Provide root CA for TightGate-Viewer centrally under Windows

If user authentication at TightGate-Pro is carried out via an Active Directory, the security certificate from TightGate-Pro must be trusted when logging in for the first time. This is necessary so that TightGate-Viewer can establish an encrypted connection to the TightGate-Pro server.

If you want to avoid the question about trusting the login appearing at the first login, you can store the root CA certificate centrally in the Windows certificate store. The following instructions describe the procedure.

Export Root CA

- Please access TightGate-Pro as administrator *maint* and select the menu item User administration > Create SSL key menu item.
- Select an existing USER and open the dialogue SSL key was created or updated for USER XYZ with OK to confirm.
- 3. The following question **Should the created certificates now be exported?** with **Yes** to confirm.
- Now connect with an SFTP programme (e.g. WinSCP) to TightGate-Pro as user Administrator config. Under the directory /home/user/.transfer/config/certs/BENUTZER you will now find the file x509_ca.pem.
- 5. Copy this file to the Windows computer into whose certificate store it is to be imported.
- 6. Name the file x509_ca.pem to x509_ca.crt .

Import certificate file into the Windows certificate store

- Double-click on the file **x509_ca.crt** file.
- The certificate opens. Click on the button Install certificate...

💀 Zertifikat 🛛 🕹	
Allgemein Details Zertifizierungspfad	
Zertifikatsinformationen	
Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.	
Ausgestellt für: internet1.intern.netz	
Ausgestellt von: internet1.intern.netz	
Gültig ab 16.12.2019 bis 13.12.2039	
Zertifikat installieren Ausstellererklärung	
ОК	×509_ca

• The certificate import wizard opens. Select **Local computer** from the list.

Dieser Assistent hilft Ihnen beim Ko	ppieren von Zertifikaten, Zertifikatvertrauenslisten und
Zertifikatssperrlisten vom Datenträ	ger in den Zertifikatspeicher.
Ein von einer Zertifizierungsstelle a Es enthält Informationen für den D Netzwerkverbindungen. Ein Zertifik gespeichert werden.	usgestelltes Zertifikat dient der Identitätsbestätigung. atenschutz oder für den Aufbau sicherer atspeicher ist der Systembereich, in dem Zertifikate
Speicherort	
Aktueller Benutzer Aktueller Computer	
Klicken Sie auf "Weiter", um den Vo	rgang fortzusetzen.
·····,-···	

• Then select the preferred certificate store and then click Finish.

ind Systembereiche, in denen Zertifikate gespeichert werden. omatisch einen Zertifikatspeicher auswählen, oder Sie können einen Zertifikate angeben. icher automatisch auswählen (auf dem Zertifikattyp basierend) te in folgendem Speicher speichern iicher:
omatisch einen Zertifikatspeicher auswählen, oder Sie können einen Zertifikate angeben. icher automatisch auswählen (auf dem Zertifikattyp basierend) te in folgendem Speicher speichern iicher:
icher automatisch auswählen (auf dem Zertifikattyp basierend) te in folgendem Speicher speichern iicher:
te in folgendem Speicher speichern iicher:
icher:
Durchsuchen
Durusduen

• A message about the successful import should appear.

😽 Zertifikat	×
Allgemein Details Zertifizierungspfad	
Zertifikatsinformationen	
Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.	
Ausgestellt für: internet1.intern.netz	-
Ausgestellt von: internet1.intern.netz	Zertifikatimport-Assistent X
Gültig ab 16.12.2019 bis 13.12.2039	Der Importvorgang war erfolgreich.
Zertifikat installieren Ausstellererklärun	ок
OK	
	×509_ca

 Finally, delete the %APPDATA%\vnc directory. The SSO login with AD should work without the TLS confirmation message appearing. The file x509_savedcerts.pem file should not be created after closing TightGate-Viewer.

Removing the certificate file from the Windows certificate store

- Log in as **administrator** on the Windows PC.
- Right-click on the **Windows icon > Run**. Enter **mmc** and confirm with **OK**.



• The Microsoft Management Console opens. In the console, please click on File > Add/Remove Snap-In... click.



• In the following window, scroll down in the left-hand sub-window, select the snap-in **certificates** and then click on **Add** button.

Lokale Benutzer und Ordner Richtlinienergebnissatz Sicherheitskonfigura Sicherheitsvorlagen TPM-Verwaltung Windows Defender WMI-Steuerung	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor		Hinzufügen >	Nach oben Nach unten
Zertifikate	Microsoft Cor	~		Erweitert

• Another window opens in which **computer account** must be selected and then **Local computer**. Close the entry with **OK** to finalise.

at-Snap-In			×	ten Sna
es Snap-In verwaltet die Zertifikate für:				
genes Benutzerkonto				
- ienstkonto				
omputerkonto				
	< Zurück	Weiter >	Abbrechen	

• Then right-click on **Own certificates > Certificates** and select the menu item **Delete**.

\overline Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Computer)\Zwischenzertifizierungsstellen\Zertifikate] Ansicht Datei Aktion Favoriten Fenster ? 🔏 🖬 🗙 🗐 🔒 | 1 1 ? Konsolenstamm Ausgestellt für Ausgestellt von Ablaufdat 🗸 🗊 Zertifikate (Lokaler Computer) internet1.int 13.12.203 1.intern.netz 🚞 Eigene Zertifikate Öffnen 🗔 Microsoft V 31.12.200: ft Root Authority > 🚞 Vertrauenswürdige Stammzertifizieru 🖏 mydemo-W o-WIN-R3CQ0DM0LO3-CA 07.01.202! Alle Aufgaben > 📔 Organisationsvertrauen 🗔 Root Agenc 01.01.204 ency 🐱 🧮 Zwischenzertifizierungsstellen Ausschneiden 🔄 www.verisic Public Primary Certificatio... 25.10.2011 📔 Zertifikatssperrliste Kopieren 📋 Zertifikate Löschen > 2 Vertrauenswürdige Herausgeber > icht vertrauenswürdige Zertifikate Eigenschaften > 🚞 Drittanbieter-Stammzertifizierungsst > 📋 Vertrauenswürdige Personen Hilfe Clientauthentifizierungsaussteller 5 Stammelemente der Vorabversion 5 🦰 Stämme testen eSIM Certification Authorities 5 > I Homegroup Machine Certificates > iii Remotedesktop 📔 Zertifikatregistrierungsanforderunge Smartcard vertrauenswürdige Stämm > > 🚞 Autoritäten für die Installation vertra > 🧮 Vertrauenswürdige Geräte

- Do not forget! Finally, save the Microsoft Management Console session with File > Save / Save as ...
- Done, the TLS confirmation message should now be displayed again when starting TightGate-Pro.

From: https://help.m-privacy.de/ -

Permanent link: https://help.m-privacy.de/doku.php/en:faq:tightgate_pro_root_ca



Last update: 2024/01/28 19:41