

Industry Online Support

NEWS

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).

Siemens provides products and solutions with industrial security functions that support the Security secure operation of plants, systems, machines and networks. Informa-In order to protect plants, systems, machines and networks against cyber threats, it is tion 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

Config	Configuration Notes		
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

				×
мос	nten Sie d	liese Anwen	dung ausruhren?	
		Name:	VncViewer	
	2	Anbieter:	Siemens AG	
		Verzeichnis:	http://172.16.34.220:5800	
Diese Anwendung wird mit uneingeschränktem Zugriff ausgeführt. Dies kann ein Risiko für Ihren Rechner und Ihre persönlichen Informationen darstellen. Führen Sie diese Anwendung nur aus, wenn Sie dem Speicherort und dem oben angegebenen Anbieter vertrauen.				
Fi	ir Anwen <u>d</u> unge	n dieses Anbieters	s und aus diesem Speicherort nicht mehr anzeigen	
E	Mehr Inform	nationen	Ausführen Abbrechen	

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.	Compared to the second	× ₩ * ₩				
	Es besteht ein Problem mit dem Sicherheitszertifikat der Website.					
	Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt. Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.	e				
	Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten Sie an den Server gesendet haben abzufangen.	die				
	Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.					
	🖉 Klicken Sie hier, um diese Webseite zu schließen.					
	Value					
	Weitere Informationen					
	Click the text "Continue loading this web page (not recommended)". The following message is displayed: "Continue?".					
	Möchten Sie fortfahren? Die Verbindung zu dieser Website ist nicht vertrauenswürdig Website: https://172.16.34.220:5800 Hinweis: Das Zertifikat ist nicht gültig und kann nicht zur Prüfung der Identität dieser Website verwendet werden. Mehr Informationen Weiter Abbrechen					
	Click the "Next >" button. The following message is displayed.					
3.	Image: Search of the search of th	× \$3 *				
	Click the icon for updating the browser page (1). The following message is displayed.					

No.	Description				
4.	x Möchten Sie diese Anwendung ausführen?				
	Name: VncViewer				
	Anbieter: Siemens AG				
	Verzeichnis: http://172.16.34.220:5800				
1	Diese Anwendung wird mit uneingeschränktem Zugriff ausgeführt. Dies kann ein Risiko für Ihren Rechner und Ihre persönlichen Informationen darstellen. Führen Sie diese Anwendung nur aus, wenn Sie dem Speicherort und dem oben angegebenen Anbieter vertrauen.				
	Für Anwendungen dieses Anbieters und aus diesem Speicherort nicht mehr anzeigen				
	Mehr Informationen Ausführen Abbrechen				
	Click "Run". The window closes automatically and the web interface "VNC Authentication" of the Sm@rtClient display is called.				
5.	 Enable the option (1) to avoid having to confirm each time. 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. 				
	← ← ← ← https://172.16.34.210:5800/ P - ♥ Zertifikatfehler C ↑ ☆ ☺				
	Datei Bearbeiten Ansicht Favoriten Extras ?				
	Disconnect Options Clipboard Record Send Ctrl-Alt-Del Refresh				
	VNC Authentication				
	Thumbprint E8:7E:2D:09:14:66:8F:50:84:3C:74:C8:77:C4:00:1C:E3:D7:A6:DB				
	Password: V Secure OK				
	< >>				
6.	The following solution shows how to clear the certificate error.				
	Note The messages described above cannot be prevented.				

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.



No.	Description
1.	 Open the certificate In the address bar you click the certificate error (1). The "Untrusted Certificate" window opens. Open the certificate (2).
	Image: Contract of the server. Password: New recommend that you close this v View certificate errors
2.	<text></text>

1 Configuration Notes

No.	Description
3.	 Certificate Import Wizard Then click the "Next >" (1) button.
	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 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, dick Next.
	< Back Next > Cancel
4.	 Enable the radio button (1). Click the "Browse" button (2).
	Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can be certificate for the certificate. Automatically select the certificate store based the type of certificate Automatically select the following store Certificate store: Browse Browse Browse Browse Browse Browse Browse Bro
	Learn more about <u>certificate stores</u>
	< <u>Back</u> Next > Cancel



No.	Description
7.	Acknowledge the warning with "Yes" (1).
	Security Warning
	You are about to install a certificate from a certification authority (CA) claiming to represent: 172.16.34.220
	Windows cannot validate that the certificate is actually from "172.16.34.220". You should confirm its origin by contacting "172.16.34.220". The following number will assist you in this process:
	Numbprint (shal): E87E2D09 14668F50 843C74C8 77C4001C E3D7AbD8 Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
	Do you want to install this certificate?
	<u>Y</u> es <u>No</u>
8.	Acknowledge the message and the certificate window with "OK".
	Certificate
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
	Issued to: 172.16.34.220 Issued by: SmartServer bui Valid from 29.03.2018
	Learn more about <u>certificates</u>
	ОК

No.	Description			
9.	 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. 			
	C C C Eile Edit View Favorites Iools Help ?			
	Disconnect Options Clipboard Record Send Ctrl-Alt-Del Refresh VNC Authentication Thumbprint E8:7E:2D:09:14:66:8F:50:84:3C:74:C8:77:C4:00:1C:E3:D7:A6:DB Password: Secure OK			

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

Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]				
Console Root	Issued To	Issued By SmartServer built-in CA		Actions Certificates
Personal Personal Certification Authorities Certificates Intermediate Certification Authorities Intermediate Certification Authorities Intermediate Certification Authorities Intermediate Certificates Inturbed Certificates InterNet Certificates InterNet People Other People Certificate Enrollment Requests Smart Card Trusted Roots	ADJU14-2044 BINPP Root AAA Certificate Services AAA Certificate Services ABAA Certificate Services ABAA Certificate Services ABAA Certificate Services AABA Certificate Services AAC Raiz Certicámara S.A. AAC Raíz Certicámara S.A. AAC Raíz Certicámara S.A. AAC RAIZ DNIE AAC RAIZ DNIE AAC RAIZ FINMT-RCM AAC RAIZ FINMT-RCM	2014-2044 BNPP ROOT AAA Certificate Services AAA Certificate Services ABA.ECOM Root CA ABLE Root CA 1 AC Raiz Certicámara S.A. AC Raiz Certicámara S.A. AC RAIZ ONIE AC RAIZ DNIE AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM	-	More Actions 🕨