

sormas

2 Faktor Authentifizierung SORMAS

Version 1.1

Stand 15.07.2022

sormas

Wahrung der Vertraulichkeit

Dieses Dokument darf ohne schriftliche Genehmigung des Helmholtz Zentrum für Infektionsforschung weder ganz noch teilweise dupliziert, an Dritte weitergegeben oder anderweitig veröffentlicht werden. Dies gilt nicht für Kopien, die für die interne Verwendung bestimmt sind.

Versionshistorie

Datum/ Uhrzeit	Beschreibung	Kürzel Autor	Version
09.12.2021	2FA Konfiguration	SRA	1.0
22.12.2021	QS des Dokumentes	BIN	1.1
15.07.2022	Bestätigung von NLI, dass das Dokument noch aktuell ist. Daher bleibt die Versionsnummer unverändert; Datum wurde aktualisiert.	bin	1.1

Inhaltsverzeichnis

Wahrung der Vertraulichkeit.....	2
Versionshistorie.....	2
1. SORMAS 2 Faktor Authentifizierung	4
1.1 Allgemein.....	4
1.2 Vorgaben / Voraussetzungen	4
1.2.1 Verwaltung der Keycloak-Instanz und mögliche Übernahme der Verantwortung durch das Gesundheitsamt.....	4
1.2.2 OTP Apps	4
1.2.3 Hardware Authenticator	5
1.3 Keycloak Konfiguration.....	5
1.3.1 Keycloak Login	5
1.3.2 Keycloak Einstellungen	6
1.3.3 SORMAS User neu anlegen.....	7
1.3.4 Bestehende User	7
1.4 2FA Konfiguration.....	8
1.4.1 E-Mail-Adresse verifizieren	8
1.4.2 QR-Code scannen	9
1.4.3 Passwort festlegen	11
1.5 SORMAS Login	12
1.5.1 Username und Passwort	12
1.5.2 2FA One-Time Code (Einmalkennwort).....	13
1.5.3 User Einstellungen.....	14

sormas

sormas

1. SORMAS 2 Faktor Authentifizierung

1.1 Allgemein

In diesem Dokument wird beschrieben, wie die 2 Faktor Authentifizierung (2FA) auf den SORMAS Instanzen aktiviert und konfiguriert wird. Die Einrichtung kann von jedem Gesundheitsamt selbständig umgesetzt werden.

1.2 Vorgaben / Voraussetzungen

Die 2 Faktor Authentifizierung wird über Keycloak für jeden User aktiviert. Für den Zugriff sind die Admin Zugangsdaten erforderlich. Für den User wird eine beliebige OTP App z.B. FreeOTP oder Google Authenticator oder ein Hardware Authenticator wie z.B. REINER SCT Authenticator, benötigt (OTP – „One-Time-Password“ bzw. auf deutsch "Einmalkennwort").

1.2.1 Verwaltung der Keycloak-Instanz und mögliche Übernahme der Verantwortung durch das Gesundheitsamt

Die Verwaltung der Keycloak-Instanzen erfolgt durch Netzlink. Sollten Sie die Verwaltung Ihrer KeyCloak-Instanz selbst übernehmen wollen, ist eine Abänderung des Kennwortes unerlässlich.

Hinweis:

Bitte beachten Sie, dass Netzlink, wenn Sie die Verwaltung Ihrer Keycloak-Instanz selbst übernehmen, keinen KeyCloak-Support leisten kann. Sie übernehmen damit die Verantwortung für die Funktionalität der Authentifizierungsinstanz selbst und müssen sich in Fehlerfällen selbstständig um die Lösung bemühen.

Wenn Sie Ihre Keycloak-Instanz selbst verwalten möchten, wenden Sie sich an den SORMAS Support bei Netzlink unter support@sormas-oegd.de. Sie erhalten dann u.a. die Admin-Zugangsdaten.

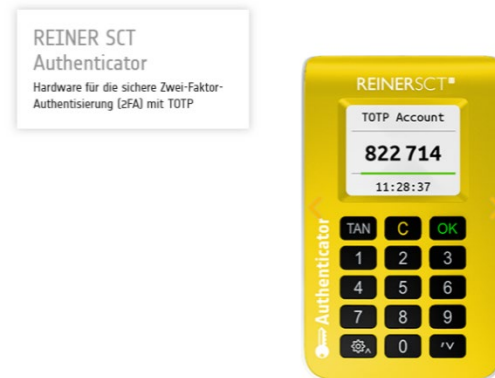
1.2.2 OTP Apps

OTP Apps stehen kostenlos in den App Stores von Apple und Google zum Download zur Verfügung. Hier einige Beispiele:

- Google Authenticator
- Microsoft Authenticator
- DUO Mobile
- FreeOTP

1.2.3 Hardware Authenticator

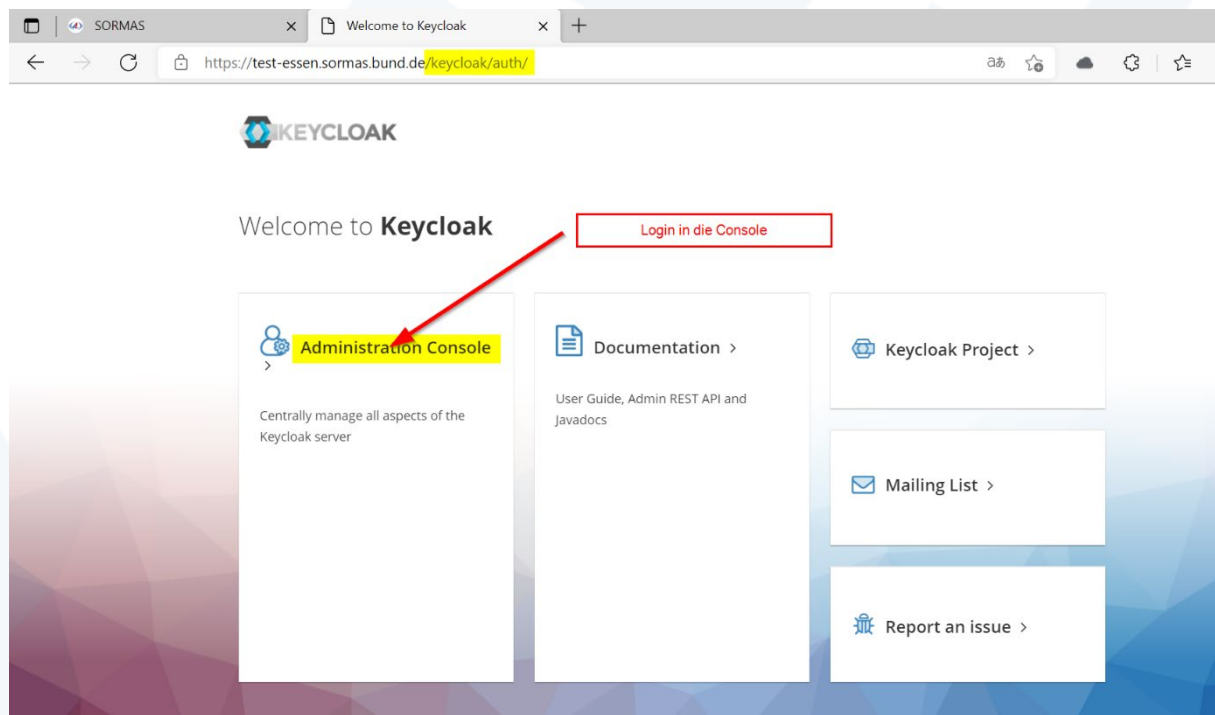
Alternativ zu den OTP Apps kann die 2 Faktor Authentifizierung auch mit einem Hardware Authenticator eingerichtet werden, z.B. von REINER SCT. Die Kosten für solche Geräte liegen bei ca. 40,-€; ggf. mit Mengenrabatt.



1.3 Keycloak Configuration

1.3.1 Keycloak Login

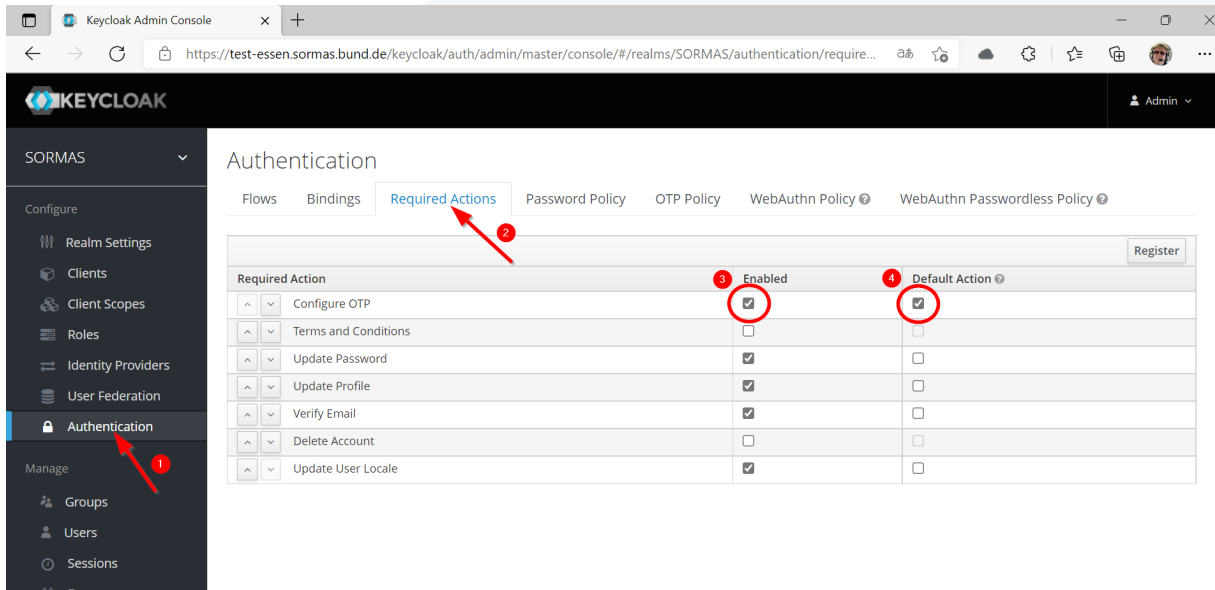
Rufen Sie die Keycloak Seite über folgende URL auf: <https://instanzname.sormas.bund.de/keycloak>. Loggen Sie sich mit den Admin Zugangsdaten auf der Console ein (s. Kapitel 1.2.1).



1.3.2 Keycloak Einstellungen

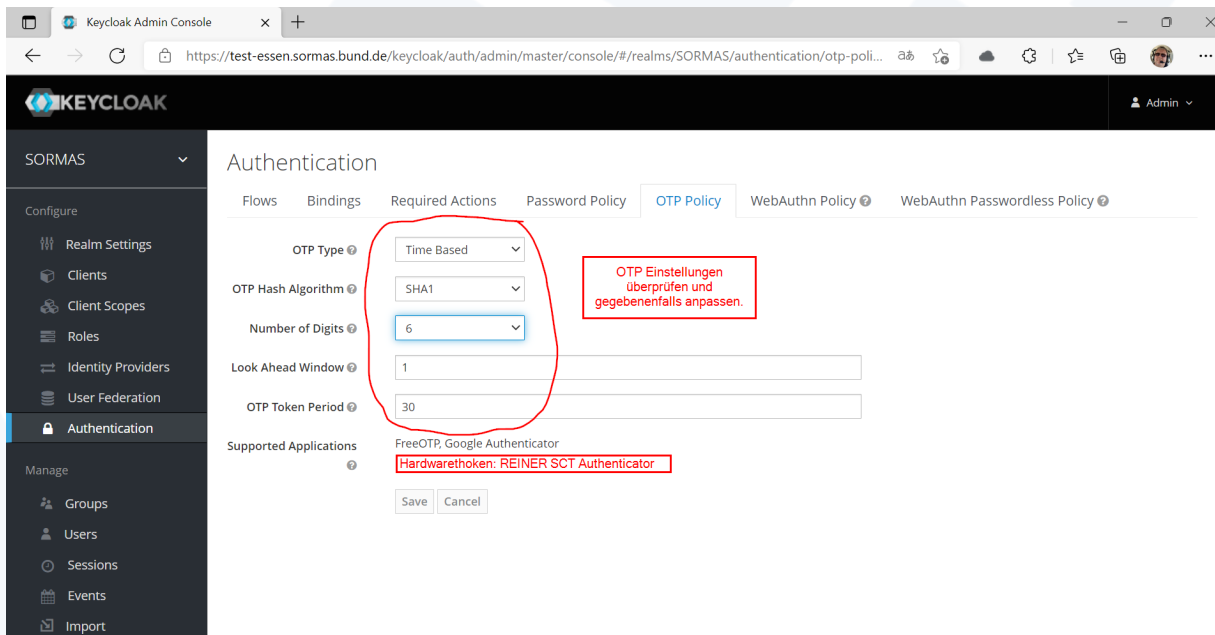
Führen Sie im Menü folgendes durch:

- Im Reiter Required Actions: die markierten Felder überprüfen und gegebenenfalls aktivieren.



Required Action	Enabled	Default Action
Configure OTP	☒	☒
Terms and Conditions	☐	☐
Update Password	☒	☐
Update Profile	☒	☐
Verify Email	☒	☐
Delete Account	☐	☐
Update User Locale	☒	☐

- Im Reiter OTP Policy: die markierten Einstellungen prüfen und gegebenenfalls anpassen,
- und abschließend die Einstellungen mit Klick auf Save speichern.



OTP Type: Time Based

OTP Hash Algorithm: SHA1

Number of Digits: 6

Look Ahead Window: 1

OTP Token Period: 30

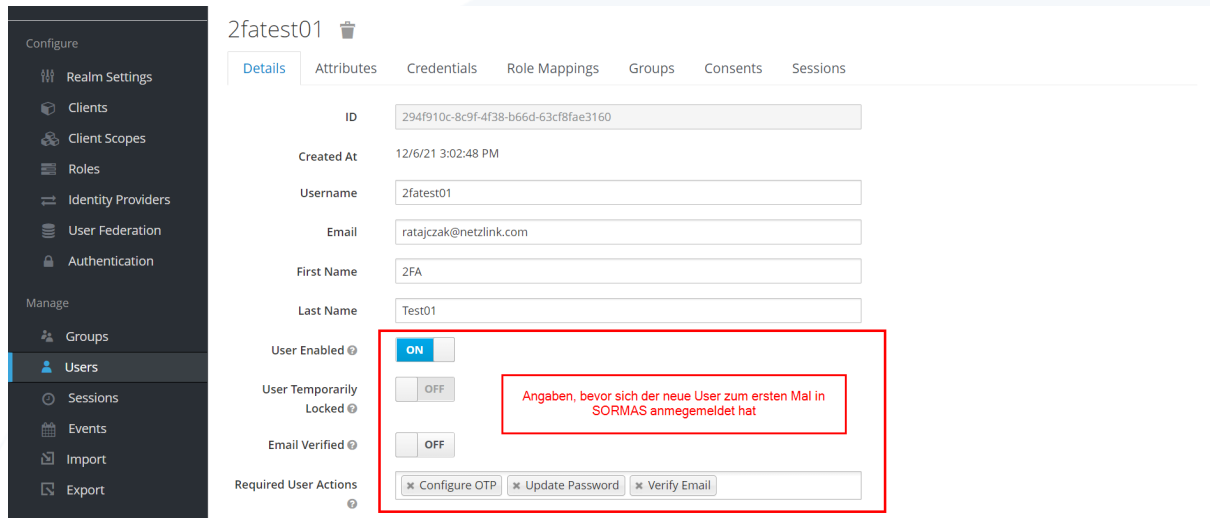
Supported Applications: FreeOTP, Google Authenticator, Hardwaretoken: REINER SCT Authenticator

Save Cancel

OTP Einstellungen überprüfen und gegebenenfalls anpassen.

1.3.3 SORMAS User neu anlegen

Für neu angelegte SORMAS User müssen die Einstellungen folgendermaßen vorgenommen werden, bevor sich die User zum 1. Mal im SORMAS anmelden.



2fatest01

Details Attributes Credentials Role Mappings Groups Consents Sessions

ID: 294f910c-8c9f-4f38-b66d-63cf8fae3160

Created At: 12/6/21 3:02:48 PM

Username: 2fatest01

Email: ratajczak@netzlink.com

First Name: 2FA

Last Name: Test01

User Enabled: ☒ ON

User Temporarily Locked: ☐ OFF

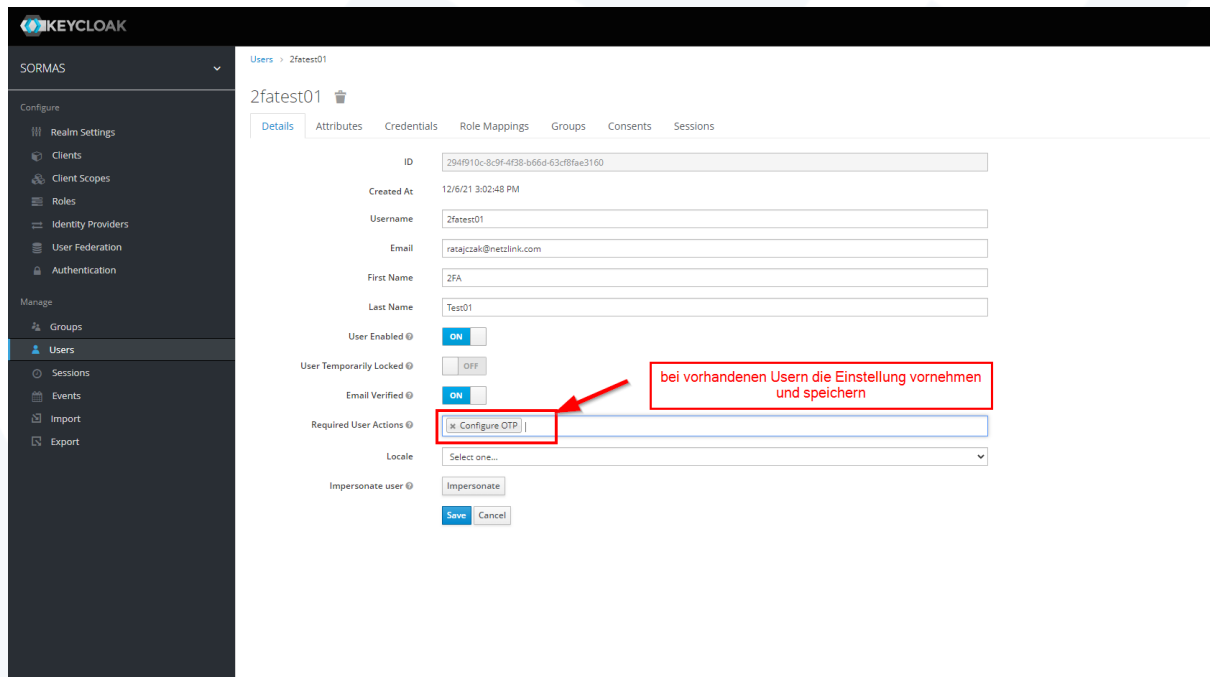
Email Verified: ☐ OFF

Required User Actions: ☒ Configure OTP ☒ Update Password ☒ Verify Email

Angaben, bevor sich der neue User zum ersten Mal in SORMAS angemeldet hat

1.3.4 Bestehende User

Um die 2 Faktor Authentifizierung bei bereits angelegten Usern zu aktivieren sind folgende Einstellungen in Keycloak vorzunehmen (s. folgende Abbildung). Bei erneuter Useranmeldung ist dann Punkt 1.4.2 durchzuführen.



KEYCLOAK

SORMAS

Users > 2fatest01

2fatest01

Details Attributes Credentials Role Mappings Groups Consents Sessions

ID: 294f910c-8c9f-4f38-b66d-63cf8fae3160

Created At: 12/6/21 3:02:48 PM

Username: 2fatest01

Email: ratajczak@netzlink.com

First Name: 2FA

Last Name: Test01

User Enabled: ☒ ON

User Temporarily Locked: ☐ OFF

Email Verified: ☒ ON

Required User Actions: ☒ Configure OTP

Locale: Select one...

Impersonate user: ☐ Impersonate

Save Cancel

bei vorhandenen Usern die Einstellung vornehmen und speichern

1.4 2FA Konfiguration

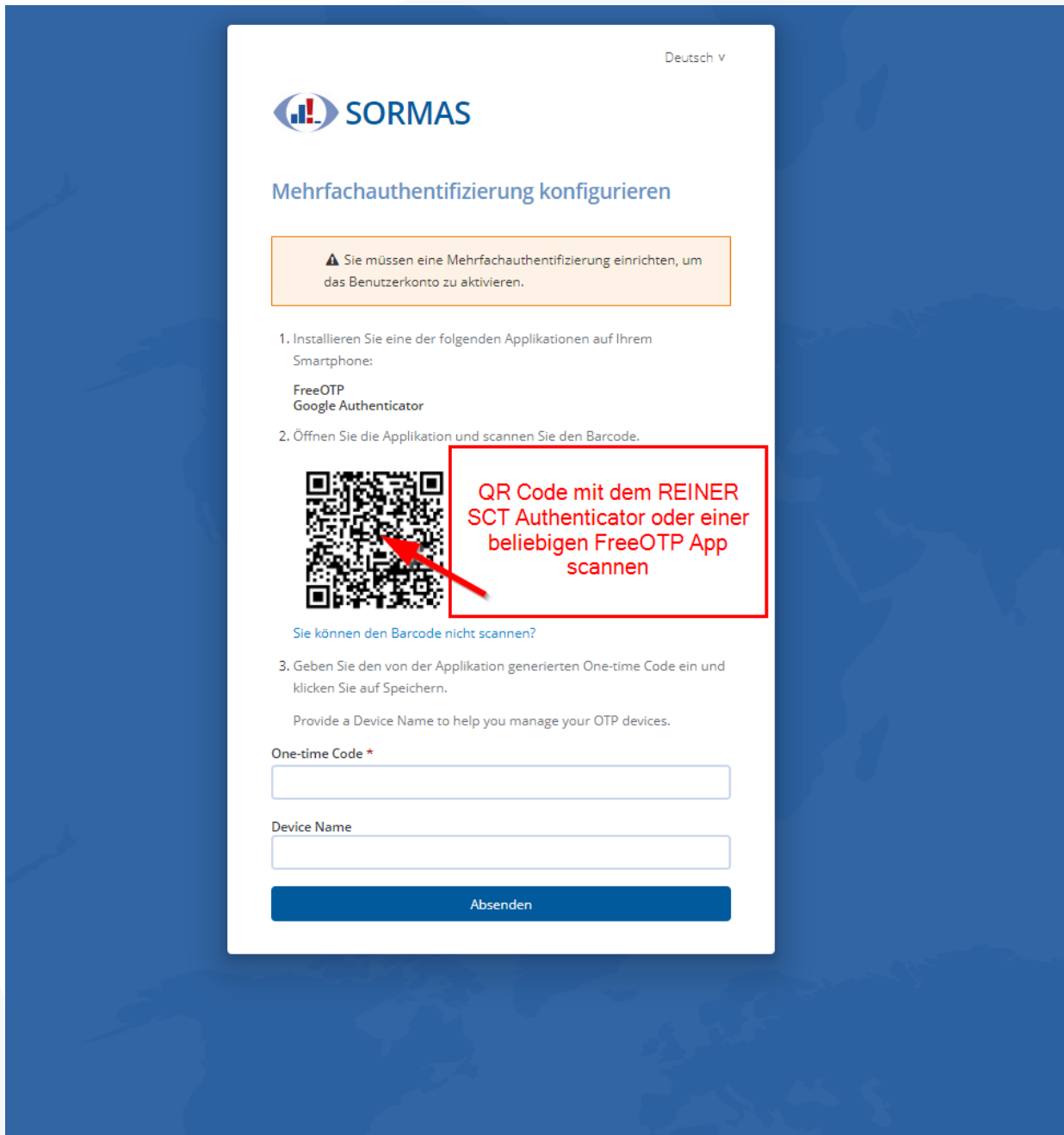
1.4.1 E-Mail-Adresse verifizieren

Das neue Userkonto muss über den Link, der nach der Anlage im SORMAS per Mail verschickt wird, aktiviert und die E-Mail-Adresse verifiziert werden. Dieser Schritt ist nur bei hinterlegter Mailadresse erforderlich.



1.4.2 QR-Code scannen

Zum Aktivieren der 2 Faktor Authentifizierung folgen Sie bitte den Schritten in den folgenden Abbildungen:



Deutsch v

 **SORMAS**

Mehrfachauthentifizierung konfigurieren

 Sie müssen eine Mehrfachauthentifizierung einrichten, um das Benutzerkonto zu aktivieren.

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

FreeOTP
Google Authenticator

2. Öffnen Sie die Applikation und scannen Sie den Barcode.



QR Code mit dem REINER SCT Authenticator oder einer beliebigen FreeOTP App scannen

[Sie können den Barcode nicht scannen?](#)

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

Provide a Device Name to help you manage your OTP devices.

One-time Code *

Device Name

Absenden

Deutsch v

 **SORMAS**

Mehrfachauthentifizierung konfigurieren

 Sie müssen eine Mehrfachauthentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie eine der folgenden Applikationen auf Ihrem Smartphone:
FreeOTP
Google Authenticator
2. Öffnen Sie die Applikation und scannen Sie den Barcode.



[Sie können den Barcode nicht scannen?](#)

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

Provide a Device Name to help you manage your OTP devices.

One-time Code *

755473

Device Name

SCT

Absenden

- Code hier eingeben, den die App oder der SCT nach dem Scannen anzeigt

- einen Namen vergeben

Zu beachten:

Bitte achten Sie darauf, dass nach dem Scannen des QR Codes und der Eingabe des One-time Codes nicht mehr als 30 Sekunden vergehen dürfen, da sonst die Einrichtung der 2 Faktor Authentifizierung fehlschlägt und der gesamte Einstellungsprozess wiederholt werden muss.

1.4.3 Passwort festlegen

Im nächsten Schritt legen Sie ein neues Passwort wie folgt fest:



The screenshot shows the SORMAS login page with the title "Passwort aktualisieren". A warning message states: "⚠ Sie müssen Ihr Passwort ändern, um das Benutzerkonto zu aktivieren." Below this are two input fields: "Neues Passwort" and "Passwort bestätigen". A blue "Absenden" button is at the bottom. Red arrows point from the input fields to a box labeled "- neues Passwort festlegen und bestätigen", and from the "Absenden" button to a box labeled "abschließend Absenden anklicken".

Deutsch v

 **SORMAS**

Passwort aktualisieren

⚠ Sie müssen Ihr Passwort ändern, um das Benutzerkonto zu aktivieren.

Neues Passwort

Passwort bestätigen

Absenden

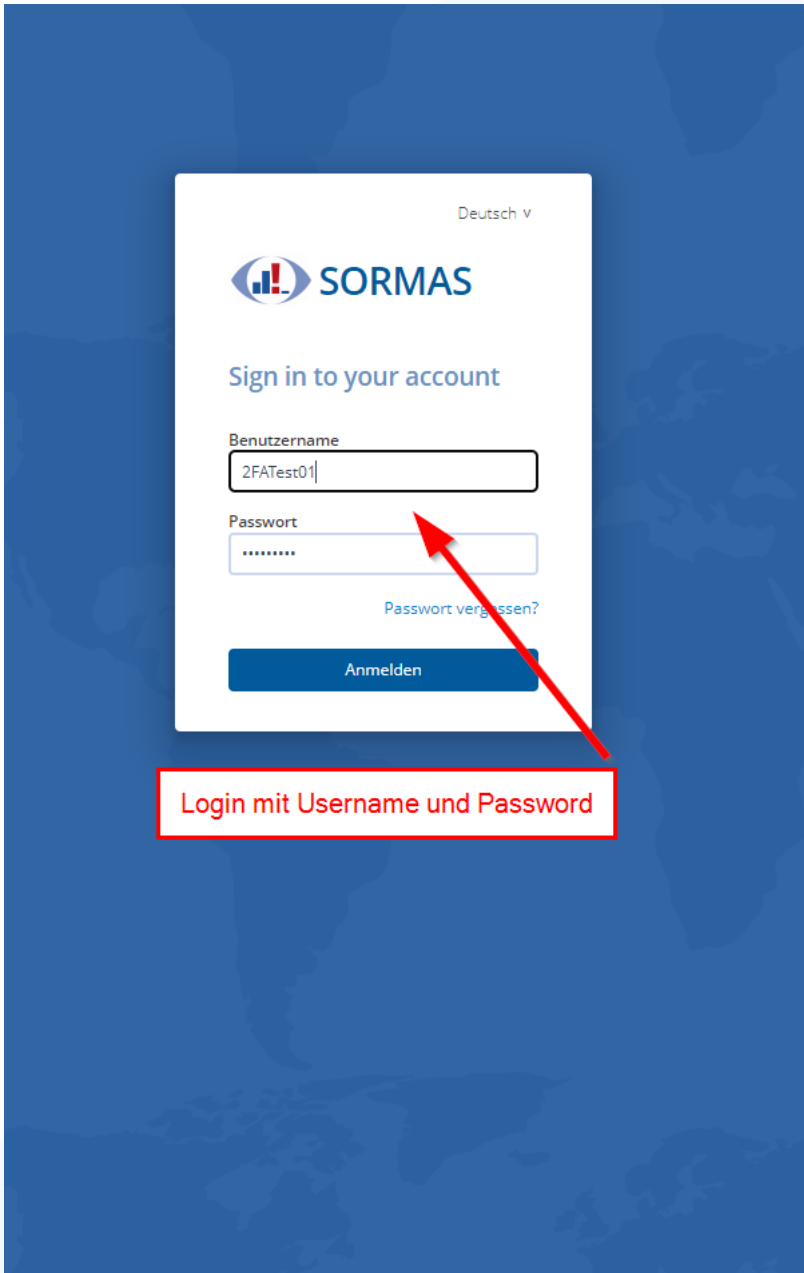
abschließend Absenden anklicken

- neues Passwort festlegen und bestätigen

1.5 SORMAS Login

1.5.1 Username und Passwort

Der Login erfolgt mit Username und Passwort wie nachfolgend dargestellt:



Deutsch v

 **SORMAS**

Sign in to your account

Benutzername

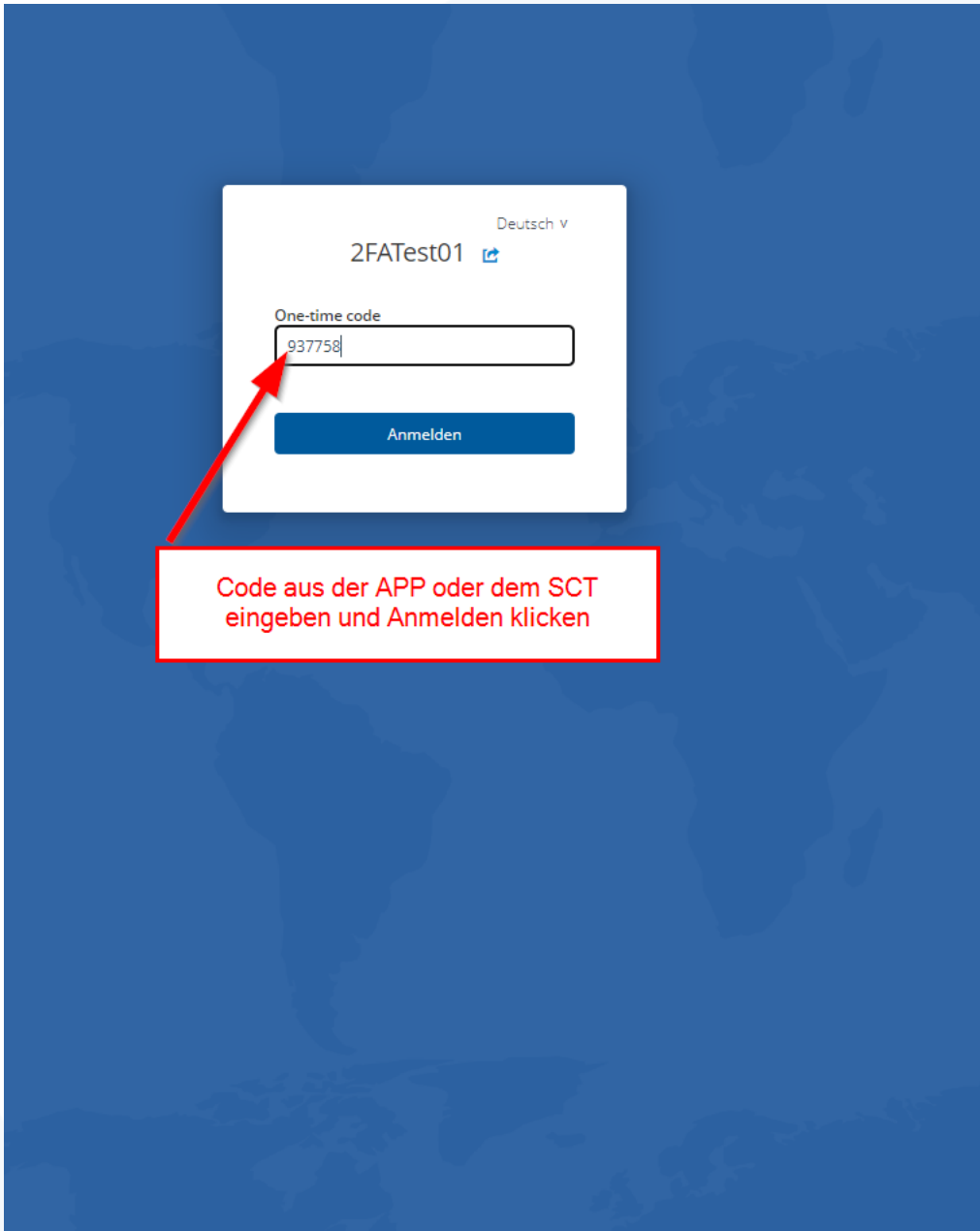
Passwort

[Passwort vergessen?](#)

Login mit Username und Passwort

1.5.2 2FA One-Time Code (Einmalkennwort)

Im nächsten Schritt den One-Time Code (Einmalkennwort) aus der OTP App oder dem REINER SCT Authenticator eingeben und mit dem Klick auf den Button „Anmelden“ bestätigen.

The screenshot shows a login interface for '2FATest01' with a language selector set to 'Deutsch'. It features a text input field labeled 'One-time code' containing the value '937758'. Below the input field is a blue button labeled 'Anmelden'. A red arrow points from a red-bordered text box to the input field. The background is a blue world map.

Deutsch v

2FATest01

One-time code

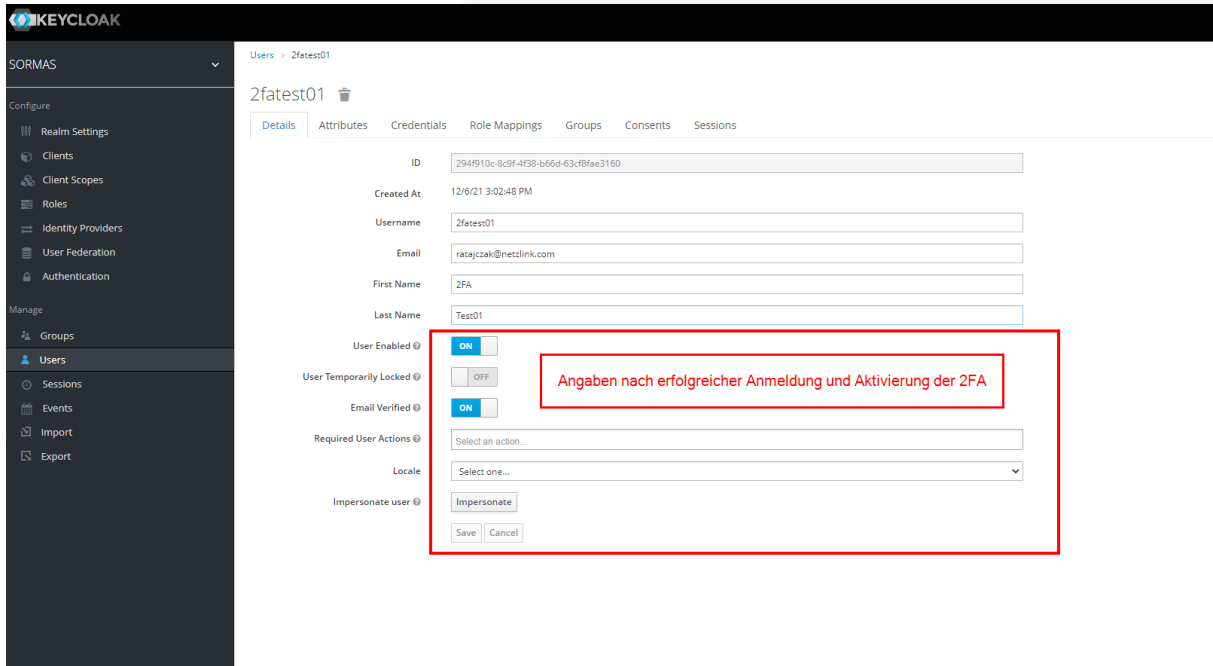
937758

Anmelden

Code aus der APP oder dem SCT eingeben und Anmelden klicken

1.5.3 User Einstellungen

Nach erfolgreicher 2 Faktor Authentifizierung-Konfiguration sehen die User Einstellungen im Keycloak folgendermaßen aus:



KEYCLOAK

SORMAS

Users > 2fatest01

2fatest01

Details Attributes Credentials Role Mappings Groups Consents Sessions

ID: 294f910c-8c9f-4f38-b66d-63cf8fae3160

Created At: 12/6/21 3:02:48 PM

Username: 2fatest01

Email: ratajczak@netzlink.com

First Name: 2FA

Last Name: Test01

User Enabled: ☒

User Temporarily Locked: ☐

Email Verified: ☒

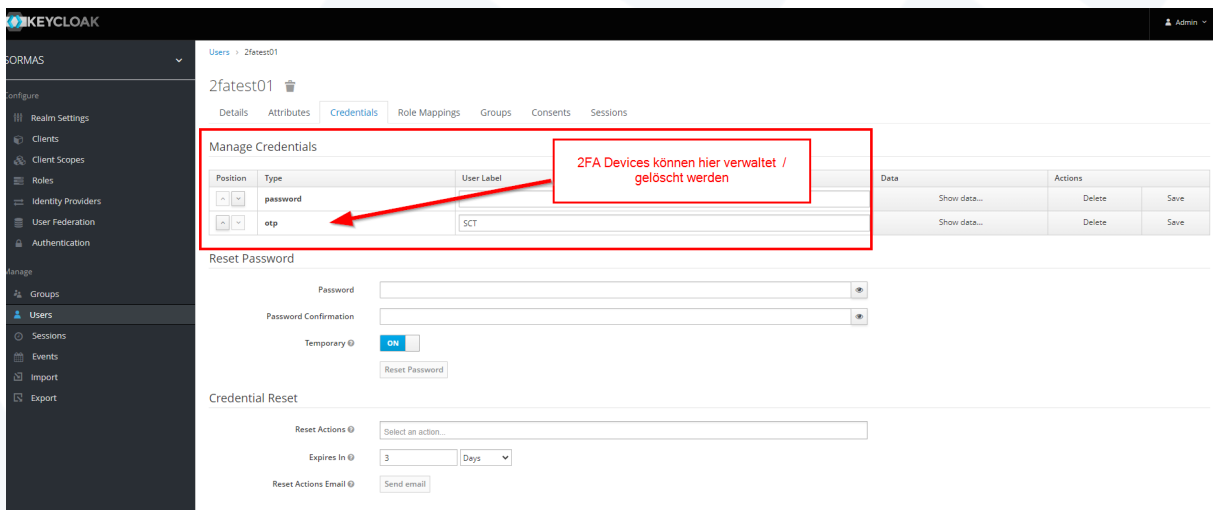
Required User Actions: Select an action...

Locale: Select one...

Impersonate user:

Angaben nach erfolgreicher Anmeldung und Aktivierung der 2FA

Die 2FA Devices können unter folgender Einstellung verwaltet und bei Bedarf gelöscht werden.



KEYCLOAK

SORMAS

Users > 2fatest01

2fatest01

Details Attributes Credentials Role Mappings Groups Consents Sessions

Manage Credentials

Position	Type	User Label
1	password	
2	otp	SCT

Reset Password

Password:

Password Confirmation:

Temporary: ☒

Credential Reset

Reset Actions: Select an action...

Expires in: 3 Days

Reset Actions Email:

2FA Devices können hier verwaltet / gelöscht werden