

RISE TaaS Client Handbuch

RISE TI

as a service



RISE TlaaS Client

Stand: 21.06.2024

Version: 1.15.0

Inhaltsverzeichnis

1	Einleitung	5
2	Installation	5
2.1	Systemvoraussetzungen.....	5
2.1.1	Hardware.....	5
2.1.2	Netzwerkeinstellungen.....	5
2.1.3	Betriebssystem	6
2.1.4	Webbrowser	6
2.1.5	Third-Party Software	6
2.1.6	Voraussetzungen für einen sicheren Betrieb	6
2.2	Kompatibilität	7
2.3	Vorbereitung.....	8
2.3.1	Windows.....	8
2.3.2	macOS	8
2.3.3	Linux	9
2.4	Installationsprozess	10
2.4.1	Windows und macOS.....	10
2.4.2	Linux	14
3	Start, Stop und Überblick der Anwendung	16
3.1	Aufrufen der Benutzeroberfläche	17
3.2	Startseite	20
3.3	Tabellen.....	21
3.4	Dialoge.....	21
4	Konnektor	21
5	Kartenterminals	22
5.1	Kartenterminalübersicht	22
5.2	Kartenterminal hinzufügen und pairen.....	23
5.3	Kartenterminal neu verbinden	25
5.4	Kartenterminal entfernen	25
5.5	Admin-Session-PIN hinterlegen.....	25
5.6	Admin-Session-PIN automatisch synchronisieren	25
5.7	Admin-Session-PIN manuell synchronisieren.....	26
5.8	Admin-Session-PIN entfernen	26
6	Karten	26
6.1	Kartenübersicht.....	26
6.2	Kartenaktionen.....	27
6.2.1	PIN-Status abfragen.....	28
6.2.2	PIN verifizieren	28
6.2.3	PIN ändern.....	28
6.2.4	PIN entsperren	28
6.2.5	Remote PIN+	29

7	Arbeitsumgebung	29
7.1	Begriffserläuterung von Mandant, Arbeitsplatz und Clientsystem	30
7.2	Verwaltung von Mandanten, Arbeitsplätzen, Clientsystemen	30
7.3	Arbeitsumgebung einrichten	31
8	Kommunikation im Medizinwesen (KIM)	32
8.1	KIM Authentisierung.....	34
8.2	Registrierung einer KIM E-Mail-Adresse	37
8.2.1	TlaaS Client	37
8.2.2	Primärsystem	39
8.3	KIM as a Service deaktivieren	40
9	Benutzerverwaltung	40
9.1	Benutzeranzeige.....	40
9.2	Benutzer hinzufügen	41
9.3	Benutzermenü.....	42
9.3.1	Passwort ändern	42
9.3.2	Benutzer löschen	43
10	Konfiguration	43
10.1	Konfiguration der TLS-Kommunikation.....	44
10.2	Konfiguration des Netzwerkadapters für das VPN.....	46
10.3	Konfigurationsverzeichnisse	47
10.4	Konfiguration der Anwendung	47
10.5	Konfiguration automatischer Software-Updates	49
10.6	Konfiguration der Kartenterminals	49
10.7	Konfiguration der WireGuard Konfigurationsdatei.....	50
11	Primärsysteme	50
11.1	Primärsystemübersicht.....	51
11.2	Primärsystem bearbeiten	51
11.3	Primärsystem entfernen	52
12	Logging	52
13	Updates	53
13.1	TlaaS Client.....	53
13.2	WireGuard.....	53
13.3	Freigegebene IP-Adressen	53
14	Konfiguration des Netzwerkes des Leistungserbringers	54
14.1	Installation des TlaaS Clients auf einem zentralen Server mit WireGuard-Client	55
14.1.1	Installation unter Windows 10/11	55
14.1.2	Installation unter Windows Server 2022	56
14.2	Verwendung eines bereitgestellten WireGuard-VPN-Tunnels.....	57
14.2.1	Konfiguration des WireGuard-VPN-Tunnels	57
14.2.2	Konfiguration eines NAT-Gateways für den WireGuard-VPN-Tunnel	58
14.2.3	Konfiguration der Routen für den WireGuard-VPN-Tunnel.....	58

14.2.4	Konfiguration des Port-Forwardings für eingehende Requests vom TlaaS-Rechenzentrum zum TlaaS Client	58
14.2.5	Konfiguration der Firewall, sodass nur bestimmte Hosts Zugriff auf den VPN-Tunnel erhalten.....	59
14.2.6	Konfiguration der Firewall, sodass der Zugriff auf den Updateserver, von wo die Updates und Serverzertifikate bezogen werden, freigegeben wird	59
15	Deinstallation	59
15.1	Windows	59
15.2	macOS.....	60
15.3	Linux	61
15.4	Entfernung eines bereitgestellten WireGuard-VPN-Tunnels.....	62
16	Fehlerbehebung	62
16.1	vKonnektor	63
16.2	Zertifikate	63
16.3	Kartenterminal	64
16.4	Karten	66
16.5	KIMaaS.....	67
16.6	Maximum Transmission Unit (MTU)	67
16.6.1	Windows.....	67
16.6.2	macOS und Linux	70
17	Kontakt	71

1 Einleitung

Diese Bedienungsanleitung beschreibt den *RISE TI as a Service (TlaaS) Client* zur Kommunikation mit dem TlaaS Rechenzentrum (RZ) und den dort zur Verfügung stehenden Konnektoren (*EBK*) sowie zur Kommunikation mit der *RISE Konnektor Verwaltungssoftware (KVS)*. Der TlaaS Client ist eine eigenständige Softwarekomponente, welche in der Einsatzumgebung des sogenannten Leistungserbringers/der Leistungserbringerin (LE) verwendet wird. Über einen mitinstallierten VPN-Client verbindet sich die Software zu einem remote erreichbaren RISE Konnektor und kann so seine Funktionalität nutzen. Dazu muss der/die LE eine den Anforderungen entsprechende korrekte und sichere Betriebsumgebung bereitstellen.

Diese Bedienungsanleitung enthält wichtige Informationen zur sicheren Installation, zum operativen Betrieb und zur Deinstallation. Lesen Sie die Bedienungsanleitung sorgfältig durch, bevor Sie die Software in den produktiven Einsatz bringen.

Diese Bedienungsanleitung wird vom Anbieter über einen sicheren Weg in der jeweils aktuellen Version zur Verfügung gestellt und richtet sich generell an Leistungserbringer, die RISE TlaaS nutzen, und an die Administratoren im Speziellen.

Bei den in diesem Dokument verwendeten Bildern handelt es sich um Symbolbilder, die nur zur Veranschaulichung dienen. Die Darstellungen können sich, abhängig von der verwendeten Betriebssystem-, Software- und Browser-Version, unterscheiden.

2 Installation

In diesem Abschnitt werden die Systemvoraussetzungen, der Installationsprozess sowie Vorgaben und Hinweise für die Installation beschrieben.

2.1 Systemvoraussetzungen

Der TlaaS Client besitzt einige Anforderungen, welche der/die LE durch Komponenten, das lokale Netzwerk oder die Betriebsumgebung erfüllen muss, um einen vollständigen, ordnungsgemäßen und sicheren Betrieb ermöglichen zu können.

2.1.1 Hardware

Um die Funktionalität des TlaaS Clients nutzen zu können, müssen entsprechende Kartenterminals und Chipkarten gemäß Bedienungsanleitung des RISE Konnektors bereitgestellt werden.

2.1.2 Netzwerkeinstellungen

Im Zuge der Installation des TlaaS Clients werden automatisch Ausnahmen für die Betriebssystem-eigene Firewall hinzugefügt. Bei der Deinstallation werden diese Ausnahmen wieder entfernt.

Werden in Ihrem Netzwerk weitere Firewalls verwendet, die die Funktion des TlaaS Clients beeinflussen, wenden Sie sich an Ihren Netzwerkadministrator.

2.1.3 Betriebssystem

Aktuell unterstützt der TlaaS Client folgende Betriebssysteme:

- Windows 10 (64-bit) 22H2
- Windows 11 (64-bit) 22H2
- Windows Server 2019
- Windows Server 2022
- macOS Version 13 (Ventura)
- macOS Version 14 (Sonoma)
- Ubuntu 22.04.4 LTS Server
- Ubuntu 24.04 LTS Server

2.1.4 Webbrowser

Für die korrekte Nutzung des TlaaS Clients empfehlen wir aktuell die Verwendung des Clients mit folgenden Webbrowsern:

- Google Chrome ab Version 125
- Microsoft Edge ab Version 125
- Mozilla Firefox ab Version 126
- Apple Safari ab Version 17.4.1

2.1.5 Third-Party Software

Für die Installation des VPN Pakets im Zuge der Installation des TlaaS Clients unter macOS wird empfohlen *Homebrew* zu installieren (siehe Abschnitt 2.3.2.1). Für Installationen ohne *Homebrew* ist es notwendig, einen gesonderten *WireGuard*-Client zu installieren und zu konfigurieren (siehe Abschnitt 2.3.2.2).

2.1.6 Voraussetzungen für einen sicheren Betrieb

Zusätzlich zu den beschriebenen funktionalen Anforderungen muss auch die Sicherheit der Betriebsumgebung des TlaaS Clients gewährleistet und eingehalten werden. Daher sind vor jedem Start der Anwendung folgende sicherheitsrelevanten Vorgaben zu beachten und sicherzustellen:

- **Schutz des Netzwerks vor Angriffen:**
Der/Die LE muss dafür sorgen, dass das lokale Netzwerk gegen unbefugten Zugriff bzw. Nutzung

geschützt ist. Des Weiteren müssen die verbundenen Systeme im Netzwerk immer auf dem aktuellsten Stand sein (regelmäßige Updates), um sie gegen Schadsoftware zu schützen, und somit auch das lokale Netzwerk.

- **Sichere Administration:**
Der/Die LE muss dafür sorgen, dass administrative Tätigkeiten in Übereinstimmung mit der Produktdokumentation durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdigen, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen geheim halten bzw. dürfen diese nicht an Unberechtigte weitergeben.
- **Schutz des privaten Schlüssels:**
Der/Die LE muss dafür sorgen, dass der private Schlüssel, welcher sich in der Konfigurationsdatei (.zip-Archivdatei) und nach der Installation in der WireGuard Konfigurationsdatei befindet, geheimgehalten wird. Der private Schlüssel wird zur Entschlüsselung von Daten als auch für die Identifikation des LE verwendet. Bei Verlust oder Veröffentlichung des privaten Schlüssels ist umgehenden Kontakt mit dem Anbieter aufzunehmen, um den Schlüssel sperren zu lassen.
- **Schutz der Betriebsumgebung:**
Der/Die LE muss dafür sorgen, dass nur gültige und vertrauenswürdige Zertifikate importiert werden. Es finden keine technischen Prüfungen der Zertifikate durch den T1aaS Client statt. Zertifikate, denen nicht mehr vertraut wird, müssen vom Benutzer über die Konfigurationseinstellungsoberfläche ausgetauscht werden.
Der T1aaS Client speichert Zertifikate und Zugangsdaten für die verschlüsselte Kommunikation in einem Schlüsselspeicher. Das Passwort wird für jede Installation individuell generiert. Es liegt in der Verantwortung des Benutzers, für eine sichere Betriebsumgebung zu sorgen und sicherzustellen, dass diese Daten geschützt bleiben, bspw. durch Installation von Betriebssystem-Updates, den Einsatz einer Firewall, Antiviren-Schutzsoftware usw. Die Maßnahmen müssen jeweils State-of-the-art-Standards bzw. darüber hinaus erfüllen.
Der T1aaS Client schreibt Logdateien, die eine Analyse der technischen Vorgänge erlauben. Der Benutzer muss durch geeignete Maßnahmen sicherstellen, dass diese Logdateien nur für autorisierte Personen zugänglich sind.
- **Installation von sicherheitsrelevanten Updates:**
Im Falle von Sicherheitsaktualisierungen wird vom T1aaS Anbieter unverzüglich eine aktualisierte T1aaS Client Version zur Verfügung gestellt. Es liegt in der Verantwortung des Benutzers die aktualisierte Version zeitnahe zu installieren.

2.2 Kompatibilität

Der T1aaS Client wurde erfolgreich mit folgenden von der gematik zugelassenen Kartenterminals getestet:

- Ingenico ORGA 6141 (Firmware-Versionen 3.8.1 und 3.8.2)
- CHERRY ST-1506 (Firmware-Versionen 4.0.0 und 4.0.25)

Hinweis: Bitte halten Sie Ihre Kartenterminal-Firmware stets aktuell.

2.3 Vorbereitung

Eine URL zum sicheren Download des TlaaS Client Installationspakets wird vom TlaaS Anbieter zur Verfügung gestellt. Vor der Installation des TlaaS Clients müssen alle Systemanforderungen überprüft und die Betriebsumgebung entsprechend vorbereitet werden.

2.3.1 Windows

Für die Installation des TlaaS Client sind Berechtigungen zum Ausführen von folgenden Programmen notwendig:

- C:\Windows\System32\cmd.exe
- C:\Windows\System32\echo.exe
- C:\Windows\System32\find.exe
- C:\Windows\System32\netsh.exe
- C:\Windows\System32\sc.exe query
- C:\Windows\System32\schtasks.exe
- C:\Windows\System32\msiexec.exe
- C:\Program Files\WireGuard\wireguard.exe (falls vorhanden)

Bitte prüfen Sie vor dem Start der Installation des TlaaS Clients, ob Ihr PC-Benutzer alle notwendigen Berechtigungen besitzt. Wenn nicht, wenden Sie sich an Ihren Netzwerkadministrator.

2.3.2 macOS

2.3.2.1 Homebrew

Um im Zuge der Installation des TlaaS Clients die automatisierte Installation und Konfiguration des *WireGuard*-VPN-Clients durchführen zu können, ist eine Installation des Paketmanagers *Homebrew*¹ notwendig. Bei manueller Installation und Konfiguration des VPN-Clients muss *Homebrew* nicht installiert werden. Zur Installation von *Homebrew* führen Sie folgende Schritte durch:

1. Öffnen Sie die Applikation *Terminal*.
2. Prüfen Sie, ob Homebrew eventuell bereits installiert ist durch Eingabe von:

which brew

Bestätigen Sie die Abfrage mit Enter. Wird ein Dateipfad ausgegeben, so ist Homebrew bereits installiert und Sie können die Applikation *Terminal* wieder schließen. Wenn nicht, fahren Sie mit dem nächsten Schritt fort.

¹ Nähere Informationen zu Homebrew finden Sie unter <https://brew.sh/>

3. Zur Installation von Homebrew geben Sie folgenden Kommandozeilenbefehl ein:

```
/bin/bash -c "$(curl -fsSL  
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Bestätigen Sie die Installation mit Enter. Eventuell werden Sie zum Eingeben des Administratorpassworts aufgefordert.

4. Bei erfolgreicher Installation zeigt die Applikation folgende Information am Ende der Ausgabe als Antwort an:

```
==> Installation successful!
```

5. Um Homebrew zu den Systempfaden hinzuzufügen, geben Sie folgende Kommandozeilenbefehle ein:

```
(echo; echo 'eval "$(/opt/homebrew/bin/brew shellenv)"') >> ~/.zprofile  
eval "$(/opt/homebrew/bin/brew shellenv)"
```

2.3.2.2 Manuelle Installation des *WireGuard*-VPN-Clients

Unter Umständen kann es erforderlich sein, den vom TaaS Client benötigten VPN-Client unabhängig vom TaaS Client zu installieren. Wird *Homebrew* nicht genutzt, ist die manuelle Installation und Konfiguration des *WireGuard*-Clients erforderlich.

Befolgen Sie dafür folgende Schritte:

1. Rufen Sie den *App Store* auf und suchen Sie nach der App *WireGuard*.
2. Nutzen Sie die Schaltfläche *LADEN*, um die App Ihren Apps hinzuzufügen. Mit einem weiteren Klick auf *INSTALLIEREN* installieren Sie die App auf Ihrem Gerät. Eventuell wird eine Bestätigung der *Apple-ID* abgefragt.
3. Starten Sie *WireGuard*.
4. Wählen Sie die Schaltfläche *Tunnel aus Datei importieren* aus.
5. Wählen Sie die Datei *VPN_Configuration_xxx.conf* in Ihrem TIC Konfigurationspaket aus.
6. Nutzen Sie die Schaltfläche *Aktivieren*, um den neu hinzugefügten Tunnel zu starten.

2.3.3 Linux

2.3.3.1 WireGuard

Wenn *WireGuard* auf dem Gerät betrieben werden soll, wo der TaaS Client installiert wird, und gewünscht ist, dass die *WireGuard*-Verbindung im Zuge der Installation vom TaaS Client automatisch eingerichtet wird, dann müssen vorab die beiden Pakete *wireguard* und *wireguard-tools* installiert werden.

Um beide Pakete zu installieren, geben Sie folgenden Befehl im Terminal ein und bestätigen diesen mit Enter:

```
sudo apt install wireguard wireguard-tools -y
```

Soll die WireGuard-Verbindung von einem anderen Gerät aufgebaut werden, so ist eine manuelle Einrichtung von WireGuard auf jenem Gerät notwendig. Auf dem Gerät, wo der TI-Client läuft, muss in diesem Fall kein Wireguard installiert werden.

2.3.3.2 Curl

Zum Download des Zertifikats wird das Programm *curl* verwendet, das auf den meisten Linux Systemen bereits standardmäßig installiert ist. Sollte es auf ihrem System noch nicht installiert sein, geben Sie folgenden Befehl ein um das Paket nachträglich zu installieren:

```
sudo apt install curl -y
```

2.4 Installationsprozess

2.4.1 Windows und macOS

Zum Start der Installation des TlaaS Clients führen Sie die, zu Ihrem Betriebssystem passende, Installationsdatei *RISE_TlaaS_Client* aus. Kurz nach dem Start der Installation wird der Setup-Assistent vorbereitet (siehe Abbildung 1). Es wird dringend abgeraten, die Installation über den Windows Task-Manager bzw. die macOS Aktivitätsanzeige abubrechen, da dies zu unerwarteten Fehlern führen kann.

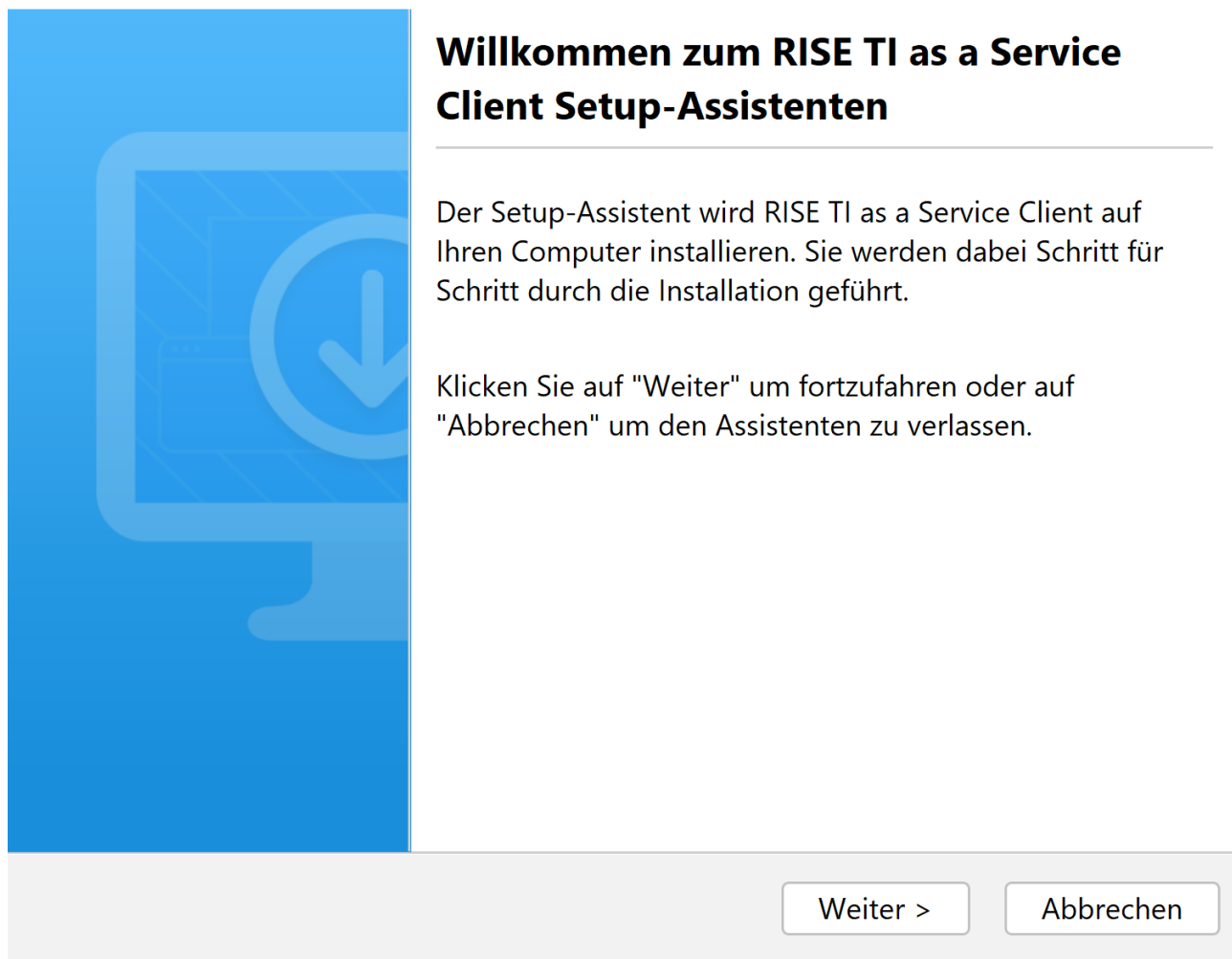


Abbildung 1: Vorbereitung des Setup-Assistenten zur Installation des TlaaS Clients

Folgende Schritte sind nun zum Abschluss der Installation notwendig:

1. **Startseite:** Folgen Sie den Anweisungen um den Installationsprozess des TlaaS Clients zu starten.
2. **Administratorberechtigung für die Installation erteilen:** Für die korrekte Installation und Funktion des TlaaS Clients wird eine Administratorberechtigung benötigt.
3. **Zielverzeichnis auswählen:** Es wird empfohlen, das Standard-Installationsverzeichnis nicht zu ändern (siehe Abbildung 2).
4. **Installationsoptionen:** Während der Installation können Sie optional folgende Einstellungen vornehmen, die beim Start des TlaaS Client bereits übernommen werden (siehe Abbildung 3):
 - **Löschen von obsoleten TI Routen:** Obsolete vorhandene Routen in die TI können mit der Installation des TlaaS Clients entfernt werden. Diese Aktion ist standardmäßig aktiviert. Insbesondere wenn ein Konnektor gewechselt wurde, müssen vorhandene Routen gelöscht werden, damit der TlaaS Client für Verbindungen in die TI verwendet wird. Wenn die Routen nicht gelöscht werden können, weil sie nicht mehr vorhanden sind, wird der Installationsprozess mit dem nächsten Schritt fortgesetzt.
 - **KIMaaS verwenden:** Wählen Sie diese Option aus, wenn Sie kein lokales Clientmodul, sondern KIM as a Service (KIMaaS) des TlaaS Anbieters nutzen möchten. Diese Aktion ist

standardmäßig deaktiviert.

Warnung: Falls Sie bereits ein lokales Clientmodul installiert haben, muss dieses zuerst deinstalliert werden bevor Sie mit der TaaS Client Installation fortfahren und KIMaaS nutzen können!

- **TaaS Client Port:** Der TaaS Client ist standardmäßig auf dem Port 8080 erreichbar. Wenn aufgrund des bestehenden Netzwerkaufbaus der TaaS Client einen anderen Port verwenden soll, kann dieser während der Installation angegeben werden.
 - **Externen Zugriff erlauben:** Wenn Sie möchten, dass der TaaS Client auch von anderen Geräten (das heißt, nicht nur von dem Gerät, auf dem der TaaS Client ausgeführt wird) erreichbar ist, können Sie diese Option aktivieren. Dies ermöglicht eine über HTTPS gesicherte Verbindung, die das Client-Zertifikat des Konnektors nutzt.
Warnung: Sollte dieses Client-Zertifikat nicht im Zertifikatsspeicher installiert sein, wird bei dem Versuch, eine Verbindung über den Webbrowser aufzubauen, eine Zertifikatswarnung ausgelöst. Es ist wichtig sicherzustellen, dass das in der Warnung angezeigte Zertifikat mit dem Client-Zertifikat übereinstimmt. Ist dies nicht der Fall, darf keine Verbindung hergestellt werden! Daher wird dringend empfohlen, das Client-Zertifikat im Zertifikatsspeicher abzulegen.
 - **TaaS Client HTTPS-Port:** Sollte die Option *Externen Zugriff erlauben* aktiviert sein, können Sie an dieser Stelle den Port festlegen, über den eine gesicherte HTTPS-Verbindung aufgebaut wird. Standardmäßig ist hier der Port 8443 vorgesehen.
 - **Automatische Updates aktivieren:** Mit dieser Option können Sie das automatische Suchen und Installieren von Updates aktivieren. Der Update-Zeitpunkt kann in der folgenden Option festgelegt werden.
 - **Update-Zeitpunkt:** Wurde die Option *Automatische Updates aktivieren* gewählt, so kann der tägliche Update-Zeitpunkt festgelegt werden. Ist eine neue Version des TaaS Clients verfügbar, so wird diese zum festgelegten Zeitpunkt installiert.
Warnung: Im Zuge eines Updates muss der TaaS Client neu gestartet werden. Es ist somit zum ausgewählten Update-Zeitpunkt mit einer möglichen Dienst-Unterbrechung zu rechnen.
Hinweis: Wird der TIC vor dem definierten Update-Zeitpunkt beendet, wird die Installation des Updates beim nächsten Start der Applikation durchgeführt.
 - **VPN-Paket nicht installieren:** Wenn Sie einen gesonderten WireGuard-Client oder ein WireGuard-fähiges VPN-Gateway nutzen, haben Sie hier die Möglichkeit, die Installation des mitgelieferten WireGuard-Clients zu überspringen. Bitte bedenken Sie dabei, dass dies eine manuelle Konfiguration des WireGuard-Clients bzw. des VPN-Gateways voraussetzt. Des Weiteren ist zu beachten, dass der TaaS Client in diesem Fall keine Aktualisierungen Ihrer bestehenden WireGuard-Installation durchführen wird, um sie auf dem neuesten Stand zu halten.
5. **TaaS Client Konfigurationsdatei auswählen:** Geben Sie den Pfad zur TaaS Client Konfigurationsdatei an, die Sie mit dem Installationspaket bereitgestellt bekommen haben. Es handelt sich um eine *.zip*-Archivdatei.

6. **Passwort für die Konfigurationsdatei eingeben:** Es handelt sich hierbei um den Bereitstellungscode, welcher im Rahmen der Produktbestellung festgelegt wurde.
7. **WireGuard Managementoberfläche (nur unter Windows):** Mit der TlaaS Client Installation wird auch der WireGuard VPN Client installiert. Dieses Tool wird für die Verbindung zum TlaaS RZ und somit zum vKonnektor benötigt. Die WireGuard Managementoberfläche erscheint kurz. Es ist keine Eingabe erforderlich.
8. **Abschluss der Installation:** Die Installation wurde erfolgreich beendet.

Achtung: Um einen einwandfreien Betrieb des TlaaS Clients garantieren zu können, muss das System nach Abschluss der Installation neu gestartet werden.

Um die grafische Benutzeroberfläche aufzurufen und die restlichen Konfigurationsschritte durchzuführen, die für die Verwendung des Clients notwendig sind, fahren Sie mit Abschnitt 3 und Abschnitt 10 fort.

Hinweis: Nur der Update-Service des TlaaS Clients wird mit Administrator-Rechten ausgeführt. Die Applikation selbst wird mit eingeschränkten Berechtigungen ausgeführt.

Hinweis: Die eingespielte Konfigurationsdatei darf nicht an Dritte weitergegeben werden. Aus Sicherheitsgründen wird empfohlen, die Konfigurationsdatei nach der Installation zu löschen.

Ziel-Ordner wählen

Wohin soll RISE TI as a Service Client installiert werden?



Bitte geben Sie an, in welchen Ordner Sie RISE TI as a Service Client installieren wollen, und klicken Sie danach auf "Weiter".

Erforderlicher Plattenplatz: 360 MB
Freier Plattenplatz: 3.454 MB

install4j

Abbildung 2: Auswahl des Installationsverzeichnis unter Windows

Installationsoptionen

Bitte wählen Sie die Installationsoptionen aus



Löschen von obsoleten TI Routen

KIMaaS verwenden ?

TaaS Client Port

Externen Zugriff erlauben

TaaS Client HTTPS-Port

Automatische Updates aktivieren

Update-Zeitpunkt :

VPN-Paket nicht installieren ?

install4j

< Zurück
Weiter >
Abbrechen

Abbildung 3: Installationsoptionen des TaaS Clients

2.4.2 Linux

Um den TaaS Client installieren zu können, müssen Sie zuerst die Paketquelle zu Ihrem System hinzufügen. Geben Sie dafür folgende Befehle im Terminal ein und bestätigen diese mit Enter:

```
sudo curl -fsSLo /usr/share/keyrings/rise-tiaas.gpg http://client.rise-tiaas.de/update-tiaas-pu/apt-repo/rise-tiaas.gpg
```

```
echo "deb [signed-by=/usr/share/keyrings/rise-tiaas.gpg] http://client.rise-tiaas.de/update-tiaas-pu/apt-repo/ stable main" | sudo tee /etc/apt/sources.list.d/rise-tiaas.list
```

```
sudo apt update
```

Um die Installation des TaaS Clients zu starten, geben Sie folgenden Befehl im Terminal ein und bestätigen diesen mit Enter:

```
sudo apt install rise_tiaas_client
```

Sollte nach einem Upgrade das Tlaas Client Service nicht verfügbar sein, aktivieren Sie das Service erneut. Geben Sie dazu folgende Befehle im Terminal ein und bestätigen diese mit Enter:

```
sudo systemctl enable rise-tiaas-client-service.service
```

```
sudo systemctl start rise-tiaas-client-service.service
```

Nachdem die Installation abgeschlossen wurde, müssen Sie den TlaaS Client mithilfe einer Konfigurationsdatei konfigurieren. Geben Sie dafür folgenden Befehl ein und bestätigen diesen mit Enter:

```
rise-tiaas-client-config <TIC_KONFIGURATIONSDATEI>
```

Ersetzen Sie durch Ihre Konfigurationsdatei, welche Sie für die Installation und Nutzung des TlaaS Clients verwenden wollen.

Nach der Angabe der Konfigurationsdatei wird der Konfigurationsassistent Sie durch die Konfiguration leiten und Ihnen Fragen stellen.

Zum Beantworten von geschlossenen Fragen stehen Ihnen Antwortmöglichkeiten hinter der Frage in eckigen Klammern ([/]) zur Auswahl. Zum Auswählen einer Antwortmöglichkeit geben Sie diese ein und bestätigen die Eingabe mit Enter. **Hinweis:** Ihnen werden bei geschlossenen Fragen Standardantworten vorgeschlagen, welche mit einem Großbuchstaben beginnen bzw. aus einem Großbuchstaben bestehen. Sie können die Standardantwort durch eine leere Eingabe auswählen. Im Folgenden sehen Sie ein Beispiel:

```
Enable external access [Y/n]:
```

Zum Beantworten der Frage mit Yes geben Sie ein Y ein oder belassen die Eingabe leer und bestätigen die Eingabe mit Enter. Zum Beantworten der Frage mit No geben Sie ein N ein und bestätigen die Eingabe mit Enter.

Zum Beantworten von offenen Fragen geben Sie Ihre Antwort ein und bestätigen diese mit Enter. **Hinweis:** Ihnen werden bei offenen Fragen Standardantworten vorgeschlagen, welche in eckigen Klammern ([/]) hinter der Frage angezeigt werden. Sie können die Standardantwort durch eine leere Eingabe auswählen. Im Folgenden sehen Sie ein Beispiel:

```
Enter the port for external access [8080]:
```

Zum Beantworten der Frage geben Sie Ihre Antwort ein und bestätigen diese mit Enter. Um die Standardantwort (8080) auszuwählen, lassen Sie die Eingabe leer und bestätigen diese mit Enter.

Hinweis: Bei der Eingabe von Antworten wird auf die Groß- und Kleinschreibung nicht geachtet.

Folgende Informationen sind für die Konfiguration notwendig:

- **KIMaaS verwenden:** Wählen Sie diese Option aus, wenn Sie KIM as a Service (KIMaaS) des TlaaS Anbieters nutzen möchten.

- **TlaaS Client Port:** Der TlaaS Client ist standardmäßig auf dem Port 8080 erreichbar. Wenn aufgrund des bestehenden Netzwerkaufbaus der TlaaS Client einen anderen Port verwenden soll, kann dieser an dieser Stelle angegeben werden.
- **Externen Zugriff erlauben:** Wenn Sie möchten, dass der TlaaS Client auch von anderen Geräten (das heißt, nicht nur von dem Gerät, auf dem der TlaaS Client ausgeführt wird) erreichbar ist, können Sie diese Option aktivieren. Dies ermöglicht eine über HTTPS gesicherte Verbindung, die das Client-Zertifikat des Konnektors nutzt.
Hinweis: Wenn der TlaaS Client auf einem System ohne einer grafischen Benutzeroberfläche (z.B. Server ohne Desktop) installiert wurde, muss der *Externe Zugriff* aktiviert sein, um von einem anderen Rechner in den TlaaS Client einzusteigen und diesen konfigurieren zu können. **Hinweis:** Wenn Sie diesen Punkt aktivieren, werden Sie aufgefordert einen ersten Benutzer anzulegen, um in den TlaaS Client einsteigen zu können. **Warnung:** Sollte dieses Client-Zertifikat nicht im Zertifikatsspeicher installiert sein, wird bei dem Versuch, eine Verbindung über den Webbrowser aufzubauen, eine Zertifikatswarnung ausgelöst. Es ist wichtig sicherzustellen, dass das in der Warnung angezeigte Zertifikat mit dem Client-Zertifikat übereinstimmt. Ist dies nicht der Fall, darf keine Verbindung hergestellt werden! Daher wird dringend empfohlen, das Client-Zertifikat im Zertifikatsspeicher abzulegen.
- **TlaaS Client HTTPS-Port:** Sollte die Option *Externen Zugriff erlauben* aktiviert sein, können Sie an dieser Stelle den Port festlegen, über den eine gesicherte HTTPS-Verbindung aufgebaut wird. Standardmäßig ist hier der Port 8443 vorgesehen.

Wenn die Konfiguration erfolgreich abgeschlossen wurde, wird Ihnen folgende Nachricht angezeigt:

Configuration of RISE TlaaS Client finished!

Achtung: Der TlaaS Client wird als Applikation im Hintergrund gestartet. Um die grafische Benutzeroberfläche aufzurufen und die restlichen Konfigurationsschritte durchzuführen, die für die Verwendung des Clients notwendig sind, fahren Sie mit Abschnitt 3 und Abschnitt 10 fort.

Hinweis: Die eingespielte Konfigurationsdatei darf nicht an Dritte weitergegeben werden. Aus Sicherheitsgründen wird empfohlen, die Konfigurationsdatei nach der Installation zu löschen.

3 Start, Stop und Überblick der Anwendung

Standardmäßig startet der TlaaS Client als Anwendung beim Hochfahren des Betriebssystems automatisch im Hintergrund. Sollte dies nicht der Fall sein oder sollten Sie den TlaaS Client manuell starten oder beenden wollen, folgen Sie den Schritten für Ihr Betriebssystem:

Windows:

1. Öffnen Sie die Windows Dienste, indem Sie in der Windows Suchleiste nach *Dienste* suchen.
2. Suchen Sie nach den beiden Diensten *RISE-TlaaS-Client Service* und *RISE-TlaaS-Client Updater*.
3. Starten bzw. Stoppen Sie die Dienste über die entsprechenden Schaltflächen.

Hinweis: Wenn Sie den TIC neu starten, stoppen Sie zuerst beide Dienste und starten anschließend beide wieder.

macOS:

1. Öffnen Sie die Applikation *Terminal*, wenn Sie sich nicht bereits in dieser befinden.
2. Führen Sie folgende Befehle zum Starten bzw. Stoppen des TlaaS Client:

Starten:

```
sudo launchctl load /Library/LaunchDaemons/com.rise-world.tiaas.client.application.plist
```

Stoppen:

```
sudo launchctl unload /Library/LaunchDaemons/com.rise-world.tiaas.client.application.plist
```

Linux:

1. Öffnen Sie die Applikation *Terminal*, wenn Sie sich nicht bereits in dieser befinden.
2. Führen Sie folgende Befehle zum Starten, Stoppen oder Neustarten des TlaaS Client aus:

Starten:

```
sudo systemctl start rise-tiaas-client-service
```

Stoppen:

```
sudo systemctl stop rise-tiaas-client-service
```

Neustarten:


```
sudo systemctl restart rise-tiaas-client-service
```

Hinweis: Es ist immer nur die Ausführung *einer* Instanz des TlaaS Clients erlaubt. Sollte die Anwendung bereits (im Hintergrund) laufen, ist kein erneuter Start möglich.

3.1 Aufrufen der Benutzeroberfläche

Nach dem Start der Anwendung kann die grafische Benutzeroberfläche des TlaaS Clients angezeigt werden. Dazu rufen Sie die URL <http://localhost:8080> über einen Webbrowser (siehe Abschnitt 2.1.4) auf.

Hinweis: Sollten Sie von einem anderen System aus auf den TlaaS Client zugreifen wollen, so können Sie eine gesicherte HTTPS-Verbindung verwenden, die über den bei der Installation angegebenen Port läuft. Wurde der TlaaS Client beispielsweise auf einem System mit der IP-Adresse 192.168.42.99 installiert und der Port 8443 für den externen Zugriff konfiguriert, können Sie den TlaaS Client über <https://192.168.42.99:8443> erreichen. Dort werden Sie zu einer Login-Seite weitergeleitet, auf der Sie sich authentifizieren müssen. Bitte beachten Sie, dass für diese Funktion der externe Zugriff während der Installation (siehe Abschnitt 2.4) konfiguriert werden muss.




BENUTZERNAME

PASSWORT

Anmelden

Login-Seite

Dafür muss auf dem System, auf das Sie zugreifen wollen, bereits ein Benutzer vorhanden sein. Sobald Sie einen Benutzernamen und ein Passwort eingegeben haben, wird die *Anmelden*-Taste aktiviert und Sie können sich einloggen.



BENUTZERNAME

PASSWORT

Anmelden

Login Seite mit ausgefülltem Formular

Sollte es diese Benutzername-Passwort-Kombination nicht geben, so erhalten Sie eine Fehlermeldung und bleiben auf der Login-Seite.

Benutzername/Passwort Kombination ist falsch!



BENUTZERNAME
superadmin

PASSWORT
••••••••

Anmelden

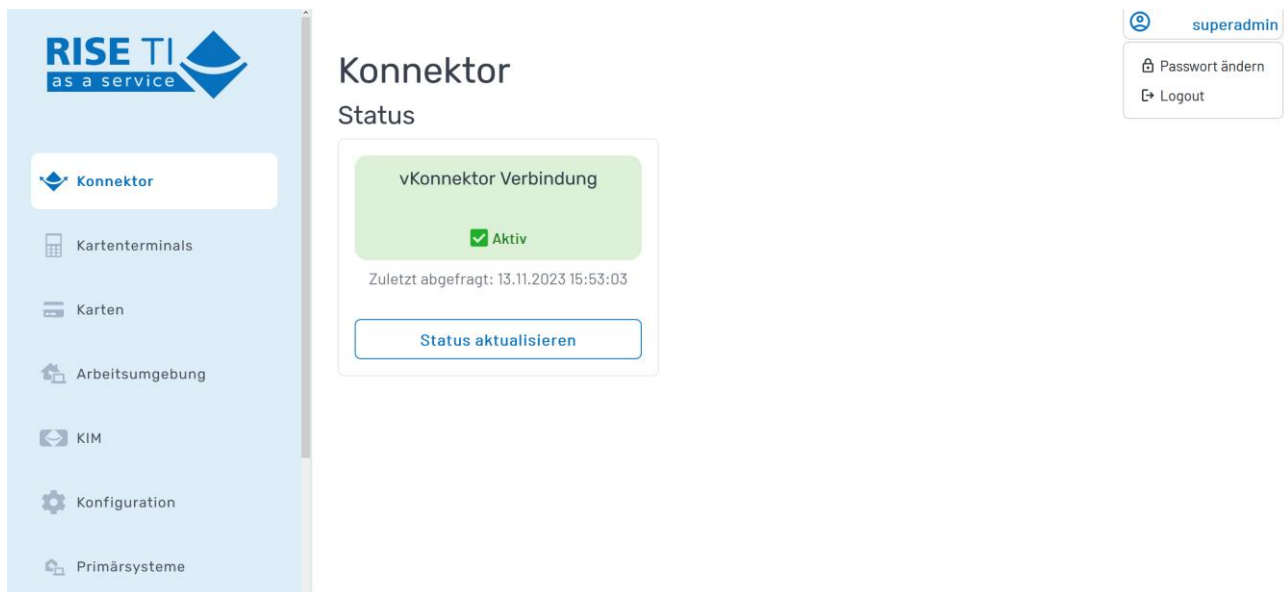
Ungültige Benutzername-Passwort-Kombination

Sollten Sie eine gültige Benutzername-Passwort-Kombination eingegeben haben, werden Sie auf die Konnektorseite (siehe Abschnitt 4) weitergeleitet.

Konnektorseite mit Profil

Sie sehen in der rechten oberen Ecke eine Leiste mit ihrem Benutzernamen. Sollten Sie diese Leiste betätigen, öffnet sich ein Menü mit zwei Optionen:

- Passwort ändern (siehe Abschnitt 9.3.1)
- Logout



Profil mit Menü

Sollten Sie die *Logout*-Taste betätigen, so werden Sie ausgeloggt und wieder auf die *Login*-Seite weitergeleitet.

3.2 Startseite

Nach dem Öffnen der Anwendung im Webbrowser wird die Startseite des TlaaS Clients angezeigt, wie in Abbildung 4 dargestellt. Von hier aus können die folgenden Menüpunkte erreicht werden:

- **Konnektor:** Hier können Sie den Verbindungsstatus zu Ihrem vKonnektor einsehen (siehe Abschnitt 4).
- **Karten:** Hier erhalten Sie eine Übersicht der gesteckten Karten und können diese verwalten (siehe Abschnitt 6).
- **Kartenterminals:** Hier können Sie Ihre Kartenterminals verwalten (siehe Abschnitt 5).
- **Arbeitsumgebung:** Hier können Sie die Arbeitsumgebung konfigurieren, die Sie zur Verwendung des vKonnektors benötigen (siehe Abschnitt 7).
- **KIM:** Falls Sie KIM as a Service nutzen möchten, können Sie hier eine Registrierung einer KIM E-Mail-Adresse durchführen oder Aktionen am Account Manager des KIM Fachdiensts authentisieren (siehe Abschnitt 8).
- **Konfiguration:** Hier können Sie Einstellungen zum TIC vornehmen und diesen neu starten (siehe Abschnitt 10).
- **Benutzerverwaltung:** Hier können Sie Benutzer für den externen Zugriff verwalten (siehe Abschnitt 9).

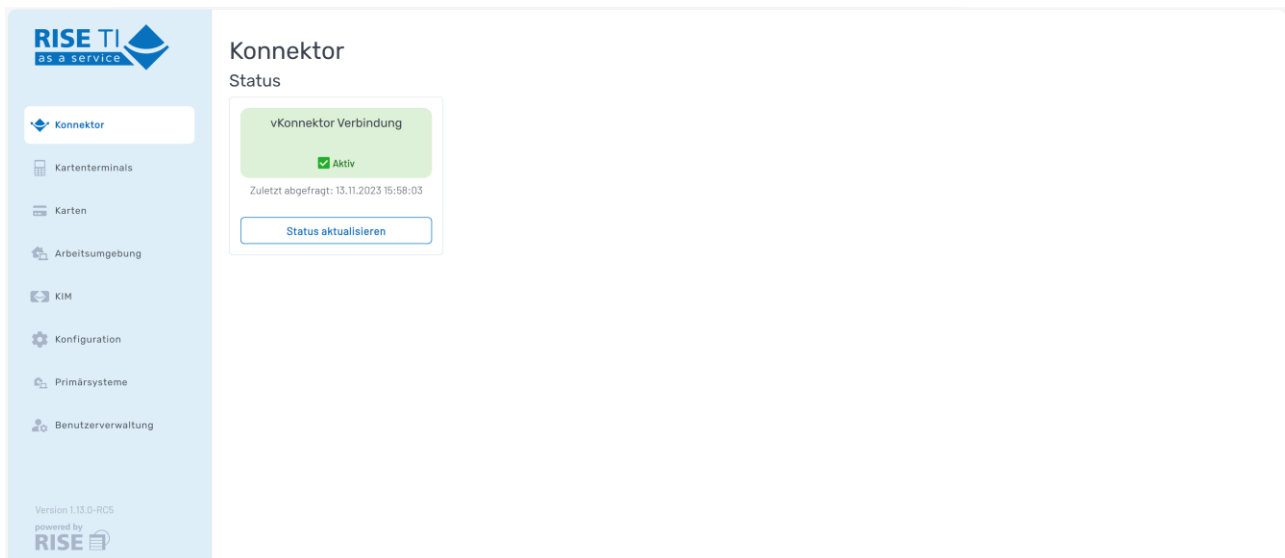


Abbildung 4: Begrüßungsbildschirm

Bitte beachten Sie:

- Beim Schließen der Benutzeroberfläche wird der TlaaS Client weiterhin im Hintergrund ausgeführt.
- Der TlaaS Client wird nach jedem Start des Betriebssystems automatisch gestartet.

3.3 Tabellen

Die im TlaaS Client einsehbaren Daten werden häufig in einer übersichtlichen Tabellenform präsentiert. Durch Auswahl der jeweiligen Spaltenüberschrift kann nach beliebigen Spalten sortiert werden. Ein neben der Spaltenüberschrift positionierter Pfeil kennzeichnet die Sortierreihenfolge: Ein nach oben zeigender Pfeil signalisiert eine aufsteigende, ein nach unten zeigender Pfeil eine absteigende Sortierung. Wenn beide Pfeile dargestellt sind, wird eine Standardsortierung angewandt.

3.4 Dialoge

Alle Dialogfenster des TlaaS Clients können auf die gleiche Weise über die Tastatur bedient werden. Beim Öffnen eines Dialogs wird automatisch das erste Element fokussiert. Die Auswahl des nächsten Elements erfolgt über die Tabulatortaste, das Zurückspringen zum vorherigen Element mittels der Tastenkombination Shift + Tabulatortaste. Ein Dialog kann jederzeit über die Escape-Taste geschlossen sowie über die Tastenkombination Strg + Eingabetaste bestätigt werden.

4 Konnektor

Unter dem Menüpunkt *Konnektor* lässt sich der aktuelle Verbindungsstatus zum vKonnektor im TlaaS RZ einsehen. Der Verbindungsstatus mit dem vKonnektor wird regelmäßig im Hintergrund überprüft und gemeinsam mit dem Datum und der Uhrzeit der letzten Abfrage in der Benutzeroberfläche dargestellt (siehe Abbildung 5 und Abbildung 6). Bei Verfügbarkeit des vKonnektors wird ein grünes, bei

Nichtverfügbarkeit ein rotes Symbol angezeigt. Zudem kann über Auswahl von *Status aktualisieren* die Prüfung des Verbindungsstatus jederzeit manuell gestartet werden.

Hinweis: Beim Aufrufen des Menüpunktes *Konnektor* wird der Status automatisch aktualisiert. Während der Aktualisierung wird der Konnektor als *nicht verfügbar* angezeigt.

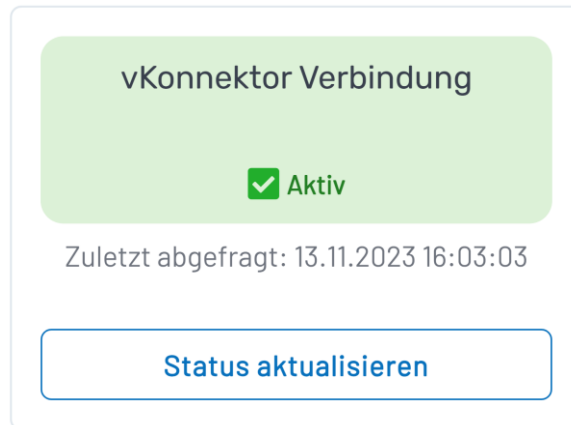


Abbildung 5: Erfolgreicher Verbindungsstatus des Konnektors

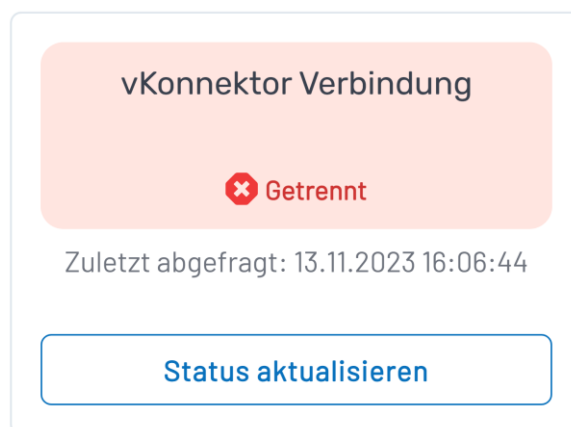


Abbildung 6: Nicht erfolgreicher Verbindungsstatus

5 Kartenterminals

Unter dem Menüpunkt *Kartenterminals* können Kartenterminals verwaltet und mit dem vKonnektor gepairt werden.

5.1 Kartenterminalübersicht

Wenn Kartenterminals mit dem TlaaS Client verbunden sind, werden diese in der Kartenterminalübersicht dargestellt (siehe Abbildung 7). Es können bis zu 20 Kartenterminals mit dem TlaaS Client verbunden sein.

Kartenterminals + Hinzufügen

HOSTNAME	LOKALE IP-ADRESSE	MAC-ADRESSE	PORT	STATUS	PROXY-STATUS	PROXY-PORT
ORGA6100-0241000000B954	192.168.42.12	00:0D:F8:0C:89:16	4742	AKTIV VERBUNDEN	AKTIV	9000

Abbildung 7: Kartenterminalübersicht

Hinweis: Es werden nur Kartenterminals aufgelistet, die mit der aktiven TlaaS Client Installation verbunden sind.

5.2 Kartenterminal hinzufügen und pairen

Um ein Kartenterminal hinzuzufügen, wählen Sie *Hinzufügen* aus, um den entsprechenden Dialog zu öffnen (siehe Abbildung 8).

Kartenterminal hinzufügen
×

NETZWERKINTERFACE

▼

KARTENTERMINAL IP-ADRESSE

Admin-Session PIN speichern

Abbrechen

Kartenterminal hinzufügen

Abbildung 8: Kartenterminals hinzufügen

Für das Pairing muss sowohl ein *Netzwerkinterface* als auch die *Kartenterminal IP-Adresse* angegeben werden.

- **Netzwerkinterface:** Name und IP-Adresse des Netzwerkinterfaces, mit dem das Kartenterminal erreichbar ist. Die IP-Adresse des Netzwerkinterfaces befindet sich üblicherweise im selben Sub-Netz wie das Kartenterminal (siehe Abbildung 9).

- **Kartenterminal IP-Adresse:** Die IP-Adresse, über die das oberhalb ausgewählte Netzwerkinterface das Kartenterminal erreichen kann. Wenden Sie sich an Ihren Netzwerkadministrator, wenn Sie nicht über Ihre Kartenterminal IP-Adresse verfügen.

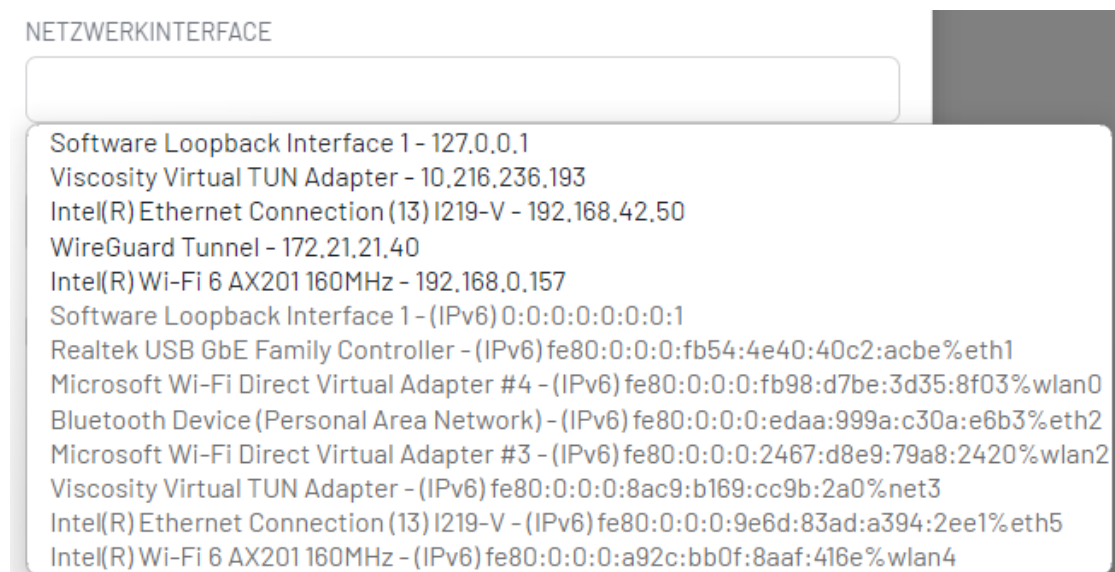


Abbildung 9: Auswahl des Netzwerkinterfaces

Um ein Kartenterminal mit den eingegebenen Daten zu verbinden, starten Sie den Prozess über die Auswahl von *Hinzufügen und Pairing starten*. Dabei werden folgende Schritte vom TlaaS Client durchgeführt:

1. Anhand der eingegebenen IP-Adresse wird ein SICCT Service Discovery Paket an das Kartenterminal gesendet.
2. Das Kartenterminal antwortet dem TlaaS Client mit einem SICCT Service Announcement.
3. Der TlaaS Client entnimmt dem SICCT Service Announcement vom Kartenterminal die für das Pairing benötigten Informationen.
4. Danach startet der TlaaS Client die Verbindung und das Pairing des Kartenterminals mit dem vKonnektor. Eine Meldung am Display des Kartenterminals bestätigt das erfolgreiche Pairing.
5. Nach dem erfolgreichen Pairing erscheint ein Dialog zur Speicherung der Admin-Session-PIN (siehe Abschnitt 5.5).
6. Es erscheint ein Hinweis zur Hinterlegung des Informationsmodells; dieses muss im TlaaS Client konfiguriert sein, damit das Kartenterminal erfolgreich mit dem vKonnektor kommunizieren kann.
7. Das erfolgreich hinzugefügte und verbundene Kartenterminal wird in der Kartenterminalübersicht angezeigt.

Sollte das Pairing des Kartenterminals fehlschlagen, wird das Kartenterminal in der Kartenterminalübersicht nicht angezeigt.

Hinweis: Bei der ersten Inbetriebnahme des TlaaS Clients und nach dem ersten erfolgreichen Pairing eines Kartenterminals über den Client, konfigurieren Sie bitte Ihre gewünschte Arbeitsumgebung, die Sie für die Nutzung mit dem vKonnektor verwenden möchten. Nähere Informationen finden Sie dazu im Abschnitt 7.

Hinweis: Falls Sie ein Primärsystem (z. B. eine Praxisverwaltungssoftware) verwenden und dort ein eigenes TLS-Client-Zertifikat für die Kommunikation mit dem TlaaS RZ verwenden möchten, übermittelt Sie bitte dieses TLS-Client-Zertifikat an den TlaaS Anbieter.

Hinweis: Es ist wichtig, dass Sie sich das Einstellungspasswort Ihres Kartenterminals gut merken, da es für Operationen (wie z.B. Pairing und Firmware Update) verwendet wird.

5.3 Kartenterminal neu verbinden

Sollte die Verbindung zwischen einem Kartenterminal und dem TlaaS Client verloren gehen, was dem Status *Aktiv und nicht verbunden* entspricht, können Sie diese Verbindung manuell wieder aufbauen. Wählen Sie dazu in der Kartenterminalübersicht *Kartenterminal neu verbinden*, um die Verbindung zum Kartenterminal erneut zu initiieren.

Hinweis: Die Kartenterminals werden grundsätzlich automatisch wieder verbunden, jedoch das kann bis zu 5 Minuten dauern. Eine manuelle Neuverbindung ist möglich, um nicht auf die automatische Wiederherstellung warten zu müssen.

5.4 Kartenterminal entfernen

Ein verbundenes Kartenterminal kann in der Kartenterminalübersicht durch die Auswahl von *Kartenterminal entfernen* wieder entfernt werden. Dafür muss die Auswahl der Aktion durch die Anzeige *Wollen Sie das Kartenterminal wirklich entfernen?* bestätigt werden.

Hinweis: Nur Kartenterminals, die durch den TlaaS Client mit dem vKonnektor verbunden wurden, können vom Benutzer entfernt werden.

5.5 Admin-Session-PIN hinterlegen

Das lokale Hinterlegen oder Aktualisieren der Admin-Session-PIN² kann durch die Auswahl von *Admin-Session-PIN hinterlegen...* im Kontextmenü des Kartenterminals erfolgen.

5.6 Admin-Session-PIN automatisch synchronisieren

Die Admin-Session-PIN wird automatisch nach dem TIC Start mit einer Verzögerung von 3 Minuten sowie in regelmäßigen Intervallen mit dem Konnektor synchronisiert. Das Synchronisationsintervall ist in der Konfigurationsdatei (Abschnitt 10.4) konfigurierbar. Bei der Synchronisation wird die PIN am Konnektor mit dem lokalen überschrieben.

² Admin-Session-PIN: Die Kartenterminal-PIN für die SICCT Admin-Session, die vom Konnektor bei Kartenterminal-Firmware Updates aufgebaut wird.

5.7 Admin-Session-PIN manuell synchronisieren

Das manuelle Synchronisieren der Admin-Session-PIN mit dem Konnektor kann durch die Auswahl von *Admin-Session-PIN synchronisieren...* im Kontextmenü des Kartenterminals erfolgen. Bei der Synchronisation wird die PIN am Konnektor mit dem lokalen überschrieben. Diese Option ist erst verfügbar, nachdem eine Admin-Session-PIN hinterlegt worden ist.

5.8 Admin-Session-PIN entfernen

Das Entfernen der Admin-Session-PIN am Konnektor kann durch die Auswahl von *Admin-Session-PIN entfernen...* im Kontextmenü des Kartenterminals erfolgen. Diese Option ist erst verfügbar, nachdem eine Admin-Session-PIN hinterlegt worden ist.

6 Karten

Unter dem Menüpunkt *Karten* erhalten Sie eine Übersicht der gesteckten Karten über alle Ihre Kartenterminals und können diese verwalten. Entsprechend dem Kartentyp stehen im zugehörigen Kontextmenü unterschiedliche Aktionen zur Auswahl.

6.1 Kartenübersicht

In der Kartenübersicht werden alle Ihre gesteckten Karten über alle Kartenterminals dargestellt (siehe Abbildung 10). Dabei werden der Kartentyp, das Kartenterminal mittels der ID und MAC-Adresse sowie das Einsteckdatum und das Ablaufdatum des Zertifikates angezeigt. Zudem können die einzelnen angezeigten Karten über ein Kontextmenü verfügen, über das ausgewählte PIN-Operationen an den Karten in den verbundenen Kartenterminals durchgeführt werden können. Nach Abfrage über das Kontextmenü wird ein Status mit zusätzlichen Informationen dargestellt.

Karten

KARTENTYP	KARTENTERMINAL	EINSTECKDATUM	ABLAUFDATUM ZERT.	STATUS
SMCBG2_1	ORGA6100-0241000000B954 (MAC: 00:0D:F8:0C:89:16)	15.12.2022 10:46	11.12.2024	SMCB: VERIFIZIERT
HBAG2_1	ORGA6100-0241000000B954 (MAC: 00:0D:F8:0C:89:16)	15.12.2022 10:46	11.12.2024	CH: TRANSPORT-PIN QES: VERIFIZIERBAR
EGKG2_1	ORGA6100-0241000000B954 (MAC: 00:0D:F8:0C:89:16)	15.12.2022 10:46	22.01.2025	
gSMC-KT	ORGA6100-0241000000B954 (MAC: 00:0D:F8:0C:89:16)	15.12.2022 10:46	06.03.2026	

Abbildung 10: Kartenübersicht

6.2 Kartenaktionen

Nachdem die Karten aufgelistet wurden, stehen Ihnen für die Kartentypen SMC-B und HBA durch Auswahl des Kontextmenüs verschiedene Operationen zur Verfügung. Dabei handelt es sich jeweils um PIN-Operationen, die mit einer Erfolgsmeldung oder einer Fehlermeldung (siehe Abschnitt 16.4) abgeschlossen werden.

Folgende Aktionen stehen zur Verfügung:

- Für SMC-B-Karten (siehe auch Abbildung 11):
 - Remote PIN+ einrichten
 - PIN-Status abfragen
 - PIN verifizieren
 - PIN ändern
 - PIN entsperren

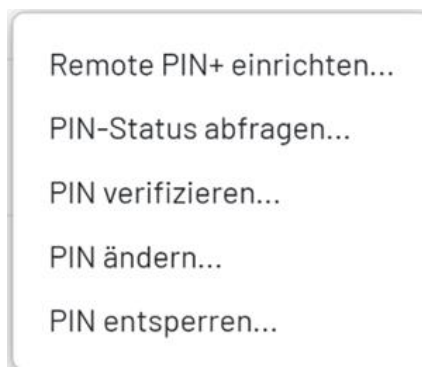


Abbildung 11: PIN-Operationen für SMC-B Karten

- Für HBA-Karten (siehe auch Abbildung 12)
 - CH-PIN-Status abfragen
 - CH-PIN ändern
 - CH-PIN entsperren
 - QES-PIN-Status abfragen
 - QES-PIN ändern
 - QES-PIN entsperren

Hinweis: Nach der Auswahl einer Operation beachten Sie bitte die Anzeige an Ihrem Kartenterminal, in dem die betreffende Karte gesteckt ist.

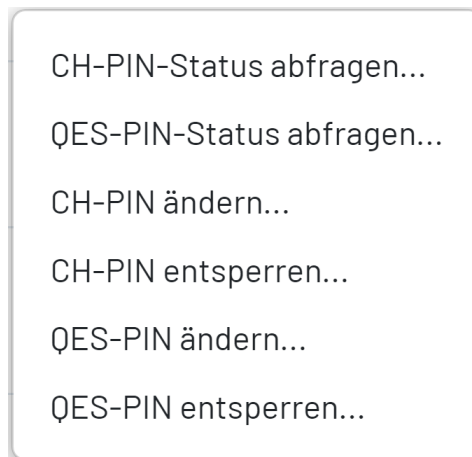


Abbildung 12: PIN-Operationen für HBA Karten

6.2.1 PIN-Status abfragen

Für transportgeschützte PINs wird die Art des Transportschutzes angegeben. Für PINs kann die Anzahl der noch verbleibenden Versuche für PIN-Verifikationen ermittelt werden oder ob die PIN bereits verifiziert wurde.

Neben der PIN für SMC-B Karten gibt es bei HBA Karten sowohl die QES-PIN für die qualifizierte elektronische Signatur und die CH-PIN für die Verschlüsselungs- und Authentifizierungsfunktionalität.

Hinweis: Wenn es für einen Kartentyp mehrere verschiedene PINs gibt, können die Operationen auf PIN-Ebene ausgewählt werden.

6.2.2 PIN verifizieren

Um eine SMC-B Karte freizuschalten, kann im TlaaS Client die Verifikation einer PIN ausgelöst werden. Bitte achten Sie auf die Meldung am Display des Kartenterminals und bestätigen Sie die Verifikation.

Bei erfolgreicher Verifikation wird der PIN-Status dargestellt, ansonsten erscheint eine Fehlermeldung entsprechend Abschnitt 16.4.

6.2.3 PIN ändern

Über die entsprechende Auswahl im Kontextmenü kann eine PIN geändert werden. Wird diese Operation ausgewählt, ist am Kartenterminal sowohl die alte als auch die neue PIN einzugeben.

Bei erfolgreicher Änderung wird eine Erfolgsmeldung angezeigt, ansonsten erscheint eine Fehlermeldung entsprechend Abschnitt 16.4.

6.2.4 PIN entsperren

Wenn eine PIN blockiert wurde, kann eine Freischaltung durch die entsprechende Auswahl im Kontextmenü der Karte ausgelöst werden. Dabei muss zunächst am PIN-Pad des Kartenterminals ein PUK eingegeben werden. Anschließend kann ebenso am Kartenterminal eine neue PIN gesetzt werden. Abschließend wird der Zähler für PIN-Eingabeversuche auf den Anfangswert zurückgesetzt.

Hinweis: Der PUK einer Karte kann maximal 10 mal eingegeben werden. Sollte der PUK nicht mehr eingebbar und die Karte gesperrt sein, muss eine neue Karte bestellt werden.

6.2.5 Remote PIN+

Die Funktion *Remote PIN+* erlaubt das automatische Verifizieren von Karten mit einer hinterlegten PIN. Aktuell steht diese Funktion nur für SMC-B Karten in Verbindung mit einem Cherry ST-1506 Kartenterminal zur Verfügung.

Um die Funktion nutzen zu können, müssen am Kartenterminal die Remote-Schnittstelle und die Remote-PIN-Eingabe für den entsprechenden Kartensteckplatz aktiviert sein. Unter dem Menüpunkt *Karten* im TIC wird der Status *PIN+ bereit* angezeigt, wenn die Funktion für diese Karte verfügbar ist (siehe Abbildung 13). Die Funktion kann über die Kartenaktion *Remote PIN+ einrichten* erstmalig eingerichtet werden. Zum Einrichten sind die PIN der Karte und die Admin-PIN des Kartenterminals notwendig. Die PINs werden verschlüsselt im TIC hinterlegt. Bei erfolgreicher Aktivierung wechselt der Status der Karte von *PIN+ bereit* zu *PIN+ aktiviert*. Der Status wird nun alle fünf Minuten vom TIC abgerufen. Wenn der Kartenstatus *Verifizierbar* ist, verifiziert die Funktion *Remote PIN+* die Karte mit der hinterlegten PIN. Mit der Kartenaktion *Remote PIN+ deaktivieren* kann die Funktion deaktiviert und die hinterlegte PIN gelöscht werden.

Hinweis: Kommt es beim Verifizieren einer Karte zu einem Fehler, wird die Funktion Remote PIN+ für diese Karte deaktiviert und muss durch eine erneute PIN-Eingabe wieder aktiviert werden.

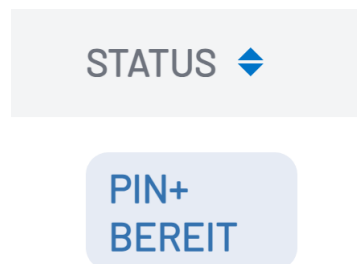


Abbildung 13: PIN+ Statusanzeige

7 Arbeitsumgebung

Unter dem Menüpunkt *Arbeitsumgebung* können Sie Mandanten, Arbeitsplätze und Clientsysteme dem vKonnektor zuweisen und die Zuordnungen von Mandanten, SMC-B Karten, Arbeitsplätzen und Clientsystemen vornehmen.

Hinweis: Aufgrund von Konnektorbeschränkungen sind die Namen von Entitäten der Arbeitsumgebung auf maximal 31 Zeichen beschränkt. Es dürfen nur Groß- und Kleinbuchstaben, Zahlen und Bindestriche sowie Unterstriche verwendet werden. Andere Sonderzeichen und Umlaute sind nicht zulässig.

Das Menü der Arbeitsumgebung ist in zwei Bereiche eingeteilt, die ähnlich funktionieren.

7.1 Begriffserläuterung von Mandant, Arbeitsplatz und Clientsystem

Mandant: Ein Mandant ist eine Organisationseinheit innerhalb einer Institution. Beispiele: Arzt, Abteilung in einem Krankenhaus, Labor

Arbeitsplatz: Damit sind alle dem Mandanten zugeordneten Arbeitsplätze gemeint. Diese beinhalten PCs, aber auch virtuelle Arbeitsplätze. Beispiele: Arztzimmer, Behandlungsraum, Rezeption

Clientsystem: Unter einem Clientsystem wird hier ein einzelnes oder eine Gruppe von Systemen verstanden, welche im LAN der Einsatzumgebung auf die Clientsystem-Schnittstelle des Konnektors zugreifen. Beispiele: Primärsystem, Praxisverwaltungssystem, Kundenverwaltungssystem

7.2 Verwaltung von Mandanten, Arbeitsplätzen, Clientsystemen

Diese Ansicht dient der Verwaltung von Mandanten, Arbeitsplätzen und Clientsysteme der Arbeitsumgebung und ist in Abbildung 14 dargestellt. Die Assoziationen dieser Entitäten miteinander und mit Kartenterminals sowie SMC-B Karten bilden die Arbeitsumgebung, die dem vKonnektor hinzugefügt werden kann.

Hinweis: Alle hinzugefügten und gelöschten Entitäten bleiben nur temporär gespeichert, bis diese durch Auswahl von *Arbeitsumgebung speichern* an den vKonnektor übertragen werden. Beim Verlassen oder Aktualisieren dieser Seite ohne vorheriger Übertragung an den vKonnektor werden alle Änderungen verworfen.

1. **Eingabe:** Fügen Sie im Eingabefeld den Namen für eine neue Entität ein.
 - Bei Erstellung eines neuen Mandanten erscheint dieser in der Übersicht der Arbeitsumgebung.
 - Arbeitsplätze lassen sich in der Übersicht der Arbeitsumgebung Mandanten zuweisen.
 - Clientsysteme lassen sich in der Übersicht der Arbeitsumgebung Mandanten zuweisen.
2. **Hinzufügen der Entität:** Nach der Eingabe des Namens erstellen Sie die Entität durch Auswahl von *Hinzufügen*.
3. **Löschen einer Entität:** Durch die Auswahl des Löschen-Symbols wird die Entität aus der Liste der vorhandenen Entitäten gelöscht.

The screenshot shows a web interface for setting up the work environment. At the top, there are two tabs: 'Arbeitsumgebung einrichten' (selected) and 'Mandanten, Arbeitsplätze, Clientsysteme'. Below the tabs, there are three main sections: 'Mandanten', 'Arbeitsplätze', and 'Clientsysteme'. Each section has a dropdown menu with a '1' next to it and a 'Hinzufügen' button with a '2' next to it. Below each dropdown, there is a list of items with a red 'X' icon and a '3' next to it. In the 'Mandanten' section, the item is 'm'. In the 'Arbeitsplätze' section, the item is 'a (Nicht zugewiesen)'. In the 'Clientsysteme' section, the item is 'c'. At the bottom left, there is a blue button labeled 'Arbeitsumgebung speichern'.

Abbildung 14: Verwaltung der Entitäten Mandant, Arbeitsplatz und Clientsystem

7.3 Arbeitsumgebung einrichten

Diese Ansicht bildet die Arbeitsumgebung des vKonnektors ab, wie in Abbildung 15 dargestellt.

- Die angelegten Mandanten erhalten jeweils einen eigenen Eintrag.
- Nach Auswahl eines Mandanten können weitere Einstellungen verändert werden.
- Alle Entitäten lassen sich über die vorhandenen Dropdown-Menüs zuweisen.
- Bei Clientsystemen und Arbeitsplätzen ist es möglich, mehrere Zuweisungen pro Mandant durchzuführen.
- Per Auswahl auf das X-Symbol lassen sich Zuweisungen der Entitäten aufheben.

Hinweis: Alle getätigten Einstellungen bleiben nur temporär gespeichert, bis diese durch Auswahl von *Arbeitsumgebung speichern* an den vKonnektor übertragen werden. Beim Verlassen oder Aktualisieren dieser Seite ohne vorheriger Übertragung an den vKonnektor werden alle Änderungen verworfen.

Abbildung 15: Mandantenansicht

8 Kommunikation im Medizinwesen (KIM)

Unter dem Menüpunkt *KIM* (Kommunikation im Medizinwesen) finden Sie Aktionen, die Sie im Rahmen von KIM as a Service (KIMaaS) durchführen können. Dieser Abschnitt ist für Sie nur relevant, wenn Sie KIMaaS verwenden möchten. Dafür ist keine Installation eines lokalen KIM Clientmoduls notwendig. Falls Sie ein lokales KIM Clientmodul bereits installiert haben, beenden und deinstallieren Sie dieses bevor Sie den TaaS Client installieren.

Der im TaaS Client integrierte *KIM Authenticator* (Authentication Client) ermöglicht die Authentisierung von Aktionen am Account Manager des KIM Fachdiensts. Weiters können Sie direkt im TaaS Client eine neue KIM E-Mail-Adresse registrieren (siehe Abbildung 16).

Sofern Sie die Option *KIMaaS verwenden* bei der TaaS Client Installation (siehe Abschnitt 2.4) ausgewählt haben, ist die KIMaaS-Funktionalität des TaaS Clients sofort verwendbar. Wurde diese Option bei der Installation nicht ausgewählt, kann die KIMaaS-Funktionalität auch nachträglich aktiviert werden. Bitte stellen Sie davor sicher, dass kein lokales Clientmodul mehr installiert ist. Dann wählen Sie unter dem Menüpunkt *KIM* die Checkbox *KIMaaS verwenden* aus und starten den TaaS Client neu um die Änderung zu übernehmen (siehe Abbildung 17). Nach dem Neustart ist die KIMaaS-Funktionalität des TaaS Clients verwendbar.

KIM

Registrierung

[KIM E-Mail Registrierung starten](#)

Wie nutze ich den KIM Authentikator?

Der KIM Authentikator hilft Ihnen, sich bei Aktionen im Account Manager des KIM Fachdienstes zu authentifizieren.

Führen Sie dazu folgende Schritte aus:

1. Öffnen Sie einen aktuellen Chrome- oder Firefox Browser.
2. Öffnen Sie den Account Manager, wählen Sie Ihre KIM Account-Aktion aus und wechseln Sie nach Start der Authentifizierung wieder in diesen Tab <https://am-ref.kim.service-ti.de>
3. Folgen Sie den Anweisungen. Nach erfolgter Authentifizierung kann die Kontoaktion im Account Manager fertig durchgeführt werden.

KIMaaS verwenden

Änderungen werden erst nach Neustart des TlaaS Clients durchgeführt.

Abbildung 16: Übersicht der KIMaaS-Funktionen im TlaaS Client

KIM

⚠ Um KIMaaS nutzen zu können, muss die lokale Clientmodulinstallation deinstalliert sein!

💡 Möchten Sie KIMaaS verwenden?

KIMaaS verwenden

Änderungen werden erst nach Neustart des TlaaS Clients durchgeführt.

Abbildung 17: Nicht aktivierte KIMaaS-Funktionen im TlaaS Client

8.1 KIM Authentisierung

Manche Aktionen im Account Manager des KIM Fachdiensts benötigen eine Authentisierung mittels des verfügbaren AUT Zertifikats einer in einem Kartenterminal gesteckten HBA bzw. SMC-B Karte. Dazu verwenden Sie bitte den im TlaaS Client integrierten KIM Authentikator.

Um den KIM Authentikator verwenden zu können, muss der TlaaS Client zunächst gestartet, entsprechend konfiguriert (siehe Abschnitt 10) und in einem Webbrowser geöffnet sein.

Öffnen Sie nun in einem weiteren Browser-Tab den Account Manager des KIM Fachdiensts um die gewünschte Aktion durchzuführen (z. B. Änderung von Accountdaten oder die Verwaltung von Abwesenheitsnotizen). Bei einer ausgewählten Aktion, die eine Authentisierung benötigt, sehen Sie im Account Manager die Meldung *“Bitte Authentisierung durchführen”*. Wechseln Sie wieder zurück in den Browser-Tab des TlaaS Clients und folgen Sie dort den Anweisungen. Wenn die Authentisierung erfolgreich war, können Sie wieder zum Account Manager zurückwechseln und die ausgelöste Aktion fertig durchführen.

Hinweis: Die Authentisierung ist nur mit einem Google Chrome oder einem Firefox Webbrowser durchführbar. Des Weiteren ist zu beachten, dass der Account Manager und der TlaaS Client in separaten Browser-Tabs geöffnet sein müssen.

Diese Anleitung finden Sie auch in der grafischen Benutzeroberfläche unter dem Menüpunkt *KIM* wie in Abbildung 18 dargestellt. Die benötigte KIM Authentisierung wird entsprechend der Anleitung im Menüpunkt *KIM* des TlaaS Clients vom Account Manager automatisch gestartet.

Wie nutze ich den KIM Authentifikator?

Der KIM Authentifikator hilft Ihnen, sich bei Aktionen im Account Manager des KIM Fachdienstes zu authentifizieren.

Führen Sie dazu folgende Schritte aus:

1. Öffnen Sie einen aktuellen Chrome- oder Firefox Browser
2. Öffnen Sie den [Account Manager](#), wählen Sie Ihre Kontotaktion aus und wechseln Sie nach Start der Authentifizierung wieder in diesen Tab
3. Folgen Sie den Anweisungen. Nach erfolgreicher Authentifizierung kann die Kontoaktion im Account Manager fertig durchgeführt werden.

Abbildung 18: Anleitung zur Verwendung des KIM Authentifikators

Folgende KIM-Account-Aktionen im Account Manager können nach erfolgter KIM Authentisierung im TlaaS Client durchgeführt werden:

- Passwort ändern
- Passwort zurücksetzen
- Stammdaten ändern
- Abwesenheitsnotiz einrichten
- Recovery E-Mail-Adresse ändern

Achtung: Beide Browser-Tabs (TlaaS Client und Account Manager) müssen die ganze Zeit der Authentisierung geöffnet bleiben.


Wenn im TlaaS Client eine KIM Authentisierung durch den Account Manager gestartet wurde, sind folgende Schritte zum Abschluss der Authentisierung notwendig:

1. **Auswahl des Aufrufkontexts für die Authentisierung:** Wählen Sie den Aufrufkontext, für den die Authentisierung durchgeführt werden soll (siehe Abbildung 19). Der Aufrufkontext umfasst die Angaben zu Mandant (*MandantId*), Arbeitsplatz (*Workplaceld*), Anwendung (*ClientSystemId*) und Identifikation des Benutzers (*UserId*). Die Angaben zur Identifikation des Benutzers (*UserId*) sind optional und nur für einen Zugriff auf eine HBA Karte erforderlich. Um die KIM Authentisierung mit einer entsprechenden SMC-B Karte durchzuführen, wählen Sie Mandant, Arbeitsplatz und Clientsystem aus. Um die KIM Authentisierung mit einer HBA Karten durchzuführen, geben Sie eine UserID ein.
Hinweis: Wenn Sie im Menü *Arbeitsumgebung* (siehe Abschnitt 7) noch keine Arbeitsumgebung eingerichtet haben, wird eine Fehlermeldung angezeigt. Sobald zumindest ein Mandant, ein Arbeitsplatz und ein Clientsystem in der Arbeitsumgebung eingetragen wurden, können Sie die KIM Authentisierung mit dem TlaaS Client nutzen.
2. **Auswahl einer Karte für die Authentisierung:** Anhand Ihres eingegebenen Aufrufkontexts werden die verfügbaren SMC-B bzw. HBA Karten geladen und zur Auswahl angezeigt (siehe Abbildung 20). Wählen Sie eine Karte aus, die Sie für die KIM Authentisierung verwenden möchten, und starten Sie die Authentisierung. Wählen Sie *Abbrechen* um zur Eingabe des Aufrufkontexts zurückzukehren.
3. **Durchführung der Authentisierung:** Mittels der Auswahl von *Authentifizierung starten* und des verfügbaren Kartenmaterials der ausgewählten Karte wird die Authentisierung durchgeführt.
Hinweis: Sofern die ausgewählte Karte nicht freigeschaltet ist, ist eine PIN-Eingabe am Kartenterminal zur Freischaltung notwendig. Folgen Sie dazu den entsprechenden Ausweisungen am Kartenterminal.

4. **Abschluss der Authentisierung:** Wenn die Authentisierung erfolgreich war, wird eine entsprechende Erfolgsmeldung angezeigt und Sie können nun die ausgewählte Aktion im Account Manager fortsetzen. Wechseln Sie dazu wieder in den noch offenen Browser-Tab des Account Managers.

Falls es zu einem Problem bei der Authentisierung gekommen ist, wird eine entsprechende Fehlermeldung mit Abbruch des Vorgangs angezeigt.


KIM E-Mail Registrierung

 **Arbeitsumgebung eingerichtet?**


Es muss zumindest ein Mandant, Arbeitsplatz und Clientsystem in der Arbeitsumgebung eingerichtet sein.

Wählen Sie den Aufrufkontext, für den die Authentisierung durchgeführt werden soll, damit im nächsten Schritt eine zugewiesene SM-B/HBA Karte ausgewählt werden kann.


MANDANT

Krankenhaus_Test 

ARBEITSPLATZ

Empfang 

CLIENTSYSTEM

ID_1 

USER ID *(optional)*

User ID eingeben

Die User ID eines HBA, der zum signieren freigeschaltet wurde, kann aus dem Primärsystem (PS) übernommen werden

Abbildung 19: Auswahl des Aufrufkontexts für die Authentifizierung

KIM E-Mail Registrierung

Wählen Sie Ihre zugewiesene SMC-B/HBA Karte aus, um die Authentisierung durchzuführen.

KARTENINHABER/-IN	KARTENTYP
<input type="radio"/> Praxis Adelheid Gräfin AdamiçTEST-ONLY	SMC_B

Abbildung 20: Auswahl der SMC-B/HBA-Karte für die Authentifizierung

8.2 Registrierung einer KIM E-Mail-Adresse

Um KIM verwenden zu können, muss ein Teilnehmer sich bei einem KIM-Anbieter zuerst registrieren. Nach erfolgter Prüfung des Antragstellers durch den KIM-Anbieter kann der Antragsteller sich als Teilnehmer mit einer eigenen KIM E-Mail-Adresse registrieren und erhält alle dazu notwendigen Informationen (u.a. einen Installationscode für die Registrierung einer KIM E-Mail-Adresse und ein KIMaaS Zertifikat).

Neben der KIM Authentisierung bietet der TaaS Client auch die Möglichkeit eine neue KIM E-Mail-Adresse zu registrieren. Um die Registrierung erfolgreich abschließen zu können muss sich der KIM-Teilnehmer mittels einer SMC-B bzw. HBA Karte authentisieren. Nach erfolgreicher Authentisierung und Registrierung der KIM E-Mail-Adresse erhält der Antragsteller vom KIM-Anbieter seine KIM-E-Mail-Adresse und kann sie ab sofort verwenden.

Die Registrierung einer neuen KIM E-Mail-Adresse kann auf zwei Arten erfolgen: (1) Start der Registrierung direkt im TaaS Client oder (2) Start der Registrierung in einem angebundenen Primärsystem. Für beide Varianten muss der TaaS Client zunächst gestartet, entsprechend konfiguriert (siehe Abschnitt 10) und in einem Webbrowser geöffnet sein.

Am Ende einer erfolgreichen Registrierung wird eine Konfigurationsdatei für das Primärsystem erstellt und in einem Unterordner *IDENTIFIER* im Applikationsverzeichnis des TaaS Clients gespeichert. Der *IDENTIFIER* entspricht dabei einer zufällig generierten Zahl, die nach erfolgter Registrierung retourniert wird. Unter Windows ist das Verzeichnis unter `C:\Users\<Username>\riseTic\kim\IDENTIFIER` zu finden. Unter macOS ist das Verzeichnis unter `/Users/<Username>/riseTic/kim/IDENTIFIER` zu finden.

8.2.1 TaaS Client

Um im TaaS Client die Registrierung einer KIM E-Mail-Adresse zu starten, wählen Sie unter dem Menüpunkt *KIM* die Aktion *KIM E-Mail registrieren* aus.


Hinweis: Die KIM E-Mail-Registrierung ist nur mit einem Google Chrome oder einem Firefox Webbrowser und nur auf demselben System (localhost) durchführbar, auf dem der TlaaS Client installiert ist.

Hinweis: Bevor Sie die KIM E-Mail-Registrierung starten, stellen Sie sicher, dass Sie alle notwendigen Informationen vorbereitet haben. Das umfasst die gewünschte KIM E-Mail-Adresse, die Sie registrieren möchten, den vom KIM-Anbieter erstellten und versendeten Installationscode, sowie ein gewünschtes Passwort für Ihren KIM Account.

Wenn im TlaaS Client eine KIM E-Mail-Registrierung gestartet wurde, sind folgende Schritte zum Abschluss der Registrierung notwendig:


1. **Authentisierung mittels KIM Authentikator:** Um eine neue KIM E-Mail registrieren zu können, müssen Sie sich mittels des verfügbaren AUT Zertifikats einer in einem Kartenterminal gesteckten HBA bzw. SMC-B Karte authentisieren. Dazu wählen Sie in einem ersten Schritt den Aufrufkontext für die Authentisierung aus. Um die KIM Authentisierung mit einer entsprechenden SMC-B Karte durchzuführen, wählen Sie Mandant, Arbeitsplatz und Clientsystem aus. Um die KIM Authentisierung mit einer HBA Karten durchzuführen, geben Sie eine UserID ein. Im nächsten Schritt wählen Sie anhand Ihres eingegebenen Aufrufkontexts eine Karte aus, die Sie für die KIM Authentisierung verwenden möchten. Details zu diesen beiden Schritten sind in Abschnitt 8.1 beschrieben (siehe Schritt 1 und 2).
Hinweis: Stellen Sie vorher sicher, dass Sie im Menü *Arbeitsumgebung* (siehe Abschnitt 7) bereits eine Arbeitsumgebung eingerichtet haben. Sobald zumindest ein Mandant, ein Arbeitsplatz und ein Clientsystem in der Arbeitsumgebung eingetragen wurden, können Sie die KIM Authentisierung mit dem TlaaS Client nutzen.
2. **Eingabe der KIM E-Mail-Adresse:** Nachdem Sie eine Karte zur Authentisierung gewählt haben, befüllen Sie das Formular zur E-Mail-Registrierung (siehe Abbildung 21). Dabei sind folgende Informationen einzugeben:
 - (a) KIM E-Mail-Adresse: Geben Sie Ihre gewünschte KIM E-Mail-Adresse und Domain ein.
 - (b) Installationscode: Dieser Code wurde Ihnen an Ihre angegebene E-Mail-Adresse geschickt.
 - (c) Initiales Passwort und eine Wiederholung davon zur Bestätigung. Anschließend wählen Sie *KIM E-Mail-Registrierung durchführen*, um die Registrierung zu starten.
3. **Durchführung der Authentisierung und KIM E-Mail-Registrierung:** Mittels der Auswahl von *KIM E-Mail-Registrierung durchführen* und des verfügbaren Kartenmaterials der ausgewählten Karte wird die Authentisierung und danach die Registrierung durchgeführt.
Hinweis: Sofern die ausgewählte Karte nicht freigeschaltet ist, ist eine PIN-Eingabe am Kartenterminal zur Freischaltung notwendig. Folgen Sie dazu den entsprechenden Ausweisungen am Kartenterminal.
4. **Abschluss der Registrierung:** Wenn die Authentisierung und Registrierung erfolgreich war, wird eine entsprechende Erfolgsmeldung angezeigt. Die KIM E-Mail-Adresse kann ab sofort verwendet werden. Zudem wird eine Konfigurationsdatei für ein Primärsystem erstellt und im Applikationsverzeichnis des TlaaS Clients gespeichert (siehe Verzeichnis oben).

KIM E-Mail Registrierung

GEWÜNSCHTE KIM E-MAIL-ADRESSE 

<input type="text" value="kim"/>	@	<input type="text" value="test"/>	<input type="text" value=".kim.telematik-test"/>
----------------------------------	---	-----------------------------------	--

Die Domain der KIM-E-Mail Adresse darf nur aus a-z, 0-9 sowie Punkt und Bindestrich bestehen

INSTALLATIONSCODE 

PASSWORT

PASSWORT WIEDERHOLEN

Abbildung 21: Eingabeformular zur Registrierung einer KIM E-Mail-Adresse

8.2.2 Primärsystem

Sie können die Registrierung einer KIM E-Mail-Adresse auch aus dem Primärsystem starten. Nach dem Start wechseln Sie in den TlaaS Client und schließen dort die Registrierung ab.

Achtung: Diese Option ist nur möglich, wenn das verwendete Primärsystem den RISE TlaaS Client unterstützt. Bei Fragen dazu wenden Sie sich an Ihren Primärsystem-Hersteller.

Hinweis: Die KIM E-Mail-Registrierung ist nur mit einem Google Chrome oder einem Firefox Webbrowser durchführbar.

Hinweis: Bevor Sie die KIM E-Mail-Registrierung starten, stellen Sie sicher, dass Sie alle notwendigen Informationen vorbereitet haben. Das umfasst die gewünschte KIM E-Mail-Adresse, die Sie registrieren möchten, den vom KIM-Anbieter erstellten und versendeten Installationscode, sowie ein gewünschtes Passwort für Ihren KIM Account.

Wenn im Primärsystem eine KIM E-Mail-Registrierung gestartet wurde, sind folgende Schritte im TlaaS Client zum Abschluss der Registrierung notwendig:

1. **Authentisierung mittels KIM Authentikator:** Um eine neue KIM E-Mail registrieren zu können, müssen Sie sich mittels des verfügbaren AUT Zertifikats einer in einem Kartenterminal gesteckten HBA bzw. SMC-B Karte authentisieren. Dazu wählen Sie anhand Ihres Aufrufkontexts eine Karte aus, die Sie für die KIM Authentisierung verwenden möchten. Details zu diesem Schritt sind in Abschnitt 8.1 beschrieben (siehe Schritt 2).

2. **Eingabe der KIM E-Mail-Adresse:** Nachdem Sie eine Karte zur Authentisierung gewählt haben, befüllen Sie das Formular zur E-Mail-Registrierung (siehe Abbildung 21). Dabei sind folgende Informationen einzugeben:
 - (a) KIM E-Mail-Adresse: Geben Sie Ihre gewünschte KIM E-Mail-Adresse ein. Die verwendete Domain kann nicht geändert werden.
 - (b) Installationscode: Dieser Code wurde Ihnen an Ihre angegebene E-Mail-Adresse geschickt.
 - (c) Initiales Passwort und eine Wiederholung davon zur Bestätigung. Anschließend wählen Sie *KIM E-Mail-Registrierung durchführen*, um die Registrierung zu starten.
3. **Durchführung der Authentisierung und KIM E-Mail-Registrierung:** Mittels der Auswahl von *KIM E-Mail-Registrierung durchführen* und des verfügbaren Kartenmaterials der ausgewählten Karte wird die Authentisierung und danach die Registrierung durchgeführt.
Hinweis: Sofern die ausgewählte Karte nicht freigeschaltet ist, ist eine PIN-Eingabe am Kartenterminal zur Freischaltung notwendig. Folgen Sie dazu den entsprechenden Ausweisungen am Kartenterminal.
4. **Abschluss der Registrierung:** Wenn die Authentisierung und Registrierung erfolgreich war, wird eine entsprechende Erfolgsmeldung angezeigt. Die KIM E-Mail-Adresse kann ab sofort verwendet werden. Zudem wird eine Konfigurationsdatei für ein Primärsystem erstellt und im Applikationsverzeichnis des TaaS Clients gespeichert (siehe Verzeichnis oben).

8.3 KIM as a Service deaktivieren

Wenn Sie die KIMaaS-Funktionalität nicht mehr verwenden möchten, dann deaktivieren Sie die Checkbox *KIMaaS verwenden* und starten den TaaS Client neu um die Änderung zu übernehmen. Nach dem Neustart ist die KIMaaS-Funktionalität des TaaS Clients nicht mehr verwendbar.

9 Benutzerverwaltung

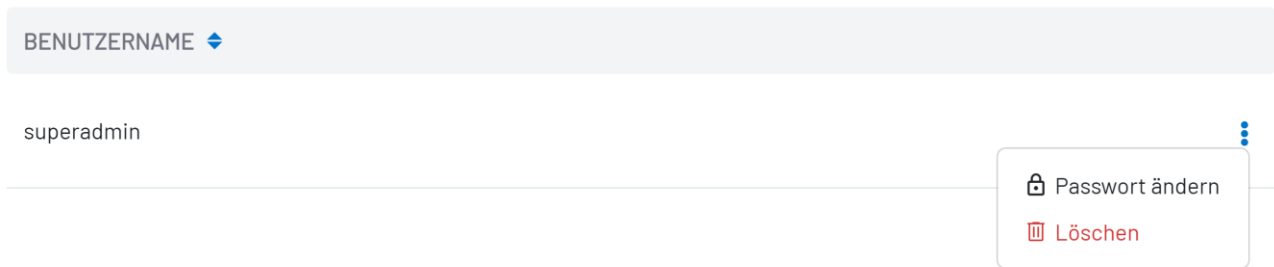
Unter dem Menüpunkt *Benutzerverwaltung* werden aktuell angelegte Benutzer angezeigt. Darüber hinaus können dort neue Benutzer erstellt und bestehende Benutzer bearbeitet oder gänzlich gelöscht werden.

Hinweis: Die Benutzerverwaltung ist nur dann verfügbar, wenn bei der Installation der externe Zugriff per HTTPS konfiguriert wurde.

9.1 Benutzeranzeige

Sollten bereits Benutzer im System hinterlegt worden sein, so erscheinen diese in einer Tabelle. Es werden lediglich der Benutzername und das Benutzermenüsymbol angezeigt. Sollten keine Benutzer hinterlegt sein, so wird eine leere Tabelle mit der Anzeige "Keine Daten vorhanden" dargestellt.

Das Benutzermenüsymbol, das ganz rechts in einer Zeile platziert ist, kann durch Auswahl geöffnet werden.

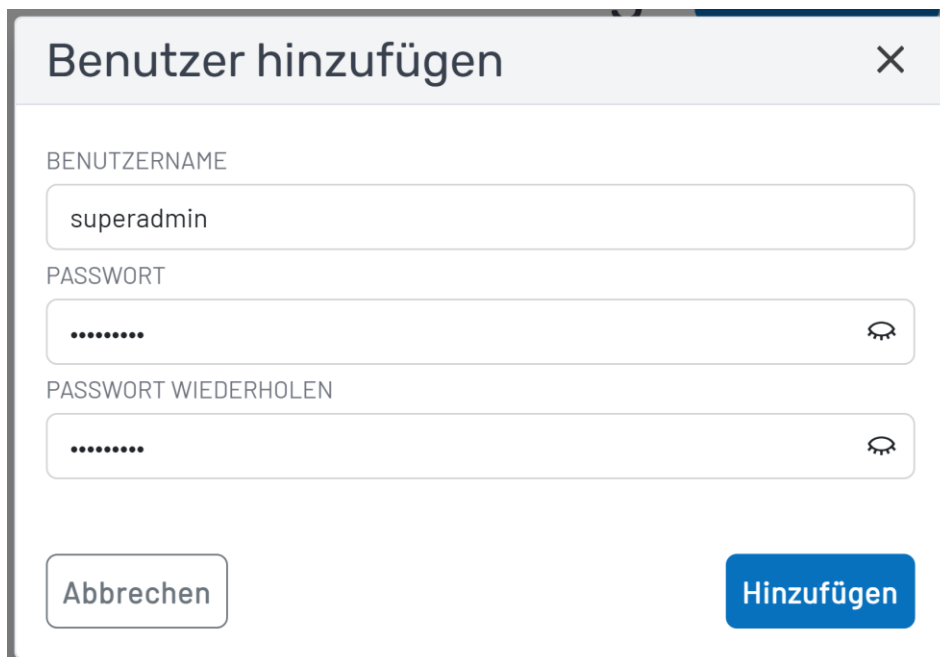


The screenshot shows a user management interface. At the top, there is a header with the text 'BENUTZERNAME' and a dropdown arrow. Below this, the user name 'superadmin' is displayed. To the right of the user name, there is a vertical ellipsis menu icon. A dropdown menu is open, showing two options: 'Passwort ändern' (Change password) with a lock icon and 'Löschen' (Delete) with a trash can icon.

Benutzeranzeige mit einem Benutzer und geöffnetem Benutzermenü

9.2 Benutzer hinzufügen

Um einen neuen Benutzer anzulegen, muss die Schaltfläche *+Hinzufügen* ausgewählt werden, welche sich rechts neben dem Titel *Benutzerverwaltung* befindet. Nach der Auswahl öffnet sich ein Formular, in das die Daten des neuen Benutzers eingeben werden können.



The screenshot shows a modal window titled 'Benutzer hinzufügen' (Add user) with a close button (X) in the top right corner. The form contains three input fields: 'BENUTZERNAME' (Username) with the value 'superadmin', 'PASSWORT' (Password) with masked characters and a visibility toggle icon, and 'PASSWORT WIEDERHOLEN' (Repeat password) also with masked characters and a visibility toggle icon. At the bottom left is a button labeled 'Abbrechen' (Cancel), and at the bottom right is a blue button labeled 'Hinzufügen' (Add).

Formular zum Hinzufügen eines neuen Benutzers

Zunächst müssen ein Benutzername und ein Passwort festgelegt werden. Bei dem Benutzernamen kann es sich um ein beliebiges Wort oder eine E-Mail-Adresse handeln. Das Passwort muss aus mindestens acht Zeichen bestehen und mindestens eine Zahl, einen Groß- und Kleinbuchstaben, sowie ein Sonderzeichen enthalten.

Entsprechen der Benutzername oder das Passwort nicht den Kriterien, so wird eine Fehlermeldung unterhalb des fehlerhaft ausgefüllten Formularfeldes angezeigt und die *Hinzufügen*-Schaltfläche kann nicht ausgewählt werden.

Sobald alle Felder korrekt ausgefüllt wurden, kann die *Hinzufügen*-Schaltfläche ausgewählt und der Benutzer angelegt werden. Dadurch wird das Formular geschlossen und die Tabelle, die nun den neuen Benutzer enthält, wird neu geladen.

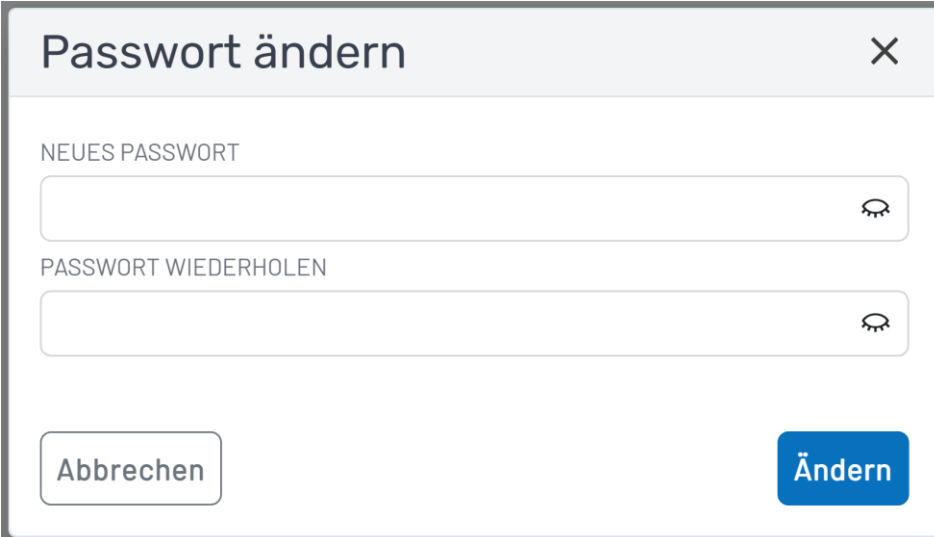
9.3 Benutzermenü

Das Benutzermenü kann durch die Auswahl der Schaltfläche, die durch das Symbol mit den drei Punkten angezeigt und sich ganz rechts in der Zeile eines Benutzers befindet, geöffnet werden. Nach der Auswahl des Symbols wird ein Menü mit zwei Optionen geöffnet:

- i. Passwort ändern
- ii. Benutzer löschen

9.3.1 Passwort ändern

Für die Änderung des Passworts eines bestehenden Benutzers kann die *Passwort ändern*-Schaltfläche im Benutzermenü ausgewählt werden. Daraufhin öffnet sich ein Formular, in welches zur Bestätigung das neue Passwort zweimal eingegeben werden muss.



Formular zum Ändern des Passworts eines Benutzers

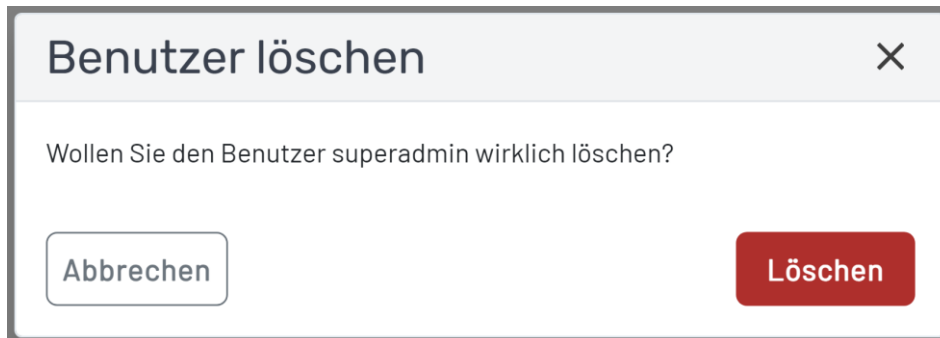
Das neue Passwort muss den in Abschnitt 9.2 genannten Kriterien entsprechen. Sollte ein ungültiges Passwort eingegeben werden, so wird eine Fehlermeldung angezeigt, die über die Kriterien informiert, denen das Passwort entsprechen muss.

Ist alles korrekt eingegeben worden, so kann die *Ändern*-Schaltfläche ausgewählt und das Passwort geändert werden.

Durch Auswahl der *Abbrechen*-Schaltfläche wird das Dialogfenster geschlossen und das alte Passwort bleibt bestehen. Wird die *Ändern*-Schaltfläche ausgewählt, so wird das Passwort geändert, das Formular geschlossen und eine Meldung über die Änderung des Passworts wird angezeigt.

9.3.2 Benutzer löschen

Für die Löschung eines Benutzers kann die *Löschen*-Schaltfläche im Benutzermenü ausgewählt werden. Daraufhin wird ein Dialog geöffnet, der fragt, ob der Benutzer tatsächlich gelöscht werden soll.



Dialog zum Bestätigen des Löschens eines Benutzers

Durch Auswahl der *Abbrechen*-Schaltfläche wird das Dialogfenster geschlossen und der Benutzer bleibt bestehen. Wird die *Löschen*-Schaltfläche ausgewählt, so wird der Benutzer gelöscht, das Dialogfenster geschlossen und eine Meldung über das erfolgreiche Löschen wird erhalten.

Achtung: Wenn der TlaaS Client auf einem System ohne grafische Benutzeroberfläche installiert worden ist und Sie alle Benutzer in der Benutzerverwaltung gelöscht haben, müssen Sie ins System, auf dem der TlaaS Client installiert ist, einsteigen und einen neuen externen Benutzer durch erneutes Konfigurieren des TlaaS Clients laut Abschnitt 2.4 anlegen um auf die Benutzeroberfläche wieder zugreifen zu können.

10 Konfiguration

In diesem Abschnitt werden die Konfigurationsmöglichkeiten des TlaaS Clients beschrieben.

Wurden die für den TlaaS Client benötigten Zertifikate bei der Installation nicht eingespielt, müssen grundlegende Einstellungen in der grafischen Benutzeroberfläche vorgenommen werden, bevor der TlaaS Client verwendet werden kann. Dazu müssen vor der Inbetriebnahme auch entsprechende Zertifikate und Schlüsselmaterial lokal vorhanden sein, die für den Betrieb notwendig sind. Diese befinden sich innerhalb des bereitgestellten Konfigurationsarchivs (.zip-Datei). Der Nutzer muss sicherstellen, dass nur vertrauenswürdige Zertifikate und Schlüssel eingebracht werden.

Die entsprechenden Zertifikate und das Schlüsselmaterial müssen vom TlaaS Anbieter über einen sicheren Kanal unter Wahrung der Vertraulichkeit und Integrität zur Verfügung gestellt werden. Dies gilt sowohl initial für die Ersteinrichtung als auch periodisch vor Ablauf des jeweils aktuell verwendeten Zertifikats.

In der grafischen Benutzeroberfläche unter dem Menüpunkt *Konfiguration* können Sie Zertifikate für die Verbindung zum TlaaS RZ importieren und speichern (siehe Abschnitt 10.1). Weitere Konfigurationsmöglichkeiten sind direkt über die TlaaS Client-Konfigurationsdatei möglich (siehe Abschnitt 10.4), die bereits im Rahmen der Installation eingespielt wurde.

10.1 Konfiguration der TLS-Kommunikation

Unter dem Menüpunkt *Konfiguration* ist es möglich, die Zertifikate und das Schlüsselmaterial für die TLS-Kommunikation zum TlaaS RZ in den lokalen KeyStore und TrustStore zu importieren und zu speichern (siehe Abbildung 22).

Konfiguration

[TlaaS Client neu starten](#)

TLS Zertifikatsverwaltung

KVS Client Zertifikat
✓ Bereits importiert

ZERTIFIKATS-DATEI
KVS-KeyStore.p12 **Durchsuchen**

Format - zB.: KVS_CLIENT_XXX.XXX.XXX.XXX.p12

PASSWORT

Aktualisieren

vKonnektor Client Zertifikat
✓ Bereits importiert

ZERTIFIKATS-DATEI
vKonnektor-KeyStore.p12 **Durchsuchen**

Format - zB.: VKON_CLIENT_XXX.XXX.XXX.XXX.p12

PASSWORT

Aktualisieren

Server-Zertifikate
✓ Bereits importiert 27.06.2023 15:35

Zertifikate automatisch beziehen

Zertifikate manuell importieren ^

Die aktuellen Server-Zertifikate können unter folgender Adresse bezogen werden:
<https://client.rise-tiaas.de/update-dev/trusted-server-certs-ltu.jws>

Keine Datei ausgewählt **Durchsuchen**

Importieren

Abbildung 22: Konfiguration der TLS-Zertifikate

Für den erfolgreichen TLS-Verbindungsaufbau und die verschlüsselte Kommunikation zum vKonnektor sind folgende Zertifikate und Schlüsselmaterial notwendig:

1. **KVS Client Zertifikat:**

Auswahl einer lokal verfügbaren passwortgeschützten *.p12-Datei mit dem KVS-Client-Zertifikat und privaten Schlüssel für die zertifikats-basierte Client-Authentifizierung mit der KVS (RISE Konnektor Verwaltungssoftware) sowie Eingabe des Passworts.

2. **vKonnektor Client Zertifikat:**

Auswahl einer lokal verfügbaren passwortgeschützten *.p12-Datei mit dem vKonnektor-Client-Zertifikat und privaten Schlüssel für die zertifikats-basierte Client-Authentifizierung mit dem TlaaS vKonnektor sowie Eingabe des Passworts.

Für diese Zertifikate wurde Ihnen in Ihrem Installationspaket jeweils eine *.p12-Datei zur Verfügung gestellt. Um die Zertifikate zu importieren, wählen Sie jeweils *Durchsuchen* und anschließend die entsprechende Datei aus.

Hinweis: Sollten Sie in Ihrem Installationspaket anstelle eines *KVS Client Zertifikats* und *vKonnektor Client Zertifikats* ein *TlaaS Client Zertifikat* vorfinden, nutzen Sie dieses sowohl für das *KVS Client Zertifikat* als auch für das *vKonnektor Client Zertifikat*.

Im nächsten Schritt geben Sie das erforderliche Passwort zur ausgewählten Zertifikats-Datei ein, das Ihnen über einen sicheren Kommunikationskanal bereitgestellt wurde. Dies ist von der Übermittlung des Installationspakets unabhängig. Ohne korrektes Passwort schlägt der Import der Zertifikats-Datei fehl.

Um den Import des Zertifikats abzuschließen, wählen Sie *Importieren* (bei bereits bestehendem Zertifikat: Auswahl von *Aktualisieren*). Nach erfolgreichem Import wird neben dem erfolgreich hochgeladenen Zertifikat ein grünes Symbol angezeigt (siehe Abbildung 23).



Abbildung 23: Erfolgreich hochgeladenes Zertifikat

Alle Zertifikate müssen korrekt hinterlegt werden, um den ordnungsgemäßen und sicheren Betrieb des TlaaS Clients zu gewährleisten.

Server-Zertifikate:

Alle weiteren benötigten Zertifikate (KVS, vKonnektor und KIM as a Service) werden automatisiert geprüft und gegebenenfalls aktualisiert. Dies geschieht zu folgenden Zeitpunkten:

- Unmittelbar nach dem Applikationsstart
- Mit einer zufälligen Verzögerung von 0 bis 24 Stunden nach dem Applikationsstart und danach in regelmäßigen Abständen von 24 Stunden

- Durch manuelles Auswählen der Schaltfläche *Zertifikate automatisch beziehen*

Die automatische Aktualisierung der Server-Zertifikate kann fehlschlagen, beispielsweise weil der Update-Server aufgrund Ihrer Netzwerkkonfiguration nicht zugänglich ist. In diesem Fall können Sie die Server-Zertifikate auch manuell herunterladen und importieren. Gehen Sie dafür folgendermaßen vor:

1. Klappen Sie das Import-Formular aus, indem Sie die Schaltfläche *Zertifikate manuell importieren* auswählen.
2. Beachten Sie die im Import-Formular angezeigte Webadresse. Öffnen Sie diese in einem Browser und laden Sie von der Webseite die neuesten Server-Zertifikate herunter. Als Alternative steht Ihnen der TlaaS Anwender-Support zur Verfügung, der Ihnen die benötigte Datei bereitstellen kann.
3. Wählen Sie danach im Import-Formular die Schaltfläche *Durchsuchen* aus und navigieren Sie zu der zuvor heruntergeladenen Datei, um diese auszuwählen.
4. Starten Sie den Import der Server-Zertifikate, indem Sie die Schaltfläche *Importieren* auswählen. Falls der Import erfolgreich durchgeführt werden konnte, erhalten Sie eine Bestätigungsmeldung.

Sollte während dieses Prozesses ein Fehler oder eine Unklarheit auftreten, wenden Sie sich bitte an den Support.

10.2 Konfiguration des Netzwerkadapters für das VPN

Wenn Sie den WireGuard-Client eines anderen Systems (in weiterer Folge *VPN-Gateway* genannt) verwenden möchten, können Sie im Menüpunkt *Konfiguration* im Abschnitt *Netzwerkadapter für das VPN* den Netzwerkadapter auswählen, der für die Verbindung zwischen dem lokalen System und dem VPN-Gateway verwendet wird.

Achtung: Diese Konfiguration beeinflusst das Verhalten der Kartenterminal- und Primärsystem-Event-Proxys. Eine falsche Einstellung kann dazu führen, dass keine Kommunikation mit den verbundenen Kartenterminals bzw. Primärsystemen möglich ist.

Zum Setzen des Netzwerkadapters wählen Sie dazu den passenden Eintrag aus der Dropdown-Liste aus und wählen Sie anschließend *Speichern*, um Ihre Auswahl zu bestätigen. Wählen Sie die Option *Lokaler VPN-Client*, wird der Netzwerkadapter mit der IP-Adresse genutzt, die dem WireGuard-VPN-Profil entspricht, das Ihnen in Ihrem Installationspaket zur Verfügung gestellt wurde (siehe Abbildung 24).

Netzwerkadapter für das VPN ⓘ

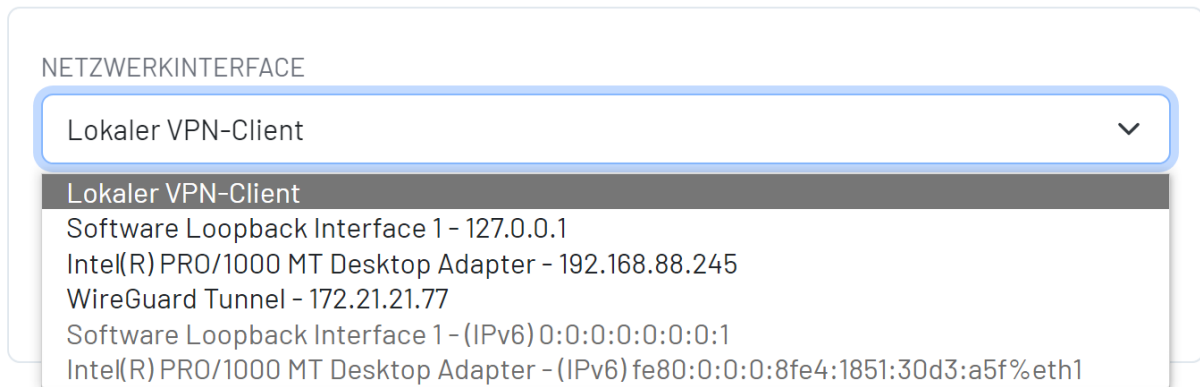


Abbildung 24: Konfiguration des Netzwerkadapters für das VPN

Hinweis: Bei der Nutzung eines VPN-Gateways wird empfohlen, auf die Installation des lokalen WireGuard-Clients während der Einrichtung des TaaS Clients zu verzichten. Weitere Details dazu finden Sie im Abschnitt Abschnitt 2.4.

10.3 Konfigurationsverzeichnisse

Die Konfiguration des TaaS Clients wird in Form von Konfigurationsdateien gespeichert. Sämtliche Konfigurationsdateien befinden sich gesammelt in einem Konfigurationsverzeichnis. Entsprechend des verwendeten Betriebssystems ist das Konfigurationsverzeichnis wie folgt definiert:

- Windows: `C:\Program Files\RISE_TaaS_Client\config`
- macOS: `/etc/rise/tic`
- Linux: `/etc/rise/riseTic`

10.4 Konfiguration der Anwendung

Eine initiale Konfiguration des TaaS Clients wird Ihnen vom TaaS Anbieter im Rahmen des Installationspakets in Form einer Konfigurationsdatei `TaaS_Client_Configuration_<Name>.yaml` zur Verfügung gestellt. Diese Konfiguration wird während der Installation des TaaS Clients eingespielt (siehe Abschnitt 2), sodass sie beim erstmaligen Start der Anwendung bereits vorliegt.

Nach der Installation kann die Konfiguration nur geändert werden, indem die Konfigurationsdatei über einen Texteditor geöffnet und bearbeitet wird. Für die Bearbeitung der Konfigurationsdatei sind Administrationsberechtigungen erforderlich. Um die Änderungen zu übernehmen, muss der TaaS Client neu gestartet werden.

Achtung: Führen Sie Änderungen in der Konfigurationsdatei nur im Zuge der Problembehandlung gemeinsam mit dem TaaS Anbieter durch. Eine falsche Konfiguration kann den ordnungsgemäßen und sicheren Betrieb des TaaS Clients stören.

In der Konfigurationsdatei des TlaaS Clients können über bereitgestellte Konfigurationsmöglichkeiten Einstellungen vorgenommen werden. Die Konfigurationsdatei befindet sich im Konfigurationsverzeichnis des TlaaS Clients (siehe Abschnitt 10.3).

Einstellungen können mithilfe eines Schlüssel-Wert-Paares in der Konfigurationsdatei definiert werden. Die Punktnotation (z. B. "ebene1.ebene2.schlüssel = MeinWert") wird in der Konfiguration durch verschachtelte Strukturen repräsentiert:

```
ebene1:
  ebene2:
    schlüssel: MeinWert
```

Jeder Punkt wird zu einer neuen Ebene in der Datei. Beachten Sie, dass Einrückungen sehr wichtig sind – ein Fehler hier kann dazu führen, dass die Konfiguration nicht korrekt gelesen wird. Stellen Sie daher sicher, dass Sie konsistente Einrückungen (jeweils zwei Leerzeichen, keine Tabulatorzeichen) verwenden, wenn Sie die Konfigurationsdatei manuell bearbeiten.

In Tabelle 1 sind die Konfigurationsmöglichkeiten mit Name in der Konfigurationsdatei, Beschreibung und Datentyp aufgelistet. Der Inhalt der Konfigurationsdatei ist von der jeweiligen Umgebung abhängig und ist entsprechend befüllt. Ist in der Konfigurationsdatei eine Einstellung nicht vorhanden, so wird vom TlaaS Client ein Standardwert angenommen. Wenn ein anderer Wert als der Standardwert verwendet werden soll, muss die Konfigurationseinstellung, falls noch nicht vorhanden, hinzugefügt und entsprechend gesetzt werden. Dabei muss beachtet werden, dass URLs mit einem "/" escaped werden.

Tabelle 1: Konfigurationsmöglichkeiten der Anwendung

Name in der Konfigurationsdatei	Beschreibung	Datentyp
tiaas.client.kvs.tic-id-header	Identifizier des TlaaS Clients	String
tiaas.client.kvs.url	IP-Adresse des TlaaS KVS im RZ	IP-Adresse
tiaas.client.wireguard.ip	IP-Adresse des VPN	IP-Adresse
tiaas.client.konnektor.url	IP-Adresse des vKonnektors	IP-Adresse
tiaas.client.security.ssl.enabled	HTTPS-Zugriff von einem anderen Host erlauben	true / false
tiaas.client.security.ssl.port	Port, der für eingehende HTTPS-Verbindungen verwendet wird	Port

10.5 Konfiguration automatischer Software-Updates

Wurde die Installationsart *Installation als Dienst* gewählt, so wird bei der Installation die zusätzliche Konfigurationsdatei *application-updater.yml* im Konfigurationsverzeichnis (siehe Abschnitt 10.3) des TlaaS Clients erzeugt. Diese Datei enthält die folgenden für die automatische Installation von Software-Updates relevanten Konfigurationsoptionen.

Tabelle 2: Konfigurationsmöglichkeiten von automatischen Software-Updates

Name in der Konfigurationsdatei	Beschreibung	Datentyp
tiaas.client.update.enabled	Aktivieren/Deaktivieren von automatischen Software-Updates	true / false
tiaas.client.update.cron	Cron-Ausdruck für die Definition des Zeitpunkts, wann Software-Updates regelmäßig (wenn verfügbar) installiert werden sollen. Der hier definierte Zeitpunkt sollte auf Randzeiten konfiguriert werden, zu welchen der TlaaS Client im Normalfall nicht benötigt wird, da im Zuge der Installation von Software-Updates der TlaaS Client neu gestartet werden muss. Dies kann zu Unterbrechungen der zur Verfügung gestellten Funktionalität führen.	Quartz Cron-Ausdruck ³

Die angeführten Konfigurationen können nur geändert werden, indem die Konfigurationsdatei über einen Texteditor geöffnet und bearbeitet wird. Um die Änderungen zu übernehmen, muss der Updater-Dienst *RISE-TlaaS-Client Updater* neu gestartet werden.

Achtung: Eine falsche Konfiguration kann dazu führen, dass automatische Software-Updates nicht oder zu einem ungünstigen Zeitpunkt ausgeführt werden und somit den ordnungsmäßigen und sicheren Betrieb des TlaaS Clients stören.

10.6 Konfiguration der Kartenterminals

Des Weiteren befindet sich die Datei *application-card-terminal.yml* im Konfigurationsverzeichnis (siehe Abschnitt 10.3) des TlaaS Clients. Diese Datei enthält die Pairing-Informationen des Kartenterminals und wird nach dem ersten Pairing-Versuch eines Kartenterminals angelegt. Kartenterminal-Port-Informationen lassen sich von Netzwerkadministratoren aus dieser Datei auslesen.

Diese Konfiguration kann nur geändert werden, indem die Konfigurationsdatei über einen Texteditor geöffnet und bearbeitet wird. Um die Änderungen zu übernehmen, muss der TlaaS Client neu gestartet werden.

³ <http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html>

Achtung: Führen Sie Änderungen in der Kartenterminal-Konfigurationsdatei nur im Zuge der Problembehandlung (siehe Abschnitt 16.3) in Abstimmung mit dem TaaS Anbieter durch. Eine falsche Konfiguration kann den ordnungsgemäßen und sicheren Betrieb des TaaS Clients stören.

10.7 Konfiguration der WireGuard Konfigurationsdatei

Die Konfigurationsdatei für den WireGuard-VPN-Tunnel wird standardmäßig während der Installation des TaaS Clients unter folgendem Ordner abgelegt:

- Windows: `C:\Program Files\WireGuard\Data\Configurations`
- macOS: `/usr/local/etc/wireguard`
- Linux: `/etc/wireguard`

Zum Öffnen des Ordners bzw. Bearbeiten der Konfigurationsdatei sind Administrator- bzw. Root-Berechtigungen erforderlich.

Wenn die gesamte WireGuard Konfigurationsdatei ausgetauscht werden muss, ist wie folgt vorzugehen:

1. Die alte TaaS-VPN-Konfigurationsdatei in dem WireGuard-Verzeichnis löschen.
2. Die neue TaaS-VPN-Konfigurationsdatei in dem WireGuard-Verzeichnis ablegen. (Unter Windows wird die Datei automatisch verschlüsselt.)
3. Den VPN-Tunnel neu starten.
 - Windows: In der WireGuard Benutzeroberfläche den Tunnel deaktivieren und anschließend wieder aktivieren.
 - macOS und Linux: Folgende zwei Kommandozeilenbefehle ausführen:

```
sudo wg-quick down tiaas-vpn  
sudo wg-quick up tiaas-vpn
```

11 Primärsysteme

Unter dem Menüpunkt *Primärsysteme* können Primärsysteme hinzugefügt werden. Dafür muss eine beliebige Bezeichnung, die IP-Adresse und der Port des Hosts, auf dem das zu verbindende Primärsystem ausgeführt wird, eingegeben werden (siehe Abbildung 25). Für jedes Primärsystem muss eine individuelle Event-Weiterleitung eingerichtet werden.

Für die erfolgreiche Event-Weiterleitung an ein Primärsystem durch den TaaS Client ist es erforderlich, dass im Primärsystem als EventTo-Adresse die Client-IP-Adresse des WireGuard-VPN-Tunnels angegeben wird. Wird der WireGuard-VPN-Tunnel direkt vom Host des TaaS Clients geöffnet, so werden die Events vom TIC empfangen und an die angegebene IP-Adresse des Primärsystems weitergeleitet. Falls der WireGuard-VPN-Tunnel von einem Router oder einer Firewall aus geöffnet wird, so muss an diesem Gerät zusätzlich eine entsprechende Port-Weiterleitung eingerichtet werden (siehe Abschnitt 14.2).

Primärsysteme hinzufügen ×

BEZEICHNUNG

IP-ADRESSE

PORT

Abbildung 25: Primärsysteme hinzufügen

Hinweis: Der Port wird sowohl als Listening-Port im TlaaS Client, als auch für die Event-Weiterleitung zum Primärsystem verwendet und muss eindeutig sein. Der TlaaS Client identifiziert das betroffene Primärsystem eindeutig durch den verwendeten Port, weshalb jedes Primärsystem einen anderen Port für die Entgegennahme der Events verwenden muss. Es darf auch keine Überschneidung mit dem Portbereich der Kartenterminals geben.

11.1 Primärsystemübersicht

Wenn Primärsysteme im TlaaS Client hinzugefügt wurden, werden diese in der Primärsystemübersicht dargestellt (siehe Abbildung 26).

Primärsysteme

BEZEICHNUNG ▾	IP-ADRESSE ▾	PORT ▾	
PVS 2	192.168.1.131	9321	⋮
PVS 1	192.168.15.1	5001	⋮

Abbildung 26: Primärsystemübersicht

11.2 Primärsystem bearbeiten

Ein Primärsystem kann in der Primärsystemübersicht durch Auswahl von *Bearbeiten* editiert werden (siehe Abbildung 27). Nach dem Speichern werden alle Event-Weiterleitungen aktualisiert.



Primärsysteme bearbeiten

BEZEICHNUNG
PVS 1

IP-ADRESSE
192.168.15.1

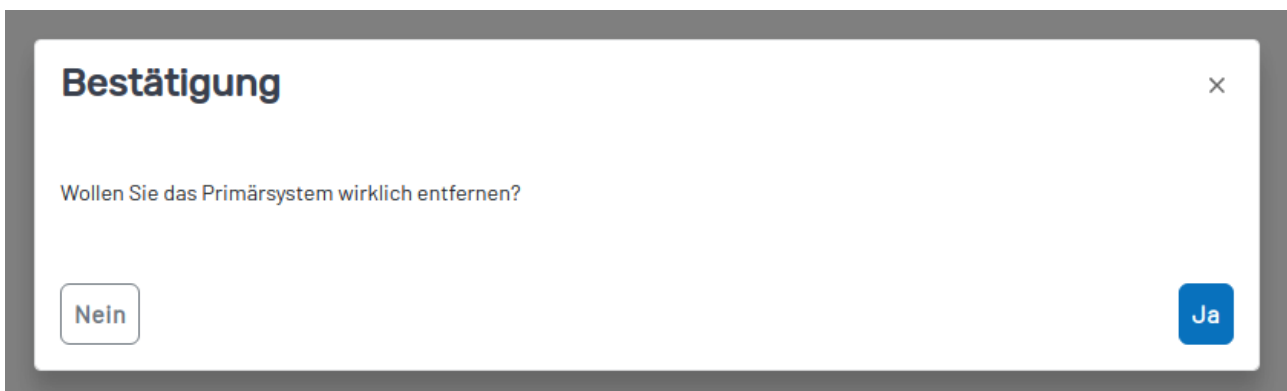
PORT
5001

Abbrechen Speichern

Abbildung 27: Primärsystem bearbeiten

11.3 Primärsystem entfernen

Ein Primärsystem kann in der Primärsystemübersicht durch Auswahl von *Löschen* entfernt werden. Dafür muss die Auswahl der Aktion durch die Anzeige *Wollen Sie das Primärsystem wirklich entfernen?* bestätigt werden (siehe Abbildung 28). Die Event-Weiterleitung für dieses Primärsystem wird daraufhin gestoppt.



Bestätigung

Wollen Sie das Primärsystem wirklich entfernen?

Nein Ja

Abbildung 28: Primärsystem löschen

12 Logging

Der TlaaS Client schreibt Logdateien, die eine Analyse und ein Nachvollziehen der technischen Vorgänge ermöglichen. Sämtliche Logdateien befinden sich gesammelt in einem Logverzeichnis. Entsprechend des verwendeten Betriebssystems ist das Logverzeichnis wie folgt definiert:

- Windows: `C:\Program Files\RISE_TlaaS_Client\log`
- macOS: `/var/log/rise/tic`
- Linux: `/var/log/rise/tic`

Bei jedem Start des TlaaS Clients wird eine neue Logdatei angelegt. Die Logdateien enthalten keine sensiblen Daten.

Kommt es im Betrieb des TlaaS Clients zu Problemen, kann Sie der TlaaS Anbieter im Zuge des Produktsupports bitten, diese Logdateien mit einem Texteditor zu öffnen, um die Fehlersuche zu vereinfachen.

13 Updates

13.1 TlaaS Client

Es werden regelmäßig Updates des TlaaS Clients zur Verfügung gestellt. Die Abfrage nach neuen Updates erfolgt automatisch während der TlaaS Client ausgeführt wird. Bei Verfügbarkeit eines neuen Updates wird dieses im Hintergrund heruntergeladen und zum voreingestellten Updatezeitpunkt installiert.

Hinweis: Für die automatischen Updates sind die Einstellungen unter Abschnitt 14.2 zu beachten.

Hinweis: Falls Sie den TlaaS Client nicht in das Standard-Installationsverzeichnis installiert haben oder Updates, die wesentliche Änderungen an der Betriebssystem-Konfiguration vornehmen, installieren, kann es notwendig sein, dem Update-Installations-Assistenten Administratorberechtigungen zu erteilen (siehe Abschnitt 2).

13.2 WireGuard

Neben der TlaaS Client Anwendung wird bei der Installation auch der WireGuard VPN-Client auf Ihrem Betriebssystem installiert. Für WireGuard werden ebenso in regelmäßigen Abständen neue Updates der Software geprüft. Diese Prüfung erfolgt wie das Update selbst automatisch im Hintergrund.

Hinweis: Falls Sie den WireGuard VPN-Client nicht mit dem TlaaS Client installieren, können keine automatischen Updates für den WireGuard VPN-Client durch den TlaaS Client durchgeführt werden.

13.3 Freigegebene IP-Adressen

Bei einem automatischen Update des TlaaS Clients wird automatisch die Liste der freigegebenen IP-Adressen in der WireGuard TlaaS-VPN Konfigurationsdatei überprüft und bei Bedarf aktualisiert.

Wird eine gesonderte Installation des WireGuard VPN-Clients verwendet muss die Liste der freigegebenen IPs bei einem TlaaS Client Update auf ihre Vollständigkeit geprüft und bei Bedarf händisch aktualisiert werden. In diesem Fall müssen folgende IPs freigegeben werden:

- 10.156.120.0/24
- 10.156.131.0/24
- 10.156.124.0/24
- 10.156.216.0/22

- 10.157.224.0/21
- 100.102.0.0/15
- 161.156.128.32/28
- 185.226.121.64/28
- 188.144.0.0/15
- 193.28.70.16/30
- 212.3.66.8/29
- 213.146.104.80/29
- 213.61.31.240/28
- 78.111.96.12/30
- 78.111.96.16/30
- 78.111.96.24/30
- 78.111.96.28/30
- 78.111.96.32/30
- 78.111.96.36/30
- 78.111.96.52/30
- 78.111.96.56/30
- 84.17.163.84/30

14 Konfiguration des Netzwerkes des Leistungserbringers

Dieses Kapitel dient als Leitfaden für die Konfiguration des Netzwerkes eines Leistungserbringers, um die folgenden Einsatzszenarien des TlaaS Clients zu ermöglichen.

1. **Installation des TlaaS Clients auf einem zentralen Server:** In diesem Szenario wird der TlaaS Client auf einem zentralen Server zusammen mit dem WireGuard-Client installiert. Andere Hosts, auf denen beispielsweise Primärsysteme installiert sind, sollen die Möglichkeit haben, den WireGuard-VPN-Tunnel des Hosts des TlaaS Clients zu nutzen, um eine Verbindung zu den Systemen im zentralen TlaaS-Rechenzentrum herzustellen.
2. **Verwendung eines bereitgestellten WireGuard-VPN-Tunnels:** In diesem Szenario soll der WireGuard-VPN-Tunnel von einem anderen Host (bspw. einem Router oder einer Firewall) vom TlaaS Client verwendet werden, um eine Verbindung zu den Systemen im TlaaS-Rechenzentrum herzustellen.

14.1 Installation des TaaS Clients auf einem zentralen Server mit WireGuard-Client

Damit andere Hosts den WireGuard-VPN-Tunnel vom Host des TaaS Clients in das TaaS-Rechenzentrum verwenden können, muss der Host des TaaS Clients den Netzwerkverkehr entsprechend routen. Dies kann durch ein *Network-Address-Translation-Gateway* (NAT-Gateway), basierend auf dem Windows-Feature *Hyper-V*, konfiguriert werden.

14.1.1 Installation unter Windows 10/11

Hinweis: Das Windows-Feature *Hyper-V* ist nur auf Windows-10- und Windows-11-Systemen ab der Pro-Edition verfügbar. Der nachfolgende Leitfaden wurde mit Windows 10 Pro und Windows 11 Pro getestet.

Sofern das Windows-Feature *Hyper-V* am Host des TaaS Clients noch nicht aktiviert ist, kann dies aus einer **Administrator PowerShell** mit dem folgenden Befehl durchgeführt werden:

```
DISM /Online /Enable-Feature /All /FeatureName:Microsoft-Hyper-V
```

Nach Eingabe des Befehls muss der Host neu gestartet werden, damit das Windows-Feature *Hyper-V* aktiviert ist. Nach dem Neustart kann das NAT-Gateway aus einer **Administrator PowerShell** mit dem folgenden Befehl aktiviert werden:

```
New-NetNat -Name tiaas-nat -InternalIPInterfaceAddressPrefix  
<IP_INTERFACE_ADDRESS_PREFIX>
```

Der Parameter `<IP_INTERFACE_ADDRESS_PREFIX>` bezeichnet hierbei den Address-Prefix des internen Netzwerkinterfaces, welches das NAT-Gateway mit dem WireGuard-VPN-Tunnel verbindet. Wenn beispielsweise das interne Netzwerk die Netzadresse 192.168.88.0 hat und die Netzwerkmaske 255.255.255.0 verwendet, so ist dieser Parameter mit 192.168.88.0/24 zu setzen und der vollständige Befehl lautet:

```
New-NetNat -Name tiaas-nat -InternalIPInterfaceAddressPrefix 192.168.88.0/24
```

Hinweis: Nach der Einrichtung des NAT-Gateways muss die Windows-Firewall entsprechend konfiguriert werden, sodass nur die Hosts, die den WireGuard-VPN-Tunnel verwenden dürfen, als Ausnahme in den Firewall-Regeln konfiguriert sind.

Nachdem das NAT-Gateway am Host des TaaS Clients eingerichtet wurde, müssen auf den Hosts, die den WireGuard-VPN-Tunnel am Host des TaaS Clients verwenden möchten, entsprechende Routing-Einträge für die betroffenen Subnetze erstellt werden. Für Windows kann dies aus einer **Administrator PowerShell** mit dem folgenden Befehl durchgeführt werden:

```
route -p add <TIAAS_SUBNET> MASK <TIAAS_SUBNET_MASK> <IP_ADDRESS_TIC_HOST>
```

Die betroffenen Netze im TaaS-Rechenzentrum lauten wie folgt:

- TaaS-Netze

- 10.156.120.0/24
- 10.156.131.0/24
- 10.156.124.0/24
- Offene Fachdienste in der Telematikinfrastruktur
 - 100.102.0.0/15
- Bestandsnetze, die über die Telematikinfrastruktur angebunden sind
 - 188.144.0.0/15
 - 212.3.66.8/29
 - 213.146.104.80/29
 - 83.236.194.125/32
 - 161.156.128.32/28
 - 84.17.163.80/30
 - 84.17.163.84/30
 - 185.226.121.64/28
 - 213.61.31.224/28
 - 213.61.31.240/28
 - 193.28.70.16/30
 - 193.175.81.64/29
 - 193.28.71.232/30

Um beispielsweise eine Route für die Hosts im TlaaS-Netz *10.156.120.0/24* über den TlaaS Client auf dem Host mit der IP-Adresse *192.168.88.251* zu erstellen, muss der folgende Befehl ausgeführt werden:

```
route -p add 10.156.120.0 MASK 255.255.255.0 192.168.88.251
```

14.1.2 Installation unter Windows Server 2022

Sollte das *Hyper-V* Modul nicht verfügbar sein, gibt es unter Windows Server 2022 die Möglichkeit unter Rollendienste das Routing Feature zu aktivieren. Danach kann das Routing und der RAS Dienst konfiguriert und somit ein NAT fertig eingerichtet werden. Anschließend müssen nur noch Client-seitig die Routen mit dem Ziel des Routing und RAS Servers in der Umgebung des Leistungserbringers gesetzt werden.

14.2 Verwendung eines bereitgestellten WireGuard-VPN-Tunnels

Falls der WireGuard-VPN-Tunnel von einem zentralen Router oder einer dedizierten Firewall bereitgestellt werden soll, so müssen die folgenden Konfigurationen auf dem Gerät getroffen werden:

- Konfiguration des WireGuard-VPN-Tunnels
- Konfiguration eines NAT-Gateways für den WireGuard-VPN-Tunnel
- Konfiguration der Routen für den WireGuard-VPN-Tunnel
- Konfiguration des Port-Forwardings für eingehende Requests vom TlaaS-Rechenzentrum zum TlaaS Client
- Konfiguration der Firewall, sodass nur bestimmte Hosts Zugriff auf den VPN-Tunnel erhalten
- Konfiguration der Firewall, sodass der Zugriff auf den Updateserver, von wo aus die Updates und Serverzertifikate bezogen werden, freigegeben wird

Diese Punkte werden im Nachfolgenden generisch beschrieben, die konkrete Konfiguration ist abhängig von Ihrem Gerät. Für die detaillierte Einrichtung konsolidieren Sie bitte das Handbuch oder den Hersteller Ihres Gerätes.

Hinweis: Sofern ein bereitgestellter WireGuard-VPN-Tunnel verwendet wird, muss in der Konfiguration des TlaaS Clients das entsprechende Netzwerkinterface ausgewählt werden, über welches der WireGuard-VPN-Tunnel erreichbar ist. Details hierzu sind im Kapitel Abschnitt 10.2 beschrieben.

14.2.1 Konfiguration des WireGuard-VPN-Tunnels

Die WireGuard-VPN-Tunnel-Konfiguration muss laut der WireGuard-VPN-Konfigurationsdatei aus dem Konfigurationspaket erstellt werden. Dafür ist sowohl das WireGuard-Netzwerkinterface als auch der WireGuard-Peer für die VPN-Verbindung in das TlaaS-Rechenzentrum einzurichten.

Für das Interface müssen aus der Sektion *[Interface]* die Werte der Felder *PrivateKey* und *Address* entnommen werden. Diese Felder haben die folgenden Bedeutungen:

- *PrivateKey* ist der private Schlüssel, mit dem empfangene Pakete über den WireGuard-VPN-Tunnel entschlüsselt werden. Dieser muss im WireGuard-Interface eingetragen werden.
- *Address* entspricht der WireGuard-VPN-Client-IP-Adresse. Diese Adresse muss dem WireGuard-Netzwerkinterface zugewiesen werden.

Für den Peer müssen aus der Sektion *[Peer]* die Werte der Felder *PublicKey*, *AllowedIPs*, *Endpoint* und *PersistentKeepalive* entnommen werden. Diese Felder haben die folgenden Bedeutungen:

- *PublicKey* ist der öffentliche Schlüssel des WireGuard-Peers, zu dem sich der WireGuard-Client verbindet. Pakete, die an einen Host von *AllowedIPs* gesendet werden, werden mit diesem verschlüsselt. Dieser muss im Peer gesetzt werden.
- *AllowedIPs* listet die Subnetze, die über den Peer erreichbar sind. Diese müssen im Peer gesetzt werden und sind in weiterer Folge auch für die Routing-Konfiguration relevant.

- *Endpoint* gibt die IP-Adresse und den Port des Peers an, zu dem sich der WireGuard-Client verbindet. Die IP-Adresse und der Port müssen im Peer gesetzt werden.
- *PersistentKeepalive* gibt die Zeitspanne in Sekunden an, in der *Keep-Alive*-Pakete an den Peer gesendet werden. Diese Konfiguration muss im Peer gesetzt werden.

Details zu WireGuard kann der offiziellen WireGuard-Dokumentation⁴ entnommen werden.

14.2.2 Konfiguration eines NAT-Gateways für den WireGuard-VPN-Tunnel

Um den Netzwerkverkehr zwischen einem Host des LE und dem TaaS-Rechenzentrum über einen zentralen Router oder eine dedizierte Firewall zu ermöglichen, muss auf diesem Router bzw. dieser Firewall *Network Address Translation (NAT)* für den Netzwerkverkehr, der über den WireGuard-Tunnel in das TaaS-Rechenzentrum geleitet werden soll, konfiguriert werden. Die betroffenen Protokolle sind *TCP* und *UDP*.

14.2.3 Konfiguration der Routen für den WireGuard-VPN-Tunnel

Um den Netzwerkverkehr in das TaaS-Rechenzentrum zu ermöglichen, muss für jedes Subnetz, das im Feld *AllowedIPs* in der WireGuard-Client-Konfiguration bzw. unter dem Kapitel Abschnitt 13.3 aufgelistet angeführt ist, eine Routing-Konfiguration zum WireGuard-Netzwerkinterface erstellt werden.

14.2.4 Konfiguration des Port-Forwardings für eingehende Requests vom TaaS-Rechenzentrum zum TaaS Client

Es muss eine Port-Forwarding-Konfiguration für eingehende Verbindungen am WireGuard-Netzwerkinterface zum TaaS-Client-Host erstellt werden. Die betroffenen Protokolle und Ports lauten wie folgt:

- Die Kartenterminal-Ports: in der Standardkonfiguration liegen diese im Bereich 9000 bis 9019, Protokoll *TCP*.
- Die Kartenterminal-Discovery-Ports: 4742 und 4743, Protokoll *UDP*.
- Die VPN-Cluster-Ports: 60000 bis 60100, Protokoll *UDP*.
- Die verwendeten Ports der Primärsysteme für den Empfang der CETP-Events: Details zur Konfiguration können dem Kapitel Abschnitt 11 entnommen werden. Die dort konfigurierten Ports müssen auf dem Host des TaaS Clients weitergeleitet werden, Protokoll *TCP*.

Alternativ kann auch der komplette eingehende Traffic (*TCP* und *UDP*) aus dem WireGuard-VPN-Tunnel an den TaaS-Client-Host weitergeleitet werden.

⁴ <https://www.wireguard.com/>

14.2.5 Konfiguration der Firewall, sodass nur bestimmte Hosts Zugriff auf den VPN-Tunnel erhalten

Nach der Konfiguration des Gerätes muss die Firewall entsprechend konfiguriert werden, sodass nur die Hosts, die den WireGuard-VPN-Tunnel verwenden dürfen, als Ausnahme in den Firewall-Regeln eingestellt sind.

14.2.6 Konfiguration der Firewall, sodass der Zugriff auf den Updateserver, von wo die Updates und Serverzertifikate bezogen werden, freigegeben wird

Sollte eine dedizierte Firewall in Verwendung sein, muss sichergestellt werden, dass der Verbindungsaufbau zum Updateserver (*client.rise-tiaas.de*) bzw. das Beziehen von Dateien freigegeben ist. Sollte dies nicht der Fall bzw. nicht gewollt sein, ist der LE selbst für das Prüfen auf Updates, Durchführung von Updates und Importieren der Serverzertifikate verantwortlich und hat mit Mehraufwand zu rechnen.

15 Deinstallation

15.1 Windows

Die Deinstallation des TlaaS Clients erfolgt über die *Apps und Features*-Liste von Windows. Zur Deinstallation gehen Sie bitte in folgender Reihenfolge vor:

1. Beenden Sie zunächst die Anwendung des TlaaS Clients.
2. Öffnen Sie die *Windows Einstellungen* (*Windows Startmenü > Einstellungen* oder *Windows-Taste + I*).
3. Wählen Sie den Menüpunkt *Apps* bzw. *Apps und Features* aus.
4. Suchen Sie in der Liste nach der Applikation *RISE TI as a Service Client* und wählen Sie den Eintrag aus.
5. Wählen Sie *Deinstallieren* und bestätigen Sie.
6. Erteilen Sie Administratorberechtigung.
7. Der Deinstallationsprozess des TlaaS Clients startet.
8. Wählen Sie aus, welche Dateien, die im Zuge der Installation und des Betriebes des TlaaS Clients erstellt wurden, nach der Deinstallation weiterhin verfügbar sein sollen (siehe Abbildung 29).
 - **Konfigurationsordner entfernen:** Diese Auswahl entfernt das Installationsverzeichnis mit der TlaaS Konfiguration, in das der TlaaS Client installiert wurde.
 - **Logdateien entfernen:** Diese Auswahl löscht alle Logdateien, die im Zuge des Betriebes erstellt wurden, von der Festplatte.

- **VPN-Tunnel entfernen:** Diese Auswahl entfernt die WireGuard-Konfiguration für den TlaaS Client, die für dessen Betrieb nötig ist.
 - **WireGuard deinstallieren:** Entfernt den WireGuard-Service, der für die korrekte Funktionalität des TlaaS Clients nötig ist.
Achtung: Wählen Sie diese Option nur aus, wenn Sie WireGuard für *keine* andere Anwendung nutzen, da deren Betrieb sonst eventuell gestört werden kann.
9. Folgen Sie den Anweisungen des Assistenten um die Deinstallation abzuschließen.
10. Falls Sie den WireGuard-VPN-Tunnel anderen Hosts im Netzwerk bereitgestellt haben (siehe Abschnitt 14.1), so müssen Sie das eingerichtete NAT Gateway wieder entfernen und gegebenenfalls das Windows Feature *Hyper-V* deaktivieren. Das NAT Gateway kann mit dem folgenden Befehl aus einer **Administrator Powershell** entfernt werden:

```
Remove-NetNat -Name tiaas-nat
```

Das Windows Feature *Hyper-V* kann mit dem folgenden Befehl aus einer **Administrator Powershell** deaktiviert werden:

```
Disable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V
```

15.2 macOS

Zur Deinstallation gehen Sie bitte in folgender Reihenfolge vor:

1. Beenden Sie zunächst die Anwendung des TlaaS Clients.
2. Öffnen Sie das Installationsverzeichnis der Applikation *RISE TI as a Service Client* in Finder. Dieses befindet sich unter */opt/rise/tic*.
3. Starten Sie das *RISE TI as a Service Client Deinstallationsprogramm*.
4. Erteilen Sie Administratorberechtigung.
5. Der Deinstallationsprozess des TlaaS Clients startet.
6. Wählen Sie aus, welche Dateien, die im Zuge der Installation und des Betriebes des TlaaS Clients erstellt wurden, nach der Deinstallation weiterhin verfügbar sein sollen (siehe Abbildung 29).
 - **Konfigurationsordner entfernen:** Diese Auswahl entfernt das Installationsverzeichnis mit der TlaaS Konfiguration, in das der TlaaS Client installiert wurde.
 - **Logdateien entfernen:** Diese Auswahl löscht alle Logdateien, die im Zuge des Betriebes erstellt wurden, von der Festplatte.
 - **VPN-Tunnel entfernen:** Diese Auswahl entfernt die WireGuard-Konfiguration für den TlaaS Client, die für dessen Betrieb nötig ist.
 - **WireGuard deinstallieren:** Entfernt das WireGuard-Service, das für die korrekte Funktionalität des TlaaS Clients nötig ist.

Achtung: Wählen Sie diese Option nur aus, wenn Sie WireGuard für *keine* andere Anwendung nutzen, da deren Betrieb sonst eventuell gestört werden kann.

7. Folgen Sie den Anweisungen des Assistenten, um die Deinstallation abzuschließen.

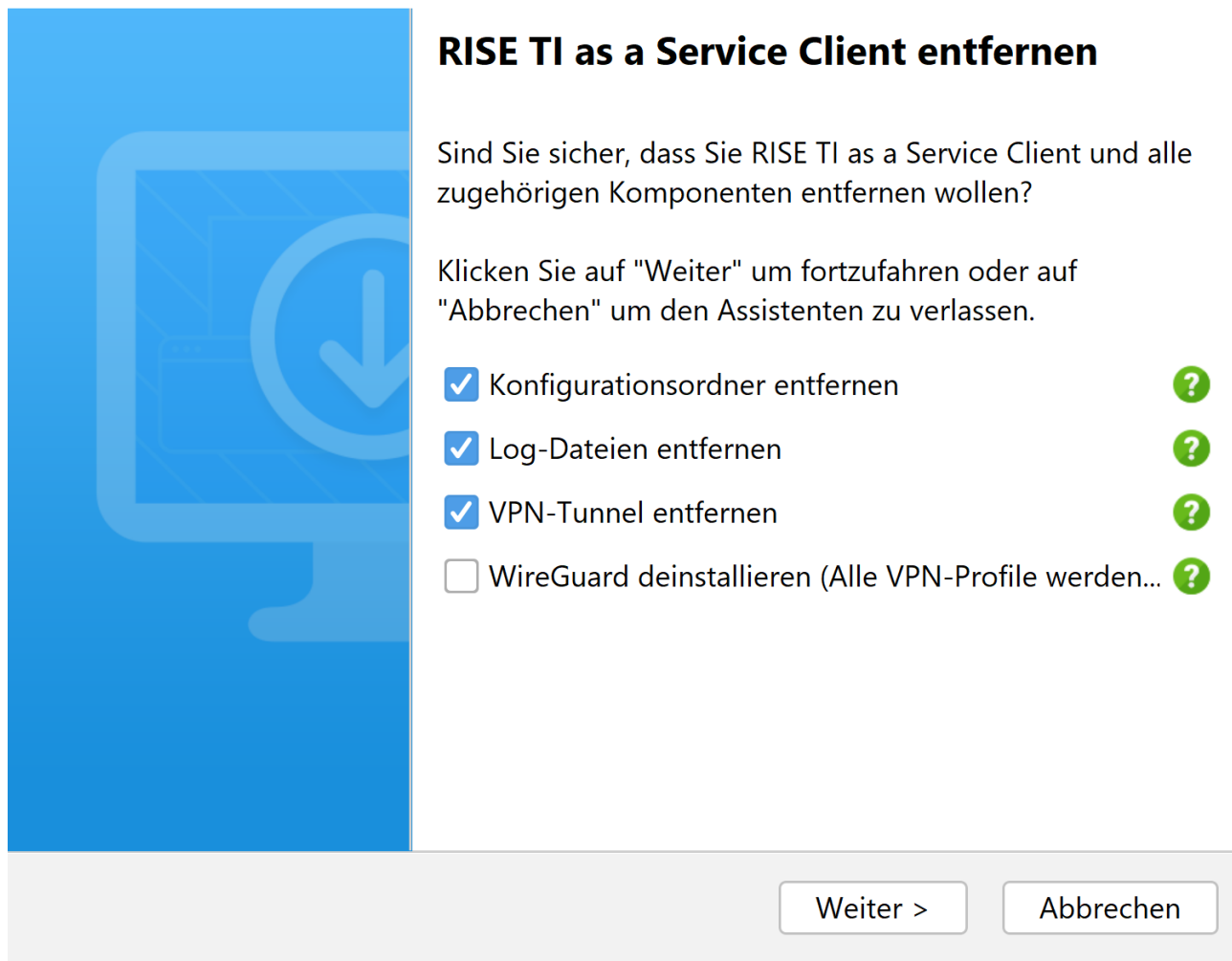


Abbildung 29: Deinstallation des TlaaS Clients

15.3 Linux

Um den RISE TlaaS Client von Ihrem System wieder zu deinstallieren, geben Sie folgenden Befehl in das Terminal ein und bestätigen diesen mit Enter:

```
sudo apt purge rise-tiaas-client
```

Hinweis: Die Pakete *WireGuard* und *WireGuard-Tools* müssen separat deinstalliert werden, sofern diese nicht mehr benötigt werden.

Um die Pakete *WireGuard* und *WireGuard-Tools* zu deinstallieren, geben Sie folgenden Befehl im Terminal ein und bestätigen die Eingabe mit Enter:

```
sudo apt purge wireguard wireguard-tools -y
```

15.4 Entfernung eines bereitgestellten WireGuard-VPN-Tunnels

Falls der WireGuard-VPN-Tunnel auf einem dedizierten Gerät eingerichtet wurde (siehe Abschnitt 14.2) so muss dieser entfernt werden. Die notwendigen Schritte hierfür sind wie folgt:

1. Entfernung der Firewall Regeln für den Zugriff auf den WireGuard-VPN Tunnel
2. Entfernung der Port-Forwarding-Konfigurationen für eingehende Requests vom TlaaS-Rechenzentrum zum TlaaS Client
3. Entfernung der Routen in den WireGuard-VPN-Tunnel
4. Entfernung des NAT-Gateways für den WireGuard-VPN-Tunnel
5. Entfernung des WireGuard Peers
6. Entfernung des WireGuard Interfaces

16 Fehlerbehebung

Im Folgenden werden mögliche Fehler aufgelistet, die während des Betriebs des TlaaS Clients auftreten können, sowie mögliche Ursachen und Lösungsvorschläge. Leer gelassene Zellen entsprechen inhaltlich der darüber stehenden Zelle.

Hinweis: Sollten Fehler mit den angegebenen Lösungsvorschlägen nach mehrmaligen Versuchen bzw. nach erneuter Installation des TlaaS Clients nicht behebbar sein, kontaktieren Sie bitte den TlaaS Anbieter-Support.

16.1 vKonnektor

Tabelle 3: Mögliche Fehlerursachen betreffend vKonnektor

Problem	Mögliche Ursache	Lösungsvorschlag
vKonnektor-Statussymbol ist rot	Keine/schlechte Verbindung mit dem Internet	Überprüfen Sie, ob Sie eine bestehende Internetverbindung haben.
	TlaaS Client-Konfiguration inkorrekt	Kontrollieren Sie die vKonnektor IP-Adresse in der Konfigurationsdatei (siehe Abschnitt 10.4). Stimmt diese nicht mit der, in der ausgelieferten Konfigurationsdatei hinterlegten vKonnektor IP-Adresse überein, passen Sie die vKonnektor IP-Adresse in der bestehende TlaaS-Client Konfigurationsdatei an.
	Keine Verbindung zum TlaaS Rechenzentrum	Kontrollieren Sie, ob der WireGuard-VPN-Tunnel in das TlaaS Rechenzentrum aufgebaut wurde. Falls Sie einen bereitgestellten WireGuard-VPN-Tunnel verwenden (siehe Abschnitt 14.2) so kontrollieren Sie, ob Ihr Gerät korrekt konfiguriert ist, sodass der WireGuard-VPN-Tunnel aufgebaut wird und andere Hosts diesen verwenden können.
	vKonnektor Zertifikat inkorrekt/ungültig	Importieren Sie das im Installationspaket übermittelte vKonnektor Zertifikat erneut (siehe Abschnitt 10.1).
	Ungültige VPN-Verbindung	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
	vKonnektor offline	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf, wenn das Problem länger als 5 Minuten besteht.

16.2 Zertifikate

Tabelle 4: Mögliche Fehlerursachen betreffend Zertifikaten

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Der angeführte KeyStore konnte nicht importiert werden. Bitte überprüfen Sie die Eingabe.	Falsches Passwort beim Import des Zertifikats	Kontrollieren Sie die Korrektheit des eingegebenen Passworts und geben es erneut ein.
Automatische Aktualisierung des Schlüsselmaterials fehlgeschlagen. Bitte starten Sie die Applikation neu.	Interner Zertifikatsfehler des TlaaS Clients	Starten Sie die Applikation des TlaaS Clients neu.

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Ein Validierungsfehler ist aufgetreten. Bitte überprüfen Sie die Eingabe	Ungültiges Dateiformat des hochzuladenden Zertifikats (sollte verhindert werden).	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.

16.3 Kartenterminal

Tabelle 5: Mögliche Fehlerursachen betreffend Kartenterminal

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Service Announcement konnte nicht empfangen werden.	Das Kartenterminal befindet sich nicht im selben Netzwerk.	Stellen Sie sicher, dass das Kartenterminal über seinen Ethernet-Port mit dem selben lokalen Netzwerk verbunden ist wie Ihr PC auf dem der TlaaS Client läuft.
	Es wurde ein falsches Netzwerkinterface ausgewählt.	Wählen Sie das korrekte Netzwerkinterface aus der angebotenen Liste aus (siehe Abschnitt 5.2).
	Es wurde eine falsche Kartenterminal IP-Adresse angegeben.	Kontrollieren Sie, ob die IP-Adresse des Kartenterminals korrekt eingegeben wurde. Vergewissern Sie sich bei Ihrem Netzwerkadministrator, dass Sie die korrekte IP-Adresse verwenden.
	Das Kartenterminal ist bereits mit einem Konnektor verbunden.	Heben Sie die Kartenterminal-Zuweisung zu diesem Kartenterminal bei allen lokalen Konnektoren auf. Besitzen Sie keine lokalen Konnektoren, nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
Kartenterminal konnte nicht in der KVS hinzugefügt werden.	Keine/schlechte Internetverbindung	Überprüfen Sie Ihre Internetverbindung.
	Ungültige VPN-Verbindung	Kontrollieren Sie, ob der vKonnektor erreichbar ist (siehe Abschnitt 4).
	Das KVS Zertifikat ist inkorrekt/ungültig.	Importieren Sie das im Installationspaket übermittelte KVS Zertifikat erneut (siehe Abschnitt 10.1). Bei bestehendem Problem, nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
	Keine Verbindung zum	Kontrollieren Sie, ob der WireGuard-VPN-

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
	TlaaS Rechenzentrum	Tunnel in das TlaaS Rechenzentrum aufgebaut wurde.
Pairing-Information konnte nicht gefunden werden.	Unzureichende Pairing-Daten wurden bei der Weitergabe der Kartenterminal-Informationen bereitgestellt.	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
Die aktualisierte Konfiguration konnte nicht geschrieben werden.	Der TlaaS Client kann die bestehende Kartenterminal-Konfigurationsdatei nicht anpassen.	Stellen Sie sicher, dass die Kartenterminal-Konfigurationsdatei <i>application-card-terminal.yml</i> (siehe Abschnitt 10.6) nicht in einem anderen Programm geöffnet ist. Der TlaaS Client muss über Schreibrechte an der Datei verfügen.
Kartenterminal bereits verbunden.	Das Kartenterminal ist bereits mit dem TlaaS Clients verbunden.	Entfernen Sie das Kartenterminal per Auswahl in der Kartenterminalübersicht (siehe Abschnitt 5.4). Erscheint das betroffene Kartenterminal nicht in der Liste, entfernen Sie es direkt aus der Kartenterminal-Konfigurationsdatei <i>application-card-terminal.yml</i> (siehe Abschnitt 10.6). Verbinden Sie das Kartenterminal neu über den TlaaS Client.
Das Kartenterminal konnte in der KVS nicht entfernt werden.	Das Entfernen des Kartenterminals am vKonnektor ist fehlgeschlagen.	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
Kartenterminal-Proxy konnte nicht gestartet werden.	Notwendige Ports für die Kommunikation zwischen vKonnektor und dem Kartenterminal sind bereits belegt.	Stellen Sie sicher, dass die vom Kartenterminal verwendeten Ports nicht durch andere Services auf Ihrem PC belegt werden.
Service Announcement konnte nicht gelesen werden.	Der TlaaS Client hat ungültige Kartenterminal-Informationen vom Kartenterminal erhalten.	Versuchen Sie, das Kartenterminal erneut hinzuzufügen (siehe Abschnitt 5.2). Bei bestehendem Problem nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
Service Discovery fehlgeschlagen.	Es ist ein Problem beim Abruf der Kartenterminal-Informationen vom	Versuchen Sie, das Kartenterminal erneut hinzuzufügen (siehe Abschnitt 5.2). Bei bestehendem Problem nehmen Sie Kontakt

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
	Kartenterminal aufgetreten.	mit Ihrem TlaaS Anbieter auf.
Socket konnte nicht geöffnet werden.	Die Schnittstelle zum Abruf der Kartenterminal-Informationen konnte nicht geöffnet werden.	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
System-Informationen konnten nicht abgefragt werden.	Die Netzwerkinterfaces konnten nicht abgerufen werden.	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
Die Pairingblöcke des Kartenterminals sind voll. Bitte die Pairingblöcke am Kartenterminal freigeben, um das Hinzufügen des Kartenterminals zu ermöglichen.	Die Pairingblöcke des Kartenterminals sind voll.	Geben Sie die Pairingblöcke auf ihrem Kartenterminal gemäß dessen Handbuch frei.

16.4 Karten

Tabelle 6: Mögliche Fehlerursachen betreffend Karten

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Fehler beim Laden der Karten, Fehler bei der PIN Verifizierung, Fehler bei der PIN Änderung, Fehler bei der PIN Entsperrung	Keine/schlechte Internetverbindung	Überprüfen Sie, ob Sie eine bestehende Internetverbindung haben.
	Kartenterminal nicht verbunden	Verbinden Sie ein Kartenterminal, um die Kartenübersicht anzuzeigen zu können.
	TlaaS Client-Konfiguration inkorrekt	Kontrollieren Sie die KVS IP-Adresse in der Konfigurationsdatei (siehe Abschnitt 10.4). Stimmt diese nicht mit der, in der ausgelieferten Konfigurationsdatei hinterlegten KVS IP-Adresse überein, passen Sie die KVS IP-Adresse in der bestehende TlaaS-Client Konfigurationsdatei an.
	KVS Zertifikat inkorrekt/ungültig	Importieren Sie das im Installationspaket übermittelte KVS Zertifikat erneut (siehe Abschnitt 10.1). Bei bestehendem Problem,

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
		nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf.
	Ungültige VPN-Verbindung	Überprüfen Sie, ob der vKonnektor erreichbar ist (siehe Abschnitt 4).
	vKonnektor offline	Nehmen Sie Kontakt mit Ihrem TlaaS Anbieter auf, wenn das Problem länger als 5 Minuten besteht.
	Keine Verbindung zum TlaaS Rechenzentrum	Kontrollieren Sie, ob der WireGuard-VPN-Tunnel in das TlaaS Rechenzentrum aufgebaut wurde.
Fehler bei der PIN Verifizierung, Fehler bei der PIN Änderung, Fehler bei der PIN Entsperrung	Bestätigung der PIN am Kartenterminal verpasst	Kartenoperation erneut durchführen und rechtzeitig am Kartenterminal bestätigen.

16.5 KIMaaS

Tabelle 7: Mögliche Fehlerursachen betreffend KIMaaS

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Die eingegebenen Informationen sind nicht korrekt. Bitte überprüfen Sie Ihre Angaben.	Eingabe eines falschen Installationscodes.	Kontrollieren Sie die Korrektheit des Installationscodes und geben Sie diesen erneut ein.

16.6 Maximum Transmission Unit (MTU)

Standardmäßig wird bei der Installation des TIC bzw. von WireGuard eine Maximum Transmission Unit (MTU) von 1420 festgelegt. Unter Umständen⁵ ist es notwendig, die MTU anzupassen. Im folgenden Beispiel wird die MTU auf 1280 gesetzt.

16.6.1 Windows

1. Öffnen Sie die Benutzeroberfläche von WireGuard. Wählen Sie die Verbindung *tiaas-vpn* und bearbeiten Sie diese.

⁵ Beispielsweise abweichender Technologiestandard des Internetanbieters

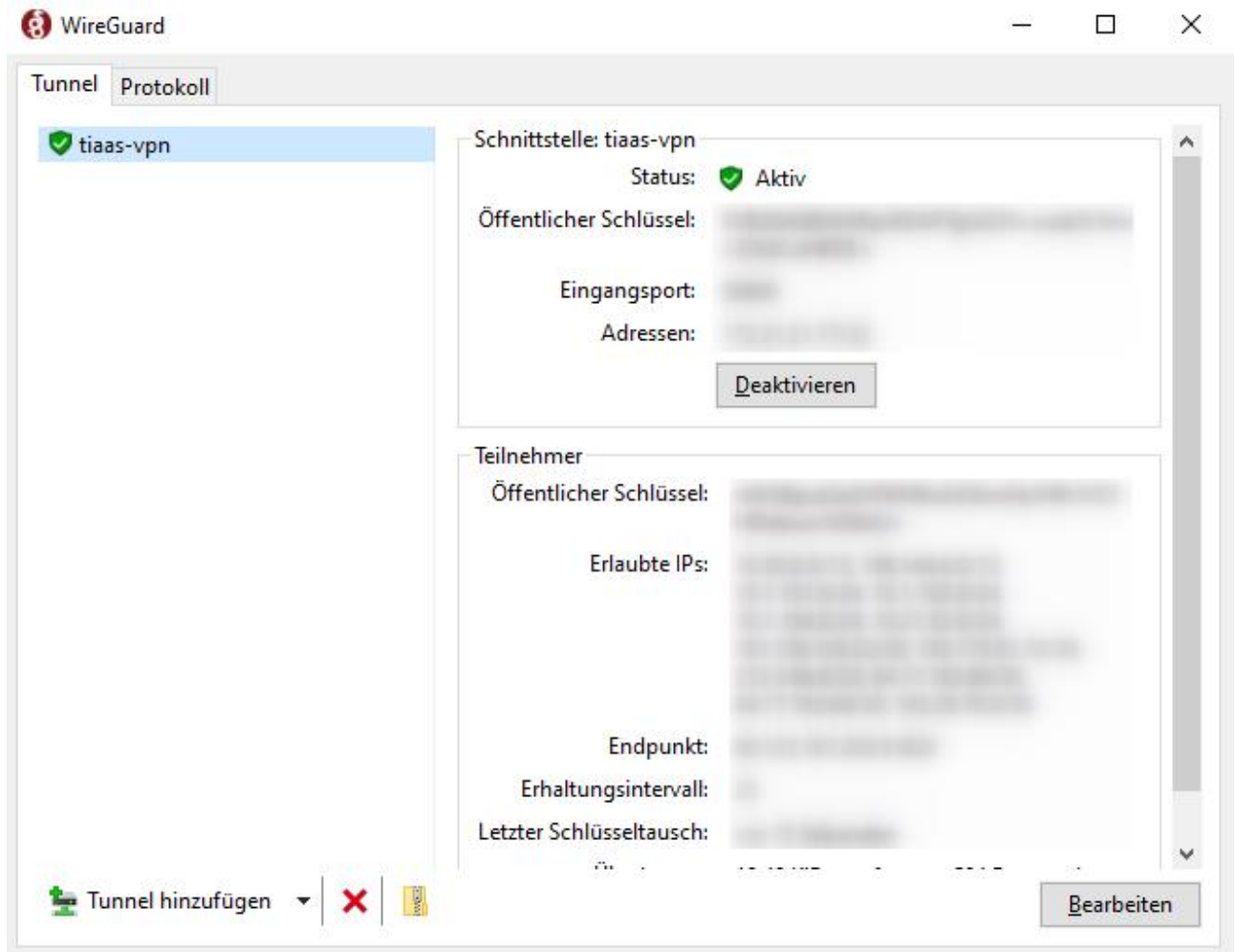


Abbildung 30: WireGuard Benutzeroberfläche

2. Im Abschnitt *[Interface]* fügen Sie in einer neuen Zeile den Text $MTU = 1280$ ein, sofern noch keine Zeile mit einem MTU-Wert existiert. Sollte bereits eine Zeile mit einem MTU-Wert im Abschnitt *[Interface]* vorhanden sein, passen Sie den Wert dieser Zeile an.

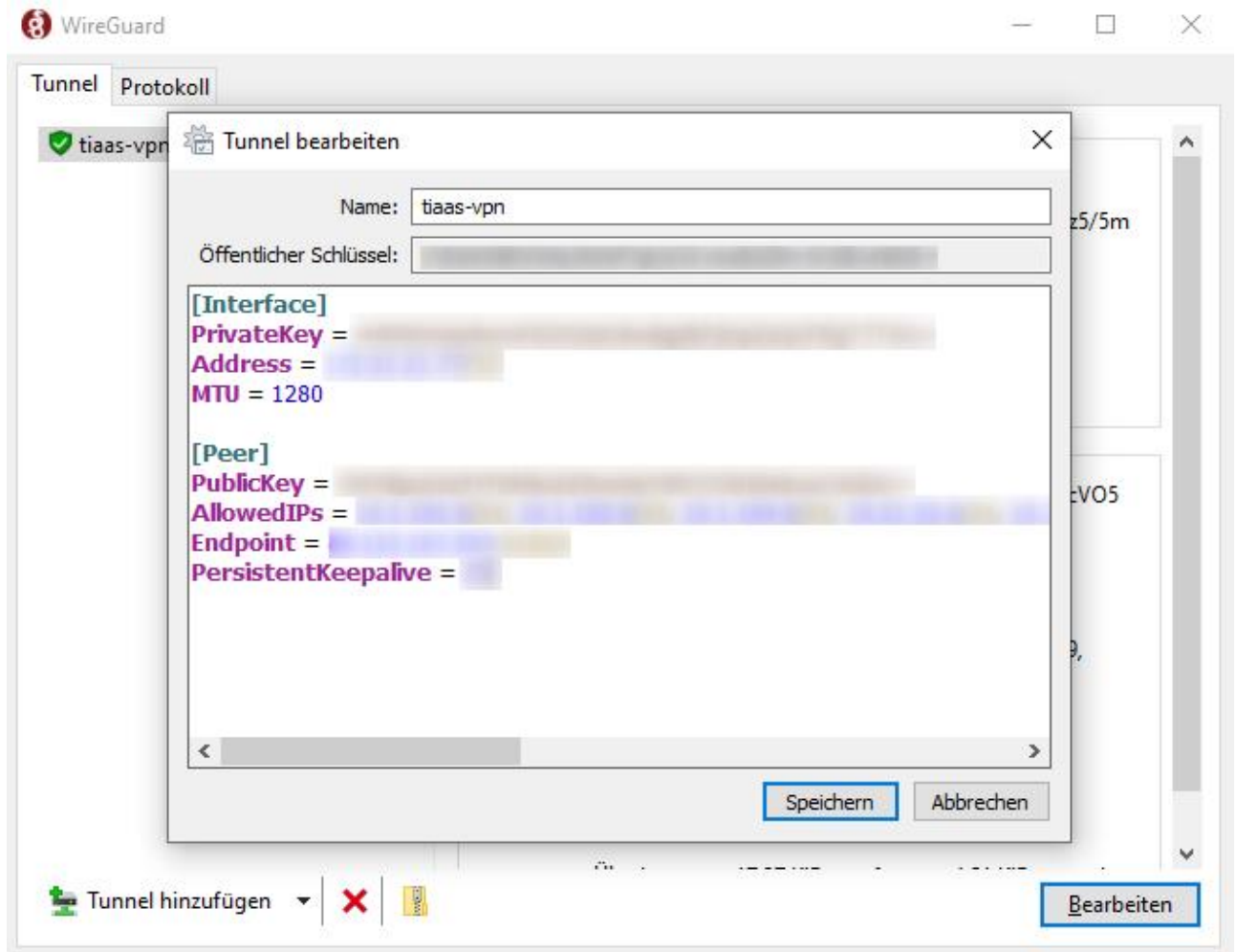


Abbildung 31: Einstellungen der WireGuard-Verbindung

- Speichern Sie die Änderungen, um das Fenster zu schließen. Die WireGuard-Verbindung wird automatisch neu gestartet.

Bei erfolgreicher Konfiguration der Verbindung wird der eingestellte MTU-Wert in der WireGuard-Benutzeroberfläche angezeigt.

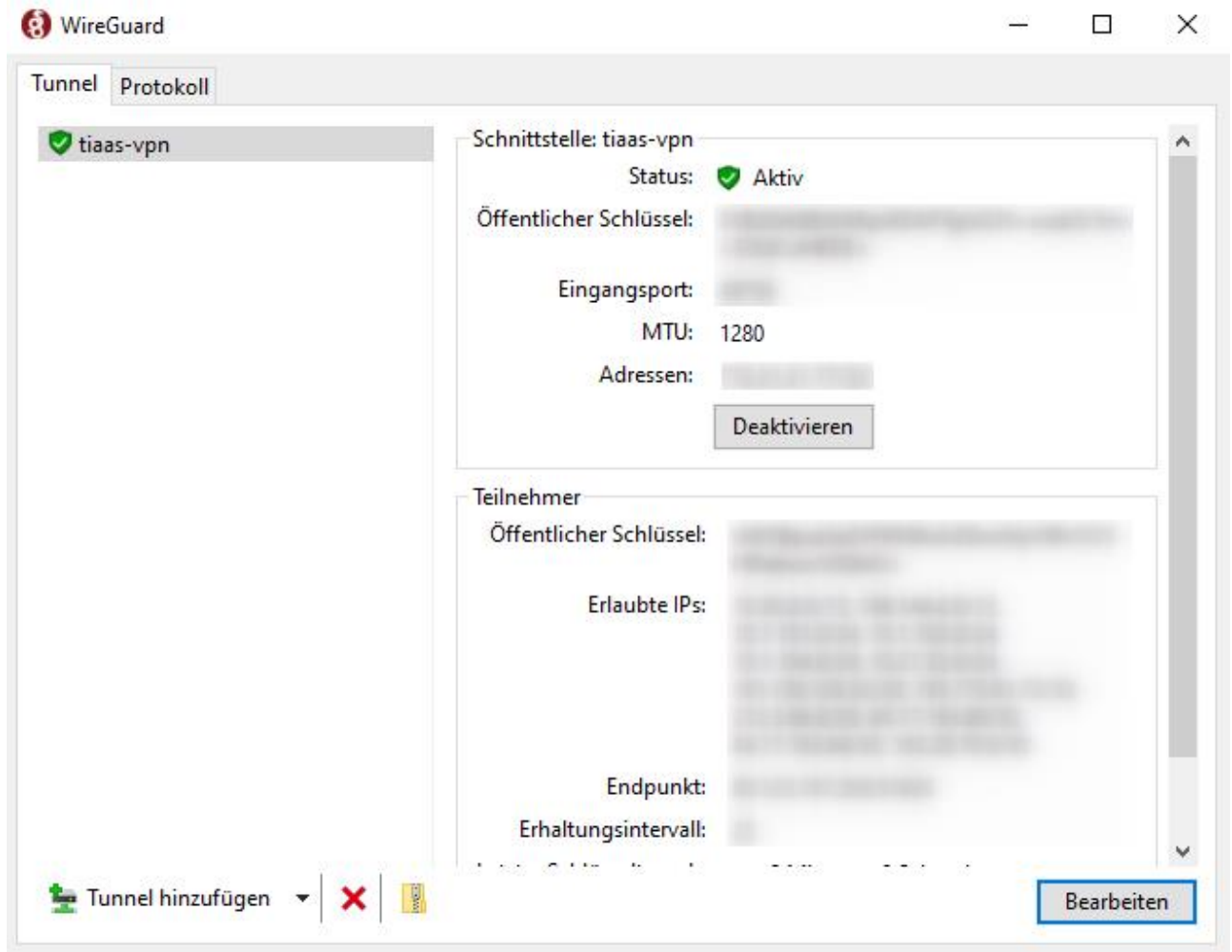


Abbildung 32: WireGuard Benutzeroberfläche mit eingestellter MTU

16.6.2 macOS und Linux

1. Falls die VPN-Verbindung nicht aktiv ist, starten Sie diese mit folgendem Kommandozeilenbefehl:

```
sudo wg-quick up tiaas-vpn
```

2. Bearbeiten Sie die Konfigurationsdatei *tiaas-vpn.conf*, welche unter */usr/local/etc/wireguard/* unter macOS und unter */etc/wireguard* unter Linux zu finden ist, mit Administrator/Root-Rechten. Im Abschnitt *[Interface]* fügen Sie in einer neuen Zeile den Text *MTU = 1280* ein, sofern noch keine Zeile mit einem MTU-Wert existiert. Sollte bereits eine Zeile mit einem MTU-Wert im Abschnitt *[Interface]* vorhanden sein, passen Sie den Wert dieser Zeile an. Speichern Sie die Datei ab.

```
[Interface]
Address = 
MTU = 1280
ListenPort = 
PrivateKey = 

[Peer]
PublicKey = 
AllowedIPs = 
Endpoint = 
PersistentKeepalive = 
```

Abbildung 33: WireGuard Konfigurationsdatei

© Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F
2320 Schwechat
Austria, Europe

<https://www.rise-world.com>
welcome@rise-world.com