Root-CA für TightGate-Viewer unter Windows zentral bereit stellen

Sofern die Benutzer-Authentifizierung beim TightGate-Pro über einen Active-Directoty erfolgt, so muss bei der ersten Anmeldung dem Sicherheitszertifikat von TightGate-Pro vertraut werden. Dies ist notwendig, damit der TightGate-Viewer eine verschlüsselte Verbindung zum TightGate-Pro Server aufbauen kann.

Möchte man vermeiden, dass die Frage zum Vertrauen der Anmeldung bei der ersten Anmeldung erscheint, so kann man das Root-CA-Zertifikat zentral im Windows Zertifikatsspeicher ablegen. Die nachfolgende Anleitung beschreibt die Vorgehensweise.

Root-CA exportieren

- Bitte am TightGate-Pro als Administrator *maint* anmelden den Menüpunkt Benutzerverwaltung > Erzeuge SSL-Schlüssel aufrufen.
- 2. Einen bestehenden BENUTZER auswählen und den Dialog **SSL-Schlüssel wurde erzeugt** oder aktualisiert für BENUTZER XYZ mit OK bestätigen.
- Die nachfolgende Frage Sollen die Erstellten Zertifikate nun exportiert werden? mit Ja bestätigen.
- Verbinden Sie sich jetzt mit einem SFTP-Program (z.B. WinSCP) mit dem TightGate-Pro als Benutzer Administrator *config*. Unter dem Verzeichnis /home/user/.transfer/config/certs/BENUTZER befindet sich nun die Datei x509 ca.pem.
- 5. Kopieren Sie diese Datei auf den Windows-Computer, in dessen Zertifikatsspeicher sie importiert werden soll.
- 6. Benennen Sie die Datei **x509_ca.pem** in **x509_ca.crt** um.

Zertifikatsdatei in den Windows-Zertifikatsspeicher importieren

- Einen Doppelklick auf die Datei x509_ca.crt ausführen.
- Es öffnet sich das Zertifikat. Klicken Sie auf die Schaltfläche Zertifikat installieren...

🙀 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	g
ОК	×509_ca

• Es öffnet sich der Assistent zum Zertifikatimport. Wählen Sie Lokaler Computer aus.

		×
🖅 🌆 Zertifikatimport-/	Assistent	
Willkomme	in	
Dieser Assistent h Zertifikatssperrlist	ilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und en vom Datenträger in den Zertifikatspeicher.	
Ein von einer Zerti Es enthält Informa Netzwerkverbindu gespeichert werda	fizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. ationen für den Datenschutz oder für den Aufbau sicherer Ingen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate en.	
Speicherort		
O Aktueller Be	nutzer	
Cokaler Com	puter	
Klicken Sie auf "W	eiter", um den Vorgang fortzusetzen.	
		nen

• Anschließend den bevorzugten Zertifikatsspeicher auswählen und anschließend auf Fertig stellen.

r tifikatspeicher Zertifikatspeicher si	ind Sustembereiche in d	lanan 7artifikata	acoeichert werden	
Zerünkatspeicher si	ind Systembereiche, in d	Jenen Zertinkate	gespeichert werden.	
Windows kann auto Speicherort für die 3	omatisch einen Zertifikat Zertifikate angeben.	speicher auswähl	en, oder Sie können eir	ien
Zertifikatspei	icher automatisch auswä	ählen (auf dem Ze	rtifikattyp basierend)	
🔿 Alle Zertifikat	e in folgendem Speiche	r speichern		
Zertifikatspe	icher:			
			Durchsuche	

• Es sollte eine Nachricht zum erfolgreichen Import erscheinen.

👼 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 Ausstellererklä	rung
	ок
	xonaTca

 Zum Schluss das Verzeichnis %APPDATA%\vnc löschen. Die SSO-Anmeldung mit AD sollte funktionieren, ohne dass die TLS-Bestätigungsmeldung erscheint. Die Datei x509_savedcerts.pem sollte nach dem Schließen des TightGate-Viewers nicht erstellt werden.

Entfernen der Zertifikatsdatei aus dem Windows-Zertifikatsspeicher

- Melden Sie sich als **Administrator** auf dem Windows-PC an.
- Rechtsklick auf das Windows-Symbol > Ausführen. Geben Sie mmc ein und bestätigen Sie mit OK.



• Die Microsoft Management Console öffnet sich. In der Konsole bitte auf Datei > Snap-In hinzufügen/entfernen... klicken.



• Im folgenden Fenster im linken Unterfenster runterscrollen, das Snap-In **Zertifikate** auswählen und anschließend auf **Hinzufügen** klicken.

erfügbare Snap-Ins:				Ausgewählte Snap-Ins:	
Snap-In IP-Sicherheitsrichtlin Komponentendienste Leistungsüberwachung Link auf Webadresse Lokale Benutzer und Ordner Richtlinienergebnissatz Sicherheitskonfigura Sicherheitsvorlagen TPM-Verwaltung Windows Defender	Anbieter Microsoft Cor Microsoft Cor	^	finzufügen >	Konsolenstamm	Erweiterungen bearbeiten Entfernen Nach oben Nach unten
WMI-Steuerung	Microsoft Cor Microsoft Cor	~			Erweitert

• Es öffnet sich ein weiteres Fenster, in dem **Computerkonto** auszuwählen ist und danach noch **Lokalen Computer**. Schließen Sie die Eingabe mit **OK** ab.

ertifikat-Snap-In		\times	
			ten Snaj
Dieses Snap-In verwaltet die Zertifikate für:			
O Eigenes Benutzerkonto			-
◯ Dienstkonto			
Computerkonto			

 Anschließend Rechtsklick auf Eigene Zertifikate > Zertifikate und Auswahl des Menüpunktes Löschen.

🕶 🐨 📶 🦂 🖼 🖱 🖼 🖙 🖬		<		1.00.000		
Konsolenstamm ===================================	Ausgestellt für		Ausgestellt von		Ablaufdat	
 Certifikate (Lokaler Computer) Eigene Zertifikate Vertrauenswürdige Stammzertifizieru Organisationsvertrauen Zwischenzertifizierungsstellen Zertifikatssperrliste Zertifikate Vertrauenswürdige Herausgeber Nicht vertrauenswürdige Zertifikate Drittanbieter-Stammzertifizierungsst Vertrauenswürdige Personen Clientauthentifizierungsaussteller Stämme testen Stämme testen EIM Certification Authorities 	internet1.in Microsoft V Microsoft V Root Agenc Vwww.verisic	Öffnen Alle Aufgaben Ausschneiden Kopieren Löschen Eigenschaften Hilfe	>	ft Root Authority o-WIN-R3CQ0DM0LO3-CA ency Public Primary Certificatio	13.12.200 31.12.200 07.01.202 01.01.204 25.10.201	
> I Homegroup Machine Certificates > I Remotedesktop						
Zertifikatregistrierungsanforderunge						
 Smartcard vertrauenswürdige Stämn Autoritäten für die Installation vertra Vertrauenswürdige Geräte 						

- Nicht vergessen! Zum Schluss die Microsoft Management Console-Session speichern mit Datei > Speichern / Speichern unter ...
- Fertig, nun sollte die TLS-Bestätigungsmeldung beim Starten von TightGate-Pro wieder angezeigt werden.

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

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



Last update: 2021/04/01 10:47