

FEHLERBEHEBUNG UNTER E-CONNECT 2.0 FÜR SYSTEMBETREUER

Version: 1.0



Inhaltsverzeichnis

1.	Einleitung	1
2.	Allgemeine Informationen und Voraussetzungen	2
2.1.	Sofortmaßnahmen zur Fehlerbehebung	2
2.2.	Am vKonnektor anmelden	2
2.3.	e-connect im DS-Win	2
2.4.	e-connect im DS4	3
3.	Gezielte Fehlersuche: TI-Status prüfen	4
3.1.	TI-Status im DS-Win und im DS4 prüfen	4
4.	VPN-Verbindung (WireGuard) prüfen	6
4.1.	Allgemeine Informationen	6
4.2.	WireGuard-Verbindung prüfen	6
4.3.	Mögliche Lösungen für WireGuard-Verbindungsprobleme	7
4.3.1.	Auf fest definierten ListenPort prüfen	8
5.	Verbindung zum Kartenterminal prüfen	9
5.1.	Allgemeine Informationen	9
5.2.	Verbindungsstatus im vKonnektor prüfen	9
5.3.	Einstellungen im RISE-TI-Client prüfen	9
5.4.	ORGA-Kartenterminal: Status der gSMC-KT Status prüfen	11
5.5.	CHERRY-Kartenterminal: Status der gSMC-KT prüfen	11
5.6.	Verbindung zum Kartenterminal prüfen	12
6.	TI-Fachdienste prüfen	13
6.1.	Erreichbarkeit der Fachdienste im DS-Win prüfen	13
6.2.	Erreichbarkeit der Fachdienste im DS4 prüfen (eRezept)	14
6.3.	Erreichbarkeit der Fachdienste im DS4 prüfen (ePA)	15
6.4.	PIN der SMC-B-Karte im vKonnektor erneut verifizieren	15
7.	DS-Win: Routen und NAT-Gruppe prüfen und neu einrichten	18
7.1.	Vorbereitung zur Einrichtung der Routen	18
7.2.	Routing-Skript mit PowerShell ausführen	18
7.3.	NAT-Gruppe am TI-Host prüfen/neu einrichten	19
7.3.1.	Routen am TI-Client prüfen/neu einrichten	19

Sehr geehrtes Praxis-Team,

das Ausführen der folgenden Arbeitsschritte trägt in vielen Fällen zur Behebung von Problemen und zur Wiederherstellung der Funktionalität von e-connect bei.

Bevor Sie unseren Support kontaktieren, stellen Sie sicher, dass Sie die aufgeführten Anweisungen vollständig geprüft bzw. durchgeführt haben.

Hinweis!

Diese Anleitung richtet sich an IT-Systembetreuer und setzt die Bedienung von cmd.exe und PowerShell sowie fundierte Kenntnisse in Netzwerktechnik und Systemadministration voraus.

Die Anleitung unterstützt bei der Analyse und Behebung von Auffälligkeiten im Zusammenhang von Dampsoft und e-connect.

Ihr Dampsoft-Team

2.1. Sofortmaßnahmen zur Fehlerbehebung

Starten Sie zunächst alle Geräte neu und prüfen Sie, ob der Fehler dadurch behoben werden konnte.

Stellen Sie sicher, dass alle Firewall-Einstellungen korrekt konfiguriert sind. Dadurch kann ein Störfall aufgrund falscher oder fehlender Einstellungen zuverlässig ausgeschlossen werden.

Folgen Sie dafür den Anweisungen in unserer Anleitung:

<https://www.dampsoft.de/storage/dokumente/dampsoft-anleitung-e-connect-firewall-kommunikationsmatrix.pdf>

RISE-Dienste können durch Virenschutz beeinträchtigt werden. Prüfen Sie, ob im Virenschutz Prozessausnahmen zu den drei RISE-Diensten gesetzt sind.

Tipp: Weitere Anleitungen finden Sie auf unserer e-connect-Serviceseite:

<https://www.dampsoft.de/service/e-connect/>

RISE-Dienste auf Windows-Betriebssystemen:

- RISE-TI-Client Maintenance Service
- RISE-TI-Client Service
- RISE-TI-Client WireGuard Service

RISE-Dienste auf macOS-Betriebssystemen:

- com.rise-world.ti-client.manager-service
- com.rise-world.ti-client.maintenance-service
- com.rise-world.ti-client.wireguard-service

Hinweis!

Die Übersicht der RISE-Dienste kann bei DS4-Kunden abweichen, da abhängig vom Installationssetup auch die WireGuard-App installiert sein kann, wodurch kein Dienst aktiv ist.

Führen Sie die Prüfungen oder Anpassungen der Konfiguration daher innerhalb der App durch.

2.2. Am vKonnektor anmelden

Um sich am vKonnektor anzumelden, folgen Sie den Anweisungen in der folgenden Anleitung:

https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf

2.3. e-connect im DS-Win

Das DS-Win wurde für das Betriebssystem Microsoft Windows programmiert.

Die TI-Dienste dürfen nur auf einer Station installiert sein. Diese Station wird als „TI-Host“ bezeichnet. Der TI-Host kann entweder ein Server oder ein Client sein.

Die zugehörigen Geräte werden als „TI-Clients“ bezeichnet. Auf den TI-Clients sind keine Dienste installiert. Die Dienste werden mit Routen konfiguriert, die es Ihnen ermöglichen, über den TI-Host auf das TI-Netzwerk zuzugreifen.

Fällt der TI-Host aus, verlieren alle zugehörigen Geräte den gesamten Zugriff auf die Telematikinfrastruktur.

2.4. e-connect im DS4

Das DS4 kann auf Arbeitsplätzen mit Ubuntu Desktop/Linux, Windows 10/11 und macOS genutzt werden. Zusätzlich wird einer der folgenden Internetbrowser in aktueller Version benötigt:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge.

Die Verarbeitung der TI-Dienste erfolgt an den Stationen über den Browser. Es werden keine Routen benötigt, um auf das TI-Netzwerk zuzugreifen.

DS4 On-Prem-Variante

Auf dem DS4 On-Prem-Server ist ausschließlich der WireGuard aktiv.

Auf einem Praxis-Client sind der TI-Client sowie WireGuard installiert.
Bei möglichen Störungen des WireGuards müssen daher sowohl der Server als auch der Client überprüft werden.

DS4 Cloud-Variante

In der Cloud-Variante sind der TI-Client sowie WireGuard vollständig auf einem einzelnen Client installiert.

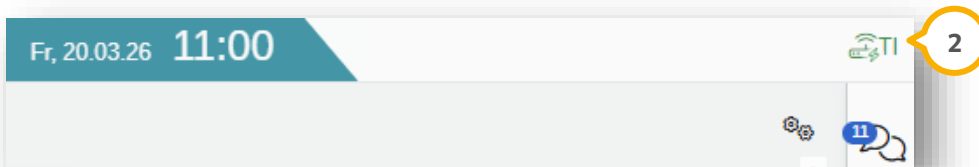
3.1. TI-Status im DS-Win und im DS4 prüfen

Die Anzeige des TI-Status zeigt im DS-Win ① sowie im DS4 ②, in welchem Bereich der Störung nachgegangen werden muss.

DS-Win



DS4



Um Störungen zu beheben, prüfen Sie den TI-Status.

Grün = Normalbetrieb

Alle Komponenten zur TI arbeiten ordnungsgemäß.

Grau = Keine Verbindung

Es besteht keine Verbindung zum vKonnektor.

Prüfen Sie folgende mögliche Ursachen:

- Die WireGuard Verbindung ist getrennt (siehe Kapitel 4).
- Die Routen am TI-Client sind inkorrekt, da die IP-Adresse vom TI-Host geändert wurde (DHCP).
Tipp: Stellen Sie die ursprüngliche IP-Adresse wieder her und nehmen Sie eine Adress-Reservierung vor.

Gelb = Hinweise/Informationen

Es liegen Hinweise oder Informationen vor. Die Funktionalität der TI ist dadurch jedoch nicht beeinträchtigt.

Prüfen Sie folgende mögliche Ursachen:

- Die PIN der SMC-B wurde noch nicht eingegeben und somit noch nicht freigeschaltet
Tipp: Eine PIN-Abfrage erfolgt automatisch beim nächsten Lesen einer Versichertenkarte
- Es liegen vKonnektor-Meldungen, zum Beispiel zu einem Protokollüberlauf, vor
(siehe: <https://www.dampsoft.de/storage/dokumente/ds-anleitung-e-connect-2-0-protokollueberlauf.pdf>).
- Der vKonnektor hat keine Verbindung zur Telematikinfrastruktur (TI)
(siehe: https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf).

Rot = Schwerwiegende Störung

Es liegt eine schwerwiegende Störung der TI-Komponenten vor.

Prüfen Sie folgende mögliche Ursachen:

- Die SMC-B wurde nicht gesteckt oder nicht erkannt.
Starten Sie das DS-Win und den Kartenleser neu. Stecken Sie die SMC-B erneut in den Kartenleser.
- Es besteht keine Verbindung zum Kartenterminal (siehe Kapitel 5).

4.1. Allgemeine Informationen

Windows

Die WireGuard-Verbindung wird unter Windows als Systemdienst betrieben und nicht als interaktive Anwendung ausgeführt.

Prüfen Sie in den Windows-Diensten, dass der „RISE-TI-Client WireGuard Service“ ausgeführt wird.

Tipp: Eine Prüfung des Verbindungsstatus ist ausschließlich über ein Kommandozeilen-Programm (z. B. in der CMD oder PowerShell) möglich.

macOS

Für DS4-Kunden, die macOS verwenden, erfolgt die Prüfung des Verbindungsstatus über das Terminal oder ein anderes Kommandozeilen-Programm.

Alternativ können Sie anstatt eines systemweiten Dienstes die WireGuard-App nutzen. In der App können Sie den Verbindungsstatus einsehen und die Konfiguration anpassen.

4.2. WireGuard-Verbindung prüfen

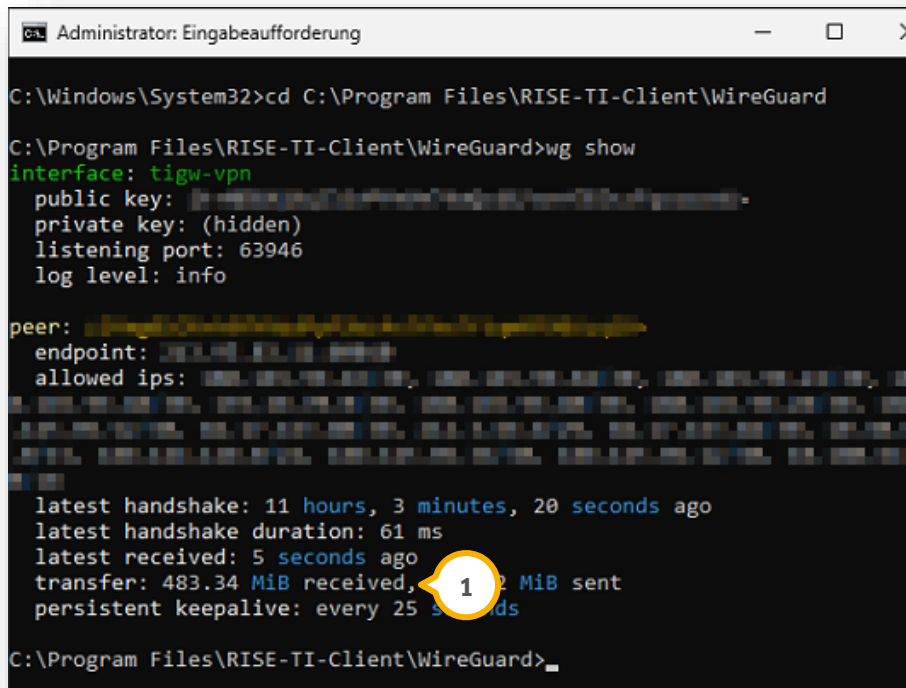
Starten Sie mit Administratorrechten ein Kommandozeilen-Programm (z. B. CMD oder PowerShell).

Wechseln Sie in eines der folgenden Verzeichnisse:

- **Windows:** „C:\Program Files\RISE-TI-Client\WireGuard“
- **macOS:** „./opt/rise/ti-client/WireGuard/“

Geben Sie den Befehl „wg show“ ein.

Führen Sie den Befehl aus, indem Sie auf die Enter-Taste drücken.



```
Administrator: Eingabeaufforderung

C:\Windows\System32>cd C:\Program Files\RISE-TI-Client\WireGuard

C:\Program Files\RISE-TI-Client\WireGuard>wg show
interface: tigw-vpn
  public key: [REDACTED]
  private key: (hidden)
  listening port: 63946
  log level: info

peer: [REDACTED]
  endpoint: [REDACTED]
  allowed ips: [REDACTED]
  latest handshake: 11 hours, 3 minutes, 20 seconds ago
  latest handshake duration: 61 ms
  latest received: 5 seconds ago
  transfer: 483.34 MiB received, 2 MiB sent
  persistent keepalive: every 25 seconds

C:\Program Files\RISE-TI-Client\WireGuard>
```

Überprüfen Sie in der Ausgabe in der Zeile „transfer“ den Wert „received“ ①.

Wenn dort keine empfangenen Daten (Wert = 0) angezeigt werden, deutet dies auf eine unvollständige oder gestörte Kommunikation der WireGuard-Verbindung hin.

Hinweis!

Die Anzeige wird nicht in Echtzeit aktualisiert. Wenn Sie Änderungen vornehmen, führen Sie den Befehl „wg show“ erneut aus.

4.3. Mögliche Lösungen für WireGuard-Verbindungsprobleme

Starten Sie den Router und die vorgeschaltete Hardware-Firewall neu und prüfen Sie, ob der Fehler dadurch behoben werden konnte.

Um den vKonnektor neu zu starten, folgen Sie den Anweisungen in der folgenden Anleitung:
https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf

Sollte keine Verbindung zum vKonnektor möglich sein, wenden Sie sich an unseren Technischen Support.

4.3.1. Auf fest definierten ListenPort prüfen

Wenn für die Verbindung ein fest definierter ListenPort verwendet wird, kann dies zu Konflikten mit anderen Anwendungen führen, die denselben Port nutzen.

Tipp: Verwenden Sie einen dynamischen Port.

Zur Prüfung und Anpassung führen Sie die folgenden Arbeitsschritte aus:

Öffnen Sie einen Dateimanager (z. B. den Windows-Explorer).

Wechseln Sie in eines der folgenden Verzeichnisse:

- **Windows:** „C:\Program Files\Rise-TI-Client\WireGuard“
- **macOS:** „/opt/rise/ti-client/WireGuard/“

Dort befindet sich die Konfigurationsdatei „tigw-vpn.conf“.

Öffnen Sie diese mit einem Texteditor (z. B. Editor).



Prüfen Sie, ob eine Zeile mit dem Eintrag „ListenPort“ vorhanden ist.

Ist dies der Fall, entfernen Sie diese Zeile vollständig.

Alternativ können Sie die Zeile auskommentieren, indem Sie ein „#“ an den Zeilenanfang setzen.

Tipp: Nehmen Sie diese Änderung bei macOS mit der Wireguard-App in der Verbindungseinstellung in der App vor.

Speichern Sie die Änderung im Texteditor.

Um die Änderung anzuwenden, starten Sie den WireGuard-Dienst neu.

Prüfen Sie in der Kommandozeile, ob sich der Verbindungsstatus verändert hat.

5.1. Allgemeine Informationen

Im Folgenden wird erläutert, wie Sie Verbindungsprobleme zu Ihren Kartenterminals prüfen. Die Prüfung kann jeweils am vKonnektor, am TI-Client oder am Kartenterminal selbst erfolgen.

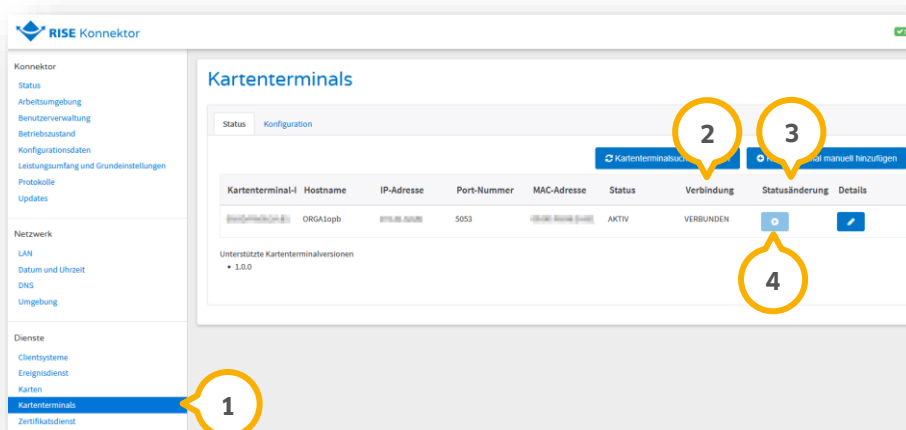
Sie können den aktuellen Status der angeschlossenen Kartenterminals über das Webinterface des Konnektors einsehen und mögliche Fehlerquellen identifizieren.

5.2. Verbindungsstatus im vKonnektor prüfen

Um sich am vKonnektor anzumelden, folgen Sie den Anweisungen in der folgenden Anleitung:

https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf

Wechseln Sie in die Übersicht „Kartenterminals“ ①.



Prüfen Sie in der Spalte „Verbindung“ ②, dass alle Terminals verbunden sind.

Wenn ein Terminal nicht verbunden ist, starten Sie einen erneuten Verbindungsaufbau.

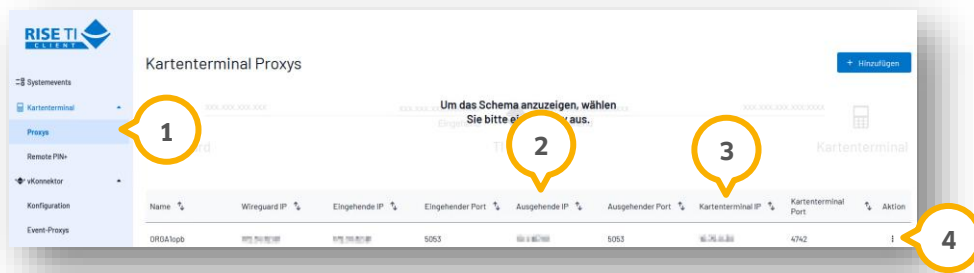
Klicken Sie dazu in der Spalte „Statusänderung“ ③ auf das Symbol ④.

Wenn die erneute Verbindung nicht erfolgreich ist, befolgen Sie die nächsten Schritte.

5.3. Einstellungen im RISE-TI-Client prüfen

Öffnen Sie am TI-Host einen Browser Ihrer Wahl und geben Sie in der Adresszeile Folgendes ein:
„https://localhost:8080“

Tipp: Sollte die Seite nicht erreichbar sein, testen Sie nacheinander die Ports 8081 bis maximal 8085, bis die Seite erreichbar ist.



Wechseln Sie in den Bereich „Proxys“ ①.

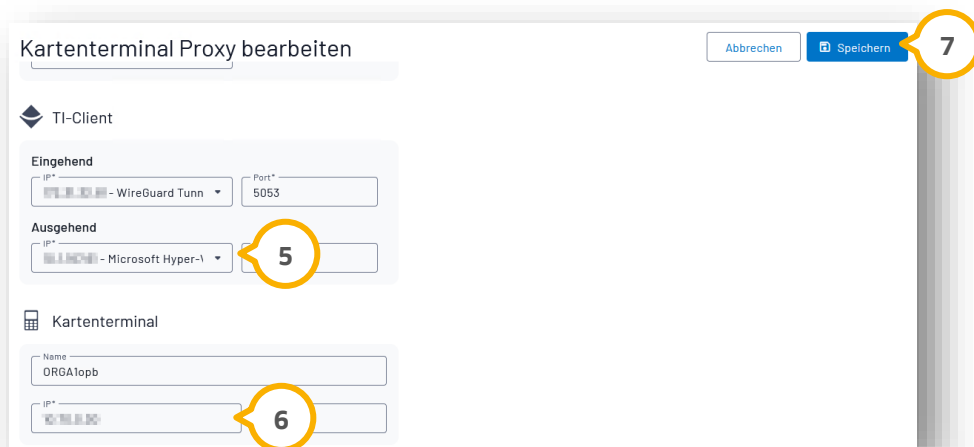
Prüfen Sie, ob die „Ausgehende IP“ ② mit der IP-Adresse des TI-Hosts übereinstimmt.

Stimmen diese nicht überein, stellen Sie am Host die ursprüngliche IP-Adresse wieder her. Stellen Sie außerdem sicher, dass die IP-Adresse dauerhaft statisch konfiguriert ist.

Prüfen Sie, ob die „Kartenterminal IP“ ③ mit der IP-Adresse vom Terminal übereinstimmt.

Stimmen diese nicht überein, stellen Sie, wenn möglich, am Kartenterminal die ursprüngliche IP-Adresse wieder her. Stellen Sie außerdem sicher, dass die IP-Adresse dauerhaft statisch konfiguriert ist.

Wenn an beiden Geräten eine Wiederherstellung der ursprünglichen IP-Adresse nicht möglich ist, rufen Sie im TI-Client über die drei Punkte ④ die Funktion „Bearbeiten“ auf.



Passen Sie die Werte ⑤ und ⑥ entsprechend an und klicken Sie auf >>Speichern<< ⑦.

5.4. ORGA-Kartenterminal: Status der gSMC-KT Status prüfen

Öffnen Sie einen Browser Ihrer Wahl und geben Sie in der Adresszeile Folgendes ein:
„https://IP-des-Kartenterminals“, z. B. „https://192.168.178.100“.

ORGA 6141 online
ORGA Neo

Verbunden
mit Management-Schnittstelle.
Adresse: [redacted]

Kartenterminal Typ	ORGA 6141 online
SICCT Terminalname	[redacted]
Host Name	[redacted]
Produkt Version	3.9.2:1.2.0
Serien Nummer	[redacted]
MAC Adresse	[redacted]
IP Adresse SICCT	[redacted]
IP Adresse Konnektor	[redacted]
TLS Status Konnektor	SICCT open
SICCT Session Status	OpenControl
VPN Status	nicht aktiv
Aktive TSL Liste	[redacted]
gSMC-KT ECC CXD	07.08.2029
gSMC-KT RSA CXD	07.08.2029

Passwort eingeben
Remote Admin Passwort [redacted]

Im Bereich ① können Sie das Gültigkeitsdatum der gSMC-KT einsehen.

Hinweis!

Wenn das Datum in der Vergangenheit liegt, ist die zugehörige gSMC-KT abgelaufen und muss ersetzt werden. Einen Ersatz können Sie über den Dampsoft Webshop beantragen.

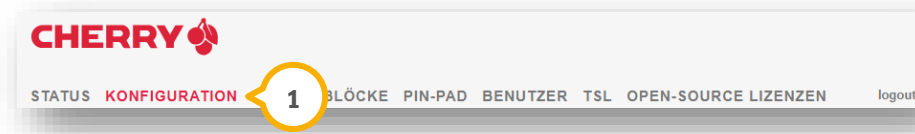
Tipp: Wenn in beiden Zeilen kein Datum angezeigt wird, entfernen Sie die Karte und setzen Sie sie erneut ein. Wird weiterhin kein Datum angezeigt, testen Sie einen anderen Kartenslot, um einen Defekt der Karte oder des Slots auszuschließen.

5.5. CHERRY-Kartenterminal: Status der gSMC-KT prüfen

Öffnen Sie einen Browser Ihrer Wahl und geben Sie in der Adresszeile Folgendes ein:
„https://IP-des-Kartenterminals“, z. B. „https:// 192.168.100.120“.

Melden Sie sich mit dem 8-stelligen Admin-Passwort am Kartenterminal an.

Wechseln Sie in die Ansicht „Konfiguration“ ①.



Scrollen Sie zu „gSMC-KT Status“ ②.



Prüfen Sie jedes Ablaufdatum in Bereich ③.

Hinweis!

Wenn das Datum in der Vergangenheit liegt, ist die zugehörige gSMC-KT abgelaufen und muss ersetzt werden. Einen Ersatz können Sie über den Dampsoft Webshop beantragen.

Tipp: Wenn in keiner der Zeilen ein Datum angezeigt wird, entfernen Sie die Karte und setzen Sie sie erneut ein. Wird weiterhin kein Datum angezeigt, testen Sie einen anderen Kartenslot, um einen Defekt der Karte oder des Slots auszuschließen.

5.6. Verbindung zum Kartenterminal prüfen

Um das Kartenterminal mit dem vKonnektor neu zu verbinden (pairen), folgen Sie den Anweisungen in der folgenden Anleitung:

<https://www.dampsoft.de/storage/dokumente/dampsoft-anleitung-e-connect-2.0-gsmc-kt-tauschen.pdf>

Bei Problemen mit dem Zugriff auf die Fachdienste prüfen Sie, ob alle folgenden Domains auf dem jeweiligen Server oder Client korrekt aufgelöst werden können:

- **Identity-Provider:**
 - idp.zentral.idp.splitdns.ti-dienste.de
- **eRezept-Fachdienste:**
 - erp.zentral.erp.splitdns.ti-dienste.de
- **ePA-Fachdienste:**
 - epa-as-1.prod.epa4all.de
 - epa-as-2.prod.epa4all.de

Testmöglichkeit der benötigten Namensauflösung (DNS) am Beispiel eRezept:

- „nslookup erp.zentral.erp.splitdns.ti-dienste.de“ muss eine IP liefern

Empfehlung zur Namensauflösung (DNS):

Stellen Sie die wie folgt endenden Domainnamen (FQDN) im DNS-Server des Domain Controllers oder des Internetrouters als DNS-Weiterleitungen an den Konnektor ein:

- *.telematik,
- *.splitdns.ti-dienste.de
- *.prod.epa4all.de

Hinweis!

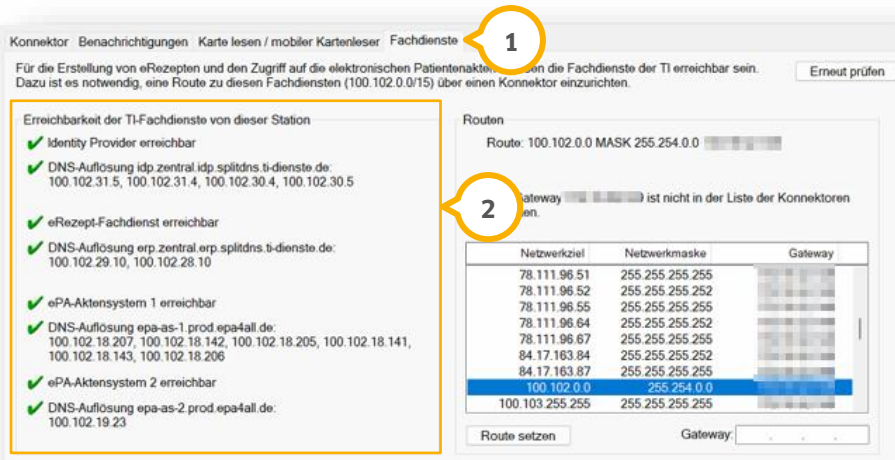
Alle IP-Adressen müssen mit 100.102. beginnen.

Wenn bei einer dieser Adressen Auslösungsprobleme auftreten, prüfen Sie Ihren DNS-Server.

6.1. Erreichbarkeit der Fachdienste im DS-Win prüfen

Um die Erreichbarkeit der TI-Fachdienste im DS-Win zu prüfen, folgen Sie dem Pfad „Einstellungen/Kartenleser/Telematik“.

Wechseln Sie in den Reiter „Fachdienste“ ①.



Wenn alle Punkte in Bereich ② mit einem grünen Häkchen angezeigt werden, sind alle Fachdienste erreichbar.

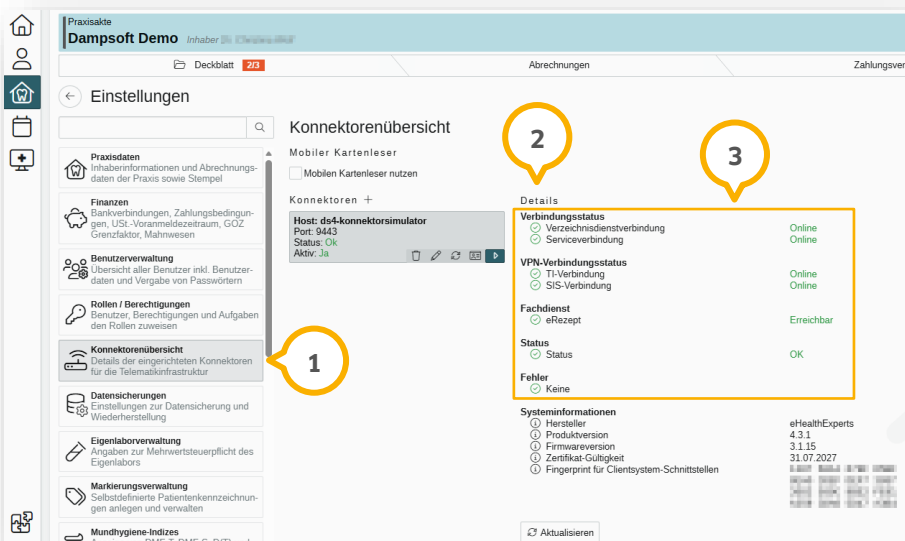
Wenn Fachdienste nicht erreichbar sind, erscheint an Stelle der grünen Häkchen ein rotes Kreuz.

Wenn ein oder mehrere Fachdienste nicht erreichbar sind, führen Sie die folgenden Arbeitsschritte durch:

- Starten Sie den vKonnektor neu.
- Prüfen Sie, ob die Route 100.102.0.0 korrekt gesetzt ist:
 - TI-Host: Diese Route muss bei Gateway auf die WireGuard-IP verweisen.
 - TI-Client: Diese Route muss bei Gateway auf die IP-Adresse vom TI-Host verweisen.
- Verifizieren Sie die PIN der SMC-B im vKonnektor neu (siehe Abschnitt 6.4).

6.2. Erreichbarkeit der Fachdienste im DS4 prüfen (eRezept)

Folgen Sie im DS4 dem Pfad „Praxisakte/Einstellungen/Konnektorenübersicht“ ①.



Klicken Sie auf „Details“ ②.

In Bereich ③ wird die Statusübersicht der TI und der eRezept-Fachdienste angezeigt

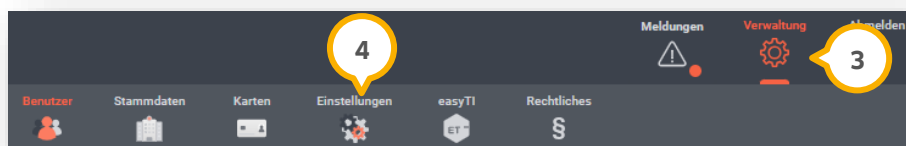
6.3. Erreichbarkeit der Fachdienste im DS4 prüfen (ePA)

Wechseln Sie in den Bereich „TI-Main-View“ ①.



Klicken Sie auf >>easyTI öffnen<< ②.

Klicken Sie im easyTI auf „Verwaltung“ ③.



Wechseln Sie in den Bereich „Einstellungen“ ④.

Scrollen Sie nach unten, bis Sie „ePA VAU-Status der Aktensysteme“ erreichen.

Prüfen Sie, ob alle ePA-Hosts mit einem grünen Häkchen angezeigt werden.

6.4. PIN der SMC-B-Karte im vKonnektor erneut verifizieren

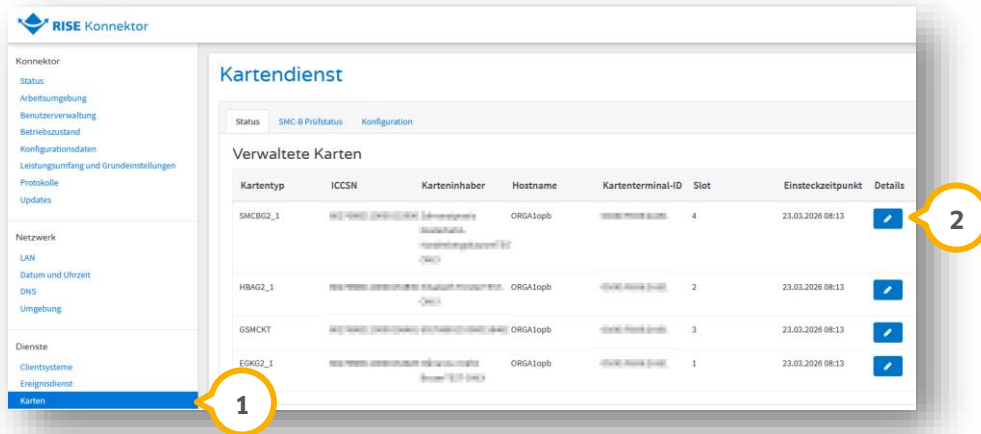
Wenn die Erreichbarkeit der Fachdienste weiterhin beeinträchtigt ist, führen Sie eine erneute Verifizierung der PIN Ihrer SMC-B-Karte durch.

Nur, wenn eine gültige und verifizierte SMC-B-Karte vorliegt, erhält der vKonnektor Zugriff auf die Fachdienste.

Um sich am vKonnektor anzumelden, folgen Sie den Anweisungen in der folgenden Anleitung:

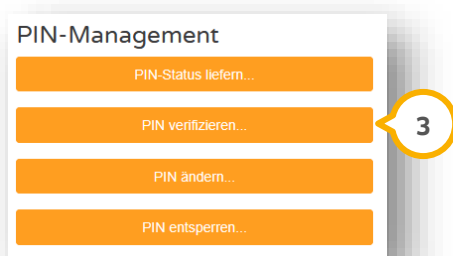
https://www.dampsoft.de/wp-content/uploads/DS_Anleitung_e-connect-2.0-Konnektor-Neustart.pdf

Wechseln Sie in die Übersicht „Karten“ ①



Klicken Sie bei Ihrer SMC-B in der Spalte „Details“ auf das Stift-Symbol ②.

Scrollen Sie nach unten und klicken Sie auf >>PIN verifizieren...<< ③.



Wählen Sie den Mandanten, das Clientsystem und einen Arbeitsplatz ④ aus.

Tipp: Der Arbeitsplatz ist der Rechner, an dem die PIN-Abfrage am Kartenterminal erscheinen soll.

PIN verifizieren

Wollen Sie die PIN der Karte verifizieren?

Karteninhaber: Zahnarztpraxis

ICCSN:

Die PIN mit folgendem Aufrufkontext aus der [Arbeitsumgebung](#) des Konnektors verifizieren:

Mandant: Mandant

Clientsystem: DSWIN

Arbeitsplatz: (lokale PIN-Eingabe)

Sie können die PIN wahlweise bei dem Kartenterminal eingeben, in dem die Karte lokal gesteckt ist. Alternativ können Sie die PIN bei dem Remote-PIN-Kartenterminal des gewählten Arbeitsplatzes eingeben.

☒ Für alle Mandanten, Clientsystem und Arbeitsplätze freischalten

Abbrechen **5** PIN verifizieren

Klicken Sie auf >>PIN verifizieren<< **5** und geben Sie die PIN direkt am Kartenterminal ein.

Prüfen Sie, ob die Fachdienste wieder erreichbar sind.

7.1. Vorbereitung zur Einrichtung der Routen

Für die Verbindung der TI-Clients zur TI wird am TI-Host eine NAT-Gruppe eingerichtet. Auf den TI-Clients werden entsprechende Routen konfiguriert, die auf den TI-Host verweisen.

Für die erneute Einrichtung der Routen oder der NAT-Gruppe wird eines der folgenden PowerShell-Skripte benötigt:

- tigw-routingv1-x.ps1
- tic-routingv1-x.ps1

Die Skripte befinden sich in einem der folgenden Verzeichnisse:

- C:\e-connect 2.0
- Lw:\TDAMP\DS\e-connect 2.0

Wenn sich dort kein Ordner mit dem Routing-Skript befindet, können Sie ein Skript im Dampsoft-Webshop herunterladen:

Öffnen Sie den Webshop: <https://shop.dampsoft.de> und melden Sie sich mit Ihren Anmeldedaten an.

Folgen Sie dem Pfad „Mein Konto/e-connect Downloads“.

Klicken Sie auf >>Routing Skript herunterladen<<.

Um das Skript von jedem PC zu erreichen, empfehlen wir, die Datei unter den folgenden Pfaden zu speichern:

- C:\e-connect 2.0
- Lw:\TDAMP\DS\e-connect 2.0

7.2. Routing-Skript mit PowerShell ausführen

Damit Sie Änderungen mit dem Routing-Skript ausführen können, müssen Sie eine PowerShell als Administrator starten.

Hinweis!

Wenn Sie das Skript ausführen, passen Sie den Pfad und den Namen des Routing-Skripts entsprechend an.

Führen Sie das Skript mit folgendem Befehl aus:

- PowerShell.exe -ExecutionPolicy Bypass -File „C:\Pfad-zum-Skript\tigw-routingv1-0.ps1“

Beispiel mit angepasstem Pfad und Namen:

- PowerShell.exe -ExecutionPolicy Bypass -File „C:\E-Connect2.0\tigw-routingv1-0\tigw-routingv1-0.ps1“

7.3. NAT-Gruppe am TI-Host prüfen/neu einrichten

Prüfen Sie, ob die NAT-Gruppe korrekt angelegt ist.

Öffnen Sie dazu am TI-Host eine PowerShell.

Geben Sie den Befehl „Get-NetNat“ ein.

Als Ergebnis sollte eine NAT-Gruppe mit dem Namen „tigw-nat“ angezeigt werden.

Prüfen Sie, ob beim Eintrag „InternalIPInterfaceAddressPrefix“ die korrekte IP-Adresse mit Präfixlänge angezeigt wird.

Sollte die NAT-Gruppe nicht korrekt eingerichtet sein oder fehlen, führen Sie das Routing-Skript aus:

Geben Sie „3“ („Alles entfernen“) ein und bestätigen Sie mit der Enter-Taste.

Wenn alles gelöscht ist, kehren Sie mit „Y“ zum Hauptmenü zurück.

Geben Sie „2“ („Host“) ein und bestätigen Sie mit der Enter-Taste.

Geben Sie erneut „2“ („NAT-Gruppe einrichten“) ein und bestätigen Sie mit der Enter-Taste.

Geben Sie die IP-Adresse des Servers/Clients mit Präfix ein (z. B. 192.168.0.10/24).

Die NAT-Gruppe wurde angelegt. Dies können Sie mit dem Befehl „Get-NetNat“ prüfen.

Starten Sie abschließend den Dienst „RISE-TI-Client WireGuard Service“ neu.

7.3.1. Routen am TI-Client prüfen/neu einrichten

Öffnen Sie auf dem TI-Client die CMD und lassen Sie sich mit dem Befehl „route print“ alle aktiven Routen anzeigen.

Vergleichen Sie, ob die IP-Adresse des TI-Hosts in den Routen jeweils als „Gateway“ hinterlegt ist oder abweicht.

Folgende Routen sollten angezeigt werden:

1	=	10.160.0.0 MASK 255.252.0.0	10	=	78.111.96.52 MASK 255.255.255.252
2	=	100.102.0.0 MASK 255.254.0.0	11	=	78.111.96.32 MASK 255.255.255.252
3	=	188.144.0.0 MASK 255.254.0.0	12	=	78.111.96.28 MASK 255.255.255.252
4	=	212.3.66.8 MASK 255.255.255.248	13	=	78.111.96.24 MASK 255.255.255.252
5	=	213.146.104.80 MASK 255.255.255.248	14	=	78.111.96.16 MASK 255.255.255.252
6	=	78.111.96.36 MASK 255.255.255.252	15	=	78.111.96.12 MASK 255.255.255.252
7	=	84.17.163.84 MASK 255.255.255.252	16	=	78.111.96.48 MASK 255.255.255.252
8	=	185.226.121.64 MASK 255.255.255.240	17	=	78.111.96.64 MASK 255.255.255.252
9	=	213.61.31.240 MASK 255.255.255.240	18	=	78.111.96.52 MASK 255.255.255.252

Wenn Abweichungen auftreten, z. B. fehlende Routen oder eine nicht übereinstimmende Gateway-IP-Adresse, müssen die vorhandenen Routen gelöscht und anschließend mit dem zugehörigen Routing-Skript neu erstellt werden.

Gehen Sie dazu wie folgt vor:

Führen Sie das Routing-Skript aus.

Geben Sie „3“ (Alles entfernen) ein und bestätigen Sie mit der Enter-Taste.

Kehren Sie mit „Y“ zum Hauptmenü zurück.

Geben Sie „1“ (Client) ein und bestätigen Sie mit der Enter-Taste.

Geben Sie „2“ (Produktiv-Umgebung) ein und bestätigen Sie mit der Enter-Taste.

Geben Sie die IP-Adresse vom TI-Host ein und bestätigen Sie mit der Enter-Taste.

Alle Routen wurden neu angelegt.

Prüfen Sie im DS-Win, ob der TI-Status grün anzeigt und die TI somit erreichbar ist (siehe Kapitel 3).

