous sessions has been reached.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

C.2.7 Non-repudiation (config change)

SE_CONFIG_CHANGE_(protocol)_(complete configuration)

Message text	{Protocol}: User {User name} has changed configuration.
Example	WBM: User Admin has changed configuration.
Explanation	User has changed the configuration data by loading a new *.cfg file.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

SE_CONFIG_CHANGE_(protocol)_(specific configuration)

Message text	{Protocol}: User {User name} has changed {Config detail} configuration.
Example	WBM: User Admin has changed opcua_server configuration
Explanation	A user has changed specific parts of the configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

SE_CONFIG_CHANGE_DELETE_(protocol)_(specific configuration)

Message text	{Protocol}: User {User name} has deleted {Config detail} configuration.
Example	WBM: User Admin has deleted opcua_server configuration
Explanation	A user has deleted specific parts of the configuration.

Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

SE_CONFIG_CHANGE_RTF_(protocol)_(reset to factory)

Message text	{Protocol}: User {User name} has initiated a reset to factory defaults.
Example	WBM: User Admin has initiated a reset to factory defaults.
Explanation	User has initiated a reset to factory settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

C.2.8 Communication integrity

SE_COMMUNICATION_DATA_INTEGRITY_ERROR_(protocol)

Message text	{Protocol}: Integrity verification failed.
Example	MQTT: Integrity verification failed.
Explanation	Proof of integrity failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.1

C.2.9 Session authenticity

SE_INVALID_SESSION_ID_(protocol)

Message text	{Protocol}: Session ID verification failed.
Example	WBM: Session ID verification failed.
Explanation	The session ID is invalid.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

C.2.10 IACS Backup

SE_BACKUP_SUCCESSFULLY_DONE_(protocol)

Message text	{Protocol}: User {User name} created backup file.
Example	Console: User <user name> created backup file.
Explanation	User has created a backup file.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.3

SE_BACKUP_FAILED_(protocol)

Message text	{Protocol}: User {User name} failed to create backup file.
Example	Console: User <user name> failed to create backup file.
Explanation	Creation of backup file by user failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.3

C.2.11 IACS Recovery and Reconstitution

SE_BACKUP_RESTORE_FAILED_(protocol)

Message text	{Protocol}: User {User name} failed to apply backup file.
Example	Console: User <user name> failed to apply backup file.
Explanation	Use of backup file by user failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

SE_BACKUP_RESTORE_SUCCESSFULLY_DONE_(protocol)

Message text	{Protocol}: User {User name} applied backup file.
Example	Console: User <user name> applied backup file.
Explanation	Backup file successfully used by user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

SE_FW_DEPLOYMENT_SUCCEEDED_(protocol)_(user)

Message text	{Protocol}: User {User name} activated the Firmware {Version}.
Example	Console: User <user name> activated the Firmware V2.
Explanation	Firmware successfully activated by user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

SE_FW_DEPLOYMENT_FAILED_(protocol)_(user)

Message text	{Protocol}: User {User name} failed to activate Firmware {Version}.
Example	Console: User <user name> failed to activate Firmware V2.
Explanation	Firmware activation by user failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Ciphers used

D

D.1 Introduction to the "Ciphers" section

The following tables list the encryption methods (ciphers) used by CC7.

The following data is specified for CC7 for each communication class:

- Services / Protocols (role)
  - Services / Protocols: The services or protocols used by CC7
  - (Role): The communication role assumed by CC7: Client, server or both

The following data is specified in the tables:

- **Category**
  Authentication/encryption method, protocol version or Cipher Suite
- **Name**
  Name of the category according to IANA
  You can find an overview of the TLS parameters and Cipher Suites on the following page:
  Link: (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4)
- **Value (hex)**
  Value (hexadecimal) of the suite according to IANA
- **Activation**
  Use in CC7
  - -
    Cipher classed as secure, not enabled by default.
  - ✓
    Cipher classed as secure, enabled by default.
  - Legacy
    Cipher no longer classed as secure
    You must explicitly enable use in CC7.

D.2 SSL

Communication between CC7 and communication partners

Services / Protocols (role):

- WBM/HTTPS (server) (RSA certificate)

Category	Name	Value (hex)	Activation
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028	✓

Cipher Suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009F	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA8	✓
Cipher Suite	TLS_DHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCAA	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CCM	0xc09F	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006B	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02F	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CCM	0xC09E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	✓
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

Services / Protocols (role):

- WBM/HTTPS (server) (ECDH certificate)

Category	Name	Value (hex)	Activation
Cipher Suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xC02C	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC024	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA9	✓
Cipher Suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xC02B	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC023	✓
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0AC	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0AD	✓
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	✓

Services / Protocols (role):

- MQTT (client)
- HTTP (client)
- S7Plus (client)

Category	Name	Value (hex)	Activation
Cipher Suite	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x0040	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x0067	✓
Cipher Suite	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x006A	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x006B	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x009E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x009F	✓
Cipher Suite	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00A2	✓
Cipher Suite	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00A3	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC023	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC024	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xC027	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xC028	✓
Cipher Suite	TLS_ECDHE_ECD-SA_WITH_AES_128_GCM_SHA256	0xC02B	✓
Cipher Suite	TLS_ECDHE_ECD-SA_WITH_AES_256_GCM_SHA384	0xC02C	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CCM	0xC09E	✓
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CCM	0xC09F	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0AC	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0AD	✓
Cipher Suite	TLS_ECDHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA8	✓
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCA9	✓
Cipher Suite	TLS_DHE_RSA_WITH_CHA-CHA20_POLY1305_SHA256	0xCCAA	✓
Cipher Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Cipher Suite	TLS_RSA_WITH_AES_256_CBC_SHA	0x0035	Legacy
Cipher Suite	TLS_RSA_WITH_AES_128_CBC_SHA	0x002F	Legacy
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0xC00A	Legacy
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xC014	Legacy
Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x0039	Legacy
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xC009	Legacy
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xC013	Legacy
Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x0033	Legacy
Protocol version	TLSv1.1	-	Legacy
Protocol version	TLSv1.2	-	✓
Protocol version	TLSv1.3	-	-

D.3 OPC UA

Services / Protocols (role):

- OPC UA (server)

Category	Name	Value (hex)	Activation
Security Policy	Basic256Sha256	-	✓
Security Policy	None	-	Legacy
Security Policy	Basic128Rsa15	-	Legacy
Security Policy	Basic256	-	Legacy
Security Policy	Aes128_Sha256_RsaOaep	-	-
Security Policy	Aes256_Sha256_RsaPss	-	-

Services / Protocols (role):

- OPC UA (client)

Category	Name	Value (hex)	Activation
Security Policy	Basic256Sha256	-	✓
Security Policy	None	-	Legacy
Security Policy	Basic128Rsa15	-	Legacy
Security Policy	Basic256	-	Legacy
Security Policy	Aes128_Sha256_RsaOaep	-	-
Security Policy	Aes256_Sha256_RsaPss	-	-

Index

T

W