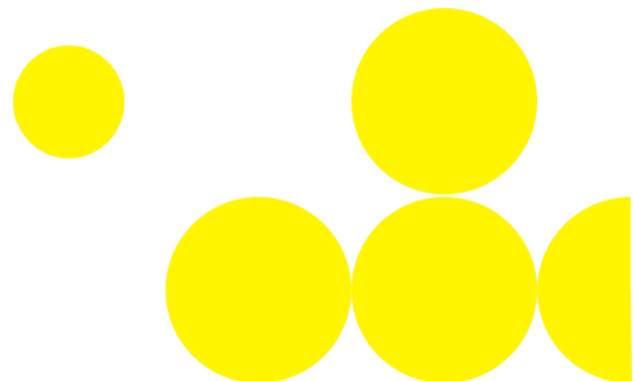


Anleitung für initiale Anmeldung mit 2-Faktor-Authentifizierung (FAQ)

ONTRAS Gastransport GmbH



Verdichterstation Bobbau




- **Wie richte ich die 2-Faktor-Authentifizierung ein?**
- Während der Übergangsphase vom 08.01.2024 bis 31.03.2024 kann die Anmeldung am Kundenportal wie bisher erfolgen (Benutzername/E-Mail-Adresse und Passwort).
- Während dieser Übergangsphase wird dem Kundenportalnutzer optional angeboten, die 2-Faktor-Authentifizierung einzurichten.
- Mit Ende der Übergangsphase am 01.04.2024 wird die Einrichtung der 2-Faktor-Authentifizierung mit dem ersten Anmeldeversuch verpflichtend.
- Um die Maske zur Einrichtung zu öffnen, muss der Link „Einrichten“ ausgewählt werden oder im Bereich der eigenen Daten (aufrufbar über den Benutzernamen oben rechts) zu den „Authentifizierung bearbeiten“ wechseln. In diesem Bereich kann die Funktion „Authenticator-Anwendung einrichten“ ausgewählt werden.

Mehrfachauthentifizierung konfigurieren

1. Installieren Sie eine der folgenden Applikationen auf Ihrem Smartphone:

- FreeOTP Authenticator
- Google Authenticator
- Microsoft Authenticator

2. Öffnen Sie die Applikation und scannen Sie den QR-Code.



[Sie können den QR-Code nicht scannen?](#)

3. Geben Sie den von der Applikation generierten One-time Code ein und klicken Sie auf Absenden.

Geben Sie einen Gerätenamen an, um die Verwaltung Ihrer OTP-Geräte zu erleichtern.

One-time Code *

Gerätename

Absenden
Abbrechen

Abbildung 1: Übersicht der möglichen Applikationen und Vorgehensweise

- Die Einrichtung des zweiten Sicherheitsfaktors erfolgt in folgenden Schritten:
 - Im ersten Schritt muss eine unterstützte Applikation auf dem Smartphone zur Einrichtung der 2-Faktor-Authentifizierung installiert werden.
 - Anschließend ist die gewählte Applikation zu öffnen.
 - **FreeOTP Authenticator:**
 - Im ersten Schritt muss „Add a token“ oder das QR-Code-Symbol ausgewählt werden.
 - Anschließend ist der im Kundenportal generierte QR-Code zu scannen.

- Im Anschluss ist es möglich, für die Anwendung ein Icon innerhalb der Applikation zu vergeben.
- Es ist zu entscheiden, ob das Smartphone immer entsperrt werden muss, um einen Code zu erhalten.

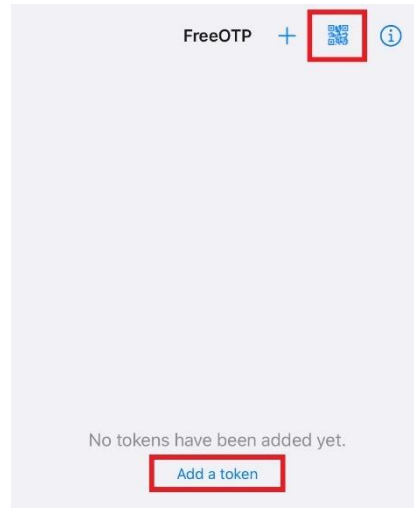


Abbildung 2: Startseite der Applikation FreeOTP Authenticator

- Nun ist das Konto und ein dazugehöriger One-time Code zu sehen.
- **Google Authenticator**
 - Zunächst muss die Schaltfläche „Code hinzufügen“ ausgewählt werden.

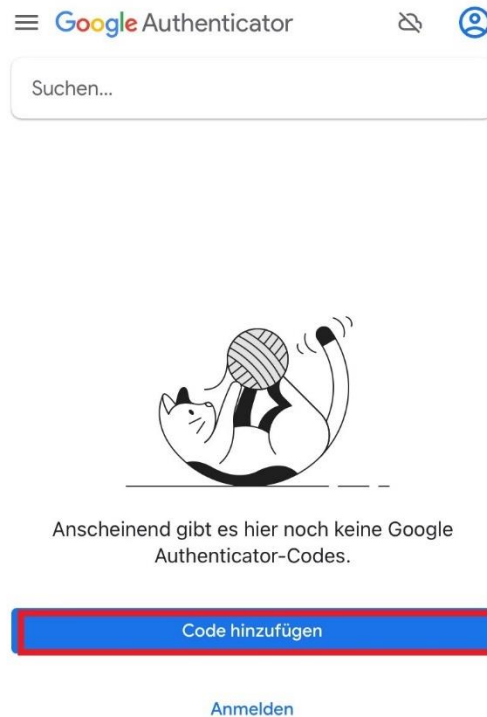


Abbildung 3: Startseite der Applikation Google Authenticator

- Im nächsten Schritt ist der Button „QR-Code scannen“ auszuwählen.
- Der im Kundenportal generierte QR-Code ist dann mit dem Smartphone einzuscannen.
- Mit der Eingabe des in der Applikation erzeugten One-time-Codes im Kundenportal ist die Einrichtung abgeschlossen.

○ **Microsoft Authenticator**

- Im ersten Schritt muss das Plus-Symbol ausgewählt werden.



Abbildung 4: Leiste auf Startseite der Applikation Microsoft Authenticator

- Als Art des Kontos ist „Anderes“ zu wählen.

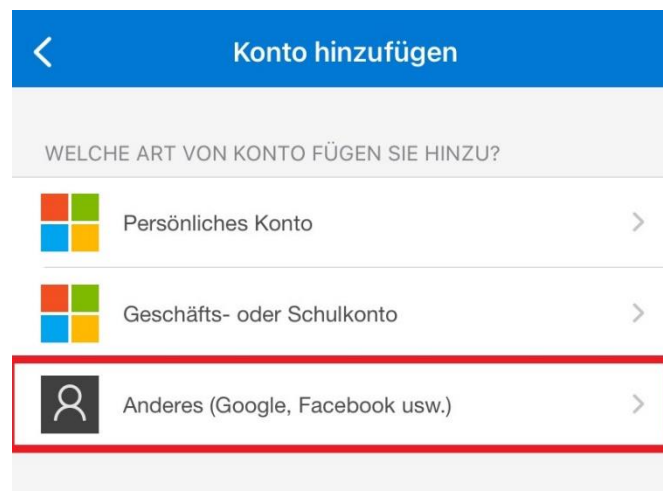


Abbildung 5: Kontoarten in der Applikation Microsoft Authenticator

- Anschließend kann der im Kundenportal generierte QR-Code gescannt werden.
- Nun ist das Konto und ein dazugehöriger One-time Code zu sehen.
- Hinweis: Wird das gleiche Gerät ein zweites Mal registriert, muss es bei Nutzung des Microsoft Authenticators dort erst entfernt werden.

○ **Physisches Gerät**

- Falls kein Mobilgerät vorhanden ist, besteht die Möglichkeit, sich mit einem physischen Gerät wie zum Beispiel dem REINER SCT Authenticator zu authentifizieren.
- Die Einrichtung des REINER SCT erfolgt in folgenden Schritten:
 - Bei erster Verwendung des Geräts ist es notwendig die Uhrzeit zu setzen.
 1. Rufen Sie mit Ihrem Internet-Browser folgende Adresse auf: www.reiner-sct.com/sync
 2. REINER SCT Authenticator mit OK-Taste einschalten
 3. ⚙-Taste drücken
 4. Zu „Uhrzeit“ navigieren (´v Taste) und mit OK-Taste auswählen
 5. „Setzen“ auswählen

6. www.reiner-sct.com/sync wird angezeigt, OK-Taste drücken
 7. Die Kamera geht an
 8. Jetzt den auf www.reiner-sct.de/sync angezeigten QR-Code abfotografieren
 9. Die Uhrzeit wird automatisch synchronisiert¹
- Dann wird das Konto für das ONTRAS Kundenportal hinzugefügt:
 1. REINER SCT Authenticator mit OK-Taste einschalten
 2. ⚙-Taste drücken
 3. „Konten“ auswählen (‘v-Taste)
 4. „Erfassen“ wählen, die Kamera öffnet sich
 5. Jetzt den im Kundenportal generierten QR-Code scannen
 6. Nun ist das Konto und ein One-time Code zu sehen
 7. Mit der Eingabe des Codes im Kundenportal ist die Einrichtung abgeschlossen
 - Die Einrichtung anderer physischer Geräte erfolgt laut Anleitung des Geräts.
- **Wiederherstellungscodes**
 - Zusätzlich zu der Authentifizierung mithilfe der Applikationen **sollten** Wiederherstellungscodes generiert werden. Diese können gespeichert, ausgedruckt oder in einen Passwort-Manager kopiert werden. Die Codes sind sicher zu verwahren. Mithilfe dieser Codes ist es möglich sich einzuloggen, wenn beispielsweise kein Zugriff auf das 2-Faktor-Gerät möglich ist.
- **Wie richte ich die Nutzung von Security-Token ein?**
 - Voraussetzung ist die erfolgreiche Einrichtung der 2-Faktor-Authentifizierung mit einem geeigneten 2-Faktor-Gerät.
 - Im angemeldeten Modus kann im Bereich der eigenen Daten (aufrufbar über den Benutzernamen oben rechts) zu „Authentifizierung bearbeiten“ gewechselt werden. In diesem Bereich kann die Funktion „Security-Token einrichten“ gewählt werden.



Abbildung 6: Maske zur Einrichtung des Security-Token

¹ [Anleitung Authenticator \(Version 1.0.3\) \(reiner-sct.com\)](http://reiner-sct.com)

- **Obwohl mein Gerät (insb. ein Reiner SCT) oder Smartphone-App für den zweiten Faktor den QR-Code richtig erkannt hat, schlägt die Einrichtung fehl oder (manchmal) ist der 6-stellige Code scheinbar falsch. Woran kann das liegen?**
 - Die Erzeugung gültiger 6-stelligen Codes ist von der genauen Uhrzeit Ihres Geräts abhängig. Ist die Uhrzeit des Geräts ungenau, akzeptiert das Portal die Codes nicht bzw. nicht die vollen 30 Sekunden, die sie ansonsten gültig wären. Bitte stellen Sie sicher, dass Ihr Gerät sekundengenau die richtige Uhrzeit hat. Smartphones stellen das in der Regel automatisch sicher, insbesondere Hardware-Geräte wie der Reiner SCT müssen manuell eingestellt werden, je nach Genauigkeit ihrer internen Uhr oder Batteriewechsels ggf. mehrmals pro Jahr. Reiner SCT bietet hierzu eine Webseite an, die die Zeitsynchronisation sehr komfortabel und genau durchführen kann: <https://www.reiner-sct.de/sync>.

- **Was mache ich, wenn ich keine Wiederherstellungscodes mehr habe und mein 2FA-Gerät verloren gegangen ist?**
 - Eine selbständige Wiederherstellung des Zugriffs ist in diesem Fall durch den Kundenportalnutzer nicht mehr möglich. Im ersten Schritt müssen hierfür die Kundenbetreuer der ONTRAS kontaktiert werden. Diese können nach entsprechender Authentifizierung des Anrufers im Kundenportal die für den Nutzer hinterlegten Geräte löschen. Im Anschluss kann der Kundenportalnutzer ein neues Gerät registrieren, um die 2-Faktor-Authentifizierung wieder durchzuführen (bitte siehe oben "Wie richte ich die 2-Faktor-Authentifizierung ein?").

- **Ich habe ein neues Gerät bekommen. Wie kann ich das neue Gerät registrieren?**
 - Hier gibt es zwei Möglichkeiten:
 - Wenn Sie das alte Gerät noch haben, können Sie sich damit anmelden und anschließend unter den eigenen Daten ein zweites Gerät registrieren. Dazu müssen Sie mit dem neuen Gerät nochmal einen QR-Code scannen, damit auch dort wieder der One-Time-Code generiert werden kann. Das Vorgehen ist genauso als würden Sie initial die 2FA einrichten. Nach Abschluss der Einrichtung können Sie zur Vollständigkeit das alte Gerät unter den eigenen Daten entfernen.
 - Alternativ geht es auch auf den Weg über die Wiederherstellungscodes, insbesondere, wenn das alte Gerät schon nicht mehr zur Verfügung steht. Nach der Anmeldung ist das Vorgehen identisch zu dem aus Variante 1, d.h. neues Gerät hinzufügen, QR-Code auf dem neuen Gerät scannen und zur Vollständigkeit das alte Gerät im Anschluss entfernen.

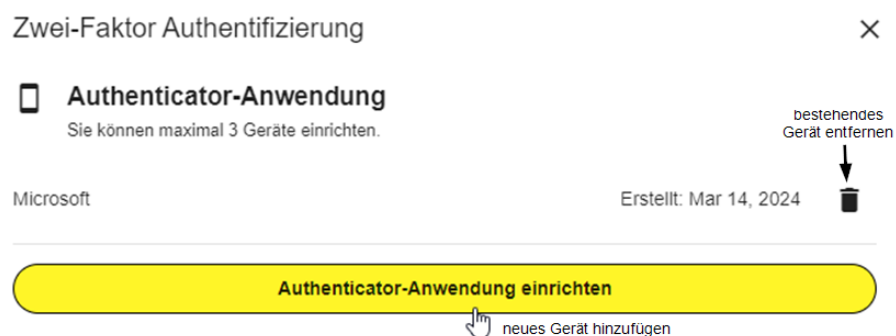


Abbildung 7: Vorgehen bei Gerätewechsel

- **Wie kann ich mein Passwort ändern?**

- Nach der Anmeldung am Kundenportal kann über den Menübereich der eigenen Daten (aufrufbar über den Benutzernamen oben rechts) der Dialog zum Ändern des Passworts aufgerufen werden. Dort kann ein neues Passwort gemäß der definierten Passwortrichtlinien vergeben werden.

- **Was mache ich, wenn ich mein Passwort vergessen habe?**

- In der Anmeldemaske vom Kundenportal steht für diesen Fall ein Absprungpunkt zur Verfügung, um über die Eingabe der E-Mailadresse oder des Benutzernamens ein neues Passwort zu vergeben.

Abbildung 8: Anmeldemaske vom ONTRAS Kundenportal

Abbildung 9: Passwort vergessen-Funktion