

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 (<u>http://www.siemens.com/corp/en/index/terms\_of\_use.htm</u>).

**Security Informati** 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 <a href="http://www.siemens.com/industrialsecurity">http://www.siemens.com/industrialsecurity</a>.

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 <u>http://www.siemens.com/industrialsecurity</u>.

## Contents

on

1	Introdu	ction	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 <u>109091876</u>.

## 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 <u>109091876</u>.

## 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.	In the area "Web server area on HMI device"			
	<ul> <li>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".</li> <li>Disable the options below (5):</li> </ul>			
	<ul> <li>Allow invalid computer names for certificates</li> </ul>			
	<ul> <li>Ignore expired certificates</li> </ul>			
	<ul> <li>Allow certificates signed by unknown publishers</li> </ul>			
4.	Save your inputs and load the settings made.			
Project Edit	C:ZertifilServer_[PC-Station]\Server_[PC-Station] View Insert Online Options Tools Window Help ve project – 회 첫 1월 급 것 1월 2 것 1월 1월 1월 1월 1월 20 <b>6</b> online 중 Gooffline 유규 18 18 2 것 - 111			
Project tre	e I Server_[PC-Station] > hmipanel [TP700 Comfort] > Connections _ I = I = X			
Devices				
Uitration Uitration	Image: Server_[PC-Station]       Image: Connections to 57 PLCs in Devices & Networks         Image: Connections       Connections         Image: Connections       Server_[PC-Station]         Image: Connections       Server_[PC-Station]         Image: Connections       Server_[PC-Station]         Image: Connections       Station         Image: Connections			
2	Online & diagnostics			
	Screens Station  FP700 Confort Interface: Interface: ETHERNET  Web server on HMI device Address: https:// PCStation User name: http:// Password: Passw			
► Contin	nguages & resources			

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.	In the area "Web server area on HMI device"	
	<ul> <li>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"</li> </ul>	
	Disable the options below (6)	
	<ul> <li>Allow invalid computer names for certificates</li> </ul>	
	<ul> <li>Ignore expired certificates</li> </ul>	
	<ul> <li>Allow certificates signed by unknown publishers</li> </ul>	
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.

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.

Note

		Procedure
12.	Connect the storage medium on w station.	hich the "Cert.cer" file is stored with the PC
13.	<ul> <li>Call the "Input Prompt" window</li> <li>In the Windows Start menu you click "Start" &gt; "Input prompt" and enter the command "cmd".</li> <li>Then click "Enter".</li> </ul>	
14.	Open the "Certificates – Current • Enter the following comman • Then click "Enter". • Administrator: C:\Windows\system32\cmd.exe Microsoft Windows [Version 6.1.?60] Copyright <c> 2009 Microsoft Corpor C:\Users\os&gt;certmgr</c>	User" window nd: "certmgr".
15	In the "Certificates, Current Llear"	window that opens you right disk "Trusted
15.	Root Certification Authorities"	window that opens you right-click Trusted
16.	Click "All Tasks > Import".	
	Certificates - Current User\Trusted File Action View Help	Root Certification Authorities]

No.	Procedure		
17.	In the "Certificate Import Wizard" window that opens you click "Next >	'.	
	Certificate Import Wizard Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and certification authority, is		
	a continuation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.         To continue, click Next.	-	
18.	18. 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 "Ope followed by "Next >".		
	Certificate Import Wizard		
	File name: a \Siemens \cert.cer Note: More than one certificate can be stored in a single file in the following formation Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)	)	
	Learn more about <u>certificate file formats</u> < Back	_	

No.	Procedure	
19.	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 >".	
	Certificate Import Wizard	
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	Automatically select the certificate store based on the type of certificate     Place all certificates in the following store     Certificate store:     Trusted Root Certification Authorities     Browse	
	Learn more about <u>certificate stores</u>	
	< Back Next > Cancel	
20.	In the "Completing the Certificate Import Wizard" window you click "Finish".	
	Certificate Import Wizard	
	Completing the Certificate Import Wizard	
	The certificate will be imported after you dick Finish.	
	You have specified the following settings: Certificate Store Selected by User Trusted Root Certifica Content Certificate File Name C: \ProgramData\Siem	
	« <u> </u>	
	< Back Finish Cancel	
21.	In the "Security Warning" window you click "Yes" to confirm installation of the certificate.	

No.	Procedure	
<ul> <li>certmgr - [Certificates - Current User\Trusted Ro</li> <li>File Action View Help</li> <li>Certificates - Current User</li> <li>Personal</li> <li>Trusted Root Certification Authorities</li> <li>Certificates</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Active Directory User Object</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Trusted People</li> <li>Certificate Enrollment Requests</li> <li>Smart Card Trusted Roots</li> </ul>	Class 3 Public Primary Certificates Class 3 Public Primary Certificat Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C GTE CyberTrust Global Root Microsoft Authenticode(tm) Ro Microsoft Root Authority Microsoft Root Certificate Auth NO LIABILITY ACCEPTED (c)97	Issued By Class 3 Public Primary Cer Class 3 Public Primary Cer Copyright (c) 1997 Micros GTE CyberTrust Global Ro hmipanel Microsoft Authenticode(tr Microsoft Root Authority Microsoft Root Certificate NO LIABILITY ACCEPTED
	PC-Station     Siemens TIA CA V13     Siemens.WinCC.AdHocSigner     Thawte Timestamping CA     UTN-USERFirst-Object     VeriSign Class 3 Public Primary     III	PC-Station Siemens TIA CA V13 Siemens.WinCC.AdHocSi Thawte Timestamping CA UTN-USERFirst-Object VeriSign Class 3 Public Pr

#### 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.

## History Table 3-1 3

Version	Date	Modification
V1.0	02/2016	First edition

③ Siemens AG 2016 All rights reserved

4

4

#### HTTPS-Connection, TIA V13 SP1, HMI Panels Entry ID: 109483471, V1.0, 04/2016