Epikur TIaaS Installation

Mit Installation einer „LOOMA“-Firewall

Handbuch für DVO

Version 1.3
Stand: 16.02.2024

Inhaltsverzeichnis

Weitere hilfreiche/benötigte Anleitungen

- Kurzanleitung Update Kartenterminals via Konnektor
  https://www.epikur.de/files/anleitungen/Kurzanleitung_Update_Kartenterminals_via_Konnektor.pdf
- Kurzanleitung Update Kartenterminals via USB-Stick
  https://www.epikur.de/files/anleitungen/Kurzanleitung_Update_Kartenterminals_via_USB-Stick.pdf
- Remote Installation (ohne Bridge-Mode / mit Switch)
  https://youtu.be/GgMgLzwFnK8
- Remote Installation (mit Bridge-Mode / ohne Switch)
  https://youtu.be/aBmeAWAgbkQ
- Checkliste für Kunde: TIaaS
  https://www.epikur.de/media/Checkliste-TIaaS.pdf
- Checkliste für Kunde: UTM
  https://www.epikur.de/media/Checkliste-HWFW-Installation.pdf

Abkürzungsverzeichnis

AP	WLAN-Access-Point (LW 500)
KIMaaS	KIM as a Service
KT	Kartenterminal
TIC	TIaaS-Client
UTM	Unified Threat Management (Firewall) (UF60)

Änderungsverzeichnis

1.3 13.02.2024

- Entfernung: Bilder und Hinweise zum Bridge-Mode
- Neu: Kurzleitfaden L.1 Kurzleitfaden: Umstellung TIaaS auf TIaaS mit LOOMA-Firewall
- Änderung der Installationsart vom TIC von Standardinstallation auf Installation als Dienst Installationsart wählen
- Änderung des Zielverzeichnisses für Zertifikate im Abschnitt Windows
- Erweiterung von Abschnitt Bestimmung Hauptrechner/Ermittlung TIC-MAC-Adresse um weitere Möglichkeiten
- Neu: Abschnitt A.5 DNS-Server ändern
- Anpassung der Bilder in Abschnitt TIC-Installation

1.2 12.12.2023

- Ergänzung: Übermittlung Port von Wireguard-VPN-Server an LOOMA Ermittlung Wireguard-Daten

1.1 01.12.2023

- Notwendige EPIKUR Version von 23.4.1.2 auf 23.4.1.3 geändert
- Änderung des Installationsablauf (Anschluss Computer weiter nach hinten verschoben)
- Ergänzung einer Erklärung im Abschnitt Anpassungen Netzwerk-Einstellungen im Konnektor
- Ergänzung Abschnitt De-Registrierung des Konnektors beim VPN-Zugangsdienst
- Überarbeitung Abschnitt Update und Einrichtung der Firewall und des APs
- Konkretisierung Abschnitt Aufrufkontext einrichten
- Neu: Abschnitt A.5 DNS-Server ändern
- Mögliche Auswirkungen
- DNS-Adressen lassen sich nicht auflösen.
- TIC sagt, dass keine Verbindung zum vKonnektor hergestellt werden kann.

Lösung
Setzen des DNS-Servers auf 8.8.8.8

Bei einer FritzBox ist dieses unter "Internet -> Zugangsdaten -> DNS Server" möglich.
Bei einem SpeedPort kann es teilweise über die Zugangsdaten eingestellt werden.

Sollte die Einstellung nicht direkt im Router vorgenommen werden können, so kann

der DNS-Server in den Netzwerkeinstellungen vom Betriebssystem gesetzt werden. Diese Anpassung ist dann allerdings auf allen Clientsystemen notwendig, die sich mit dem Rechenzentrumskonnektor verbinden möchten.

A.6 Neustart TIC

- **Unter MacOS**
- Neu: Abschnitt A.7 Einrichtung des Festplattenvollzugriffs für EPIKUR unter MacOS
- Erweiterung Abkürzungsverzeichnis

1.0 17.11.2023

- Initiale Version

Vorwort

Die vorliegende Anleitung richtet sich ausschließlich an Techniker, die speziell für die Anbindung von Praxen an die Telematikinfrastruktur geschulte wurden. Sie ersetzt nicht die Lektüre der gerätespezifischen Dokumentationen.
Von einer Einrichtung oder Änderung der gesetzten Parameter durch nicht geschulte Benutzer wird dringend abgeraten. Bitte beachten Sie, dass nach unsachgemäßer Einrichtung oder Veränderung der Parameter ein Support im Rahmen des Pakets ‚Betrieb & Wartung' durch EPIKUR nicht gewährleistet werden kann. Dies gilt auch im Fall einer Selbstinstallation.

Wichtige Kontaktdaten

Epikur	Tel. +49 30 340 601 100	E-Mail: info@epikur.de
Epikur Vertrieb	Tel. +49 30 340 601 101	E-Mail: vertrieb@epikur.de
Epikur Anwendungsberatung	Tel. +49 30 340 601 122	E-Mail: support@epikur.de
Epikur Technischer Support	Tel. +49 30 340 601 123	E-Mail: support@epikur.de
LOOMA	Tel. +49 391 50 54 6080	E-Mail: support@looma-it.de

Epikur DVO-Hotline	**Tel. +49 30 644 924 730**

1 Vorbereitung

1.1 Vorbereitung durch Epikur

- Versand Firewall und AP durch DVO (SAG)
- Bereitstellung Schulungsvideo
- Bereitstellung Checkliste
- EPIKUR Version > 23.4.1.3 für den Kunden freigeben

1.2 Vorbereitung durch Kunden

- Sind genug Steckdosen vorhanden?
    - 1x für Firewall
    - 1x für WLAN-Access-Point
    - 1x für einen Switch
- EPIKUR auf eine Version > 23.4.1.3 updaten
- Selbststudium des Kundenvideos
- Auspacken der Firewall und des WLAN-Access-Points
- Passwort des Routers
- Sudo/Admin-Passwort vom PC bereithalten
- Admin-PIN vom Kartenterminal bereithalten
- Kartenterminal Updaten (Version: min. 3.8.2)
- Ggf. Passwort vom Secunet-Konnektor bereithalten

2 Ablauf der Installation

3 Kunden aufklären und Daten einholen

1. Soll in diesem Termin eine neue gSMC-KT und/oder SMC-B getauscht werden?
   → Wenn ja, vor Umzug Katenmaterial tauschen und danach mit RZK pairen.
2. Welche Geräte sind im Netzwerk?
   ➔ Dokumentieren, da hier später die Zertifikate für die SSL-Inspection hinterlegt werden müssen.
3. Update auf EPIKUR min. Version: 23.4.1.3 durchgeführt?
   ➔ Falls nicht, bitte durchführen.
4. Via TeamViewer auf das Endgerät des Kunden schalten und LOOMA hinzuholen.

3.1 Ermittlung/Update Kartenterminal-Version

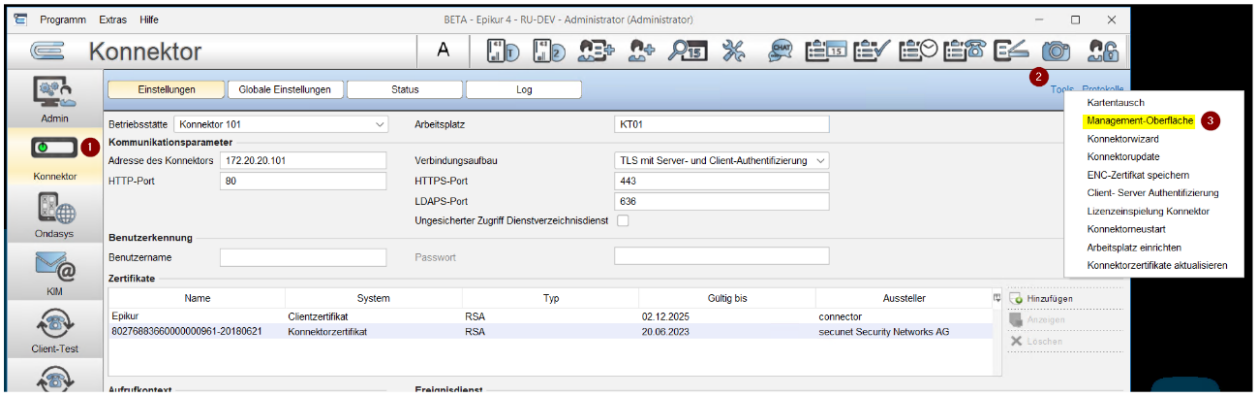
Sie überprüfen die Version Ihres ORGA 6141 online direkt am Display des Kartenterminals über: Menü > Service (3) > Status (2) > Firmware Version. Die neue Version 3.8.2 ist seit Ende Juni 2022 verfügbar und muss zwingend installiert sein. Die Installation ist über folgende Wege möglich:

- Update über den secunet Konnektor (siehe separate Kurzanleitung)
- Update über USB-Stick (siehe separate Kurzanleitung)

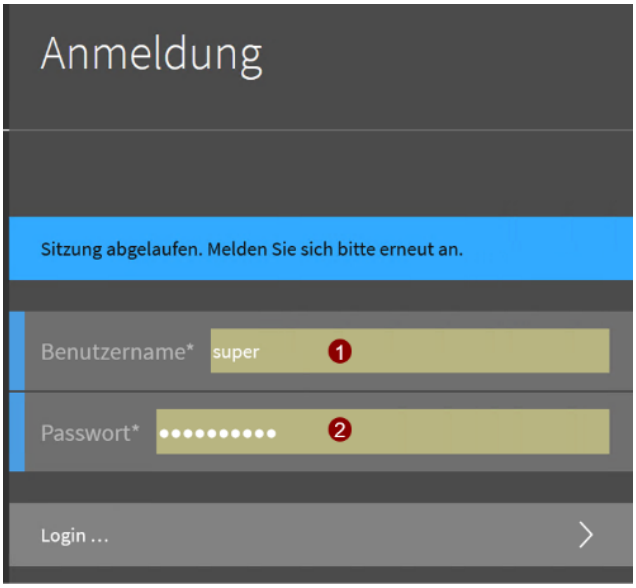
3.2 Dokumentation Aufrufkontext Konnektor

Dieser Schritt ist nur notwendig, wenn ein Umzug von Secunet auf TIaaS stattfindet.

- Login im Konnektor
  - Aufruf via URL (https://<*ipDesKonnektors*>:8500/management)
  - oder via EPIKUR
    - Konnektor-Einstellungen öffnen (1)
    - Auf Tools klicken (2)
    - Auf Management-Oberfläche klicken (3)

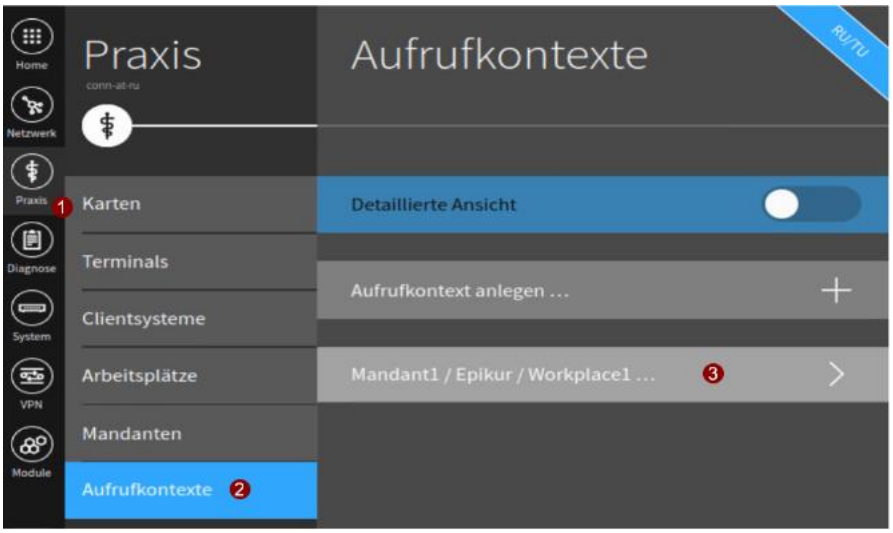


- Nutzer ist üblicherweise “super” (1)
- Passwort-Eingabe durch Kunden (2)

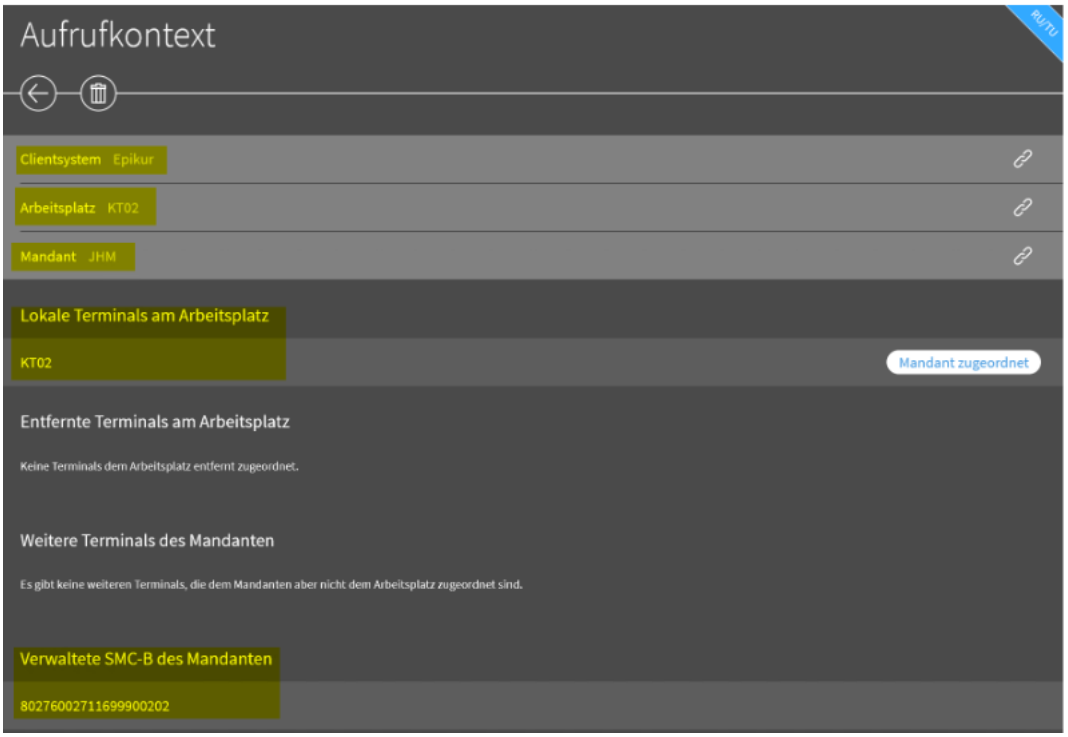


3.2.1 Dokumentation Aufrufkontext

- Klick auf Praxis (1)
- Klick auf Aufrufkontexte (2)
- Aufrufkontext auswählen (3)

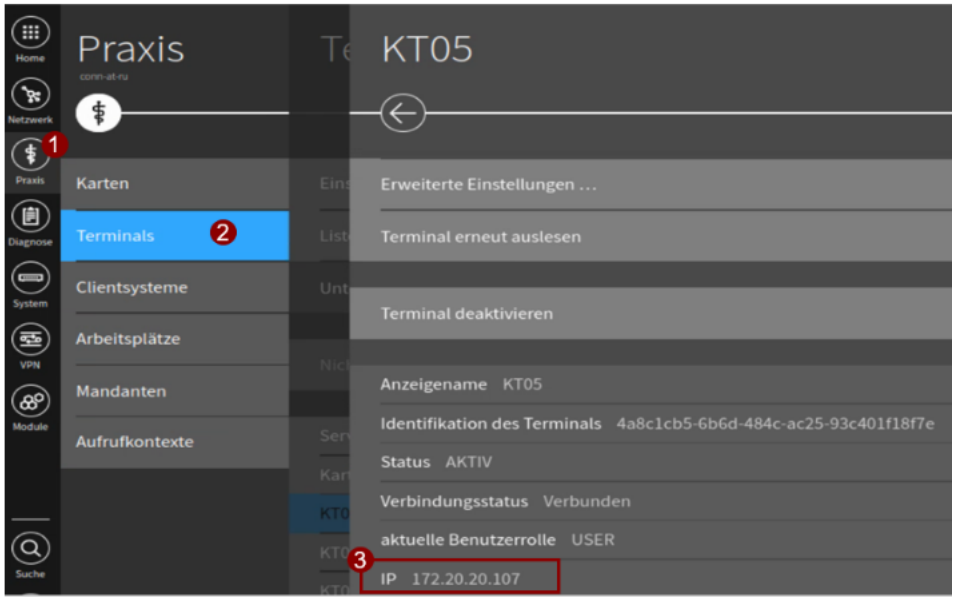


- Aufrufkontexte notieren - Screenshot von der Übersicht und Detail-Seiten machen und für später abspeichern
    - Diese werden später für die Konfiguration des TICs benötigt. **Hintergrund: Der alte „Secunet“-Aufrufkontext soll auch bei TIaaS beibehalten werden!**



- Klick auf Praxis
- Klick auf Terminals

- Zugeordnete Terminals jeweils auswählen und IP notieren - Screenshot von KTs machen und für später abspeichern.



3.3 Firewall-Einrichtungsdaten an LOOMA übergeben

LOOMA erhält mit der Terminbuchung bereits einige Daten über den Kunden.
Zusätzlich werden noch einige nun zu ermittelnde Daten benötigt.
Diese Daten müssen noch übergeben werden:

- Seriennummer von Firewall (Modell UF60) (siehe Abschnitt Ermittlung Seriennummern und Cloud-PINs)
- Cloud-PIN von Firewall (siehe Abschnitt Ermittlung Seriennummern und Cloud-PINs)

- TIC-MAC (siehe Abschnitt Bestimmung Hauptrechner/Ermittlung TIC-MAC-Adresse)
- Wireguard-Interface-IP (siehe Abschnitt Ermittlung Wireguard-Daten)
- WireGuard-Private-Key (siehe Abschnitt Ermittlung Wireguard-Daten)

- Seriennummer vom AP (Modell LW500) (siehe Abschnitt Ermittlung Seriennummern und Cloud-PINs)
- Cloud-PIN vom AP (siehe Abschnitt Ermittlung Seriennummern und Cloud-PINs)

3.4 Ermittlung Seriennummern und Cloud-PINs

Die Seriennummer und Cloud PINs sind an den Kunden zusammen mit der Hardware gesendet worden.

- Die Seriennummer steht auf der Rückseite des Gerätes
- Die Cloud PIN steht auf dem beiliegenden Beipackzettel/Handbuch

Diese Daten müssen an LOOMA übermittelt werden.

=> Nach der Übermittlung der Daten legt LOOMA die Firewall und den AP in der Cloud an.

3.5 Bestimmung Hauptrechner/Ermittlung TIC-MAC-Adresse

Für die Einrichtung ist die Bestimmung eines „Hauptrechners“ notwendig. Auf diesem wird später der TIC installiert.

Bei einer Client-Server-Umgebung ist der TIC bevorzugt auf dem Server-Rechner zu installieren.

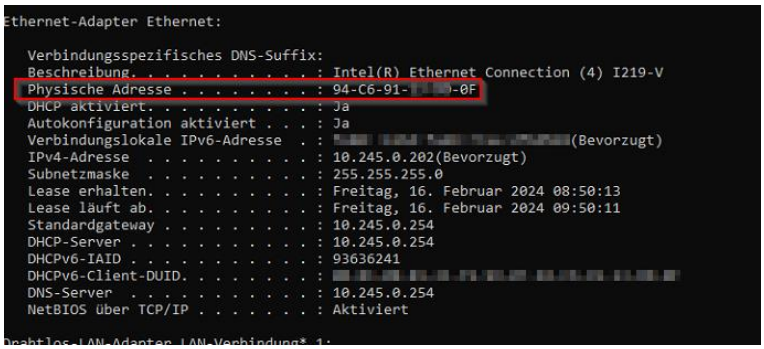
Über diesen Hauptrechner laufen die Verbindungen des Kartenterminals in das Rechenzentrum sowie die Weiterleitung der Konnektor-Ereignisse an die Clientsysteme. Der Rechner muss im Praxisbetrieb also immer eingeschaltet sein.

Im Folgenden werden verschiedene Wege erklärt, die MAC-Adresse zu ermitteln.

Sind mehrere Adressen aufgeführt, besitzt der Computer mehrere Netzwerk-Interfaces (WLAN, LAN, etc.). Hier muss in Abstimmung mit dem Kunden entschieden werden, welches Interface für die Einrichtung von TIaaS sinnvoll ist.
Ist der Computer immer via LAN angeschlossen, sollte hier LAN bevorzugt gewählt werden.

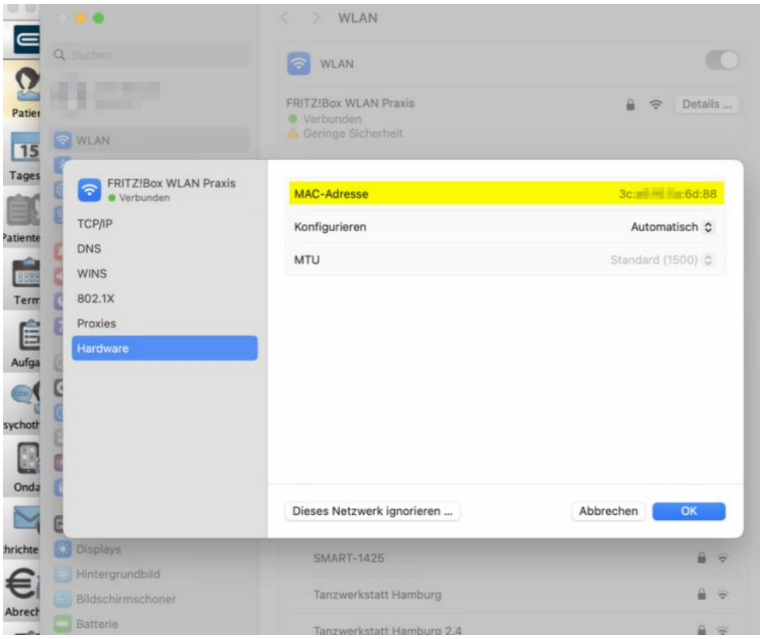
3.5.1 Möglichkeit 1 - Via Terminal (Windows)

Über den Befehl „*ipconfig /all*“ in der Eingabeaufforderung kann sich eine Liste der Netzwerkinterfaces ausgeben werden.
In der Zeile „Physikalische Adresse“ ist jeweils die MAC-Adresse zu finden.



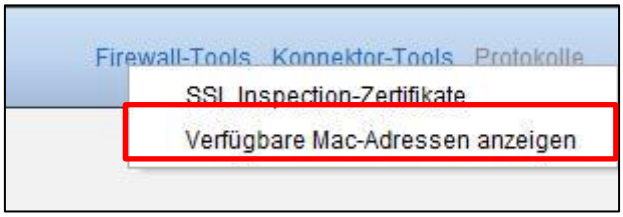
3.5.2 Via Einstellungen (MacOS)

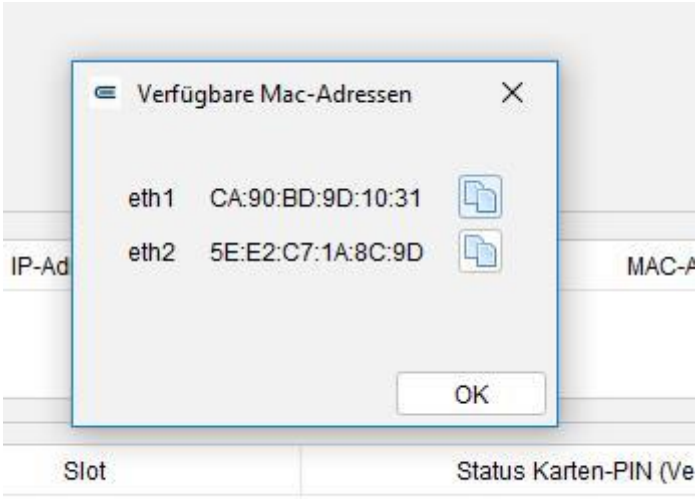
- Die Systemeinstellungen öffnen
- Zu „Netzwerk“ oder „WLAN“ navigieren
- Netzwerkverbindung auswählen
- „Details …“ klicken
- In Ansicht „Hardware“ wechseln
- MAC-Adresse kopieren



3.5.3 Via EPIKUR

In EPIKUR können (als Administrator angemeldet) in der Ansicht „Konnektor“ unter dem Punkt Firewall-Tools die verfügbaren MAC-Adressen angezeigt werden.

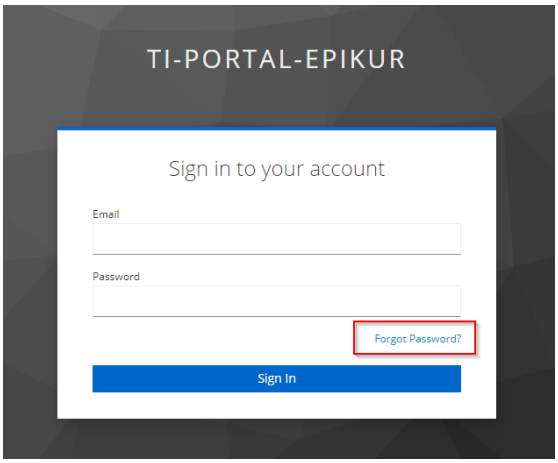




3.6 Ermittlung Wireguard-Daten

Dem Kunden wurde vor der Installation eine E-Mail inkl. eines Downloadlinks für das Installationspaket zugesendet. Das Installationspaket wurde entweder von Kunden bereits heruntergeladen oder kann unter https://epikur.ti-portal.de heruntergeladen werden. Hierfür besteht der Benutzername aus der E-Mail-Adresse des Kunden, welche bei der Bestellung vergeben wurde. Das Passwort zum TI-Portal, sollte dem Kunden vorliegen.

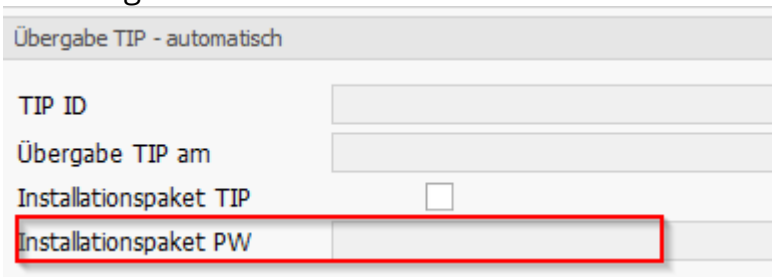
Hinweis: Sollte der Kunde keine E-Mail hierzu erhalten haben, oder sich nicht mehr an das TI-Portal Passwort erinnern, kann die „Passwort Zurücksetzen“ Funktionalität hierfür genutzt werden.



Nach erfolgreichem Herunterladen bzw. Bereitstellung durch den Kunden muss diese Zip-Datei mit dem dazugehörigen Passwort entpackt werden.

Hinweis: Dieses Passwort liegt dem Kunden nicht vor.

1. Externer DVO
   - Das Passwort liegt Ihnen mit Ihrem Auftrag vor.
2. Interner DVO
   - Das Passwort befindet sich:
     - für Rolloutaufträge unter: https://vault.intra.epikur.de/
     - TI-Portalaufträge: in der Cobra-Bestellmaske unter:
     -

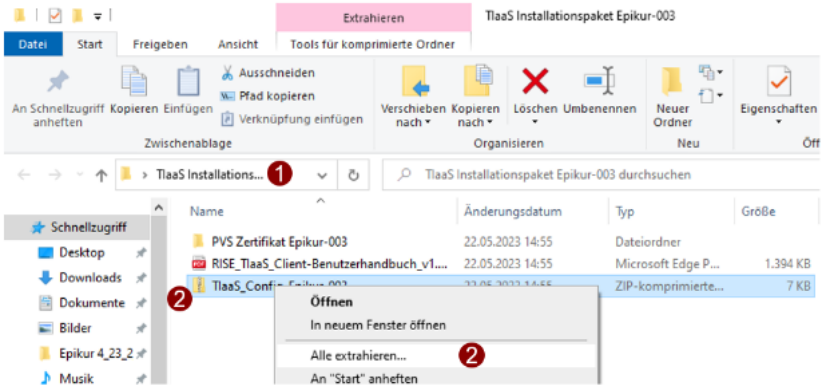


2.1 Installationspaket Bereitstellung Rolloutaufträge

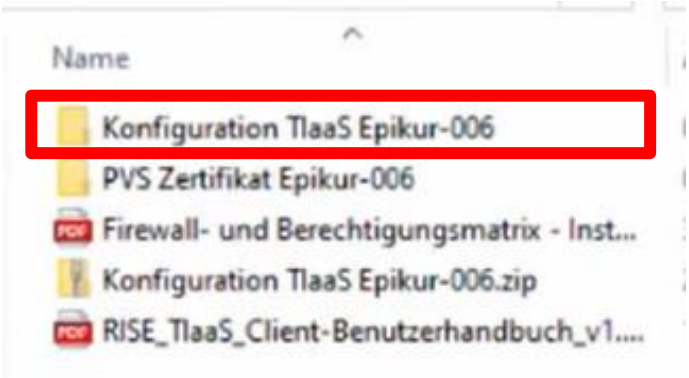
- Installationspaket (“TIC-Installationspaket_Epikur-XXXX.zip”) auf dem Netzlaufwerk unter “Y:\Produkte\PdM_Projekte\Rechenzentrumskonnektor\80_Kunden\RISE-Zugänge\<kundennummer>” raussuchen.
- Passwort für Installations-/ und Konfigurationspaket aus dem Password-Tresor raussuchen.
- Bei Einzelplatz und Server ZIP-Datei “TIC-Installationspaket_Epikur-XXXX.zip” via TeamViewer auf Desktop des Kunden-PCs verschieben.

- Beim Client ZIP-Datei “Zusaetzliche Wireguard Epikur-XXXX.zip” via TeamViewer auf Desktop des Kunden- PCs verschieben.
- ZIP-Dateien “TIC-Installationspaket_Epikur-XXXX.zip” und “Zusaetzliche Wireguard Epikur-XXXX.zip” in den Ordern ./<benutzer>/Epikur4 oder ./<benutzer>/EpikurClient verschieben.
    - Dieser Schritt dient dazu, das Konfigurationspaket in der “Obhut” des Kunden zu belassen und einen späteren Zugriff darauf zu ermöglichen.
- ZIP-Datei “TIC-Installationspaket_Epikur-XXXX.zip” und “Zusaetzliche Wireguard Epikur-XXXX.zip” entpacken (Passwort/Bereitstellungscode für den Kunden notwendig).

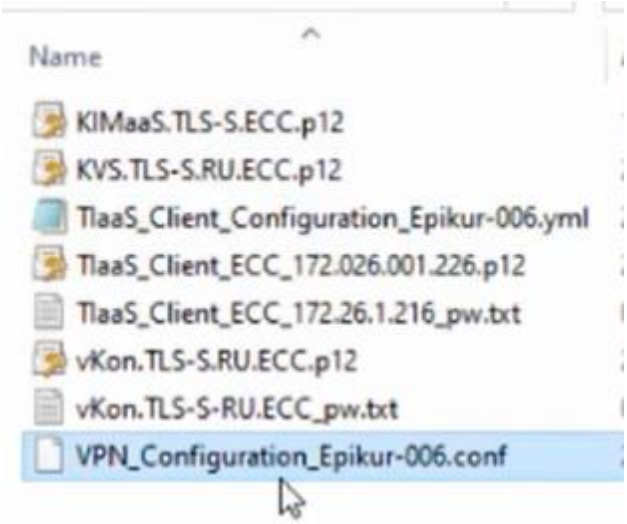
- Entpackter Ordner “TIC-Installationspaket_Epikur-XXXX.zip” öffnen.
- ZIP-Datei „TIaaS_Config_Epikur-XXXX.zip“ aus dem Ordner “TIC-Installationspaket_Epikur-XXXX.zip” entpacken (erneut dasselbe Passwort/ Bereitstellungscode für den Kunden notwendig – wie im vorherigen Schritt).
    - Original ZIP-Datei beibehalten! Diese wird später bei der Installation des TICs benötigt.



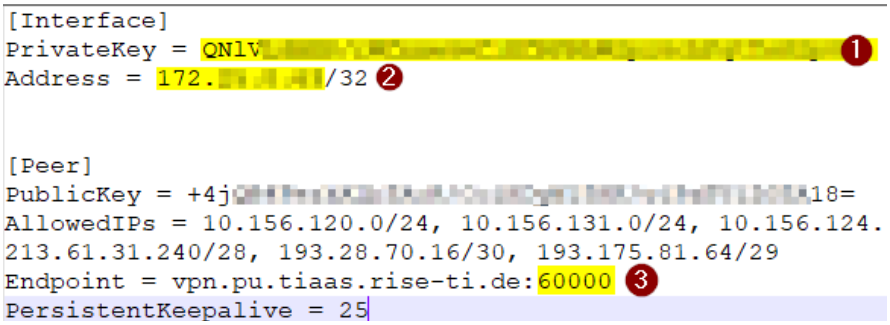
In Extrahierten Ordner befinden sich mehrere Dateien.



Im Ordner „Konfiguration TIaaS Epikur“ befinden sich die benötigten Dateien.



- Datei VPN_Configuaration_XXXXX.conf öffnen
  - Nach dem Öffnen sind der Private Key sowie die IP-Adresse sichtbar.



- Folgende Daten müssen an LOOMA weitergegeben werden
  - Private Key (Zeile 2)
  - IP-Adresse (Zeile 3)
    Bitte beachten: Nur die IP-Adresse ohne Subnetzmaske.

- Port vom VPN-Endpunkt (Zeile 9)
  Eine Zahl im Bereich von 60000 und 60100

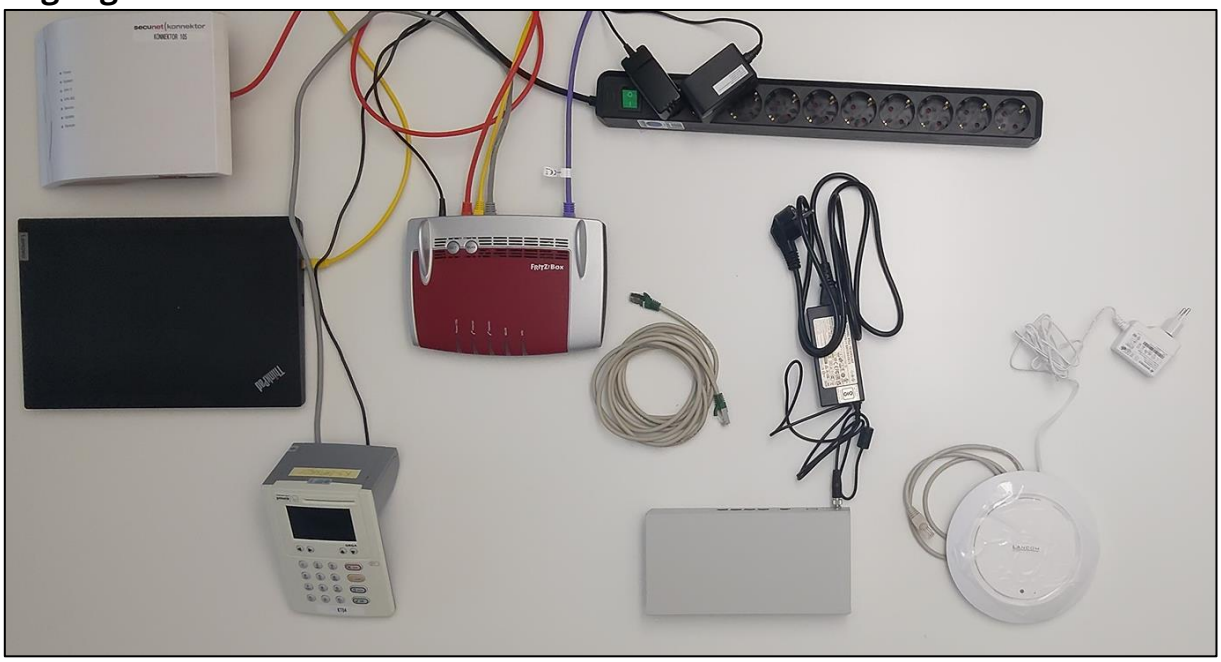
Möglicher Fehlerfall: Passwort für die Zip-Datei liegt nicht vor.
Wenn das Passwort nicht vorliegt, besteht die Möglichkeit, dieses im TI-Portal abzurufen.

Sollte es sich um einen Rolloutauftrag handeln, so wurde Ihnen das Passwort via Textdatei mit dem Auftrag übermittelt. Sollte dies nicht der Fall sein, nehmen Sie bitte Kontakt mit Ihrem Auftraggeber auf, sodass das Anliegen weitererfolgt werden kann. Die entsprechenden Kontaktmöglichkeiten entnehmen Sie bitte der Anleitung Andernfalls sollte das Passwort wie in 3.6.1 und 3.6.2 beschrieben zur Verfügung gestellt worden sein.

4 Hardware Firewall einrichten

Siehe oben: Link zum Video

Ausgangssituation



4.1 Anschluss der Firewall

- LAN-Kabel der Firewall in ETH 0 Port der Firewall stecken.
- Anderes Ende in freien Port des Routers stecken.

    - Sollte kein Port im Router frei sein, so kann z. B. das Kartenterminal abgesteckt werden.
    - Zum besseren „Monitoren“ sollte der Computer, auf dem der TeamViewer läuft, weiter mit dem Router verbunden bleiben.
- Netzteil der Firewall in Steckdose stecken.

4.2 Anschluss des WLAN-Access-Points

- LAN-Kabel am AP in LAN 1 (PoE) Port stecken.
- Anderes Ende in freien Port des Switches stecken.
- Netzteil des AP in Steckdose stecken.

4.3 Update und Einrichtung der Firewall und des APs

4.3.1 Für SAG-Techniker

- Anruf bei LOOMA
- Übergabe der Txt-Datei mit allen erhobenen Daten

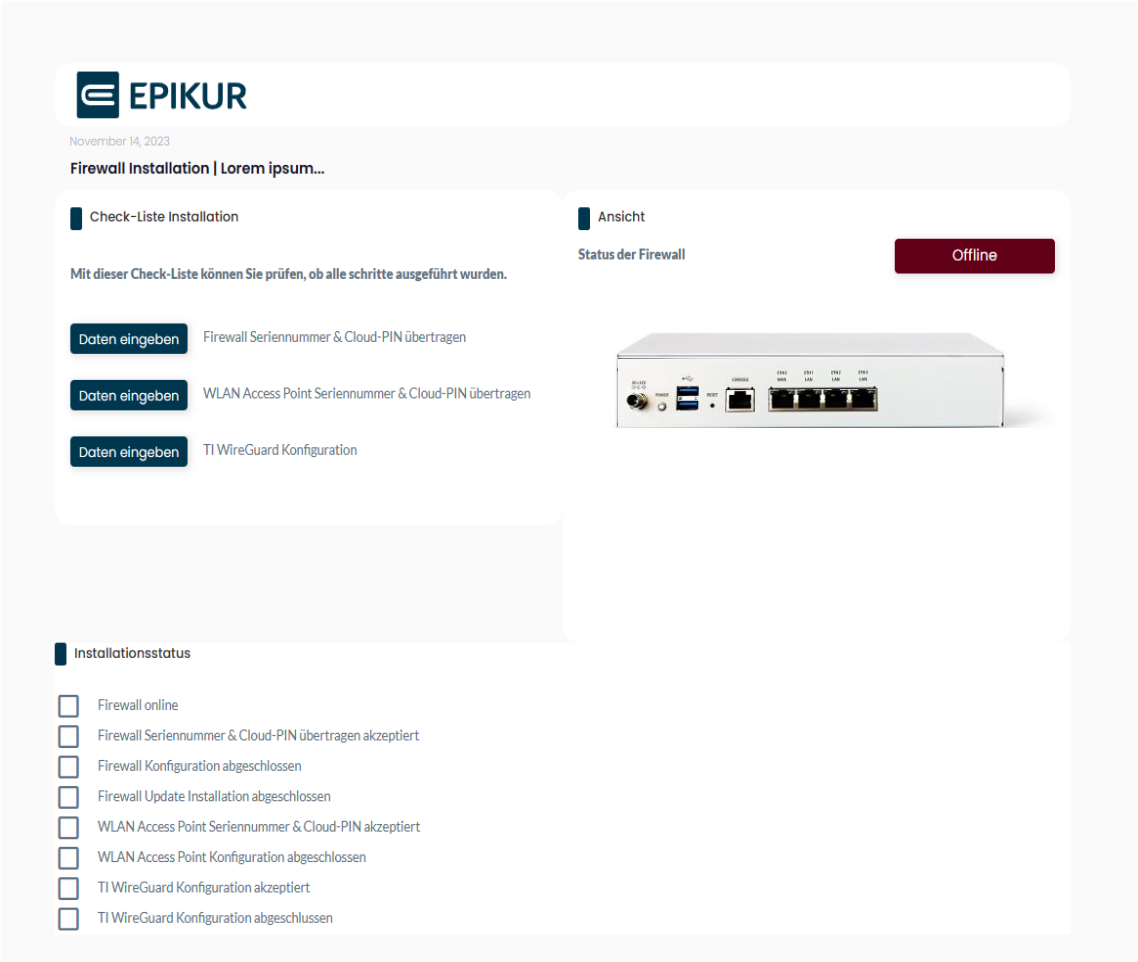
Im Anschluss startet der LOOMA-Techniker direkt mit dem Update der Firewall und dem Ausrollen der Konfiguration.

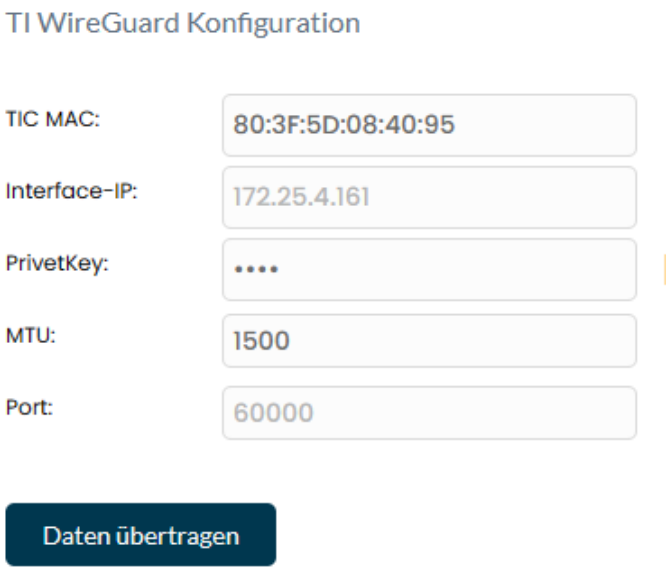
Sobald dieser Prozess abgeschlossen ist, meldet sich der LOOMA-Techniker über einen Rückruf zurück.

Während des Update- und Rollout-Prozesses kann mit den Schritten bis zum Abschnitt Anschluss Computer fortgefahren werde

4.3.2 Für Epikur-Techniker

- Aufruf des LOOMA-Onboarding-Portals (https://lmc.looma.online)
- LOOMA-Termin anlegen
    - Auftragsnummer beginnend mit EPITEC_ und Kundennummer
- Firewall-Daten eingeben und bestätigen
- AP-Daten eingeben und bestätigen
- WLAN-Konfiguration eingeben und bestätigen
    - SSID = Praxis-*BSNR*
    - Das WLAN-Passwort ist vom Kunden zu wählen oder an diesen zu übergeben.
- WireGuard-Daten eingeben und bestätigen





Am gebuchten Termin startet der LOOMA-Techniker mit dem Update und der Konfiguration. Der Fortschritt ist auf der Onboardings-Seite live einsehbar.

4.4 Anpassungen Netzwerk-Einstellungen im Konnektor

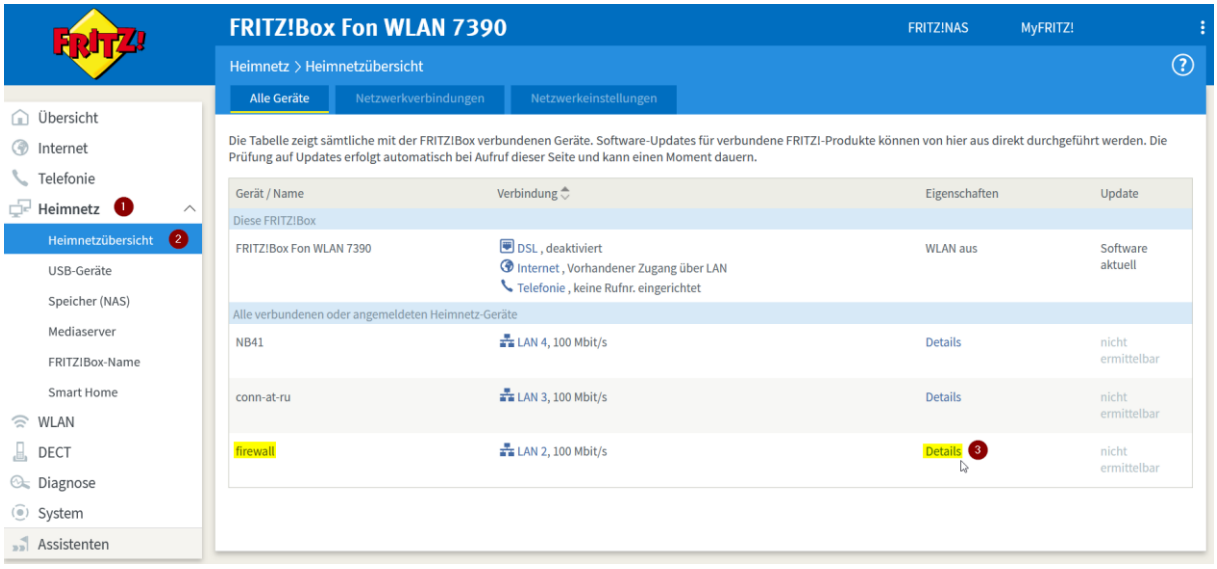
Dieser Schritt ist nur notwendig, wenn ein Umzug von Secunet auf TIaaS stattfindet.

Die folgende Anpassung ist notwendig, damit später aus dem Firewall-Netz ein Zugriff auf den Konnektor erfolgen kann, ohne dass der Konnektor von dem Router an die Firewall angeschlossen werden muss.

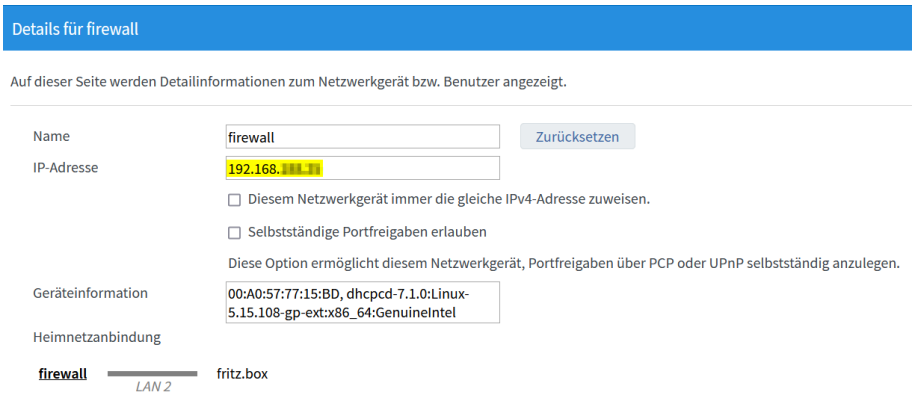
4.4.1 Ermittlung IP-Adresse der Firewall im Router-Subnetz

Hier am Beispiel einer Fritz!Box

- Login auf dem Router
- Navigation via „Heimnetz“ (1) -> „Heimnetzübersicht“ (2) zu den Netzwerkgeräten
- Details (3)



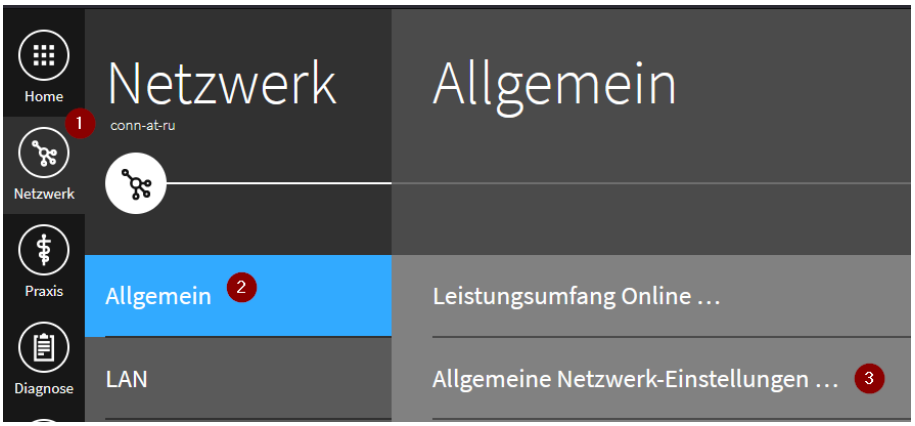
- IP-Adresse ermitteln



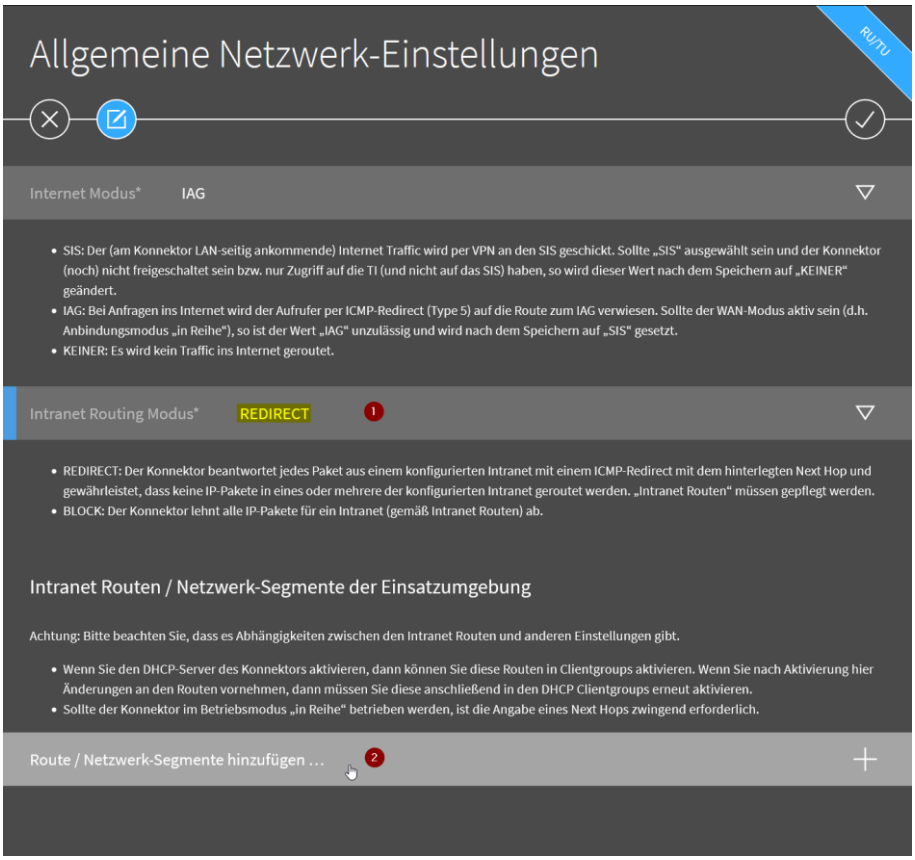
4.4.2 Anpassung der Netzwerk-Einstellungen Konnektor

- Login im Konnektor

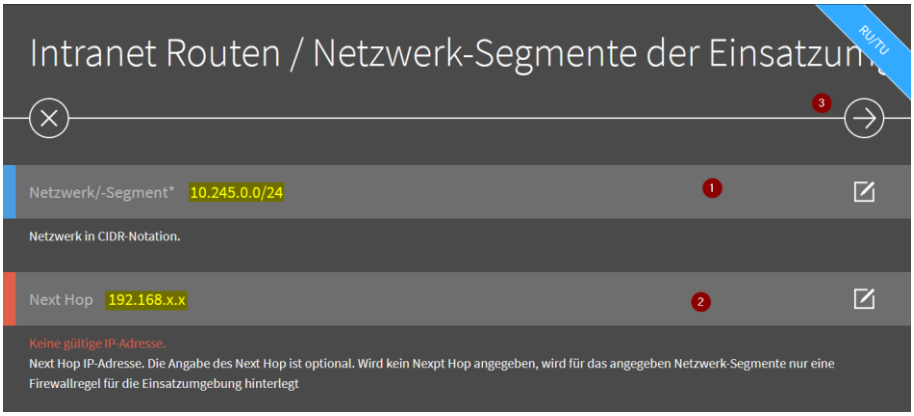
- Klick auf „Netzwerk“ (1)
- Klick auf „Allgemein“ (2)
- Klick auf „Allgemeine Netzwerk-Einstellungen“ (3)



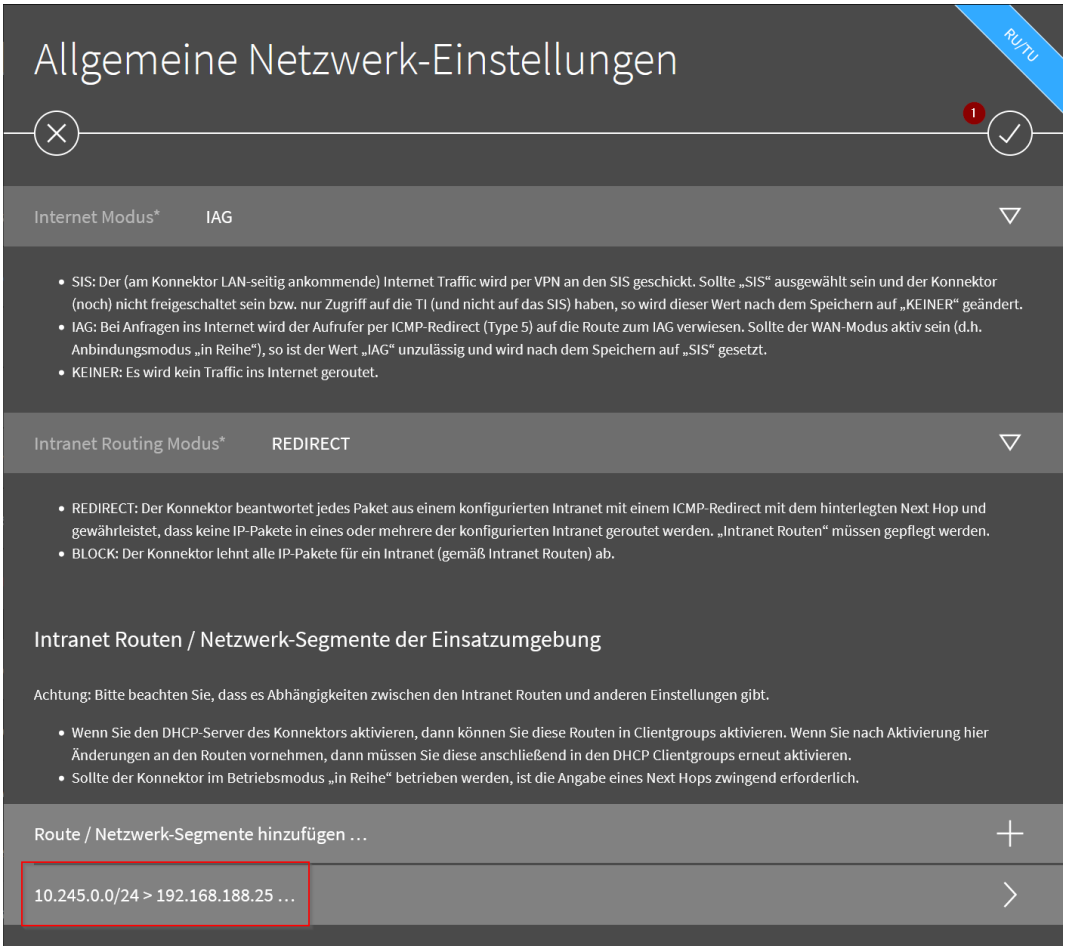
- „Internet Routing Modus“ auf „REDIRECT“ stellen (1)
- „Route / Netzwerk-Segmente hinzufügen…“ klicken (2)



- „Netzwerk/-Segment“ auf 10.245.0.0/24 setzen (1)
- „Next Hop“ auf die IP-Adresse der Firewall setzen, welche im vorherigen Schritt ermittelt wurde (2)
- Pfeil „->“ klicken (3)



- Die Einstellungen über den „Haken“ (1) übernehmen



4.4.3 De-Registrierung des Konnektors beim VPN-Zugangsdienst

- Klick auf „VPN“ (1)
- Klick auf „VPN-Zugangsdienst“ (2)
- Contract ID kopieren und abspeichern (um ggf. bei Abbruch des Termins eine erneute Registrierung des Konnektors vorzunehmen) (3)
- Klick auf „Konnektorfreischaltung zurücknehmen“ (3)

- Hinweis bestätigen
- Ggf. andere SMC-B und Mandanten auswählen
- Weiter

- Hinweis bestätigen

4.5 Anschluss Kartenterminal

4.5.1 Orga 6461

- LAN-Kabel des KTs am Router abziehen

- In freien Port des Switches stecken

DHCP-Deaktivieren

Einstellungen (2) –> LAN Parameter (2) –> DHCP (2) –> Ein/Aus (1) -> „Aus“

Eingabe mit OK bestätigen.

IP-Adresse vergeben

Einstellungen (2) –> LAN Parameter (2) –> IP Adresse (3)

010.245.000.[210-240]

Eingabe mit OK bestätigen.

Subnetzmaske setzen

Einstellungen (2) –> LAN Parameter (2) –> Subnet Mask (4)

255.255.255.0

Eingabe mit OK bestätigen.

Gateway setzen

Einstellungen (2) –> LAN Parameter (2) –> Gateway/DNS (5) –> Gateway (1)

010.245.000.254

Eingabe mit OK bestätigen.

DNS setzen

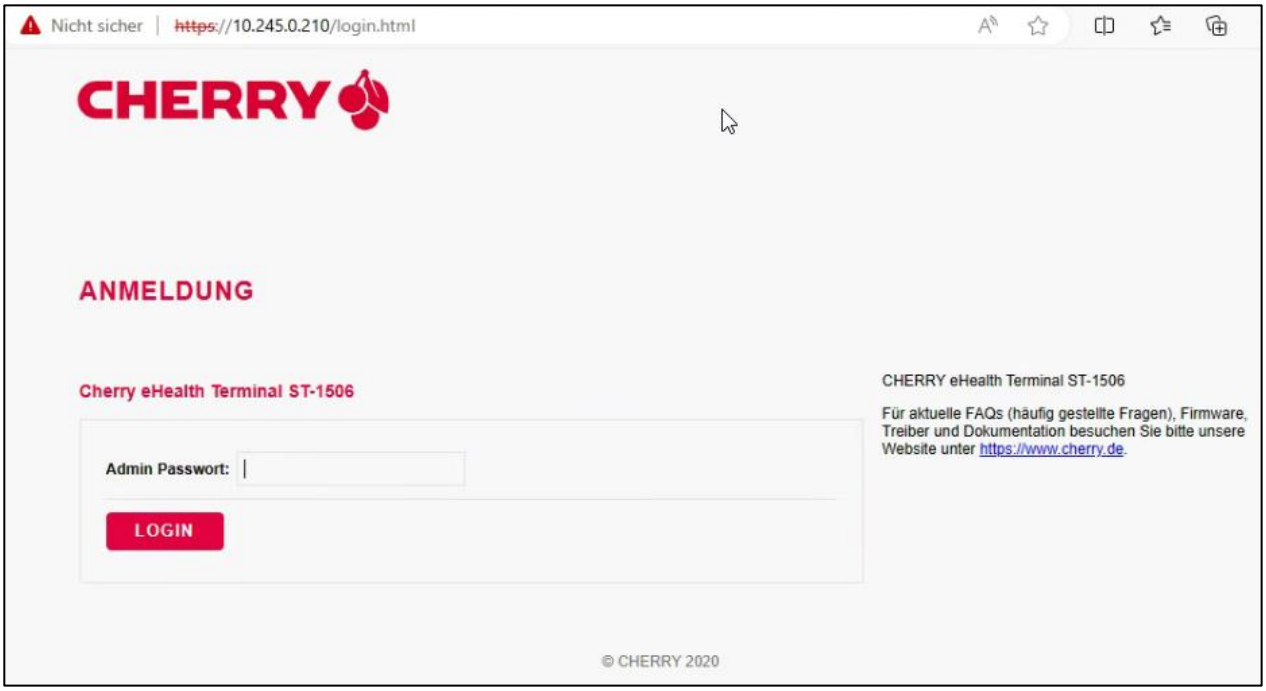
Einstellungen (2) –> LAN Parameter (2) –> Gateway/DNS (5) –> DNS (2)

010.245.000.254

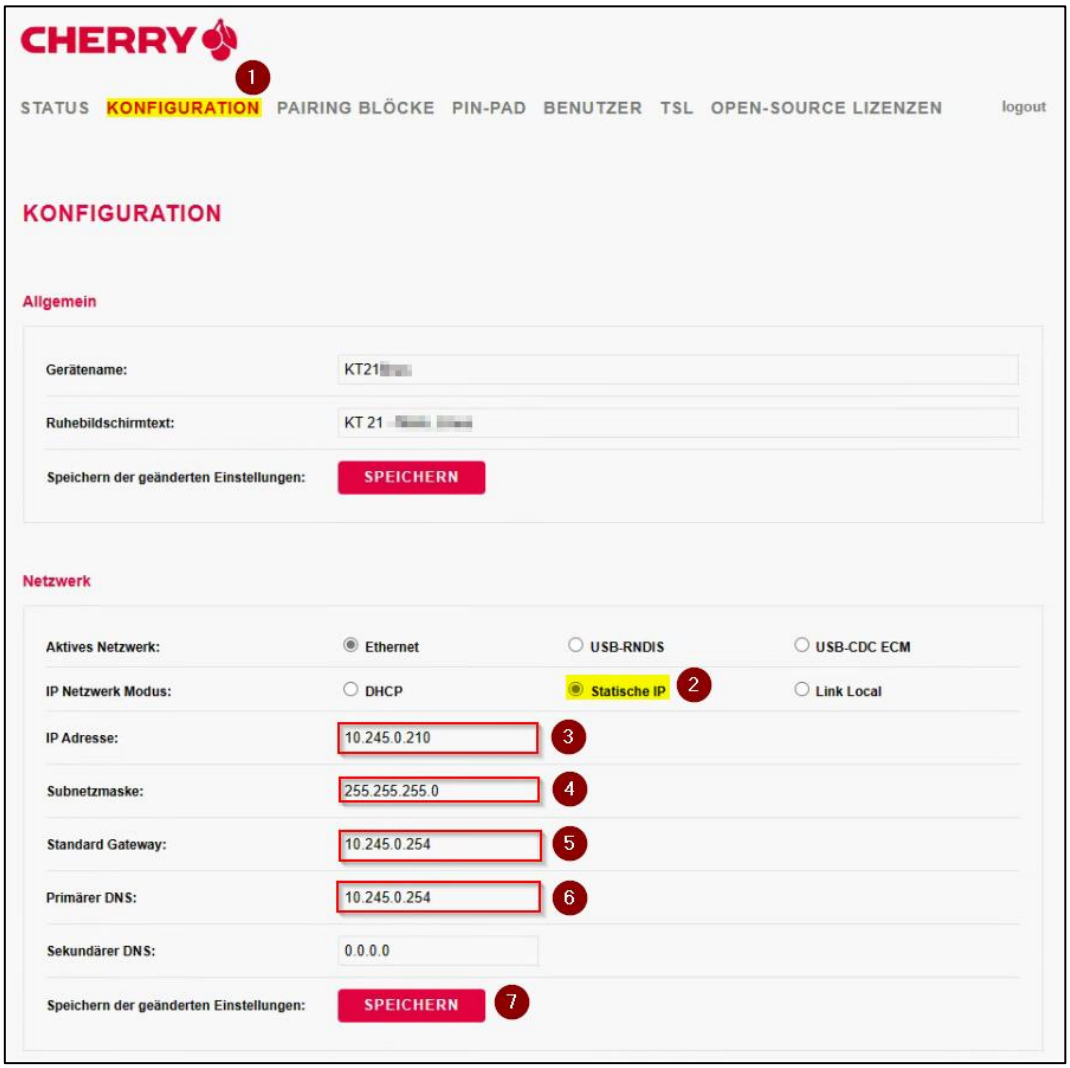
Eingabe mit OK bestätigen.

4.5.2 Cherry ST-1506

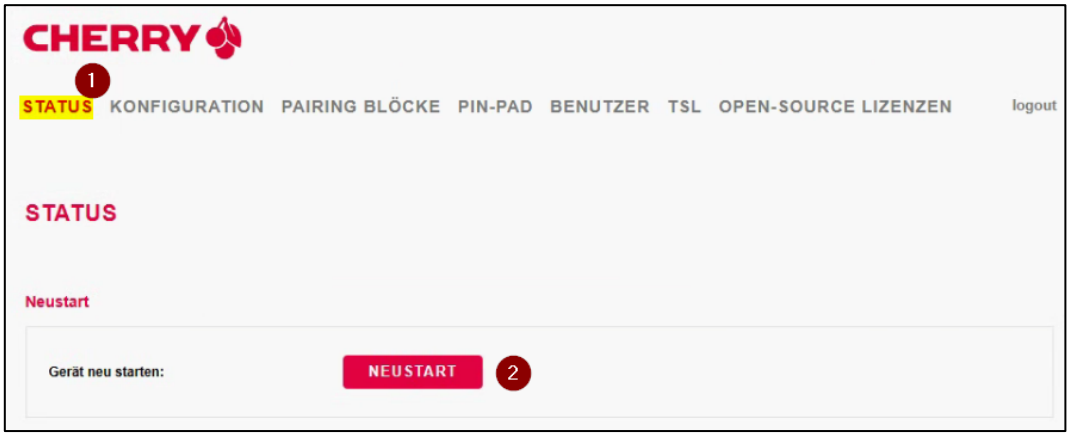
- https://<IpDesKT> aufrufen.
- Mit Admin-PIN vom KT anmelden.



- In Reiter „Konfiguration“ wechseln (1).
- IP Netzwerk Modus auf „Statische IP“ ändern (2).
- IP-Adresse vergeben (3): **010.245.000.[210-240]**
- Subnetzmaske setzen (4): **255.255.255.0**
- Standard Gateway setzen (5): **10.245.0.254**
- Primärer DNS setzen (6): **10.245.0.254**
- „Speichern“ klicken (7).



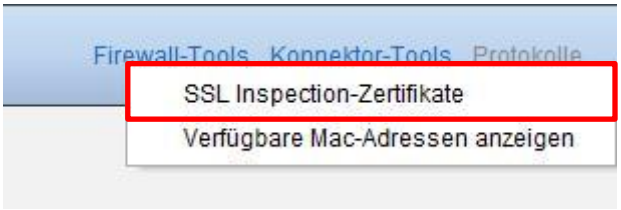
- In den Reiter „Status“ wechseln (1).
- Das Kartenterminal neustarten (2).



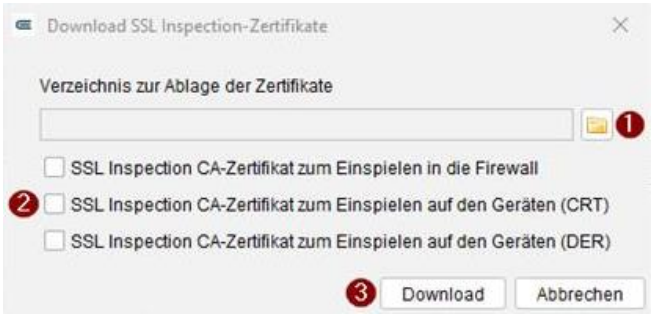
5 Einrichtung SSL Inspection CA-Zertifikate

5.1 Abruf SSL Inspection CA-Zertifikate für Firewall

- Via EPIKUR 4 Funktion (Administrator -> Konnektor-Ansicht)



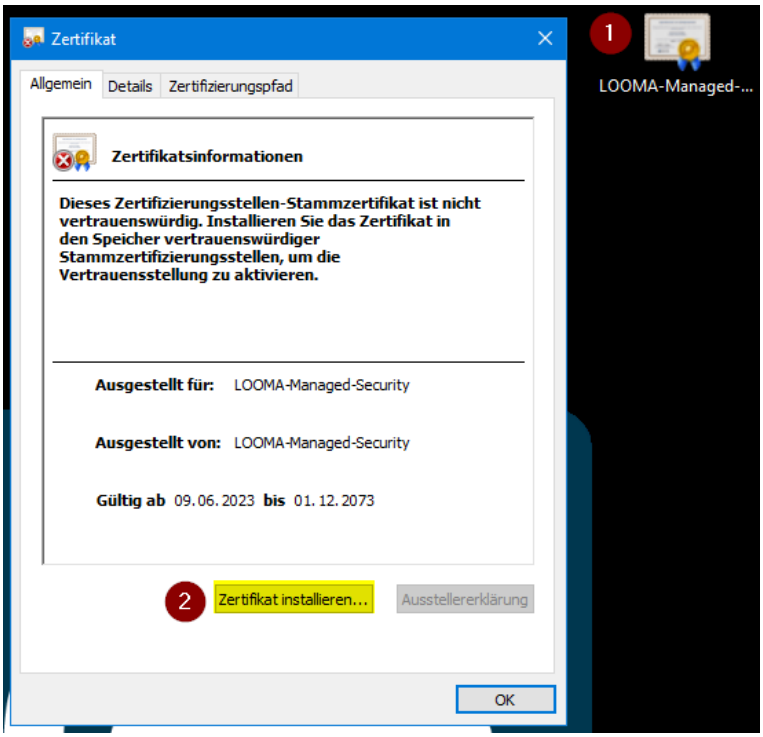
- Auf ALLEN Netzwerkgeräten, die eine Verbindung ins Internet aufbauen, muss das Zertifikat für die SSL Inspection hinterlegt werden.
    - Es stehen zwei Typen zur Verfügung: CRT und DER. Die meisten Systeme können das Format CRT problemlos verarbeiten.



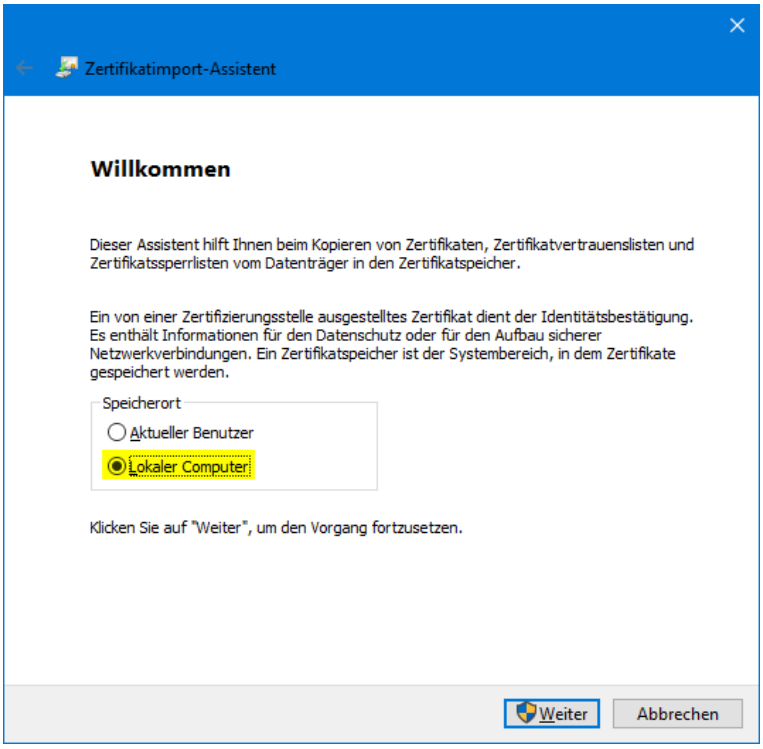
5.2 Installation der SSL-Inspection-CA-Zertifikate auf den Endgeräten in der Praxis

5.2.1 Windows

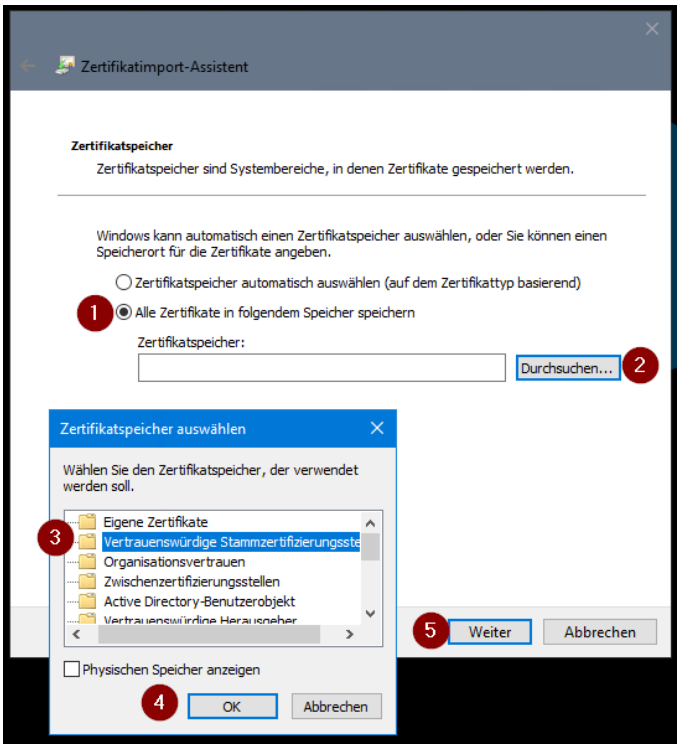
- Die heruntergeladene Datei mit einem Doppelklick öffnen (1).
- „Zertifikat installieren …“ klicken (2).



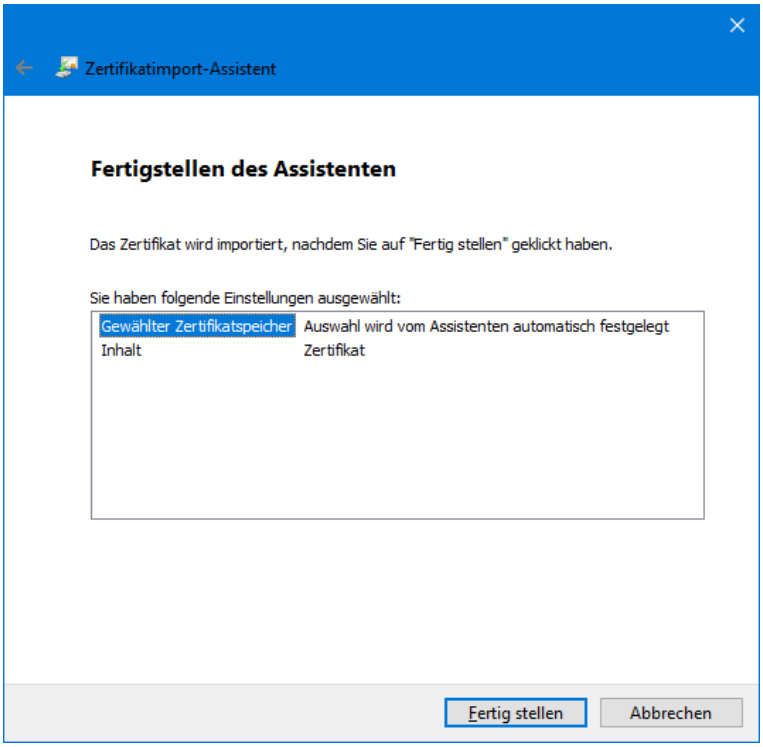
- Speicherort auf „Lokaler Computer“ ändern und „Weiter“ klicken.
- Administrator-Frage bestätigen oder das Administrator-Passwort eingeben lassen.



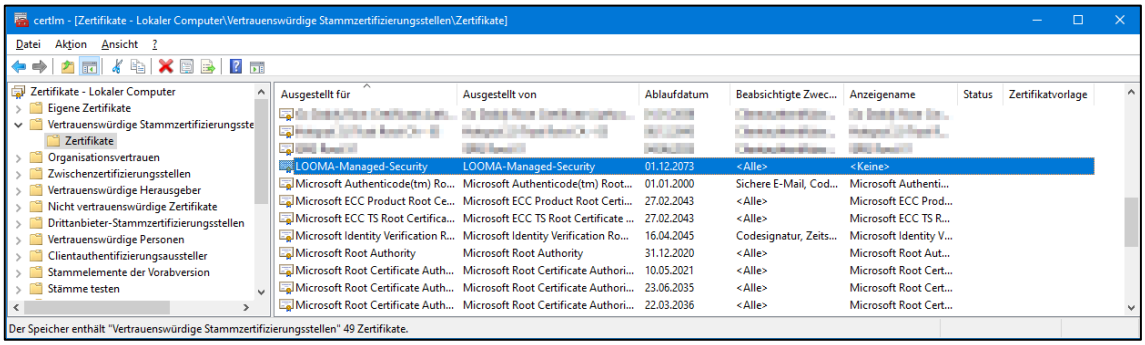
- Die Einstellung auf „Alle Zertifikate in folgendem Speicher speichern“ ändern (1).
- „Durchsuchen…“ klicken (2).
- „Vertrauenswürdige Stammzertifizierungsstellen“ auswählen (3).
- „OK“ klicken (4).
- „Weiter“ klicken (5).



- „Fertig stellen“ klicken.



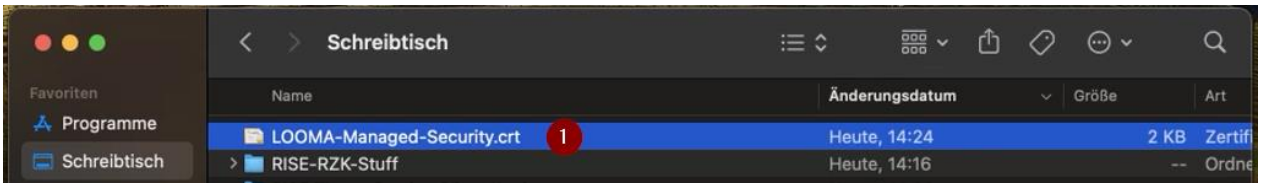
Das Zertifikat wurde nun in den Zertifikatsspeicher von Windows importiert und ist in der Benutzerzertifikatsverwaltung unter *Zwischenzertifizierungsstellen -> Zertifikate* zu finden:



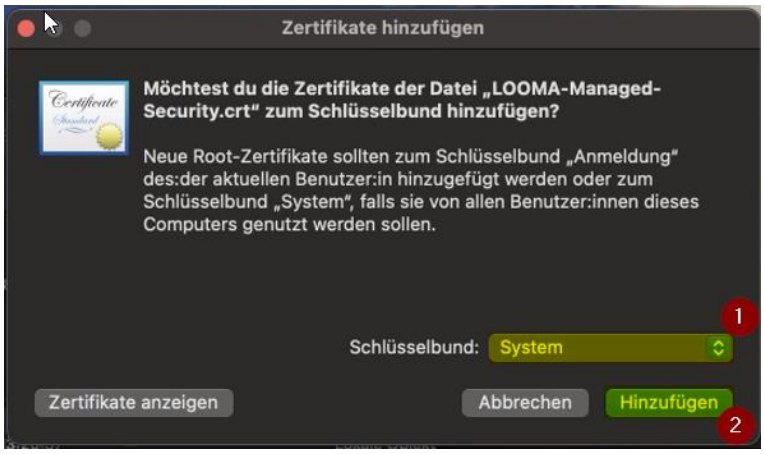
5.2.2 Mac

Zwischen den folgenden Schritten ist es mehrfach notwendig, dass das Administrator-Passwort vom Mac eingegeben werden muss.

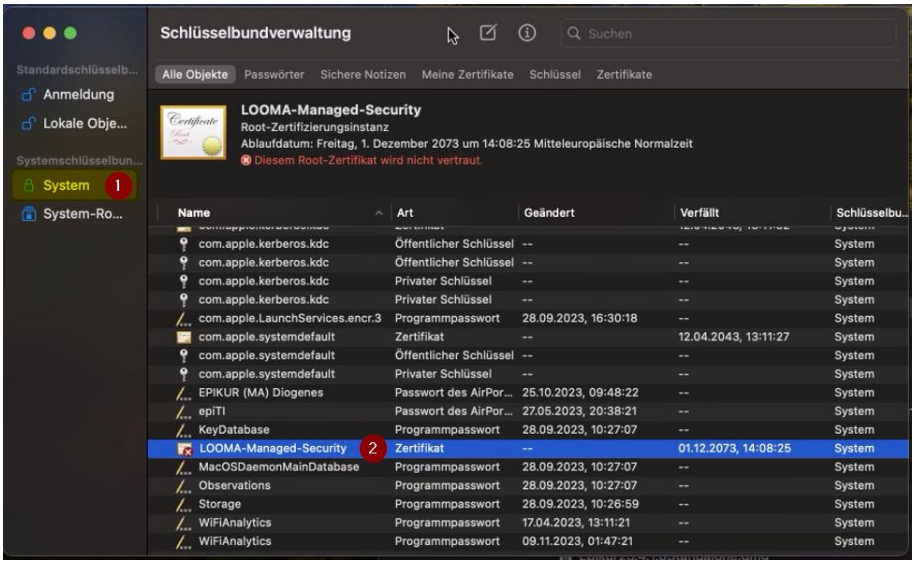
- Das heruntergeladene Zertifikat mit Doppelklick öffnen.



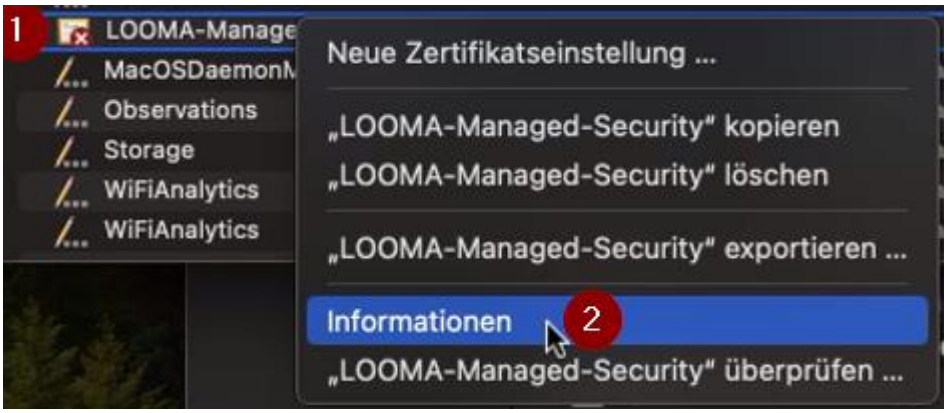
- Schlüsselbund auf „System“ ändern.
- „Hinzufügen“ klicken.



- In der automatisch geöffneten Schlüsselbundverwaltung auf die Ansicht „System“ wechseln (1).
- Den Eintrag „LOOMA-Managed-Security“ suchen (2).



- Rechtklick auf den Eintrag (1).
- „Informationen“ anklicken (2).



- Den ggf. eingeklappten Bereich „Vertrauen" ausklappen (1).
- „Bei Verwendung dieses Zertifikats" auf die Option „Immer vertrauen" ändern (2). Die Subtypen werden automatisch gesetzt und dürfen nicht verändert werden.

- Das Fenster schließen und die Aktualisierung der Einstellungen durch Eingabe des Administratorpassworts bestätigen lassen.

6 TIC-Deinstallation

Dieser Schritt ist nur notwendig, wenn der Kunde bereits auf TIaaS umgestellt worden ist.

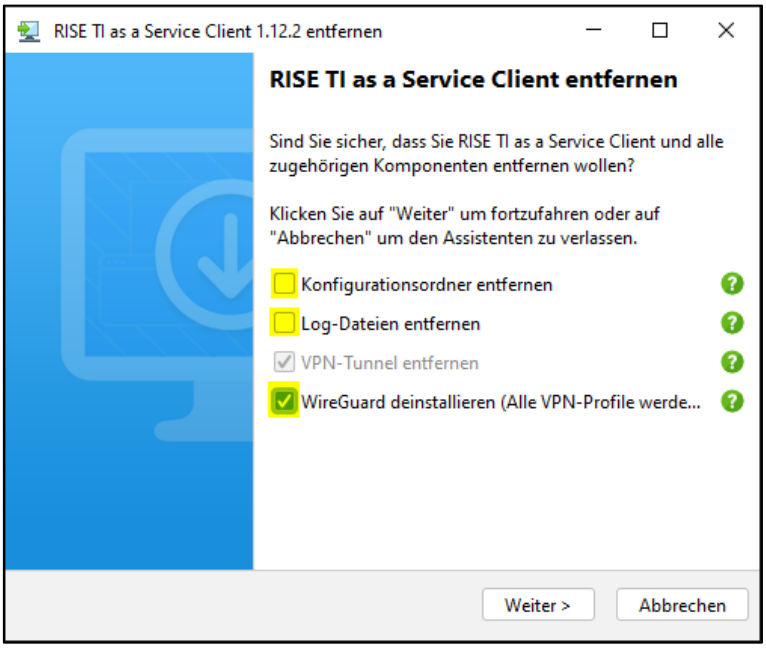
Wenn der Kunde die Netzwerk-Variante von EPIKUR verwendet, so ist der TIC auf allen Arbeitsplätzen vollständig zu deinstallieren!

6.1.1 Windows

- Rechts-Klick auf „Start“ (1).
- „Apps und Features“ öffnen (2).

- Das Programm „RISE TI as a Service Client 1.XX.X“ suchen (1).
- Auf „Deinstallieren“ klicken (2).
- Auf „Deinstallieren“ klicken (3).

- Administrator-Frage bestätigen oder das Administrator-Passwort eingeben lassen.
- Folgende Konfiguration vornehmen:
  - Konfigurationsordner entfernen -> Haken entfernen.
  - Log-Dateien entfernen -> Haken entfernen.
  - WireGuard deinstallieren -> Haken setzten.

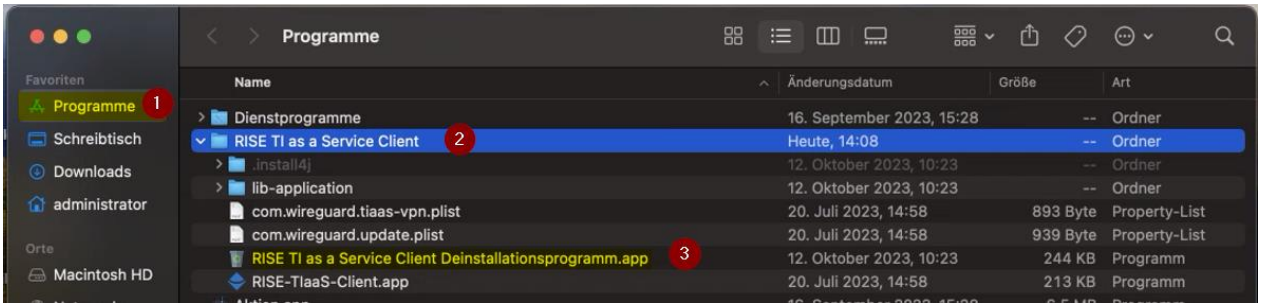


- Auf „Weiter“ klicken.
- Nach Deinstallation: Auf „Fertigstellen“ klicken.

6.1.2 Mac

Deinstallation TIC

- Unter Programme (1) den Ordner „RISE TI as a Service Client“ (2) suchen.
- In dem Ordner die Datei „RISE TI as a Service Client Deinstallationsprogramm.app“ (3) öffnen.
- Eingabe des Administratorpassworts.



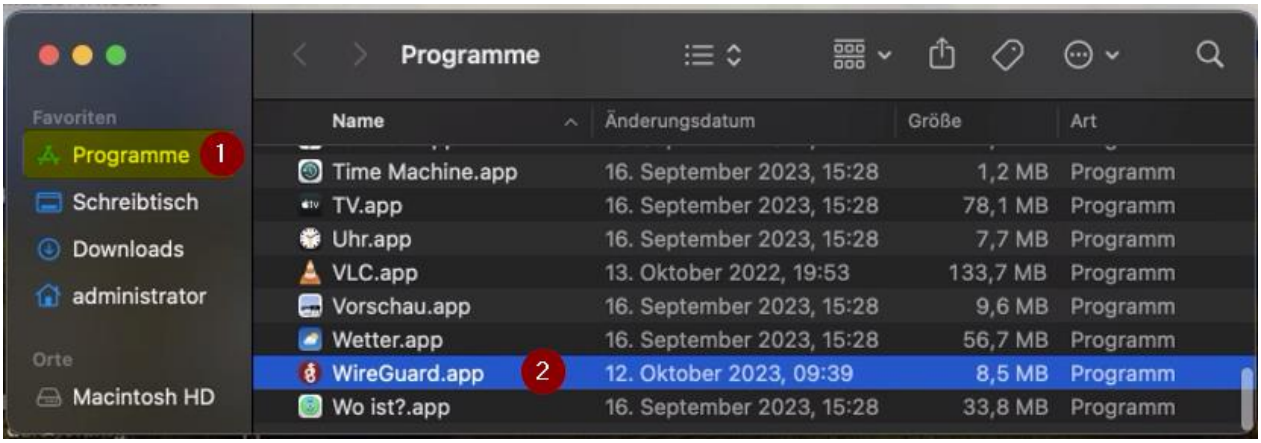
- Folgende Konfiguration vornehmen:
  - Konfigurationsordner entfernen -> Haken entfernen.
  - Log-Dateien entfernen -> Haken entfernen.

- Auf „Weiter“ klicken.
- Nach Deinstallation: Auf „Fertigstellen“ klicken.

Deinstallation WireGuard

- WireGuard in Infoleiste (oben rechts vom Bildschirm) suchen (1).
- Über Klick auf das Icon Kontextmenü öffnen.
- „WireGuard beenden“ klicken (2).

- Unter Programme (1) den Eintrag „WireGurad.app“ (2) suchen.



- Über Rechtsklick auf den Eintrag das Kontextmenü öffnen.
- „In den Papierkorb legen“ anklicken.

7 TIC-Installation

7.1 TIC herunterladen

Die Installation des TICs erfolgt nur auf dem Hauptrechner (siehe Abschnitt Bestimmung Hauptrechner/Ermittlung TIC-MAC-Adresse). Somit ist der Download auch nur auf diesem Gerät notwendig.

Windows → https://client.rise-tiaas.de/installer/tiaas-client-installer_windows.exe
Mac → https://client.rise-tiaas.de/installer/tiaas-client-installer_macos.dmg

7.2 TIC-Installation

Hinweis für MacOS:
Der Installer lässt sich bei neueren MacOS-Versionen nicht über einen Doppelklick öffnen und es wird ein Fehler anzeigt, dass diesem Programm nicht vertraut wird. Über einen Rechtsklick auf das Installer-Icon und dann „Öffnen“ kann der Installer problemlos gestartet werden.

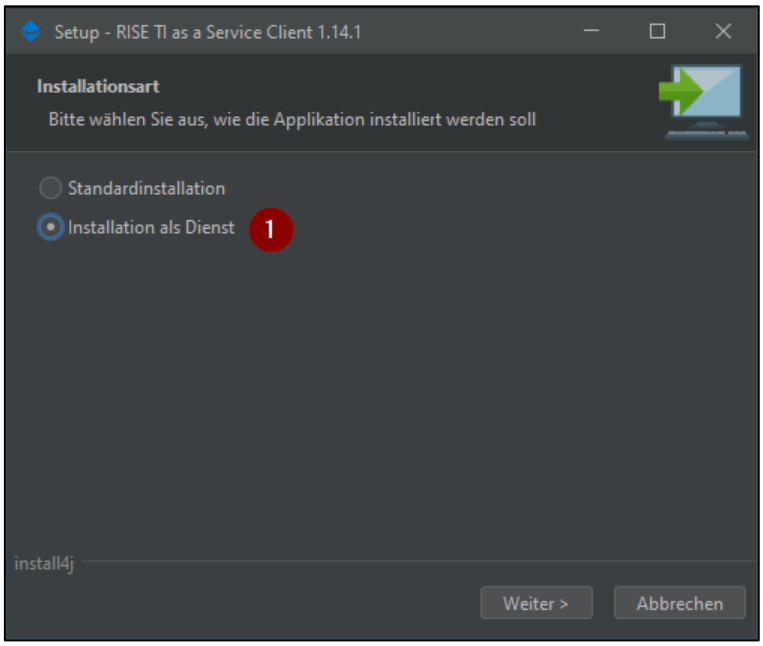
7.2.1 Willkommen

- Auf „Weiter“ klicken.

7.2.2 Installationsart wählen

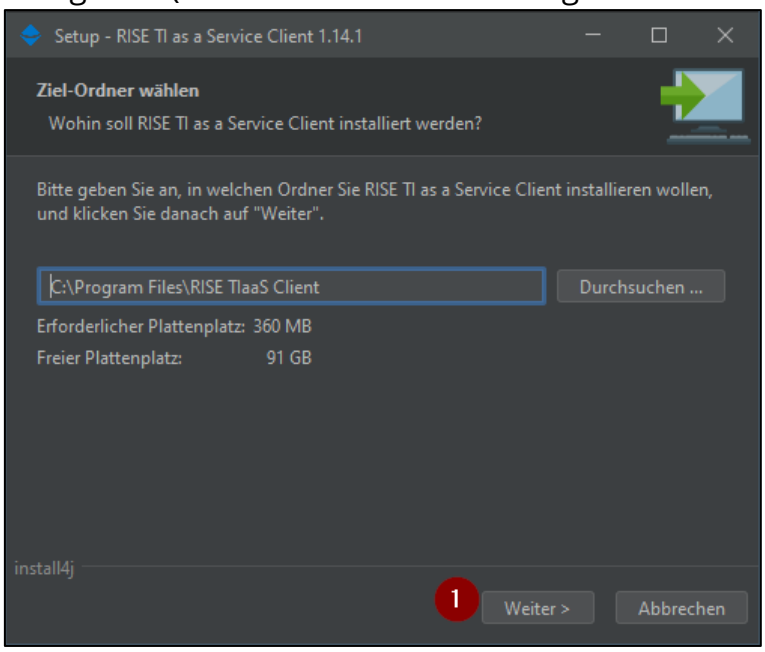
Dieser Schritt entfällt ab der TIC-Version 1.14.2

- „Installation als Dienst“ auswählen.
- Weiter klicken.
- Der Nutzer wird aufgefordert die Installation als Administrator zu genehmigen. Dieses muss ggf. durch die Eingabe des Administrator/Sudo-Kennworts bestätigt werden.



7.2.3 Zielordner wählen

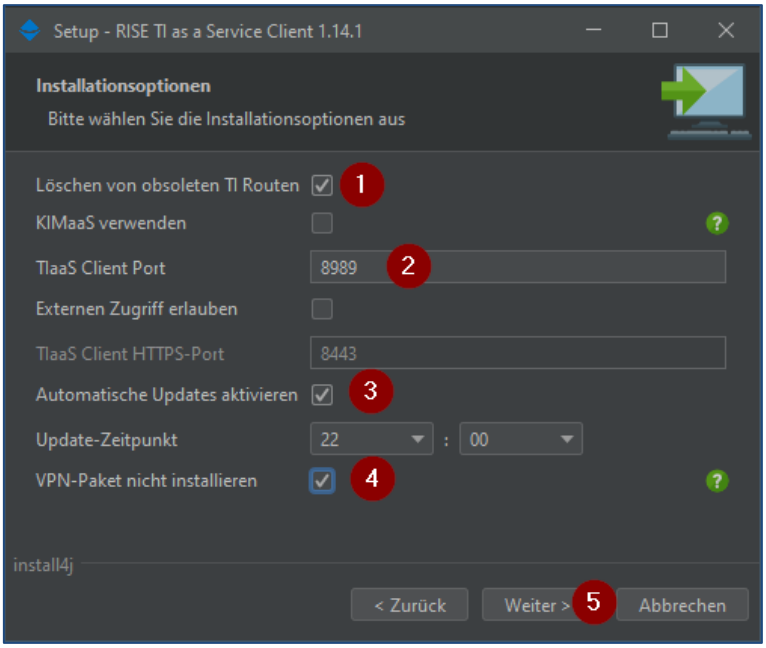
- Einfach weiter gehen (korrekter Pfad ist hinterlegt - nicht ändern!).



7.2.4 Installationsoptionen

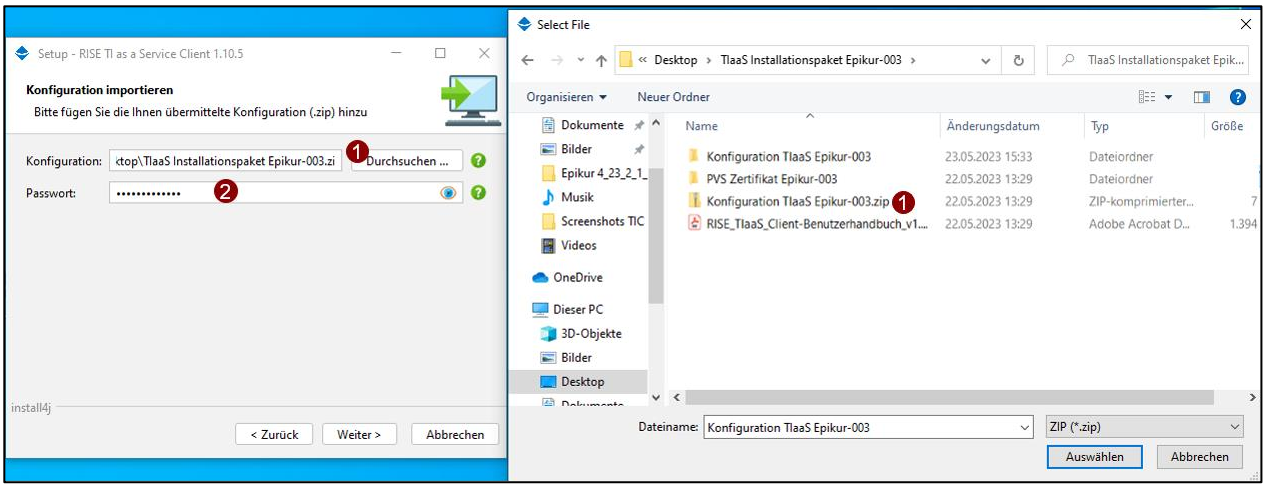
- Löschen von obsoleten TI Routen → Haken setzen (1).
- KIMaaS verwenden → Haken nicht setzen.
- TIaaS Client Port von "8080" ändern zu - > "8989" (2).
- Automatische Updates aktivieren → Haken setzen (3).

- VPN-Pakte nicht installieren → Haken setzen (4).
- Auf „Weiter“ klicken (5).



7.2.5 Installationsoptionen

- ZIP-Konfigurationspaket ("TIaaS_Config_Epikur-XXXX.zip") aus dem entpackten Installationspaket ("TIC-Installationspaket_Epikur-XXXX) auswählen → nicht den entpackten Ordner "TIaaS_Config_Epikur-XXXX" auswählen, sondern die ZIP-Datei.
- Erneut Passwort/Bereitstellungscode für den Kunden zur Verwendung der ZIP-Datei eingeben.
- Anschließend auf „Weiter“ klicken.
- Wenn gefragt wird, ob die Datei „application.yaml“ überschrieben werden soll: „Ja“ klicken.



7.2.6 Installation abschließen

- Bei macOS: Zugriffsrechte auf "System Events" erlauben.
- Administrator-Passwort eingeben.
- Installation durchführen und fertigstellen.

8 Anschluss Computer

Sobald der LOOMA-Techniker bestätigt, dass die Konfiguration auf die Firewall und den AP ausgerollt wurde, kann mit diesem Schritt fortgeführt werden.

Vor dem Anschluss des Computers an die Firewall ist sicher zu stellen, dass die Netzwerkkonfiguration auf „DHCP“ und nicht auf „statische IP-Adresse“ steht.

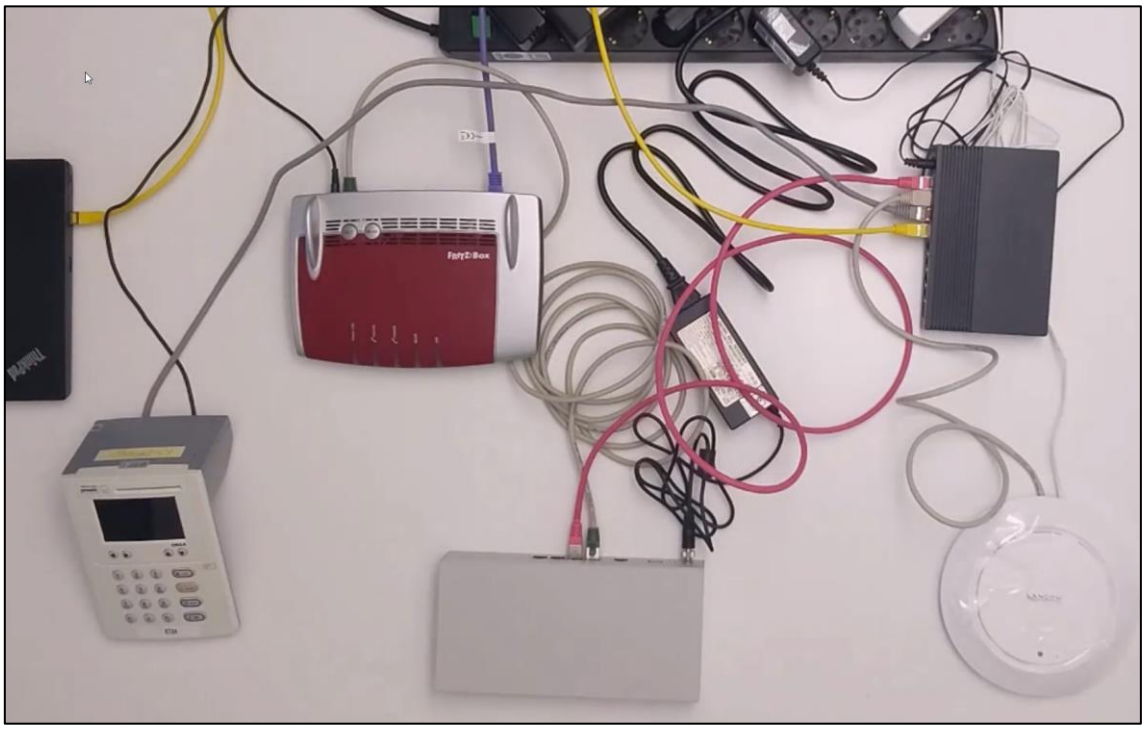
Wenn Computer via LAN verbunden:

- Wenn via LAN verbunden: LAN-Kabel des Computers am Router abziehen.
- In freien Port des Switches stecken.

Wenn Computer via WLAN verbunden:

- WLAN-Netzwerk von Router-WLAN auf AP-WLAN ändern.
    - Das WLAN-Netz heißt: „Praxis-*BSRN*“.

Finale Situation



Portbelegung

Port an Firewall	**Gerät**
ETH 0	LAN von Router
ETH 1	Switch
ETH 2	Nicht benutzbar
ETH 3	Nicht benutzbar

Alle Netzwerkgeräte (AP, KTs, Computer, etc.) werden an den Switch angeschlossen.

8.1 Erneuerung der DHCP-Releases auf den Computern

Vor dem Umstecken des jeweiligen Netzwerkgerätes ist sicher zu stellen, dass das Netzwerkgerät auf DHCP umgestellt wurde oder die Statische IP-Adresse auf das neue Subnetz angepasst wurde.
Das Setzten einer statischen IP-Adresse darf – wenn überhaupt – nur bei Netzwerkgeräten vorgenommen werden, die das Praxisnetz niemals verlassen.
Unsere Empfehlung ist, alle Netzwerkgeräte (mit Ausnahme des KT) auf DHCP umzustellen.

- LAN-Kabel abziehen und neu einstecken.
- Via Terminal:

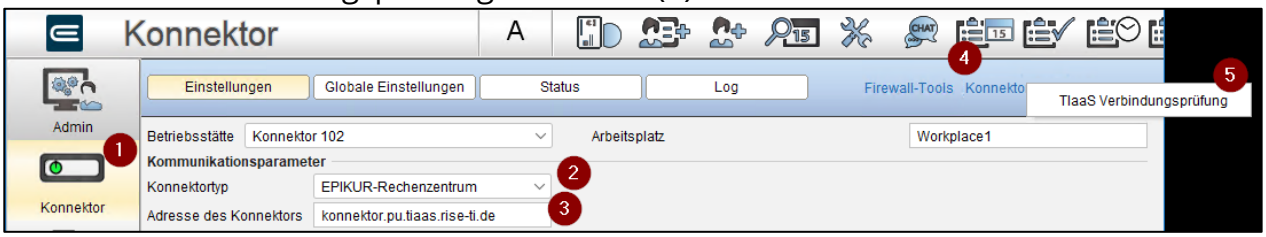
    - Windows: ipconfig /renew
- Via Oberfläche (macOS):
    - Mac-Menü „Apple“ -> „Systemeinstellungen“ -> „Netzwerk“
    - Netzwerkdienst auswählen
    - „Details“ -> „TCP/IP“
    - „DHCP-Lease erneuern“ klicken

Die neue IP sollte jetzt 10.245.0.x sein.

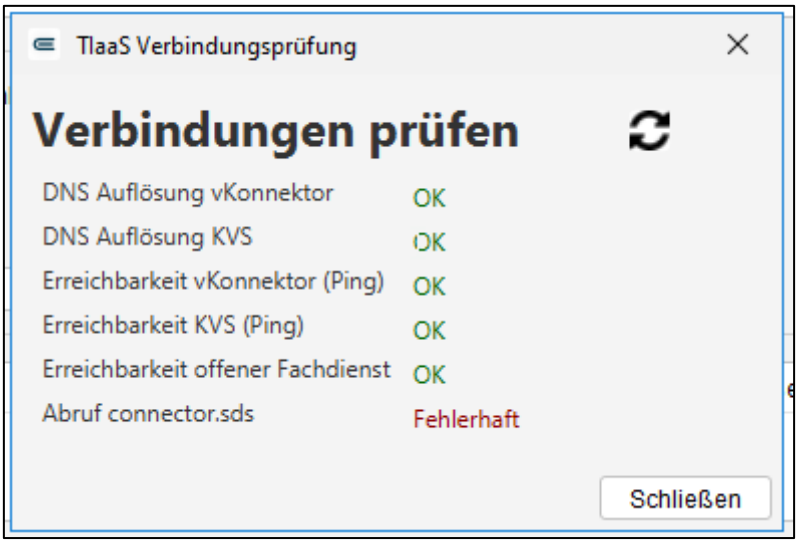
- Auf dem Hauptrechner 10.245.0.190

9 Verbindungstest Firewall

- In EPIKUR aus Administrator anmelden.
- In die Ansicht „Konnektor“ wechseln (1).
- Den Konnektortyp auf „EPIKUR-Rechenzentrum“ umstellen (2).
- Die Adresse des Konnektors überprüfen (wird automatisch gesetzt) (3).
- Auf „Konnektor-Tools“ klicken (4).
- TIaaS Verbindungsprüfung anwählen (5).



Da noch keine Zertifikate in EPIKUR hinterlegt sind, wird der Test „Abruf connector.sds“ fehlschlagen. Die Zertifikate werden zu einem späteren Zeitpunkt in EPIKUR hinterlegt.



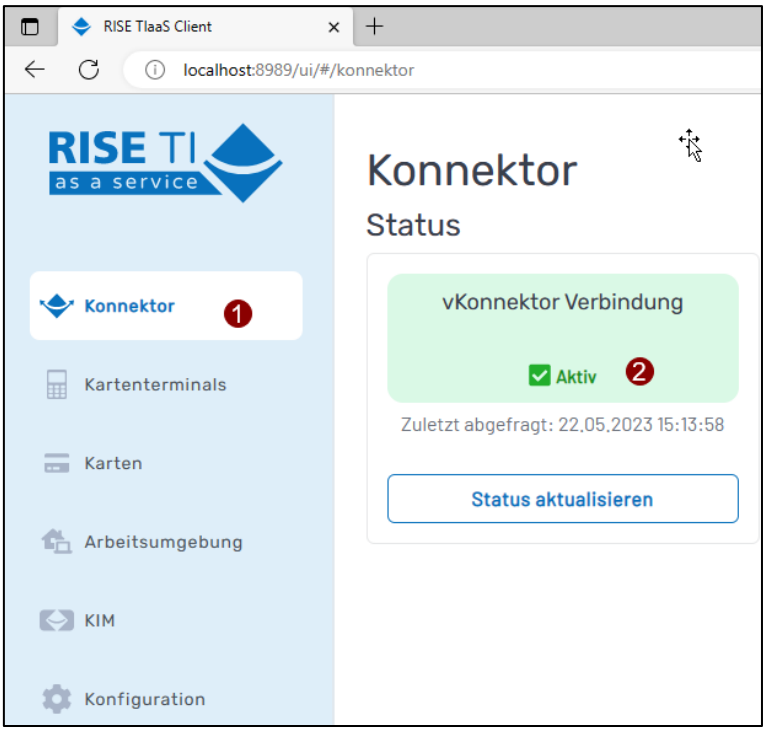
Schlägt einer der beiden DNS-Auflösungs-Tests fehl, so ist diese Anlagen zu beachten: A.4 DNS-Rebind-Schutz und A.5 DNS-Server ändern

10TIC konfigurieren

- http://localhost:8989 aufrufen.

10.1 Verbindung vKonnektor prüfen

- „Status aktualisieren“ klicken.
- Status prüfen.
  - Wenn aktiv: weiter zum nächsten Schritt.
  - Wenn inaktiv: siehe Anhang A.1 Manuelles Einspielen der Zertifikate in den TIC.



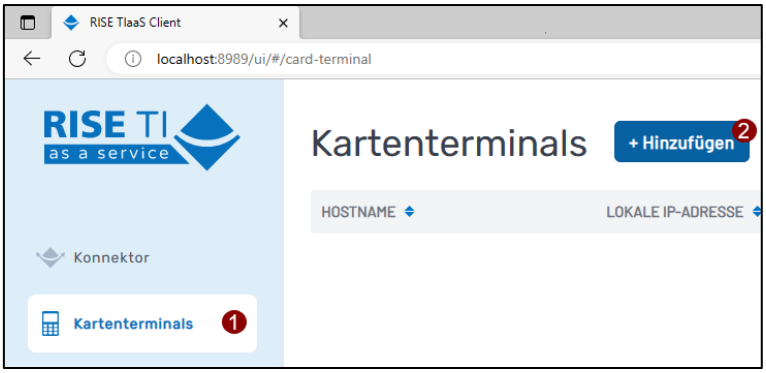
10.2 Netzwerkadapter für das VPN setzten

- Auf Ansicht „Konfiguration“ wechseln.
- Unter „Netzwerkadapter für das VPN“ das Interface „10.245.0.190“ auswählen.
- Speichern.

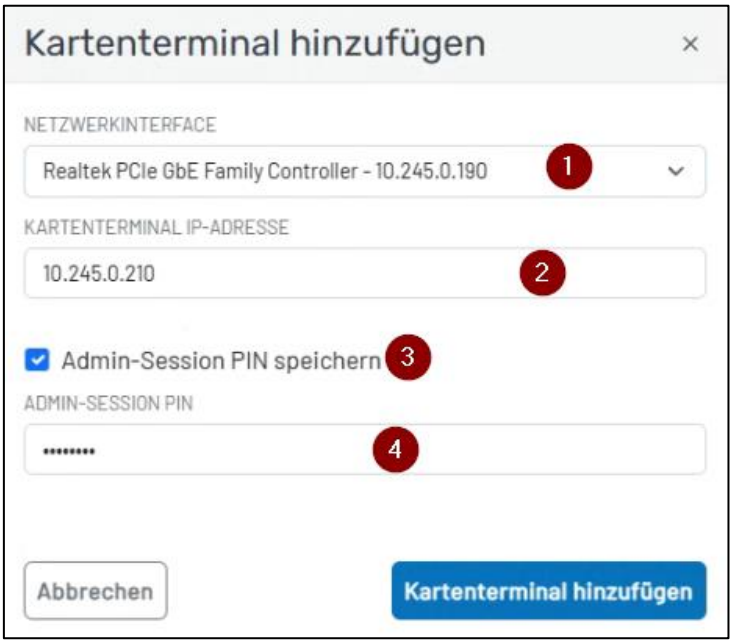
10.3 Kartenterminal verbinden

Ggf. ist vorher die Admin-Session auf dem Kartenterminal zu aktivieren (siehe Anhang A.2 Admin Session konfigurieren)

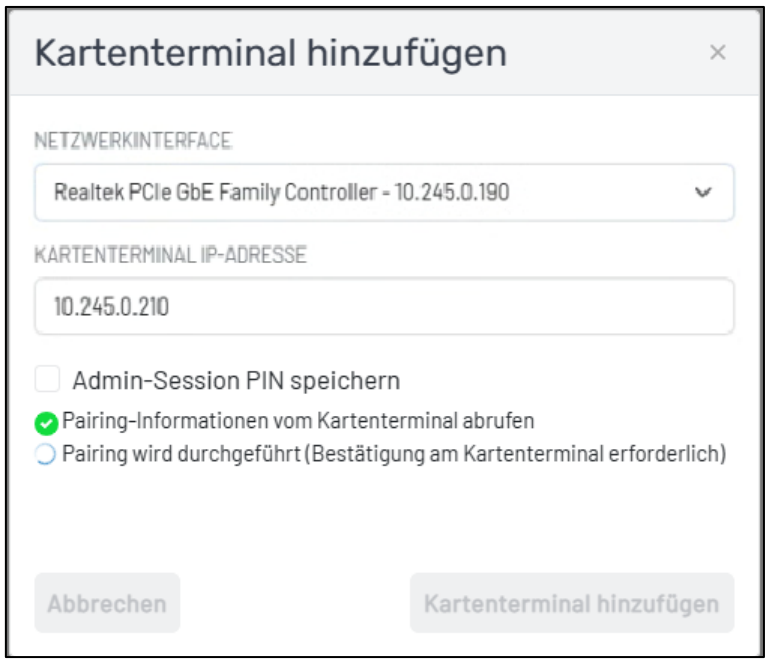
- Ggf. vorher das alte KT entfernen.
- Auf Ansicht „Kartenterminals“ wechseln.
- „Hinzufügen“ klicken.



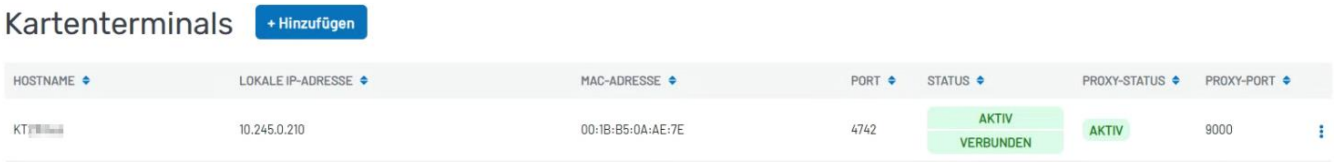
- Netzwerkinterface 10.245.0.190 auswählen (1).
- IP vom Kartenterminal eingeben (2)
  - 10.245.0.[210-240].
- Admin-Session PIN speichern -> Haken setzen (3).
- Admin-PIN vom KT eingaben (lassen) (4).



- Pairing am KT bestätigen.



War das Pairing erfolgreich, wird das KT in der Übersicht angezeigt:



Sollte der Fehler „Pairing-Blöcke voll“ angezeigt werden: Siehe Anhang A.2 Pairing-Blöcke löschen).
Wird ein unspezifischer Fehler angezeigt siehe Anhang A.3 Fehlerhandling Kartenterminal-Pairing).

10.4 Aufrufkontext einrichten

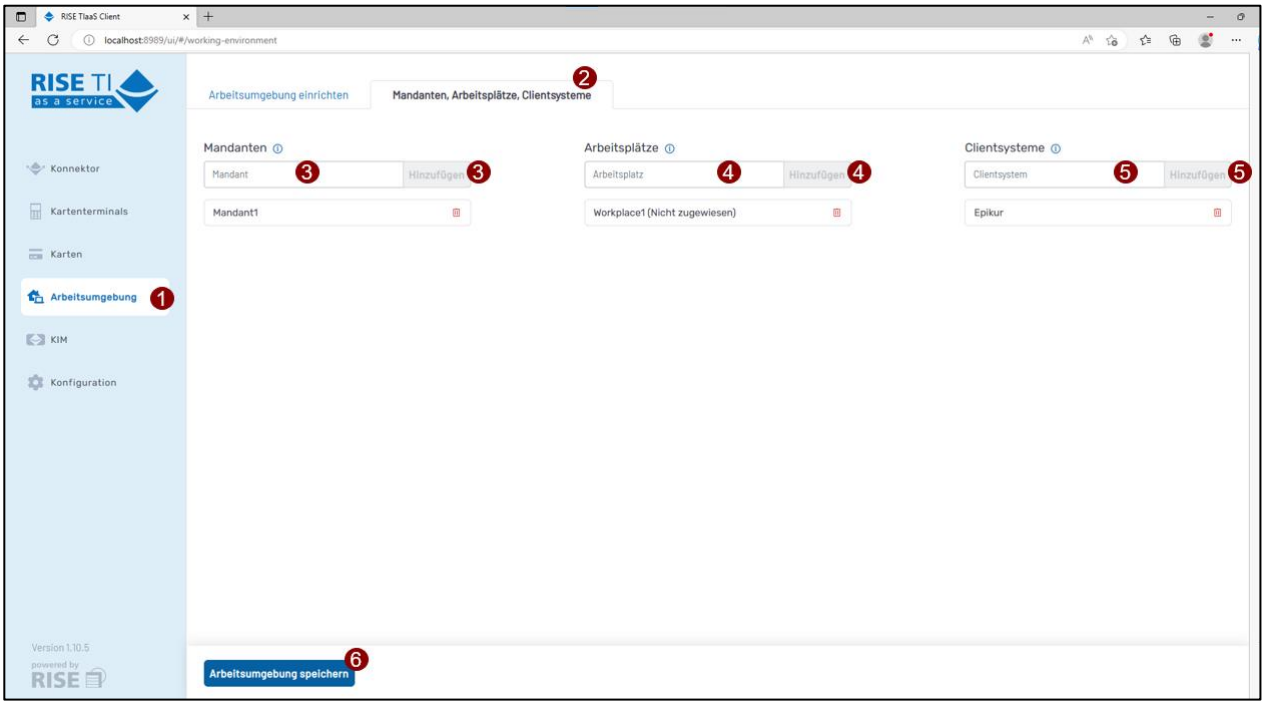
Dieser Schritt ist nur notwendig, wenn ein Umzug von Secunet auf TIaaS stattfindet.

Nun den zuvor erstellten Screenshot des Aufrufkontextes verwenden!

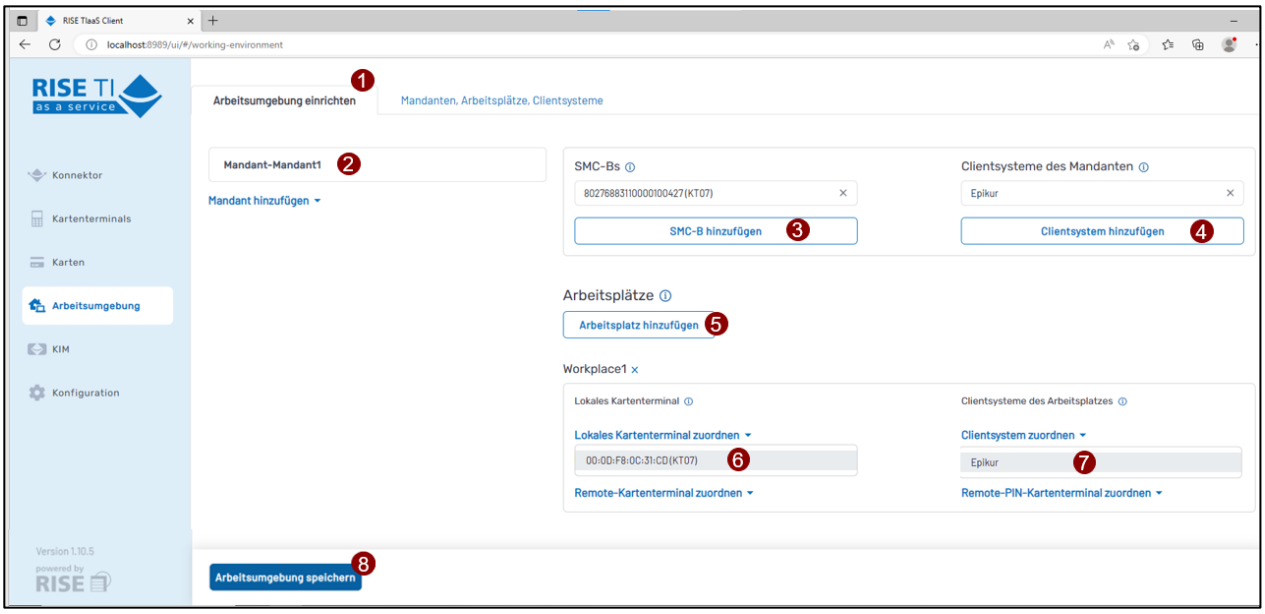
Bei Umzug Secunet auf TIaaS: Die bisherigen Aufrufkontexte sollen nicht verändert und entsprechend aus dem Konnektor oder EPIKUR übernommen werden.

- In Ansicht „Arbeitsumgebung“ wechseln.
- Klick auf „Mandanten, Arbeitsplätze, Clientsysteme“.

- Eingabe des Mandanten und Klick auf „Hinzufügen“.
    - Syntax: M + *BSNR*
- Eingabe des Arbeitsplatzes und Klick auf „Hinzufügen“.
    - Frei wählbar, z.B. Empfang, Labor
    - Sollten keine Umlaute (ä, ö, ü) enthalten
- Eingabe des Clientsystems und Klick auf „Hinzufügen“.
    - Syntax: Epikur
- Klick auf „Arbeitsumgebung speichern“.



- Klick auf „Arbeitsumgebung einrichten“.
- Auswahl des erstellten Mandanten.
- Auswahl der entsprechenden SMC-B und „SMC-B hinzufügen“ klicken.
- Auswahl des erstellten Clients und „Clientsystem hinzufügen“ klicken.
- Lokales Kartenterminal zuordnen und Auswahl des Kartenterminals.
- Lokales Clientsystem zuordnen und Auswahl des erstellten Clients.
- Arbeitsumgebung **speichern.**



10.5 Primärsysteme hinterlegen

Dieser Schritt ist nur bei einer Netzwerkvariante von EPIKUR notwendig.

Damit die Konnektor-Events an den jeweiligen EPIKUR-Client weitergeleitet werden können, muss im TIC jeder Client als „Primärsystem“ hinterlegt werden.

10.5.1 Berechnung Port für Ereignisdienst

Ein Primärsystem/EPIKUR-Client wird durch die IP-Adresse und einen Port definiert. Der zu konfigurierende Port lässt sich anhand des vierten Oktetts der IP-Adresse ableiten.

Gleichung

$$IP = 10.245.0.x \rightarrow 10000 + x = Port$$

Erklärung

- Bei der IP-Adresse 10.245.0.**2** ist das vierte Oktett eine **2**
- Auf die 2 wird 10000 (Zehntausend) addiert -> 10**002**
- Der Port für das Primärsystem mit der IP-Adresse 10.245.0.2 ist 10002

Beispiele

IP	Viertes Oktett	Port
10.245.0.2	2	10002
10.245.0.11	11	10011

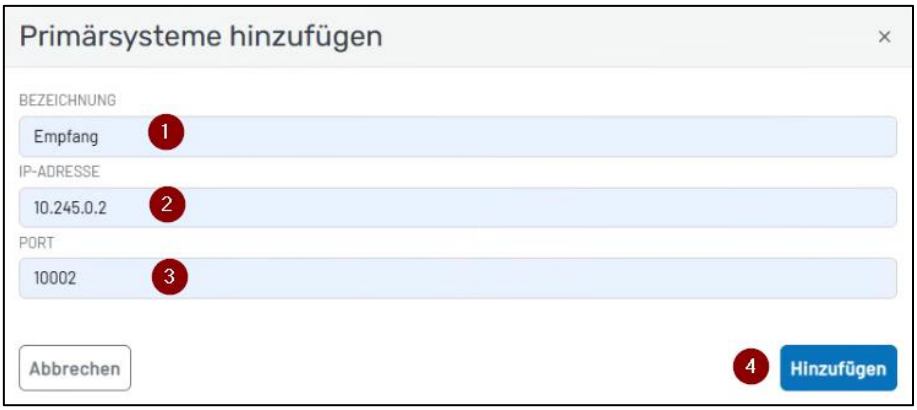
10.245.0.112	112	10112

Von dieser Berechnung darf nicht abgewichen werden, da EPIKUR automatisch – entsprechend dieser Formel – den Port für den Ereignisdienst bestimmt.

10.5.2 Primärsystem hinzufügen

- In die Ansicht „Primärsysteme“ wechseln (1).
- „+ Hinzufügen“ klicken (2).

- Bezeichnung des Primärsystems eingeben (z. B. Empfang, Büro, Labor) (1).
- IP-Adresse des Primärsystems/EPIKUR-Clients eingeben (2).
- Port des Primärsystems eingeben (3) (siehe Berechnung Port für Ereignisdienst).
- „Hinzufügen“ klicken (4).



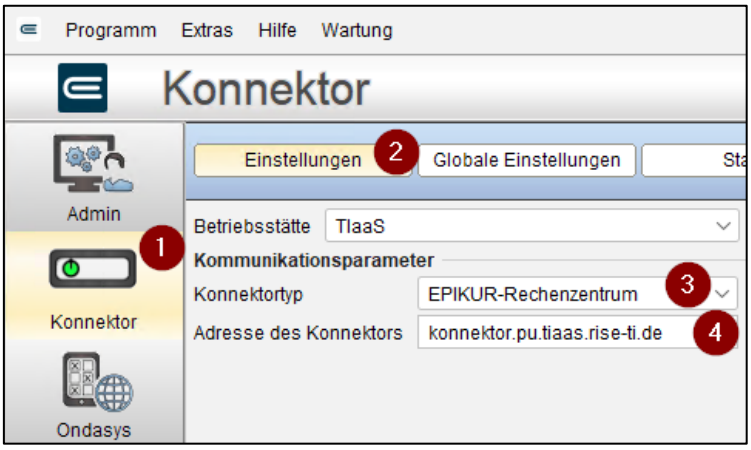
Wurden die Primärsysteme hinzugefügt, so sieht die Übersicht vergleichbar mit dem folgenden Bild aus:

11 EPIKUR konfigurieren

11.1 Kommunikationsparameter umstellen

Dieser Schritt ist nur notwendig, wenn ein Umzug von Secunet auf TIaaS stattfindet.

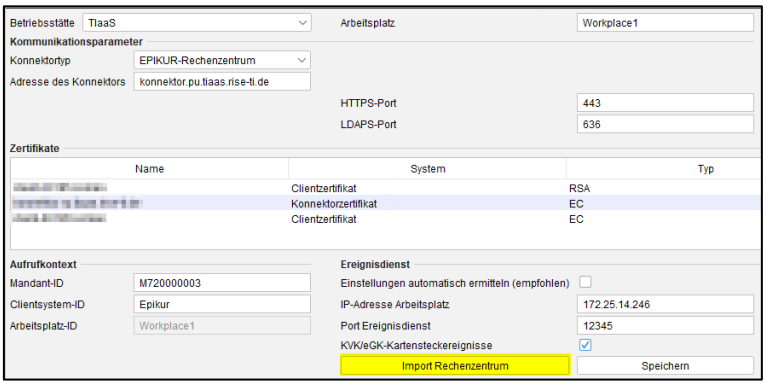
- Einloggen als Administrator und Konnektor-Einstellungen aufrufen (1, 2).
- Konnektor-Typ auf "EPIKUR-Rechenzentrum" umstellen (3).
- Konnektor-Adresse auf "konnektor.pu.tiaas.rise-ti.de" setzten (wird vorbefüllt) (4).



11.2 Automatischer Import des Installationspakets

Dieser Schritt ist nur notwendig, wenn ein Umzug von Secunet auf TIaaS stattfindet.

- Durch Klick auf “Import Rechenzentrum” kann der automatische Import gestartet werden.

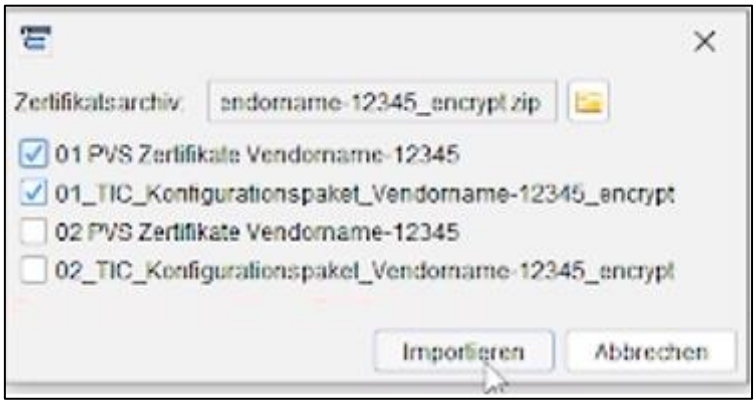


- Anschließend kann das Installationspaket ausgewählt werden → verschlüsseltes und nicht entpacktes Installationspaket als ZIP-Datei - “TIC-Installationspaket_Epikur-XXXX.zip”.
- PW zur Entschlüsselung eingeben.

- Auf "Übernehmen" klicken.
- Die benötigten Ordner auswählen.
    - Es wird je Installation der Ordner „PVS_Zertifikate …“ und „TIC_Konfigurationspaket …“ benötigt.
    - Wenn nur 1 Installationspaket in der ZIP-Datei enthalten ist, werden die Ordner „PVS_Zertifikate …“ und „TIC_Konfigurationspaket …“ nur 1-mal auswählbar. Sind mehrere Installationspakete enthalten, werden die Ordner mehrmals angezeigt/ sind mehrmals wählbar. In diesem Fall sind die Ordner mit voranstehender Zahl "XX" nummeriert.
        - z. B. 01 für das erste Installationspaket).
    - **WICHTIG:** Stehen mehrere Zertifikate in dem Ordner „PVS Zertifikat …“ zur Auswahl und wurden diese in EPIKUR importiert, so ist das Zertifikats-Paar (RSA, ECC) mit der niedrigsten Nummer zu wählen. Alle restlichen Zertifikate müssen aus EPIKUR entfernt werden. Hintergrund: Die hinterlegten Zertifikate werden von jedem Client genutzt und dürfen nur einmal hinterlegt werden.

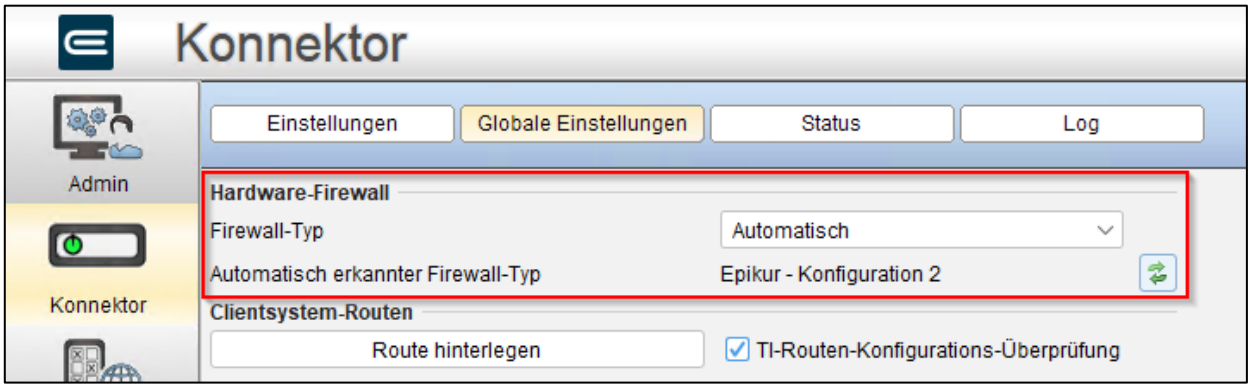
Falsche Zertifikate führen dazu, dass ggf. keine KIM-Nachrichten versendet werden können.

- Anschließend auf „Importieren“ klicken
  → Zertifikate werden importiert. Die IP-Adresse des Arbeitsplatzes wird ebenfalls automatisch übertragen.



11.3 Firewall-Typ überprüfen

Ab der EPIKUR-Version 23.4.1.3 steht eine Einstellung für den Firewall-Typ in EPIKUR zu Verfügung. In der Standardeinstellung wird der Typ automatisch bestimmt und angezeigt.

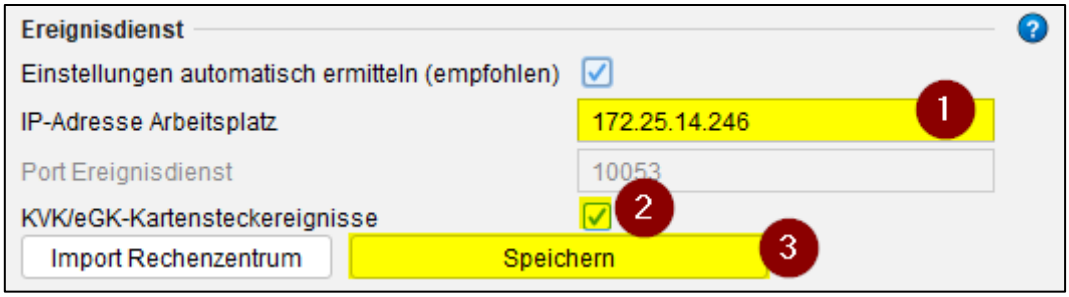


Es gilt ausschließlich zu überprüfen, ob der automatisch bestimmte Typ auf „EPIKUR – Konfiguration 2“ steht. Ist dieses der Fall, besteht kein Handlungsbedarf. Hintergrund: „EPIKUR – Konfiguration 2“ steht für die LOOMA-Firewall-Konfiguration. Die Konfiguration „EPIKUR – Konfiguration 1“ beschreibt den „alten“ Konfigurationsstand der EPIKUR-Firewalls.

11.4 Ereignisdienst konfigurieren

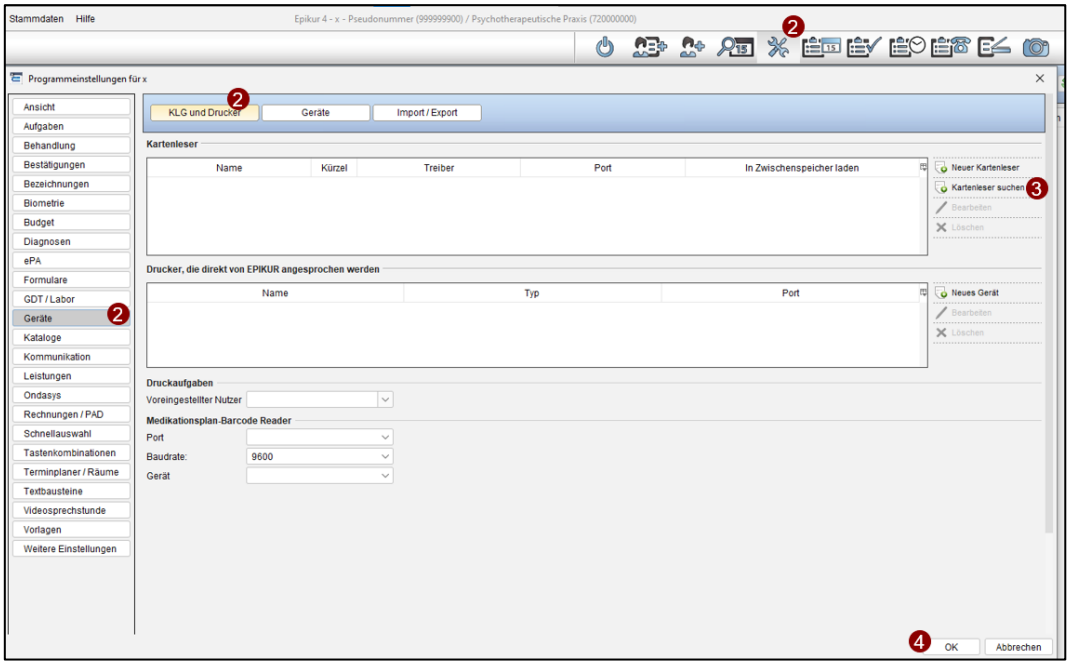
Wenn der automatische Import des Installationspakets erfolgreich war, so ist die IP-Adresse Arbeitsplatz bereits korrekt übernommen worden.
Ist es zu einem Fehler gekommen, so ist die IP-Adresse (Wireguard-Interface-IP) aus dem Schritt Firewall-Einrichtungsdaten an LOOMA übergeben einzugeben (1).

- Checkbox für KVK/eGK-Kartensteckereignisse setzten (2).
- Speichern (3).



11.5 Kartenlesegeräte neu hinzufügen

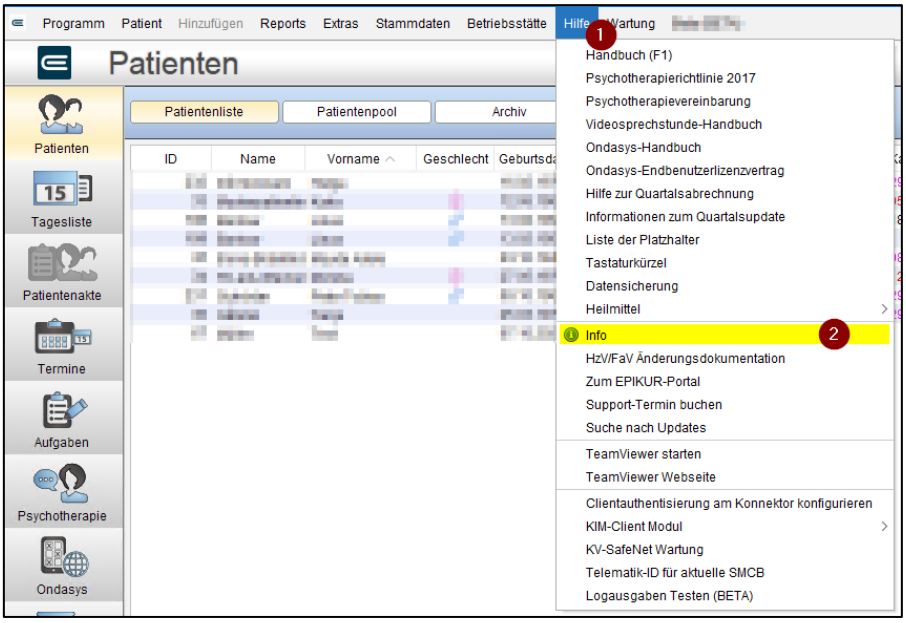
- Als Admin ausloggen und als Nutzer anmelden.
- Klick auf Programmeinstellungen → Geräte → KLG und Drucker (2).
- Wenn noch Kartenterminals gespeichert sind, diese zuerst entfernen.
- Klick auf Kartenleser suchen (In Toolbar) und KT neu hinzufügen (3).
- Klick auf OK und EPIKUR neu starten (4).



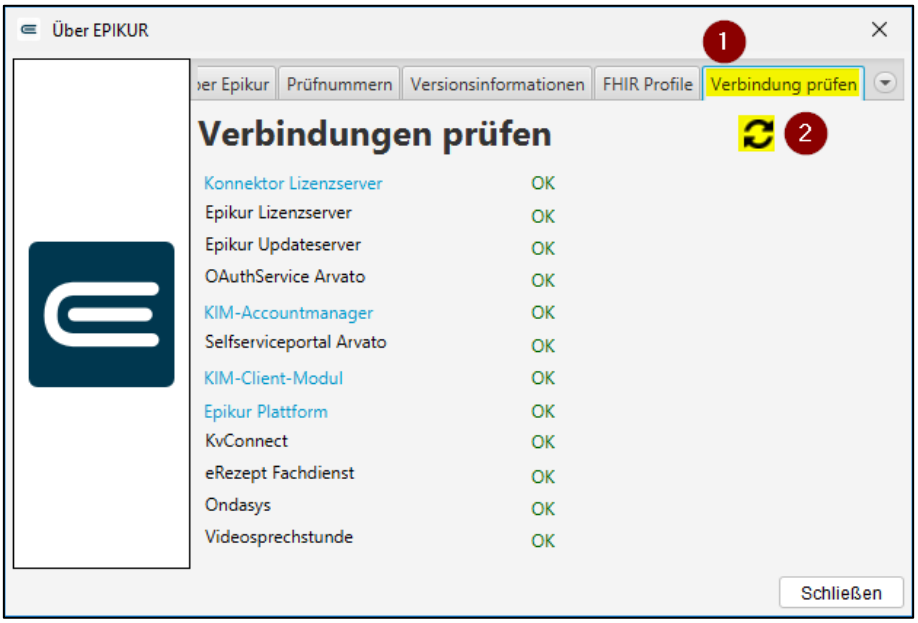
11.6 EPIKUR-TI-Funktionen testen

11.6.1 Verbindungstest

- Als Nutzer anmelden.
- Im Menü „Hilfe“ öffnen (1).
- „Info“ anklicken (2).



- In den Tab „Verbindungen prüfen“ wechseln (1).
- Bei Bedarf Verbindungstest erneut starten (2).

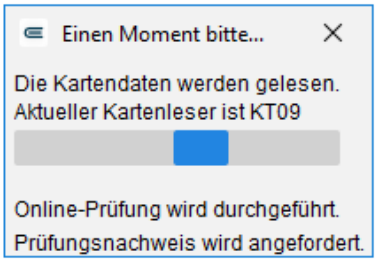


11.6.2 Karte einlesen

Manuell

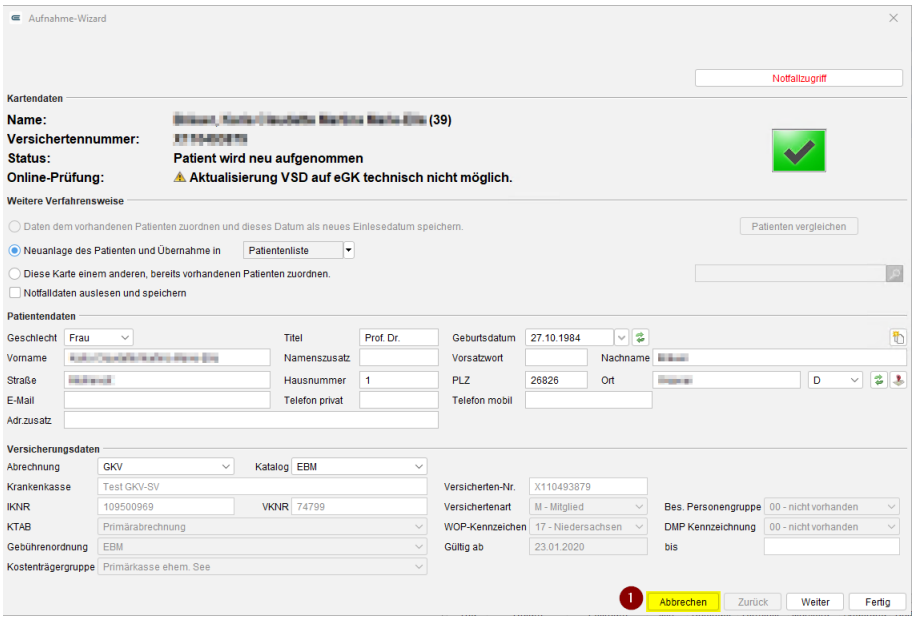
- Als angemeldeter Nutzer in der Systemleiste (oben rechts) auf das Icon des Kartenlesers klicken.

Wenn sich das im Folgenden dargestellte Dialogfenster öffnet, können Karten eingelesen werden.

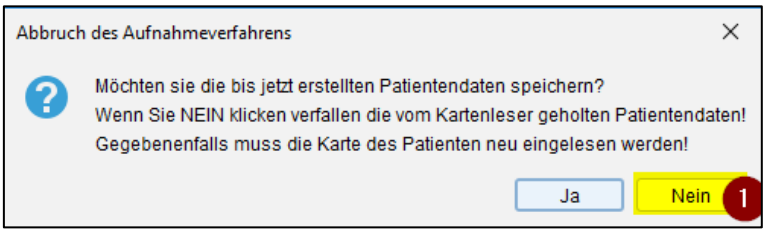


Im Normalfall sollen die eingelesenen Kartendaten nicht in EPIKUR übernommen werden (z. B. die private Versichertenkarte des Kunden).

- Im Aufnahme-Wizard auf „Abbrechen“ klicken (1).



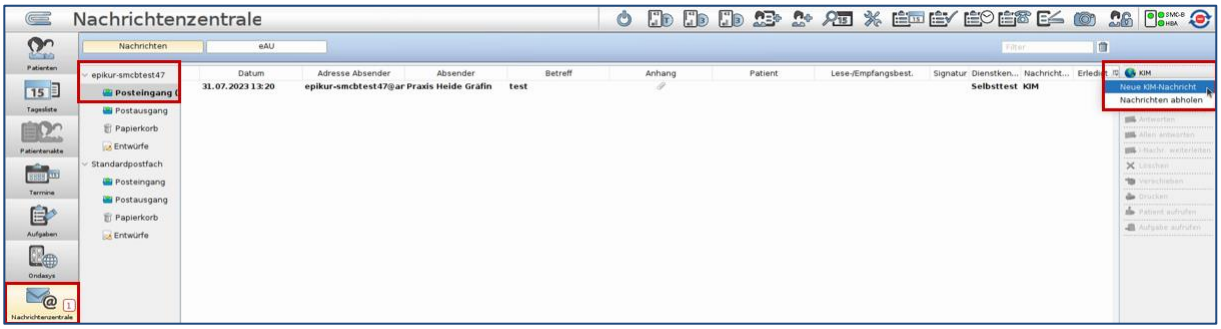
- Die folgende Popup-Meldung über „Nein“ bestätigen (1).



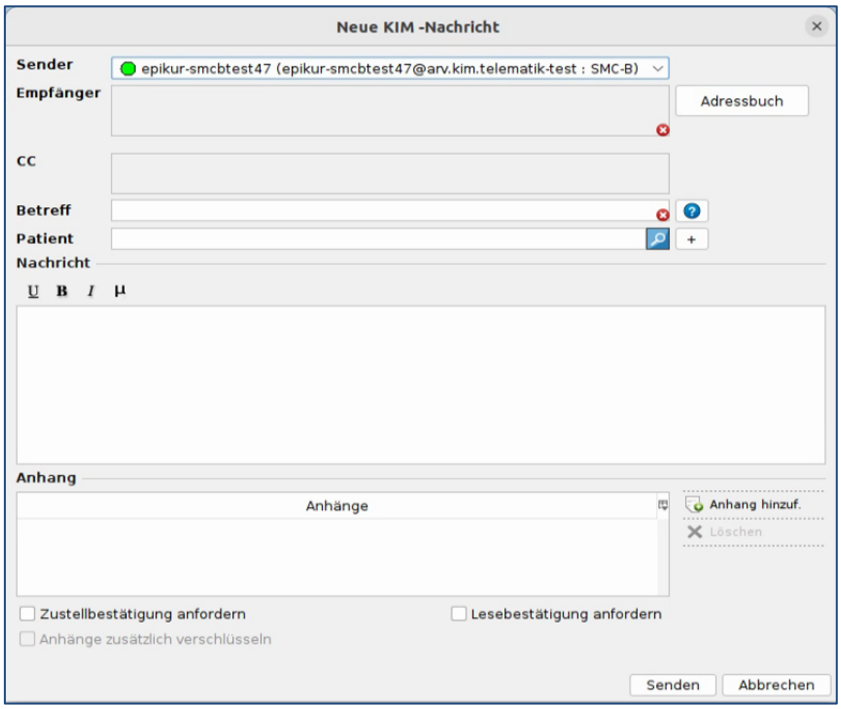
Automatisch (Über Kartensteckereignis)
Wird eine Karte in das Kartenlesegerät gesteckt, sollte sich der Aufnahme-Wizard automatisch öffnen.
Die Kartendaten sollten entsprechend hier auch nicht gespeichert werden.

11.6.3 KIM-Nachricht versenden

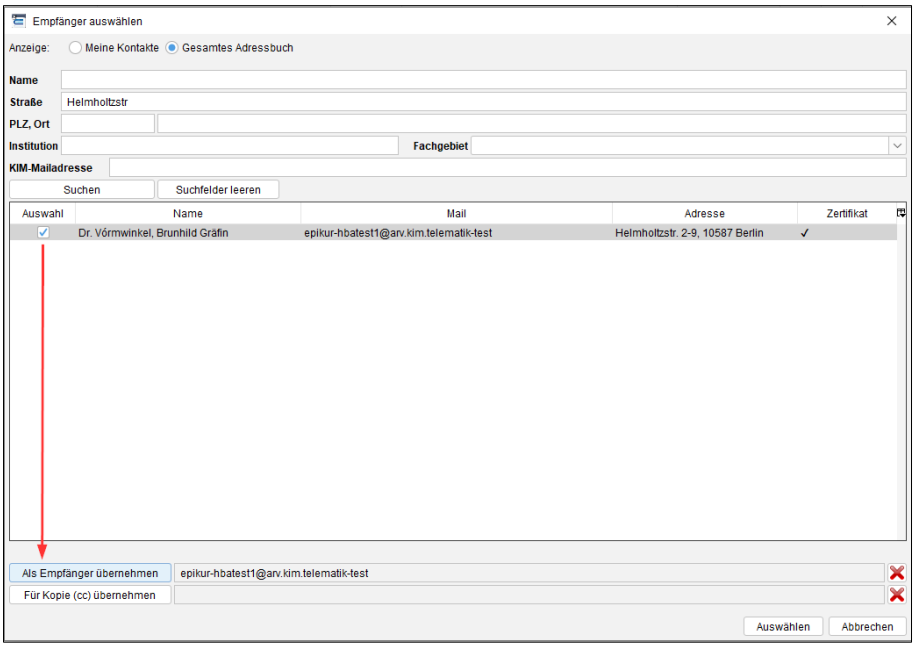
- Die „Nachrichtenzentrale“ von EPIKUR öffnen.
- KIM-Postfach auswählen durch Klick auf den Postfachnamen und „Neue KIM-Nachricht“ wählen.



- Zur Auswahl von Daten für die Felder „Empfänger“ auf den Button „Adressbuch“ klicken.



- In die Anzeige „Gesamtes Adressbuch“ wechseln.
- In das Feld „KIM-Mailadresse“ die KIM-Adresse des Postfachs eintragen (vgl. Screenshot davor in der Auswahl „Sender“.
- Über „Suchen“ die Suche starten.
- Gefundenen Eintrag auswählen.
- „Als Empfänger übernehmen“ klicken.
- „Auswählen“ klicken.



Es wird nun automatisch zum vorherigen Dialog zurückgekehrt.

- Der Nachricht einen Betreff „Test“ geben.
- Der Nachricht einen kurzen Inhalt geben (z. B. „Test123“).
- „Senden“ klicken.

Die Erwartung ist, dass die KIM-Nachricht erfolgreich versendet werden kann.

War der Versand erfolgreich, so ist der Abruf der KIM-Nachricht zu überprüfen.

- KIM -> Nachrichten abrufen (siehe erste Screenshot).

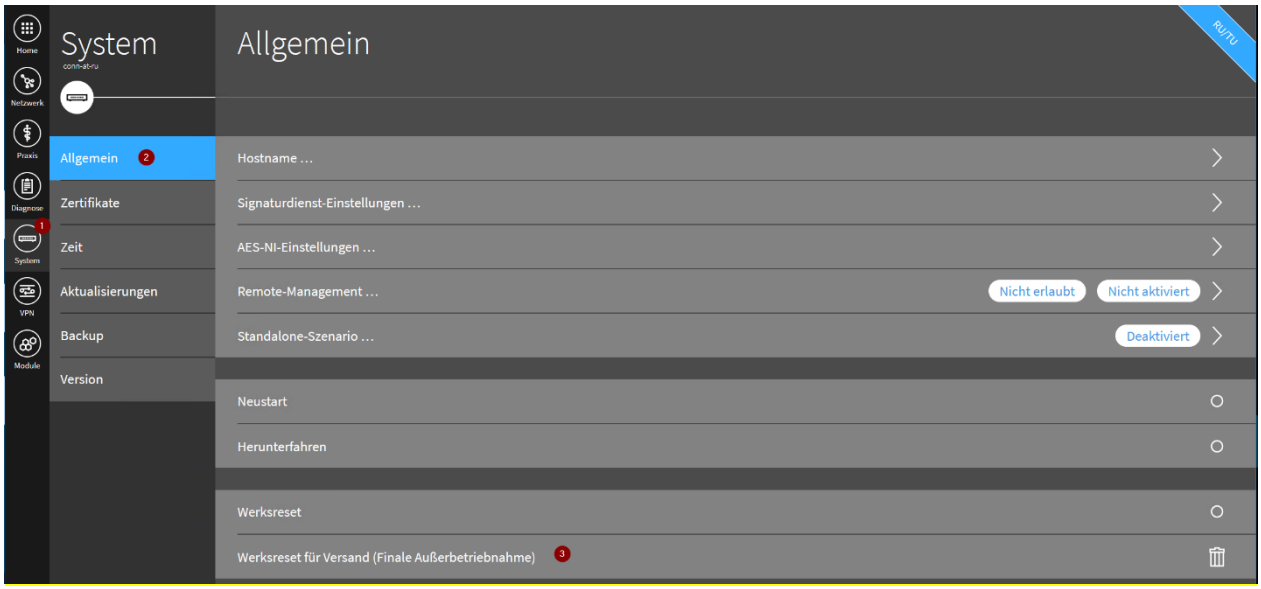
Die Erwartung ist, dass die zuvor versendete KIM-Nachricht erfolgreich abgerufen werden kann und in der Nachrichtenübersicht erscheint.

12 Finale Außerbetriebnahme vom Konnektor

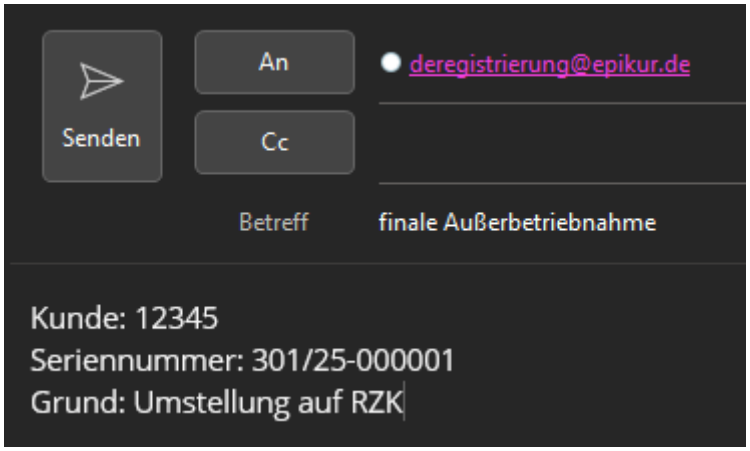
Dieser Schritt ist nur notwendig, wenn ein Umzug von Secunet auf TIaaS stattfindet.

Nach erfolgreichen Verbindungs-Tests kann der alte Secunet Konnektor final außer Betrieb genommen werden.

- Konnektor-Oberfläche erneut aufrufen.
- *System (1) → Allgemein (2)* öffnen.
- Klick auf „Werksreset für Versand (Finale Außerbetriebnahme)“ (3) und dessen Durchführung.



- Anschließend Konnektor vom Strom und LAN trennen.
- Hinweis: Bitte belassen Sie den final außer Betrieb genommenen Konnektor vor Ort.
- Der Konnektor muss vom Auftraggeber (Kunden) an Secunet gesendet werden. Hierfür wird diesem eine Versandmarke zur Verfügung gestellt.
- Hinweis: Eine Versandmarke kann erst erstellt werden, wenn die finale Außerbetriebnahme an den Epikur-Support gemeldet wird! Bitte teilen Sie mit, welches Gerät Sie zu welchem Zeitpunkt final außer Betrieb genommen haben. Geben Sie zudem bitte die Kundennummer, den Grund der Außerbetriebnahme sowie die Seriennummer des Geräts an und schicken Sie die E-Mail mit dem Betreff „finale Außerbetriebnahme“ an deregistrierung@epikur.de



13Einrichtung der WLAN-Geräte

Das neue WLAN-Netzwerk ist bei Bedarf auf allen WLAN fähigen Netzwerkgeräten zu hinterlegen, welche in dem sicheren Praxisnetz benötigt werden.

Das „alte“ WLAN des Routers kann der Kunde gerne deaktivieren, da alle Praxisgeräte nur noch über den AP verbunden sein sollten.

14Sonstige Netzwerkgeräte ändern

Abschließend gilt es alle weiteren Netzwerkgeräte zusammen mit dem Kunden auf die Funktionalität zu überprüfen.

Ggf. muss das Gerät neu gestartet werden, um sich eine neue IP-Adresse zu beziehen. Ist die IP-Adresse auf dem Gerät statisch gesetzt worden, so muss diese durch den Kunden auf das neue Netzwerk angepasst werden.

Im Speziellen ist hier an einen Netzwerk-Drucker zu denken.

Kurzleitfäden

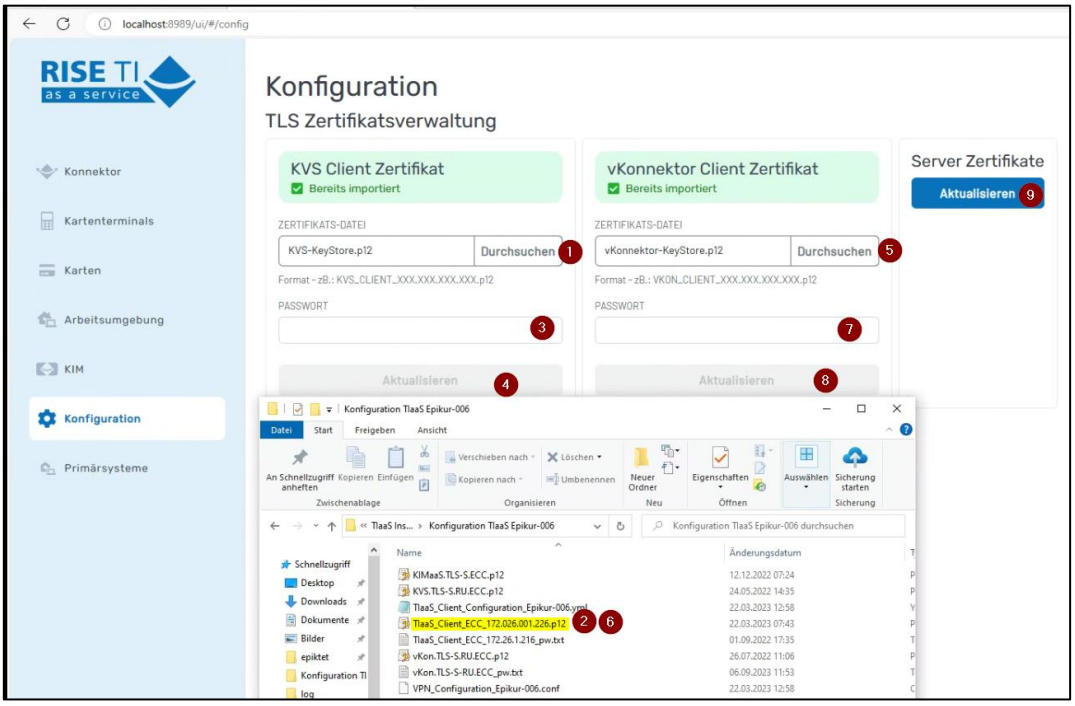
L.1 Kurzleitfaden: Umstellung TIaaS auf TIaaS mit LOOMA-Firewall

In diesem Abschnitt werden die notwendigen Schritte für den Umzug einer bestehenden TIaaS Installation auf eine mit LOOMA-Firewall beschrieben.

Anhang

A.1 Manuelles Einspielen der Zertifikate in den TIC

- KVS Client Zertifikat und vKonnektor Client Zertifikat ("TIaaS_Client_ECC_XXX.XXX.XXX.XXX.p12" → 1 Zertifikat für beide Clients) aus entpacktem Ordner "TIaaS_Config_Epikur-XXXX" auswählen (2,6), PW aus Datei im gleichen Ordner ("TIaaS_Client_ECC_XXX.XXX.XXX.XXX_pw.txt") rauskopieren → zum Öffnen der Datei ist Passwort/Bereitstellungscode für den Kunden notwendig, in TIC-Passwortfeld einfügen (3, 7) und auf Aktualisieren klicken (4, 8).
- Server Zertifikate -> „Aktualisieren“ klicken (9).



A.2 Pairing-Blöcke löschen

Sollte das Pairing fehlschlagen, sind möglicherweise schon alle Pairing-Blöcke im Terminal belegt. Hierzu können einzelne oder alle Pairings im ORGA 6141 online unter
Menü -> Einstellungen -> SICCT Parameter -> Pairings
gelöscht werden.

A.2 Admin Session konfigurieren

Die folgenden Einstellungen werden direkt am Kartenterminal vorgenommen.

- Am Kartenterminal auf „Menü“ drücken

- Zu „Einstellungen“ navigieren
- PIN für das Kartenterminal eingeben
- Zu „SICCT Parameter“ navigieren
- Zu „Zugriffsrechte“ navigieren
- Zu „Admin Session“ navigieren
- Auf „EIN“ setzen
- Zu “Download“ navigieren
- Auf „EIN“ setzen
- Auf „X STOP“ drücken
- Zu „Neustart“ navigieren und Neustart betätigen (OK)

Nachdem Ihr Kartenterminal sich neugestartet hat:

- Am Kartenterminal auf „Menü“ drücken
- Navigieren Zu „Einstellungen“ navigieren
- PIN für das Kartenterminal eingeben
- Zu „SICCT Parameter“
- Zu „Session Admin“ navigieren
- Neue PIN eingeben.

Hinweis: Diese PIN wird für die Konfiguration im TIC benötigt und sollte sich vom Kunden notiert werden.

A.3 Fehlerhandling Kartenterminal-Pairing

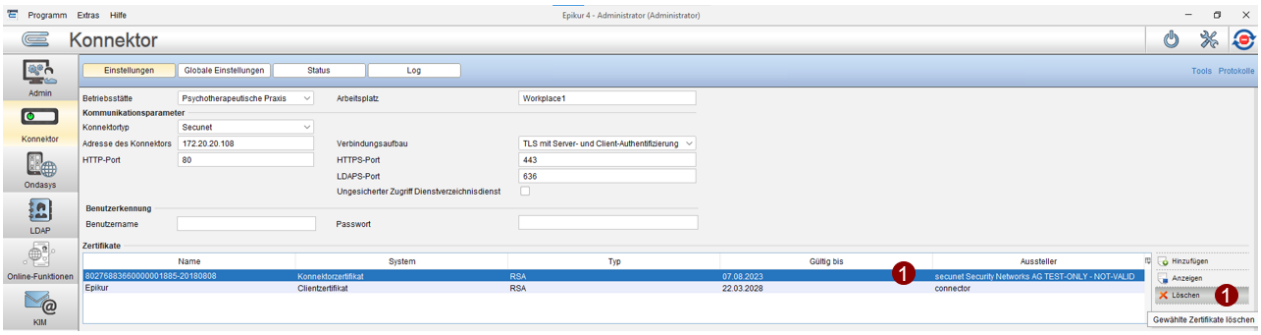
- Ist das KT via IP pingbar?
- Ist die Version des KTs >= 3.8.2?
- Ist die gSMC-KT noch gültig?
  Wenn die gSMC-KT abgelaufen ist, verweigert der Konnektor die Verbindung und das Pairing scheitert recht schnell. Wenn ein Pairing sehr schnell (wenige Sekunden) mit dem KVS-Fehler abbricht, ist das ein guter Hinweis darauf, dass die gSMC-KT abgelaufen sein könnte.
- KT neu starten.
- Überprüfen des Hostnames.
  Der Hostname darf keine ungültigen Zeichen enthalten (vor allem keine Leerzeichen am Ende). Auch, wenn ein generischer Name für ein KT vergeben wurde, kann es zu Problemen kommen, wenn ein KT auf dem betroffenen Konnektor schon den gleichen Hostnamen bekommen hat. Es empfiehlt sich, die Hostnamen möglichst einzigartig zu halten.
    - *Menü → Einstellungen (2) → Eingabe Amin-PIN (8-stellig) → LAN Parameter (1) → Gerätename (1)*

- Mit den Pfeiltasten bis ganz ans Ende navigieren.
- Mit “Clear” Leerzeichen löschen.
- Mit “OK” bestätigen.
- KT neustarten.

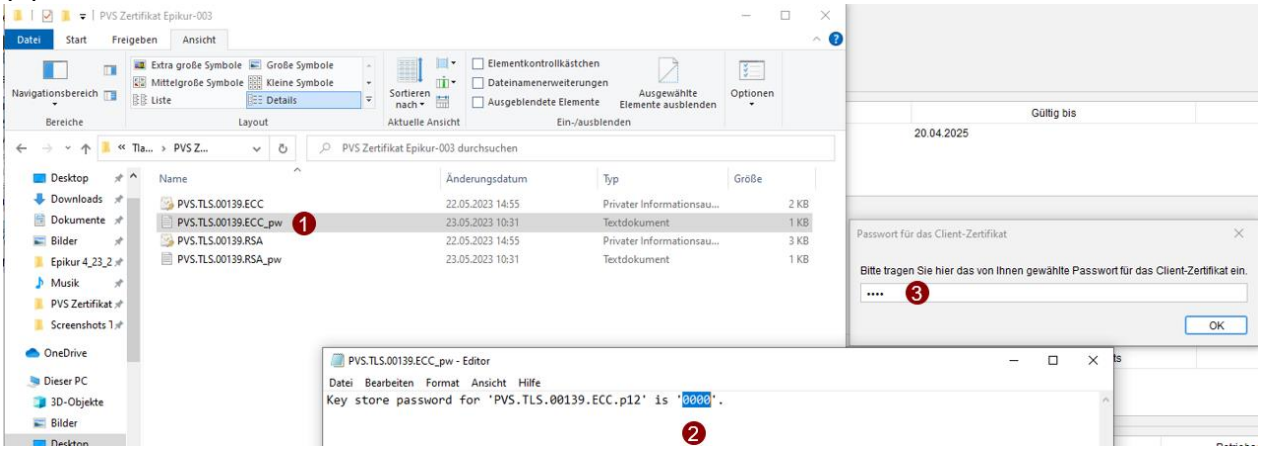
- KT zurücksetzen
  - *Menü → Service (3) → Werkseinstellungen (3) → via Admin-PIN (1) → Eingabe Amin-PIN (8-stellig) → Bestätigen*
  - KT setzt sich zurück.
  - Admin-PIN 2x eingeben.
  - Bestätigen.
  - Statische IP-Adresse erneut setzen.

A.3 Manueller Import der Zertifikate

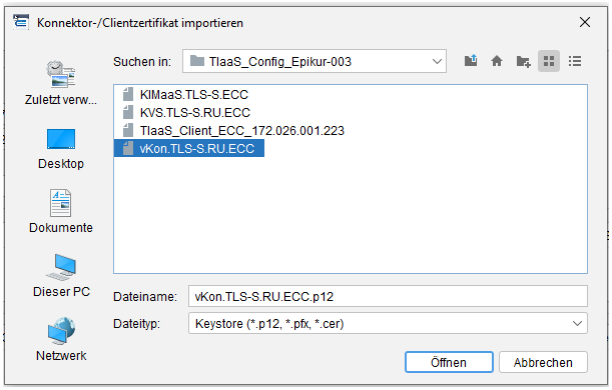
- Alle Zertifikate löschen: Jeweils das vorhandene Zertifikat auswählen (1) und löschen (2), bis alle Zertifikate entfernt sind.



Beim Import der Zertifikate ist eine Passwort-Eingabe notwendig. Das Passwort ist jeweils in einer Textdatei (1) gespeichert, welche neben dem Zertifikat liegt. Das Passwort (2) kann so kopiert und bei der Abfrage durch EPIKUR eingefügt werden (3).



- Neue Zertifikate (RSA-Client-Zertifikat, ECC-Client-Zertifikat, ECC-Konnektor-Zertifikat) aus dem entpackten Config-ZIP einspielen:
    - Für jedes Zertifikat bei der Tabelle Zertifikate auf „Hinzufügen“ klicken,
    - Das Konnektor-ECC-Zertifikat (vKon.TLS-S.PU.ECC.p12) aus entpacktem Ordner "TIaaS_Config_Epikur-XXXX" (,welcher in dem entpackten Ordner “TIC-Installationspaket_Epikur-XXXX” liegt,) auswählen für den Import. → Passwort ist für alle Kunden "000000" (6x Null),



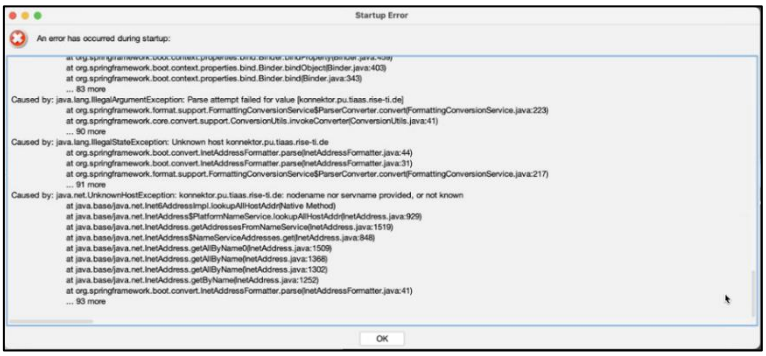
    - Das Client-ECC-Zertifikat (PVS_ECC_client-XXXXX.konlan.p12) und das Client RSA-Zertifikat (PVS_RSA_client-XXXXX.konlan.p12) aus dem Ordner "PVS Zertifikat Epikur-XXXX" (,welcher in dem entpackten Ordner “TIC-Installationspaket_Epikur-XXXX” liegt,) importieren.
        - Stehen mehrere Zertifikate in dem Ordner „PVS Zertifikat …“ zur Auswahl, so ist das Zertifikats-Paar (RSA, ECC) mit der niedrigsten Nummer zu wählen.
          Hintergrund: Die hinterlegten Zertifikate werden von jedem Client genutzt und können/müssen nur einmal hinterlegt werden.
- Nachdem die Kommunikationsparameter eingestellt wurden und alle 3 Zertifikate importiert sind, kann auf „Speichern“ geklickt werden.
  → Verbindung zum Konnektor und KT sollte aufgebaut werden können.

A.4 DNS-Rebind-Schutz

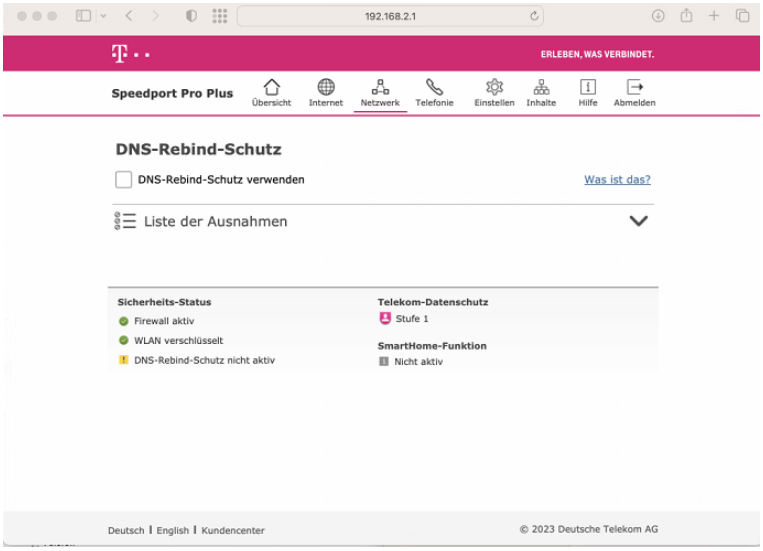
Speedport-Router (Telekom) haben ggf. einen DNS-Rebind-Schutz konfiguriert, welcher die Auflösung der RISE-URLs blockiert.

Mögliche Auswirkungen

Der TIC stürzt bspw. beim Start mit der folgenden Fehlermeldung ab.



Lösung
DNS-Rebind-Schutz im Speedport in der Ansicht Netzwerk deaktivieren oder eine Ausnahme für die URLs (*.rise-ti.de) hinzufügen.



A.5 DNS-Server ändern

Mögliche Auswirkungen

- DNS-Adressen lassen sich nicht auflösen.
- TIC sagt, dass keine Verbindung zum vKonnektor hergestellt werden kann.

Lösung
Setzen des DNS-Servers auf 8.8.8.8

Bei einer FritzBox ist dieses unter "Internet -> Zugangsdaten -> DNS Server" möglich.
Bei einem SpeedPort kann es teilweise über die Zugangsdaten eingestellt werden.

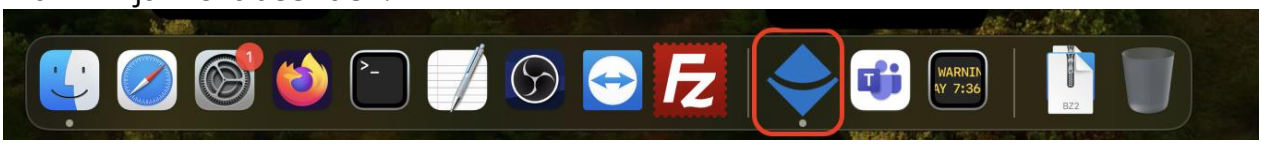
Sollte die Einstellung nicht direkt im Router vorgenommen werden können, so kann

der DNS-Server in den Netzwerkeinstellungen vom Betriebssystem gesetzt werden. Diese Anpassung ist dann allerdings auf allen Clientsystemen notwendig, die sich mit dem Rechenzentrumskonnektor verbinden möchten.

A.6 Neustart TIC

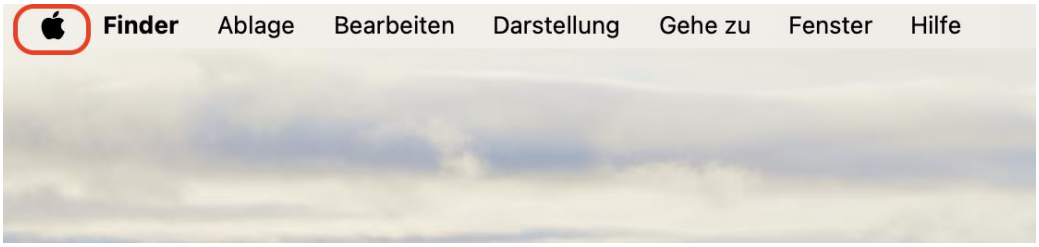
Unter MacOS (Standardinstallation)

Zuerst einmal ist wichtig zu erkennen, ob der TIC überhaupt aktiv läuft, sonst muss man ihn ja nicht beenden:



→ hier sieht man im rot markierten Bereich in der sog. „Dock-Leiste“ am unteren Rand einen kleinen grauen Punkt, der anzeigt, dass das Programm aktiv läuft
Achtung: die Dock-Leiste kann ähnlich, wie in Windows ausgeblendet sein und wird erst sichtbar, wenn man den Mauszeiger an den Fensterrand bewegt; ggf. kann die Dockleiste auch vertikal angeordnet sein

- Auf den „Apfel-Button“ oben links (in allen macOS-Versionen gleich) klicken

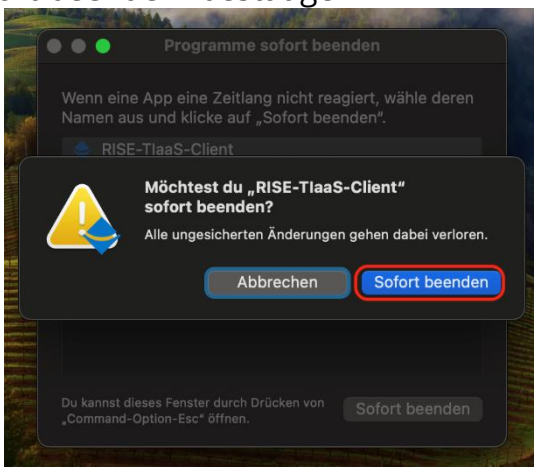


- Im Drop-Down-Menü auf den Eintrag „Sofort Beenden“ klicken

- Programm „RISE-TIaaS-Client“ auswählen (1)

- Auf „Sofort beenden“ klickten (2)

- Meldung mit „Sofort beenden“ bestätigen



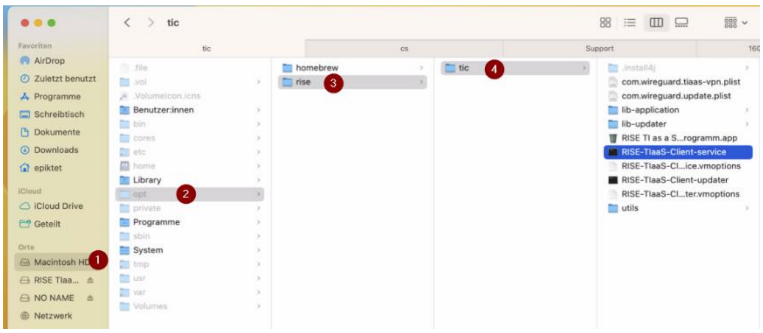
Daraufhin sollte nach ggf. kurzer Wartezeit in dem „Sofort Beenden“-Fenster der Eintrag für das Programm RISE-TIaaS-Client verschwinden:

und in dem Dock-Leisten-Eintrag des Programms sieht man keinen kleinen grauen Punkt mehr unterhalb des Programm-Icons

- Über einen Klick auf das Icon in der Dock-Leiste kann der TIC wieder gestartet werden.
  Alternativ kann die Anwendung aus Programme -> RISE-TIaaS-Client gestartet werden.

Unter MacOS (Dienst)

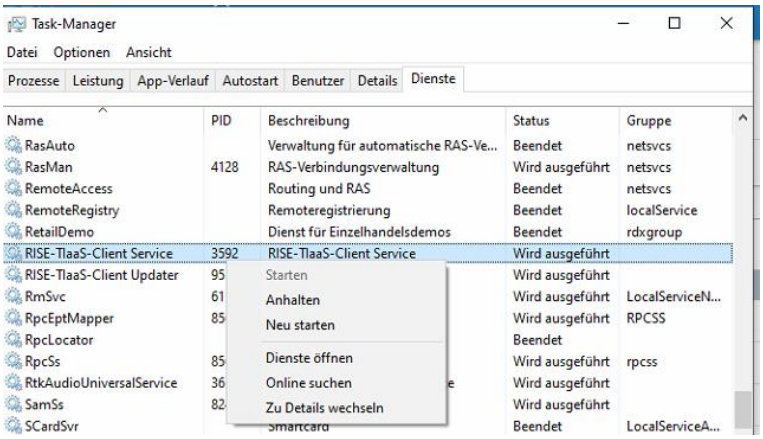
- Die App „Aktivitätsanzeige“ öffnen
- Dienst beenden
- Finder öffnen
- Ggf. Versteckte Ordner/Dateien einblenden [CMD] + [SHIFT] + [.]
- Navigation via zu /opt/rise/tic
- RISE-TIaaS-Client-service starten



Wenn Dienst nicht aufgeführt: Neustart über Weboberfläche vom TIC

Unter Windows (Dienst)

- Taskmanager öffnen
- In Reiter „Dienste“ wechseln
- Eintrag „RISE-TIaaS-Client-Service“ suchen
- Rechtsklick auf Eintrag
- „Neustarten“ auswählen



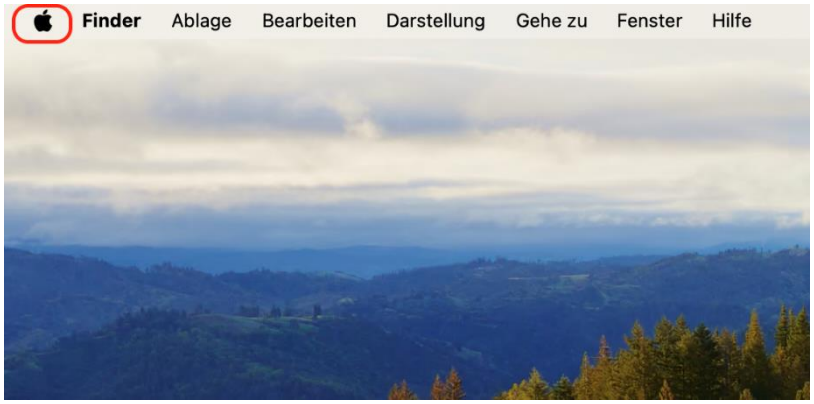
A.7 Einrichtung des Festplattenvollzugriffs für EPIKUR unter MacOS

Wichtig im Folgenden ist, dass man hierfür administrative Berechtigungen benötigt, sodass ein nicht privilegierter Benutzer die Eingabe nicht tätigen kann!

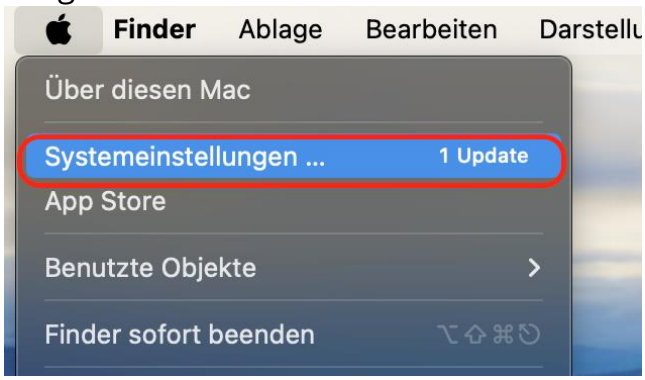
Außerdem wird im Folgenden exemplarisch die Einrichtung für die EPIKUR4-Einzelplatzvariante gezeigt, funktioniert aber analog auch für die Netzwerkvariante, in der man jedoch den EPIKUR4-Client (nicht den EPIKUR4-Server) hinterlegt

Achtung: diese Anleitung wurde zwar mit macOS 14 erstellt, allerdings sah es in früheren macOS-Versionen (vor macOS 13) noch ein wenig anders aus, sodass damals keine Listenansicht (da für Mobil, also iOS, optimiert/vorbereitet) für die versch. Einstellungsbereiche existierte, sondern eine Symbol-Ansicht.
Die für diese Anleitung relevante Einstellungskategorie hieß aber auch damals schon so, wie sie bis einschl. macOS 14 heißt. Ggf. kann man im Einstellungsfenster aller Betriebssysteme auch konkrete Begriffe (z.B. „Datenschutz“ oder „Festplattenvollzugriff“) suchen via Suchleiste innerhalb des Fensters i.d.R. oben rechts, falls die Bebilderungen unten nicht ausreichen.
Innerhalb der Einstellungskategorie „Datenschutz & Sicherheit“ sieht es dann wiederum sehr ähnlich aus in einer Liste von Einstellungsmöglichkeiten

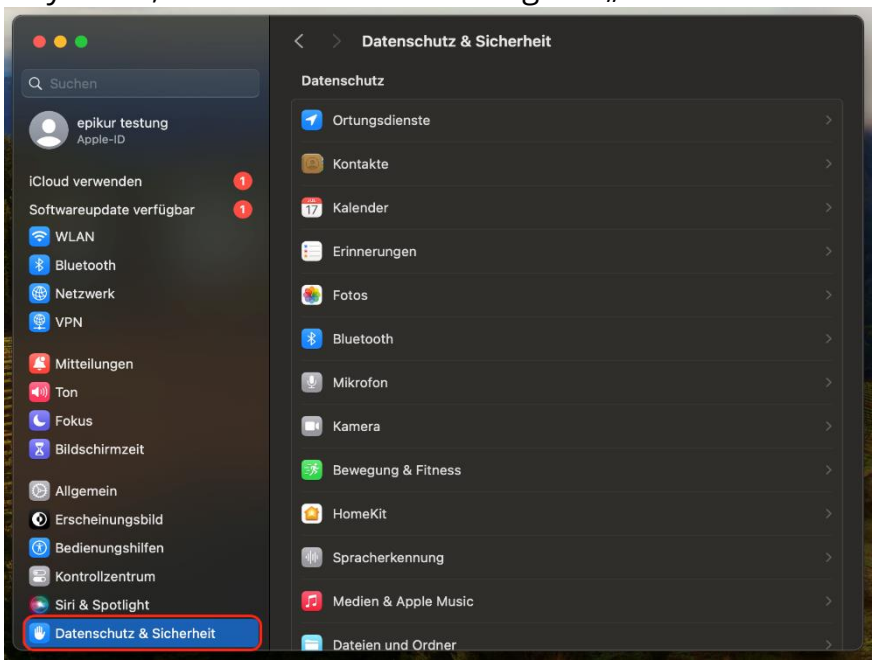
Die Systemeinstellungen müssen aufgerufen werden, wofür es versch. Wege gibt; in allen macOS-Versionen oben links findet man den im Folgenden sichtbaren Apfel-Button, den man klickt:



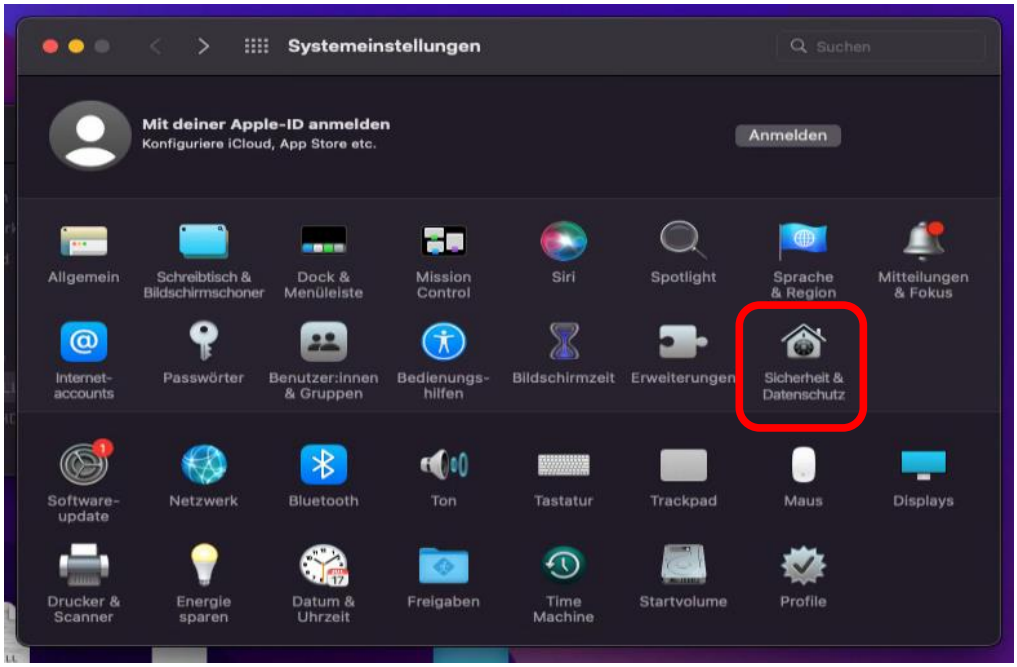
- Im sich daraufhin öffnenden Drop-Down-Menü klickt man auf „Systemeinstellungen“



- Daraufhin öffnet sich die gesuchte Einstellungsoberfläche des Betriebssystems; hier wählt man die Kategorie „Datenschutz & Sicherheit“:

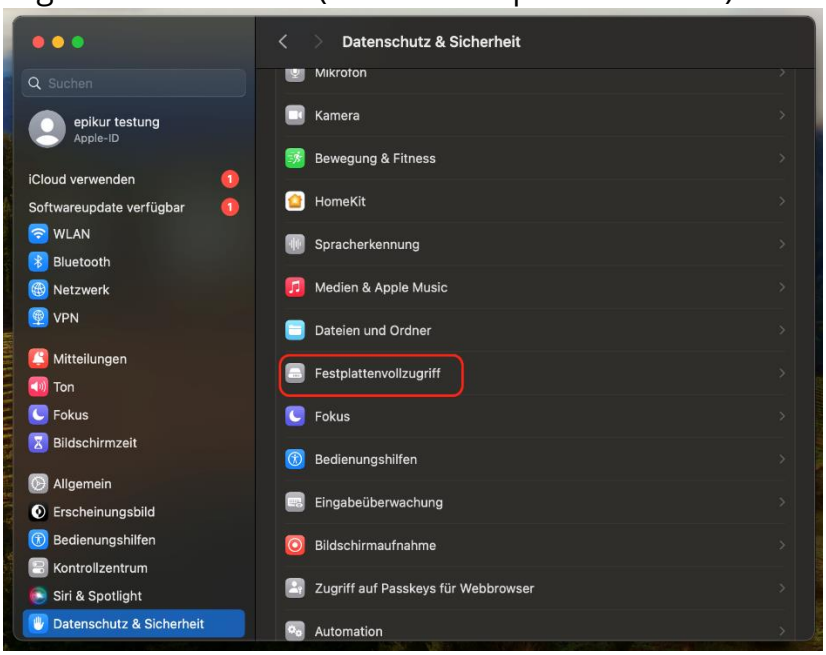


→ hier als Darstellung in macOS 13 und macOS 14



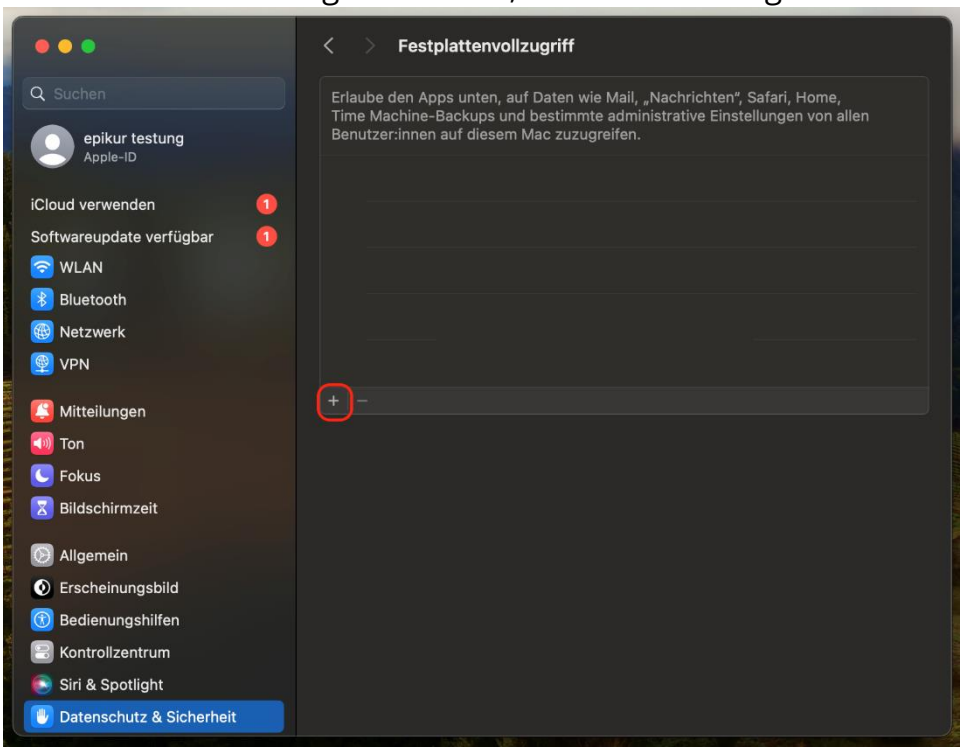
→ hier als Darstellung in macOS 12 (und ältere Versionen sehen sehr ähnlich aus); hier muss man dann in der aufgerufenen Einstellungskategorie auf das Schloss-Symbol unten links klicken und das Admin-User-Passwort eingeben und kann dann in den Reiter „Datenschutz“ wechseln

Nachdem nun die passende Kategorie aufgerufen wurde, sollte in etwa wie folgt (in älteren Versionen als macOS 13 sehr ähnlich) eine Auswahl von konkreten Datenschutzkategorie sichtbar sein (hier am Beispiel macOS 14):



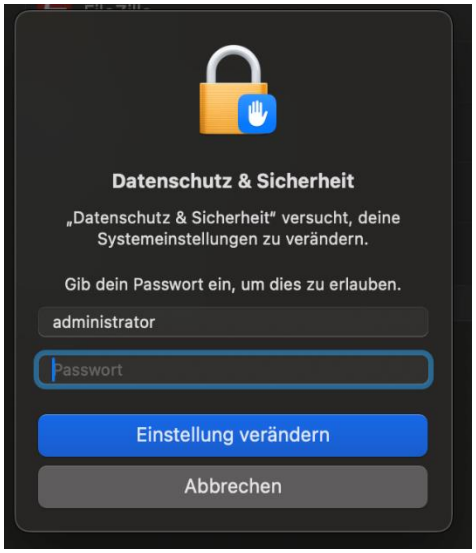
→ hier wählt man nun „Festplattenvollzugriff“ ausgeblendet

Nachdem dies getan wurde, sieht das wie folgt aus:



→ hier klickt man auf den Plus-Symbol-Button

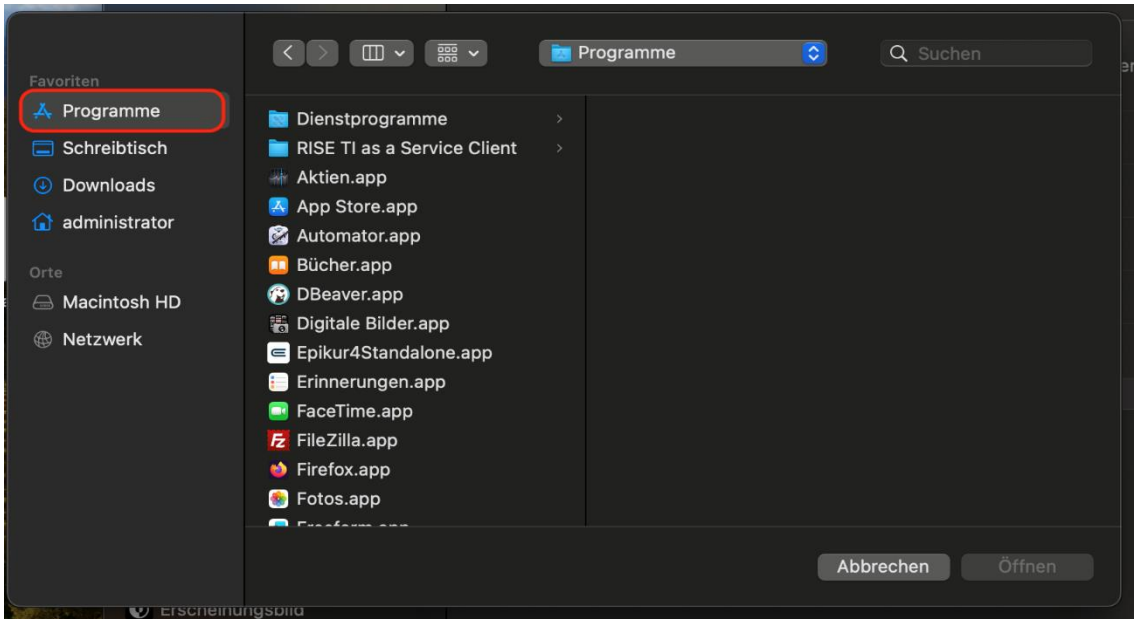
Nun sollte die Admin-Benutzer-Passwort-Abfrage erscheinen (nur in macOS 13 aufwärts, in älteren macOS-Versionen war das anders zu lösen; siehe oben):



→ hier gibt man die entsprechenden Daten ein: der Endanwender sollte natürlich nicht nur das Passwort seines Benutzers kennen, sondern auch wissen, ob sein Benutzer, der hier im Screenshot voreingestellt ist, aber nicht zwangsläufig korrekt sein muss, auch wirklich die Admin-Kompetenz hat (dies stellt man in einer anderen

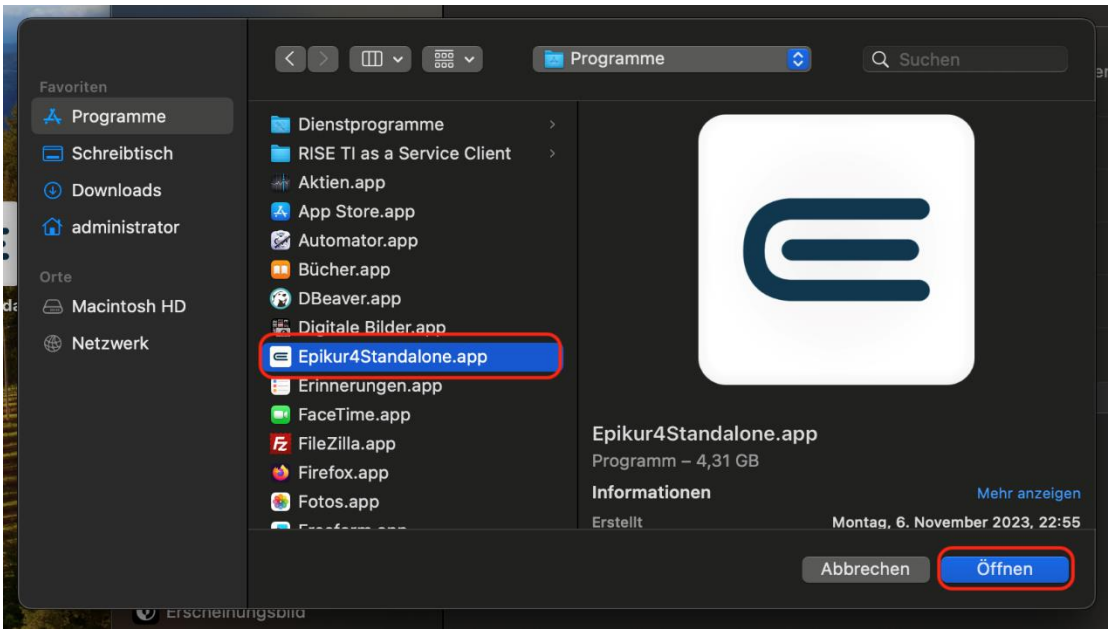
Systemeinstellungskategorie „Benutzer:innen & Gruppen“ ein, wo der Benutzer die Eigenschaft „Benutzer:in darf diesen Computer verwalten“ haben muss)

Sollte die Eingabe erfolgreich gewesen sein, müsste folgender Dateiauswahl-Dialog angezeigt werden, in dem man das Programm selbst aufrufen muss (standardmäßig ist das im sog. Programme-Verzeichnis zu finden, aber grundsätzlich könnte das Programm auch auf dem „Schreibtisch“ oder irgendwo anders liegen, denn schlussendlich ist das nur ein ausführbarer Ordner (eine macOS-Besonderheit)):



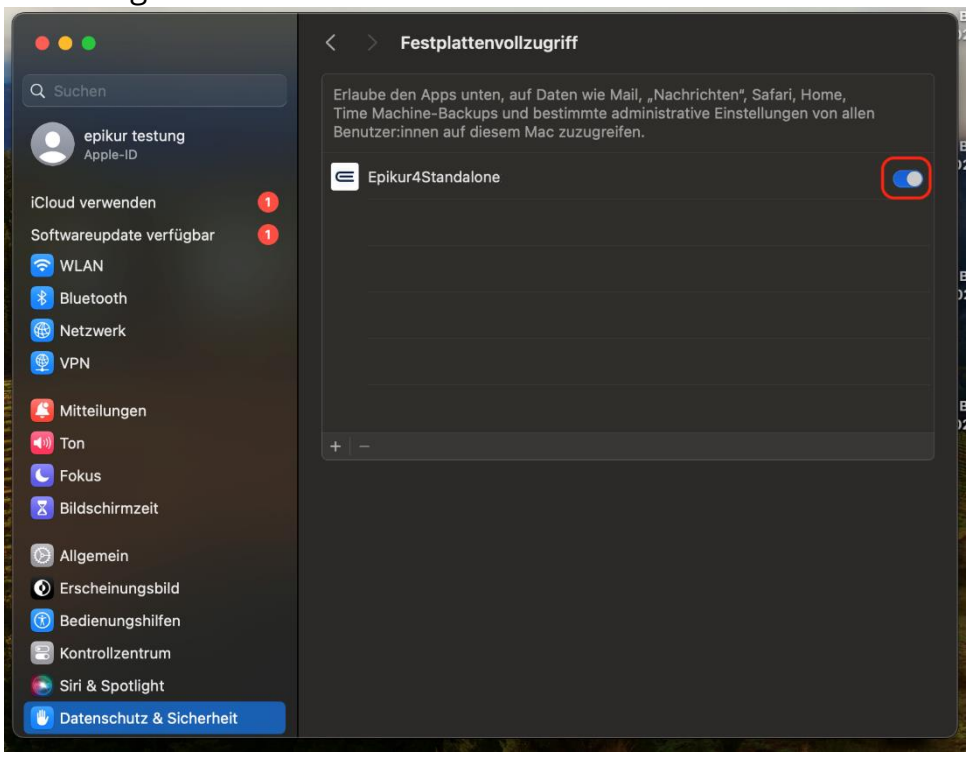
→ hier wird „Programme“ ausgewählt, sodass man alle Programme sieht

Im Anschluss wählt man den passenden Eintrag aus (EP: „Epikur4Standalone“, NW: „Epikur4“ für den Client) und klickt „Öffnen“:



-> ob dort am Programmnamen noch „.app“ dranhängt oder nicht spiel keine Rolle und ist nur eine einstellbare Anzeigeeigenschaft

Nun sollte das Programm in der Liste auftauchen:



→ der rot markierte Schalter ist wichtig und sollte einen aktiven Zustand darstellen
→ falls der Schalter nicht aktiv ist, dann muss dieser noch aktiviert werden

Zuletzt sollte EPIKUR komplett beendet werden und dann wieder gestartet werden; dann greift diese Einstellung auch wirklich (zur Not tut es auch ein kompletter Rechnerneustart)