

The background image shows a man in a light blue shirt from the side, looking at a tablet. He is in a factory or industrial setting with various machines and equipment visible in the background. Overlaid on the image are several digital graphics: a large '24/7' with a circular arrow, a 'NEWS' section with a person icon, a 'Home' button, and a network diagram with three people icons connected by lines. There are also binary code (0s and 1s) and a clock visible in the background.

SIEMENS

Ingenuity for life

Sending emails over secure email connections with S7-1500 and S7-1200

STEP 7 V16, 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

Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Principle of operation.....	5
1.3 Components used	6
2 Engineering	7
2.1 Hardware setup	7
2.2 Configuration and parameter assignment	8
2.2.1 Find provider certificate and download	8
2.2.2 Allow email account access from the CP	11
2.2.3 Enable global security functions.....	16
2.2.4 Create security user and log in for the global security settings.....	17
2.2.5 Import provider certificate in the STEP 7 (TIA Portal) global certificate manager.....	19
2.2.6 Assign provider certificate in the local certificate manager of the module.....	20
2.2.7 Connect the module to the internet	25
2.2.8 Configure the DNS Server.....	27
2.2.9 Enter parameters for system data types of the "TMAIL_C" instruction in STEP 7 (TIA Portal)	29
2.2.10 Parameter assignment for "TMAIL_C" instruction	33
2.2.11 Setting the module clock time	35
2.2.12 Determine hardware identifier of the module	40
3 Useful information	41
3.1 SMTP servers and ports of the providers.....	41
3.2 Overview of the system data types of "TMAIL_C"	41
3.3 Alternative solutions	43
3.3.1 Integrating certificates into STEP 7 V13	43
3.3.2 Configure CP 1543-1 in STEP 7 V13.....	45
3.3.3 Set up a secure connection to an email server in STEP 7 V13	46
4 Appendix	50
4.1 Service and support	50
4.2 Links and literature	51
4.3 Change documentation	51

1 Introduction

1.1 Overview

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

Using the "TMAIL_C" instruction, you can send an email via the Ethernet port of an S7-1500 CPU of V2.0 and higher or S7-1200 CPU of V4.1 and higher, a communications module (CM) or communications processor (CP).

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

The following CPs send secure emails via the instruction "TMAIL_C" version 4.0 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

Using the "TMAIL_C" instruction version 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 status V2.5 to do this.

Using the "TMAIL_C" instruction version 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 status V4.4 to do this.

In chapter [3.2](#) you will find an overview of the system data types which are used to set the data needed for the sending process.

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

1.2 Principle of operation

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

Figure 1-1

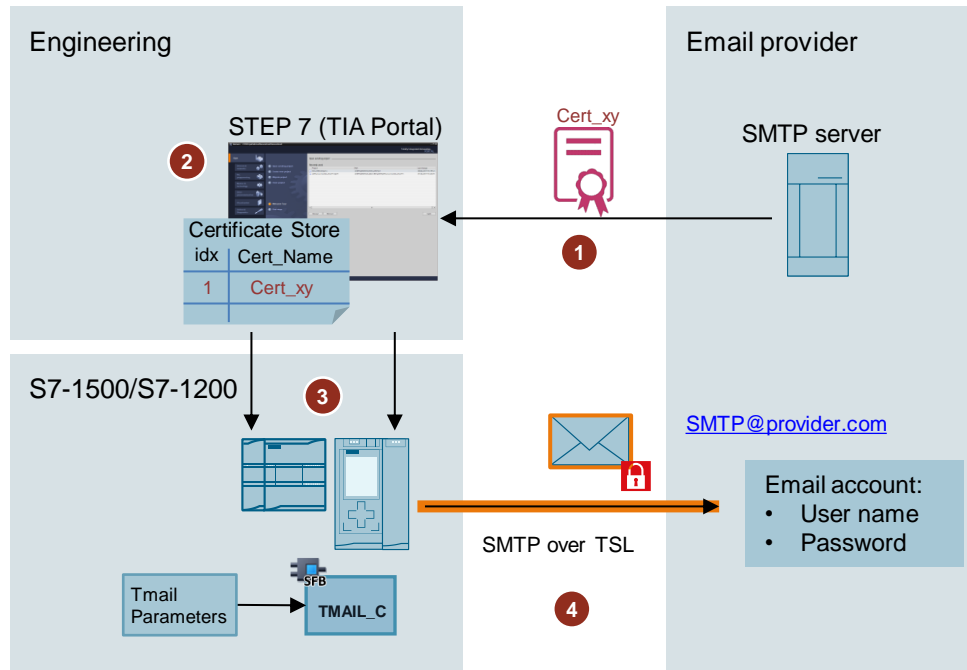


Table 1-2

Step	Description
1	Find the certificate of the email provider. In the email account, allow the CPU or communications processor (CP) to access the email account via SMTP or SMTPS.
2	Import the certificate of the email provider in STEP 7 (TIA Portal)
3	Perform the following configuration steps in the S7-1500 or S7-1200 station: <ul style="list-style-type: none"> Add the certificate which you imported to STEP 7 (TIA Portal) to the CPU or CP. Establish connection between the CPU and the internet, or between the CP and the internet. Configure the DNS Server Call the instruction "TMAIL_C" in the user program of the S7 CPU and enter parameters for it. Set the time of the S7 CPU.
4	Send the email via the secure connection (SNMP over TLS)

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_en.pdf	-

2 Engineering

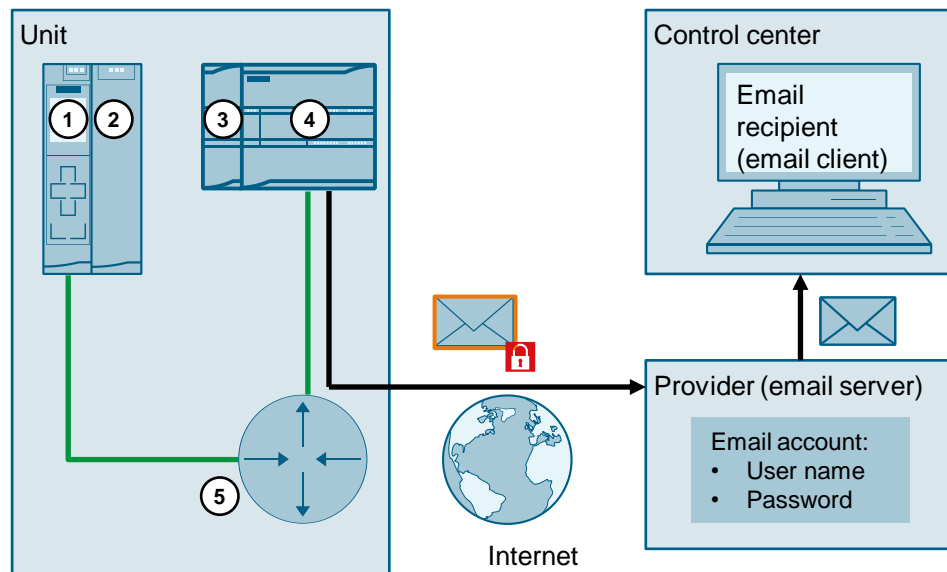
The sample project is protected. Log on with following credentials:

- User name: admin
- Password: Siemens.1

2.1 Hardware setup

The following figure shows the hardware setup.

Figure 2-1



The following table shows the IP addresses of the system's hardware components.

Table 2-1

No.	Components	IP address	Subnet mask
1	CPU 1513-1 PN	192.168.178.35	255.255.255.0
2	CP 1543-1	192.168.178.36	255.255.255.0
3	CPU 1214C	192.168.178.45	255.255.255.0
4	CP 1243-1	172.168.178.46	255.255.255.0
5	DSL router	192.168.178.1	255.255.255.0

2.2 Configuration and parameter assignment

2.2.1 Find provider certificate and download

Overview

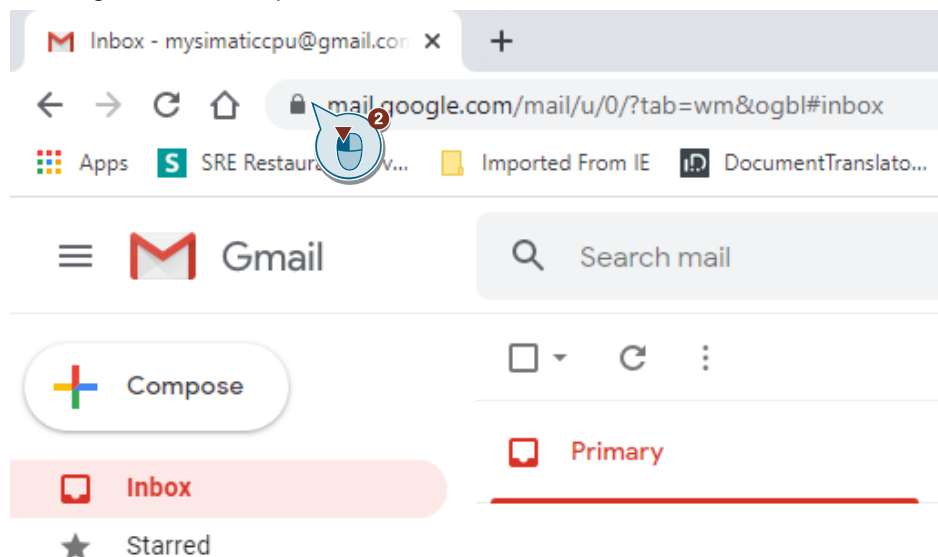
A certificate is a public key signed by its owner (in this case, the email provider) that guarantees its authenticity and integrity.

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

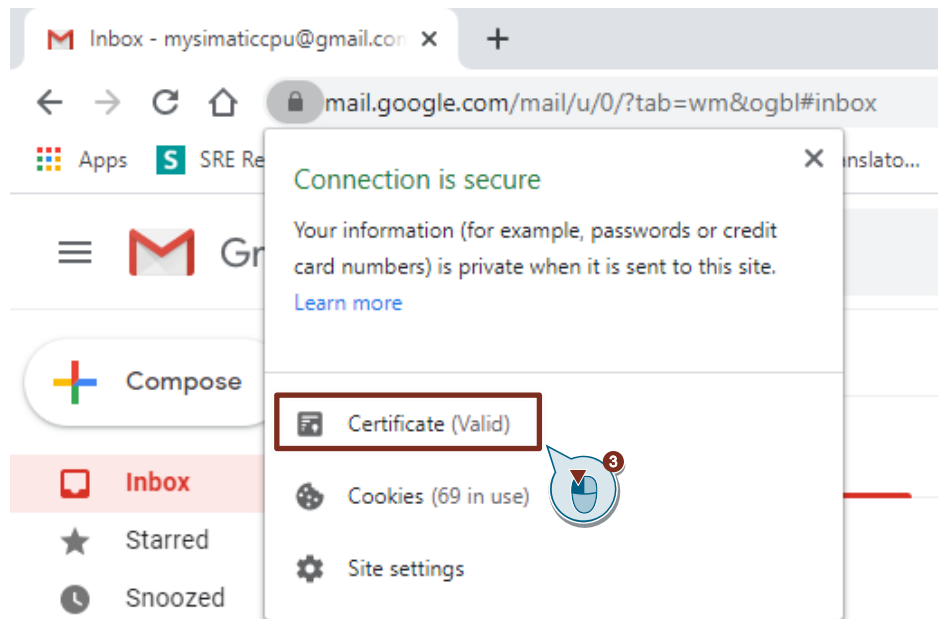
Find provider certificate

The application example shows an example of 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.

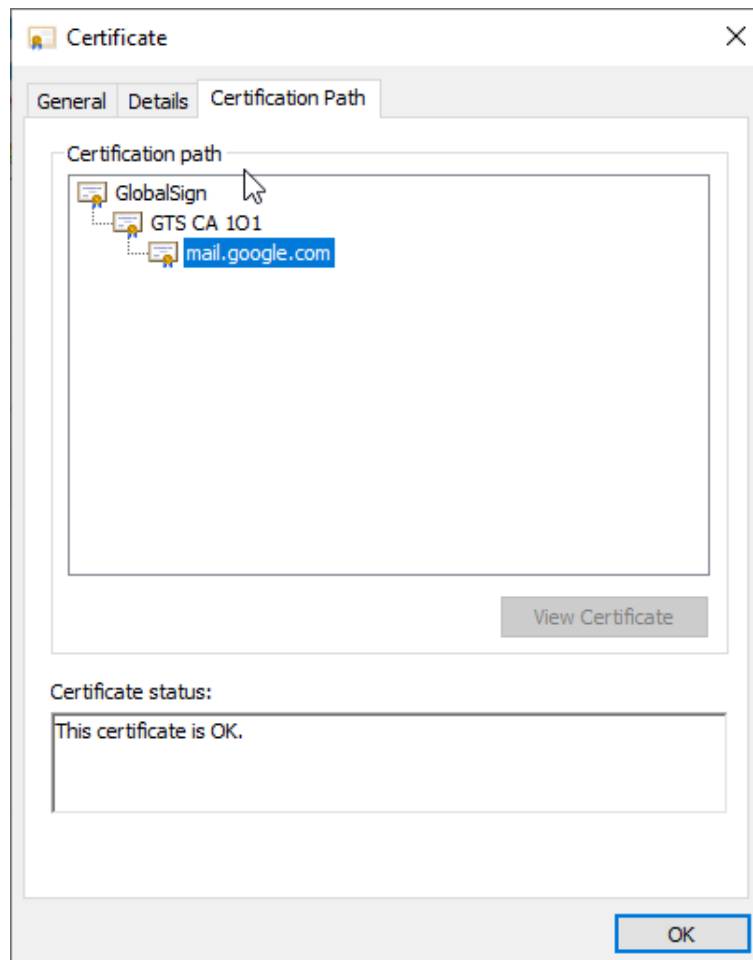
1. Log in to your Gmail account to find the certificate of your provider.
2. In Google Chrome's input bar, click the "View site information" icon.



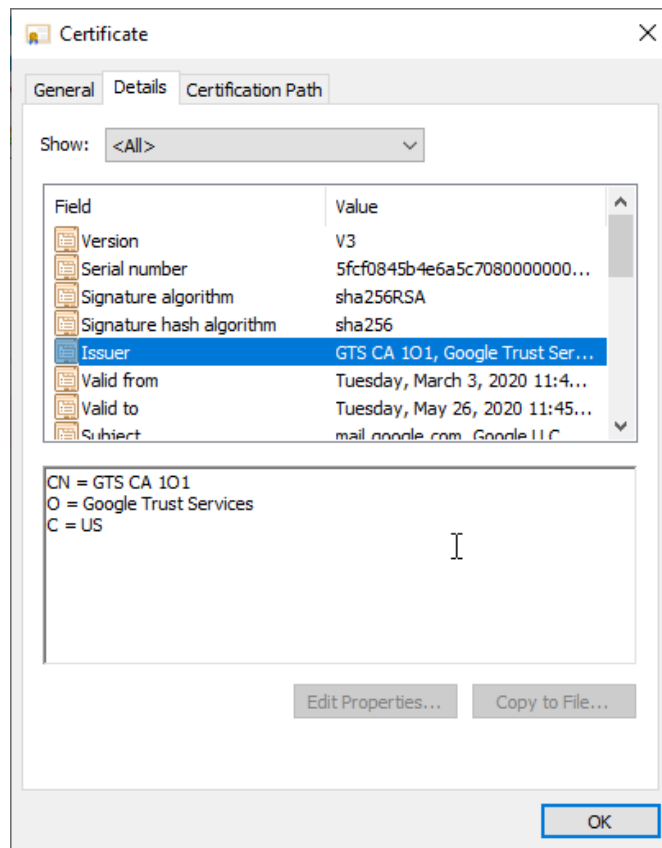
3. Click "Certificate". The "Certificate" dialog opens.



4. Open the "Certification Path" tab. The name of the certificate used by your provider will be shown here. Gmail uses the "GlobalSign" certificate.



5. Open the "Details" tab. The issuer of the certificate can be found here. The issuer of the "GlobalSign" certificate is "Google Trust Services".



Download provider certificates

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

As an example, we have provided the links to the certificates of Telekom and Google in [Table 2-2](#).

Table 2-2

Name of certificate	Used by	Link
T-TeleSec GlobalRoot Class 3 Issuer: T-Systems International GmbH	Web.de GMX	T-Telesec GlobalRoot Class 3
Global Sign: GS Root R2 Issuer: Google Trust Services	Gmail	Google Trust Services
T-TeleSec GlobalRoot Class 2 Issuer: T-Systems Enterprise Services GmbH	T-Online	T-Telesec GlobalRoot Class 2

2.2.2 Allow email account access from the CP

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:

- GMX
- Web.de
- T-Online
- Gmail

First log in to your email account.

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".

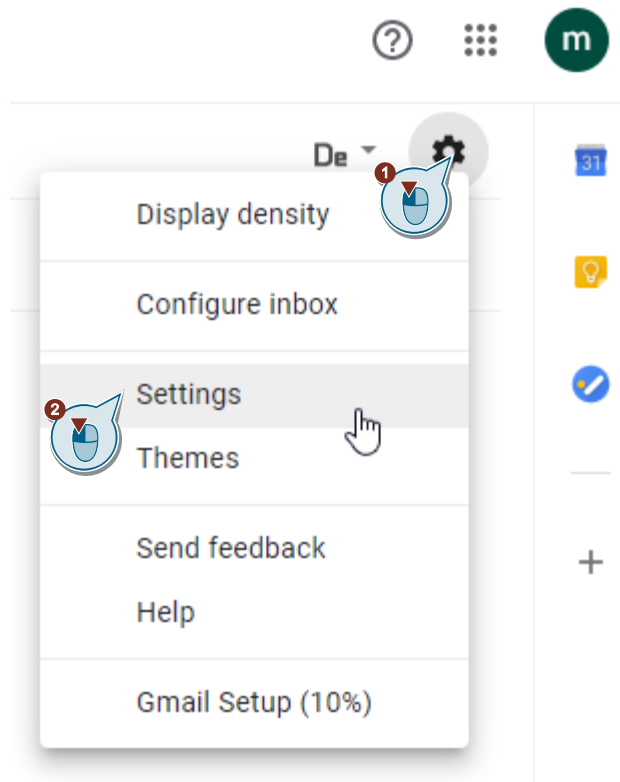
T-Online

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

Gmail

1. Click the "Settings" icon.
2. Select the "Settings" context menu.



3. Open the "Forwarding and POP/IMAP" tab.
4. Under "POP download" enable the function "Enable POP for all mail".
5. Under "IMAP access" enable the function "Enable IMAP".

6. Click "Save Changes".

Settings

General
Labels
Inbox
Accounts and Import
Filters and Blocked Addresses
Forwarding and POP/IMAP
Add-ons
Chat

Forwarding:
[Learn more](#)

Add a forwarding address

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

POP download:
[Learn more](#)

1. Status: **POP is enabled** for all mail
☐ 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 keep Gmail's copy in the Inbox

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 Trash
☐ Immediately delete the message forever

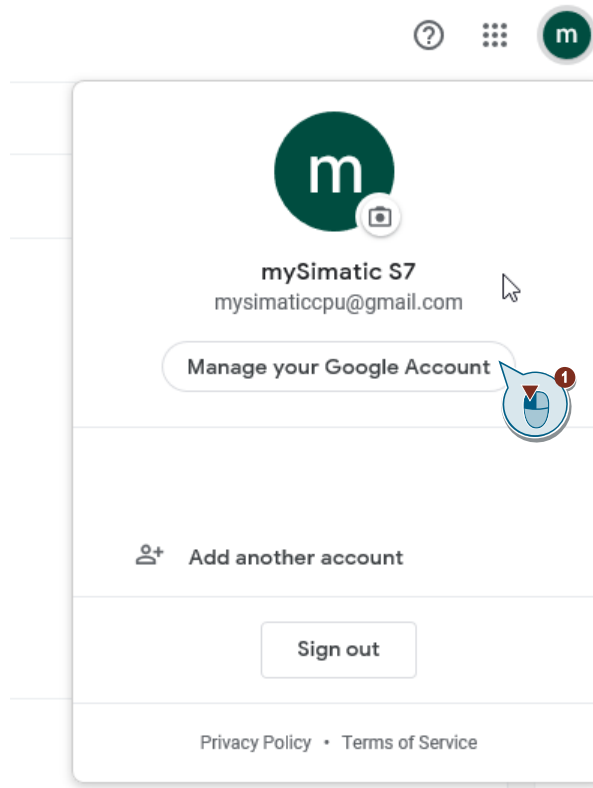
Folder size limits
☒ Do not limit the number of messages in an IMAP folder (default)
☐ Limit IMAP folders to contain no more than this many messages 1,000

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

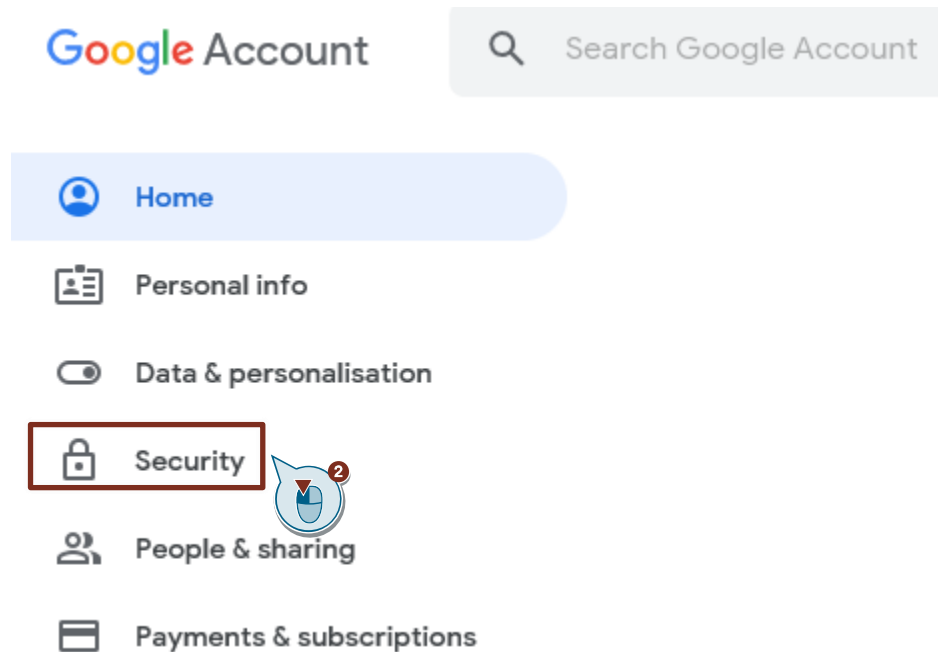
Save Changes Cancel

In order for the S7 CPU to be able to authenticate itself with Gmail using the user name and password, it is necessary to allow access through less secure apps in the Gmail account.

1. Click "Manage your Google Account".




2. Select "Security" in your Google account.




3. Enable access through less secure apps.

Less secure app access

Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account. To keep your account secure, Google will automatically turn this setting OFF if it's not being used. [Find out more](#)

 On

[Turn off access \(recommended\)](#)



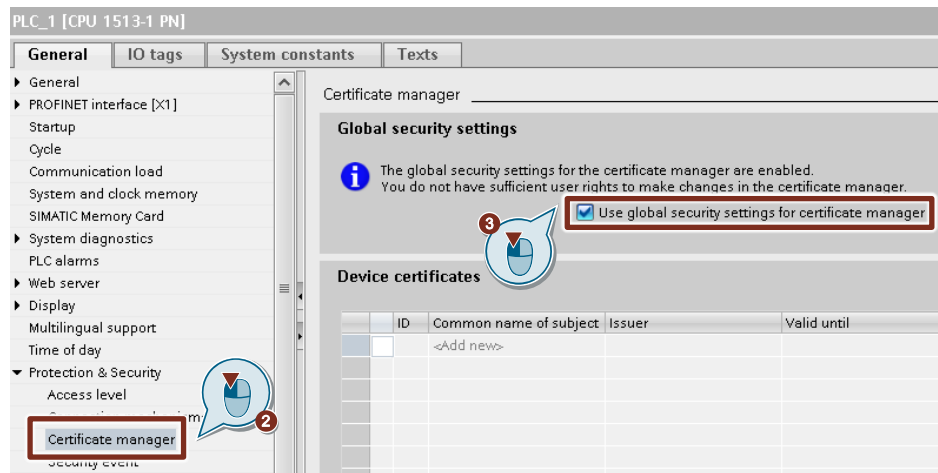
2.2.3 Enable global security functions

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.

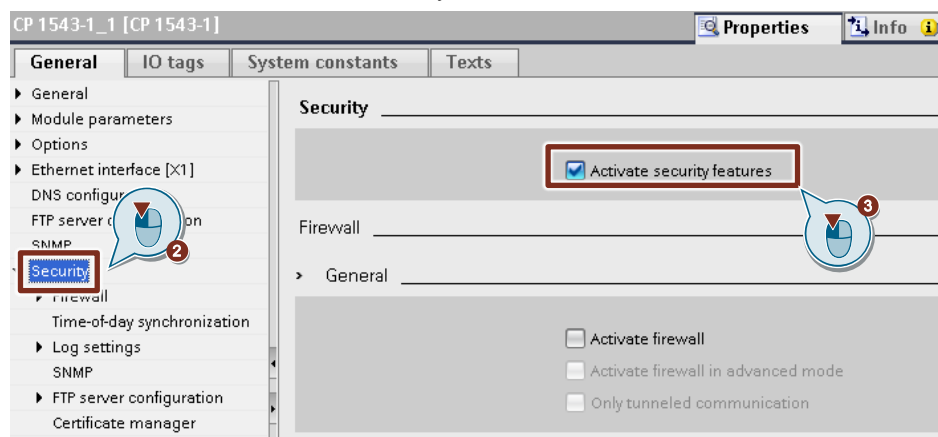
Enable global security settings in the CPU

1. Select the CPU in the device or network view. The properties of the CPU are displayed in the inspection window.
2. In the "General" tab select "Protection & Security > Certificate manager".
3. Enable the function "Use global security settings for certificate manager".



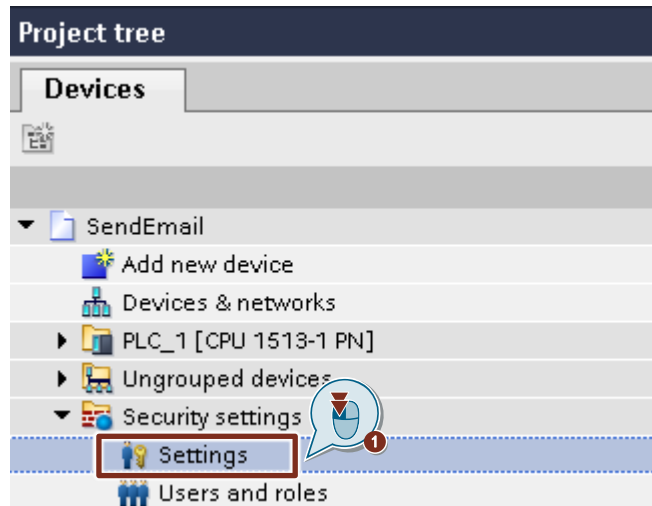
Enable global security settings in the CP

1. Select the CP in the device or network view. The properties of the CP are displayed in the Inspector window.
2. In the "General" tab select "Security".
3. Enable the function "Activate security features".

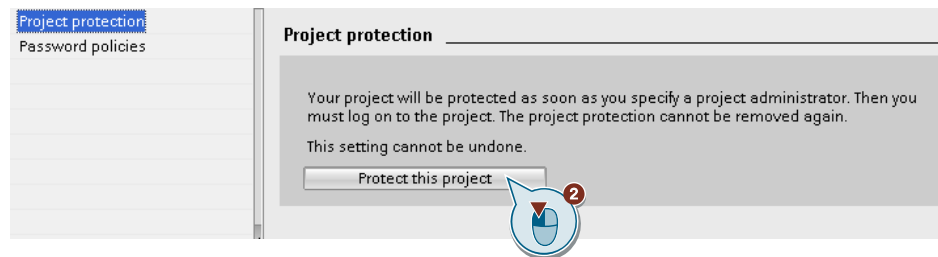


2.2.4 Create security user and log in for the global security settings

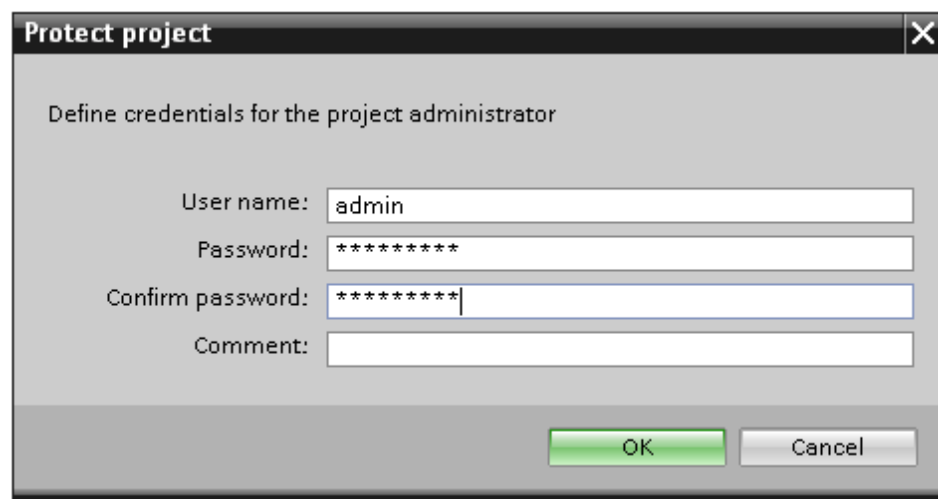
1. In the project navigation, double click in the folder "Security settings" on the item "Settings".
The user administration editor opens and the project protection area is displayed.



2. Click the "Protect this project" button.



This opens the dialog "Protect project".

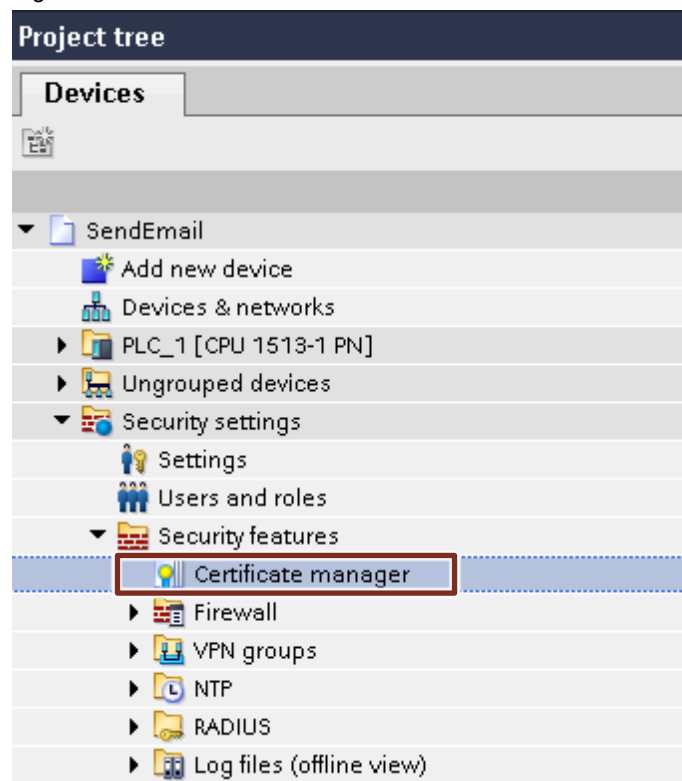


3. Enter a username and password.
The password must comply with the following guidelines:
 - At least one uppercase letter
 - At least one special character (special characters § and ß are not allowed)
 - At least one number
4. Enter the password again to confirm.
5. You may enter a comment if required.
6. Confirm your entries with "OK".

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 the entry "Security settings > Security features".

Figure 2-2



2.2.5 Import provider certificate in the STEP 7 (TIA Portal) 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"

Follow the instructions below to import the provider certificates into STEP 7 (TIA Portal).

1. Double-click on the "Certificate manager" entry in the project navigation under "Security settings > Security features".
2. Select the appropriate tab for the certificate you want to import, for example, "Trusted certificates and root certification authorities".
3. Right click in the tab to open the context menu.
4. Click "Import".



5. Select the import format of the certificate.
 - CER, DER, CRT or PEM for certificates without a private key
 - P12 (PKCS12 archive) for certificates with a private key.
6. Click on "Open" to import the certificate.

Result

The provider certificate is located in the global certificate manager.

Figure 2-3

ID	Common name of subject	Issuer	Valid to	Used as	Private key	Method
41	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	Sunday, October 2, 2033	Certification authority	No	None
42	T-TeleSec GlobalRoot Class 3	T-TeleSec GlobalRoot Class 3	Sunday, October 2, 2033	Certification authority	No	None
43	GlobalSign	GlobalSign	Wednesday, December 15, 2021	Certification authority	No	None

2.2.6 Assign provider certificate in the local certificate manager of the module

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

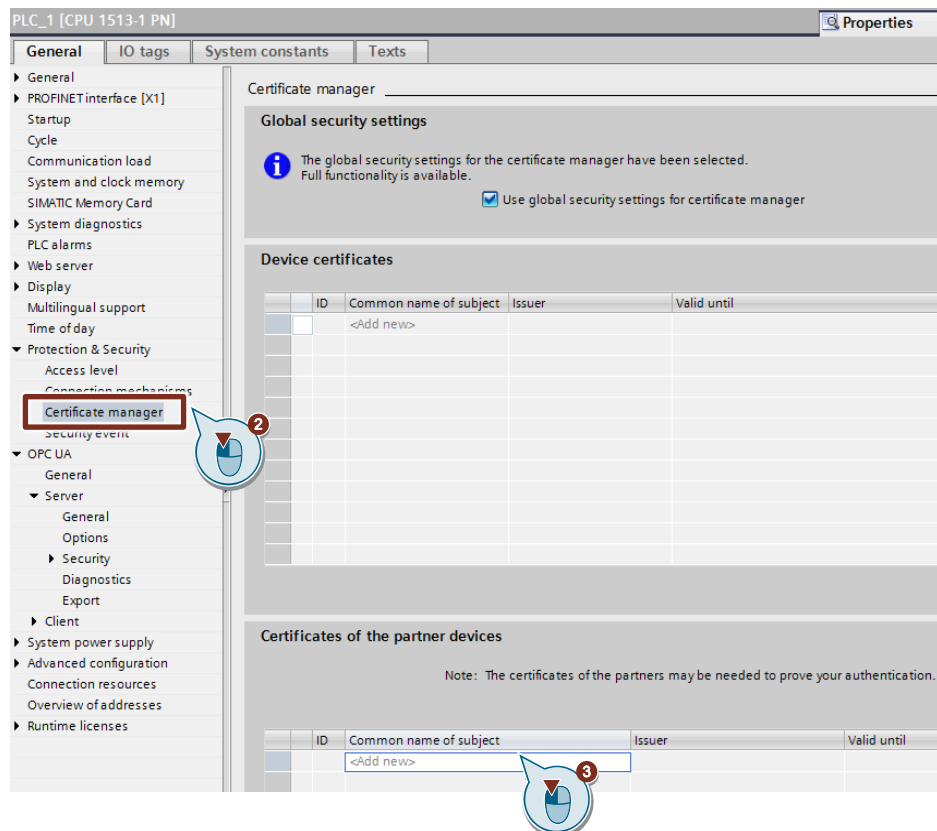
In order to authenticate the provider, it is necessary to load its CA certificate into the S7 CPU or the CP. Only those device certificates that you have assigned to the module as device certificates via the local certificate manager are loaded onto the module.

This assignment is performed in the local security settings for the assembly in the "Certificate manager" item using the table editor "Certificates of the partner devices". When assigning certificates, the certificates from the global certificate manager are available.

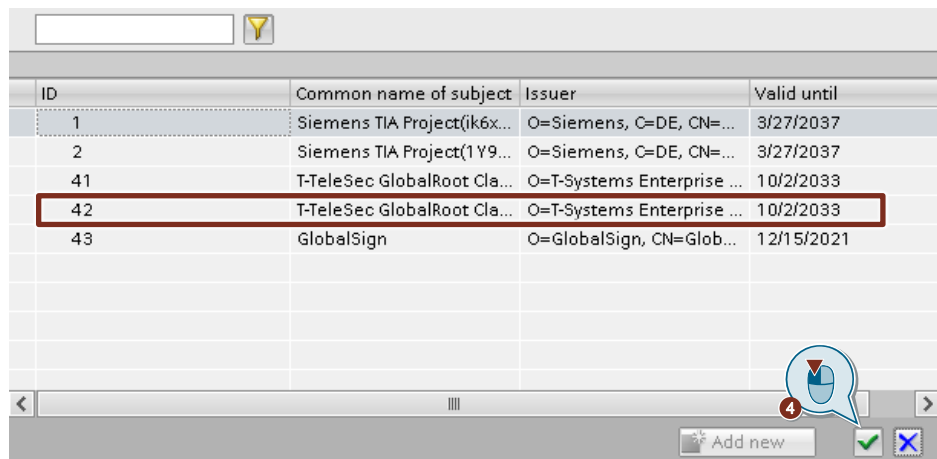
Assign provider certificate in the local certificate manager of the CPU

The following steps will show you how to assign the provider certificate to the S7 CPU in the local certificate manager.

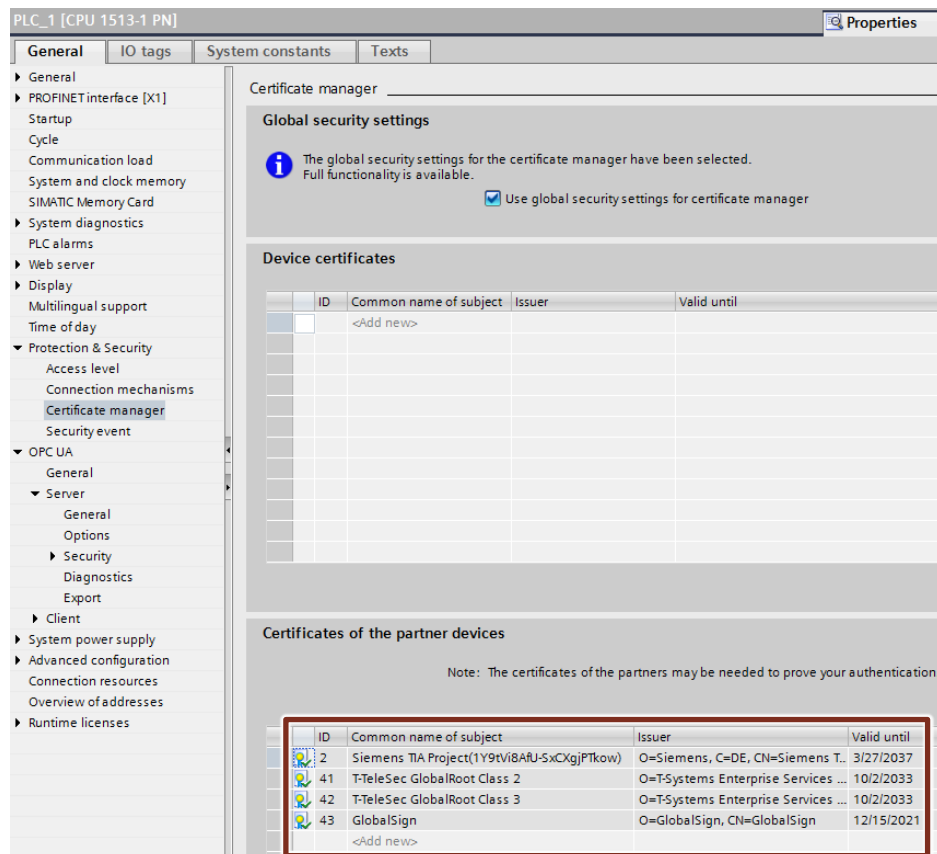
1. Select the CPU in the device or network view. The properties of the CPU are displayed in the inspection window.
2. In the area navigation of the "General" tab, select "Protection & Security > Certificate Manager".
3. Click an empty line in the column "Common name of subject" in the table "Certificates of the partner devices".
A dropdown menu will open for selecting a certificate.



4. Select the provider certificate that you need and confirm your selection.



5. The provider certificate is added to the table "Certificates of the partner devices".



6. Later, specify the ID of the provider certificate in the parameter data set "TMail_QDN_SEC".

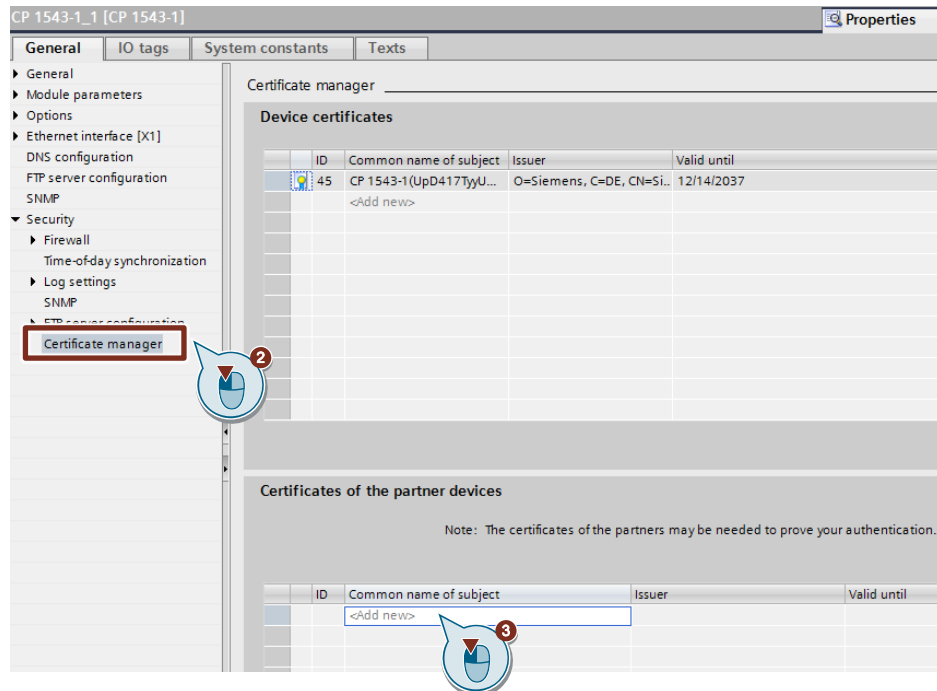
▼ connParamWebDe	TMail_QDN_SEC	
■ InterfaceId	HW_ANY	64
■ ID	CONN_OUC	16#1
■ ConnectionType	Byte	16#22
■ ActiveEstablished	Bool	true
■ WatchDogTime	Time	T#0ms
■ MailServerQDN	String[254]	'smtp.web.de.'
■ UserName	String[254]	'username@web.de'
■ PassWord	String[254]	'password'
■ ▼ From	EMAIL_ADDR	
■ LocalPartPlusAtSign	String[64]	'username@'
■ FullQualifiedDomainName	String[254]	'web.de'
■ RemotePort	UInt	587
■ ActivateSecureConn	Bool	true
■ ExtTLSCapabilities	Byte	16#0
■ TLSServerCertRef	UDInt	42



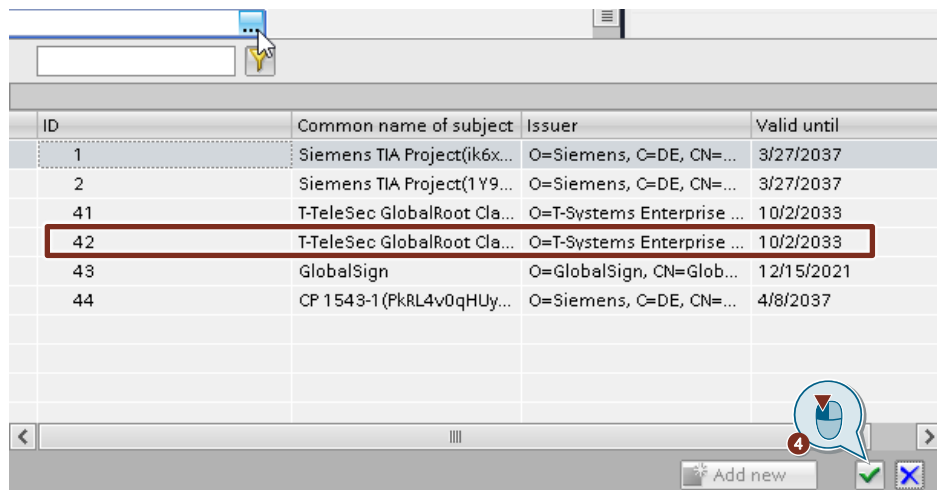
Assign provider certificate to the CP in the local certificate manager

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

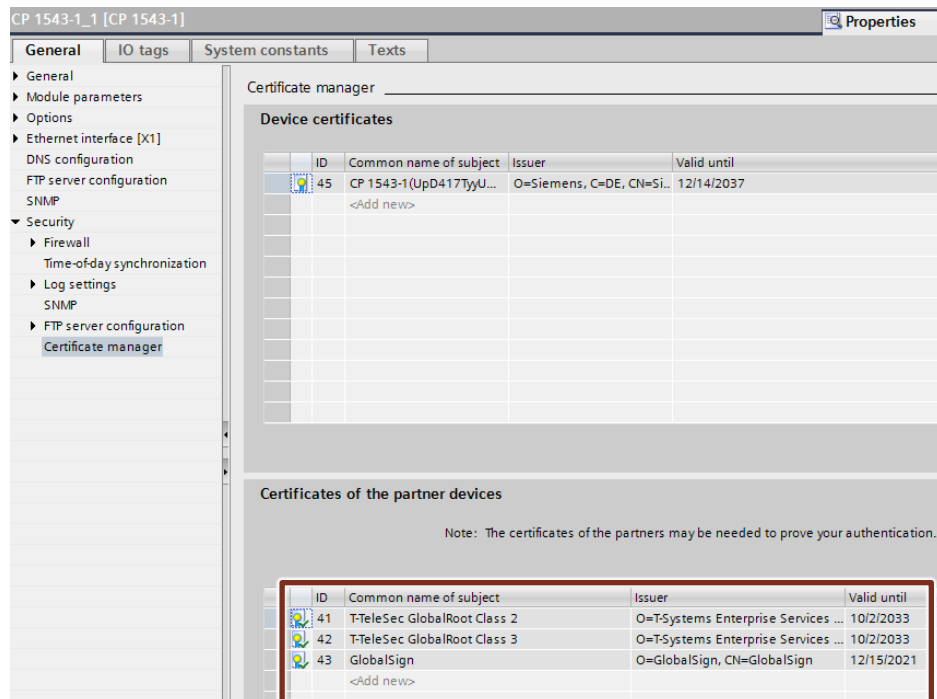
1. Select the CP in the device or network view. The properties of the CP are displayed in the Inspector window.
2. In the area navigation of the "General" tab, select "Security > Certificate Manager".
3. Click an empty line in the column "Common name of subject" in the table "Certificates of the partner devices".
A dropdown menu will open for selecting a certificate.



4. Select the provider certificate that you need and confirm your selection.



5. The provider certificate is added to the table "Certificates of the partner devices".



6. Later, specify the ID of the provider certificate in the parameter data set "TMail_QDN_SEC".

▼ connParamWebDe		TMail_QDN_SEC	
■	InterfaceId	HW_ANY	259
■	ID	CONN_OUC	16#1
■	ConnectionType	Byte	16#22
■	ActiveEstablished	Bool	true
■	WatchDogTime	Time	T#0ms
■	MailServerQDN	String[254]	'smtp.web.de.'
■	UserName	String[254]	'username@web.de'
■	PassWord	String[254]	'password'
■	▼ From	EMAIL_ADDR	
■	LocalPartPlusAtSign	String[64]	'username@'
■	FullQualifiedDomainName	String[254]	'web.de'
■	RemotePort	UInt	587
■	ActivateSecureConn	Bool	true
■	ExtTLSCapabilities	Byte	16#0
■	TLSServerCertRef	UDInt	42



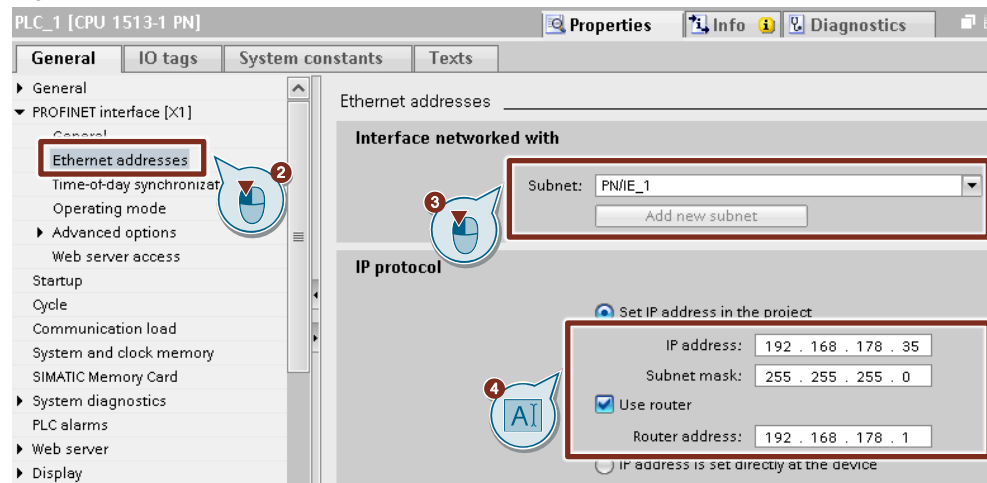
2.2.7 Connect the module to the internet

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

In the hardware configuration, set the IP address and subnet mask of the CPU or the CP, and the IP address of the router.

Set the CPU's IP address

Figure 2-4



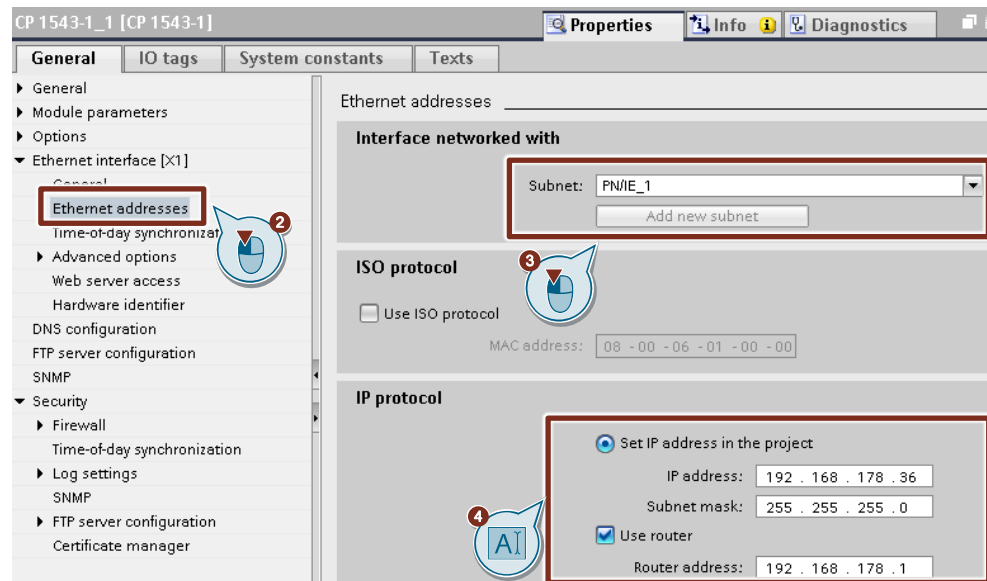
1. Select the CPU in the network or device view. The properties of the CPU are displayed in the inspection window.
2. In the area navigation of the "General" tab, select the item "Ethernet addresses" under "PROFINET interface [X1]".
3. Select the newly-created subnet, e.g. PN/IE_1 or click the "Add new subnet" to network the Ethernet port of the CPU.
4. Make the following settings:
 - IP address: 192.168.178.35
 - Subnet mask: 255.255.255.0
 - Internal IP address of the DSL router

Note

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

Set the IP address of the CP

Figure 2-5



1. Select the CP in the network or device view. The properties of the CP are displayed in the Inspector window.
2. In the area navigation of the "General" tab, select the item "Ethernet addresses" under "Ethernet interface [X1]".
3. Select the newly-created subnet, e.g. PN/IE_1 or click the "Add new subnet" to network the Ethernet port of the CP.
4. Make the following settings:
 - IP address: 192.168.178.36
 - Subnet mask: 255.255.255.0
 - Internal IP address of the DSL router: 192.168.178.1

Note

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

2.2.8 Configure the DNS Server

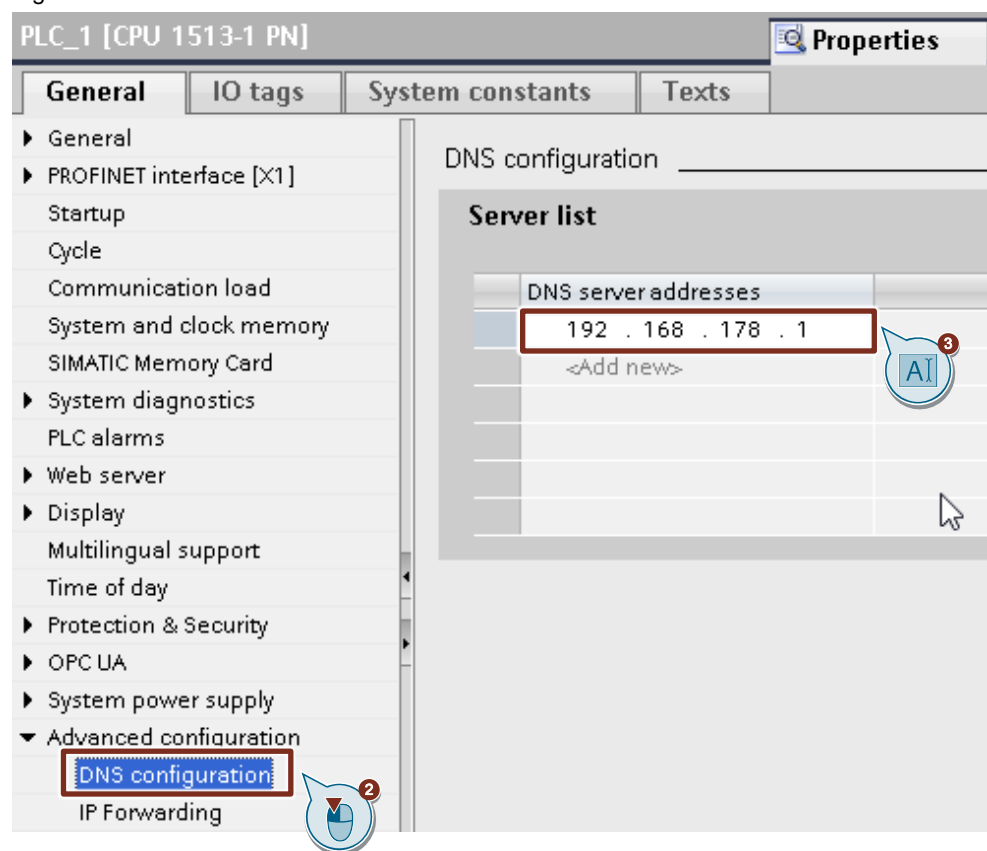
The instruction "TMAIL_C" for sending an email from the STEP 7 program addresses the SMTP server via the following data structures.

- "TMail_QDN_SEC"
- "TMail_FQDN"

These data structures address the SMTP server fully-qualified via the name of the SMTP server. For this reason it is necessary to configure the DSL router as DNS server in the CPU or in the CP.

Configure DNS server in the CPU

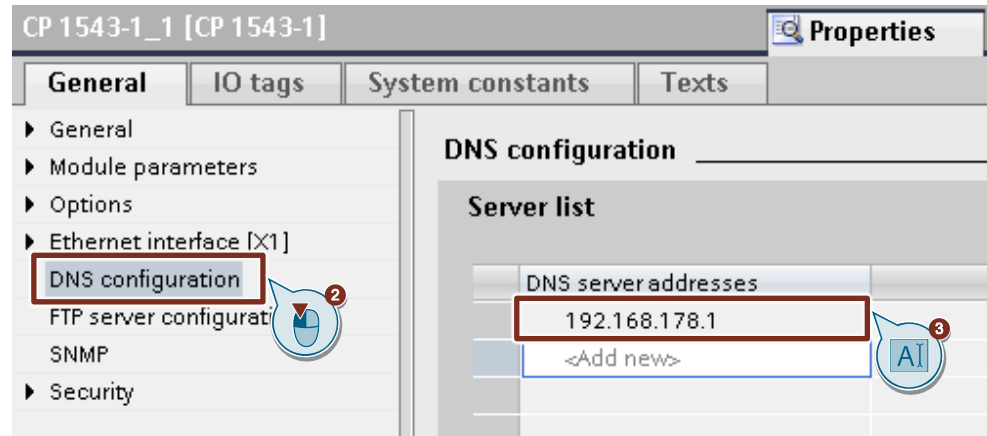
Figure 2-6



1. Select the CPU in the network or device view. The properties of the CPU are displayed in the inspection window.
2. In the area navigation of the "General" tab, select "Advanced configuration > DNS configuration".
3. Add the internal IP address of the DSL router as DNS server address in the server list.

Configure DNS server in the CP

Figure 2-7



1. Select the CP in the network or device view. The properties of the CP are displayed in the Inspector window.
2. In the area navigation of the "General" tab, select "DNS configuration".
3. Add the internal IP address of the DSL router as DNS server address in the server list.

2.2.9 Enter parameters for system data types of the "TMAIL_C" instruction in STEP 7 (TIA Portal)

Depending on the use case, the following system data types are available for parameterization of a secure email connection to the "TMAIL_C" instruction:

- "TMail_V4_SEC"
- "TMail_V6_SEC"
- "TMail_QDN_SEC"

In the following sections we will explain the parameters of the system data types "TMail_QDN_SEC" and "TMail_V4_SEC".

You can find an overview of all system data types in chapter [3.2](#).

Parameter assignment for 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 2-3

Parameter	Data type	Value	Description
Interfaceld	LADDR	64	Hardware identifier of the Ethernet port of the CPU or CP (see chapter 2.2.12)
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. Note With "TMAIL_C" version V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerQDN	STRING[254]	For ex.: 'smtp.web.de'	FQDN (Full Qualified Domain Name) of the email server from which you wish to send an email to a recipient.

Parameter		Data type	Value	Description
UserName		STRING[254]	For ex.: 'username@web.de'	The user name 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]	For ex.: 'password'	
From		EMAIL_ADDR	-	Sender address of the email which is defined with the following two STRING parameters.
	LocalPartPlusAtSign	STRING[64]	For ex.: 'username@'	Local part of the sender address including @ sign.
	FullQualifiedDomain Name	STRING[254]	For ex.: 'web.de'	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"> • 25 (unsecured) • 465 (secured) • 587 (secured)
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#42	Certificate number of the provider which was entered in the STEP 7 (TIA Portal) certificate manager (see chapter 2.2.6).

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 2-4

Parameter	Data type	Value	Description
Interfaceld	LADDR	261	Hardware identifier of the Ethernet port of the or CP (see chapter 2.2.12)
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#0 ms	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process. Note With "TMAIL_C" version V6 or higher, the value Zero is allowable for the parameter "WatchDogTime".
MailServerAddress	IP_V4	For ex.: 213.165.67.108	IP address of the email server (in IPv4 format) from which you wish to send an email.
UserName	STRING[254]	For ex.: 'username@web.de'	The user name 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]	For ex.: 'password'	

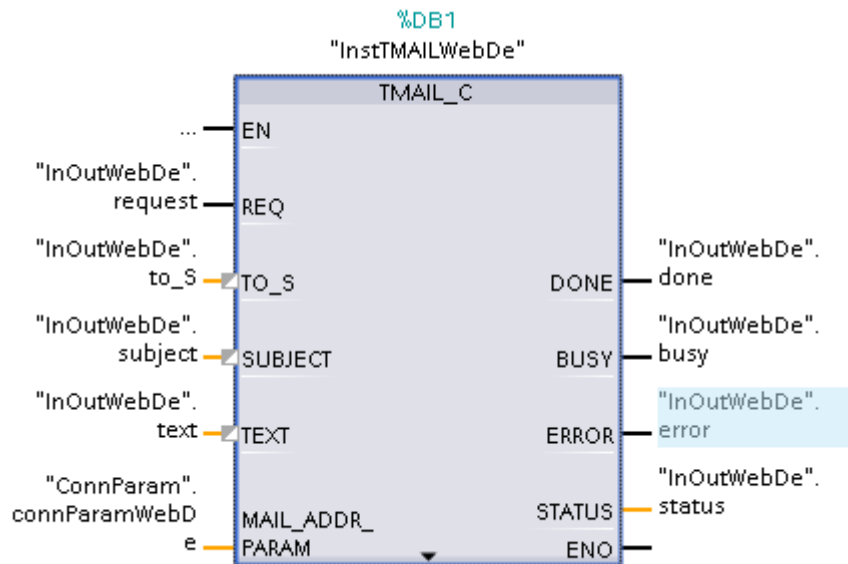
Parameter	Data type	Value	Description
From	EMAIL_ADDR	-	Sender address of the email which is defined with the following two STRING parameters.
LocalPartPlusAtSign	STRING[64]	For ex.: 'username@'	Local part of the sender address including @ sign.
FullQualifiedDomain Name	STRING[254]	For ex.: 'web.de'	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"> • 25 (unsecured) • 465 (secured) • 587 (secured)
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#42	Certificate number of the provider which was entered in the STEP 7 (TIA Portal) certificate manager (see chapter 2.2.6).

2.2.10 Parameter assignment for "TMAIL_C" instruction

Cyclically call the instruction "TMAIL_C" in the user program of the S7-1500 CPU or S7-1200 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.

Figure 2-8



Input parameter

The following table shows the input parameters of the "TMAIL_C" instruction.

Table 2-5

Input parameter	Data type	Description
REQ	Bool	Control parameters 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 (see chapter 2.2.9)

Output parameters

The following table shows the output parameters of the "TMAIL_C" instruction.

Table 2-6

Output parameters	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 Return value or error information from the TMAIL_C instruction

2.2.11 Setting the module clock time

Setting the CPU clock time

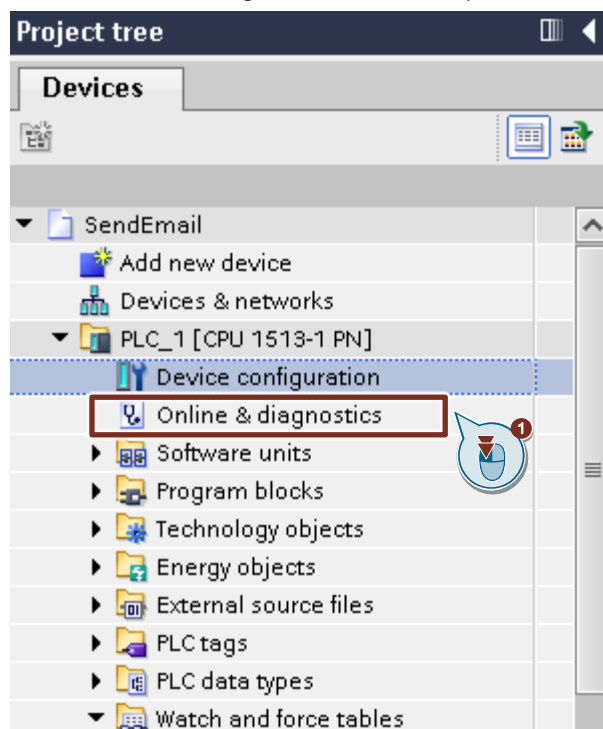
Because a certificate always has a time period over which it is valid, the time of the S7 CPU that wants to encrypt with this certificate must also be in this time period.

With a brand new S7 CPU or after an overall reset of the S7 CPU, the internal clock is set to a default value that lies outside the certificate runtime. The certificate is then marked as invalid.

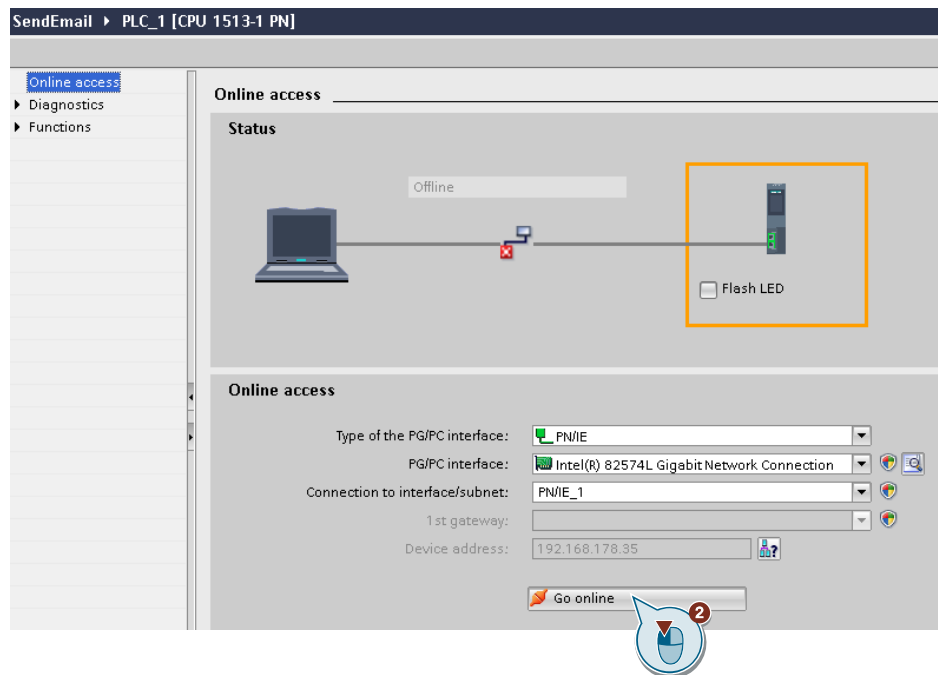
Setting the time manually

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

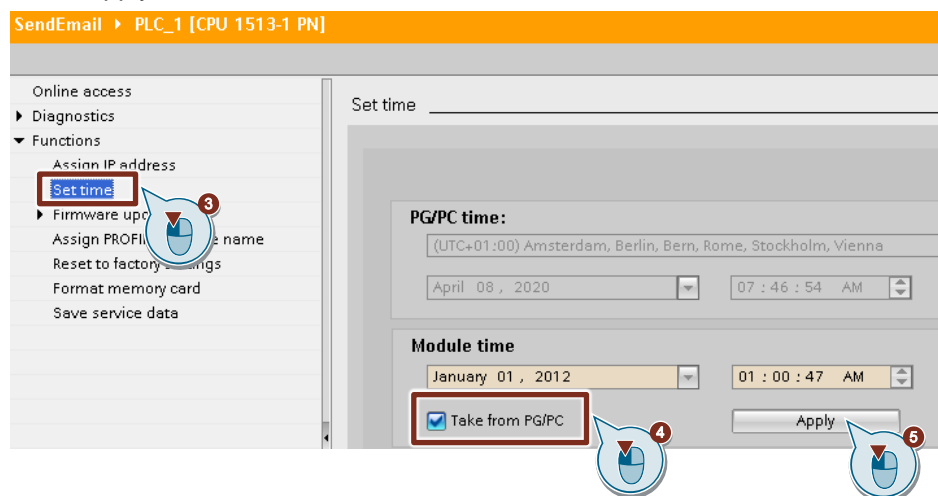
1. In the project navigation, double click "Online & diagnostics" in the device folder of the S7 CPU.
The Online and Diagnostics view will open.



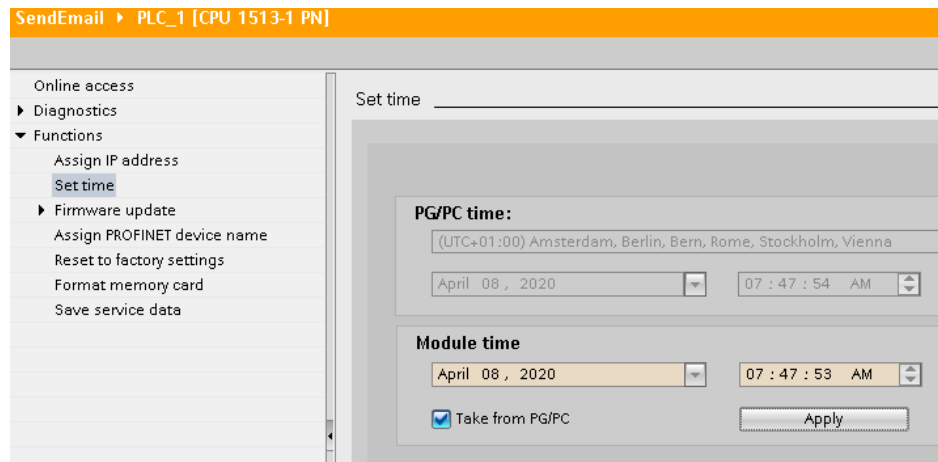
- Click the button "Go online".



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



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



Synchronize CPU time with NTP method

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

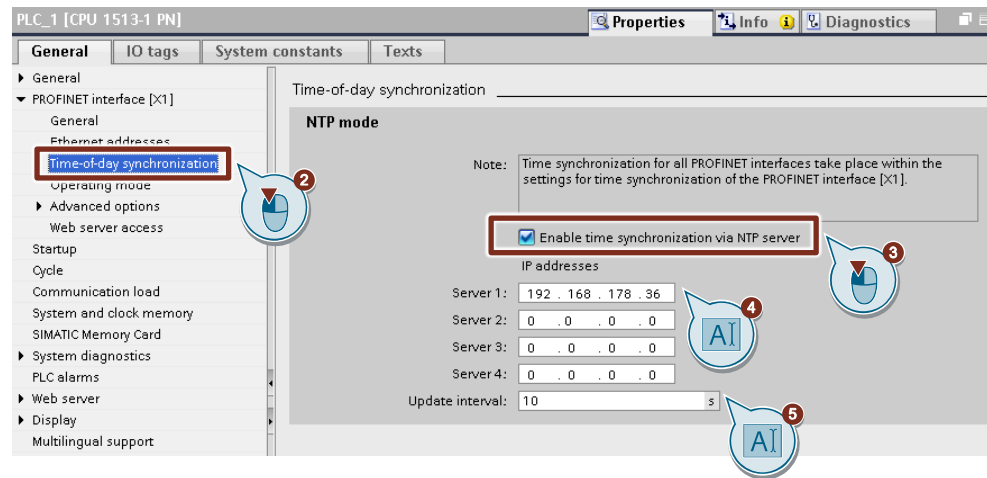
For the NTP method, the S7 CPU sends clock time requests at regular intervals (in client mode) to NTP servers in the subnet (LAN). Using the answers from the servers, the most reliable and accurate time is determined and the time of the CPU is synchronized.

For time synchronization sources you will address using the IP address, e.g. a communications 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 S7-1500 CPU:

Figure 2-9



1. Select the CPU in the network or device view. The properties of the CPU are displayed in the inspection window.
2. In the area navigation of the "General" tab, select the item "Time-of-day synchronization" under "PROFINET interface [X1]".
3. Enable the function "Enable time synchronization via NTP".
4. At the parameters "Server 1" to "Server 4", enter the IP addresses of up to 4 NTP servers.
5. Set the time interval of the clock requests at the "Update interval" parameter. Set the interval between 10 s and 86400 s.

Set the time of the CP

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.

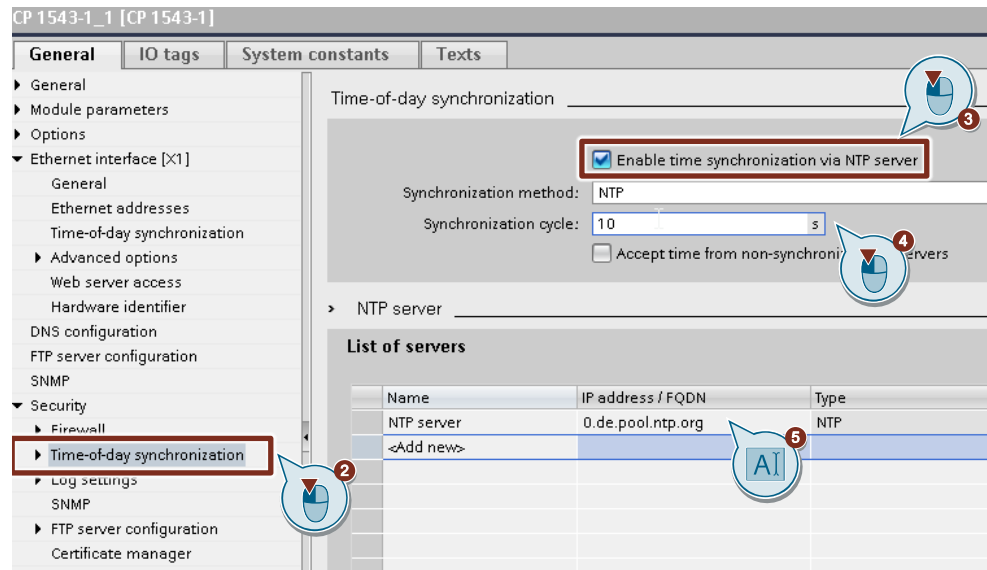
You can synchronize the CP's time using the NTP method with an NTP server.

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:

Figure 2-10



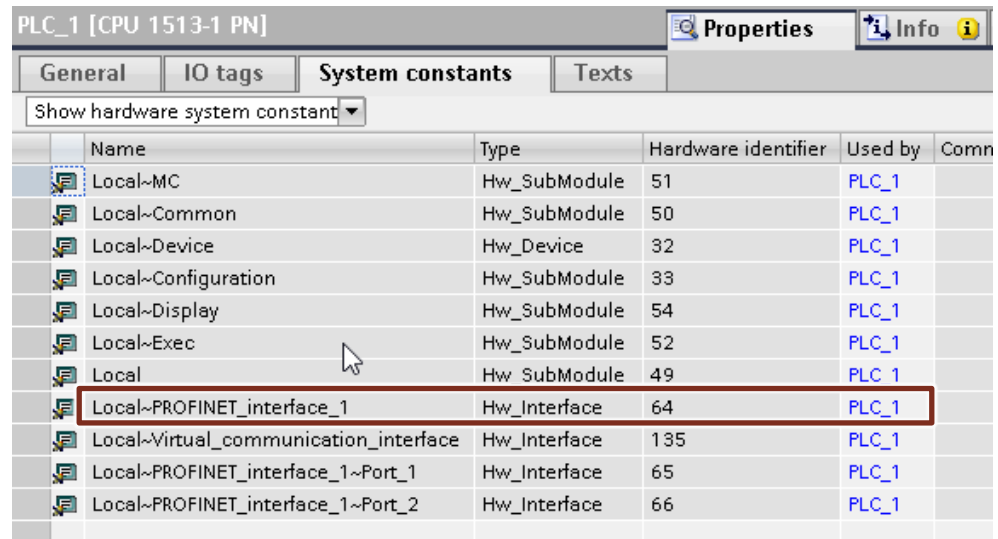
1. Select the CP in the network or device view. The properties of the CP are displayed in the Inspector window.
2. In the area navigation of the "General" tab, select the item "Time-of-day synchronization" under "Security".
3. Enable the function "Enable time synchronization via NTP".
4. Set the time interval of the time requests at the "Synchronization method" parameter. Set the sync cycle between 10 s and 86400 s.
5. Enter the IP address or DNS name of the NTP server in the list of servers.

2.2.12 Determine hardware identifier of the module

Find the hardware identifier of the CPU or CP in the hardware configuration.

Determine hardware identifier of the CPU

Figure 2-11

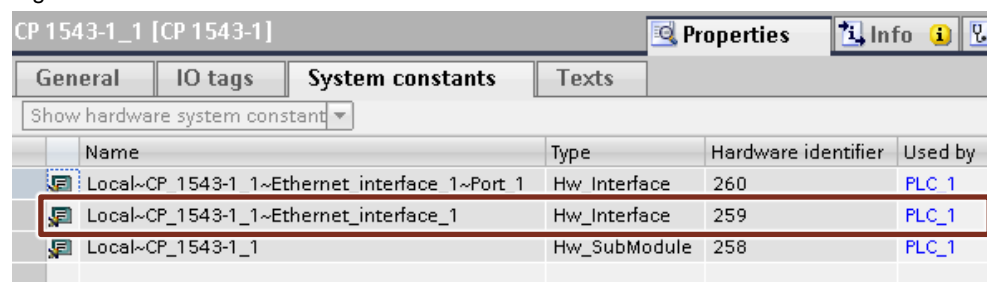


Name	Type	Hardware identifier	Used by	Comm
Local~MC	Hw_SubModule	51	PLC_1	
Local~Common	Hw_SubModule	50	PLC_1	
Local~Device	Hw_Device	32	PLC_1	
Local~Configuration	Hw_SubModule	33	PLC_1	
Local~Display	Hw_SubModule	54	PLC_1	
Local~Exec	Hw_SubModule	52	PLC_1	
Local	Hw_SubModule	49	PLC_1	
Local~PROFINET_interface_1	Hw_Interface	64	PLC_1	
Local~Virtual_communication_interface	Hw_Interface	135	PLC_1	
Local~PROFINET_interface_1~Port_1	Hw_Interface	65	PLC_1	
Local~PROFINET_interface_1~Port_2	Hw_Interface	66	PLC_1	

1. Select the CPU in the network or device view. The properties of the CPU are displayed in the inspection window.
2. Select the "System constants" tab to display the hardware identifier of the CPU's Ethernet port.

Determine hardware identifier of the CP

Figure 2-12



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

1. Select the CP in the network or device view. The properties of the CP are displayed in the Inspector window.
2. Select the "System constants" tab to display the hardware identifier of the CP's Ethernet port.

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	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 Overview of the system data types of "TMAIL_C"

The following tables present you with an overview of all system data types of the "TMAIL_C" instruction.

Table 3-2

System data type	STEP 7 V13		STEP 7 V14		SMTP (S) Ports
	Secured connection (SNMP over TLS)	Unsecured connection	Secured connection (SNMP over TLS)	Unsecured connection	
TMail_V4	Yes ¹⁾	Yes ²⁾	Yes ¹⁾	Yes ²⁾	Cannot be set.
TMail_V6	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Cannot be set.
TMail_FQDN	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Cannot be set.
TMail_V4_SEC	No	No	Yes ¹⁾	Yes ¹⁾	Can be set
TMail_V6_SEC	No	No	Yes ¹⁾	Yes ¹⁾	Can be set
TMail_QDN_SEC	No	No	Yes ¹⁾	Yes ¹⁾	Can be set
TMAIL_C instruction	V3.0		V4.0		
Library "Open user communication"	V4.1		V5.0		

¹⁾ Only supported via Ethernet port of the CP.

²⁾ Supported via the Ethernet port of the S7-1500 CPU from V2.0, of the S7-1200 CPU from V4.1, and of the CP.

System data type	STEP 7 V13		STEP 7 V16		SMTP (S) Ports
	Secured connection (SNMP over TLS)	Unsecured connection	Secured connection (SNMP over TLS)	Unsecured connection	
TMail_V4	Yes ¹⁾	Yes ²⁾	Yes ¹⁾	Yes ²⁾	Cannot be set.
TMail_V6	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Cannot be set.
TMail_FQDN	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Cannot be set.
TMail_V4_SEC	Yes ³⁾	Yes ³⁾	Yes ⁴⁾	Yes ⁴⁾	Can be set
TMail_V6_SEC	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Yes ¹⁾	Can be set
TMail_QDN_SEC	Yes ³⁾	Yes ³⁾	Yes ⁴⁾	Yes ⁴⁾	Can be set
TMAIL_C instruction	V5.0		V6.0		
Library "Open user communication"	V6.0		V7.0		

¹⁾ Only supported via Ethernet port of the CP.

²⁾ Supported via the Ethernet port of the S7-1500 CPU from V2.0, of the S7-1200 CPU from V4.1, and of the CP.

³⁾ Supported via the Ethernet port of the S7-1500 CPU from V2.5, and of the CP.

⁴⁾ Supported via the Ethernet port of the S7-1500 CPU from V2.5, of the S7-1200 CPU from V4.4, and of the CP.

[Table 1-1](#) shows which CPs support the following system data types for sending a secured email.

- TMail_QDN_SEC
- TMail_V4_SEC
- TMail_V6_SEC

3.3 Alternative solutions

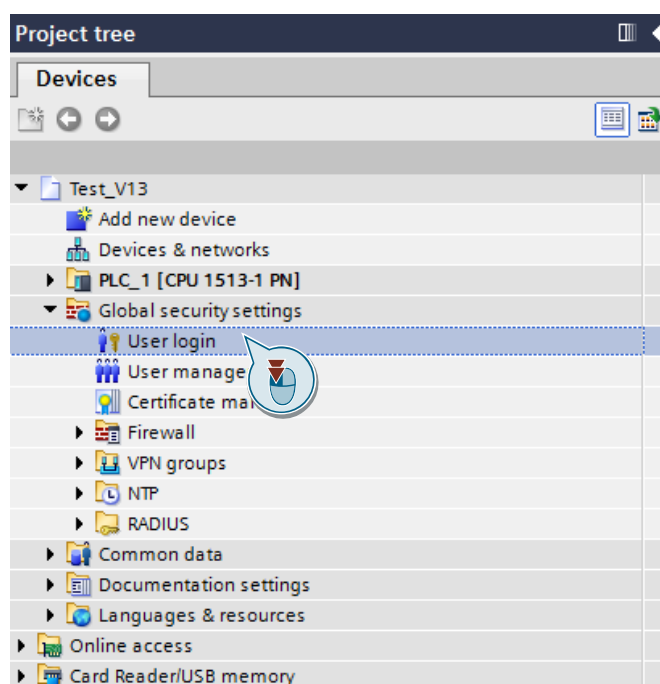
This chapter shows how to establish a secure connection to a mail server in STEP 7 V13 with the "TMAIL_C" instruction.

3.3.1 Integrating certificates into STEP 7 V13

Add the certificate of the provider in STEP 7 V13. In this application example the certificate "Telekom Root CA 2 Certificate" will be added:

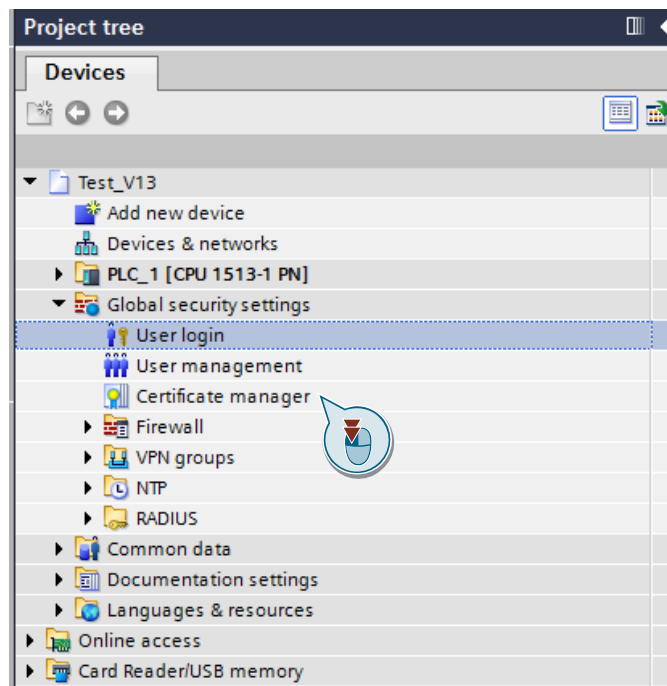
1. In order to log in the security user with user name and password for the global security settings, double click in the project navigation under "Global security settings" on "User login".

Create a new security user is none has been created. The security user must be logged in to add the provider certificate in the certificate manager.



3 Useful information

2. In order to open the certificate manager in the working area, double click "Certificate manager" in the project navigation under "Global security settings".



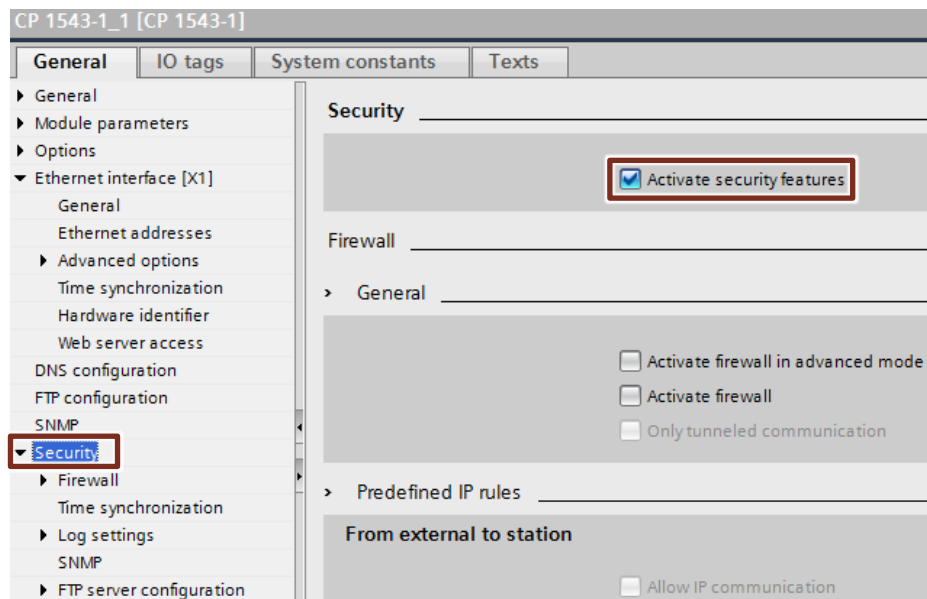
3. In the tab "Trusted certificates and root certification authorities", import for example the certificate "Telekom Root CA 2".

The screenshot shows the 'Certificate manager' window with the 'Trusted certificates and root certification authorities' tab selected. The window title is 'Test_V13 > Global security settings > Certificate manager'. The tab bar shows 'CA', 'Device certificates', and 'Trusted certificates and root cert...'. The main area contains a table with the following data:

Trusted certificates and root certification authorities				
Applicant	Issuer	Valid to	Used as	Private key
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Certificate	No
Thawte Premium Server CA	Thawte Premium Server CA	1/1/2021	Certificate	No
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/10/2019	Certificate	No

3.3.2 Configure CP 1543-1 in STEP 7 V13

1. Establish a connection between CP 1543-1 and the internet (see chapter [2.2.7](#)).
2. Configure the DNS server (see chapter [2.2.8](#)).
3. Set the clock time of the S7-1500 CPU (see chapter [2.2.11](#)).
4. In the area navigation of the "Properties" tab, select "Security" and enable the function "Activate security features".



3.3.3 Set up a secure connection to an email server in STEP 7 V13

Depending on the use case, the following system data types are available for parameterization of a secure email connection to the "TMAIL_C" instruction:

- "TMail_V4"
- "TMail_V6"
- "TMail_FQDN"

In the following sections we will explain the parameters of the system data types "TMail_FQDN" and "TMail_V4".

Parameter assignment for system data type "TMail_FQDN"

The email server is addressed via its fully-qualified domain name (FQDN) with the system data type "TMail_FQDN". The destination port cannot be set. The following table shows the structure of the "TMail_FQDN" system data type.

Table 3-3

Parameter	Data type	Value	Description
Interfaceld	LADDR	261	Hardware identifier of the Ethernet port of the CP 1543-1 (see chapter 2.2.12)
ID	CONN_OUC	1	Connection ID
Connectiontype	BYTE	16#22	Connection type For FQDN, select 16#22 as connection type.
ActiveEstablishment	BOOL	-	Status bit The status bit is set to "1" when the connection is established.
CertIndex	BYTE	16#1	Set the parameter "CertIndex" to 1. You hereby specify that a secure email connection is being set up.
WatchDogTime	TIME	T#1m	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process.
MailServerQDN	STRING[254]	For ex.: 'smtp@provider.com'	FQDN (Full Qualified Domain Name) of the email server from which you wish to send an email.
UserName	STRING[254]	For ex.: 'myUserName'	The user name and password is how the connection is identified.

3 Useful information

Parameter		Data type	Value	Description
PassWord		STRING[254]	For ex.: 'myUserPassWord'	
From		EMAIL_ADDR	-	Sender address of the email which is defined with the following two STRING parameters.
	LocalPartPlusAtSign	STRING[64]	For ex.: 'myName@'	Local part of the sender address including @ sign.
	FullQualifiedDomain Name	STRING[254]	For ex.: 'provider.com'	FQDN (Fully Qualified Domain Name) of the email server.

Parameter assignment for system data type "TMail_V4"

Using the system data type "TMail_V4", the email server will be addressed via the IP address in IPv4. The destination port cannot be set. The following table shows the structure of the "TMail_V4" system data type.

Table 3-4

Parameter	Data type	Value	Description
Interfaceld	LADDR	261	Hardware identifier of the Ethernet port of the CP 1543-1 (see chapter 2.2.12)
ID	CONN_OUC	1	Connection ID
Connectiontype	BYTE	16#20	Connection type For IPv4, select 16#20 as connection type.
ActiveEstablishment	BOOL	-	Status bit The status bit is set to "1" when the connection is established.
CertIndex	BYTE	16#1	Set the parameter "CertIndex" to 1. By setting the "CertIndex" parameter to 1, you indicate that you intend to set up a secure email connection.
WatchDogTime	TIME	T#1m	Time monitoring of the execution. Use this parameter to define the maximum execution time of the sending process.
MailServerAddress	IP_V4	For ex.: 213.165.67.108	IP address of the email server (in IPv4 format) from which you wish to send an email.
UserName	STRING[254]	For ex.: 'myUserName'	The user name and password is how the user identifies him/herself as the owner of the email account to the email provider.
PassWord	STRING[254]	For ex.: 'myUserPassWord'	

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]	For ex.: 'myName@'	Local part of the sender address including @ sign.
	FullQualifiedDomain Name	STRING[254]	For ex.: 'provider.com'	FQDN (Fully Qualified Domain Name) of the email server.

Parameter assignment for "TMAIL_C" instruction

In the user program of the S7 CPU, call the instruction "TMAIL_C" with one of the system data types "TMail_V4", "TMail_V6" or "TMail_FQDN" (see chapter [2.2.10](#)).

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

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:

www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

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:

www.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

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

4.2 Links and literature

Table 4-1

No.	Subject
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/46817803
\3\	SIMATIC STEP 7 Professional V16 https://support.industry.siemens.com/cs/ww/en/view/109773506

4.3 Change documentation

Table 4-2

Version	Date	Change
V1.0	06/2017	First edition
V2.0	04/2020	Added section for sending a secure email via the integrated Ethernet port of the CPU