CHECKLISTE

Vorbedingungen zur Anbindung an das TI-Gateway von AKQUINET

Folgende Punkte sind zur Anbindung an das TI-Gateway Voraussetzung bzw. vor dem Installationstermin zu beschaffen. Bitte ziehen Sie Ihren IT-Dienstleister oder IT-Verantwortlichen zur Beschaffung der Informationen und zur Teilnahme am Anbindungstermin hinzu. Sollte der Termin wegen fehlender Mitwirkungspflicht des Kunden nicht erfolgreich sein, wird der nachfolgende Termin kostenpflichtig.

	THEMA	ANMERKUNG
1	Rechner mit Admin-Zugang	Sie benötigen die Adminrechte für den Rechner, um eine Software herunterladen und installieren zu dürfen.
2	Authenticator App für Multi-Faktor-Authentifizierung (MFA)	Es ist sinnvoll, die Authenticator App nicht auf einem Handy, sondern auf dem Rechner zu installieren, damit mehrere Mitarbeitende darauf zugreifen können. • Vorschlag für Apple-Rechner mit macOS-Betriebssystem: TOTP Authenticator - 2FA Authentifizierungs App • Vorschlag für Computer mit Windows-Betriebssystem: TOTP Authenticator - 2FA with local Sync & Widgets
3	Login-Daten für Ihren Internet-Router	Abhängig davon, welchen Router Sie einsetzen, kann es notwendig sein, Ihren Internetprovider zu kontaktieren.
4	Login-Daten für die TI-Einstellung in Ihrem PVS / AVS / KIS System	Sie können Ihren Anbieter alternativ auch gerne zum Termin einladen.
5	Admin-PIN für Ihre Kartenlesegeräte	Ob Sie die richtige PIN haben, können Sie überprüfen, indem Sie über das Menü des Kartenlesegerätes in die Einstellungen navigieren. Hier werden Sie nach dem PIN gefragt. Orga: Menü → 2. Einstellung Cherry: Menü → Admin-Menü
6	Freigeschaltete SMC-B Karte inkl. PIN und PUK muss vorhanden sein	Die Karte muss nach erfolgter Umstellung auf das TI-Gateway einmal neu verifiziert werden. **Hinweis**: Nach Erhalt der Karte muss diese im Portal des Kartenherausgebers freigeschaltet worden sein.
7	Zugang zum KIM-Clientmodul (URL und Port)	Auch im KIM-Clientmodul müssen die neuen Konnektordaten eingetragen werden. Hierfür ist Zugang zum Konfigurationsmenü notwendig.
8	Zugangsdaten zum Konnektor	Bei **Secunet** Konnektor: Backup des Konnektors inkl. Passwort
9	Sicherstellen, dass alle Kartenleser die aktuelle Firmware haben	• Orga - 3.9.0 • Cherry - 4.0.25
10	Für die Fernwartung durch das Support-Team bitte zum Termin die Fernsteuerungssoftware „Rustdesk“ installieren	• Für Windows nutzen Sie bitte den Link RustDesk_Windows mit dem Kennwort **15#qqbqK** • Für Linux nutzen Sie bitte den Link RustDesk_Linux-Ubuntu mit dem Kennwort **m^hB4hr8** • für Mac nutzen Sie bitte den Link RustDesk_MAC mit dem Kennwort **`F3g1cbk**

Vorbereitung für Ihren Installationstermin für das TI-Gateway (TIG)

Damit Ihre Konnektorinstanz erfolgreich und sicher an das TI-Gateway (TIG) angebunden werden kann, führen Sie bitte die folgenden Schritte sorgfältig und in der angegebenen Reihenfolge durch. Diese Checkliste unterstützt Sie dabei, alle notwendigen Vorbereitungen vollständig und nachvollziehbar zu treffen.

---

1. Registrierung im TI-Gateway Portal https://ti-gateway.akquinet.de

Ihr Zugang zur Telematikinfrastruktur beginnt mit der Registrierung im sogenannten "TI-Gateway Portal" – dem zentralen Einstiegspunkt für das weitere Onboarding.

- Von uns erhalten Sie eine E-Mail mit einem persönlichen Einladungslink zum TI-Gateway Portal.
- Das TI-Gateway Portal ist Ihre zentrale Plattform für:
  - die Registrierung und Verwaltung Ihres Benutzerkontos,
  - das sichere Login über Zwei-Faktor-Authentifizierung,
  - sowie den späteren Zugriff auf Ihre Konnektorinstanz.

Was ist zu tun?

1. Öffnen Sie den Einladungslink in einem aktuellen Webbrowser (z. B. Google Chrome, Firefox).
2. Erstellen Sie ein Benutzerkonto:
   - Vergeben Sie ein sicheres Passwort (mindestens 12 Zeichen, Kombination aus Buchstaben, Zahlen und Sonderzeichen).
   - Aktivieren Sie die Zwei-Faktor-Authentifizierung (TOTP = Time-based One-Time Password), z. B. mit einer Authenticator-App auf Ihrem Rechner oder Smartphone.

Nach erfolgreicher Registrierung ist Ihr Zugang zum TI-Gateway Portal eingerichtet und Sie können mit dem nächsten Schritt fortfahren.

---

2. TI-Gateway Key installieren und einrichten

Der "TI-Gateway Key" ist eine lokale Desktop-Anwendung, mit der Sie Ihre Konnektorinstanz verwalten. Er muss auf einem Rechner in Ihrer Einrichtung (z. B. in der Arztpraxis) installiert werden.

Wofür ist der TI-Gateway Key da?

- Durchführung des Onboardings Ihrer Konnektorinstanz
- Technische Prüfung und Administration Ihrer Konnektoren
- Aufbau eines sicheren Kommunikationskanals zur Telematikinfrastruktur

So gehen Sie vor:

1. Laden Sie die passende Version des TI-Gateway Keys herunter (Downloadlink erhalten Sie von uns nach Versand der Firewall; verfügbar für Windows, macOS und Linux).
2. Installieren Sie die Anwendung auf einem Computer, der mit Ihrem Praxisnetzwerk verbunden ist.
3. Starten Sie den TI-Gateway Key. Klicken Sie auf den Button „Mit TI-Gateway Portal einloggen“.
4. Es öffnet sich ein Browserfenster: Melden Sie sich dort mit Ihren Zugangsdaten aus Schritt 1 an (Passwort + TOTP).
5. Danach kehrt die Anwendung automatisch in den Vordergrund zurück.
6. Legen Sie nun ein Wiederherstellungspasswort fest. Dieses benötigen Sie, falls das System zurückgesetzt werden muss – bewahren Sie es sicher auf (z. B. im Passwortmanager).

Nach erfolgreicher Anmeldung sehen Sie ggf. bereits eine Ihrer Konnektorinstanzen im System. Bevor Sie diese in Betrieb nehmen, müssen die Netzwerkinfrastruktur und die Hardware eingerichtet sein.

---

3. Hardware vorbereiten

3.1 Kartenterminals anschließen

Ein Kartenterminal ist ein Gerät, in das sogenannte SMC-Karten (elektronische Sicherheitskarten) gesteckt werden. Diese Karten identifizieren Ihre Einrichtung im System der Telematikinfrastruktur und ermöglichen die sichere Authentifizierung.

Sie benötigen:

- Ein oder mehrere Kartenterminals
- Eine SMC-B-Karte (für Leistungserbringer)
- Eine gSMC-KT-Karte (für das Kartenterminal selbst)
- Netzteil und Netzwerkkabel

So schließen Sie alles richtig an:

1. Stecken Sie die SMC-B-Karte (Institutionenkarte) in das Kartenterminal. Versiegeln Sie diese ggf. mit einem Schutzsiegel laut Herstellerangaben.
2. Verbinden Sie das Kartenterminal mit dem Netzteil und schließen Sie es an die Stromversorgung an.
3. Stecken Sie nun die gSMC-KT-Karte in das Terminal und versiegeln Sie auch diese.
4. Verbinden Sie das Kartenterminal mit einem Switch oder Router im selben lokalen Netzwerk wie die Fortigate 40F und der PC mit TI-Gateway Key.
5. Prüfen Sie über das Gerätemenü oder die Herstellerdokumentation, ob:
    - die aktuellste Firmware installiert ist,
    - die TSL-Liste (Trust Service List) aktuell und aktiviert ist.
6. Prüfen Sie, ob ausreichend freie Pairing-Blöcke vorhanden sind (notwendig für die Verbindung mit dem Konnektor). Löschen Sie ggf. nicht mehr benötigte Pairings (siehe Wissensdatenbank des Herstellers).

Hinweis: Die Kartenterminals dürfen nicht direkt an einen LAN-Port der Fortigate 40F angeschlossen werden.

3.2 Fortigate 40F anschließen

Die Fortigate 40F ist eine speziell konfigurierte Firewall, die die VPN-Verbindung zur Telematikinfrastruktur aufbaut.

So verbinden Sie die Fortigate korrekt:

1. Schließen Sie die Fortigate 40F an die Stromversorgung an.
2. Verbinden Sie den **WAN-Port** der Fortigate 40F mit Ihrem Switch oder Router.

Die Fortigate bezieht automatisch ihre Konfiguration über die FortiCloud und stellt anschließend eine VPN-Verbindung zum sogenannten "TI-Gateway Gate" her – dem gesicherten Einstieg in die TI.

Wichtig: Stellen Sie sicher, dass die Fortigate Internetzugang hat. Die Konfiguration und Aufbau der VPN-Verbindung kann 5–10 Minuten dauern.

---

4. VPN-Verbindung prüfen

Sobald die Fortigate läuft, können Sie im TI-Gateway Portal überprüfen, ob die VPN-Verbindung korrekt aufgebaut wurde.

So prüfen Sie die Verbindung:

1. Loggen Sie sich im TI-Gateway Portal ein.
2. Navigieren Sie zum Menüpunkt „VPN-Zugänge“.
3. Sehen Sie dort nach, ob die Verbindung als aktiv angezeigt wird.

Falls keine Verbindung besteht:

- Prüfen Sie die Internetverbindung der Fortigate.
- Vergewissern Sie sich, dass das Netzwerkkabel im richtigen Port steckt (WAN-Port).
- Warten Sie ein paar Minuten und klicken Sie auf „Liste aktualisieren“.

---

5. Routing einrichten

Damit der Datenverkehr aus Ihrem lokalen Netzwerk über die Fortigate zur Telematikinfrastruktur (TI) geleitet wird, müssen sogenannte statische Routen eingerichtet werden. Dies kann im Router oder in der Firewall geschehen.

Was ist eine Route?

Eine Route legt fest, über welches Gerät ein bestimmter Netzwerkverkehr gesendet wird. In unserem Fall sollen Anfragen an die TI-Adressen immer über die Fortigate geleitet werden.

So richten Sie das Routing ein:

1. Öffnen Sie die Administrationsoberfläche Ihres Routers oder Ihrer Firewall.
2. Ermitteln Sie die aktuelle IP-Adresse der Fortigate 40F (diese wurde per DHCP vergeben).
3. Reservieren Sie diese IP-Adresse dauerhaft (statische Zuordnung), damit sich die Fortigate nicht ändert.

Nun richten Sie folgende Routen ein:

ZWECK	NETZWERK/DESTINATION	SUBNETZMASKE	GATEWAY
Konnektornetz	100.106.0.0	255.255.240.0	lokale Forti-IP
Offene Fachdienste	100.102.0.0	255.255.0.0	lokale Forti-IP

Alternativ: Lokale Routen direkt auf den Clients setzen

Wenn Sie keine Änderungen im Router vornehmen möchten oder können, können die Routen auch direkt auf dem betroffenen Rechner gesetzt werden.

Windows (PowerShell als Administrator):

route add -p 100.106.0.0 MASK 255.255.240.0 {lokale Forti-IP}
route add -p 100.102.0.0 MASK 255.255.0.0 {lokale Forti-IP}

macOS (Terminal):

sudo route -n add -net 100.106.0.0/20 {lokale Forti-IP}
sudo route -n add -net 100.102.0.0/16 {lokale Forti-IP}

Hinweis: macOS speichert Routen nicht dauerhaft. Verwenden Sie ein Startskript, um die Routen nach jedem Neustart automatisch zu setzen.

Linux:

sudo ip route add 100.106.0.0/20 via {lokale Forti-IP}
sudo ip route add 100.102.0.0/16 via {lokale Forti-IP}

Abschluss

Wenn Sie alle beschriebenen Schritte erfolgreich durchgeführt haben, ist Ihre IT-Umgebung vollständig für die Anbindung an das TI-Gateway vorbereitet. Die finale Einrichtung und Inbetriebnahme Ihrer Konnektorinstanz kann nun erfolgen.

Sollten Sie bei einem Schritt unsicher sein oder technische Schwierigkeiten auftreten, zögern Sie nicht, unseren technischen Support zu kontaktieren. Wir unterstützen Sie gerne persönlich.

Wir gehen davon aus, dass Sie als Apotheke die RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT erfüllen.