

SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet CP 1545-1

Operating Instructions

Preface

Application and functions	1
LEDs, connectors	2
Installation, wiring, commissioning, operation	3
Configuration	4
Program blocks	5
Diagnostics and maintenance	6
Technical specifications	7
Approvals	8
Dimension drawings	9
Syslog messages	A

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.

Preface

CAUTION

To prevent injury, read the manual before use.

Validity of the document

This document is valid for the following product:

- CP 1545-1
Article number 6GK7545-1GX00-0XE0
Hardware product version 1
Firmware version V1.0

Communication processor for connecting SIMATIC S7-1500 to Industrial Ethernet
Communication functions: TCP/IP, UDP, S7, FTP Client/Server, E-mail, Connection to cloud systems via MQTT



Figure 1 S7-1500 with CP 1545-1 (right)

Purpose of the document

The document describes the application and properties of the device. It supports you during configuration and shows maintenance and diagnostic options.

Required experience

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

- General electrical engineering
- Automation engineering / STEP 7 Professional

Product names and abbreviations

The following terms and abbreviations are used in this document:

- **CP / device / module**
Designations for the communication processor CP 1545-1
- **ES**
Engineering station (STEP 7 Professional)
- **Station**
SIMATIC S7 station
- **WBM**
Abbreviation for "Web Based Management", the Web pages of the application for configuration and diagnostic data.

Document on the Internet

You will also find the current issue of this document on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/man>)

Cross references

In this manual there are often 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

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

You will find license conditions in the following document on the supplied data medium:

- OSS_CP15451_99.pdf

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit

Link: (<http://www.siemens.com/industrialsecurity>)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

Link: (<http://www.siemens.com/industrialsecurity>)

Firmware

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

Documentation for the S7-1500

The documentation of the SIMATIC products has a modular structure and covers topics relating to your automation system.

The complete documentation for the S7-1500 system consists of a system manual, function manuals, device manuals or operating instructions.

The STEP 7 information system (online help) also supports you in configuring and programming your automation system.

The following table shows additional documents that supplement this CP manual and are available on the Internet.

Table 1 Overview of the documentation for S7-1500

Topic	Documentation	Most important contents
System description	System manual: S7-1500 Automation System (https://support.industry.siemens.com/cs/ww/en/view/59191792)	<ul style="list-style-type: none"> • Application planning • Installation • Connecting • Commissioning
System diagnostics	Function manual: System diagnostics (https://support.industry.siemens.com/cs/ww/en/view/59192926)	<ul style="list-style-type: none"> • Overview • Diagnostics evaluation for hardware/software
Communication	Function manual: Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925)	<ul style="list-style-type: none"> • Overview

Topic	Documentation	Most important contents
	Function manual: Web Server https://support.industry.siemens.com/cs/ww/en/view/59193560	<ul style="list-style-type: none"> • Function • Operation
	SIMATIC NET - Industrial Ethernet / PROFINET - system manual <ul style="list-style-type: none"> • Industrial Ethernet Link: https://support.industry.siemens.com/cs/ww/de/view/27069465 • Passive network components Link: https://support.industry.siemens.com/cs/ww/en/view/84922825 	<ul style="list-style-type: none"> • Ethernet networks • Network configuration • Network components
Interference-free installation of control systems	Function Manual: Interference-free installation of control systems https://support.industry.siemens.com/cs/ww/en/view/59193566	<ul style="list-style-type: none"> • Basics • Electromagnetic compatibility • Lightning protection • Housing selection
Cycle and response times	Function manual: Cycle and Response Times https://support.industry.siemens.com/cs/ww/en/view/59193558	<ul style="list-style-type: none"> • Basics • Calculations

Device defective

If a fault develops, please send the device to your SIEMENS service center 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

	Preface	3
1	Application and functions	13
1.1	Application	13
1.2	Communication services.....	13
1.3	Cloud communication	14
1.4	Further functions	15
1.5	Industrial Ethernet Security.....	17
1.6	Configuration limits and performance data	18
1.6.1	General characteristic data	18
1.6.2	Characteristic data CloudConnect	18
1.6.3	Characteristics of S7 communication	19
1.6.4	Characteristic data for OUC and FETCH/WRITE	19
1.6.5	Characteristic data for FTP / FTPS mode.....	21
1.6.6	Characteristics of security - firewall rules	21
1.7	Software requirements	22
1.8	Hardware requirements (CPUs)	22
2	LEDs, connectors.....	23
2.1	LEDs	23
2.2	Gigabit interface.....	25
3	Installation, wiring, commissioning, operation	27
3.1	Important notes on using the device	27
3.1.1	Notes on use in hazardous areas	27
3.1.2	Notes on use in hazardous areas according to ATEX / IECEx	28
3.1.3	Notes on use in hazardous areas according to UL HazLoc and FM	29
3.2	Installing and connecting up	30
3.3	Commissioning - Downloading the configuration data	31
3.4	Operating mode of the CPU: Reaction of the CP	32
4	Configuration	33
4.1	STEP 7 Professional.....	33
4.2	Security recommendations	33
4.3	Restricting communications services in the CPU	36
4.4	IP configuration	37
4.4.1	Points to note about IP configuration.....	37
4.4.2	Restart after detection of a duplicate IP address in the network	37
4.4.3	IP routing.....	38

4.4.4	Programmed connections: Restriction of firewall rules.....	38
4.5	Time-of-day synchronization.....	39
4.6	SNMP.....	40
4.7	FTP server configuration.....	41
4.7.1	Configuring the FTP server function.....	41
4.7.2	Layout and structure of the FTP configuration list.....	43
4.7.3	FTPS access.....	43
4.8	CloudConnect.....	44
4.8.1	Configuration.....	44
4.8.1.1	Notes on data structuring and configuration.....	44
4.8.1.2	Configuration rules.....	45
4.8.1.3	Overview of configuration.....	46
4.8.1.4	"CloudConnect" parameter group.....	47
4.8.1.5	Onboarding in MindConnect IoT Extension.....	49
4.8.1.6	Operand areas and tags.....	50
4.8.2	Parameters of the topics / groups.....	50
4.8.2.1	Configuring topics or groups.....	50
4.8.2.2	Configuring the data points.....	51
4.8.2.3	Data types.....	52
4.8.2.4	Trigger.....	53
4.8.2.5	User data format.....	57
4.8.3	Properties dialog of the topics.....	61
4.8.3.1	Quality of Service (QoS).....	61
4.9	Security.....	61
4.9.1	Security user.....	62
4.9.2	Firewall.....	62
4.9.2.1	Firewall sequence when checking incoming and outgoing frames.....	62
4.9.2.2	Notation for the source IP address (advanced firewall mode).....	62
4.9.2.3	HTTP and HTTPS not possible with IPv6.....	62
4.9.3	Online functions.....	63
4.9.3.1	Online security diagnostics via port 8448.....	63
4.9.3.2	Settings for online security diagnostics and downloading to station with the firewall activated.....	63
4.9.4	Log settings - Filtering of the system events.....	64
4.9.5	Certificate manager.....	64
4.9.5.1	Certificates.....	64
4.9.5.2	Handling certificates.....	64
5	Program blocks.....	67
5.1	Program blocks for communication.....	67
5.2	Changing the IP address during runtime.....	71
5.3	Block for the FTP client function.....	72
5.3.1	FTP_CMD.....	72
5.3.2	Input parameter - FTP_CMD.....	73
5.3.3	Job blocks for FTP_CMD.....	75
5.3.4	Output parameters and status information FTP_CMD.....	80
5.3.5	Structure of the data blocks (file DB) for FTP client operation.....	84

6	Diagnostics and maintenance	87
6.1	Diagnostics options.....	87
6.2	Connect online	88
6.3	Diagnostics with SNMP.....	89
6.4	Update firmware.....	91
6.5	Replacing a module without a programming device.....	94
7	Technical specifications	95
7.1	Technical specifications	95
7.2	Pinout of the Ethernet interface	96
7.3	Permitted cable lengths - Ethernet	96
7.4	Permitted cable lengths - Gigabit Ethernet	96
8	Approvals.....	97
9	Dimension drawings.....	103
A	Syslog messages.....	105
	Index.....	109

Application and functions

1.1 Application

Application

The CP is intended for operation in an S7-1500 automation system. The CP enables the S7-1500 to be connected to Industrial Ethernet and to a cloud system.

With a combination of different security measures such as firewall and protocols for data encryption, the CP protects the S7-1500 or even entire automation cells from unauthorized access. It also protects the communication between the S7 station and communications partners from spying and manipulation.

1.2 Communication services

Communications services

The CP supports the following communication services:

- **Open User Communication (OUC)**

Open User Communication supports the following communications services via the CP using programmed or configured communications connections:

- ISO transport (complying with ISO/IEC 8073)
- TCP (according to RFC 793), ISO-on-TCP (according to RFC 1006) and UDP (according to RFC 768)

With the interface via TCP connections, the CP supports the socket interface to TCP/IP available on practically every end system.

- Multicast over UDP connection

Multicast operation is enabled via IP addressing during connection configuration.

- E-mail

Send e-mail to an e-mail server via SMTP (port 25) or SMTPS (port 587) with authentication.

For the blocks, see section Program blocks (Page 67).

- **MQTT**

MQTT for connecting the S7-1500 to a cloud system. For information on the communication functions and cloud systems, see section Cloud communication (Page 14).

- **S7 communication**
 - PG communication
 - Operator control and monitoring functions (HMI communication)
 - Data exchange over S7 connections
- **FTP/FTPS**

FTP functions (File Transfer Protocol) for file management and access to data blocks on the CPU

 - FTP server
 - Can be activated via the configuration
 - FTP client
 - Configurable via program blocks.
 - For the blocks, see section Program blocks (Page 67).
- **E-mail**

See above (OUC).
- **HTTP/HTTPS**
 - Web server of the CPU: Monitoring devices and process data with HTTP/HTTPS
 - If you do not require the function, you can disable it in the STEP 7 configuration and disable port 80 ("Access to the Web server" parameter group).
- **FETCH/WRITE**

FETCH/WRITE services as server (corresponding to S5 protocol) via ISO transport, ISO-on-TCP and TCP connections

The S7-1500 with the CP is always the server (passive connection establishment).

The fetch or write access (client function with active connection establishment) is performed by a SIMATIC S5 or a third-party device / PC.

You will find detailed information on configuring the communication functions in the STEP 7 help system.

1.3 Cloud communication

Protocols for the cloud connection

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

- MQTT
 - According to OASIS standard version 3.1 / 3.1.1

Cloud systems and communication functions

The CP supports the connection to cloud systems that support broker functionality with the MQTT protocol.

The configuration of cloud access ("Cloud operator") is adapted to communication with the following cloud systems:

- MindSphere (Siemens)
 - Service: MindConnect IoT Extension
 - Function of the CP:
 - Publisher
- Other cloud
 - Profile for another cloud system
 - Function of the CP:
 - Publisher
 - Subscriber
 - Possible cloud systems are:
 - AWS (Amazon)
 - Service: IoT Core
 - Azure (Microsoft)
 - Service: IoT Hub
 - IBM Cloud (IBM)
 - Service: Watson IoT Platform

1.4 Further functions

Time-of-day synchronization with NTP (Network Time Protocol)

The CP sends timeofday queries at regular intervals to an NTP server and synchronizes its local time of day.

The time is also be forwarded automatically to the CPU modules in the S7 station allowing the time to be synchronized in the entire S7 station.

The CP supports NTP (secure) for secure time transmission.

Addressable with the factoryset MAC address

To assign the IP address to a new CP (direct from the factory), it can be accessed using the preset MAC address on the interface being used. Online address assignment is made in STEP 7.

SNMP agent

The CP supports data queries over SNMP in version V1 (Simple Network Management Protocol). It delivers the content of MIB objects according to the MIB II standard and Automation System MIB.

The CP supports SNMPv3 when security functions are activated.

IP configuration (IPv4 / IPv6)

- The CP supports the use of IP addresses according to IPv4 and IPv6.
- You can configure how and with which method the CP is assigned the IP address, the subnet mask and the address of a gateway.
- The IP configuration and the connection configuration (IPv4) can also be assigned to the CP by the user program, see section Program blocks (Page 67). Does not apply to S7 connections.

IP routing

The CP supports static IP routing (IPv4) to other CMs/CPs.

For details, see section IP routing (Page 38).

IPv6 addresses - area of use on the CP

An IPv6 address can be used for the following communication services:

- FTP server mode
- FTP client mode with addressing via a program block
- E-mail transfer with addressing via a program block

Access to the Web server of the CPU

Via the LAN interface of the CP, you have access to the Web server of the CPU. With the aid of the Web server of the CPU, you can read out module data from a station. "Access to the Web server" can be activated for the Ethernet interface in the configuration.

Refer to the documentation for the Web server; see section Preface (Page 3)

Note

Web server access via HTTPS

The Web server of a SIMATIC S7-1500 station is located in the CPU. For this reason, when there is secure HTTPS access to the Web server of the station using the IP address of the CP, the SSL certificate of the CPU is displayed.

S5/S7 addressing mode for FETCH/WRITE

The addressing mode can be configured for FETCH/WRITE access as S7 or S5 addressing mode. The addressing mode specifies how the position of the start address is identified during data access. The S7 addressing mode applies only to data blocks (DBs).

Read the additional information in the online help of STEP 7.

1.5 Industrial Ethernet Security

All-round protection - the task of Industrial Ethernet Security

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. The data transfer from the external network connected to the CP can be protected various security measures:

- Data espionage (FTPS, HTTPS)
- Data manipulation
- Unauthorized access

Secure underlying networks can be operated via additional Ethernet/PROFINET interfaces implemented by the CPU or additional CPs.

Security functions of the CP for the S7-1500 station

As result of using the CP, the following security functions are accessible to the S7-1500 station on the interface to the external network:

- Firewall
 - IP firewall with stateful packet inspection (layer 3 and 4)
 - Firewall also for "non-IP" frames according to IEEE 802.3 (layer 2)
 - Limitation of the transmission speed
 - Global and user-specific firewall rules

The protective function of the firewall can be applied to the operation of single devices or several devices, as well as entire network segments.

- Logging

To allow monitoring, events can be stored in log files that can be read out using STEP 7 or can be sent automatically to a Syslog server.
- FTPS (explicit mode)

For encrypted transfer of files.
- NTP (secure)

For secure time-of-day synchronization
- SMTPS

For secure transfer of e-mails via port 587

1.6 Configuration limits and performance data

- **SNMPv3**
For secure transmission of network analysis information safe from eavesdropping
Observe the information in section Security recommendations (Page 33).

1.6 Configuration limits and performance data

1.6.1 General characteristic data

Characteristic	Explanation / values
Total number of freely usable connections on Industrial Ethernet	118 The value applies to the total number of connections of the following types: <ul style="list-style-type: none">• S7 connections• Connections for open communications services• FTP (FTP client)

Note

Connection resources of the CPU

Depending on the CPU type, different numbers of connection resources are available. The number of connection resources is the decisive factor for the number of configurable connections. This means that the values that can actually be achieved may be lower than specified in this section describing the CP.

1.6.2 Characteristic data CloudConnect

Number of connections to the cloud

- **Number of sessions with the broker**
Max. 1 session

Amount of process data for the cloud connection

- **Tags in the data area of S7 CPUs**
 - Max. 500 tags

Number of topics/groups

- **Number of configurable topics or groups**
 - Max. 500

1.6.3 Characteristics of S7 communication

S7 communication provides data transfer via the ISO Transport or ISO-on-TCP protocols.

Characteristic	Explanation / values
Total number of freely usable S7 connections on Industrial Ethernet	Max. 118
LAN interface - data field length generated by CP per protocol data unit (PDU = protocol data unit)	<ul style="list-style-type: none"> • For sending: 480 bytes / PDU • For receiving: 480 bytes / PDU
Number of reservable OP connections *	Max. 4
Number of reservable PG connections *	Max. 4
Number of HTTP connections for Web	Max. 4

* The CPU reserves connection resources. Take the specified values into account for programmed connections also.

Note

Maximum values for an S7-1500 station

Depending on the CPU you are using, there are limit values for the S7-1500 station. Note the information in the relevant documentation.

1.6.4 Characteristic data for OUC and FETCH/WRITE

Open User Communication (OUC) provides access to communication over TCP, ISO-on-TCP, ISO transport and UDP connections.

The following characteristics are important (OUC + FETCH/WRITE):

Characteristic	Explanation / values
Number of connections	<p>Number of configured and programmed connections (ISO transport + ISO-on-TCP + TCP + UDP + FETCH/WRITE + e-mail):</p> <ul style="list-style-type: none"> • Max. 118 in total <p>Of which maximum:</p> <ul style="list-style-type: none"> – TCP connections: 0...118 ¹⁾ – ISO-on-TCP connections: 0...118 – ISO transport connections: 0...118 – UDP connections (specified and free) in total: 0...118 – Connection for e-mail: 0...1 – Connections for FETCH/WRITE: 0...16 <p>Notes: ¹⁾Avoid receive overload The flow control on TCP connections cannot control permanent overload of the recipient. You should therefore make sure that the processing capabilities of a receiving CP are not permanently exceeded by the sender (approximately 150200 messages per second).</p>
Maximum data length for program blocks	<p>Program blocks allow the transfer of user data in the following lengths:</p> <ul style="list-style-type: none"> • ISO-on-TCP, TCP, ISO transport: 1 to 64 kB • UDP: 1 byte to 2 KB • E-mail <ul style="list-style-type: none"> – Job header + user data: 1 to 256 bytes – E-mail attachment: up to 64 kB
LAN interface max. data field length generated by CP per protocol data unit (TPDU = transport protocol data unit)	<ul style="list-style-type: none"> • sending <ul style="list-style-type: none"> ISO transport, ISOonTCP, TCP: 1452 bytes / TPDU • receiving <ul style="list-style-type: none"> – ISO transport: 512 bytes / TPDU – ISO-on-TCP: 1452 bytes / TPDU – TCP: 1452 bytes / TPDU

Note

Connection resources of the CPU

Depending on the CPU type, different numbers of connection resources are available. The number of connection resources is the decisive factor for the number of configurable connections. This means that the values that can actually be achieved may be lower than specified in this section describing the CP.

You will find detailed information on the topic of connection resources in the "Communication" function manual, refer to the section Preface (Page 3).

Restrictions for UDP

- Restrictions UDP broadcast / multicast
To avoid overloading the CP due to high broadcast / multicast frame traffic, the receipt of UDP broadcast / multicast on the CP is limited
- UDP frame buffering
Length of the frame buffer: At least 7360 bytes
Following a buffer overflow, newly arriving frames that are not fetched by the user program are discarded.

1.6.5 Characteristic data for FTP / FTPS mode

TCP connections for FTP

FTP actions are transferred from the CP over TCP connections. The following characteristics apply:

- FTP client mode
You can use a maximum of 32 FTP sessions.
Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).
- FTP server mode
You can operate a maximum of 16 FTP sessions at the same time.
Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).

Program block FTP_CMD for FTP client mode

For communication, use the program block FTP_CMD.

The block execution time in FTP depends on the reaction times of the partner and the length of the user data. A generally valid statement is therefore not possible.

1.6.6 Characteristics of security - firewall rules

Firewall rules (advanced firewall mode)

The maximum number of firewall rules in advanced firewall mode is limited to 256.

The firewall rules are divided up as follows:

- Maximum 226 rules with individual addresses
- Maximum 30 rules with address ranges or network addresses (e.g. 140.90.120.1 - 140.90.120.20 or 140.90.120.0/16)
- Maximum 128 rules with limitation of the transmission speed ("bandwidth limitation")

1.7 Software requirements

Software for configuration and online functions

To configure and use the CP, the following configuration tool is required:

- STEP 7 Professional V15.1
 - + Update 3
 - + Support Package of CP 1545-1 V1.0

1.8 Hardware requirements (CPUs)

Compatible CPUs

The CP can be used with the following CPUs:

- S7-1500

All CPUs that can be configured in STEP 7 as of firmware version V2.0 from the following series:

- Standard CPUs (CPU 15xx)
- Compact CPUs (CPU 15xxC)

Compatible communications modules

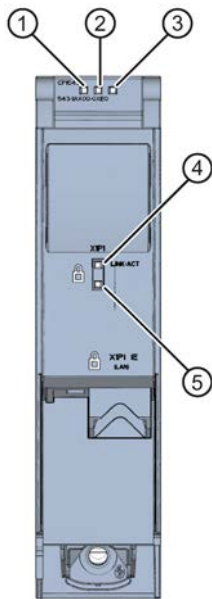
The CP 1545-1 can be used in a rack beside a CP 1543-1 or CM 1542-1.

The CP 1545-1 cannot be used as a replacement part for a CP 1543-1.

LEDs, connectors

2.1 LEDs

LEDs



- ① RUN LED
- ② ERROR LED
- ③ MAINT LED
- ④ LINK/ACT LED
- ⑤ Reserve LED

Figure 2-1 LED display of the CP 1545-1 (without front cover)

Meaning of the LED symbols

The LED symbols in the following tables have the following significance:




























Green LED	Red LED	Yellow LED	Description
□	□	□	LED off
■	■	■	LED on (continuous)
☀	☀	☀	LED flashes

2.1 LEDs

Meaning of the LED displays

The CP has the following 3 LEDs to display the current operating status and the diagnostics status: The table shows the meaning of the various combinations of LED states.









Table 2- 1 Meaning of the LEDs "RUN", "ERROR", "MAINT"

RUN (green)	ERROR (red)	MAINT (yellow)	Meaning
			No supply voltage on the CP or supply voltage too low
			LED test during startup
			CP startup
			CP is in RUN mode. No disruptions.
			A diagnostics event has occurred.
			Maintenance demanded
			Downloading the user program
			<ul style="list-style-type: none"> Missing or incomplete CP configuration Loading firmware
			Module fault (LEDs flashing synchronized)

Meaning of the LED displays of the Ethernet interface X1 P1

The LED LINK/ACT (green/yellow) indicates the status and the activity of the port of the Ethernet interface:

Table 2- 2 Meaning of the "LINK/ACT" LED

LINK/ACT		Meaning
 green off	 yellow off	No connection to Ethernet No Ethernet connection between CP and communication partner No sending / receiving of data via Ethernet
 flashing green	 yellow off	"LED flash test", see STEP 7 help ("Hardware diagnostics")
 green on	 yellow off	Connection to Ethernet Existing Ethernet connection between CP and communication partner
 green on	 flickers yellow	Send / receive data via Ethernet

2.2 Gigabit interface

Ethernet interface with gigabit specification and security access

The CP has an Ethernet interface according to the gigabit standards IEEE 802.3. The Ethernet interface supports autocrossing, autonegotiation and autosensing.

The Ethernet interface allows a secure connection to external networks via a firewall. The CP provides the following protective function:

- Protection of the S7-1500 station in which the CP is operated;
- Protection of the underlying company networks connected to the other interfaces of the S7-1500 station.

You will find the pin assignment of the sub RJ-45 jack in section Pinout of the Ethernet interface (Page 96).


Installation, wiring, commissioning, operation


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.


3.1 Important notes on using the device

3.1.1 Notes on use in hazardous areas

 WARNING
EXPLOSION HAZARD
Do not open the device when the supply voltage is turned on.

 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 (see IEC 60664-1).

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

3.1 Important notes on using the device

 **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 50 to 60 °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.

3.1.2 Notes on use in hazardous areas according to ATEX / IECEx

 **WARNING**

DIN rail

In the ATEX and IECEx area of application only the Siemens DIN rail 6ES5 710-8MA11 may be used to mount the modules.

 **WARNING**

Requirements for the cabinet/enclosure

To comply with EC Directive 2014/34 EU (ATEX 114) or the conditions of IECEx, this enclosure or cabinet must meet the requirements of at least IP54 (in compliance with EN 60529) according to EN 60079-7.

 **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**

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

 **WARNING**

LAN connection (Local Area Network)

A LAN or LAN segment with all the interconnected devices should be contained completely in a single low voltage power distribution system in a building. The LAN is designed either for "Environment A" according to IEEE802.3 or "Environment 0" according to IEC TR 62102.

Do not connect any electrical connectors directly to the telephone network (Telephone Network Voltage) or a WAN (Wide Area Network).

3.1.3

Notes on use in hazardous areas according to UL HazLoc and 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**


Do not remove or replace while circuit is live when a flammable or combustible atmosphere is present.


 **WARNING**


Explosion hazard


Do not disconnect equipment when a flammable or combustible atmosphere is present.

3.2 Installing and connecting up

 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
Substitution of components may impair suitability of the equipment.

 WARNING
Substitution of components may impair suitability for Division 2.

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

3.2 Installing and connecting up

Installation and connecting up

 WARNING
Read the system manual "S7-1500 Automation System" Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System", see Preface (Page 3).
Power supply off Make sure that the power supply is turned off when installing/uninstalling the devices.

Procedure installation and connection

1. When installing and connecting up, keep to the procedures described for installing I/O modules in the system manual "S7-1500 Automation System".
2. Connect the CP to the Industrial Ethernet via the RJ-45 socket (bottom side of the CP).
For the pin assignment of the Ethernet interface, see section Pinout of the Ethernet interface (Page 96).
3. Switch on the power supply of the S7 station.
4. Close the front covers of the modules.
During operation, keep the hinged front panel closed.

3.3 Commissioning - Downloading the configuration data

Requirement: Complete configuration

Commissioning the CP fully is only possible if the STEP 7 project data of the station is complete.

Download

The remaining steps in commissioning involve downloading the STEP 7 project data.

The CP is supplied with the relevant configuration data by downloading the configuration data to the CPU.

The configuration data can be downloaded to the CPU via a memory card or any Ethernet/PROFINET interface of the S7-1500 station. To load the station via Ethernet, connect the engineering station on which the project data is located to the Ethernet interface of the CPU.

You will find more detailed information on loading in the following sections of the STEP 7 online help:

- "Compiling and loading project data"
- "Using online and diagnostics functions"

3.4 Operating mode of the CPU: Reaction of the CP

Switching the CPU: RUN → STOP

You can switch the operating mode of the CPU between RUN and STOP via STEP 7.

Note

RUN/STOP LED of the CP

The green RUN/STOP LED of the CP continues to be lit green regardless of the STOP mode of the CPU.

In the STOP state of the CPU, the CP remains in the RUN state. The following behavior applies to the CP:

- This applies to established connections (ISO Transport, ISO-on-TCP, TCP, UDP):
 - Programmed connections are retained.
 - Configured connections are terminated.
- The following functions remain enabled:
 - Configuration and diagnostics of the CP
 - System connections for configuration, diagnostics and PG channel routing still exist.
 - Web diagnostics
 - S7 routing function
 - Time-of-day synchronization

Configuration

4.1 STEP 7 Professional

Configuration in STEP 7

You perform the configuration of the CP in STEP 7 Professional.

You will find the required STEP 7 version in the section Software requirements (Page 22).

4.2 Security recommendations

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

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Check regularly for new features on the Siemens Internet pages.
 - Here you can find information on Industrial Security:
Link: (<http://www.siemens.com/industrialsecurity>)
 - Here you can find information on security industrial communication:
Link: (<http://w3.siemens.com/mcms/industrial-communication/en/ie/industrial-ethernet-security/Seiten/industrial-security.aspx>)
 - You can find a publication on the topic of network security (6ZB5530-1AP0x-0BAx) here. Link:
(https://w3app.siemens.com/mcms/infocenter/content/en/Pages/order_form.aspx?nodeKey=key_518693&infotype=brochures&linkit=null)
Enter the following filter: 6ZB5530
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.

Information regarding product news and new firmware versions is available at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/dl>)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the PC directly to the Internet. If a connection from the CP to the Internet is required, enable the security functions or arrange for suitable protection before the CP, for example a SCALANCE S with firewall.

Security functions of the product

Use the options for security settings in the configuration of the product. These includes among others:

- Protection levels
Configure access to the CPU under "Protection and Security".
- Security function of the communication
 - Enable the security functions of the CP and set up the firewall.
If you connect to public networks, you should use the firewall. Think about the services you want to allow access to the station via public networks. By using the "bandwidth restriction" of the firewall, you can restrict the possibility of flooding and DoS attacks.
The FETCH/WRITE functionality allows you to access any data of your PLC. The FETCH/WRITE functionality should not be used in conjunction with public networks.
 - Use the secure protocol variants HTTPS, FTPS, NTP (secure) and SNMPv3.
 - Use the program blocks for secure OUC communication (Secure OUC).
 - Leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CP disabled.
- Protection of the passwords for access to program blocks
Protect the passwords stored in data blocks for the program blocks from being viewed. You will find information on the procedure in the STEP 7 information system under the keyword "Know-how protection".
- Logging function
Enable the function in the security configuration and check the logged events regularly for unauthorized access.

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.

- Make sure that all passwords are protected and inaccessible to unauthorized personnel. See also the preceding section for information on this.
- Do not use one password for different users and systems.

Protocols

Secure and non-secure protocols

- Only activate protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.
- Deactivate DHCP at interfaces to public networks such as the Internet, for example, to prevent IP spoofing.

Table: Meaning of the column titles and entries

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 status**
 - Open
The port is always open and cannot be closed.
 - Open after configuration
The port is open if it has been configured.
 - Open (login, when configured)
As default the port is open. After configuring the port, the communications partner needs to log in.
 - Open with block call
The port is only opened when a suitable program block is called.
- **Authentication**
Specifies whether or not the protocol authenticates the communications partner during access.

4.3 Restricting communications services in the CPU

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
DCP	93 (UDP)	Open	Open	No
S7 and online connections	102 (TCP)	Open	Open *	No
Online security diagnostics	8448 (TCP)	Closed	Open after configuration	No
HTTP	80 (TCP)	Closed	Open after configuration	No
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
FTP	20 (TCP) 21 (TCP)	Closed	Open after configuration	No
FTPS	989 (TCP) 990 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)

* For information on avoiding opening port 102 during diagnostics, see section Online security diagnostics via port 8448 (Page 63).

Ports of communication partners and routers

Make sure that you enable the required client ports in the corresponding firewall on the communications partners and in intermediary routers.

These can be:

- Broker port
 - MQTT unsecured: 1883 (TCP)
 - MQTT via TLS: 8883 (TCP)

The port number can be set in the configuration.

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP) - Open in CP on block call (outgoing only)
- SMTPS / 587 (TCP) - Open in CP on block call (outgoing only)
- Syslog / 514 (UDP)

4.3 Restricting communications services in the CPU

Communications services without connections

The CPU can be a server for a series of communications services without connections being configured for the CPU. Other communications partners can access CPU data. This means that it is no longer possible for the local CPU to control communication with the clients.

The reliability of these communications services is set by the "Connection mechanisms" parameter in the "Protection & Security" parameter group of the CPU.

"Permit access with PUT/GET communication from remote partner"

- Option enabled

Access to CPU data from the client side is permitted.

- Option disabled

Read and write access to CPU data is only possible with communication connections that require configuration or programming both for the local CPU and for the communications partner.

Connections for which the local CPU is only a server (no configuration/programming of communication with the partner) are not possible.

The following communications services of the CP relate to a CPU \geq V2.

When the option is disabled, the following is not possible:

- PUT/GET access via the CP
- FETCH/WRITE access via the CP

When the option is disabled, the following is possible:

- FTP access via the CP

4.4 IP configuration

4.4.1 Points to note about IP configuration

Configured S7 and OUC connections cannot be operated if the IP address is assigned using DHCP

Note

If you obtain the IP address using DHCP, any S7 and OUC connections you may have configured will not work. Reason: The configured IP address is replaced by the address obtained via DHCP during operation.

4.4.2 Restart after detection of a duplicate IP address in the network

To save you timeconsuming troubleshooting in the network, during startup the CP detects double addressing in the network.

Behavior when the CP starts up

If double addressing is detected when the CP starts up, the CP changes to RUN and cannot be reached via the Ethernet interface. The ERROR LED flashes.

4.4.3 IP routing

IP routing via the backplane bus

The CP supports static IP routing (IPv4) to other CMs/CPs:

- CP 1545-1
- CM 1542-1 V2.0
- CP 1543-1 V2.0

IP routing runs via the configured default router.

You can use IP routing, for example, for Web server access by lower-level modules.

With IP routing, the data throughput is limited to 1Mbps. Remember this in terms of the number of modules involved and the expected data traffic via the backplane bus.

Configuration

You can activate the IP routing in STEP 7 via the following parameter:

"Ethernet interface > Ethernet addresses > IP routing between communication modules"

If you use several CPs in a station, only one of the modules in the station may be configured as a router.

When the security function is activated, additional IP firewall rules are created, which you can modify in advanced firewall mode of the Global Security settings.

4.4.4 Programmed connections: Restriction of firewall rules

Restrictions with programmed connections and configured security functions

In principle, it is possible to set up communications connections program-controlled using the program block TCON and at the same time by configuring the firewall.

Note

Partner IP addresses not in firewall rules

When configuring specified connections (active endpoints) in STEP 7, the IP addresses of the partners are not entered automatically in the firewall configuration.

4.5 Time-of-day synchronization

General rules

The CP supports the following mode for timeofday synchronization:

- NTP mode (NTP: Network Time Protocol)

Note**Recommendation for setting the time**

Synchronization with a external clock at intervals of approximately 10 seconds is recommended. This achieves as small a deviation as possible between the internal time and the absolute time.

Note**Special feature of time-of-day synchronization using NTP**

If the option "Accept time from non-synchronized NTP servers" is not selected, the response is as follows:

If the CP receives a time of day frame from an unsynchronized NTP server with stratum 16, the time of day is not set according to the frame. In this case, none of the NTP servers is displayed as "NTP master" in the diagnostics; but rather only as being "reachable".

Security

In the extended NTP configuration, you can create and manage additional NTP servers.

Note**Ensuring a valid time of day**

If you use security functions, a valid time of day is extremely important. If you do not obtain the time-of-day from the station (CPU), we therefore recommend that you use the NTP (secure) method.

Configuration

For more detailed information on configuration, refer to the STEP 7 online help of the "Time-of-day synchronization" parameter group.

4.6 SNMP

SNMP

The CP supports the following SNMP versions:

- **SNMPv1**

Available with security functions disabled.

Note that with this read and write access to the module is possible. In this case, other settings are not possible.

The configuration of the community strings is only possible if the security functions are enabled.

The CP uses the following community strings to authenticate access to its SNMP agent via SNMPv1:

Access to the SNMP agent in the CP	Community string for authentication in SNMPv1 *)
Read access	public
Read and write access	private

*) Note the use of lowercase letters!

Note

Security of the access

For security reasons, change the preset and generally known strings "public" and "private".

- **SNMPv3**

Available only when security functions are enabled

You can find additional details in the section Diagnostics with SNMP (Page 89).

Configuration

- **"Enable SNMP"**

If the option is enabled, communication via SNMPv1 is enabled on the CP.

If the option is disabled, queries from SNMP clients are not replied to by the CP either via SNMPv1 or via SNMPv3.

4.7 FTP server configuration

4.7.1 Configuring the FTP server function

CP configuration

Configure the FTP server function of the CP in the following parameter group.

- With security functions disabled: "FTP server configuration"
- With security functions enabled: "Security > FTP server configuration"

Requirements in the CPU configuration and programming

Use the following settings to allow FTP access:

- In the CPU configuration in "Protection & Security > Connection mechanisms":
Disable the option "Access via PUT/GET communication...".
- As file DBs create data blocks of the type "Array of byte".

S7-1500 CP as FTP server

The functionality described here allows you to transfer data in the form of files to or from an S7-1500 station using FTP commands. At the same time, the conventional FTP commands for reading, writing and managing files can also be used.

Access to the following data of the S7-1500 is possible:

- **Data blocks of the CPU**

Name of the directory:

/cpu1 / DBx

"DBx" is the name of the relevant data block e.g. DB10.

- **SIMATIC memory card of the CPU**

The function is supported as of the following firmware versions:

- CPU: V2.0
- CP 1543-1: V2.0
- CP 1545-1: V1.0

Name of the directory:

/mmc_cpu1

Access to the following folders of the SIMATIC memory card is possible:

- /DATALOGS
Directory for log files
- /RECIPES
Directory for recipe files

Note

FTP access to the SIMATIC memory card of the CPU: CPU STOP possible

Note that the cards have a limited capacity. If the memory space of the SIMATIC memory card is completely occupied due to storage of large amounts of data, the CPU changes to STOP.

- Use a card with adequate storage capacity.
- Avoid writing large amounts of data often to the SIMATIC memory card using FTP.

Reading/writing via DBs of the CPU

To transfer data with FTP via data blocks, create the required DBs in the CPU. Due to their special structure, these are known as file DBs.

When it receives an FTP command, the CP acting as FTP server queries its assignment table to find out how the data blocks used for file transfer in the CPU will be mapped to files. You make the data block assignment in the STEP 7 configuration of the CP (FTP configuration).

For information on the structure of the file DB, refer to section Structure of the data blocks (file DB) for FTP client operation (Page 84).

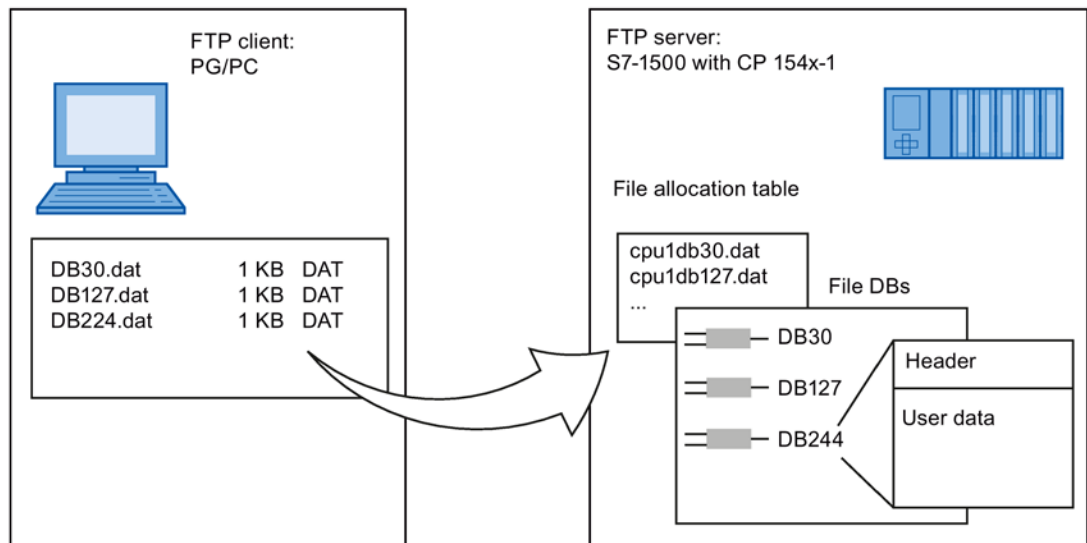


Figure 4-1 S7-CPU with CP 154x-1 as FTP server for the S7 CPU data

4.7.2 Layout and structure of the FTP configuration list

DB assignment in STEP 7

The fields of the table in the data block assignment in STEP 7 have the following meaning and syntax:

Column title	CPU	DB	File name	Comment
Meaning	Assignment of the CPU Selectable from drop-down list	No. of the data block (file DB) Selectable from drop-down list	The file name assigned to the file DB Automatic name proposal; entry can be edited.	Informal comment
Example	cpu1 [PLC_1]	20	cpu1_db20.dat	Measured values plant 1

Notes on the syntax

The following applies to the file name of a file DB:

- The file name begins with "cpuX" (where X=1 for S7-1500).

Note

Keep to the notation (lower case for "cpu" and no leading spaces at the start of the row). Otherwise, the files will not be recognized.

- Length: maximum 64 characters (including "cpuX")

4.7.3 FTPS access

FTPS access only with security functions enabled

FTPS access to the S7-1500 station as an FTP server is only possible if a user with suitable rights has been created in the STEP 7 project. This means that the security functions must be enabled on the CP. For this, security settings are available in the global user administration.

4.8 CloudConnect

4.8.1 Configuration

4.8.1.1 Notes on data structuring and configuration

Data structures

To access the process data for cloud communication, the CP accesses the DB tags of the CPU. The data that is referenced in the DB tag is configured in the CP via data points.

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

- Other cloud (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.
- Siemens MindSphere - MindConnect IoT Extension
 - Groups

A group can contain one or multiple data points.
You can create one or more groups.
 - Topic

All groups are permanently assigned to the standard topic "s/us" of the MindConnect IoT Extension.

Topic and group names

Configuration of the topic names:

- 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.

4.8.1.2 Configuration rules

Configuration rules

Observe the following rules for configuration:

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

Note

Consistency check of parameters for Publisher and Subscriber

If the CP 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 QualityCode of the message is "GOOD", the subscriber writes the received data into the data block of its CPU.

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

Recommendations

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

The later assignment and evaluation of the published data is facilitated if the names refer to the process data of the stations.

For example, by inserting forward slashes (/), you can create hierarchy levels for later evaluation by the subscriber.

- Example for topic/group names
You want to name a group or a topic "Motor5". The data is assigned to the S7 station "Station1".
For this example, the topic/group name "Station1/Motor5" would make sense.
- Example for data point names
"Plant1/Unit1/Aggregate1/DB1_Signal1"

Data points and DBs

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 blocks
 - In a CPU, create separate DBs only for the publisher function and only for the subscriber function.
- 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
 - Create a separate DB in the assigned CPU for each possible subscriber.
 - If a subscriber subscribes to data from multiple publishers, configure a different DB number for the respective DB intended for this subscriber in the CPUs of the different publishers.
 - This prevents tags from different publishers from having an identical data point name if the data point names use the DB number as part of the name.
- Subscriber
 - Create a separate DB for each publisher in the assigned CPU.

4.8.1.3 Overview of configuration

Configuring cloud access - Overview

1. To allow the cloud application to access the process image, create the required DBs and DB tags in the local CPU.
 - The data points of the topics/groups (see below) access these DB tags; see section Operand areas and tags (Page 50).
2. Create at least one user with the role "NET Administrator" in the Global Security settings.
3. First, configure the parameter group "Security > CloudConnect" for cloud access of the CP.

Activate cloud communication and select the cloud provider:

- Siemens MindSphere - MindConnect IoT Extension
- Other cloud

For the supported cloud providers, refer to the section Cloud communication (Page 14).

Configure the other parameters; see section "CloudConnect" parameter group (Page 47).

4. Then expand the project tree:
Station > Local modules > CP 1545-1 > Cloud connection
Depending on the cloud provider:
 - MindSphere
> "Groups"
Click "Add group".
 - Other cloud
> "Published topics" / "Subscribed topics"
Click "Add topic".Open the new group or topic with a double-click, insert data points and configure them.
5. Open the properties dialog of the topic / group via the "Properties" shortcut menu.
 - Configure the name and optional "Author" and "Comment" of the topic / group.
 - Configure the QoS parameter for topics ("Other cloud") . See section Quality of Service (QoS) (Page 61) for more on this.

4.8.1.4 "CloudConnect" parameter group

General

- **Activate CloudConnect**
Activates communication with a cloud system via the Ethernet interface of the CP.
- **Cloud provider**
Select the desired cloud provider:
 - Siemens MindSphere - MindConnect IoT Extension
 - Other cloud (profile for other cloud system)
- **Device name**
Validity: MindConnect IoT Extension only
For the meaning, see Onboarding in MindConnect IoT Extension (Page 49).
- **Scan cycle of tags**
Cycle (ms) in which the DB tags of the CPU are queried.
Take note of the effects on the transferred data volume, see section Trigger (Page 53).
- **Topics with time stamp**
When this option is enabled, the current time stamp is added to each value at the time of each publication.

Broker configuration

- **MQTT / MQTT via TLS**

Alternatively, select one of the following protocol variants:

- MQTT (unencrypted transmission)
- MQTT via TLS (encrypted transmission)

- **Minimum TLS version**

Defines the TLS version used by the CP and the partner.

- **Broker certificate**

The parameter is only active when you have enabled encrypted transmission "MQTT via TLS". In this case, you need a certificate from your cloud provider.

Default setting: "Automatic". With the "Automatic" setting, a certificate from the trusted certificates is assigned.

To manually assign the certificate, follow these steps.

- Import the partner certificate:

Global security settings > Certificate manager > Trusted certificates > right mouse click

- Assign the certificate to the CP:

Select certificate in the "Trusted certificates" list > right mouse click

The certificate appears in the "Certificates of the partner devices" list on the CP in the parameter group "Security > Certificate manager".

- Now select the imported certificate in the "Broker certificate" drop-down list.

- **Broker address**

Address of the broker server (IPv4 address or host name)

- **Broker port**

Port number of the broker server

- Port 1883 is preset for unencrypted transmission (MQTT).
- Port 8883 is preset for encrypted transmission (MQTT via TLS).

- **Client ID**

Enter the client ID that was assigned by your service provider or that you defined.

Max. 23 characters from the ASCII band (hex) 0x20 .. 0x7F

- **Clean session**

When this 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.

Broker monitoring

- **Keepalive interval**

Monitoring time of the connection with the broker

If no further data is available for transmission within the configured time after the data is sent, the CP sends a keep-alive frame to the broker.

Changes to the value after commissioning are applied after "Download to device" and voltage OFF → ON.

Broker authentication

- **Enable authentication**

When this option is enabled, the connection to the broker is established with authentication. If possible, use TLS to transmit the 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 that was assigned by your service provider or that you defined.

4.8.1.5 Onboarding in MindConnect IoT Extension

Device parameters

With a connection to Siemens MindSphere - MindConnect IoT Extension, two parameters are used to identify your device during the Onboarding process once the connection is established between the CP and MindConnect IoT Extension.

- **Device Name**

Assign the name in the parameter group "Security > CloudConnect > General" of the CP.

The CP is registered with the Onboarding process under this name.

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

- **Device Type**

The parameter cannot be configured and is permanently set with the following string:

– c8y_MQTTDevice

The parameter is required in MindConnect IoT Extension to determine the device type.

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/25625>)

4.8.1.6 Operand areas and tags

Operand area

Tags from the following operand areas of the CPU can be used for the transfer of data of the S7 station:

- Data block (global DB)

Note during the configuration in the properties dialog of the DB:

- Enable the attribute "DB accessible from OPC UA".

Configuring the DB tags

When configuring the DB tags, note the following:

- Enable the option "Accessible from HMI/OPC UA".
- Enable the option "Writable from HMI/OPC UA".

Required for write access

You can find the data types that can be used for the cloud connection in the section Data types (Page 52).

4.8.2 Parameters of the topics / groups

4.8.2.1 Configuring topics or groups

Configuration under different cloud operators

By selecting the cloud provider, you determine whether topics or groups are configured for the data transmission:

- MindConnect IoT Extension

You can create several groups.

A group can contain multiple data points.

In IoT Extension, a group corresponds to the structure characteristic "Series". All groups are permanently assigned to the standard topic "s/us".

- Other Cloud

You can create several topics.

A topic can contain multiple data points.

4.8.2.2 Configuring the data points

Inserting data points in a topic / group

After creating a topic or a group, click in the "PLC tag" cell of the first free line of the table.

Select the desired DB tag of a DB of the CPU via the object selection dialog. For the DB tags, see Operand areas and tags (Page 50).

The DB tag is transferred to the table as a data point, the properties and parameters are displayed below.

The table lists all configurable data points.

Configuring data points

- **Name**
Configured name of the data point
- **PLC tag**
Configured name of the DB tag
- **Data type**
Configured data type of the data point
For the supported data types, see Data types (Page 52).
- **Attribute**
⇒ Validity: MindConnect IoT Extension
The attribute is applied to the user data as <ADDITIONAL_ATTRIBUTE>; see section User data format (Page 57).
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/s²
 - % = 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/m²)

Other compound units of the SI system can also be specified, for example:

m/h, m/s, m, km, mW, kW, mWh, mA, VArh

4.8.2.3 Data types

Supported data types

The table lists the configurable data types.

Table 4- 1 Data types available for Cloud access

S7 data types type (bits / bytes)	<DATAPOINT_TYPE> *
Bool (1)	BOOL
Byte (8)	UINT8
Char (8)	CHAR
USInt (8)	UINT8
Int (16)	INT16
UInt (16)	UINT16
Word (16)	UINT16
Real (32)	SINGLE_FLOAT
DWord (32)	UINT32
DInt (32)	INT32
UDInt (32)	UINT32
LReal (64)	DOUBLE_FLOAT
String (2..256 Char)	S7_STRING
Date_And_Time (8)	S7_DT
DTL (12)	S7_DTL

* <DATAPOINT_TYPE> indicates the data type on publication.

For the publication of the useful data and the tag, <DATAPOINT_TYPE> see section User data format (Page 57).

4.8.2.4 Trigger

Time and volume of the transmitted data

Requirements for the transmission of data to the 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 transfer

You specify the time when the values of data points are transferred to the broker for each data point with the "Trigger".

Volume of transferred data

The following data is transferred together to the broker as soon as the value of a data point is pending for transfer:

- Other cloud
Transfer values of all data points of a topic
- MindConnect IoT Extension
Transfer values of all data points of a group

Duration of transfer (value trigger)

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.

Note

Transfer in "Scan cycle of tags"

When the trigger condition of a value trigger is met, the data is transferred to the broker with each scan cycle of tags.

You configure the "scan cycle of tags" on the CP in the parameter group "Security > CloudConnect".

Trigger

You use the triggers to specify the conditions that initiate transmission of the saved value to the Cloud or the broker.

Up to two trigger types can be selected per tag:

- **Time trigger**

- Cyclic
- Time (daily / weekly / monthly)

- **Value trigger**

The following trigger types can be selected:

- Deviation (transfer on deviation)
- Threshold LOW / Threshold HIGH
- Range inside / Range outside

See below for the meaning.

You can combine a time trigger and a value trigger per tag. When configuring two types of triggers, both have the same validity.

As soon as one of the two trigger conditions is met, the transfer is triggered.

Not all trigger types can be combined for a tag in practice. The following trigger combinations are supported:

Permitted trigger combinations	
Trigger 1	Trigger 2
Cyclic	Value trigger
Time	-
Value trigger	Cyclic

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

Trigger types

Time trigger

- Cyclic

Cyclic transmission - configurable in milliseconds

The value is transmitted cyclically.

- 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.

Note:

If a month has fewer days than the configured day (e.g. the 31st), no value is transferred at the end of the month.

Value trigger

For all value triggers, note the value range of the data type of the respective data point. The respective trigger value is configured depending on the value range.

- Deviation

The value is transferred as soon as it deviates by the configured amount from the last value stored in the CPU.

The transfer is triggered on occurrence of the following conditions:

- New value > (last saved value + positive deviation)
- New value < (last saved value - positive deviation)
- New value > (last saved value - negative deviation)
- New value < (last saved value + negative deviation)

Configuration of the value 0 (zero) is not permitted.

- Threshold LOW

The value is transferred as soon as it drops below the configured value.

The transfer is triggered on occurrence of the following conditions:

- New value < configured threshold LOW

- Threshold HIGH

The value is transferred as soon as it exceeds the configured value.

The transfer is triggered on occurrence of the following conditions:

- New value > configured threshold HIGH

- Range within

The value is transferred as soon as it is inside the configured range.

The transfer is triggered on occurrence of the following conditions:

- Low range limit < New value < High range limit

- Range outside

The value is transferred as soon as it is outside the configured range.

The transfer is triggered on occurrence of the following conditions:

- Low range limit > New value
- High range limit < New value

The value ranges of the value triggers depend on the data type of the data point.

Data and trigger types

Not every data type supports all the trigger types. The table lists the configurable data types and specifies the supported trigger types for each data type.

- Trigger types marked with "x" are supported.
- Trigger types marked with "-" are not supported.

Table 4- 2 Trigger support of data types

S7 data type type (bits / bytes)	Supported triggers	
	Time trigger	Value trigger
Bool (1)	x	x (only value 0)
Byte (8)	x	x
Char (8)	x	x
USInt (8)	x	x
Int (16)	x	x
UInt (16)	x	x
Word (16)	x	x
Real (32)	x	x
DWord (32)	x	x
DInt (32)	x	x
UDInt (32)	x	x
LReal (64)	x	x
String (2..256 Char)	x	-
Date_And_Time (8)	x	-
DTL (12)	x	-

Value ranges of the data types

Threshold values are configured for the trigger types "Deviation", "Threshold LOW", "Threshold HIGH", "Range within" and "Range outside".

The most important data types that are suitable for threshold triggers have the following value ranges:

- USInt: 0...255
- Int: -32768...32767
- UInt: 0...65535
- DInt: -2147483648...+2147483647
- UDInt: 0...4294967295
- Real: 1.175495e-38...3.402823e+38

Value ranges of S7 analog input modules

With an integer (Int: 0...32767), 270 corresponds to about 1 % of the raw value of an S7 analog input module (27648 = 100 %).

4.8.2.5 User data format

User data format

Different cloud systems use a different format of user data. The user data are output in the following formats:

- MindConnect IoT Extension
Format for the connection to MindSphere (Siemens) / IoT Extension ("Cloud operator" parameter)
- JSON
Format for the connection to Other Cloud ("Cloud provider" parameter)
Cloud services that expect JSON format for processing topics.
- XML
(not used)

The CP uses the UTF-8 character encoding for formatting the user data.

User data format - MindConnect IoT Extension

```
<DATAPOINTS_BEGIN> SEPARATOR=\\n>200,<DATAPOINT_NAME>,<GROUP>,<DATAPOINT_VALUE>,  
<ADDITIONAL_ATTRIBUTE>,<DATAPOINT_QUALITY_CODE><DATAPOINTS_END>
```

User data format - JSON PubSub (Other cloud)

```
{ "Timestamp": "<PUBLISH_TIMESTAMP>", "DataItems": [  
<DATAPOINTS_BEGIN> SEPARATOR=,\\n>: { "Variable": "<DATAPOINT_NAME>",  
"Type": "<DATAPOINT_TYPE>", "Value": "<DATAPOINT_VALUE>",  
"QualityCode": "<DATAPOINT_QUALITY_CODE>" }  
<DATAPOINTS_END> ] }
```

Code components

The code for formatting the user data consists of the components listed below.

The following description of the individual code components is structured as follows:

- **Code component**
 - <Syntax>
 - Meaning
 - Examples (not for all components)

Code components: Syntax and meaning

- **Time stamp**

<PUBLISH_TIMESTAMP>

Meaning: Time of the publication

– Example:

Syntax: "<PUBLISH_TIMESTAMP>"

Results in string: "2018-08-20T13:58:16.192313634+00:00"

- **Start of data with separators**

<DATAPOINTS_BEGIN>

Start of a text block that is repeated for sending data.

"<DATAPOINTS_BEGIN>" must be listed before "<DATAPOINTS_END>" (end of the text block, see below).

"SEPARATOR=" is a separator character, "\" is a masking character and the second "\" is a placeholder for the "Backslash" separator. The character combination separates the individual user data by a backslash.

– Example for the transmission of data:

Syntax: "<DATAPOINTS_BEGIN> SEPARATOR=\\n>200,<DATAPOINT_NAME>,<GROUP>,<DATAPOINT_VALUE>,<DATAPOINTS_END>"

Results in: Character string with backslash as separator between the values and after the last sent value.

- **200**

<200>

Function code (MindConnect IoT Extension)

- **Data point / Tag**

<DATAPOINT_NAME>

Name of the data point

- **Group**

<GROUP>

Group Name

- **Value**

<DATAPOINT_VALUE>

Value of the data point

- **Attribute**

<ADDITIONAL_ATTRIBUTE>

Attribute (MindConnect IoT Extension)

- **Data type**

<DATAPOINT_TYPE>

Data type of the data point output by the device

For the output of the data types, see section Operand areas and tags (Page 50).

- **QualityCode**

<DATAPOINT_QUALITY_CODE>

Quality status of the value

See below for the meaning.

- **End of data**

<DATAPOINTS_END>

End of data transfer

Example of transferred user data (JSON PubSub)

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

The topic contains three tags 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 tags.

```
{ "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" } ] }
```

QualityCode

Transmission and QualityCode

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

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

- **GOOD**

The value is valid.

- **BAD**

The value of the tag is not valid or not current. Possible causes:

- CPU in STOP
- Value not current
- Error while reading the tag

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

- Publisher → Cloud

The publication of CP messages as a publisher is independent of the value of the status.

- Cloud → Subscriber

The receipt of messages by the CP as a 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 CPU by the CP as subscriber.

Connection abort and QualityCode

The behavior on a connection abort is as follows:

- **Connection abort between CP and CPU**

- During the connection abort

The CP sends the topic with empty strings for the values and the QualityCode "BAD".

- Recurring connection

When the trigger condition is met, the CP sends the topic with the current values and the QualityCode "GOOD".

- **Connection abort between CP and cloud**

- During the connection abort - Cable at CP pulled

The CP does not send data.

- During the connection abort - Cloud server cannot be reached

The CP sends the last valid values once with the QualityCode "GOOD".

- Recurring connection

For the behavior, see the following section.

Data buffering and QoS

In the event of a connection abort between the CP and cloud server, the CP saves the last 16 data frames of a group or topic with "QoS" = 1 or 2 in its frame memory.

The frame memory has a capacity of 16. It operates chronologically; in other words, the oldest data is sent first (FIFO principle). As of the 17th data frame, the oldest data frame in the frame memory is overwritten.

Recurring cloud connection

Depending on the configured QoS value, the following behavior is in effect for a recurring connection between CP and cloud server.

- QoS = 0

The CP sends the current values with the quality "Good".

- QoS = 1 / 2

The CP sends the saved values with the quality "Good".

Afterwards, the current values are sent after the trigger conditions are triggered.

4.8.3 Properties dialog of the topics

4.8.3.1 Quality of Service (QoS)

Properties of a topic - Quality of Service (QoS)

The parameter becomes accessible when you expand the CP in the navigation area under the local modules and open the properties dialog of a topic via the shortcut menu.

- **Required Quality of Service (QoS)**

This is where you define the desired transmission behavior (Quality of Service) of this topic.

The configured value should be fulfilled by the broker if possible. Check which reaction is performed by the broker you use if it does not meet the required QoS level. Some brokers select the level closest to the required level in this case. Other brokers output an error message.

- QoS 0

Transfer no more than once

The CP sends the topic once to the broker. The CP does not expect an acknowledgment.

If the topic is not received by the broker, it is lost.

- QoS 1

Transfer at least once

The CP sends the topic to the broker until it receives a PUBACK packet as acknowledgment from the broker.

- QoS 2

Transfer exactly once

The CP 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.

4.9 Security

You will find an overview of the range and use of the security functions in section Industrial Ethernet Security (Page 17).

For the configuration limits of the security functions refer to the section Characteristics of security - firewall rules (Page 21).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 62).

4.9.1 Security user

Creating a security user

You need the relevant configuration rights to be able to configure security functions. For this purpose, you need to create at least one security user with the corresponding rights.

Navigate to the global security settings > "User and roles" > "Users" tab.

1. Create a user with the associated parameters such as authentication mode, session duration, etc.
2. Assign this user the role "NET Standard" or "NET Administrator" in the area below "Assigned roles".

After logging on, this user can make the necessary settings in the STEP 7 project.

In the future, continue to log on as this user when working on security parameters.

4.9.2 Firewall

4.9.2.1 Firewall sequence when checking incoming and outgoing frames

Each incoming or outgoing frame initially runs through the MAC firewall (layer 2). If the frame is discarded at this level, it is not checked by the IP firewall (layer 3). This means that with suitable MAC firewall rules, IP communication can be restricted or blocked.

4.9.2.2 Notation for the source IP address (advanced firewall mode)

If you specify an address range for the source IP address in the advanced firewall settings of the CP, make sure that the notation is correct:

- Separate the two IP addresses only using a hyphen.
Correct: 192.168.10.0-192.168.10.255
- Do not enter any other characters between the two IP addresses.
Incorrect: 192.168.10.0 - 192.168.10.255

If you enter the range incorrectly, the firewall rule will not be used.

4.9.2.3 HTTP and HTTPS not possible with IPv6

It is not possible to use HTTP and HTTPS communication on the Web server of the station using the IPv6 protocol.

If the firewall is enabled in the local security settings in the entry "Firewall > Predefined IPv6 rules": The selected check boxes "Allow HTTP" and "Allow HTTPS" have no function.

4.9.3 Online functions

4.9.3.1 Online security diagnostics via port 8448

Security diagnostics via port 8448

Requirement: Access to the Web server of the CP is activated via HTTPS.

If you want to perform security diagnostics in STEP 7 Professional, follow the steps below:

1. Select the CP in STEP 7.
2. Open the "Online & Diagnostics" shortcut menu.
3. In the "Security" parameter group, click the "Connect online" button.

In this way, you perform the security diagnostics via port 8448.

4.9.3.2 Settings for online security diagnostics and downloading to station with the firewall activated

Setting the firewall for online functions

With the security functions enabled, follow the steps outlined below:

1. In the global security settings (see project tree), select the entry "Firewall > Services > Define services for IP rules".
2. Select the "ICMP" tab.
3. Insert a new entry of the type "Echo Reply" and another of the type "Echo Request".
4. Now select the CP in the S7 station.
5. Enable the advanced firewall mode in the local security settings of the CP in the "Security > Firewall" parameter group.
6. Open the "IP rules" parameter group.
7. In the table, insert a new IP rule for the previously created global services as follows:
 - Action: Allow; "From external -> To station " with the globally created "Echo request" service
 - Action: Allow; "From station -> to external" with the globally created "Echo reply" service
8. For the IP rule for the Echo Request, enter the IP address of the engineering station in "Source IP address". This ensures that only ICMP frames (ping) from your engineering station can pass through the firewall.

4.9.4 Log settings - Filtering of the system events

Communications problems if the value for system events is set too high

If the value for filtering the system events is set too high, you may not be able to achieve the maximum performance for the communication. The high number of output error messages can delay or prevent the processing of the communications connections.

In "Security > Log settings > Configure system events", set the "Level:" parameter to the value "3 (Error)" to ensure the reliable establishment of the communications connections.

4.9.5 Certificate manager

4.9.5.1 Certificates

Assignment of certificates

If you use communication with authentication for the CP, you need to import certificates of the communications partners into the STEP 7 project and download them to the CP with the configuration data.

1. Import third-party certificates of all communications partners using the certificate manager in the global security settings.
2. Then assign the certificates of all its communications partners to the CP, either:
 - Using the "Trusted certificates and root certification authorities" table in the global security settings
 - Using the "Certificates of the partner devices" table in the local certificate manager of the module (security)

In this table, also include the certificates of communications partners whose certificates were generated in the same STEP 7 project.

For a description of the procedure, refer to the section Handling certificates (Page 64).

4.9.5.2 Handling certificates

Certificate for authentication

If you have configured secure communication with authentication for the CP, own certificates and certificates of the communications partner will be required for communication to take place.

All nodes of a STEP 7 project with enabled security functions are supplied with certificates. The STEP 7 project is the certification authority.

Note

No certificate with security functions disabled.

If the security functions of the CP are disabled in the STEP 7 project, no certificate will be generated for the CP.

A certificate is created for every application of the CP that requests a certificate. It is shown in STEP 7 in "Global security settings > Certificate manager > Device certificates". As well as additional information, you will find the respective usage of the certificate there (service/application).

You can call up more information about the certificate by selecting the certificate in the table and selecting the shortcut menu "Show".

So that the CP can communicate with non-Siemens partners when the security functions are enabled, the relevant certificates of the partners must be exchanged during communication. To supply the CP with third-party certificates, follow the steps below:

1. Importing third-party certificates from communications partners
 - ⇒ Global security settings of the project (certificate manager)
2. Assigning certificates, either:
 - Global security settings > Certificate manager > "Trusted certificates and root certification authorities"
 - Local security settings of the CP > Certificate manager > "Certificates of the partner devices"

The steps are described in the following sections.

Importing third-party certificates from communications partners

Import the certificates of the communications partners of third-party vendors using the certificate manager in the global security settings of the STEP 7 project. Follow the steps outlined below:

1. Save the third-party certificate in the file system of the PC of the connected engineering station.
2. In the STEP 7 project open the global certificate manager:
 - Global security settings > Certificate manager
3. Open the "Trusted certificates and root certification authorities" tab.
4. Click in a row of the table can select the shortcut menu "Import".
5. In the dialog that opens, import the certificate from the file system of the engineering station into the STEP 7 project.

Assigning certificates in the global security settings

Import the partner certificate via: Global security settings > Certificate manager > Trusted certificates > right mouse click. Assign the certificate to the CP (select certificate > right mouse click).

1. Open the "Trusted certificates and root certification authorities" tab.
2. Select the desired certificate.
3. Select "Assign" in the shortcut menu (right mouse button).
4. Select the desired module in the subsequent dialog.

After the assignment, the certificate appears in the "Certificates of the partner devices" table in the local certificate manager of the module.

Assigning certificates locally

To be able to use an imported certificate for the CP, it needs to be displayed in the "Security" parameter group of the CP.

In this table, also include the certificates of communications partners whose certificates were generated in the same STEP 7 project.

Proceed as follows to import:

1. In the STEP 7 project select the CP.
2. Navigate to the parameter group "Security > Certificate manager".
3. In the table, double-click on the cell with the entry "<Add new>".

The "Certificate manager" table of the Global security settings is displayed.

4. In the table, select the required third-party certificate and to adopt it click the green check mark below the table.

The selected certificate is displayed in the local table of the CP.

Exporting certificates for applications of third-party vendors (e.g. logging server)

For communication with applications of third-party vendors, the third-party application generally also requires the certificate of the CP.

You export the certificate of the CP for communications partners from third-party vendors in much the same way as when importing (see above). Follow the steps outlined below:

1. In the STEP 7 project open the global certificate manager:
Global security settings > Certificate manager
2. Open the "Device certificates" tab.
3. In the table select the row with the required certificate and select the shortcut menu "Export".
4. Save the certificate in the file system of the PC of the connected engineering station.

Now you can transfer the exported certificate of the CP to the system of the third-party vendor.

Certificate for logging server

If you use a logging server in your system, export the SSL certificate for the authentication of the CP on the server.

Change certificate: Subject Alternative Name

STEP 7 adopts the properties "DNS name", "IP address", and "URI" of the "Subject Alternative Name" (SAN) parameter from the STEP 7 configuration data.

You can change this parameter of a certificate in the certificate manager of the global security settings. To do this, select the a certificate in the table of device certificates and call the shortcut menu "Renew". Properties of the parameter "Alternative name of the certificate owner" changed in STEP 7 are not adopted by the STEP 7 project.

Program blocks

5.1 Program blocks for communication

Using the program blocks

The program blocks (instructions) listed below can be used for communication between S7 stations.

Communication via program blocks is not configured. The configurable program blocks are available as an interface in your STEP 7 user program.

You will find details on the program blocks in the information system of STEP 7.

Recommendation: If possible, use the current version of a module.

Note

Different program block versions

Note that in STEP 7 you cannot use different versions of a program block in a station.

Supported program blocks for Open User Communication (OUC)

You can find the program blocks in STEP 7 in the "Instructions > Communication > Open User Communication" task card.

The following blocks are available:

- **TSEND_C / TRCV_C**

Compact blocks for:

- Connection establishment / termination and sending data
- Connection establishment / termination and reception of data

Use alternatively blocks for connection setup / disconnection and separate blocks for sending / receiving data:

- **TCON / TDISCON**

Connection establishment / connection termination

- **TUSEND / TURCV**

Sending and receiving data via UDP

- **TSEND / TRCV**

Sending and receiving data via TCP or ISOonTCP

- **TMAIL_C**

Sending e-mails

To transfer encrypted e-mails, the precise time of day is required on the CP. Configure the time-of-day synchronization.

For changing configuration data of the CP during runtime:

- **T_CONFIG**

Program-controlled configuration of the IP parameters

Refer to the information on T_CONFIG and on the SDTs "IF_CONF_..." in the section Changing the IP address during runtime (Page 71).

Note

Requirement in the CP configuration

To be able to change the IP parameters program controlled, the option "IP address is set directly at the device" must be enabled in the configuration of the IP address of the Ethernet interface of the CP.

Block for the FTP client of the CP

You can find the program blocks in STEP 7 in the "Instructions > Communication > Communication processor > SIMATIC NET CP".

- **FTP_CMD**

Block for the FTP client function

Setting up FTP connections and transferring files to and from an FTP server

Refer to the description in the section Block for the FTP client function (Page 72).

Connection descriptions in system data types (SDTs)

The blocks listed above use the CONNECT parameter for the relevant connection description.

TMAIL_C uses the parameter MAIL_ADDR_PARAM.

The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

Create the SDT required for every connection description as a data block (global DB).

The SDT type is generated by entering the name in the declaration table of the block manually not by selecting an entry from the "Data type" drop-down list but by entering it in the "Data type" box for example "TCON_IP_V4". The corresponding SDT is then created with its parameters.

Using the SDTs

- **TCON_IP_v4**

For transferring data via TCP or UDP

- **TCON_QDN**

For TCP or UDP communication via the fully qualified domain name (FQDN)

- **TCON_IP_RFC**

For transferring data via ISO-on-TCP (direct communication between two S7 stations)

- **TADDR_Param**

For transferring data via UDP

- **TMail_V4**

For transferring e-mails addressing the e-mail server using an IPv4 address

- **TMail_V6**

For transferring e-mails addressing the e-mail server using an IPv6 address

- **TMail_FQDN**

For transferring e-mails addressing the e-mail server using its name (FQDN)

For secure transfer:

- **TCON_IP_V4_SEC**

For the secure transfer of data via TCP or UDP

- **TCON_QDN_SEC**

For secure TCP or UDP communication via the fully qualified domain name (FQDN)

- **TMail_V4_SEC**

For secure transfer of e-mails addressing the e-mail server using an IPv4 address

- **TMail_V6_SEC**

For secure transfer of e-mails addressing the e-mail server using an IPv6 address

- **TMail_QDN_SEC**

For secure transfer of e-mails addressing the e-mail server using the host name

You will find the description of the SDTs with their parameters in the STEP 7 information system under the relevant name.

Connection establishment and termination

Connections are established using the program block TCON. Note that a separate program block TCON must be called for each connection.

A separate connection must be established for each communications partner even if identical blocks of data are being sent.

Connection can be terminated after successful data transmission. A connection is also terminated by calling TDISCON.

Note

Connection abort

If an existing connection is aborted by the communications partner or due to disturbances on the network, the connection must also be terminated by calling TDISCON. Make sure that you take this into account in your programming.

Program blocks - overview

The following program blocks (instructions) are available for the CP.

Table 5- 1 Blocks of the Open User Communication

Protocol	Program block (instruction)	System data type
TCP	<ul style="list-style-type: none"> TSEND_C/TRCV_C or	<ul style="list-style-type: none"> TCON_IP_v4 TCON_Configured
ISO-on-TCP	<ul style="list-style-type: none"> TCON/TDISCON + TSEND/TRCV 	<ul style="list-style-type: none"> TCON_IP_RFC
ISO		<ul style="list-style-type: none"> TCON_ISOnative
UDP	<ul style="list-style-type: none"> TCON/TDISCON + TUSEND/TURCV 	<ul style="list-style-type: none"> TCON_IP_v4
E-mail	<ul style="list-style-type: none"> TMAIL_C 	<ul style="list-style-type: none"> TMAIL_V4 TMAIL_V6 TMAIL_V6_SEC

Table 5- 2 Block for communication services of the CP

Protocol	Program block (instruction)	System data type
FTP	<ul style="list-style-type: none"> FTP_CMD 	<ul style="list-style-type: none"> FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME FTP_FILENAME FTP_FILENAME_PART

Table 5- 3 Block for configuration of the Ethernet interface or an NTP/DNS server

Function	Program block (instruction)	System data type
Configuration of the Ethernet interface	<ul style="list-style-type: none"> T_CONFIG 	<ul style="list-style-type: none"> IF_CONF_V4 IF_CONF_V6 IF_CONF_NTP IF_CONF_DNS IF_CONF_MAC

5.2 Changing the IP address during runtime

Changing address parameters during runtime

You can change the following address parameters of the CP at runtime controlled by the program:

- IP address
- Subnet mask
- Router address

Program-controlled changing of the IP parameters is supported by program blocks. The program blocks access address data stored in a suitable system data type (SDT).

Apart from the address parameters of the CP, with T_CONFIG the address parameters of DNS servers (IF_CONF_DNS) and NTP servers (IF_CONF_NTP) can also be changed program controlled.

The following program blocks and system data types can be used:

- **T_CONFIG**

Together with SDT:

- IF_CONF_V4
- IF_CONF_V6
- IF_CONF_MAC
- IF_CONF_DNS
- IF_CONF_NTP

The address parameters can only be configured with temporary validity in the CP. In the respective "IF_CONF_..." SDT, the "Mode" = 2 parameter must be set.

Note**No feedback from the CP**

"T_CONFIG" does not support feedback from the CP to the CPU. Errors in the block call or in setting the address parameter are not reported. The block outputs "BUSY" or "DONE" regardless of whether the address parameter was set.

You will find detailed information on programming the blocks in the STEP 7 information system.

Requirements in the CP configuration

To be able to change the IP parameters program controlled, the option "IP address is set directly at the device" must be enabled in the configuration of the IP address of the Ethernet interface of the CP.

5.3 Block for the FTP client function

5.3.1 FTP_CMD

FTP_CMD

You will find the block in STEP 7 in the "Instructions" task card under "Communication > Communications processor > SIMATIC NET CP" when the Main [OB1] is open.

Using the FTP_CMD instruction, you can establish FTP connections and transfer files from and to an FTP server.

Data transfer is possible using FTP or FTPS (secure SSL connections).

Note

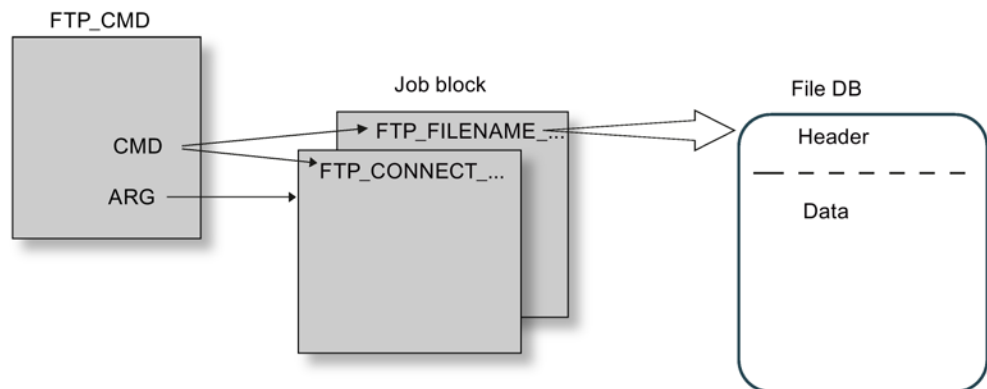
FTPS: Comparing certificates

FTPS requires a comparison of the certificates between FTP server and FTP client. If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server. Import the certificate of the FTP server as a trusted certificate in the certificate manager.

How it works

The FTP_CMD instruction references a job block (ARG) in which the FTP command is specified. Depending on the type of FTP command (CMD), this job block uses different data structures for parameter assignment. Suitable data types (UDTs) are available for these various structures.

The following diagram shows the call structure:



Job blocks

The following data structures are used for the job blocks:

- Connection establishment

Various data structures are available for the connection establishment using the following types of access:

- FTP_CONNECT_IPV4: Connection establishment with IP addresses according to IPv4

- FTP_CONNECT_IPV6: Connection establishment with IP addresses according to IPv6
- FTP_CONNECT_NAME: Connection establishment with server name (DNS)
- Data transfer
 - For the data transfer, two different data structures are available:
 - FTP_FILENAME: Data structure for access to a complete file
 - FTP_FILENAME_PART: Data structure for read access to a data area

Data transfer in the file DB

The data transfer is achieved using data blocks containing a header for job data and the area for the user data. The data block is specified in the job buffer.

You will find the description of an example file DB in the STEP 7 information system.

5.3.2 Input parameter - FTP_CMD

Explanation of the input parameters

You supply the FTP_CMD instruction with the following input parameters:

Table 5- 4 Formal parameters of the FTP_CMD instruction - input parameters

Parameter	Declaration	Data type	Memory area	Meaning / remarks
REQ	Input	BOOL	E, A, M, DB, L	Starts the send job on a rising edge.
ID *	INPUT	INT	1, 2 ... 64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
CMD *	INPUT	BYTE	See following table "Commands".	FTP command to be executed when the instruction is called. You will find value ranges for the FTP command types after the table. The FTP command specified here must be specified identically in the job block (ARG parameter). If a command is not supported by the CP firmware, an error message with STATUS = 8F6BH is output.
ARG *	INPUT	VARIANT	See following table "Commands".	Job block References the data area with the execution parameters suitable for the FTP command. Specific data types (UDT) are used depending on the FTP command. The UDTs are shown below. The ANY data type is not permitted for the pointer to be specified here!

* The values of the input parameters "ID" and "CMD" overwrite the value of the input parameter "ARG".

FTP commands in the "CMD" parameter

The following table shows you the significance of the commands of the "CMD" parameter and which UDTs you use to supply the job blocks.

Table 5- 5 Command types

CMD (command type)	Relevant job blocks / UDT	Meaning / handling
0 (NOOP)	*	The called FB does not execute any actions. The status codes are set as follows when these parameters are supplied: DONE=1; ERROR=0; STATUS=0
1 (CONNECT)	FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME	FTP connection establishment With this command, the FTP client establishes an FTP connection to an FTP server (port 21). The connection is available under the connection ID specified here for all further FTP commands. Data is then exchanged with the FTP server specified for this user.
2 (STORE)	FTP_FILENAME	This function call transfers a data block (file DB) from the FTP client (S7-CPU) to the FTP server. Caution: If the file (file DB) already exists on the FTP server, it will be overwritten.
3 (RETRIEVE)	FTP_FILENAME	This function call transfers a file from the FTP server to the FTP client (S7-CPU). Caution: If the data block (file DB) on the FTP client already contains a file, it will be overwritten.
4 (DELETE)	FTP_FILENAME	With this function call, you delete a file on the FTP server.
5 (QUIT)	*	With this function call, you close the FTP connection specified in "ID".
6 (APPEND)	FTP_FILENAME	Similar to "STORE", the "APPEND" command saves a file on the FTP server. With "APPEND", the file on the FTP server is, however, not overwritten. The new content is appended to the existing file. If the file (file DB) does not exist on the FTP server, it will be created.
7 (RETR_PART)	FTP_FILENAME_PART	Using the "RETR_PART" command (retrieve part) , you can request a section of a file from the FTP server. If very large files are involved, this allows you to restrict the read to the part you currently require. To do this, you need to know the structure of the file. Enter the required part of the file using the two parameters "OFFSET" and "LEN" in FB40.

* With the command types 0 (NOOP) and 5 (QUIT) a freely selectable job block (UDT) must be specified. This is not evaluated.

5.3.3 Job blocks for FTP_CMD

Meaning

You supply the FTP_CMD instruction with a job block using the ARG parameter. The structure depends on the FTP command type. By using the default data types (UDT), the instruction recognizes the type of the job block. Below, you will find the relevant data types (UDTs) for the following job blocks:

- FTP connection establishment with IP address according to IPv4
- FTP connection establishment with IP address according to IPv6
- FTP connection establishment with server name
- Write and read access and other FTP commands
- FTP command RETR_PART

Job block for FTP connection establishment with IP address according to IPv4

For FTP connection establishment with IP address according to IPv4, the following data structure is used.

Table 5- 6 FTP_CONNECT_IPV4

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPCmd	BYTE	1	FTP command "CONNECT" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 73). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server.
UserName	STRING[32]	'benutzer'	User name for the login on the FTP server

5.3 Block for the FTP client function

Parameter	Type	Range of values	Meaning / remarks
Password	STRING[32]	'password'	Password for the login on the FTP server
FTPserverIPAddr	IP_V4	ADDR(1) ... ADDR(4)	IP address of the FTP server as Array[1..4] of Byte, where 1 byte specifies one block of the address. Example: ADDR(1) specifies the first address block (the first byte of the address).

Job block for FTP connection establishment with IP address according to IPv6

For FTP connection establishment with IP address according to IPv6, the following data structure is used.

Table 5- 7 FTP_CONNECT_IPV6

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPCmd	BYTE	1	FTP command "CONNECT" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 73). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server.
UserName	STRING[32]	'user'	User name for the login on the FTP server
Password	STRING[32]	'password'	Password for the login on the FTP server
FTPserverIPAddr	IP_V6	ADDR(1) ... ADDR(16)	IP address of the FTP server as Array[1..16] of Byte, where 2 bytes specify one block of the address. Example: ADDR(1) + ADDR(2) specify the first address block.

Job block for FTP connection establishment with server name

For FTP connection establishment specifying the server name, the following data structure is used. The server name is assigned to an IP address using DNS.

Table 5- 8 FTP_CONNECT_NAME

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPcmd	BYTE	1	FTP command "CONNECT" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 73). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server.
UserName	STRING[32]	'benutzer'	User name for the login on the FTP server
Password	STRING[32]	'passwort'	Password for the login on the FTP server
FTPserverName	STRING[254]		IP address of the FTP server

Job block for write and read access and other FTP commands

The following data structure is used for the FTP commands store, retrieve, delete and append.

Table 5- 9 FTP_FILENAME

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPcmd	BYTE	2, 3, 4, 6	FTP command "STORE / RETRIEVE / DELETE / APPEND" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 73). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server.
DataBlockNumber	UINT		The data block specified here contains the file DB to be read / written.
LenFilename	UINT	0...1000	The "LenFilename" parameter for specifying the total length of the file name is not evaluated. Instead the length information in the string of the "Filename" parameter is evaluated.
Filename	ARRAY[0..3] OF STRING[254]		File name of the destination or source file. The four strings for the file name are concatenated and transferred to the server as a complete string.

Job block for the RETR_PART FTP command

The following data structure is used for the RETR_PART FTP command.

Table 5- 10 FTP_FILENAME_PART

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPcmd	BYTE	7	FTP command "RETR_PART" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 73). The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP Client, the certificate must be imported from the FTP server.
Offset	DWORD		Offset in bytes starting at which the file will be read.
Length	DWORD		Sublength in bytes that is read starting at the value specified in "OFFSET". Special features: <ul style="list-style-type: none"> If "DW#16#FFFFFFFF" is specified, the available rest of the file will be read. Result OK (DONE = 1, STATUS = 0) if no other error occurred. When OFFSET > length of the original file: Length of the destination file (ACT_LENGTH in file DB): 0 bytes on the CPU. Result OK (DONE = 1, STATUS = 0) if no other error occurred. When OFFSET + LEN > length of the original file (and LEN ≠ 0xFFFFFFFF): Length of the destination file (ACT_LENGTH in file DB): Available bytes starting at "OFFSET". Result OK (DONE = 1, STATUS = 0) if no other error occurred.

5.3 Block for the FTP client function

Parameter	Type	Range of values	Meaning / remarks
DataBlockNumber	UINT		The data block specified here contains the file DB to be read / written.
LenFilename	UINT	0...1000	The "LenFilename" parameter for specifying the total length of the file name is not evaluated. Instead the length information in the string of the "File-name" parameter is evaluated.
Filename	ARRAY[0..3] OF STRING[254]		File name of the destination or source file.

FTP access using the FTP_CMD instruction - parameters for command types NOOP and QUIT

Supply the FTP_CMD with a reference to a job block with the following command types as well:

CMD = 0 (NOOP)

CMD = 5 (QUIT)

The content of the job block is not evaluated when these command types execute, the type (UDT) of the specified job block is therefore unimportant.

Note

Response if the reference to the FTP job block is missing

If this reference is not supplied, the command is not executed. The instruction remains blocked in an apparent execution status without any feedback to the user program on the interface.

5.3.4 Output parameters and status information FTP_CMD

Parameters BUSY, DONE and ERROR

You control the execution status with the parameters BUSY, DONE, ERROR and STATUS. The BUSY parameter indicates the processing status. With the DONE parameter, you check whether or not a job was correctly executed. The ERROR parameter is set if errors occur during execution of "FTP_CMD". Error information is output in the STATUS parameter.

The following table shows the relationship between the parameters BUSY, DONE and ERROR:

BUSY	DONE	ERROR	Description
1	-	-	The job is being processed.
0	1	0	The job was completed successfully.
0	0	1	The job was terminated with an error. The cause of the error is specified in the STATUS parameter.
0	0	0	No new job was assigned.

Evaluating status codes

Note**Evaluation**

- Evaluation for BUSY = 0

Do not evaluate the status displays until BUSY = 0.

- Status 8FxxH

For entries coded with status 8FxxH, refer to the information in the STEP 7 Standard and System Functions reference manual. The chapter describing error evaluation with the RET_VAL output parameter contains detailed information.

Table 5- 11 FTP_CMD: Meaning of the STATUS parameter in conjunction with DONE and ERROR

DONE	ERROR	STATUS	Meaning
0	0	0000H	No job is being executed.
1	0	0000H	the job was completed without error.
0	0	7001H	The job was initiated for the first time.
0	0	7002H	Job still running.
0	1	80C4H	Communication error (occurs temporarily, it is usually best to repeat the job in the user program).
0	1	8183H	The configuration does not match the job parameters.
0	1	8401H	Unknown error Possible causes: <ul style="list-style-type: none"> • A timeout was detected on the connection. • The FTP server has aborted the connection. Remedy: Send the QUIT and CONNECT commands again to re-establish the connection.
0	1	8402H	The connection has an error status. The timeout of the connection may have been exceeded or the FTP server may have terminated the connection. Remedy: Send the QUIT and CONNECT commands to re-establish the connection.
0	1	8403H	Login has failed.
0	1	8404H	FTP server is not obtainable.
0	1	8405H	Transfer has failed.
0	1	8406H	Timeout for current action
0	1	8407H	File was not found on the FTP server.
0	1	8408H	Transfer not possible.
0	1	8409H	File could not be fetched.
0	1	8410H	Setting the TCP port for the data connection has failed.
0	1	8411H	Offset information does not match.
0	1	8412H	Error changing the specified directory
0	1	8413H	Error receiving data

5.3 Block for the FTP client function

DONE	ERROR	STATUS	Meaning
0	1	8414 _H	Error sending data
0	1	8415 _H	Specified CMD (command type) was rejected by the client.
0	1	8416 _H	Connection was closed by the FTP server.
0	1	8418 _H	Error in the user data. Possible causes: <ul style="list-style-type: none"> • File name is empty. • Data length is "0". • etc.
0	1	8419 _H	There is no socket resource available to open a data connection.
0	1	8420 _H	There is no socket resource available to open a control connection.
0	1	8421 _H	Error opening the file DB to be read
0	1	8422 _H	Error opening the file DB to be written
0	1	8423 _H	Connection establishment to the FTP server has failed.
0	1	8424 _H	Internal error
0	1	8425 _H	Format error in the domain name
0	1	8426 _H	There are too many DNS queries pending.
0	1	8427 _H	The specified DNS server could not assign the specified domain name.
0	1	8428 _H	There is no connection resource available.
0	1	8429 _H	Unknown channel ID
0	1	8430 _H	The file DB is too short.
0	1	8431 _H	Error when writing to the file DB.
0	1	8432 _H	Error when reading from the file DB.
0	1	8433 _H	Error when accessing the file DB.
0	1	8434 _H	Action was aborted.
0	1	8435 _H	Channel will be reset.
0	1	8436 _H	Unexpected server reply
0	1	8437 _H	Certificate could not be verified.
0	1	8438 _H	Unknown error occurred.
0	1	8439 _H	The FTP command causes an error. The cause must be looked for on the FTP server (REST command).
0	1	8440 _H	The FTP server does not support the requested SSL protocol.
0	1	8446 _H	After the FTP password was sent to the FTP server, an unexpected code was returned by the FTP server.
0	1	8451 _H	An error was signaled when attempting to change the transmission mode from binary to ASCII.
0	1	8455 _H	A memory request has failed on the CM/CP.
0	1	8460 _H	A problem has occurred handling SSL/TLS.
0	1	8469 _H	Interface error The specified output interface could not be used. Remedy: Set the interface to be used for outgoing connections.
0	1	8475 _H	The SSL certificate or the SSH md5 fingerprint was not considered trusted.

DONE	ERROR	STATUS	Meaning
0	1	8476 _H	Nothing was received from the FTP server. In the current status, an incorrect response must be assumed.
0	1	8477 _H	The specified "Crypto engine" (cryptographic module) was not found.
0	1	8478 _H	The attempt to set the selected SSL "Crypto engine" as the default failed.
0	1	8480 _H	A problem has occurred with the certificate of the FTP client.
0	1	8481 _H	The specified number could not be used.
0	1	8482 _H	The FTP server uses a coding that is not supported.
0	1	8484 _H	The maximum file size was exceeded.
0	1	8485 _H	The file DB was modified while being processed to be sent or the file DB is incorrectly structured.
0	1	8489 _H	Data could not be sent. There is not enough memory available for the action on the FTP server.
0	1	8492 _H	The file already exists. The file will not be overwritten.
0	1	8496 _H	A problem occurred reading the SSL CA certificate.
0	1	8497 _H	An unexpected error occurred in the SSH session.
0	1	8498 _H	It was not possible to terminate the SSL connection.
0	1	8499 _H	The socket is not ready for sending/receiving. Wait until it is ready and try again.
0	1	8501 _H	The SSL certificate check by the FTP server has failed.
0	1	8507 _H	A timeout has occurred establishing the connection during the active FTP session while waiting for the FTP server.
0	1	8F54 _H	The "EXIST" bit in the file DB header is not set.
0	1	8F55 _H	Header status bit: Locked
0	1	8F56 _H	The NEW bit in the file DB header was not reset
0	1	8F6B _H	<p>Possible causes:</p> <ul style="list-style-type: none"> • Bad value for the CMD parameter Values from 0 to 15 are permitted. • An FB40 command is not supported. <p>Possible cause: Incorrect firmware of the CP</p> <p>Remedy: Firmware update (with older CPs, use the functions FC 40...FC 44 instead of FB 40.)</p>
0	1	8F7F _H	Internal error, for example, illegal ANY reference.

5.3.5 Structure of the data blocks (file DB) for FTP client operation

How it works

To transfer data with FTP, create data blocks (file DBs) on the CPU of your S7 station. These data blocks must have certain structure to allow them to be handled as transferable files by the FTP services. They consist of the following sections:

- Section 1: File DB header (has a fixed length of 20 bytes)
- Section 2: User data as "Array [..] of Byte" or "Array [..] of Char" (has a variable length and structure)

Data consistency

Make sure that you do not access the same file DB more than once at the same time.

Creating a file DB

1. Create a new data block in STEP 7.
2. Open the block editor.
3. In the block editor of the DB, select the line you want to use as the start line for the file DB.
4. In the "Data type" column, enter the type "FILE_DB_HEADER" using the keyboard.
A data structure with the header structure required for the file DB is created.
5. Set the "WRITEACCESS" parameter to "true" to enable access.
6. Enter a value for the length of the user data at the "MAX_LENGTH" parameter.
7. Below this, create a data field of the type "Array [..] of Byte" or "Array [..] of Char" for the user data to be sent.

The size of the field must match the specification of "MAX_LENGTH" in the header.

File DB header for FTP client mode

The file DB header described here is identical to the file DB header described for server mode.

Parameter	Type	Value / meaning	Supply
EXIST	BOOL	<p>The EXIST bit indicates whether the user data area contains valid data.</p> <p>The retrieve FTP command executes the job only when EXIST=1.</p> <ul style="list-style-type: none"> 0: The file DB does not contain valid user data (file does not exist). 1: The file DB contains valid user data (file exists). 	<p>The DELETE FTP command sets EXIST=0.</p> <p>The STORE FTP command sets EXIST=1.</p>
LOCKED	BOOL	<p>The LOCKED bit is used to restrict access to the file DB.</p> <ul style="list-style-type: none"> 0: The file DB can be accessed. 1: The file DB is locked. 	<p>The "STORE" and "RETRIEVE" FTP commands set LOCKED=1 when they are executed if the bit was previously at 0.</p> <p>The user program on the S7 CPU can also set or reset LOCKED during write access to achieve data consistency.</p> <p>This results in mutual locking between the user program and FTP handling to ensure consistency.</p> <p>Recommended sequence in the user program:</p> <ol style="list-style-type: none"> 1. Check LOCKED bit (if = 0) 2. Set WRITEACCESS bit = 0 3. Check LOCKED bit (if = 0) 4. Set LOCKED bit = 1 5. Write data 6. Set LOCKED bit = 0
NEW	BOOL	<p>The NEW bit indicates whether data has been modified since the last read access.</p> <ul style="list-style-type: none"> 0: The content of the file DB is unchanged since the last write access. The user program of the S7 CPU has registered the last modification. 1: The user program of the S7 CPU has not yet registered the last write access. 	<p>After execution, the stor FTP command sets NEW=1</p> <p>After reading the data, the user program in the S7-CPU must set NEW=0 to allow a new "RETRIEVE" command.</p>

5.3 Block for the FTP client function

Parameter	Type	Value / meaning	Supply
WRITEACCESS	BOOL	<ul style="list-style-type: none"> 0: The user program has write access rights for the file DBs on the S7 CPU. 1: The user program has no write access rights for the file DBs on the S7 CPU. 	<p>During the configuration of the DB, the bit is set to an initialization value.</p> <p>Recommendation: Whenever possible, the bit should remain unchanged! In special situations, adaptation during operation is possible.</p>
ACT_LENGTH	DINT	Current length of the user data area. The content of this field is only valid when EXIST = 1.	The current length is updated following write access.
MAX_LENGTH	DINT	Maximum length of the user data area (length of the entire DB less 20 bytes header).	The maximum length should be specified during configuration of the DB. The value can also be modified by the user program during operation.
FTP_REPLY_CODE	INT	Unsigned integer (16-bit) containing the last reply code from FTP as a binary value. The content of this field is only valid when EXIST = 1.	Updated by the FTP protocol handler with the FTP command processing of the server.
DATE_TIME	DATE_AND_TIME	Date and time of the last modification to the file. The content of this field is only valid when EXIST = 1.	<p>The current date is updated following a write access.</p> <p>If the function for forwarding the time of day is used, the entry corresponds to the time that was passed on.</p> <p>If the function for forwarding the time of day is not used, a relative time is entered. The reference is the startup time of the CP (initialization value: 01.01.1994 00:00h).</p>

Diagnostics and maintenance

6.1 Diagnostics options

You have the following diagnostics options available for the module:

LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 23).

STEP 7: The "Diagnostics" tab in the Inspector window

If your engineering station is connected to the module via Ethernet, information on the connection status of the ES with the module can be found here.

STEP 7: Diagnostic functions via the "Online & Diagnostics" shortcut menu

Using the online functions, you can read various diagnostics information of the module from an engineering station on which the STEP 7 project is stored and perform maintenance functions.

You will find additional information on the diagnostics functions of STEP 7 in the STEP 7 information system.

Diagnostics

Here, you can obtain the following static information on the selected module:

- General
General information on the module
- Diagnostics status
Information on the diagnostics status
- Ethernet interface
Address and statistical information
- Time
Specification of the current time in the module and the time source
- Security
Status information and log entries

Functions

You can run the following functions here:

- Firmware update
For a description, see section Update firmware (Page 91).
- Assign IP address
- Assign PROFINET device name
- Save service data

STEP 7: Online connection

Establish the online connection to the module via the "Connect online" shortcut menu.

For the procedure, refer to the section Connect online (Page 88).

Web server

On a PC, you can access the Web pages of the CPU via HTTP/HTTPS. These pages provide various information.

For access to the content, see Preface (Page 3).

SNMP

You will find detailed information about the supported functions in the section Diagnostics with SNMP (Page 89).

6.2 Connect online

Online functions


Together with STEP 7, the CP offers various diagnostic and maintenance functions at the engineering station (ES). The ES and the CP must be in the same subnet for this.

Establishing an online connection via Ethernet

Procedure:

1. Connect the ES to the network.
2. Open the relevant STEP 7 project on the ES.
3. Select the CP.
4. Enable the online functions using the "Connect online" icon.
5. In the "Connect online" dialog, select the entry "PN/IE" from the "Type of PG/PC interface" drop-down list.

6. In the "PG/PC interface" drop-down list, select the interface of the ES.

You can use the  icon to the right of the drop-down list to check the settings of the interface.

7. In the "Connect with interface/subnet" drop-down list, select the interface of the station

8. Click "Start search".

If a connection is possible, the station is displayed.

9. Select the station in the table of target devices.

The path is possible both via the CP or the CPU.

10. Click "Connect".

Terminate online connection

On completion of the online session, terminate the online connection again using the "Disconnect" button.

See also

Online functions (Page 63)

6.3 Diagnostics with SNMP

Requirement

The requirement for using SNMP is the enabling of the function in the configuration.

SNMP (Simple Network Management Protocol)

SNMP is a protocol for diagnostics and managing networks and nodes in the network. To transmit data, SNMP uses the connectionless UDP protocol.

The information on the properties of SNMP-compliant devices is entered in MIB files (MIB = Management Information Base).

You will find detailed information on SNMP and the Siemens Automation MIB in the manual "Diagnostics and Configuration with SNMP" that you will find on the Internet:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15392/man>)

Performance range of the CP

The CP supports the following SNMP versions:

- SNMPv1
- SNMPv3 (with activated Security functions)

Traps are not supported by the CP.

Supported MIBs in SNMPv1

The CP supports the following MIBs:

- **MIB II (acc. to RFC1213)**

The CP supports the following groups of MIB objects:

- System
- Interfaces
- IP
- ICMP
- TCP
- UDP
- SNMP

- **LLDP MIB**

- **Siemens Automation MIB**

Note the rights for writing to the MIB objects, see the next section (SNMPv3).

Supported MIB objects in SNMPv3

If SNMPv3 is enabled, the CP returns the contents of the following MIB objects:

- **MIB II (acc. to RFC1213)**

The CP supports the following groups of MIB objects:

- System
- Interfaces
- IP (IPv4/IPv6)
- ICMP
- TCP
- UDP
- SNMP

The "Interfaces" MIB object provides status information about the CP interfaces.

The following groups of the standard MIB II are not supported:

- Adress Translation (AT)
- EGP
- Transmission

- **LLDP MIB**

- **Siemens Automation MIB**

Note that write access is permitted only for the following MIB objects of the "System" group:

- sysContact
- sysLocation
- sysName

A set sysName is sent as the host name using DHCP option 12 to the DHCP server to register with a DNS server.

For all other MIB objects and groups, only read access is possible for security reasons.

Access rights using community names (SNMPv1)

TCP uses the following community strings to control the permissions for access to the SNMP agent:

Table 6- 1 Access rights in the SNMP agent

Type of access	Community string *)
Read access	public
Read and write access	private

*) Note the use of lowercase letters!

Note

Security of the access

For security reasons, change the generally known strings "public" and "private".

6.4 Update firmware

New firmware versions of the CP

If a new firmware version is available for the CP, you will find this on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/dl>)

Firmware files have the file format *.upd.

Save the firmware file on your PC.

There are different ways of loading a new firmware file on the CP:

- Online functions of STEP 7 via Ethernet
- Loading the firmware file into the CPU from an SD card

Note

SD card only for firmware file

For the firmware file, you need a SIMATIC SD memory card, for example (article numbers):

- 6AV6671-8XB10-0AX1
- 6AV2181-8XP00-0AX0
- 6AV2181-8AQ10-0AX0

The firmware update card may not contain any other files. An SD card with configuration data cannot be used.

Note

Duration of the firmware update

Downloading a new firmware file can take several minutes.

Always wait until the completion of the firmware update can be recognized from the LEDs (see below).

Loading the firmware with the online functions of STEP 7 via Ethernet

Requirements:

- The CPU of the station is accessible via Ethernet.
- The engineering station and the CPU are located in the same subnet.
- The new firmware file is stored on your engineering station.
- The engineering station is connected to the network.
- The relevant STEP 7 project is open on the engineering station.

Procedure:

1. Select the station that you want to update with a new firmware.
2. Enable the online functions using the "Connect online" icon.
3. In the "Connect online" dialog, select the Ethernet interface in the "Type of PG/PC interface" list box.
4. Select the CPU of the station.
5. Click on "Start search" to search for the module in the network and to specify the connection path.

When the module is found it is displayed in the table.

6. Connect using the "Connect" button.

The "Connect online" wizard guides you through the remaining steps in installation.

7. Select the CPU in the network view and select the "Online & Diagnostics" shortcut menu (right-click).

8. In the navigation panel of the Online & Diagnostics view select the entry "Functions > Firmware update".
9. Using the "Browse" button (parameter group "Firmware loader") search for the new firmware file in the file system of the engineering station.
10. Start to download the firmware with the "Start update" button when the correct version of the signed firmware is displayed in the "Status" output box.

You will find further information on the online functions in the STEP 7 information system.

Loading the firmware via the SD card

You can find detailed information on using an SD card in the S7-1500 System Manual, see Preface (Page 3).

Requirements:

- You have copied the new firmware file from your PC to the SD card using a suitable card reader.
- Optional: You have saved a backup file of the currently used firmware file.

Procedure:

1. Set the operating mode switch of the CPU to STOP.
Ensure that no write functions (e.g. online or test functions) are active in the STOP state.
2. Remove the SIMATIC Memory Card with the configuration data from the slot of the CPU.
3. Insert the SD card with the firmware file in the card slot of the CPU.

The firmware update starts shortly after the card has been inserted. The display shows the following: "STOP - FW UPDATE"

If errors occur, appropriate messages are displayed.

After completing the firmware update, the display shows a result page.

A successful firmware update can be recognized by the following LED pattern from the CPU:

- RUN lights up yellow.
- MAINT flashing yellow.

4. Remove the SD card and insert the SIMATIC Memory Card again.
5. Set the operating mode switch of the CPU to RUN.

The CP uses the new firmware during startup.

For the LED pattern of the CP during the startup, see section LEDs (Page 23).

6.5 Replacing a module without a programming device

Configuration data when swapping modules

The configuration data of the CP is stored on the CPU. This makes it possible to replace this module with a module of the same type (identical article number) without a PG.

Note

Configured MAC address is adopted

When setting the ISO protocol, remember that MAC address set previously during configuration is transferred by the CPU to the new CP module.

Swapping modules for address reference via DHCP (IPv4)

One option in the IP configuration of the CP is to obtain the IP address from a DHCP server.

Note

Recommendation: Configuring a client ID

When replacing modules, remember that the factoryset MAC address of the new module is different from the previous module.

When the factory default MAC address of the new module is sent to the DHCP server, the DHCP server returns a different or no IP address.

Ideally, you should therefore configure IP as follows:

- Always configure a client ID and configure your DHCP server accordingly. This ensures that the CP always receives the same IP address from the DHCP server after swapping a module.

If you have configured a new MAC address instead of the MAC address set in the factory, the configured MAC address will always be transferred to the DHCP server. In this case, the new CP also has the same IP address as the previous module.

Technical specifications

7.1 Technical specifications

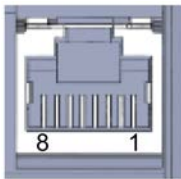
Technical specifications - CP 1545-1		
Article number	6GK7545-1GX00-0XE0	
Attachment to Industrial Ethernet		
Quantity	1 x gigabit interface (X1 P1)	
Design	RJ-45 jack, galvanically isolated	
Properties		
<ul style="list-style-type: none"> • Standard • Transmission speeds • Other properties 	<ul style="list-style-type: none"> • 1000BASE-T, IEEE 802.3ab • 10 / 100 / 1000 Mbps • Half duplex/full duplex, autocrossover, autonegotiation 	
Power supply		
Design	Via S7-1500 backplane bus (15 V)	
Further electrical data		
Current consumption (typical)	300 mA from S7-1500 backplane bus	
Effective power loss (typical)	4.5 W	
Insulation	Tested to:	DC 780 V (type test)
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 ... +40 °C
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 95 % 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 ₂ S	• < 0,1 ppm
Design, dimensions and weight		
Module format	Compact module S7-1500, single width	
Degree of protection	IP20	
Weight	320 g	
Dimensions (W x H x D)	35 x 147 x 129 mm	
Mounting type	S7-1500 standard rail mounting	

You can find additional data in the section Application and functions (Page 13) as well as in the S7-1500 System Manual, see Preface (Page 3).

7.2 Pinout of the Ethernet interface

Pinout of the gigabit Ethernet interfaces

The table below shows the pin assignment of the Ethernet interface X1.

View of the RJ-45 jack	Pin	Signal name	Assignment
	1	D1+	D1+ bidirectional
	2	D1-	D1- bidirectional
	3	D2+	D2+ bidirectional
	4	D3+	D3+ bidirectional
	5	D3-	D3- bidirectional
	6	D2-	D2- bidirectional
	7	D4+	D4+ bidirectional
	8	D4-	D4- bidirectional

7.3 Permitted cable lengths - Ethernet

Permitted cable lengths - Ethernet	Alternative combinations per length range
0 ... 55 m	<ul style="list-style-type: none"> Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180 Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet
0 ... 85 m	<ul style="list-style-type: none"> Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180 Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet
0 ... 100 m	<ul style="list-style-type: none"> Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180 Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet

See also Siemens Mall: (<https://mall.industry.siemens.com>)

7.4 Permitted cable lengths - Gigabit Ethernet

Permitted cable lengths - Gigabit Ethernet	Alternative combinations
0 ... 60 m	<ul style="list-style-type: none"> Max. 60 m IE FC TP Flexible Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE
0 ... 100 m	<ul style="list-style-type: none"> Max. 90 m IE FC TP Standard Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE

See also Siemens Mall: (<https://mall.industry.siemens.com>)

Approvals

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals - with the exception of the certificates for shipbuilding - have only been obtained when there is a corresponding mark on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate. The approvals for shipbuilding are an exception to this.

Certificates for shipbuilding and national approvals

The device certificates for shipbuilding and special national approvals can be found in Siemens Industry Online Support on the Internet:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15340/cert>)

EC declaration of conformity



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

- **2014/30/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

The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft
 Digital Industries
 P.O. Box 48 48
 90026 Nuremberg
 Germany

You will find the EC Declaration of Conformity on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/cert>)

The current versions of the standards can be seen in the EC Declaration of Conformity and in the certificates.

IECEX

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

IECEX classification:

- Ex ec IIC T4 Gc

Certificate: IECEx DEK 18.0019X

Applied standards:

- EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

You can see the current versions of the standards in the IECEx certificate that you can find on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/cert>)

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 28).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you can find on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/78381013>)

ATEX



The product meets the requirements of the EC directive:2014/34/EC "Equipment and Protective Devices for Use in Potentially Explosive Atmospheres".

ATEX approval:

- II 3 G Ex ec IIC T4 Gc

Type Examination Certificate: DEKRA 18 ATEX 0027X

Applied standards:

- EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

The current versions of the standards can be seen in the EC Declaration of Conformity, see above.

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 28).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find here:

- In the SIMATIC NET Manual Collection under "All documents" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- On the Internet at the following address:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/78381013>)

EMC

Until 19.04.2016 the product meets the requirements of the EC Directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive).

Applied standards:

- EN 61000-6-4
Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
- EN 61000-6-2
Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments

RoHS

The product meets the requirements of the EC directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Applied standard:

- EN 50581

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 Notes on use in hazardous areas according to UL HazLoc and FM (Page 29).

Note

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

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).

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 사용하는 것을 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.

Marking for the customs union



EAC (Eurasian Conformity)

Eurasian Economic Union of Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan

Declaration of conformity according to the technical regulations of the customs union (TR ZU)

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/25625/cert>)

Dimension drawings

All dimensions in the dimension drawings are in millimeters.

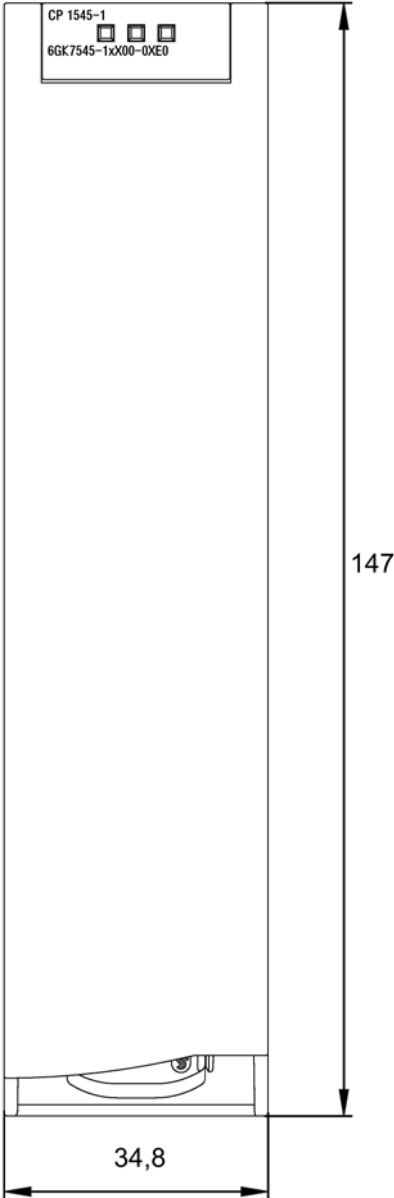


Figure 9-1 Front view

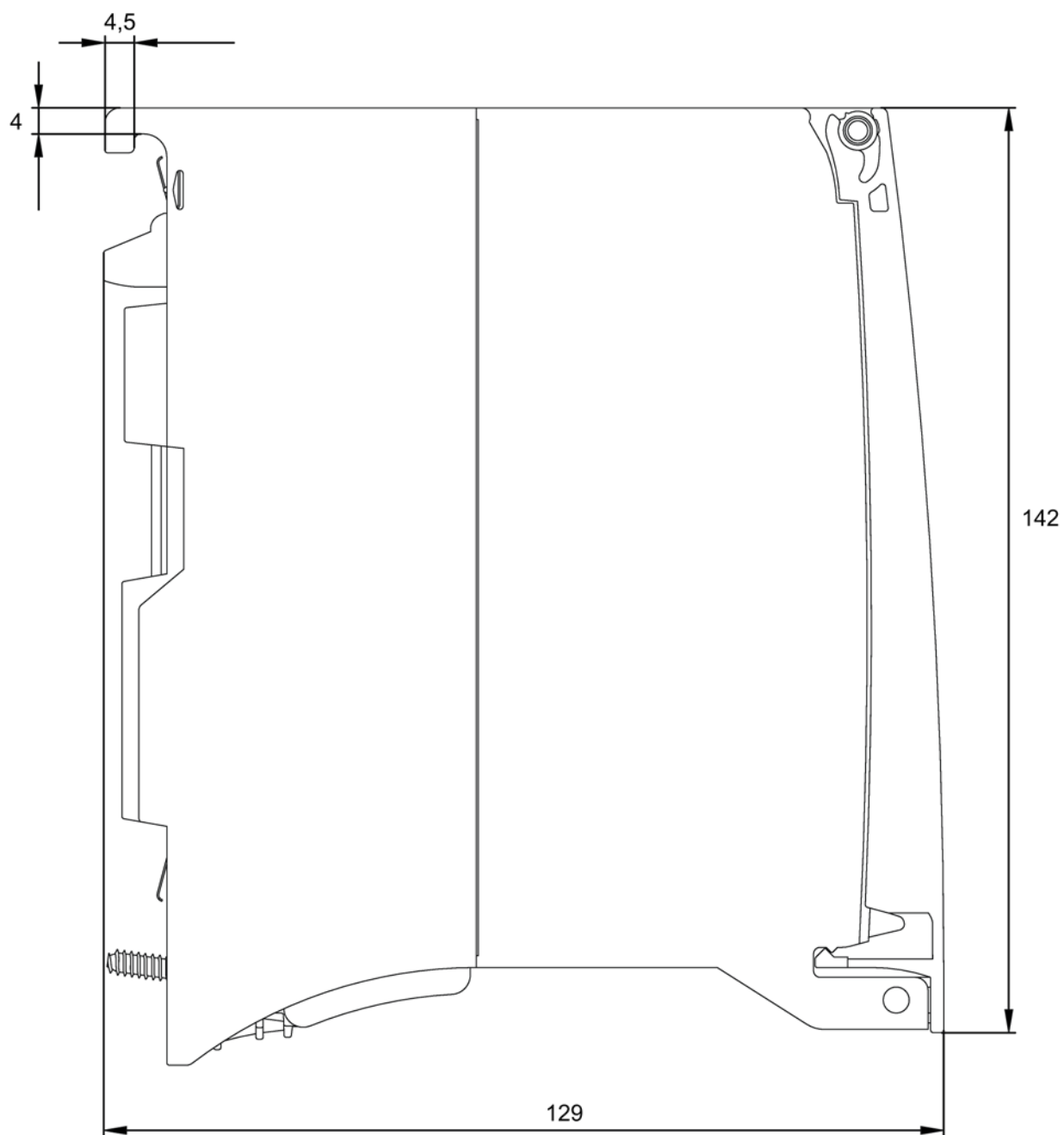


Figure 9-2 Side view

Syslog messages

The product outputs Syslog messages according to RFC 5424. The messages are based on IEC 62443-3-3.

You can find a more detailed description of the individual messages below.

A.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: <ul style="list-style-type: none"> • Severity (Severity) <p>Possible values:</p> <ul style="list-style-type: none"> – 0 Emergency – 1 Alert – 2 Critical – 3 Error – 4 Warning – 5 Notice – 6 Information – 7 Debug • Facility (Origin) <p>Possible values, e.g.: Sub-system, service, user</p>
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

A.2 Tags in Syslog messages

Part / Parameter	Explanation
HOSTNAME	Identifies the source device by either: <ul style="list-style-type: none"> • 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 host name or the configured IPv4 address
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"] <ul style="list-style-type: none"> • tzKnown This parameter specifies whether the time zone is known in the source device. <ul style="list-style-type: none"> - 1 = known - 0 = unknown • isSynced This parameter specifies whether the source device is synchronized with a reliable external time source, e.g. via NTP. <ul style="list-style-type: none"> - 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>

A.2 Tags in Syslog messages

The tags are displayed in the section "Syslog messages" in the field "Message text" within curly brackets {variable}.

The output messages can contain the following tags:

Tag	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
{Src port} {Dest port}	Port number (decimal)	%d	0 ... 65535
{Src mac} {Dest mac}	Source/destination MAC address	%02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	Layer 4 protocol or service used that generated the event.	%s	UDP TCP WBM Telnet SSH Console PNIO PB OPC TFTP SFTP
{Group}	Name for identification of the group (string without spaces)	%s	ITservice
{User name}	String (without spaces) that identifies the authenticated user by his or her name.	%s	<Name>
{Local interface}	Symbolic name of the local interface	%s	Console
{Action user name} or {Destination user name}	Identifies the destination user based on his/her name. This is not the authenticated user.	%s	<First name>.<Name>
{Role}	Symbolic name of the role	%s	Administrator
{Time minute} {Timeout}	Number of minutes	%d	44
{Time second}	Number of seconds	%d	44
{Failed login count}	Number of failed login attempts	%d	10
{Max sessions}	Maximum number of sessions	%d	10
{Trigger pin}	String (without spaces) for an IO pin that triggered the event.	%s	DI1
{Firewall rule}	String (with spaces) for a firewall rule set	%s	Rule1
{Subject}	String (with spaces) for the subject in the certificate. Used as part of the certificate-based authentication and must also include Unicode characters.	%s With UTF8 code: %S	Subject
{Config detail}	String (with spaces) for the identification of a part of the configuration	%s	OpenVPN
{Connection name}	Name of the VPN connection		Connection_1

A.3 Messages

Tag	Description	Format	Possible values or example
{Firewall accept}	Firewall action executed (accepted package)		ACCEPT
{Firewall action reject}	Firewall action executed (rejected package)		REJECT DROP
{Length}	Length of the network packet (in bytes)	%d	52
{Network interface}	Symbolic name of a network interface	%s	vlan 1

A.3 Messages

The product outputs the following SYSLOG messages, sorted by classes.

A.3.1 Non-repudiation

A.3.1.1 15.1_SE_CONFIG_CHANGE_(protocol)_(configuration)

Message text	{Protocol}: User {User name} has changed configuration.
Example	Console: User admin has changed configuration.
Explanation	User has changed the configuration data by loading new configuration data.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Index

A

Abbreviations/acronyms, 4
Article numbers, 3

C

Connection abort, 59
Connection resources of the CPU, 18
Connections for Web
 Quantity, 19
Cross references (PDF), 4

D

Data buffering, 60
Data management - Configuration data, 94
Data transmission (cloud), 53
DHCP, 94
Disposal, 6
DNS server - program-controlled change, 71
Double addressing in the network, 37

E

E-mail, 13
E-mail connection, 20
EMC - electromagnetic compatibility, 97
Ethernet interface, 25
 Configuration via T_CONFIG, 70

F

FETCH/WRITE, 14, 37
 S5/S7 addressing mode, 17
FETCH/WRITE connections, 20
Firewall, 17
FTP, 37
FTP (FTP client), 18
FTP client
 Configuration limits, 21
FTP server
 Configuration limits, 21
FTP_CMD, 72
 Block execution time, 21

FTPS, 17
FTPS - Security, 43

G

Gigabit specification, 25
Glossary, 6

H

Hardware product version, 3
HMI communication, 14

I

Instruction
 FTP_CMD, 70
 T_CONFIG, 70
 TCON, TSEND/TRCV, 70
 TDISCON, 70
 TMAIL_C, 70
 TSEND_C/TRCV_C, 70
 TUSEND/TURCV, 70
Instructions (OUC), 67
IP address
 Via DHCP, 37
IP address - program-controlled change, 71
IP configuration
 IPv4 / IPv6, 16
IP routing, 38
IPv6 address
 Use, 16
ISO transport connections, 20
ISO-on-TCP (RFC 1006), 13
ISO-on-TCP connections, 20
ISO-Transport (RFC 8073), 13

L

Logging, 17
Logging server, 66

M

MAC address, 15
MIB, 89

Multicast (UDP), 13

N

NTP, 15

NTP (secure), 17, 39

NTP server, 39

NTP server - program-controlled change, 71

O

Online diagnostics, 87

Online functions, 88

OP connections

Quantity, 19

Open User Communication (OUC), 13

Operating mode of the CPU, 32

OUC (Open User Communication), 67

P

PG communication, 14

PG connections

Quantity, 19

Port 8448, 63

Product name, 4

Program blocks - max. Data length, 20

Programmed communications connections, 38

Programmed connections

Quantity, 19

PUT/GET, 37

Q

QoS, 60

QualityCode, 59

R

Recycling, 6

Replacement part, 22

RUN → STOP, 32

S

S7 communication, 14

S7 connections, 18

Number of freely usable, 19

Safety notices, 27

Security diagnostics, 63

Service & Support, 7

SIMATIC NET glossary, 6

SMTS, 17

SNMP, 40, 89

SNMPv3, 18

Software

Version, 3

Special notes

Ensuring a valid time of day, 39

Recommendation for setting the time, 39

Response if the reference to the FTP job block is missing, 80

STEP 7 - version, 22

System data type

FTP_..., 70

TCON_..., 70

TMail_..., 70

T

TCP (RFC 793), 13

TCP connections, 20

TCP connections for FTP, 21

Time-of-day synchronization, 15

Training, 7

U

UDP

Restrictions, 21

UDP (RFC 768), 13

UDP connections, 20

UDP frame buffering, 21

W

Web server, 16