



Direktion für Inneres und Justiz
Amt für Geoinformation
Abteilung Grundstückinformationen

Reiterstrasse 11
3013 Bern
+41 31 633 33 11
info.agi@be.ch
www.be.ch/agi

Amt für Geoinformation, Reiterstrasse 11, 3013 Bern

Leitstelle GRUDA-AV (AGI)
gruda@be.ch

Unsere Referenz:

5. Mai 2026

Anleitung für die Zwei-Faktor-Authentifizierung (2FA) in der Applikation Capitastra-CGE

Die Anwenderinnen und Anwender von Capitastra-CGE (Capitastra-GUI-Erneuerung) können anhand dieser Anleitung ihre Zwei-Faktor-Authentifizierung (2FA) einrichten und anwenden.

Inhaltsverzeichnis

1. **Einrichten der Zwei-Faktor-Authentifizierung (2FA) für Capitastra-CGE.....2**
2. **Anwenden der Zwei-Faktor-Authentifizierung (2FA) für Capitastra-CGE10**

1. Einrichten der Zwei-Faktor-Authentifizierung (2FA) für Capitastra-CGE

- 1.1. Starten Sie Capitastra-CGE (Link siehe [Handbuch GRUDA-AV](#)).
- 1.2. Geben Sie ihren **vierstelligen** Benutzernamen, z.B. **mabc** und das Passwort ein und bestätigen Sie die Eingabe mit dem «Anmelden» Button.

Benutzername

Passwort

[Passwort vergessen?](#)

☐ Angemeldet bleiben

Anmelden

- 1.3. Installieren Sie eine Authenticator-Applikation (z.B. [FreeOTP](#), **Google Authenticator** [Android](#) / [iOS](#) oder **Microsoft Authenticator** [Android](#) / [iOS](#)) auf Ihrem Smartphone, sofern Sie nicht bereits eine Authenticator-Applikation installiert haben.

Authentifizierung einrichten

⚠ Sie müssen eine Mobile Authentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie [FreeOTP](#) oder [Google Authenticator](#) auf Ihrem Smartphone.

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



[Code manuell eingeben?](#)

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

One-time code *

Gerätename

Absenden

- 1.4. Öffnen Sie die Authenticator-Applikation auf Ihrem Smartphone und scannen Sie den QR-Code oder wählen Sie «Code manuell eingeben?».

Authentifizierung einrichten

⚠ Sie müssen eine Mobile Authentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie **FreeOTP** oder **Google Authenticator** auf Ihrem Smartphone.

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



[Code manuell eingeben?](#)

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

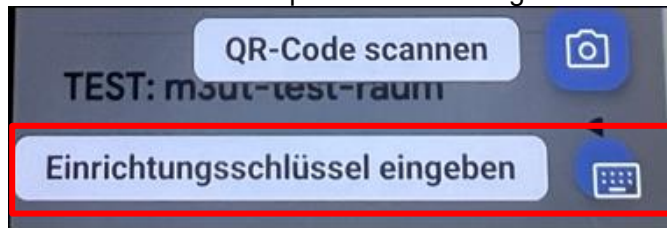
One-time code *

Gerätename

Absenden

- 1.4.1. Hinweis: Wenn Sie den Link «Code manuell eingeben?» nutzen, gehen Sie gemäss den folgenden Punkten 1.4.2 bis 1.4.7 vor. Ansonsten springen Sie zum [Punkt 1.5](#).
- 1.4.2. Öffnen Sie die Applikation (in diesem Beispiel den «Google Authenticator») und tippen Sie unten rechts auf das Plus-Zeichen (+).

1.4.3. Wählen Sie den Menüpunkt «Einrichtungsschlüssel eingeben».



1.4.4. Geben Sie im Feld «Codename» einen frei wählbaren Namen ein, aber wählen Sie diesen so, dass Sie diesen bei mehreren Schlüsseln wieder erkennen.

A screenshot of a mobile application interface titled 'Codedetails eingeben'. The interface has a back arrow on the top left. There are three input fields. The first field is labeled 'Codename' and is highlighted with a red rectangular border. The second field is labeled 'Mein Schlüssel'. The third field is labeled 'Schlüsseltyp' and has a dropdown menu with the value 'Zeitbasiert' selected.

- 1.4.5. Geben Sie im Feld «Mein Schlüssel» den Code ein, welcher auf der Maske (auf dem PC) «Authentifizierung einrichten» unter dem Punkt 2. ersichtlich ist und zwar inklusive der Leerzeichen (Hinweis: den Wert «Zeitbasiert» im Feld «Schlüsseltyp» können Sie so belassen).

← Codedetails eingeben

Codename

Mein Schlüssel

Schlüsseltyp
Zeitbasiert ▼

Authentifizierung einrichten

⚠ Sie müssen eine Mobile Authentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie **FreeOTP** oder **Google Authenticator** auf Ihrem Smartphone.
2. Öffnen Sie die Applikation und verwenden Sie zum Erstellen des Kontos den folgenden Code.
GVHT MRSH O5ZT M4TQ MQ3D KM3O MJKH MY2N
3. Verwenden Sie beim Erstellen folgende Konfigurationswerte, falls sie benötigt werden.

Typ	zeitbasiert (time-based) (TOTP)
Algorithmus	HmacSHA1
Ziffern	6
Intervall	30
4. Geben Sie den von der Applikation generierten **One-time Code** ein und klicken Sie auf Absenden.

One-time code *

Gerätename

Absenden

- 1.4.6. Geben Sie im Feld «One-time code*» den Code (ohne Leerzeichen) ein, welcher Ihnen auf dem «Google Authenticator» angezeigt wird (z.B. 266321). Das Feld «Gerätename» muss nicht ausgefüllt werden. Schliessen Sie die Eingabe mit dem «Absenden» Button ab.

TEST: m3ut-999

266 321

Authentifizierung einrichten

⚠ Sie müssen eine Mobile Authentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie **FreeOTP** oder **Google Authenticator** auf Ihrem Smartphone.
2. Öffnen Sie die Applikation und verwenden Sie zum Erstellen des Kontos den folgenden Code.
GVHT MRSH O5ZT M4TQ MQ3D KM3O MJKH MY2N
[Hier den QR-Code scannen?](#)
3. Verwenden Sie beim Erstellen folgende Konfigurationswerte, falls sie benötigt werden.

Typ	zeitbasiert (time-based) (TOTP)
Algorithmus	HmacSHA1
Ziffern	6
Intervall	30
4. Geben Sie den von der Applikation generierten **One-time Code** ein und klicken Sie auf Absenden.

One-time code *

Gerätename

Absenden

- 1.4.7. Sofern Sie die Punkte 1.4.2 bis 1.4.6 angewendet haben, können Sie den folgenden Punkt 1.5 überspringen.

- 1.5. Auf Ihrem Smartphone wird in der Authenticator-Applikation nach dem Scannen des QR-Codes ein One-time code ausgegeben, welchen Sie in das Feld «One-time code *» übertragen. Das Feld «Gerätename» muss nicht ausgefüllt werden. Schliessen Sie die Eingabe mit dem «Absenden» Button ab.

Authentifizierung einrichten

 Sie müssen eine Mobile Authentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie **FreeOTP** oder **Google Authenticator** auf Ihrem Smartphone.

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



[Code manuell eingeben?](#)

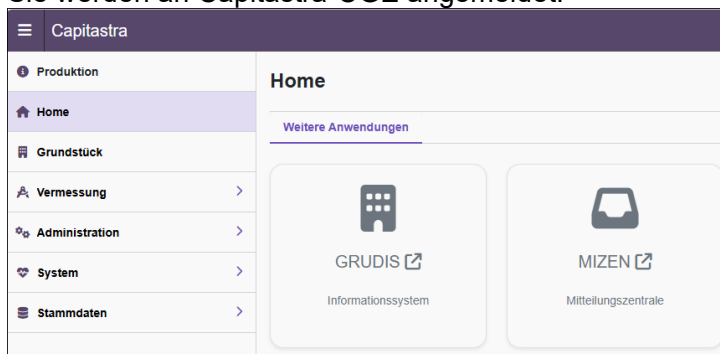
3. Geben Sie den von der Applikation generierten **One-time Code** ein und klicken Sie auf Absenden.

One-time code *

Gerätename

Absenden

1.6. Sie werden an Capitastra-CGE angemeldet.

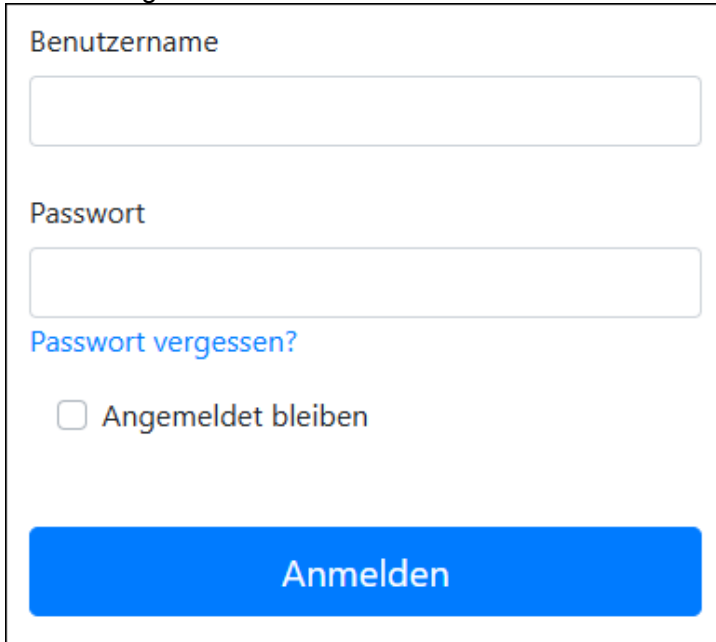


1.7. Bei Problemen wenden Sie sich an gruda@be.ch.

2. Anwenden der Zwei-Faktor-Authentifizierung (2FA) für Capitastra-CGE

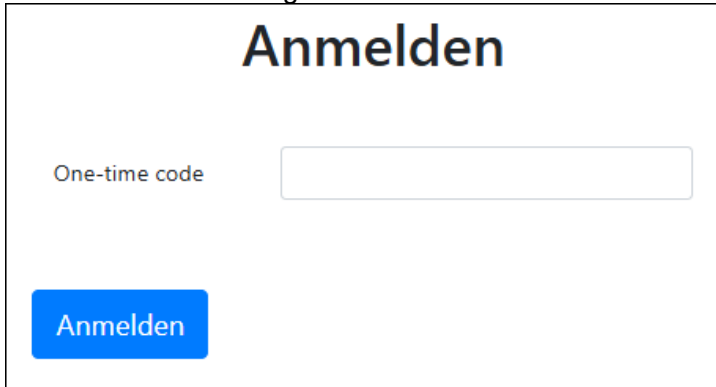
2.1. Starten Sie Capitastra-CGE (Link siehe [Handbuch GRUDA-AV](#)).

2.2. Geben Sie ihren **vierstelligen** Benutzernamen, z.B. **mabc** und das Passwort ein und bestätigen Sie die Eingabe mit dem «Anmelden» Button.



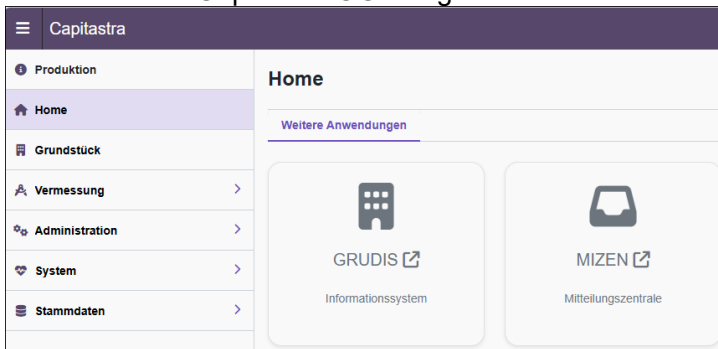
The login form is enclosed in a black border. It contains the following elements from top to bottom: a label 'Benutzername' above a text input field; a label 'Passwort' above a text input field; a blue link 'Passwort vergessen?'; a checkbox labeled 'Angemeldet bleiben'; and a large blue button with the white text 'Anmelden'.

2.3. Starten Sie auf Ihrem Smartphone die Authenticator-Applikation, welche Sie unter dem [Punkt 1.3](#) installiert haben und geben Sie den One-time code im Feld «One-time code» ein und schliessen Sie die Eingabe mit dem «Anmelden» Button ab.



The screen has a black border and a large title 'Anmelden' at the top. Below the title is a label 'One-time code' next to a text input field. At the bottom left is a blue button with the white text 'Anmelden'.

2.4. Sie werden an Capitastra-CGE angemeldet.



The screenshot shows the Capitastra application interface. On the left is a dark purple sidebar with a menu containing 'Produktion', 'Home' (highlighted), 'Grundstück', 'Vermessung', 'Administration', 'System', and 'Stammdaten'. The main area has a title 'Home' and a section 'Weitere Anwendungen' with two tiles: 'GRUDIS Informationssystem' and 'MIZEN Mitteilungszentrale'.

2.5. Bei Problemen wenden Sie sich an gruda@be.ch.