

SIEMENS

Ingenuity for life

Industry Online Support

Home

Why do you get an error message when opening the Sm@rtClient with the internet browser?

WinCC (TIA Portal) Advanced / V15 / Sm@rtService

<https://support.industry.siemens.com/cs/ww/en/view/101977510>

Siemens
Industry
Online
Support



This entry originates from Siemens Industry Online Support. The conditions of use specified there apply (www.siemens.com/nutzungsbedingungen).

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. 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 the 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	Configuration Notes	3
1.1	Message "Run this application?"	3
1.2	Message "Continue loading this web page?"	4

1 Configuration Notes

Additional settings are needed to operate the Sm@rtClient with the internet browser depending on the version of the operator panel used and the version of Java used.

A description of possible messages and how to clear them is given in this document.

This entry is valid for WinCC (TIA Portal) V15 and operator panels with versions V13.0.1 and higher in conjunction with the Java 8 software.

The following components have been used for the description:

- Operator panel: TP1200 Comfort Panel.
- IP address: 172.16.34.220.
- Service: "Start Sm@rtServer remote access" enabled.
- Web browser: Microsoft Internet Explorer V11.
- Oracle: Java V8.

1.1 Message "Run this application?"

Input in the address bar of the Internet Explorer (without encryption).

- <http://172.16.34.220:5800/>

Message

Figure 1-1



Solution

Click "Run". The window closes automatically and the web interface "VNC Authentication" of the Sm@rtClient display is called.

Note

Enable the option (1) to avoid having to confirm each time.

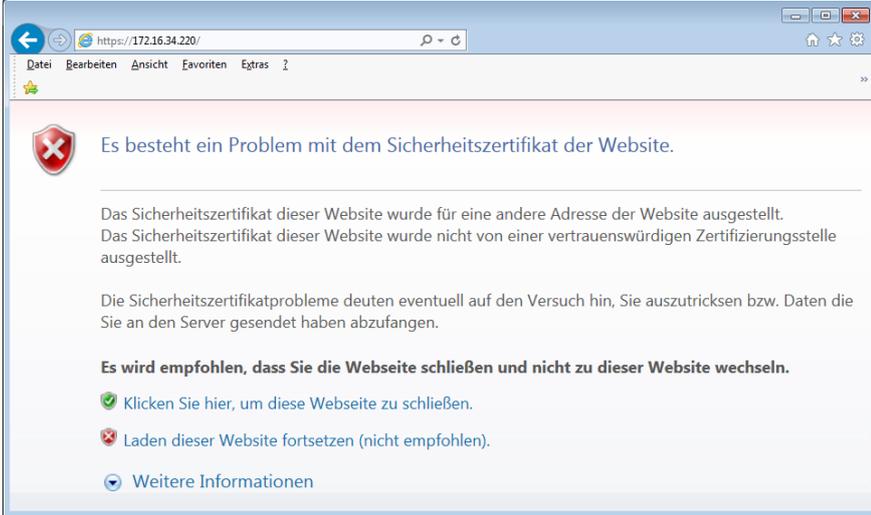
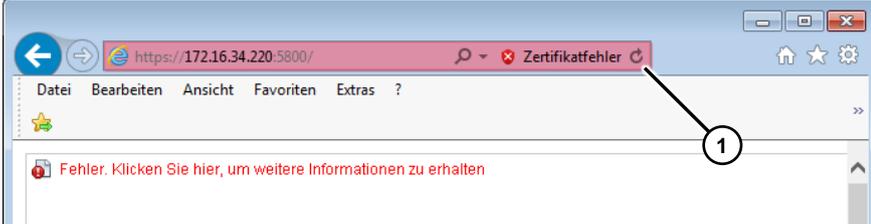
1.2 Message "Continue loading this web page?"

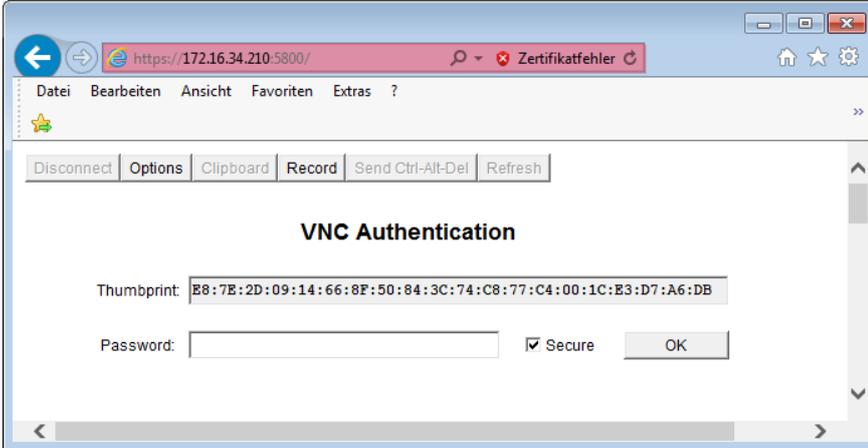
Input in the address bar of the Internet Explorer (with encryption).

- <https://172.16.34.220:5800/>

Messages

Table 1-1

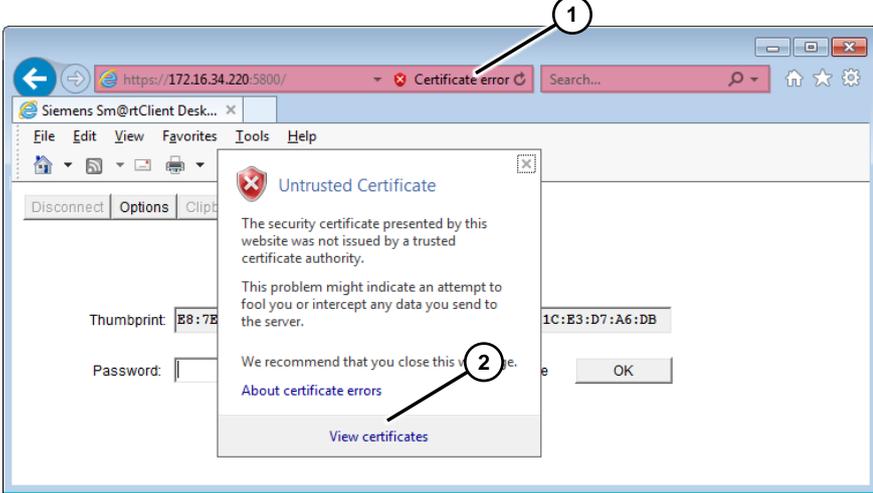
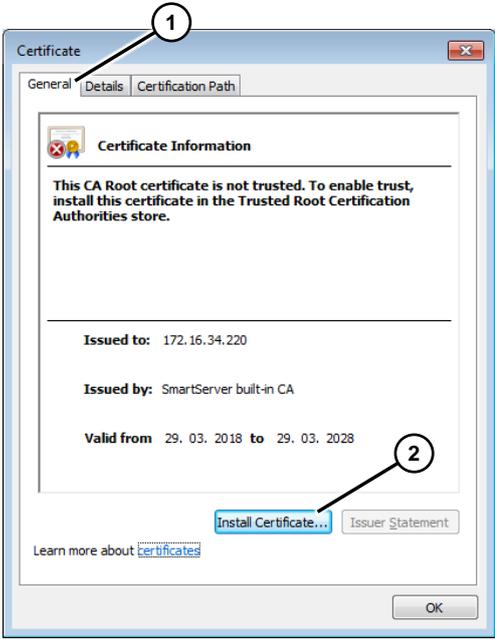
No.	Description
1.	 <p>Click the text "Continue loading this web page (not recommended)". The following message is displayed: "Continue?".</p>
2.	 <p>Click the "Next >" button. The following message is displayed.</p>
3.	 <p>Click the icon for updating the browser page (1). The following message is displayed.</p>

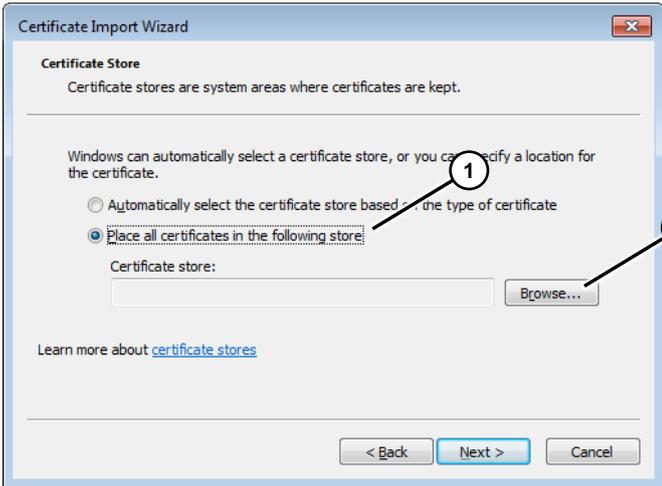
No.	Description
4.	 <p>Click "Run". The window closes automatically and the web interface "VNC Authentication" of the Sm@rtClient display is called.</p> <p>Note Enable the option (1) to avoid having to confirm each time.</p>
5.	<p>View of the web interface "VNC Authentication" of the Sm@rtClient display. The address bar of the web browser stays red because of the certificate error. This does not adversely affect the function.</p> 
6.	<p>The following solution shows how to clear the certificate error.</p> <p>Note The messages described above cannot be prevented.</p>

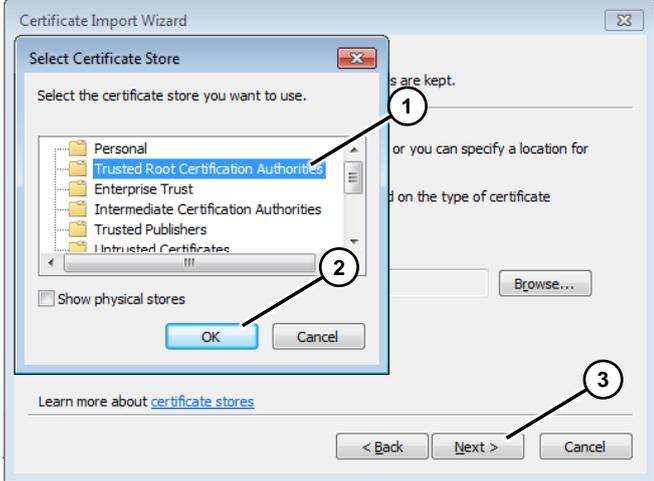
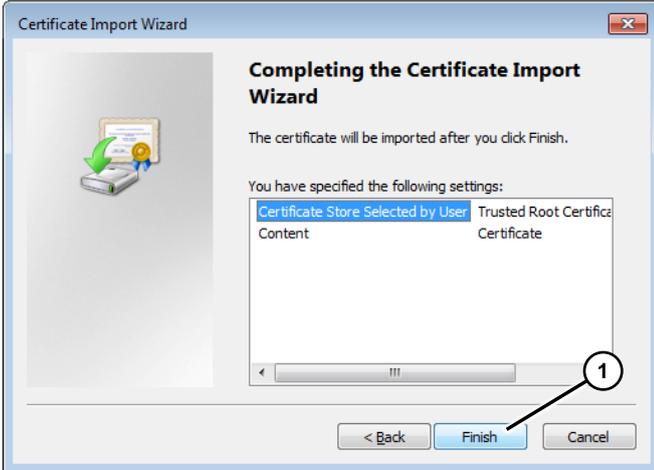
Solution

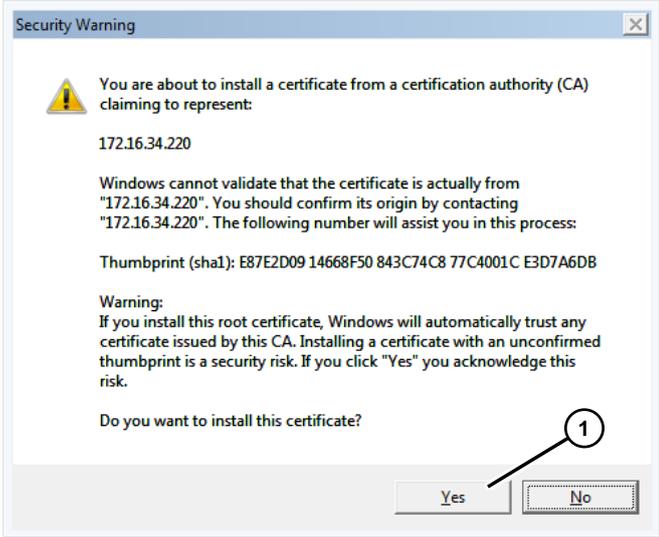
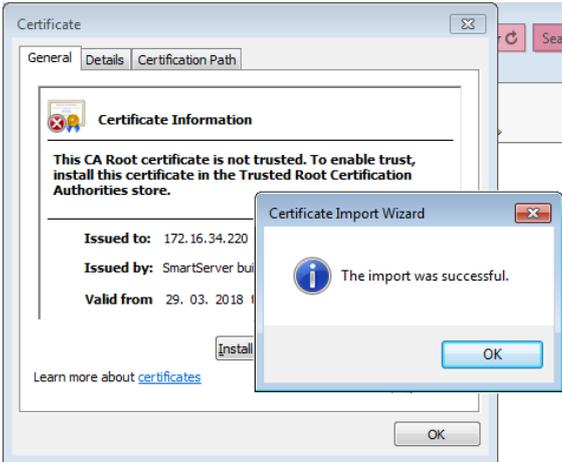
To stop the certificate error from being displayed you have to install the certificate of the TP1200 Comfort Panel in the certificate folder of the Windows operating system.

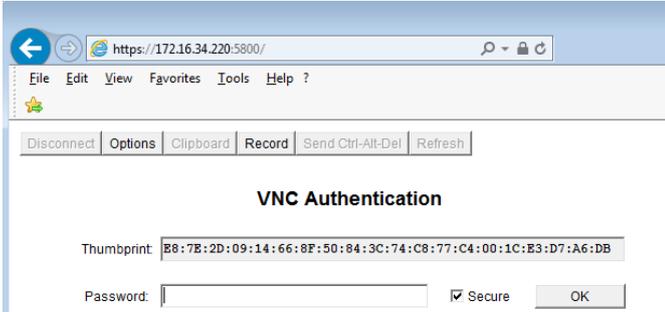
Table 1-2

No.	Description
1.	<p>Open the certificate</p> <ul style="list-style-type: none"> In the address bar you click the certificate error (1). The "Untrusted Certificate" window opens. Open the certificate (2). 
2.	<p>Certificate view</p> <ul style="list-style-type: none"> Open the "General" tab (1). Click the "Install Certificate..." button (2). The Certificate Import Wizard opens. 

No.	Description
<p>3.</p>	<p>Certificate Import Wizard</p> <ul style="list-style-type: none"> Then click the "Next >" (1) button. 
<p>4.</p>	<ul style="list-style-type: none"> Enable the radio button (1). Click the "Browse..." button (2). 

No.	Description
5.	<ul style="list-style-type: none"> Mark the folder "Trusted Root Certification Authorities" (1) and confirm the input with "OK" (2). Click the "Next >" (3) button. 
6.	<ul style="list-style-type: none"> Click the "Finish" button (1) to close the wizard. 

No.	Description
7.	<ul style="list-style-type: none"> Acknowledge the warning with "Yes" (1). 
8.	<ul style="list-style-type: none"> Acknowledge the message and the certificate window with "OK". 

No.	Description
9.	<ul style="list-style-type: none"> Close and re-open the web browser to apply the settings. Enter the address of the operator panel again in the address bar. After the logon routine no certificate error is displayed in the address bar. This completes the settings. 

Display installed certificates

Proceed as follows to check/edit the installed certificates.

- Call the Microsoft Management Console (MMC) via Windows Start menu > Find mask "mmc" > Start mmc.exe.
- In the MMC console click "File > Add/Remove Snap-In..." (alternatively CTRL+M).
- In the "Available Snap-Ins" window you select the "Certificates" snap-in and add it to the "Selected Snap-Ins" window via the "Add >" button. A window opens. Select the option "Use own user account".
- Confirm the entry with "OK".
- Now different certificate folders are displayed. Open the "Trusted Root Certification Authorities" folder.

View of the installed certificate.

Figure 1-2

