

SIEMENS



FAQ • 04/2016

How do you establish an HTTPS connection between WinCC Runtime Advanced and a Comfort Panel?

WinCC V13 SP1 Update 4 / HMI Operator Panels



<https://support.industry.siemens.com/cs/ww/en/view/109483471>

This entry originates from Siemens Industry Online Support. The conditions of use specified there apply (http://www.siemens.com/corp/en/index/terms_of_use.htm).

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 only form one element of such a concept.

Customers are responsible to prevent unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

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

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

Contents

1	Introduction	3
1.1	Components Used	3
2	Description	4
2.1	Scenario 1: SIMATIC PC Station as HTTPS Server and a Comfort Panel as HTTPS Client	4
2.2	Scenario 2: Comfort Panel as HTTPS Server and a SIMATIC PC Station as HTTPS Client.	7
3	History	13

1 Introduction

HTTP Connection

An HTTP connection is used in local networks for fast, unencrypted transmission of non-critical data.

HTTPS Connection

An HTTPS connection provides a secured HTTP connection between operator panels. At the beginning of the communication both operator panels have to be authenticated with certificates. The user data are encrypted to ensure secure communication.

Manual

More information on the topic of communication via SIMATIC HMI HTTP is available in the system manual WinCC Advanced V13 SP1 in Entry ID [109091876](#).

1.1 Components Used

This entry has been created with the components below.

Software Components

Table 1-1

Component	Qty.	Article number	Software version
WinCC TIA V13	1	6AV2102-0AA03-0AA5	SP1 Update 4
MS Windows 7	1	--	Enterprise SP1
MS Windows CE	1	--	Version 6.00

Hardware Component

Component	Qty.	Article number	Note
TP700 Comfort	1	6AV2 124-0GC01-0AX0	V13.0.1.0
PLC S7-1500	1	6ES7 515-2AM00-0AB0	CPU 1515-2 PN, V1.7

2 Description

This entry gives you two scenarios for configuring an HTTPS connection between WinCC Runtime Advanced and a TP700 Comfort Panel in WinCC (TIA Portal) V13 SP1 and shows you how to install certificates on each of the operator panels.

- **Scenario 1:**
[PC-Station as HTTPS Server and a Comfort Panel as HTTPS Client.](#)
- **Scenario 2:**
[Comfort Panel as HTTPS Server and a PC Station as HTTPS Client.](#)

Note This entry shows the Runtime settings of an existing connection to be made for a WinCC Advanced V13 SP1 taking the example of an existing project for a Comfort Panel TP700.

The project must have been transferred to the Comfort Panel TP700 and a connection is established to the WinCC Advanced V13 SP1.

More information on the topic of HTTP and HTTPS connections is available in the system manual WinCC Advanced V13 SP1 in Entry ID [109091876](#).

2.1 Scenario 1: SIMATIC PC Station as HTTPS Server and a Comfort Panel as HTTPS Client

Configuring the HTTPS client connection

The table below shows the Runtime settings to be made in WinCC Advanced V13 SP1.

Note The settings below are for the following scenario:

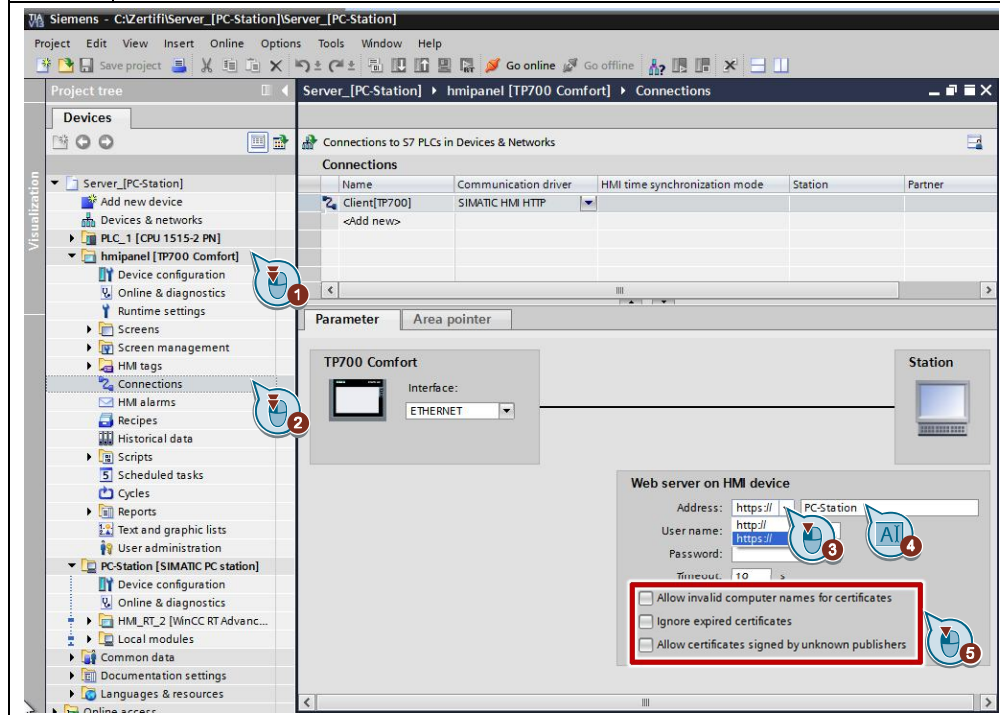
- The SIMATIC PC station is the server: "PC station"
- The Comfort Panel is the client: "hmipanel"

Table 2-1

No.	Procedure
1.	In the project navigation you double-click the Comfort Panel "hmipanel (TP700 Comfort)" which has already been created. (1)
2.	In the project navigation you double-click the "Connections" editor (2).

No.	Procedure
3.	<p>In the area "Web server area on HMI device"</p> <ul style="list-style-type: none"> • For "Address:" you select the option "https:" (3) and enter the computer name under which the Web server can be reached on the HMI device (4), for example: "PC station". • Disable the options below (5): <ul style="list-style-type: none"> ○ Allow invalid computer names for certificates ○ Ignore expired certificates ○ Allow certificates signed by unknown publishers

4.	Save your inputs and load the settings made.
----	--



Note

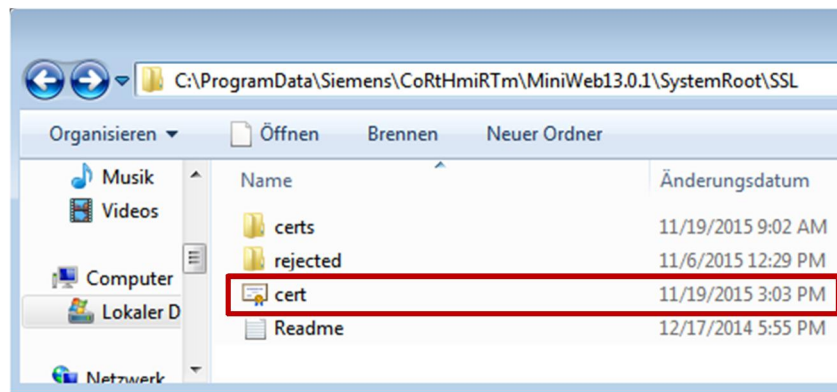
- For an HTTP connection you can enter either the IP address or the computer name of the Web server.
- For an HTTPS connection you must enter the **computer name** of the Web server. This is because the certificate is created based on the computer name.

Creating a certificate

The first time an HTTPS client is accessed the HTTPS server generates the certificate itself and saves it in the "Cert.cer" file.

Note In this case the SIMATIC PC station "PC station" is the HTTPS server.

Figure 2-1



- The saved "Cert.cer" file is located in the following directory:
"C:\ProgramData\Siemens\CoRtHmiRTm\MiniWeb13.0.1\SystemRoot\SSL"
- To install the certificate created on the HTTPS client you save the created "Cert.cer" file on a storage medium.

Installing a certificate on the HTTPS client

The table below shows how to install the created certificate on a Comfort Panel (HTTPS client) based on Windows CE.

Table 2-2

No.	Procedure
1.	Connect the storage medium on which the "Cert.cer" file is stored with the Comfort Panel.
2.	Open the Control Panel.
3.	In the menu you double-click "Certificates".
4.	In the "Certificates" window that opens you click the "Import..." button.
5.	The "Import Certificate or..." dialog window opens.
6.	In the "From a File" menu you click "OK" and in the file browser you select the "Cert.cer" file located in the storage medium.

Result

- The certificate created by the HTTPS server has already been installed on the HTTPS client.
- When renewed access to the HTTPS client the connection to the HTTPS server is established successfully.

2.2 Scenario 2: Comfort Panel as HTTPS Server and a SIMATIC PC Station as HTTPS Client.

Configuring the HTTPS client connection

The table below shows the Runtime settings to be made in WinCC V13 SP1 on the control room PC.

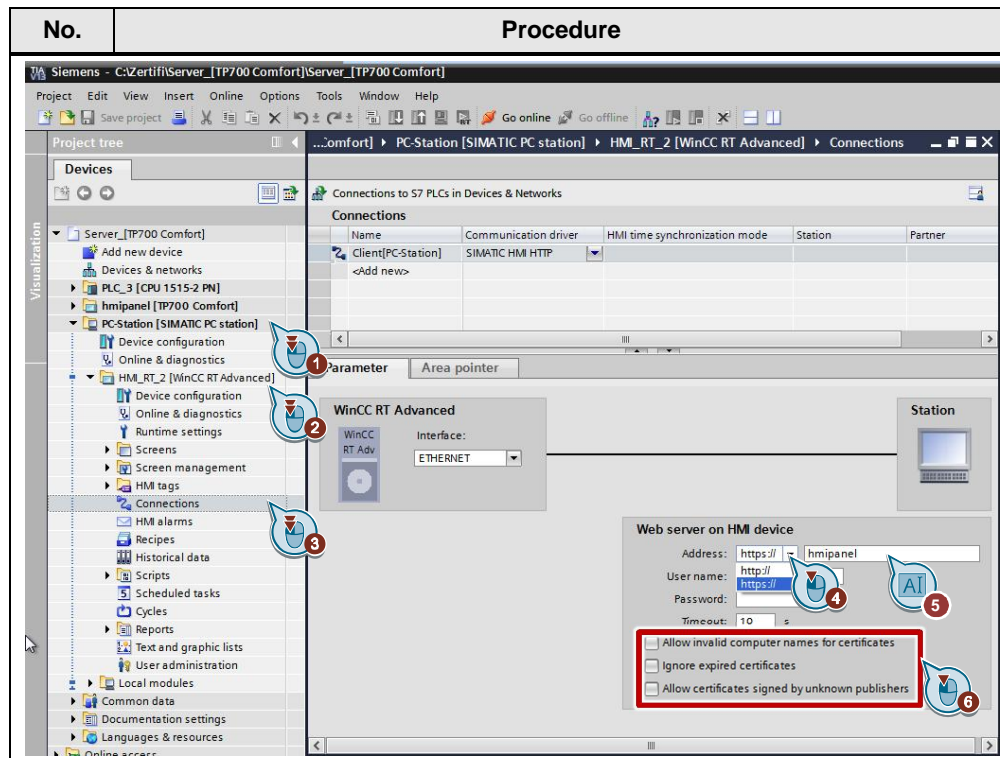
Note

The settings below are for the following scenario:

- The Comfort Panel is the server: "hmipanel"
- The SIMATIC PC station is the client: "PC station"

Table 2-3

No.	Procedure
7.	In the project navigation you double-click the SIMATIC PC station "PC station" already created. (1)
8.	In the project navigation you double-click the "HMI_RT_2 [WinCC RT Advanced]" editor (2).
9.	In the project navigation you double-click the "Connections" editor (3).
10.	<p>In the area "Web server area on HMI device"</p> <ul style="list-style-type: none"> • For "Address:" you select the option "https:" (4) and enter the computer name under which the Web server can be reached on the HMI device (5), for example: "hmipanel" • Disable the options below (6) <ul style="list-style-type: none"> ○ Allow invalid computer names for certificates ○ Ignore expired certificates ○ Allow certificates signed by unknown publishers
11.	Save your inputs and load the settings made.



Note

- For an HTTP connection you can enter either the IP address or the computer name of the Web server.
- For an HTTPS connection you must enter the **computer name** of the Web server. This is because the certificate is created based on the computer name.

Creating a certificate

The first time an HTTPS client is accessed the HTTPS server generates the certificate itself and saves it in the "Cert.cer" file.

Note

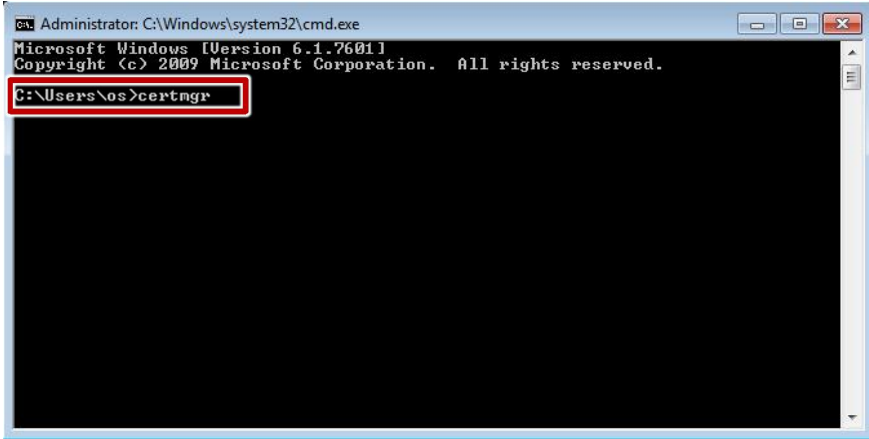
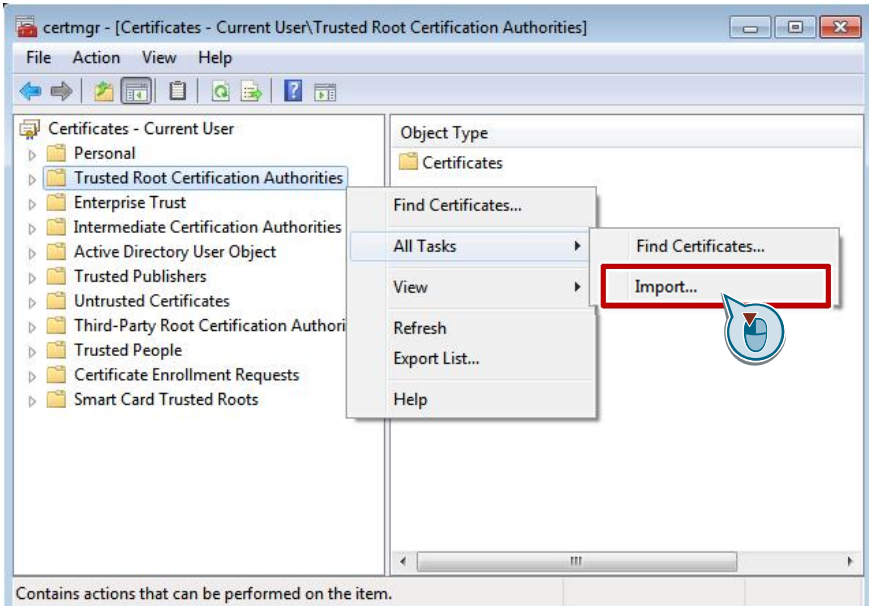
In this case the Comfort Panel "TP700 Comfort" is the HTTPS server.


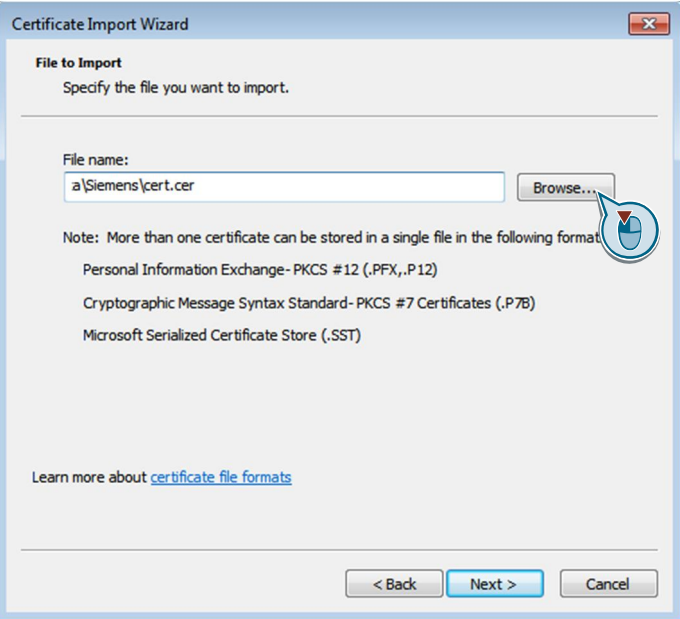
- The saved "Cert.cer" file is located in the following directory in the Comfort Panel based on Windows CE: "flash\simatic\SystemRoot\SSL".
- To install the certificate created on the HTTPS client you save the created "Cert.cer" file on a storage medium.

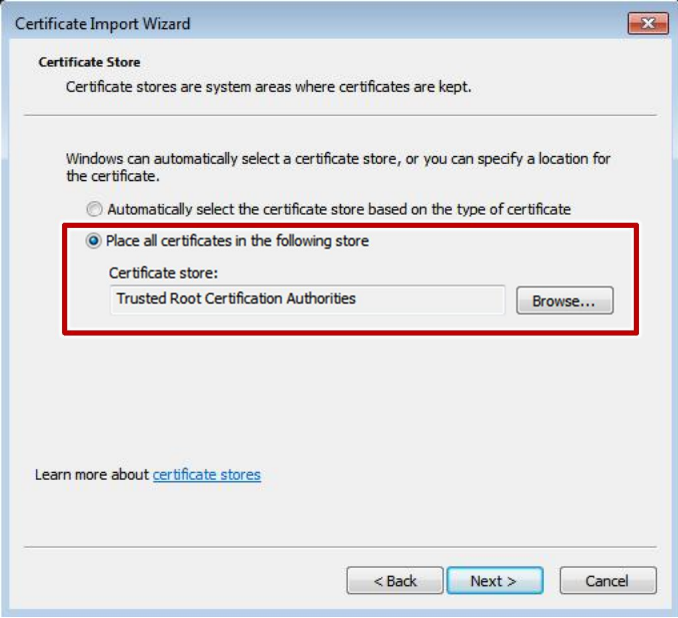
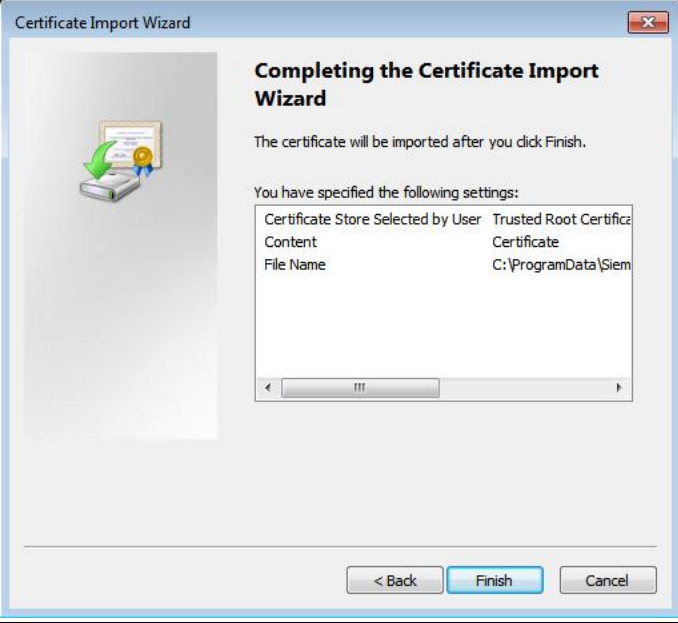
Installing a certificate on the HTTPS client

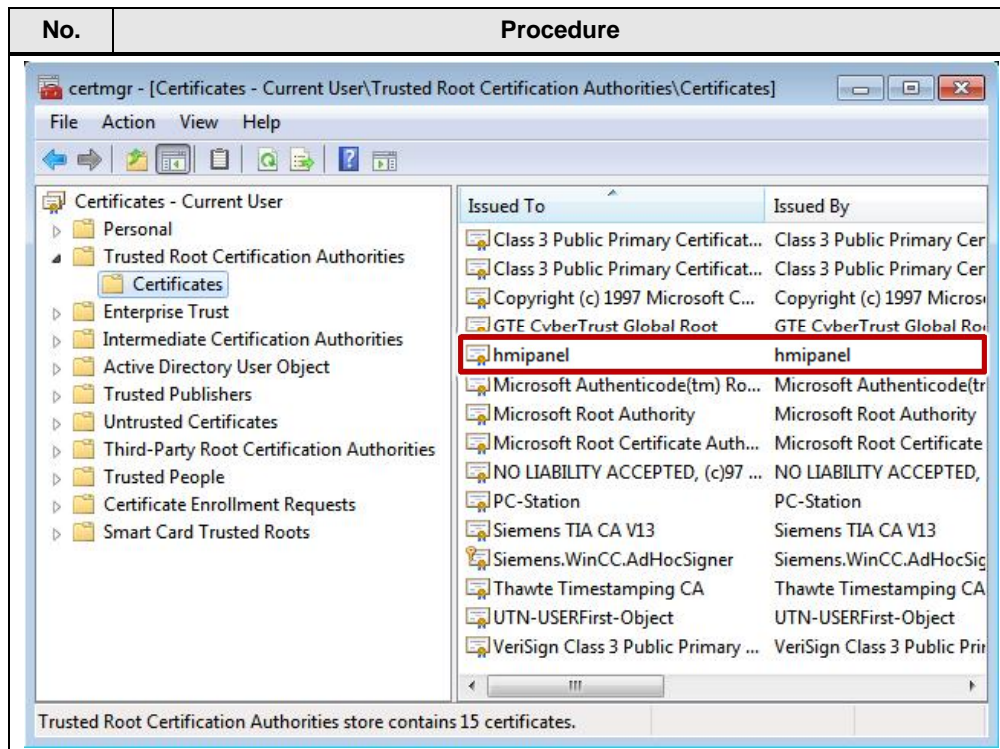
The table below shows how to install the created certificate on a PC station (HTTPS client) based on Windows 7.

Table 2-4

No.	Procedure
12.	Connect the storage medium on which the "Cert.cer" file is stored with the PC station.
13.	<p>Call the "Input Prompt" window</p> <ul style="list-style-type: none"> In the Windows Start menu you click "Start" > "Input prompt" and enter the command "cmd". Then click "Enter".
14.	<p>Open the "Certificates – Current User" window</p> <ul style="list-style-type: none"> Enter the following command: "certmgr". Then click "Enter". 
15.	In the "Certificates - Current User" window that opens you right-click "Trusted Root Certification Authorities"
16.	<p>Click "All Tasks > Import...".</p> 

No.	Procedure
17.	<p>In the "Certificate Import Wizard" window that opens you click "Next >".</p> 
18.	<p>In the "File to Import" window you click "Browse..." and in the file browser you select the "Cert.cer" file located in the storage medium. Then you click "Open" followed by "Next >".</p> 

No.	Procedure
19.	<p>In the "Certificate Store" window you make sure that the certificate is correctly stored in the "Trusted Root Certification Authorities" certificate store. Then click "Next >".</p> 
20.	<p>In the "Completing the Certificate Import Wizard" window you click "Finish".</p> 
21.	<p>In the "Security Warning" window you click "Yes" to confirm installation of the certificate.</p>



Result

- The certificate created by the HTTPS server has already been installed on the HTTPS client.
- When renewed access to the HTTPS client the connection to the HTTPS server is established successfully.

3 History

Table 3-1

Version	Date	Modification
V1.0	02/2016	First edition

4