



**SIEMENS**



Industry Online Support

The image shows a man in a light blue shirt using a tablet in a factory setting. Overlaid on the scene are various digital interface elements: a 'NEWS' section with a profile icon, a '24/7' icon with a circular arrow, a 'Home' button, and a network diagram with three nodes. The background is a blurred industrial environment with a clock on the wall.

**Sending emails over  
secure email  
connections with an  
S7-1500 or S7-1200**

SIMATIC STEP 7 (TIA Portal), TMAIL\_C

<https://support.industry.siemens.com/cs/ww/en/view/46817803>

Siemens  
Industry  
Online  
Support



# Legal information

## Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

## Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness, and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

## Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://support.industry.siemens.com>) shall also apply.

## Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: <https://www.siemens.com/industrialsecurity>.

# Table of contents

<b>Legal information</b> .....	<b>2</b>
<b>1 Introduction</b> .....	<b>4</b>
1.1 Overview .....	4
1.2 Principle of operation .....	5
1.3 Components used.....	6
<b>2 Engineering</b> .....	<b>7</b>
2.1 Preparing the environment .....	7
2.2 Email account: loading the provider certificate .....	8
2.2.1 Find the provider certificate .....	8
2.2.2 Download provider certificates .....	11
2.3 Email account Allowing controller access .....	12
2.3.1 Instructions for Gmail.....	12
2.3.2 Brief instructions for other email providers .....	23
2.4 TIA project: Setting up IP addresses .....	24
2.5 TIA Portal: Setting the time.....	28
2.5.1 Set the CPU's clock .....	28
2.5.2 Set the CP's clock.....	32
2.6 TIA Portal: Finding the hardware identifier .....	34
2.7 TIA Portal: Module security settings .....	35
2.7.1 Enable global security settings in the CPU .....	35
2.7.2 Create and sign in a security user .....	37
2.7.3 Enable global security settings in the CP .....	38
2.8 TIA Portal: Importing provider certificate .....	40
2.9 TIA Portal: Using MAIL_C .....	44
2.9.1 Parameters of the "TMAIL_C" instruction .....	44
2.9.2 Create global data block .....	46
2.9.3 Parameterize tags.....	49
2.9.4 Call "TMAIL_C" instruction and interconnect .....	54
2.10 Operation .....	55
<b>3 Useful information</b> .....	<b>56</b>
3.1 SMTP servers and ports of the providers .....	56
3.2 "TMAIL_C" instruction.....	56
3.3 System data types of "TMAIL_C" .....	58
<b>4 Appendix</b> .....	<b>62</b>
4.1 Service and support.....	62
4.2 Industry Mall .....	63
4.3 Links and literature .....	63
4.4 Change documentation .....	63

# 1 Introduction

## 1.1 Overview

Email is a common mechanism for sending error statuses or warnings from industrial plants to a control center or operators. The SIMATIC S7 product range contains products which support this protocol.

### "TMAIL\_C" instruction

Using the "TMAIL\_C" instruction, you can send an email via the Ethernet interface of a SIMATIC S7-1500 CPU (firmware 2.0 or higher) or a S7-1200 CPU (firmware 4.1 or higher), a communication module (CM) or a communication processor (CP).

For safety reasons, most email servers today only support secure connections. Therefore, the communication processors which support the "send email" function have been extended with the methods for secure email connections.

### "TMAIL\_C" on a CP

The following CPs send secure emails via the instruction "TMAIL\_C" V4.0 or higher.

Table 1-1

CP	Item number	Firmware version
CP 1543-1	6GK7543-1AX00-0XE0	From V2.0
CP 1545-1	6GK7545-1GX00-0XE0	From V1.0
CP 1542SP-1 IRC	6GK7542-6VX00-0XE0	From V1.0
CP 1543SP-1	6GK7543-6WX00-0XE0	From V1.0
CP 1243-1	6GK7243-1BX30-0XE0	From V2.1
CP 1242-7 GPRS V2	6GK7242-7KX31-0XE0	From V2.1
CP 1243-7 LTE	6GK7243-7KX30-0XE0 6GK7243-7SX30-0XE0	From V2.1
CP 1243-8 IRC	6GK7243-8RX30-0XE0	From V2.1

### "TMAIL\_C" on the CPU

Using the "TMAIL\_C" instruction V5.0 or higher, you can send secure emails via the integrated Ethernet port of an S7-1500 CPU. The S7-1500 CPU needs at least firmware V2.5 to do this.

Using the "TMAIL\_C" instruction V6.0 or higher, you can send secure emails via the integrated Ethernet port of an S7-1200 CPU. The S7-1200 CPU needs at least firmware V4.4 to do this.

### Application example

This application example will demonstrate how to set up a secure connection (SMTP over TLS) to an email server with the integrated Ethernet port of a CPU or a CP.

## 1.2 Principle of operation

### Schematic representation

The following Figure shows the most important relationships between the components involved and the steps necessary to set up a secure connection (SMTP over TLS) to an email server.

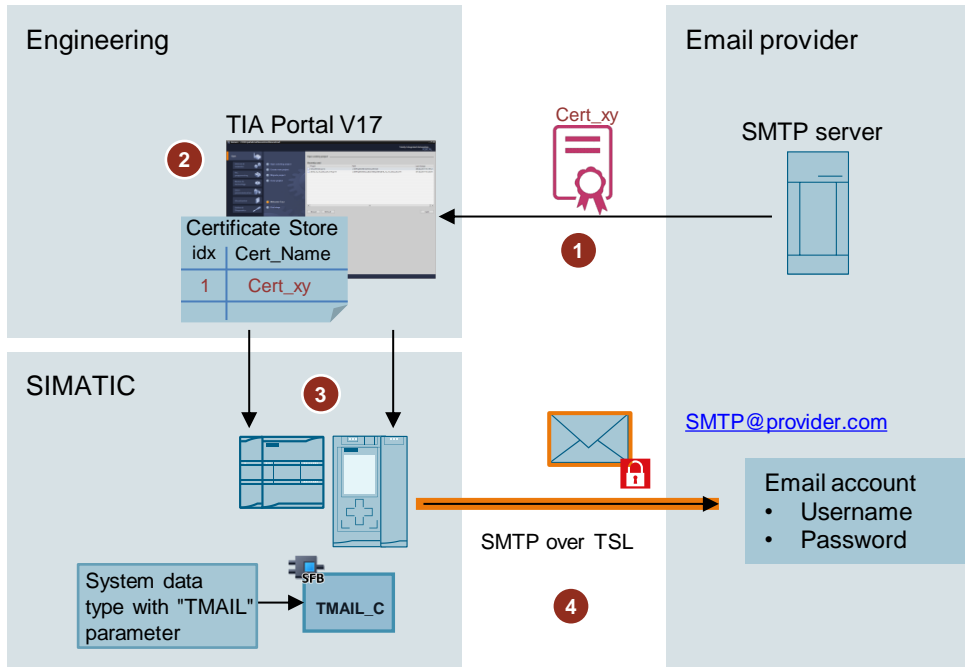


Table 1-2

Step	Description
1	Find the certificate of the email provider. In the email account, allow the CPU or communication processor (CP) to access the email account via SMTP or SMTPS.
2	Import the certificate of the email provider into TIA Portal V17.
3	In the SIMATIC controller, perform the following configuration steps: <ul style="list-style-type: none"> <li>• add the imported certificate to the module</li> <li>• establish a connection between the CPU/CP and the internet</li> <li>• configure the DNS server</li> <li>• call the instruction "TMAIL_C" in the user program of the CPU and enter parameters for it</li> <li>• set up time synchronization in the module</li> </ul>
4	Send the email via the secure connection (SMTP over TLS).



## "TMAIL\_C"

Using the "TMAIL\_C" instruction, you can send an email over a secure connection via the Ethernet port of an S7-1500 or an S7-1200, a communication module (CM) or communication processor (CP).

You will use a system data type to address the email server. The following structures are available:

- TMail\_V4\_SEC: Addressing via the IP address according to IPv4
- TMail\_V6\_SEC: Addressing via the IP address according to IPv6
- TMail\_QDN\_SEC: Addressing via the fully qualified domain name (FQDN)

**Note**

For more information on the "TMAIL\_C" instruction and the system data types, see [chapter 3](#).

## 1.3 Components used

The following hardware and software components were used to create this application example:

Table 1-3

Components	Quantity	Item number	Note
CPU 1513-1 PN	1	6ES7513-1AL01-0AB0	Alternatively, you can also use any other S7-1500 CPU V2.5 onward, an ET 200SP CPU V2.5 onward or an S7-1200 CPU V4.4 onward.

**Note**

If you use an S7-1500 CPU earlier than V2.5, an ET 200SP CPU earlier than V2.5 or an S7-1200 CPU earlier than V4.4, you will need a CP in order to send secure email (see [Table 1-1](#)).

This application example consists of the following components:

Table 1-4

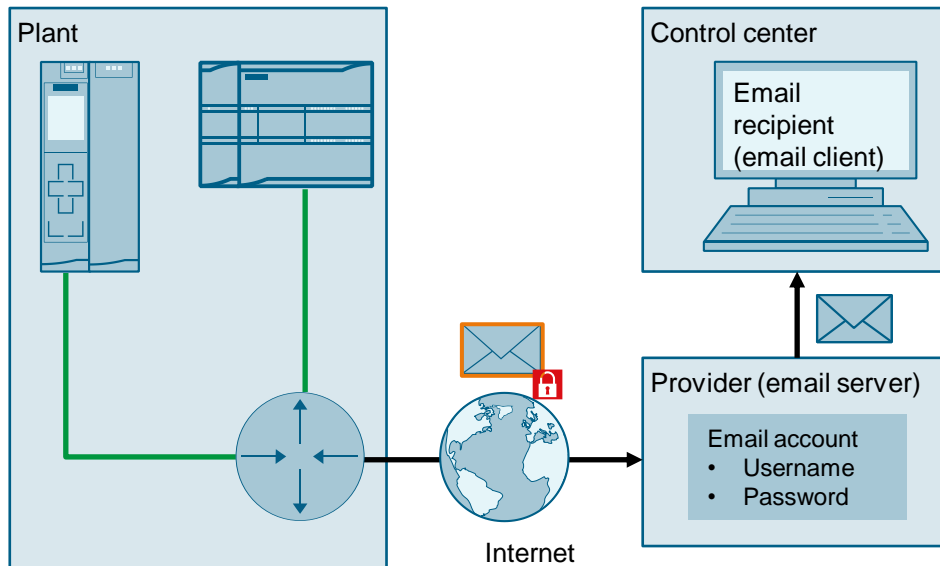
Components	File name	Note
Document	46817803_EMail_with_SimaticS7_V30_en.pdf	-
Project	46817803_EMail_with_SimaticS7.zip	TIA V17

## 2 Engineering

### 2.1 Preparing the environment

#### Hardware setup

The following Figure shows the hardware setup in a hypothetical plant.



Connect the Ethernet port of the CPU or CP with the router that has a connection to the internet (e.g. DSL router).

#### IP addresses

Make sure that your CPU or CP is in the same subnet as the DSL router and that each IP address has only been assigned once within the subnet.

The following static IP addresses were used in the TIA Portal project of this application example:

Table 2-1

No.	Components	IP address	Subnet mask
1	CPU 1513-1 PN	172.16.60.30	255.255.0.0
2	DSL router	172.16.0.1	255.255.0.0

#### TIA Portal project

Open your TIA Portal project or create a new project with your hardware components. When you add the CPU, follow the instructions from the Security Wizard and adjust the security functions to suit your needs.

This application example provides a prefabricated TIA Portal project for your CPU 1513-1 PN. The "TMAIL\_C" instruction has already been integrated within this TIA Portal project and assigned parameters.

#### Note

The example project is protected. Log in with the following credentials:

- Username: admin
- Password: Siemens.1

## 2.2 Email account: loading the provider certificate

### Overview

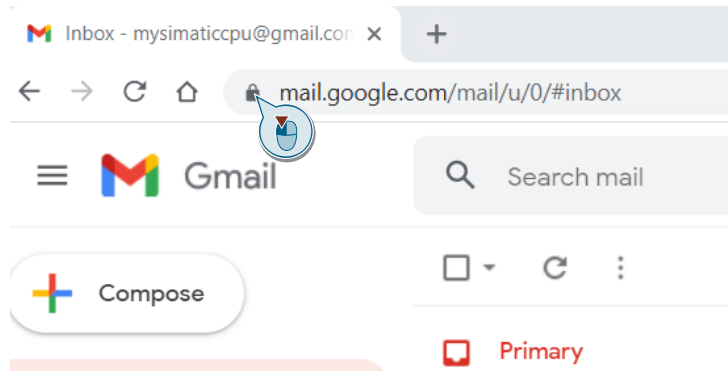
A certificate is a public key signed by its owner (in this case, the email provider) that guarantees its authenticity and integrity.

This certificate must first be found and then downloaded from the provider's website.

### 2.2.1 Find the provider certificate

The application example demonstrates how to find the certificate of the provider Gmail from Google. Google Chrome will be used as a web browser. The dialog boxes will appear differently for other internet browsers.

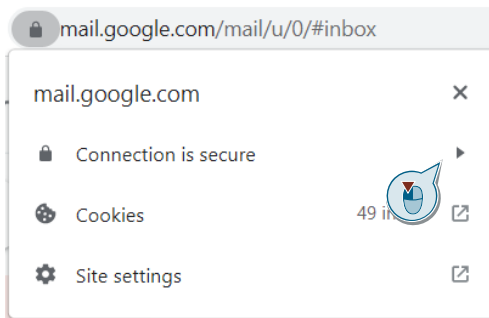
1. Log in to your Gmail account to find the certificate of your provider.
2. In Google Chrome's input bar, click the "View site information" icon (padlock icon).



The dialog for "mail.google.com" will open.

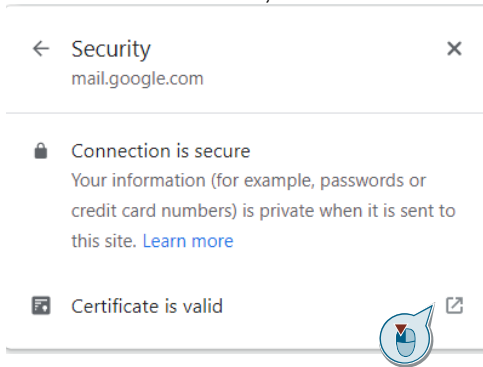


3. To view the connection details, click on "Connection is secure".



The "Security" dialog opens.

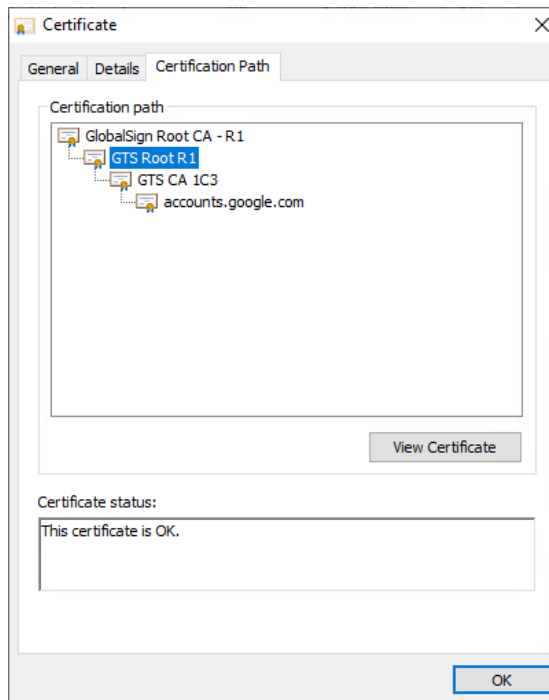
4. To view the certificate, click on "Certificate is valid".



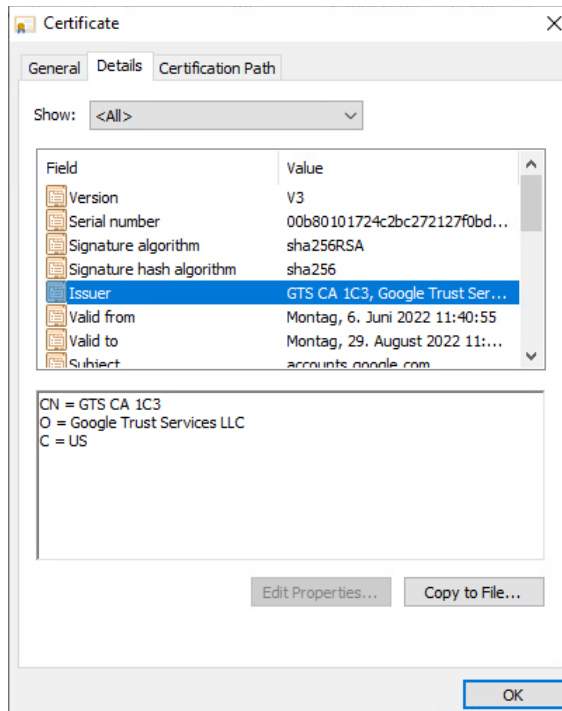
## Result

The "Certificate" dialog will open.

The "Certification Path" tab displays the name of the certificate used by your provider. In this example, Gmail uses the certificate "GTS Root R1".



You can find the certificate issuer in the "Details" tab. The "Issuer" of the certificate "GTS Root R1" is "GTS CA 1C3" from "Google Trust Services".



Accordingly, you need the certificate "GTS Root R1" from "Google Trust Services". Download this certificate in "PEM" format from the Google website (see [Table 2-2](#)).

## 2.2.2 Download provider certificates

Every provider typically offers the in-use certificates for download on its website.

As an example, we provide the links to the certificates of Telekom and Google in the Table below.

Table 2-2

Name of certificate	Used by	Link
T-TeleSec GlobalRoot Class 3 Issuer: T-Systems International GmbH	Web.de GMX	<a href="#">T-Telesec GlobalRoot Class 3</a>
Global Sign: GTS Root R1 Issuer: Google Trust Services	Gmail	<a href="#">Google Trust Services</a>
T-TeleSec GlobalRoot Class 2 Issuer: T-Systems Enterprise Services GmbH	T-Online	<a href="#">T-Telesec GlobalRoot Class 2</a>

Download the certificate you need and then save it locally on your computer.

## 2.3 Email account Allowing controller access

In your email account, allow the CPU or CP to access your email account via SMTP or SMTPS. This process is set up differently for each provider.

The following instructions show how to allow the CPU or CP access to an email account from these providers:

- Gmail (detailed explanation in [chapter 2.3.1](#))
- GMX (see [chapter 2.3.2](#))
- Web.de (see [chapter 2.3.2](#))
- T-Online (see [chapter 2.3.2](#))

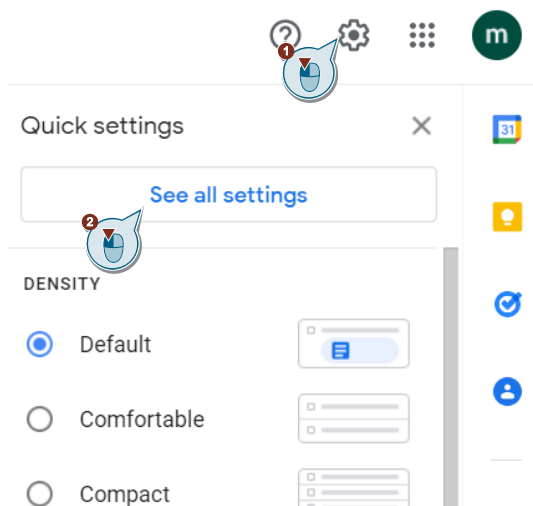
Log in to your email account.

### 2.3.1 Instructions for Gmail

#### Enable POP and IMAP

Proceed as follows to enable POP and IMAP for Gmail:

1. Click the "Settings" icon.  
To view all settings, click the "See all settings" button.




The full settings menu appears.

- Open the "Forwarding and POP/IMAP" tab.  
Under "POP download", enable the function "Enable POP for all mail".  
Under "IMAP access", enable the function "Enable IMAP".

Settings

General Labels Inbox Accounts and Import Filters and blocked addresses **Forwarding and POP/IMAP** Add-ons Chat and Meet

**Forwarding:**  
[Learn more](#)  


Tip: You can also forward only some of your messages by [creating a filter!](#)

---

**POP download:**  
[Learn more](#)

**1. Status: POP is enabled** for all emails

- Enable POP for **all mail** (even mail that's already been downloaded)
- Enable POP for **mail that arrives from now on**
- Disable POP**

 **2. When messages are accessed with POP**


**3. Configure your email client** (e.g. Outlook, Eudora, Netscape Mail)  
[Configuration instructions](#)

---

**IMAP access:**  
(access Gmail from other clients using IMAP)  
[Learn more](#)

**Status: IMAP is enabled**

- Enable IMAP
- Disable IMAP

 **When I mark a message in IMAP as deleted:**

- Auto-Expunge on - Immediately update the server. (default)
- Auto-Expunge off - Wait for the client to update the server.

**When a message is marked as deleted and expunged from the last visible IMAP folder:**

- Archive the message (default)
- Move the message to the Bin
- Immediately delete the message forever

- Click "Save Changes".

**IMAP access:**  
(access Gmail from other clients using IMAP)  
[Learn more](#)

**Status: IMAP is enabled**

- Enable IMAP
- Disable IMAP

**When I mark a message in IMAP as deleted:**


- Auto-Expunge on - Immediately update the server. (default)
- Auto-Expunge off - Wait for the client to update the server.

**When a message is marked as deleted and expunged from the last visible IMAP folder:**

- Archive the message (default)
- Move the message to the Bin
- Immediately delete the message forever

**Folder size limits**

- Do not limit the number of messages in an IMAP folder (default)
- Limit IMAP folders to contain no more than this many messages

**Configure your email client** (e.g. Outlook, Thunderbird, iPhone)  
[Configuration instructions](#) 

## Result

POP and IMAP are enabled and the settings have been saved.

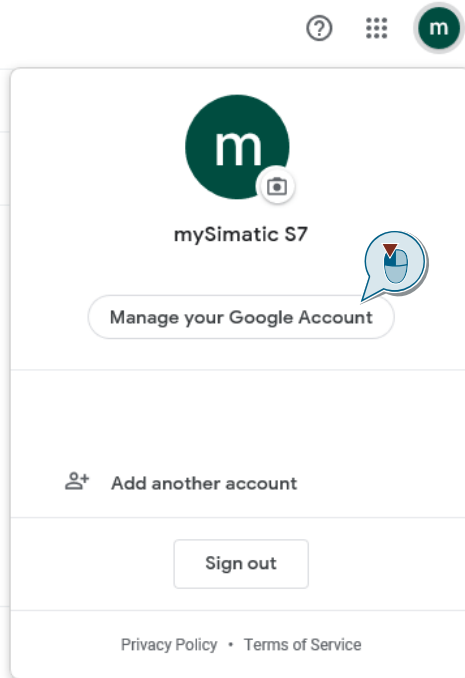
### Set up two-factor authentication

To grant access to your email account to an application that does not support the "Sign in with Google" option, you will need to generate an app password.

Generating an app password requires two-factor authentication.

To activate two-factor authentication and then generate an app password, proceed as follows:

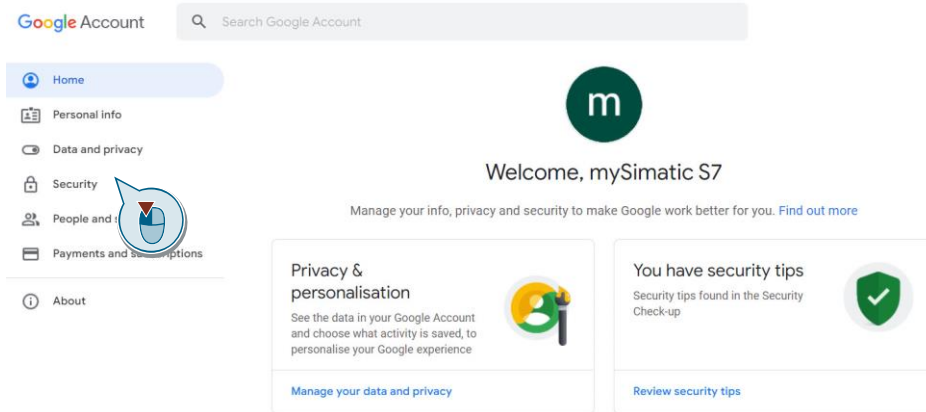
1. Click "Manage your Google Account".



The data and privacy settings will open.



2. Select "Security".

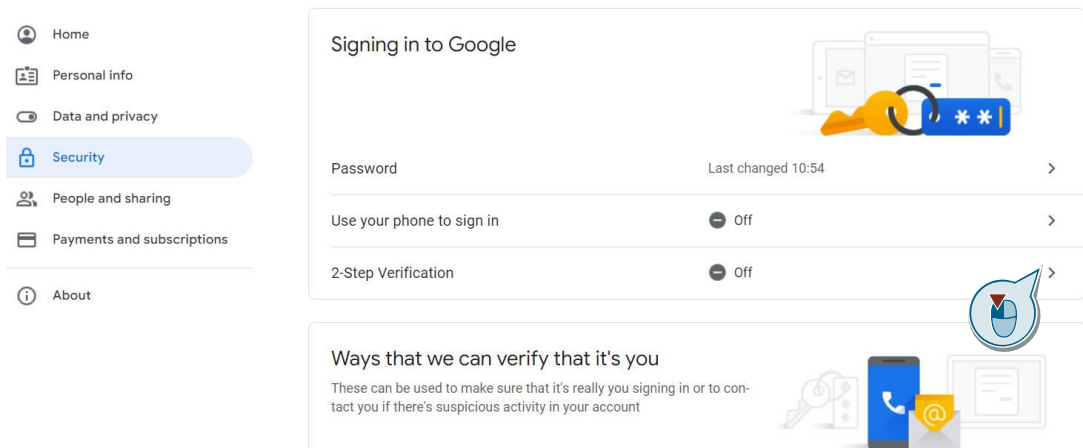


The security settings will open.

3. Go to the "Signing in to Google" section and click on "2-Step Verification".

Note

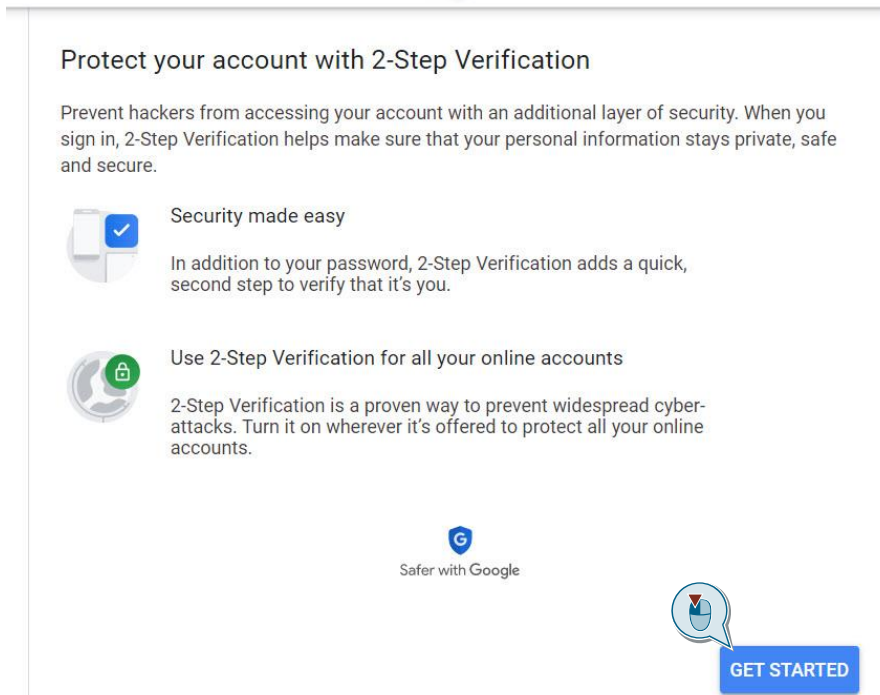
If you have already set up two-factor authentication for your Gmail account, this section will already show the "App passwords" item. If this is the case, skip the steps below and go to the section "[Generate app password](#)" in this chapter.



The two-factor authentication setup dialog opens.

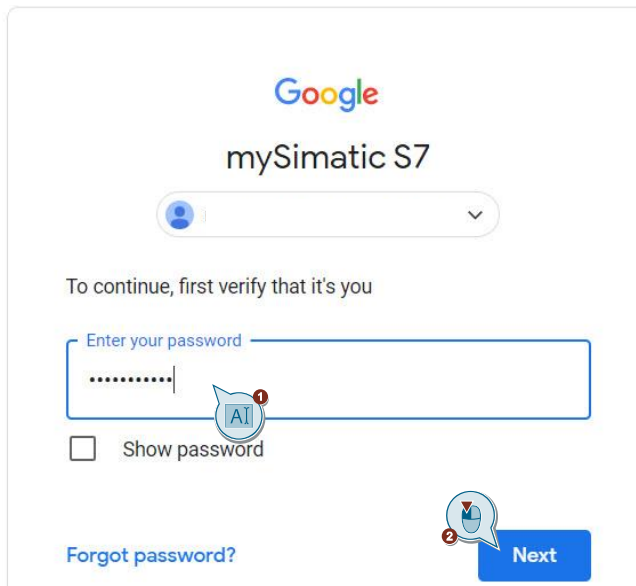
4. Click on "GET STARTED".

← 2-Step Verification



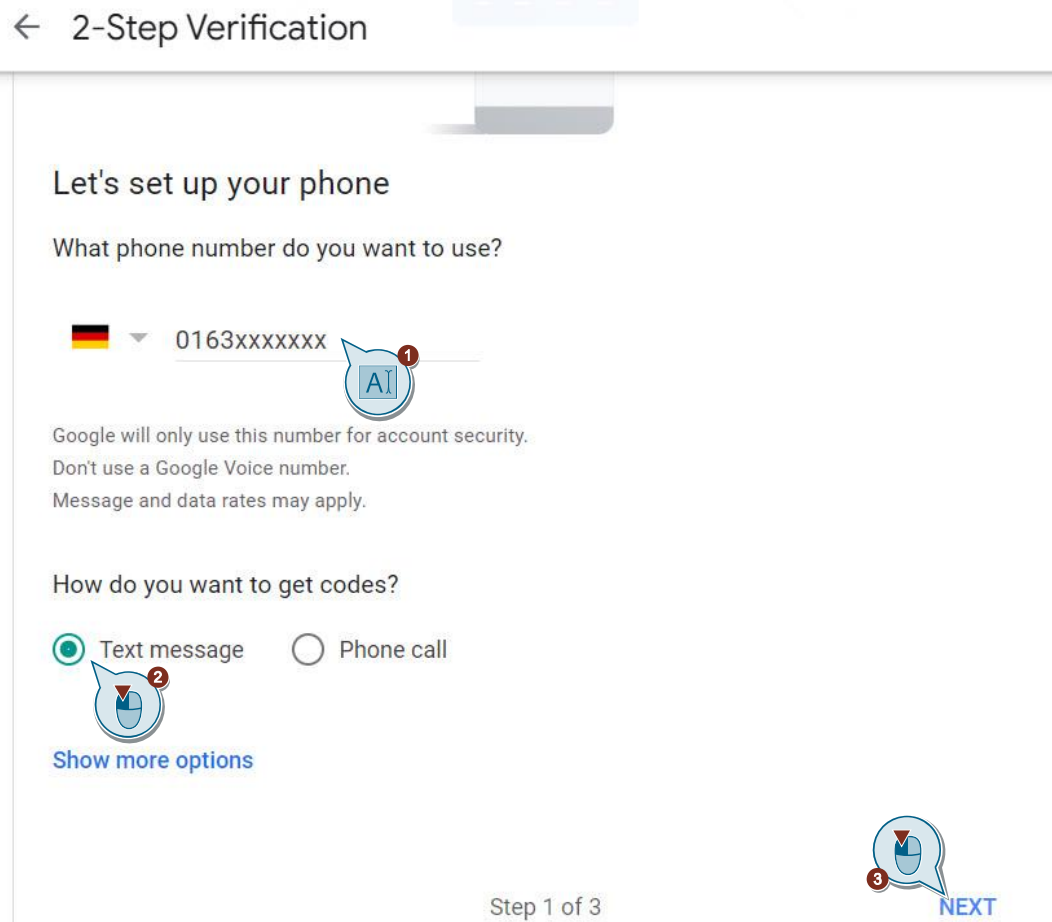
The sign-in dialog appears.

5. Log in to your email account.  
Enter the password for your email account and click "Next".



The first step for setting up two-factor authentication will appear.

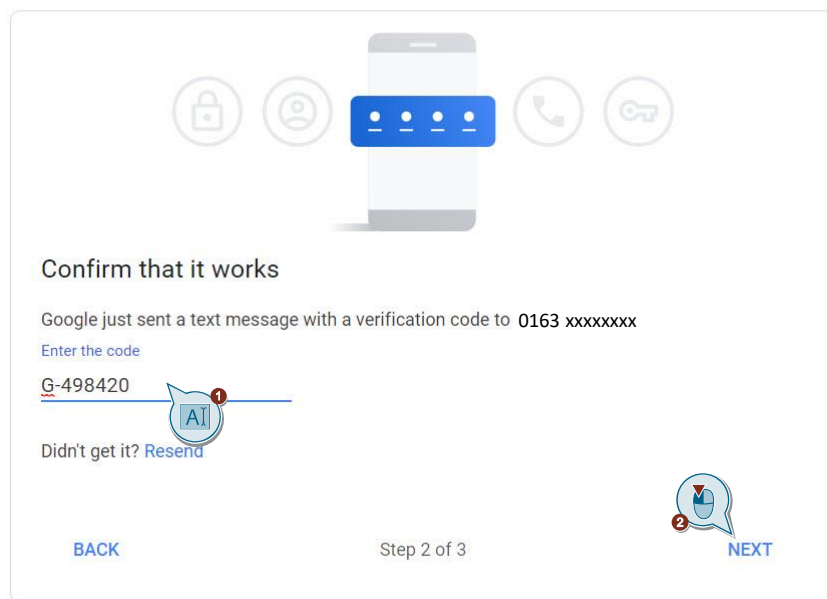
6. In this step, select a second factor to authenticate with.  
In this example, two-factor authentication is set up with a smartphone. Enter your phone number in the field and select how you would like to receive the code, for example via SMS. Click "Next".



The phone number will be validated and, in this example, a code will be sent by SMS to the phone number you entered.  
The second step for setting up two-factor authentication will appear.

7. In the second step, enter the code that you received on your smartphone by SMS or phone call.

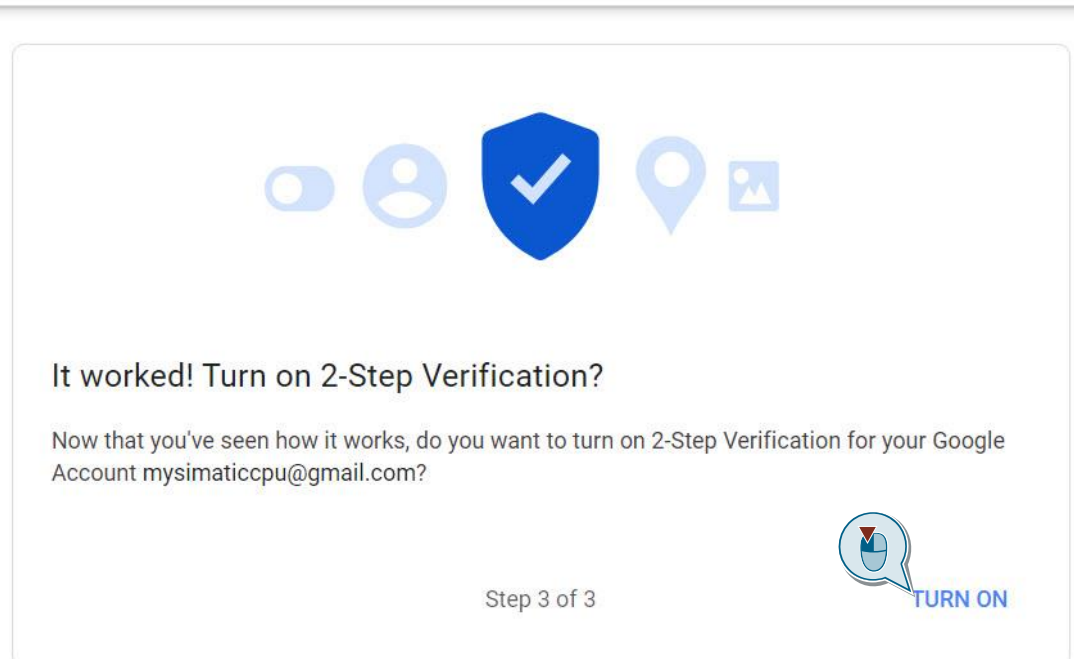
← 2-Step Verification



The code will be validated.  
The third step for setting up two-factor authentication will appear.

8. If validation was successful, click "TURN ON" in the third step to enable two-factor authentication.

← 2-Step Verification



### Result

Two-factor authentication has been set up.

#### ← 2-Step Verification


2-Step Verification is ON since 27 Jun 2022

[TURN OFF](#)

#### Available second steps

A second step after entering your password verifies that it's you signing in. [Learn more](#)

**Note:** If you sign in to your Google Account on any eligible phone, Google prompt will be added as another method for 2-Step Verification.



**Voice or text message (Default)** ?

0163 Verified

Verification codes are sent by text message.

>

#### Add more second steps to verify that it's you

Set up additional backup steps so that you can sign in even if your other options aren't available.

### Generate app password

Follow the steps below to generate an app password:

1. To open the overview page of the security settings, click the arrow icon before "2-Step Verification".

#### ← 2-Step Verification


2-Step Verification is ON since 27 Jun 2022

[TURN OFF](#)

#### Available second steps

A second step after entering your password verifies that it's you signing in. [Learn more](#)

**Note:** If you sign in to your Google Account on any eligible phone, Google prompt will be added as another method for 2-Step Verification.



**Voice or text message (Default)** ?

0163 Verified

Verification codes are sent by text message.

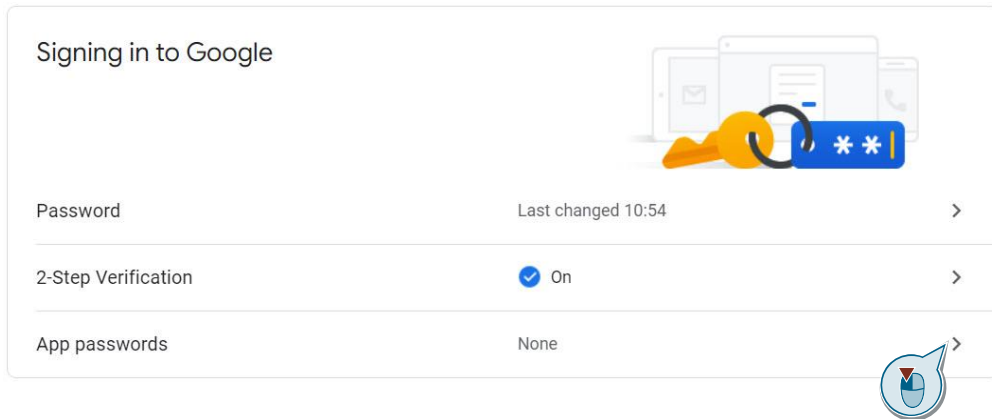
>

#### Add more second steps to verify that it's you

Set up additional backup steps so that you can sign in even if your other options aren't available.

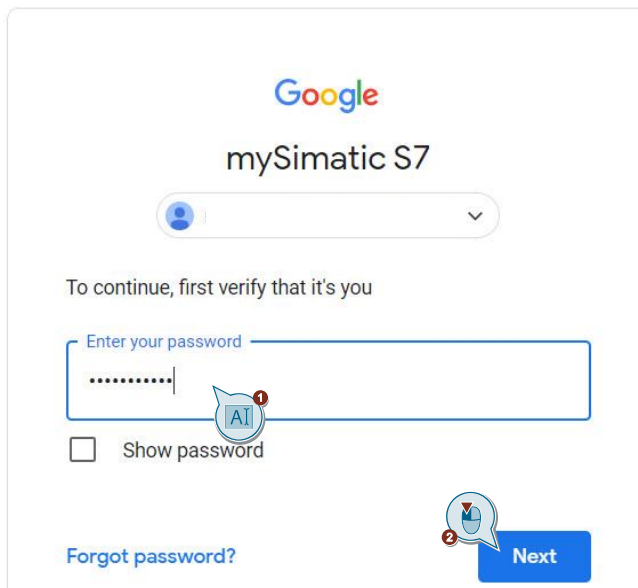
The security settings overview page opens.

2. In the "Signing in to Google" section, click on "App passwords".



The sign-in dialog appears.

3. Log in to your email account.  
Enter the password for your email account and click "Next".

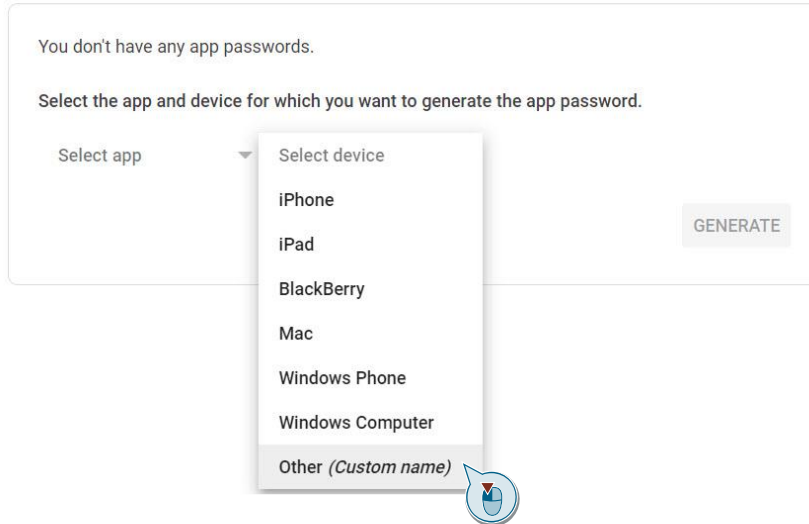


The app password generation dialog appears.



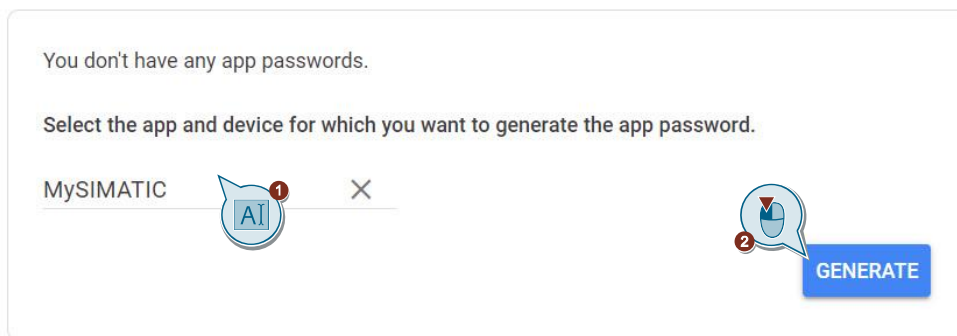
4. Open the dropdown list by "Select device" and select "Other (Custom name)".  
← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)



5. Enter a name for the device, e.g. "MySIMATIC", then click on "GENERATE".  
← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)



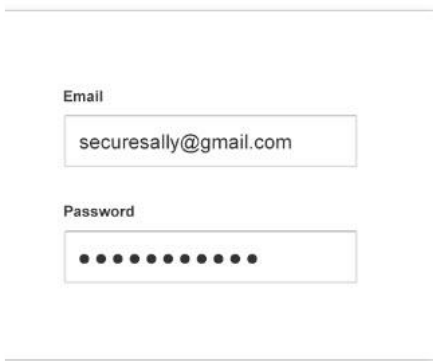
**Result**

An app password will be generated and shown in a new dialog. Note down this password. You will use this password in the SIMATIC to sign into your email account. Enter the parameter in the "PassWord" parameter in the system data type for the "TMAIL\_C" instruction (see [chapter 2.9.3](#)).

**Note**

This code shown here is just an example. Your string will be different.

**Generated app password**



Your app password for your device

barj lmek outw cazr

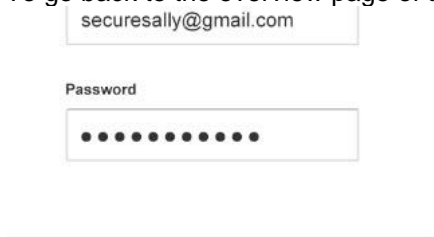
How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

DONE

- 6. To go back to the overview page of the security settings, click on "DONE".



the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.



### **2.3.2 Brief instructions for other email providers**

#### **GMX**

1. In the "Start" or "E-Mail" tab, click on Settings.
2. Select "POP3/IMAP request".
3. Enable the function "Allow POP3 and IMAP access".
4. Click "Save".

#### **Web.de**

1. In the "Start" or "E-Mail" tab, click on Settings.
2. Select "POP3/IMAP request".
3. Enable the function "Allow POP3 and IMAP access".
4. Click "Save".

#### **T-Online**

T-Online access allows access from any email client. Here only a valid email password is necessary.

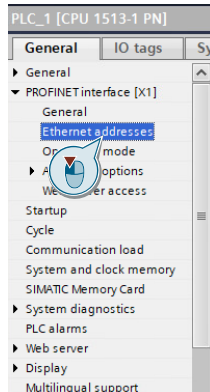
1. Click the "Settings" icon.
2. Select "Passwords".
3. Under "Password for email program", click "Change password for email program".
4. Set a password.

## 2.4 TIA project: Setting up IP addresses

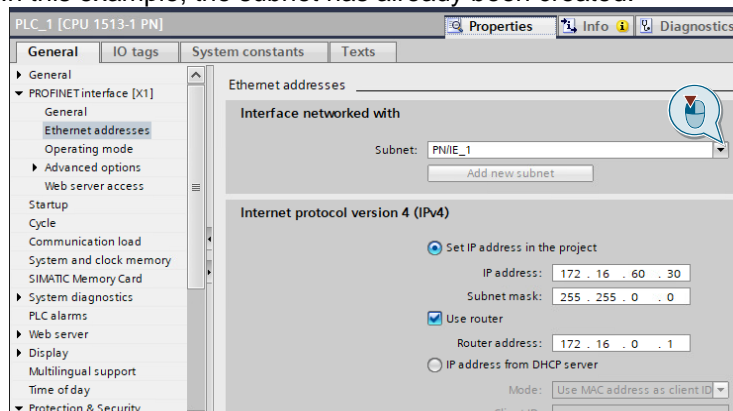
### Configure module IP addresses

Proceed as follows to set the IP address of the CPU or CP:

1. In the Network view or the Device view, select the CPU or CP. The properties of the CPU or CP appear in the Inspector window. In the area navigation of the "General" tab, select the item "Ethernet addresses" under "PROFINET interface [X1]".

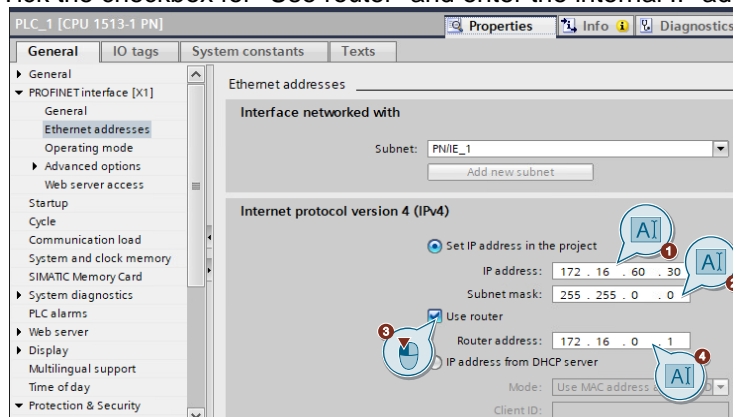


2. To network the Ethernet interface, select an already existing subnet, for example PN/IE\_1. If you have not created a subnet, then create one by clicking "Add new subnet". In this example, the subnet has already been created.



The "Ethernet addresses" pane appears.

3. Enter the IP address and subnet mask of the CPU or CP.  
Tick the checkbox for "Use router" and enter the internal IP address of the DSL router.



**Note**

The IP address of the CPU or CP and the internal IP address of the DSL router must be in the same IP subnet.

### Configure the DNS server

Depending on the system data type you are using, the "TMAIL\_C" instruction allows you to address the email provider with an IP address or a fully qualified domain name.

To address the email provider or an NTP server with its name, it is necessary to configure a DNS server in the CPU or CP.

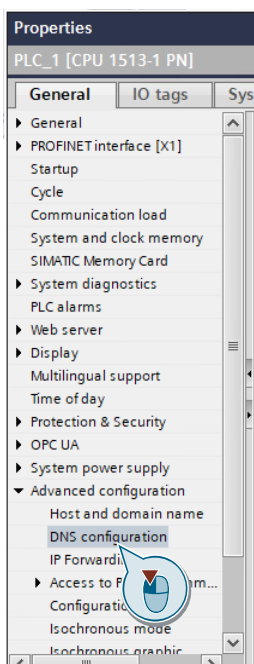
**Note**

If your DSL router is DNS-capable, you can enter the internal IP address of the DSL router as the DNS server.

Otherwise, use a DNS server such as 1.1.1.1

Follow these steps:

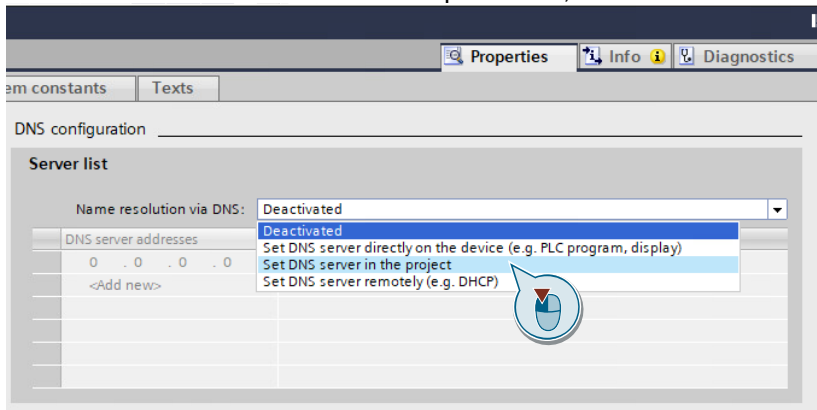
1. Select the CPU or CP in the network or device view. The properties will appear in the Inspector window. Open the "General" tab in the area navigation. You can find the DNS configuration here:
  - For the CPU, in the menu "Advanced configuration > DNS configuration"
  - For the CP, in the menu "DNS configuration"



The "DNS configuration" pane appears.

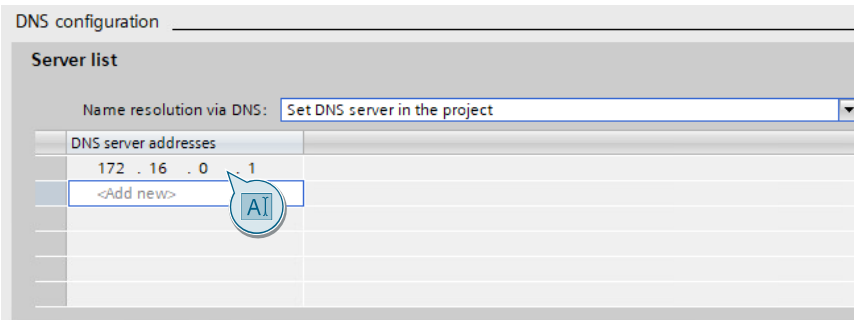


2. In the "Name resolution via DNS" dropdown list, select "Set DNS server in the project".



The "DNS server addresses" column becomes editable.

3. Add the internal IP address of the DSL router as the DNS server address in the server list.



### Result

You have configured a DNS server.

## 2.5 TIA Portal: Setting the time

Because a certificate always has a time period over which it is valid, the clock time of the CPU or CP that wants to encrypt with this certificate must also be in this time period.

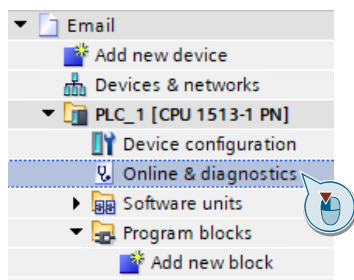
With a brand new CPU or CP, or after a full reset of the CPU, the internal clock will be set to a default value that lies outside the certificate runtime. The certificate will then be marked as invalid.

### 2.5.1 Set the CPU's clock

#### Set the time manually

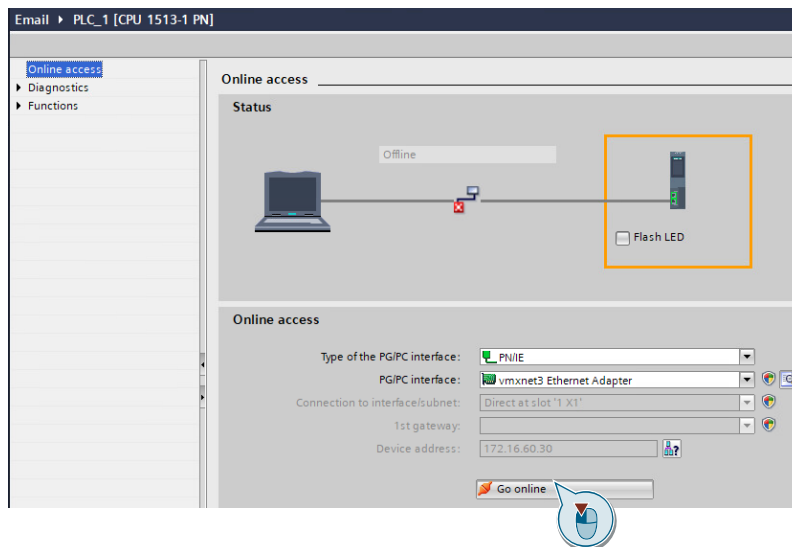
One option is to set the time manually. Follow these steps:

1. In the project tree, double-click "Online & diagnostics" in the device folder of the CPU.



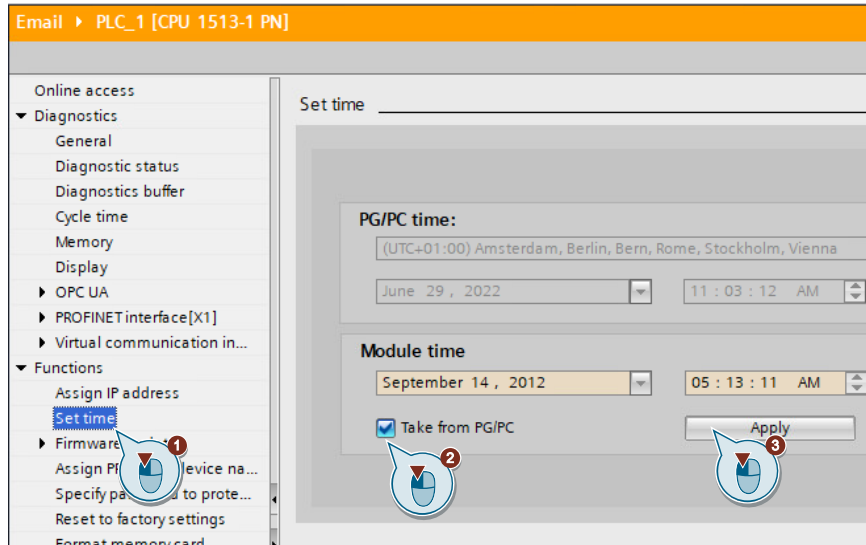
The Online and Diagnostics view will open.

2. Click the button "Go online".



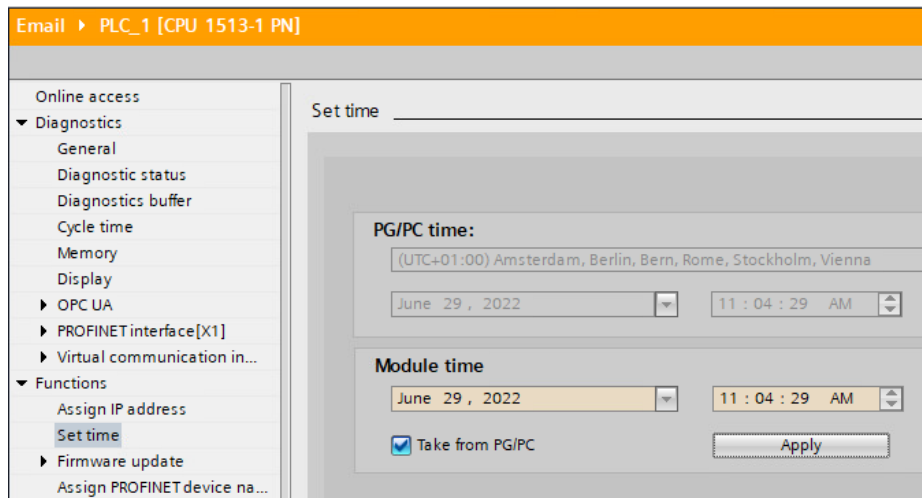
The online view opens.

3. In the area navigation of the Online and Diagnostics view, select "Set time" under "Functions".  
Enable the function "Take from PG/PC".  
Click "Apply".



### Result

The module clock matches the time of the PG/PC.



## Synchronize CPU time with NTP method

You can synchronize the CPU's time with an NTP server using the NTP method.

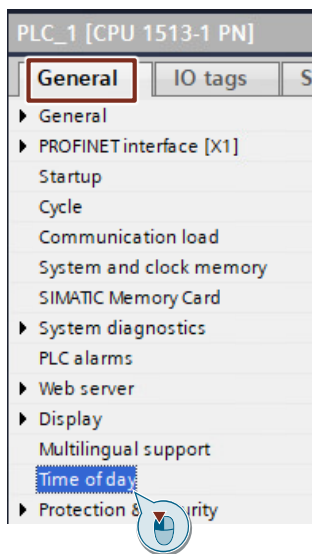
For the NTP method, the CPU sends clock time requests at regular intervals (in client mode) to NTP servers in the subnet (LAN). Using the answers from the servers, the most reliable and accurate time is determined and the time of the CPU is synchronized.

For time synchronization sources you will address using the IP address, e.g. a communication processor (CP) or an HMI device.

The update interval defines the interval between the time queries (in seconds). The value of the interval ranges between 10 seconds and one day. In NTP mode, it is generally UTC (Universal Time Coordinated) which is taken. UTC corresponds to GMT (Greenwich Mean Time).

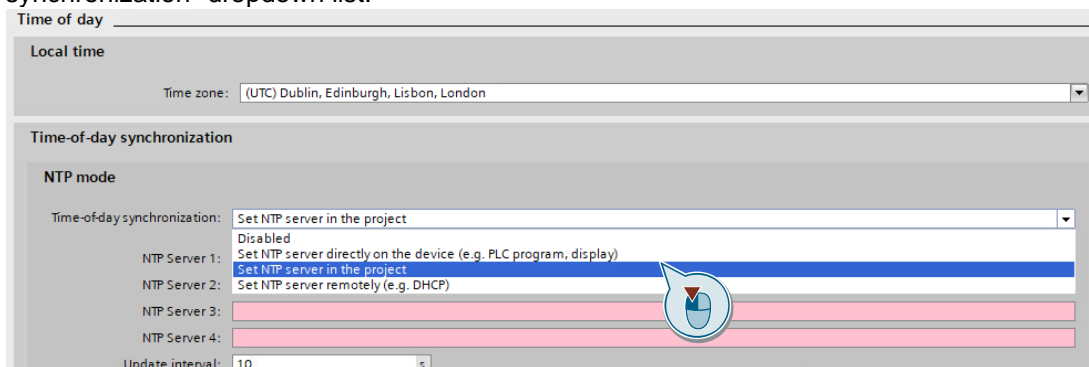
Proceed as follows to configure one or more NTP servers for the CPU:

1. Select the CPU in the network or device view. The properties of the CPU are displayed in the Inspector window. In the area navigation of the "General" tab, select "Time of day".



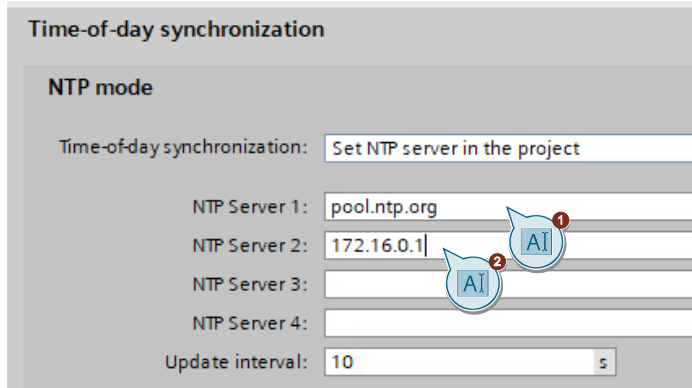
The "Time of day" pane opens.

2. In the "NTP mode" section, select "Set NTP server in the project" from the "Time-of-day synchronization" dropdown list.

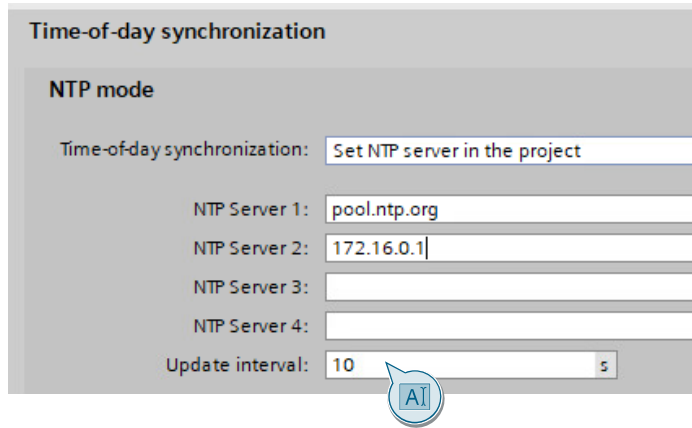


This item will be selected in the dropdown list.

- At the parameters "NTP Server 1" through "NTP Server 4", enter the IP addresses of up to four NTP servers.



- Set the time interval of the clock requests at the "Update interval" parameter. Set the interval between 10 s and 86400 s.



**Note**

If you address an NTP server with a name, for example "pool.ntp.org", then you must configure a DNS server in the CPU (see [chapter 2.4](#)).

**Result**

You have set up NTP time synchronization in the CPU.

## 2.5.2 Set the CP's clock

Because a certificate always has a time period over which it is valid, the time of the CP that wants to encrypt with this certificate must also be in this time period.

You can synchronize the CP's time using the NTP method with an NTP server.

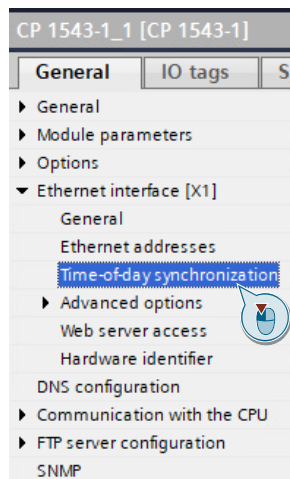
The CP sends time queries at regular intervals to an NTP server and synchronizes its local time of day.

Moreover, the time will be automatically forwarded to the CPU in the S7 station, thus synchronizing the time in the entire S7 station.

Proceed as follows to configure one or more NTP servers for the CP:

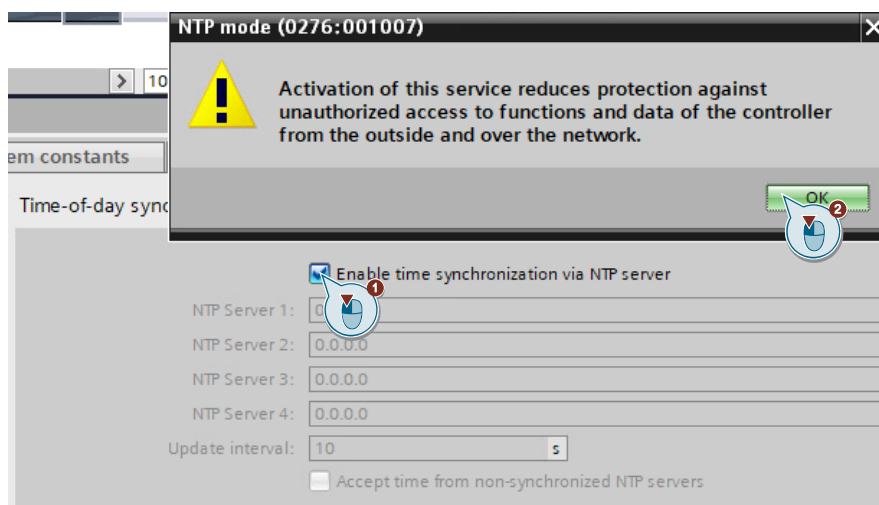
1. Select the CP in the network or device view. The properties of the CP are displayed in the Inspector window.

In the area navigation of the "General" tab, select "Time-of-day synchronization" under "Ethernet interface [X1]".



The "Time-of-day synchronization" pane opens.

2. Enable the function "Enable time synchronization via NTP server" and acknowledge the warning message with "OK".



- At the parameters "NTP Server 1" through "NTP Server 4", enter the IP addresses of up to four NTP servers.

Time-of-day synchronization

Enable time synchronization via NTP server

NTP Server 1: 172.16.0.1

NTP Server 2: 0.0.0.0

NTP Server 3: 0.0.0.0

NTP Server 4: 0.0.0.0

Update interval: 10 s

Accept time from non-synchronized NTP servers

- Enter the time interval of the clock requests at the "Update interval" parameter. Set the sync cycle between 10 s and 86400 s.

Time-of-day synchronization

Enable time synchronization via NTP server

NTP Server 1: 172.16.0.1

NTP Server 2: 0.0.0.0

NTP Server 3: 0.0.0.0

NTP Server 4: 0.0.0.0

Update interval: 10 s

Accept time from non-synchronized NTP servers

**Note**

If you address an NTP server with a name, for example "pool.ntp.org", then you must configure a DNS server in the CP (see [chapter 2.4](#)).

**Result**

You have set up NTP time synchronization in the CP.

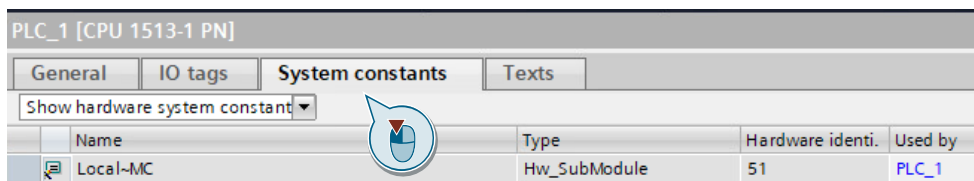
## 2.6 TIA Portal: Finding the hardware identifier

For the "TMAIL\_C" instruction, you will need the hardware identifier of the Ethernet port on the CPU or CP.

### Finding the hardware identifier

Proceed as follows to find the hardware identifier of the Ethernet port on the CPU or CP:

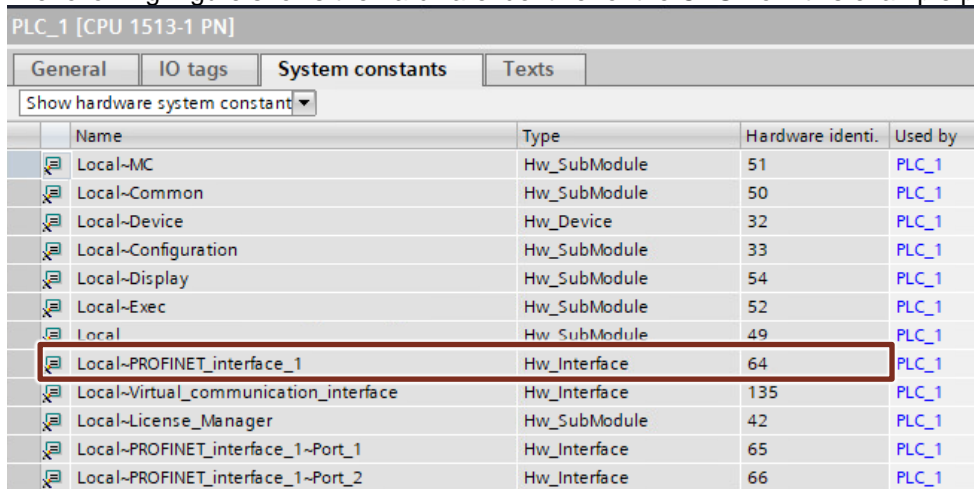
1. In the Network view or the Device view, select the CPU or CP. The properties of the module appear in the Inspector window.
2. To display the hardware identifier of the module, select the tab "System constants".



Name	Type	Hardware identi.	Used by
Local-MC	Hw_SubModule	51	PLC_1

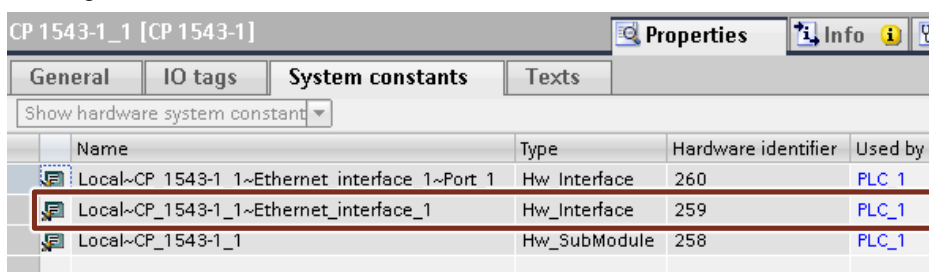
3. You need the hardware identifier of the Ethernet port on the module. Note down the value of the hardware identifier.

The following Figure shows the hardware identifier of the CPU from this example project:



Name	Type	Hardware identi.	Used by
Local-MC	Hw_SubModule	51	PLC_1
Local-Common	Hw_SubModule	50	PLC_1
Local-Device	Hw_Device	32	PLC_1
Local-Configuration	Hw_SubModule	33	PLC_1
Local-Display	Hw_SubModule	54	PLC_1
Local-Exec	Hw_SubModule	52	PLC_1
Local	Hw_SubModule	49	PLC_1
Local-PROFINET_interface_1	Hw_Interface	64	PLC_1
Local-Virtual_communication_interface	Hw_Interface	135	PLC_1
Local-License_Manager	Hw_SubModule	42	PLC_1
Local-PROFINET_interface_1-Port_1	Hw_Interface	65	PLC_1
Local-PROFINET_interface_1-Port_2	Hw_Interface	66	PLC_1

The Figure below shows the hardware identifier of a CP:



Name	Type	Hardware identifier	Used by
Local-CP 1543-1 1-Ethernet interface 1-Port 1	Hw Interface	260	PLC 1
Local-CP_1543-1_1-Ethernet_interface_1	Hw_Interface	259	PLC_1
Local-CP_1543-1_1	Hw_SubModule	258	PLC_1

### Result

You have found the hardware ID of the CPU or CP. You will enter the hardware identifier in the "Interfaceld" parameter of the system data type of the "TMAIL\_C" instruction (see [chapter 2.9.3](#)).



## 2.7 TIA Portal: Module security settings

In order to enable the security functions in the CPU or CP, a user with sufficient configuration permissions must log in.

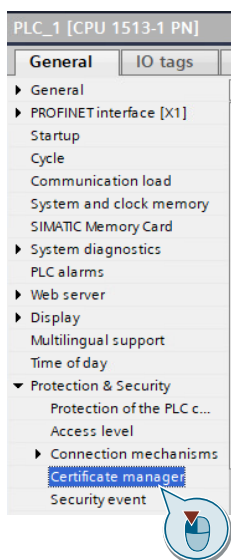
A Security user is allowed to make global security changes.

### 2.7.1 Enable global security settings in the CPU

To enable the global security settings in the CPU, proceed as follows:

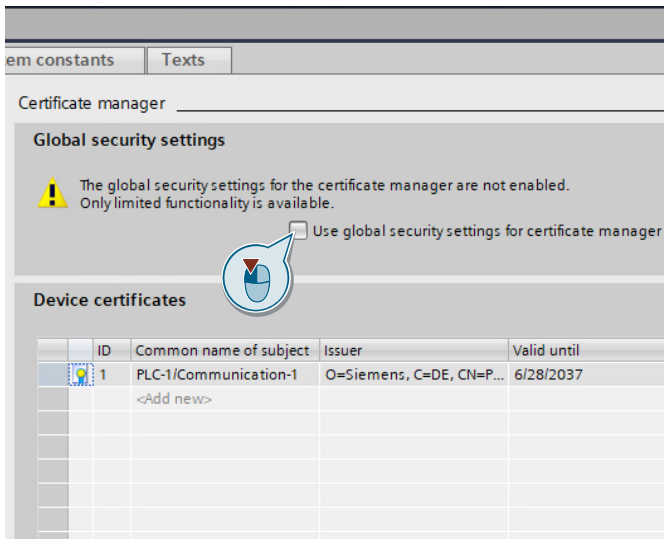
1. In the Device or Network view, select the CPU. The properties of the CPU are displayed in the Inspector window.

In the "General" tab, select "Protection & Security > Certificate manager".



The "Certificate manager" pane opens.

- In the "Global security settings" section, enable the function "Use global security settings for certificate manager".



A warning message appears.

- Confirm it with "OK".



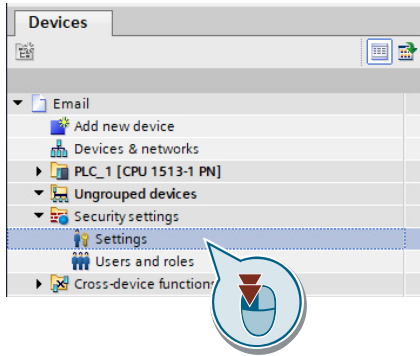
**Result**

The global security settings are enabled in the CPU.

### 2.7.2 Create and sign in a security user

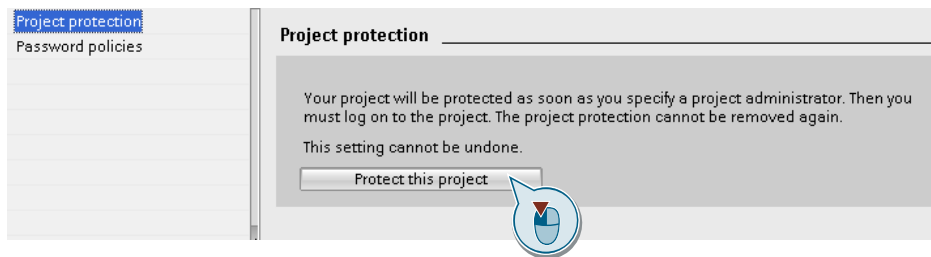
To create a security user and sign in with it, proceed as follows:

1. In the project tree, double-click in the "Security settings" folder on the item "Settings".



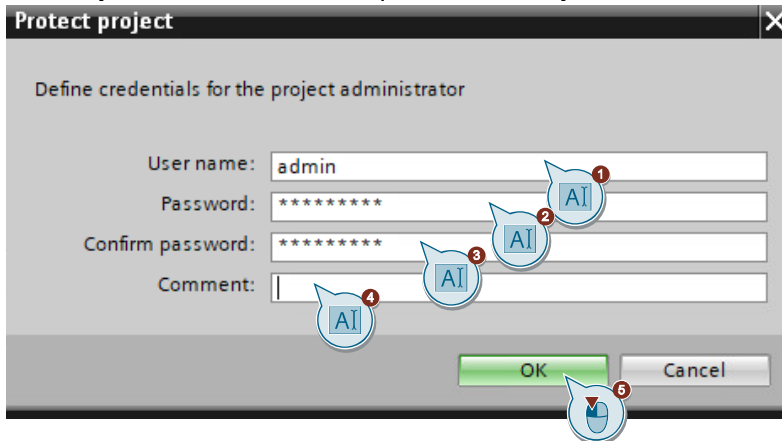
The user administration editor opens and the project protection area is displayed.

2. Click the "Protect this project" button.



The "Project protection" dialog opens.

3. Enter a username and password, then confirm the password. You may enter a comment if required. Confirm your entries with "OK".

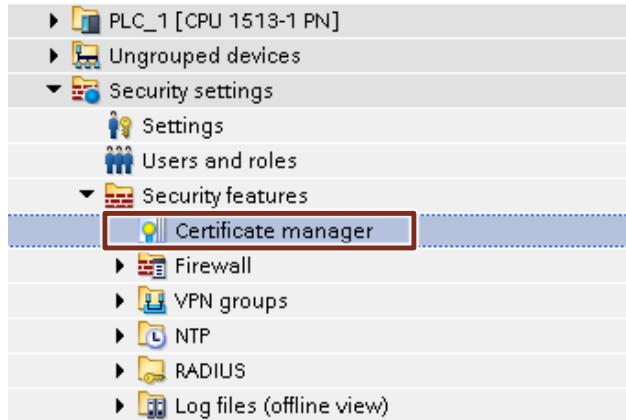


The dialog closes.

**Result**

User administration is active. You are logged in as project administrator and can use the security functions.

Once you have logged in, the line "Certificate manager" will appear under "Security settings > Security features".

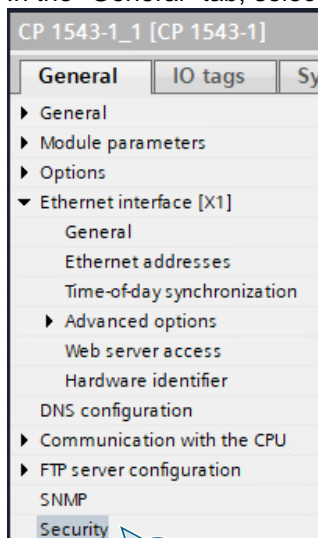
**2.7.3 Enable global security settings in the CP**

To enable the global security settings in the CP, first designate a security user and then sign in (see [chapter 2.7.2](#)).

Then proceed as follows:

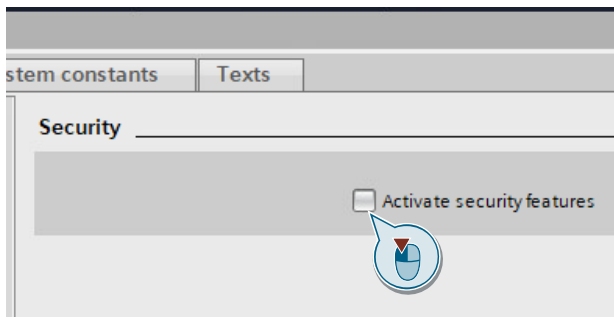
1. Select the CP in the device or network view. The properties of the CP are displayed in the Inspector window.

In the "General" tab, select "Security".



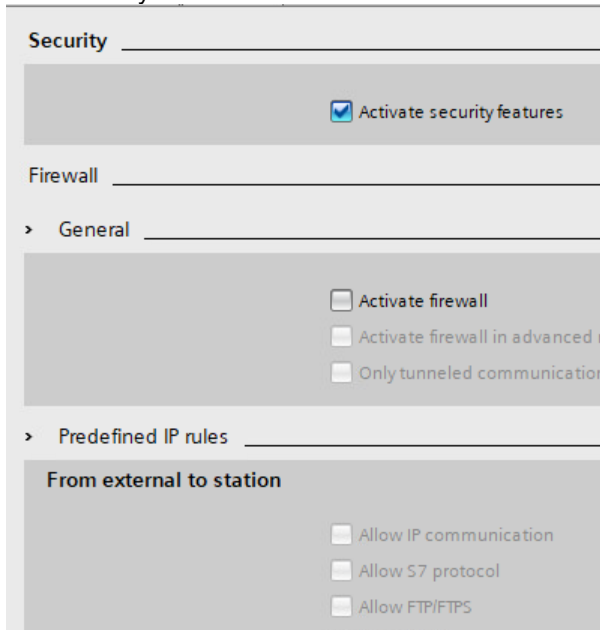
The "Security" pane appears.

2. Enable the function "Activate security features".



**Result**

The security features have been enabled in the CP. New panes are now visible.



## 2.8 TIA Portal: Importing provider certificate

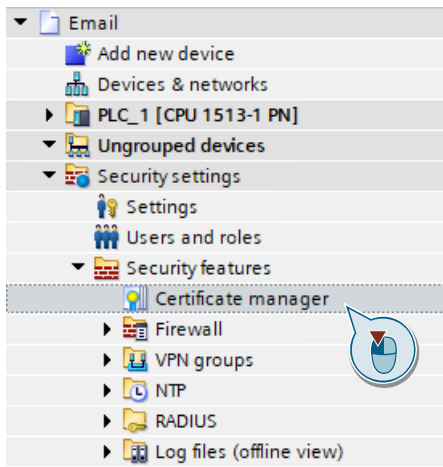
### Import provider certificate into the global certificate manager

Using the global certificate manager, you have the ability to import external certificates into TIA Portal. In the "Certificate manager" you will receive access to all certificates in the project, divided into the following tabs:

- "Certification Authority (CA)"
- "Device certificates"
- "Trusted certificates and root certification authorities"

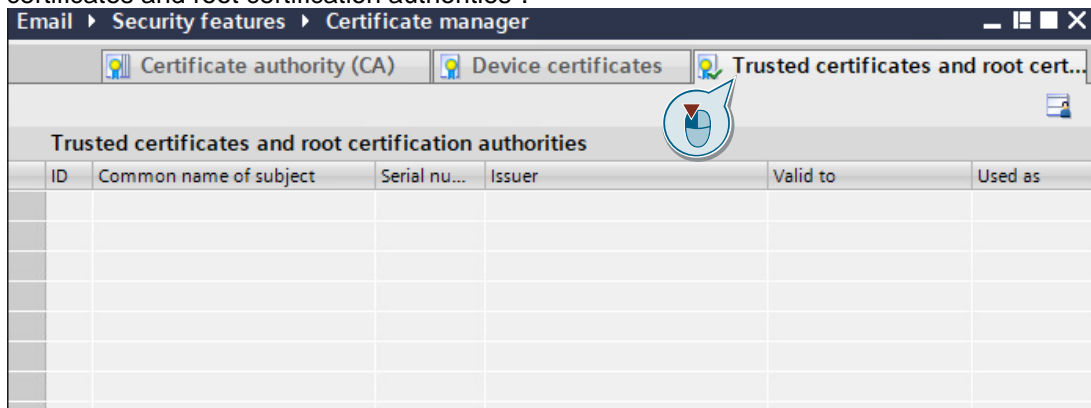
Proceed as follows to import the provider certificates into TIA Portal:

1. Under "Security settings > Security features" in the project tree, double-click on "Certificate manager".

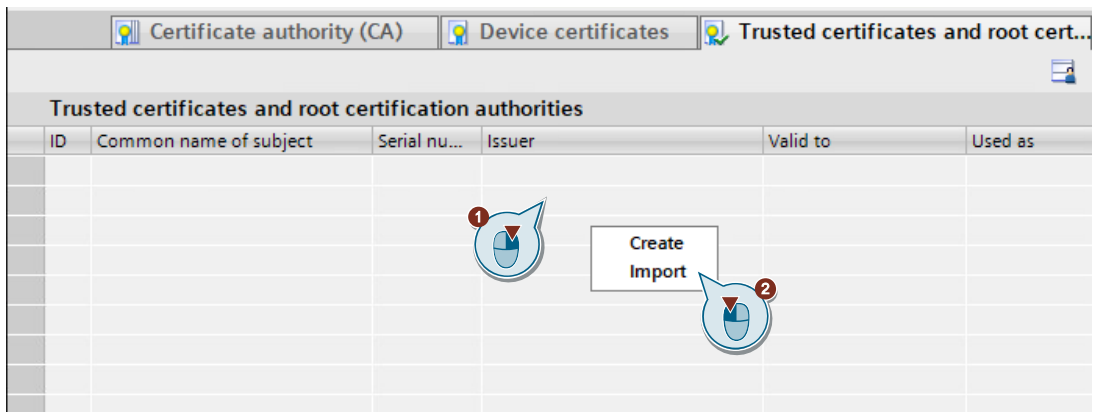


The certificate manager opens.

2. Select the appropriate tab for the certificate you want to import, for example, "Trusted certificates and root certification authorities".

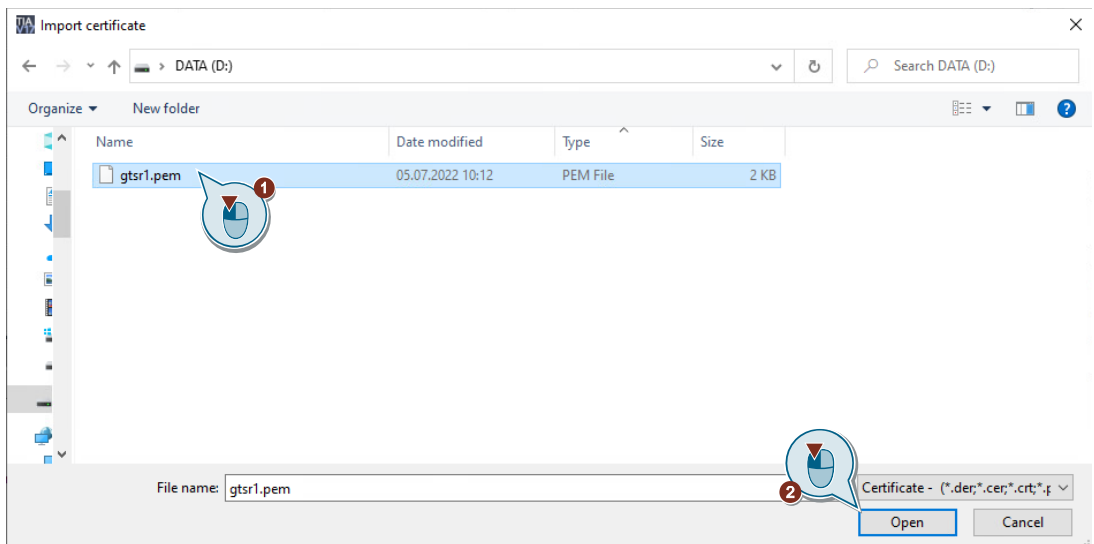


- To open the context menu, right-click inside the tab. Select "Import" from the context menu.



The dialog for selecting a certificate opens.

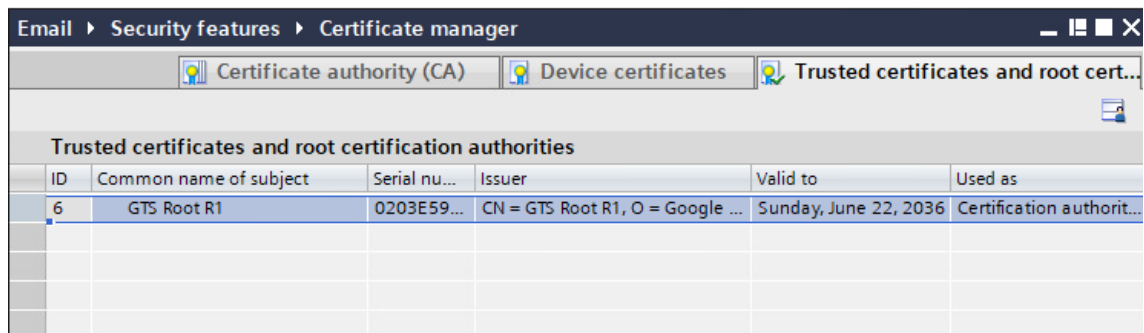
- Navigate to the folder where you saved the provider certificate (see [chapter 2.2.2](#)) and click "Open".



The dialog closes.

### Result

The provider certificate is located in the global certificate manager.



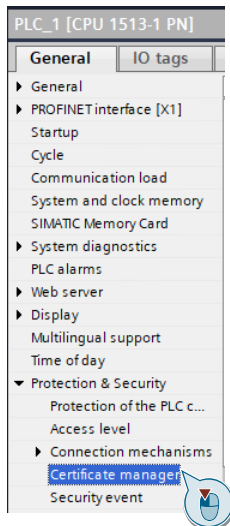
## Assign provider certificate to the local certificate manager

The provider certificate is initially only located in the global certificate manager in TIA Portal. Certificates imported via the certificate manager into the global security settings are not automatically assigned to the corresponding modules.

In order to authenticate the provider, it is necessary to load its CA certificate into the CPU or the CP. Only the device certificates that you have assigned to the module as device certificates via the local certificate manager will be loaded to the module.

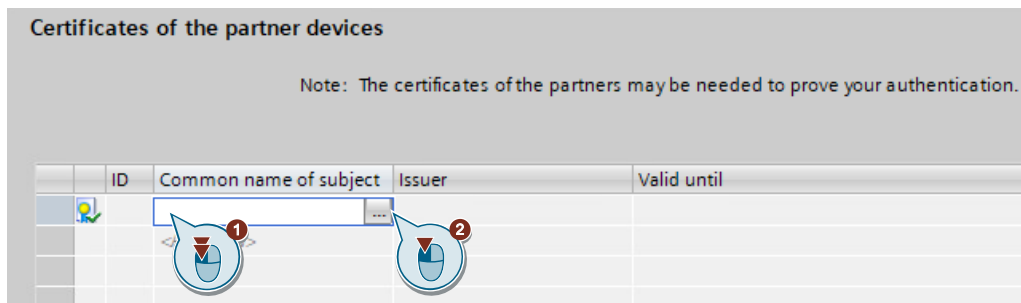
The following steps will show you how to assign the provider certificate to the CPU or CP in the local certificate manager.

1. Select the CPU or CP in the device or network view. The properties will appear in the Inspector window. In the area navigation, go to the "General" tab. Open the local certificate manager. You can find the local certificate manager as follows:
  - With the CPU, in the menu "Protection & Security > Certificate manager"
  - With the CP, in the menu "Security > Certificate manager"



The local certificate manager appears.

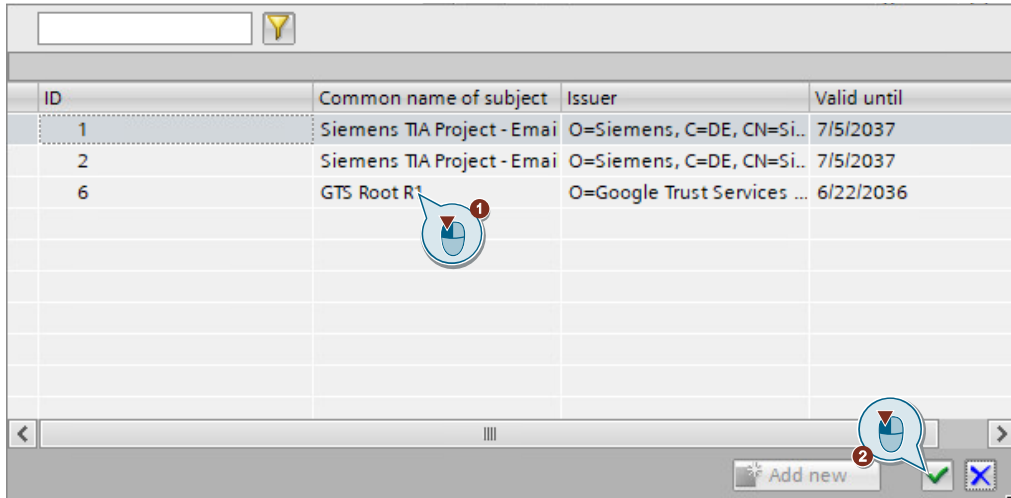
2. In the section "Certificates of the partner devices", double-click in the "Common name of subject" column of an empty table row, then click on "...".



A dropdown menu will open for selecting a certificate.



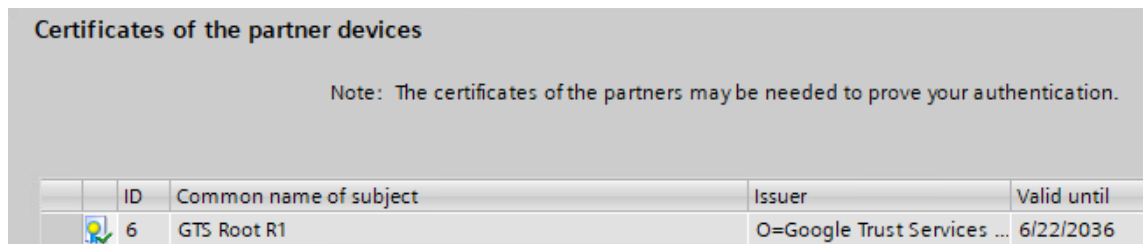
3. Select the provider certificate that you need and confirm your selection with the green checkbox.



The dropdown menu closes.

**Result**

The provider certificate is added to the table "Certificates of the partner devices"; the unique project-wide ID (here: ID = 6) appears. You will need this ID for the "TLSServerCertRef" parameter in the system data type of the "TMAIL\_C" instruction (see [chapter 2.9.3](#)).



## 2.9 TIA Portal: Using MAIL\_C

The "TMAIL\_C" instruction lets you send an email over a secure connection via the Ethernet port of a CPU, CM or CP.

Depending on which format you wish to address the email server in, you will use the following structure at the "MAIL\_ADDR\_PARAM" parameter of the "TMAIL\_C" instruction:

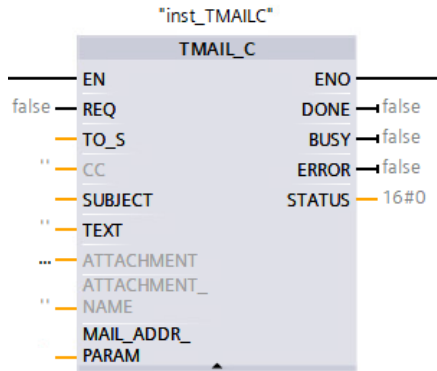
- TMail\_V4\_SEC: Addressing via the IP address according to IPv4
- TMail\_V6\_SEC: Addressing via the IP address according to IPv6
- TMail\_QDN\_SEC: Addressing via the fully qualified domain name (FQDN)

**Note**

Only system data types that support a secure connection will be listed. For more information on the "TMAIL\_C" instruction and the system data types, see [chapter 3](#).

### 2.9.1 Parameters of the "TMAIL\_C" instruction

The following Figure illustrates the call of the "TMAIL\_C" V6.1 instruction:



The following Table shows the input parameters of the "TMAIL\_C" instruction.

Table 2-3

Input parameter	Data type	Description
REQ	BOOL	Control parameter The input parameter REQ enables sending of an email in the event of a positive edge.
TO_S	STRING	Receiver address String with a max. length of 240 characters (byte).
SUBJECT	STRING	Subject of the email String with a max. length of 240 characters (byte).
TEXT	STRING	Text of the email String with a max. length of 240 characters (byte). If an empty string is assigned to this parameter, the email will be sent without any text.
MAIL_ADDR_PARAM	VARIANT	Connection parameters: Parameters of the connection and address of the email server. The connection parameters are summarized in the system data type <ul style="list-style-type: none"> <li>• Tmail_QDN_SEC,</li> <li>• Tmail_v4_SEC or</li> <li>• Tmail_v6_SEC</li> </ul>

The following Table shows the output parameters of the "TMAIL\_C" instruction.

Table 2-4

Output parameter	Data type	Description
DONE	BOOL	State parameter DONE = 0: Job is not yet started or is still being run. DONE = 1: Job completed with no errors.
BUSY	BOOL	State parameter BUSY = 0: The processing of TMAIL_C has completed BUSY = 1: Sending the email not yet completed
ERROR	BOOL	State parameter ERROR = 0: No error ERROR = 1: An error occurred during processing. STATUS provides detailed information on the type of error.
STATUS	WORD	State parameter Returned value or error information from the "TMAIL_C" instruction

## 2.9.2 Create global data block

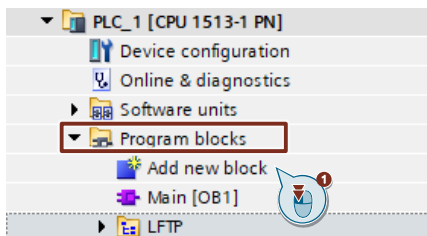
In this chapter, you will create a global data block for the parameters of the "TMAIL\_C" instruction. The parameters are structured as follows:

- Control parameter
- Parameters for the email
- Parameters for the connection and the address of the email server

### Create data block

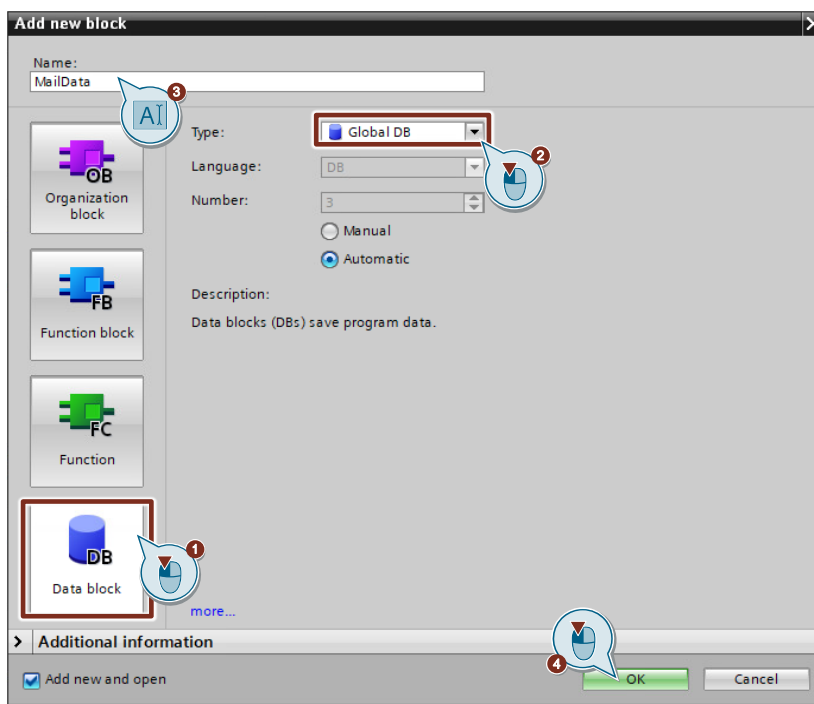
Proceed as follows to create a new global data block:

1. In the project tree, navigate to the device folder of the CPU.
2. Open the "Program blocks" folder and double-click the "Add new block" command.



The dialog "Add new block" opens.

3. Create a new Global DB and assign a block name, e.g. "MailData". Acknowledge the dialog with "OK".



The "Add new block" dialog closes.

### Result

The new data block appears in the program folder of the CPU.

## Control parameter

Open the data block.

Define the following control tags in the data block. Double-click "<Add new>" in an empty row to do this.

▼ Static	
■ ▼ control	Struct
■ request	Bool
■ done	Bool
■ busy	Bool
■ error	Bool
■ status	Word

## Email parameters

To create the email parameters, add the tags shown below.

Double-click "<Add new>" in an empty row to do this.

▼ emailParam	Struct
■ recipientAddress	String
■ subject	String
■ text	String

## Email server parameters

Extend the data block by adding the system data type that you need to address the email server. This example uses the system data type "TMail\_QDN\_SEC".

Double-click "<Add new>" in an empty row to do this.

▼ serverParam	TMail_QDN_SEC
■ InterfaceId	HW_ANY
■ ID	CONN_OUC
■ ConnectionType	Byte
■ ActiveEstablished	Bool
■ WatchDogTime	Time
■ MailServerQDN	String[254]
■ UserName	String[254]
■ PassWord	String[254]
■ ▶ From	EMAIL_ADDR
■ RemotePort	UInt
■ ActivateSecureConn	Bool
■ ExtTLSCapabilities	Byte
■ TLSServerCertRef	UDInt

**Result**

The data block with all the necessary tags has been declared.

Static	
control	Struct
request	Bool
done	Bool
busy	Bool
error	Bool
status	Word
<Add new>	
emailParam	Struct
recipientAddress	String
subject	String
text	String
<Add new>	
serverParam	TMail_QDN_SEC
InterfaceId	HW_ANY
ID	CONN_OUC
ConnectionType	Byte
ActiveEstablished	Bool
WatchDogTime	Time
MailServerQDN	String[254]
UserName	String[254]
PassWord	String[254]
From	EMAIL_ADDR
RemotePort	UInt
ActivateSecureConn	Bool
ExtTLSCapabilities	Byte
TLSServerCertRef	UDInt

### 2.9.3 Parameterize tags

Assign values to the email parameters and the email server parameters in the data block. Specify your own recipient address, username, password and certificate ID.

**Note**

For help on parameterization of the system data type, refer to the Figure below or see [chapter 3.3](#).

MailData			
Name	Data type	Start value	
Static			
control	Struct		
request	Bool	false	
done	Bool	false	
busy	Bool	false	
error	Bool	false	
status	DWord	16#0	
<Add new>			
emailParam	Struct		
recipientAddress	String	'testperson@gmail.com'	
subject	String	'TestMail'	
text	String	'My First email from PLC'	
serverParam	TMail_QDN_SEC		
InterfaceId	HW_ANY	64	
ID	CONN_OUC	100	
ConnectionType	Byte	22	
ActiveEstablished	Bool	true	
WatchDogTime	Time	T#0ms	
MailServerQDN	String[254]	'smtp.gmail.com.'	
UserName	String[254]	'myEmail@gmail.com'	
PassWord	String[254]	'barjlmekoutqcazr'	
From	EMAIL_ADDR		
LocalPartPlusAt...	String[64]	'myEmail@'	
FullQualifiedD...	String[254]	'gmail.com'	
RemotePort	UInt	587	
ActivateSecureConn	Bool	true	
ExtTLSCapabilities	Byte	16#0	
TLSServerCertRef	UDInt	6	

**Parameterize system data type "TMail\_QDN\_SEC"**

The email server is addressed via its fully-qualified domain name (FQDN) with the system data type "TMail\_QDN\_SEC".

Table 2-5

Parameter	Data type	Value	Description
Interfaceld	LADDR	64	Hardware identifier of the Ethernet port of the CPU or CP (see <a href="#">chapter 2.6</a> )
ID	CONN_OUC	1	Connection ID
ConnectionType	BYTE	16#22	Connection type For FQDN, select 16#22 as connection type.
ActiveEstablishment	BOOL	True	Actively or passively establish connection. Because the CPU or CP is always the SMTP client, this parameter must be set to "True".
WatchDogTime	TIME	T#0ms	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process. <b>Note</b> With "TMAIL_C" V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerQDN	STRING[254]	e.g.: 'smtp.gmail.com.'	FQDN (full qualified domain name) of the email server from which you wish to send an email to a recipient (see <a href="#">chapter 3.1</a> ). Note the period at the end.
UserName	STRING[254]	e.g.: 'username@gmail.com'	Username and password for identifying the email account. For Gmail, use the "app password" as the password (see <a href="#">chapter 2.3.1</a> ).
PassWord	STRING[254]	e.g.: 'password'	
From	EMAIL_ADDR	-	Sender address of the email which is defined with the following two STRING parameters.



Parameter	Data type	Value	Description
LocalPartPlusAtSign	STRING[64]	e.g.: 'username@'	Local part of the sender address including @ sign.
FullQualifiedDomainName	STRING[254]	e.g.: 'gmail.com'	FQDN (fully qualified domain name) of the email server
RemotePort	UINT	587	TCP port of the email server Value range: <ul style="list-style-type: none"> <li>• 25 (unsecured)</li> <li>• 465 (secured)</li> <li>• 587 (secured)</li> </ul> (see <a href="#">chapter 3.1</a> )
ActivateSecureConn	BOOL	true	True = Secure SMTP connection
ExtTLSCapabilities	BYTE	16#0	Value range: 16#0, 16#1 For 16#1, the alternative applicant is verified in the server's certificate. The IP address or DNS name entered there must match the IP address or the DNS name of the server.
TLSServerCertRef	UDINT	16#6	Certificate number of the provider assigned in the TIA Portal certificate manager (see <a href="#">chapter 2.8</a> ).

### Parameter assignment for system data type "TMail\_v4\_SEC"

Using the system data type "TMail\_V4\_SEC", the email server will be addressed via the IP address in IPv4.

Table 2-6

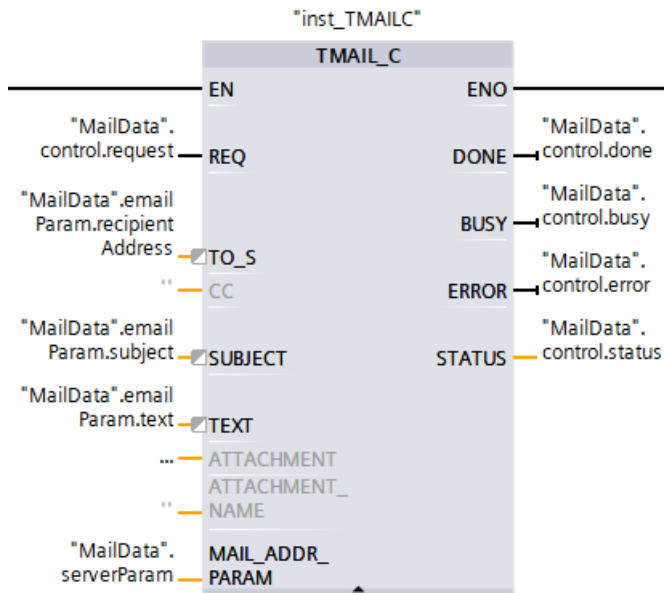
Parameter	Data type	Value	Description
Interfaceld	LADDR	261	Hardware identifier of the Ethernet port of the CPU or CP (see chapter <a href="#">2.6</a> )
ID	CONN_OUC	1	Connection ID
ConnectionType	BYTE	16#20	Connection type For IPv4, select 16#20 as connection type.
ActiveEstablishment	BOOL	True	Establish connection actively/passively. Because the CPU or CP is always the SMTP client, this parameter must be set to "True".
WatchDogTime	TIME	T#1m	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process. <b>Note</b> With "TMAIL_C" V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerAddress	IP_V4	e.g.: 213.165.67.108	IP address of the email server (in IPv4 format) from which you wish to send an email.
UserName	STRING[254]	e.g.: 'username@gmail.com'	Username and password for identifying the email account.
PassWord	STRING[254]	e.g.: 'password'	For Gmail, use the "app password" as the password (see <a href="#">chapter 2.3.1</a> ).

Parameter	Data type	Value	Description
From	EMAIL_ADDR	-	Sender address of the email which is defined with the following two STRING parameters.
LocalPartPlusAtSign	STRING[64]	e.g.: 'username@'	Local part of the sender address including @ sign.
FullQualifiedDomain Name	STRING[254]	e.g.: 'gmail.com'	FQDN (fully qualified domain name) of the email server
RemotePort	UINT	587	TCP port of the mail server Value range: <ul style="list-style-type: none"> <li>• 25 (unsecured)</li> <li>• 465 (secured)</li> <li>• 587 (secured)</li> </ul> (see <a href="#">chapter 3.1</a> )
ActivateSecureConn	BOOL	True	True = Secure SMTP connection False = unsecured SMTP connection. In this case the subsequent parameters are irrelevant.
ExtTLSCapabilities	BYTE	16#0	Value range: 16#0, 16#1 For 16#1, the alternative applicant is verified in the server's certificate. The IP address or DNS name entered there must match the IP address or the DNS name of the server.
TLSServerCertRef	UDINT	16#6	Certificate number of the provider assigned in the TIA Portal certificate manager (see <a href="#">chapter 2.8</a> ).

### 2.9.4 Call "TMAIL\_C" instruction and interconnect

Cyclically call the "TMAIL\_C" instruction in the user program of the CPU. You can find the "TMAIL\_C" instruction in the "Instructions" Task Card under "Communication > Open user communication".

The following Figure illustrates the call of the instruction "TMAIL\_C" in the user program.

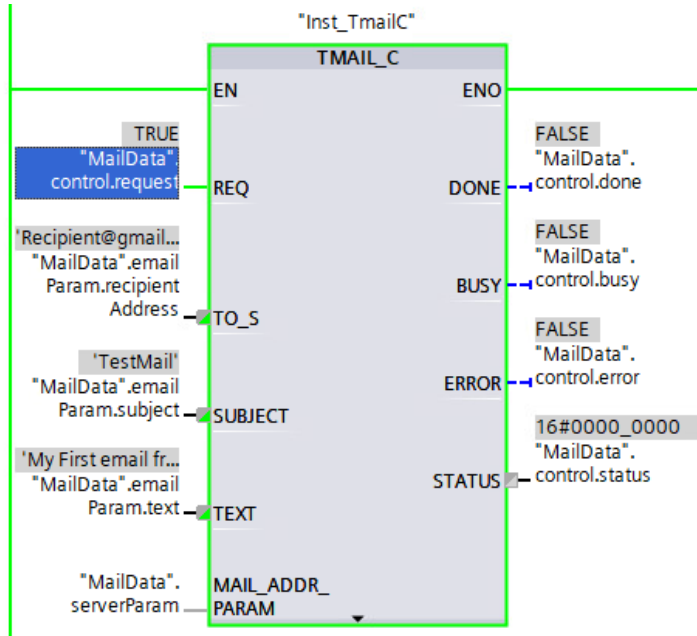


Interconnect the inputs and outputs of the instruction with the tags from the "MailData" data block (see [chapter 2.9.1](#)).

Compile the program and download it to the controller.

## 2.10 Operation

Control the "TMAIL\_C" instruction with a rising edge at the "REQ" parameter.  
Set the tag <MailData.control.request> to TRUE.



The "TMAIL\_C" instruction will send an email to the recipient referenced at the "TO\_S" parameter.

### Result

You will see the email in your recipient's email account.

^ Unread



## 3 Useful information

### 3.1 SMTP servers and ports of the providers

The following Table shows the SMTP servers and ports of some providers.

Table 3-1

Provider	SMTP server	TCP port
Web.de	smtp.web.de	587
GMX	mail.gmx.net	587
T-Online	securesmtp.t-online.de	587, 465
Gmail	smtp.gmail.com	587, 465

**Note**

Ping the SMTP server from a PG/PC to find the IP address of the SMTP server. Enter the ping command, e.g. ping smtp.web.de, in the Command Prompt.

### 3.2 "TMAIL\_C" instruction

**Description**

The "TMAIL\_C" instruction lets you send an email over a secure connection via the Ethernet port of an S7-1500 or S7-1200, CM or CP.

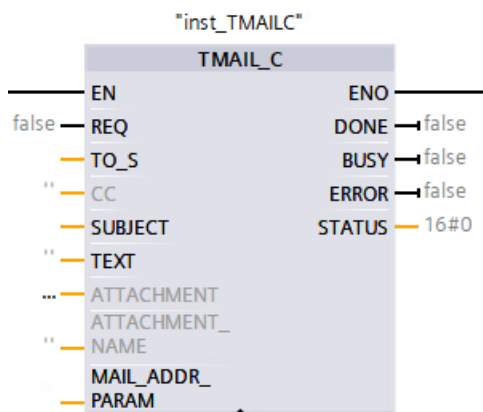
The Table below shows you which version of "TMAIL\_C" to use with which module:

Table 3-2

Module	Version of "TMAIL_C"
CP	V4.0 or higher
S7-1500 with FW 2.5 or higher	V5.0 or higher
S7-1200 with FW 4.4 or higher	V6.0 or higher

**Call**

The following Figure illustrates the call of the instruction "TMAIL\_C" in V6.1:



**Parameter**

The parameters have the following meanings:

Table 3-3

Parameter	Data type	Declaration	Meaning
REQ	BOOL	Input	Control parameter; dispatches email when rising edge detected
TO_S	STRING	Input	Receiver addresses; STRING with a maximum length of 240 characters (byte).
CC	STRING	Input	CC'd recipient addresses (optional); STRING with a maximum length of 240 characters (byte). Same email address format as with the "TO_S" parameter.
SUBJECT	STRING	Input	Email subject; STRING with a maximum length of 240 characters (byte).
TEXT	STRING	Input	email text (optional); STRING with a maximum length of 240 characters (byte). If an empty string is assigned to this parameter, the email will be sent without any text.
ATTACHMENT	VARIANT	Input	Email attachment (optional); Reference to a Byte/Word/Double field (ArrayOfByte, ArrayOfWord or ArrayOfDWord) with a maximum length of 64 KB. If no value is assigned, the email will be sent without an attachment.
ATTACHMENT_NAME	STRING	Input	Name of the email attachment (optional); reference to a string with a maximum length of 50 characters (byte) for defining the file name of the attachment. If an empty string is assigned to this parameter, the email attachment will be received with a name assigned by the email receiving program. Therefore, it is recommended to use a defined file name.
MAIL_ADDR_PARAM	VARIANT	Input	Parameters of the connection and address of the email server. Use the provided system data types (see <a href="#">chapter 3.3</a> ).
DONE	BOOL	OUTPUT	State parameter
BUSY	BOOL	OUTPUT	State parameter
ERROR	BOOL	OUTPUT	State parameter
STATUS	WORD	OUTPUT	State parameter

### Rules for the "TO\_S" parameter

The parameters "TO\_S" and "CC" are strings that can contain, for the example, the following:

- admin@mydomain.com, <ruby@mydomain.com>

Observe the following rules when entering the parameters:

- In OUC versions < V6.0 (S7-1500) or < V7.0 (S7-1200), it is recommended to enter a space and a "<" before each address. "<" is optional in all other instruction versions.
- In OUC versions < V6.0 (S7-1500) or < V7.0 (S7-1200), it is recommended to enter a ">" after each address. ">" is optional in all other instruction versions.
- A comma must be entered the addresses in "TO\_S" and "CC".

For reasons involving the runtime and memory, the "TMAIL\_C" instruction does not check the syntax at the "TO\_S" and "CC" parameters.

## 3.3 System data types of "TMAIL\_C"

### Description

In the structure "TMail\_V4\_SEC", "TMail\_V6\_SEC" or "TMail\_QDN\_SEC" at the "MAIL\_ADDR\_PARAM" parameter, you will define which connection will be used to send the email; here you also store the address of the email server and the login credentials.

Depending on which format you wish to address the email server in, you will use the following structure at the "MAIL\_ADDR\_PARAM" parameter:

- TMail\_V4\_SEC: Addressing via the IP address according to IPv4
- TMail\_V6\_SEC: Addressing via the IP address according to IPv6
- TMail\_QDN\_SEC: Addressing via the fully qualified domain name (FQDN)

#### Note

We only describe the system data types that support a secure connection.



**Parameter assignment for system data type "TMAIL\_v4\_SEC"**

Using the system data type "TMail\_V4\_SEC", the email server will be addressed via the IP address in IPv4.

Table 3-4

Parameter	Data type	Description
Interfaceld	LADDR	Hardware identifier of the Ethernet port of the CPU or CP (see <a href="#">chapter 2.6</a> )
ID	CONN_OUC	Connection ID
Connectiontype	BYTE	Connection type For IPv4, select 16#20 as connection type.
ActiveEstablishment	BOOL	Active / passive connection setup. Because the CPU or CP is always the SMTP client, this parameter must be set to "True".
WatchDogTime	TIME	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process. <b>Note</b> With "TMAIL_C" V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerAddress	IP_V4	IP address of the email server (in IPv4 format) from which you wish to send an email.
UserName	STRING[254]	The username and password are how the user identifies him/herself as the owner of the email account to the email provider (authentication method: AUTH-LOGIN).
PassWord	STRING[254]	
From	EMAIL_ADDR	Sender address of the email which is defined with the following two STRING parameters.
LocalPartPlusAtSign	STRING[64]	Local part of the sender address including @ sign.
FullQualifiedDomainName	STRING[254]	FQDN (fully qualified domain name) of the email server
RemotePort	UINT	TCP port of the mail server Value range: <ul style="list-style-type: none"> <li>• 25 (unsecured)</li> <li>• 465 (secured)</li> <li>• 587 (secured)</li> </ul> (see <a href="#">chapter 3.1</a> )
ActivateSecureConn	BOOL	True = Secure SMTP connection False = unsecured SMTP connection. In this case the subsequent parameters are irrelevant.
ExtTLSCapabilities	BYTE	Value range: 16#0, 16#1 For 16#1, the alternative applicant is verified in the server's certificate. The IP address or DNS name entered there must match the IP address or the DNS name of the server.
TLSServerCertRef	UDINT	Certificate number of the provider assigned in the TIA Portal certificate manager (see <a href="#">chapter 2.8</a> ).

**Parameter assignment for system data type "TMAIL\_v6\_SEC"**

The system data type "TMail\_V6\_SEC" is used to address the email server with an IP address in IPv6.

Table 3-5

Parameter	Data type	Description
Interfaceld	LADDR	Hardware identifier of the Ethernet port of the CPU or CP (see <a href="#">chapter 2.6</a> )
ID	CONN_OUC	Connection ID
Connectiontype	BYTE	Connection type For IPv6, select 16#21 as connection type.
ActiveEstablishment	BOOL	Establish connection actively/passively. Because the CPU or CP is always the SMTP client, this parameter must be set to "True".
WatchDogTime	TIME	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process. <b>Note</b> With "TMAIL_C" V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerAddress	IP_V6	IP address of the email server (in IPv6 format) from which you wish to send an email.
UserName	STRING[254]	The username and password are how the user identifies him/herself as the owner of the email account to the email provider (authentication method: AUTH-LOGIN).
PassWord	STRING[254]	
From	EMAIL_ADDR	Sender address of the email which is defined with the following two STRING parameters.
LocalPartPlusAtSign	STRING[64]	Local part of the sender address including @ sign.
FullQualifiedDomainName	STRING[254]	FQDN (fully qualified domain name) of the email server
RemotePort	UINT	TCP port of the mail server Value range: <ul style="list-style-type: none"> <li>• 25 (unsecured)</li> <li>• 465 (secured)</li> <li>• 587 (secured)</li> </ul> (see <a href="#">chapter 3.1</a> )
ActivateSecureConn	BOOL	True = Secure SMTP connection False = unsecured SMTP connection. In this case the subsequent parameters are irrelevant.
ExtTLSCapabilities	BYTE	Value range: 16#0, 16#1 For 16#1, the alternative applicant is verified in the server's certificate. The IP address or DNS name entered there must match the IP address or the DNS name of the server.
TLSServerCertRef	UDINT	Certificate number of the provider assigned in the TIA Portal certificate manager (see <a href="#">chapter 2.8</a> ).

**System data type "TMAIL\_QDN\_SEC"**

The email server is addressed via its fully-qualified domain name (FQDN) with the system data type "TMail\_QDN\_SEC".

Table 3-6

Parameter	Data type	Description
Interfaceld	LADDR	Hardware identifier of the Ethernet port of the CPU or CP (see <a href="#">chapter 2.6</a> )
ID	CONN_OUC	Connection ID
Connectiontype	BYTE	Connection type For FQDN, select 16#22 as connection type.
ActiveEstablishment	BOOL	Actively or passively establish connection. Because the CPU or CP is always the SMTP client, this parameter must be set to "True".
WatchDogTime	TIME	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process. <b>Note</b> With "TMAIL_C" V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerQDN	STRING[254]	FQDN (full qualified domain name) of the email server from which you wish to send an email to a recipient. Note the period at the end when assigning the parameter.
UserName	STRING[254]	The username and password are how the user identifies him/herself as the owner of the email account to the email provider (authentication method: AUTH-LOGIN).
PassWord	STRING[254]	
From	EMAIL_ADDR	Sender address of the email which is defined with the following two STRING parameters.
LocalPartPlusAtSign	STRING[64]	Local part of the sender address including @ sign.
FullQualifiedDomain Name	STRING[254]	FQDN (fully qualified domain name) of the email server
RemotePort	UINT	TCP port of the mail server Value range: <ul style="list-style-type: none"> <li>• 25 (unsecured)</li> <li>• 465 (secured)</li> <li>• 587 (secured)</li> </ul> (see <a href="#">chapter 3.1</a> )
ActivateSecureConn	BOOL	True = Secure SMTP connection False = unsecured SMTP connection. In this case the subsequent parameters are irrelevant.
ExtTLSCapabilities	BYTE	Value range: 16#0, 16#1 For 16#1, the alternative applicant is verified in the server's certificate. The IP address or DNS name entered there must match the IP address or the DNS name of the server.
TLSServerCertRef	UDINT	Certificate number of the provider assigned in the TIA Portal certificate manager (see <a href="#">chapter 2.8</a> ).

## 4 Appendix

### 4.1 Service and support

#### Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

[support.industry.siemens.com](https://support.industry.siemens.com)

#### Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers

– ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

[siemens.com/SupportRequest](https://siemens.com/SupportRequest)

#### SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

[siemens.com/sitrain](https://siemens.com/sitrain)

#### Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

[support.industry.siemens.com/cs/sc](https://support.industry.siemens.com/cs/sc)

#### Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

[support.industry.siemens.com/cs/ww/en/sc/2067](https://support.industry.siemens.com/cs/ww/en/sc/2067)

## 4.2 Industry Mall



The Siemens Industry Mall is the platform on which the entire Siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:

[mall.industry.siemens.com](https://mall.industry.siemens.com)

## 4.3 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support <a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
\2\	Link to this entry page of this application example <a href="https://support.industry.siemens.com/cs/ww/en/view/46817803">https://support.industry.siemens.com/cs/ww/en/view/46817803</a>
\3\	TIA Portal V17 manual <a href="https://support.industry.siemens.com/cs/de/en/view/109798671">https://support.industry.siemens.com/cs/de/en/view/109798671</a>

## 4.4 Change documentation

Table 4-2

Version	Date	Modifications
V1.0	06/2017	First version
V2.0	04/2020	Added section for sending a secure email via the integrated Ethernet port of the CPU
V2.1	12/2020	Updated screenshot in chapter 2.2.6
V3.0	07/2022	Update for new Google policies and TIA V17