

Zwei-Faktor-Authentifizierung nutzen

Inhaltsverzeichnis

- [Was ist eine Zwei-Faktor-Authentifizierung?](#)
- [Zwei-Faktor-Authentifizierung aktivieren](#)
- [Der erste Login mit Zwei-Faktor-Authentifizierung](#)
- [Ein paar abschließende Hinweise](#)

Passende Videos

Inhalt nach Stichwort

Es ist kein Inhalt mit den angegebenen Stichworten vorhanden

Ähnliche Artikel

- [Zwei-Faktor-Authentifizierung nutzen](#)

Was ist eine Zwei-Faktor-Authentifizierung?



Es gibt diverse Formen der Zwei-Faktor-Authentifizierung. Diese Beschreibung bezieht sich ausschließlich auf die von Nextcloud genutzte Form.

Überall dort wo Sie sich mit einem Benutzernamen und einem Passwort anmelden, gibt es ein Problem: Sobald Ihr Passwort in fremde Hände gelangt ist Ihr entsprechender Account nicht mehr sicher. Alles was mit diesem Account machbar ist, kann auch von dieser fremden Person durchgeführt werden. Verlieren Sie bspw. Ihr Passwort für Ihr Amazon-Konto, so kann jemand auf Ihre Kosten einkaufen. Ähnlich ist es auch bei Nextcloud. Mit dem Verlust Ihres Passworts sind Ihre Dateien nicht länger Ihre Dateien.

In den letzten Jahren hat sich daher zunehmend die sogenannte Zwei-Faktor-Authentifizierung verbreitet. Dabei wird zusätzlich zum üblichen ersten Faktor – Ihr Passwort – ein zweiter Faktor bei der Anmeldung abgefragt. Nextcloud verwendet als zweiten Faktor einen **sechs-stelliger numerischen Code**. Im Gegensatz zu Ihrem Passwort wird dieser Code **automatisch generiert**. Jeder Code wird dabei in relativ **kurzen Zeitabständen** neu generiert und der vorherige Code wird ungültig.

Aber warum ist das jetzt sicherer als ohne? Ganz einfach. Eine fremde Person kann selbst dann nichts mit einem Code anfangen, wenn Sie diesen irgendwo angeben – den dieser ändert sich wenige Sekunden später und ist damit **unbrauchbar**. Und ohne den Code ist auch das Passwort nutzlos.

Es stellt sich nun natürlich die Frage wie Sie selbst an den automatisch generierten Code mit kurzer Lebensdauer kommen. Auch hierfür gibt es eine einfache Antwort. Ihr **Smartphone dient als Code-Generator**. Mit Hilfe sogenannter TOTP-Apps können Sie auf Ihrem Smartphone einen Code-Generator installieren, welche für die Zwei-Faktor-Authentifizierung eingesetzt werden kann und mit Nextcloud funktioniert. Wir empfehlen hierfür die [Google Authenticator App](#).



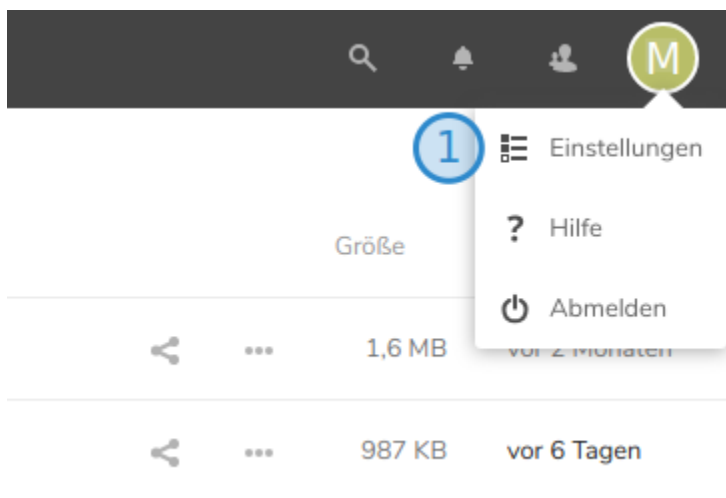
Für die, die es interessiert...

TOTP steht für "Time-based One-time Password". Frei übersetzt generieren TOTP-Apps also zeitlich begrenzte Wegwerf-Passwörter. Und das ist auch der Grund, wieso diese deutlich sicherer sind, als normale Kennwörter. Und das auch nur in Kombination mit Ihrem "normalen" Passwort.

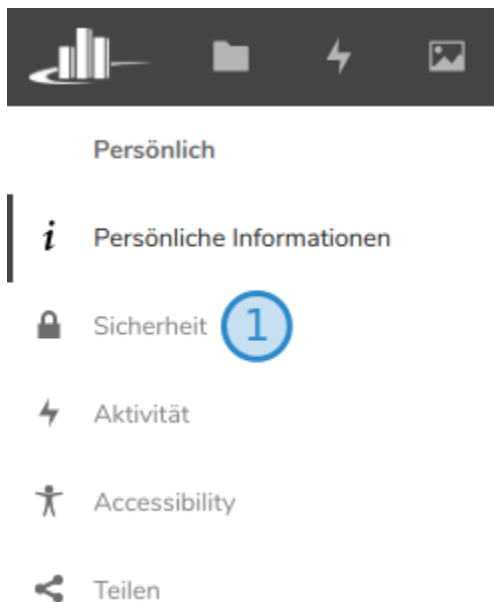
Zusätzlich ist wichtig zu beachten, dass die Zwei-Faktor-Authentifizierung nur über die Weboberfläche aktiv ist. Verwenden Sie bspw. eine der Apps für Ihr Smartphone oder den [Desktop-Client](#), so greift die Zwei-Faktor-Authentifizierung hingegen nur bei der ersten Anmeldung. Danach ist keine Anmeldung mehr erforderlich.

Zwei-Faktor-Authentifizierung aktivieren

Melden Sie sich in Ihrem Browser in [Nextcloud](#) an und klicken Sie auf Ihr Profilbild (wenn Sie keins gesetzt haben, wird hier der erste Buchstabe Ihres Namen angezeigt). Es öffnet sich ein Dropdown-Menü. Öffnen Sie Ihre Einstellungen indem Sie auf "Einstellungen" (Markierung 1) klicken.



Nachdem die neue Ansicht geladen wurde, sehen Sie am linken Rand des Browsers ein weiteres Menü. Klicken Sie auf den Menüpunkt "Sicherheit" (Markierung 1).



Ihre Sicherheitseinstellungen werden nun geöffnet. Sie finden in dieser Ansicht den Punkt "TOTP aktivieren" (Markierung 1). Hinter dieser Option verbirgt sich die Zwei-Faktor-Authentifizierung. Klicken Sie auf das Kontrollkästchen um diese zu aktivieren.

Persönlich

i

Persönliche Informationen

🔒

Sicherheit

⚡

Aktivität

♿

Accessibility

🔗

Teilen

Geräte & Sitzungen

Aktuell in Ihrem Konto angemeldete Web-, Desktop- und Mobil-Clients.

| Gerät | Letzte Aktivität |
|--|------------------|
| <div><div>🖥️</div><div>Diese Sitzung</div></div> <div><div>App-Name</div><div>Neues App-Passwort erstellen</div></div> | vor einer Minute |

Zwei-Faktor-Authentifizierung

🔒

Backup-Code

Backup-Codes wurden erzeugt. 0 von 10 Codes wurden benutzt.

Backup-Codes erneuern

Wenn Sie die Backup-Codes erneuern, werden die alten Codes automatisch ungültig.

📱

TOTP (Authenticator app)

1

☐ TOTP aktivieren

Ihre Anzeige sollte sich nun wie in der folgenden Abbildung verändert haben. Den angezeigten QR-Code (Markierung 1) benötigen Sie im nächsten Schritt. Also schließen Sie den Browser nicht.

Persönlich

Persönliche Informationen

Sicherheit

Aktivität

Accessibility

Teilen

Diese Sitzung

vor einer Minute

App-Name

Neues App-Passwort erstellen

Zwei-Faktor-Authentifizierung

Backup-Code

Backup-Codes wurden erzeugt. 0 von 10 Codes wurden benutzt.

Backup-Codes erneuern


Wenn Sie die Backup-Codes erneuern, werden die alten Codes automatisch ungültig.

TOTP (Authenticator app)

☐ TOTP aktivieren

Ihr neuer TOTP-Schlüssel ist:

Für eine schnelle Konfiguration, QR-Code mit der TOTP-App scannen:



1

Nachdem Sie die App konfiguriert haben, geben Sie unten einen Testcode ein, um sicherzustellen, dass alles funktioniert:

Authentifizierungscode

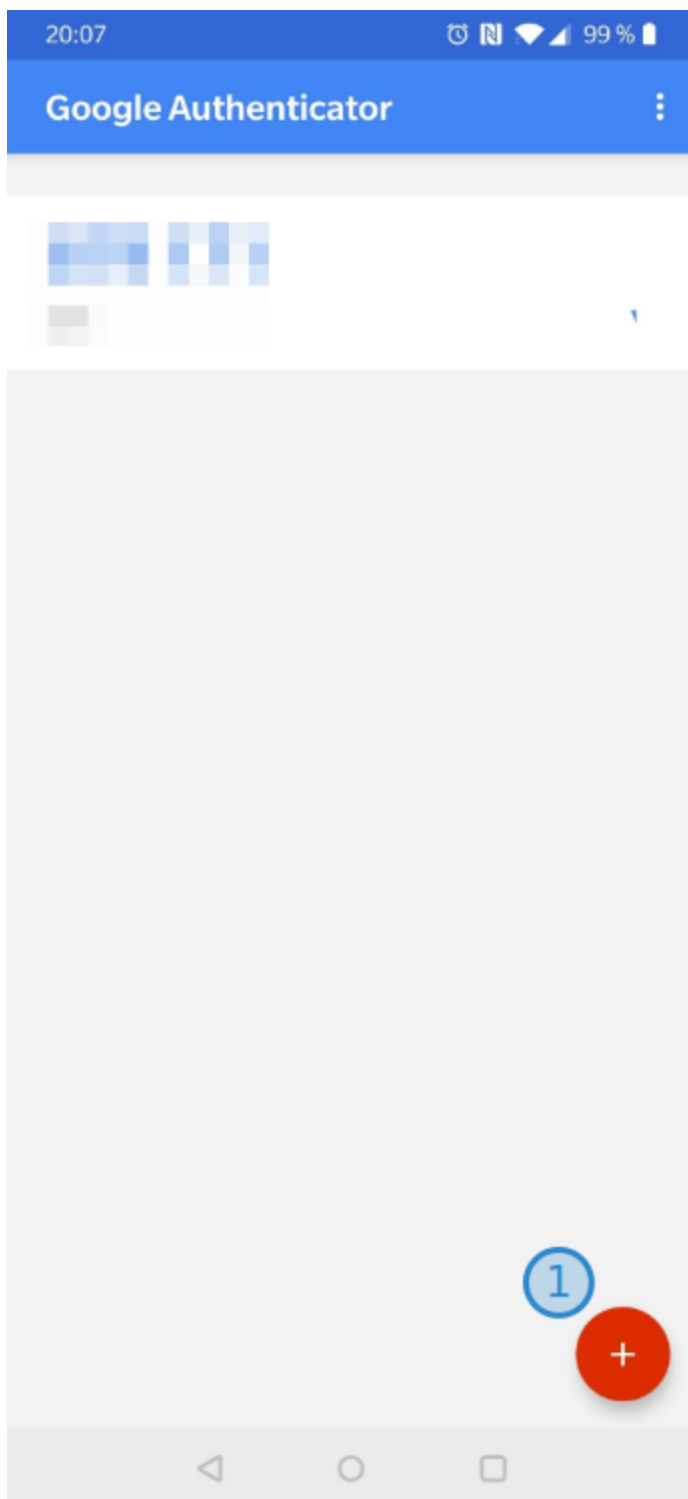
Überprüfen

Wechseln Sie zu Ihrem Smartphone. Sie benötigen eine TOTP App um den zweiten Faktor einzurichten. Bei Android können Sie bspw. die [Google Authenticator App](#) oder die [FreeOTP+](#) App aus dem Play Store installieren. Bei Apple können Sie zum Beispiel die App [OTP Auth](#) aus dem App Store laden. Wir zeigen die Einrichtung hier am Beispiel der Google Authenticator App.

Nach erfolgreicher Installation öffnen Sie diese. Sie sollten nun die folgende Ansicht sehen. Klicken Sie auf den roten Button mit dem Plus-Zeichen (Markierung 1).

Gibt es auch Alternativen zur Google Authenticator App?

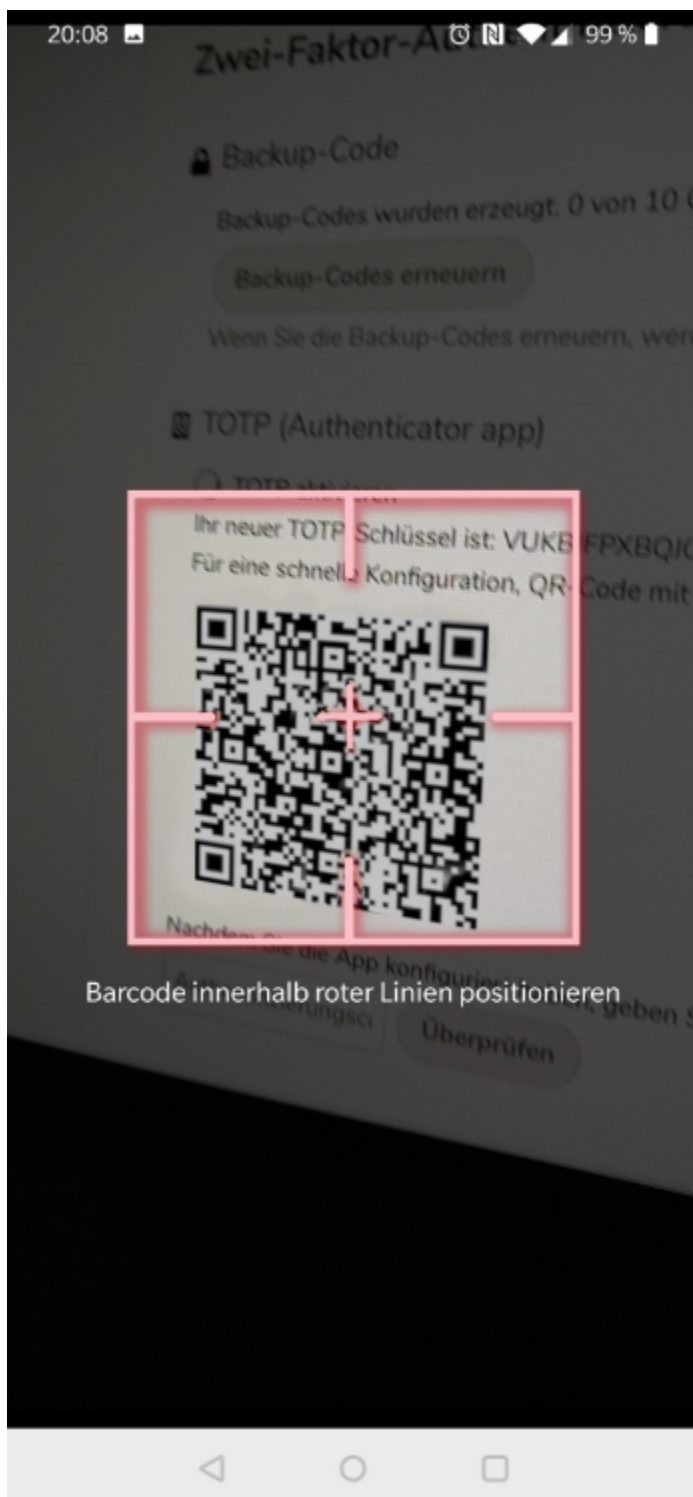
Ja, es gibt diverse Alternativen. Suchen Sie einfach im Play Store nach "TOTP" und installiere Sie die für Sie passende App.



Im sich öffnenden Menü sehen Sie zwei Option. Wählen Sie "Barcode scannen" (Markierung 1).

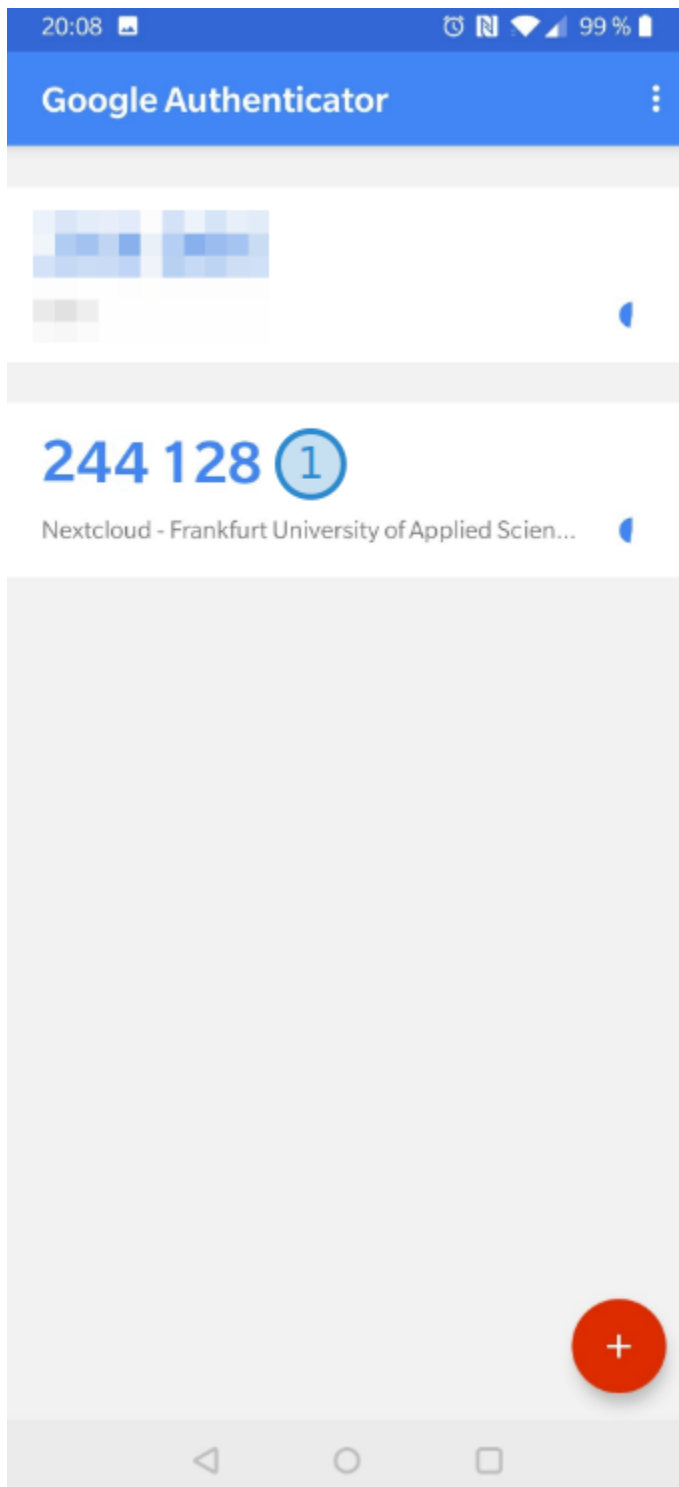


Ihnen wird nun der Barcode-Scanner angezeigt. Halten Sie die Kamera Ihres Smartphones über den QR-Code, welcher noch Ihrem Browser in Nextcloud angezeigt wird. Der Code muss sich im rosa Rechteck befinden. Warten Sie bis der QR-Code gescannt wurde und sich der Scanner schließt.



Barcode innerhalb roter Linien positionieren

Sie gelangen zurück zu Übersicht der Google Authenticator App. Ab sofort wird Ihnen hier immer der aktuellste Code zur Anmeldung an Nextcloud angezeigt (Markierung 1).



Lassen Sie Ihre Smartphone aktiv und wechseln Sie zu Ihrem Browser und Nextcloud zurück. Geben Sie im Textfeld (Markierung 1) unterhalb des QR-Codes den in der Google Authenticator App angezeigten Code ein. Klicken Sie auf "Überprüfen" (Markierung 2). Der QR-Code wird daraufhin ausgeblendet und die Aktivierung der Zwei-Faktor-Authentifizierung ist abgeschlossen. Ab der nächsten Anmeldung an der Weboberfläche von Nextcloud werden Sie ab sofort nach dem Code, welchen Sie in der Google Authenticator App finden, gefragt.

Persönlich

i

Persönliche Informationen

🔒

Sicherheit

⚡

Aktivität

♿

Accessibility

🔗

Teilen

Diese Sitzung

App-Name

Neues App-Passwort erstellen

vor einer Minute

Zwei-Faktor-Authentifizierung

🔒 Backup-Code

Backup-Codes wurden erzeugt. 0 von 10 Codes wurden benutzt.

Backup-Codes erneuern

Wenn Sie die Backup-Codes erneuern, werden die alten Codes automatisch ungültig.

📱 TOTP (Authenticator app)

☐ TOTP aktivieren

Ihr neuer TOTP-Schlüssel ist:

Für eine schnelle Konfiguration, QR-Code mit der TOTP-App scannen:

Nachdem Sie die App konfiguriert haben, geben Sie unten einen Testcode ein, um sicherzustellen, dass alles funktioniert:

1

244128

Überprüfen

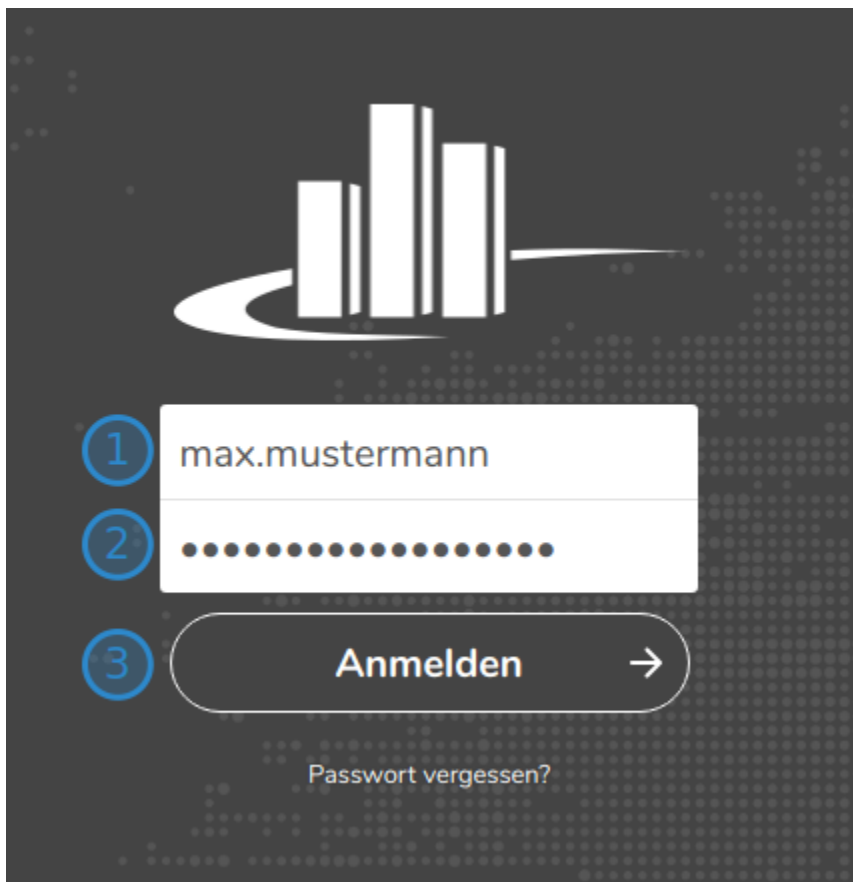
2

Der erste Login mit Zwei-Faktor-Authentifizierung



Fall Sie bereits wissen, wie der Login mit Zwei-Faktor-Authentifizierung funktioniert, können Sie diese Teil überspringen.

Melden Sie sich von Nextcloud ab (es kann eine Weile dauern bis Nextcloud die Abmeldung durchgeführt hat). Die Loginseite erscheint. Geben Sie wie gewohnt Ihren Benutzernamen (Markierung 1) und Ihr Passwort (Markierung 2) ein. Klicken Sie auf "Anmelden" (Markierung 3).



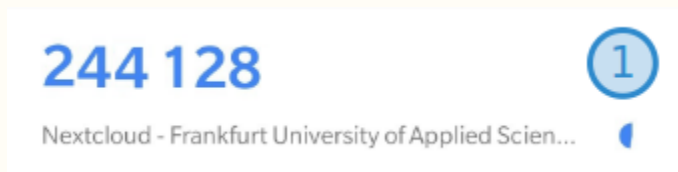
Ohne die Zwei-Faktor-Authentifizierung würden Sie nun direkt auf die Startseite von Nextcloud gelangen. Da Sie diese nun allerdings aktiviert haben, sehen Sie ab sofort bei jeder Anmeldung die folgende Ansicht. Geben Sie im Textfeld (Markierung 1) den aktuellen Code aus der Google Authenticator App ein und klicken anschließend auf "Übermitteln" (Markierung 2).



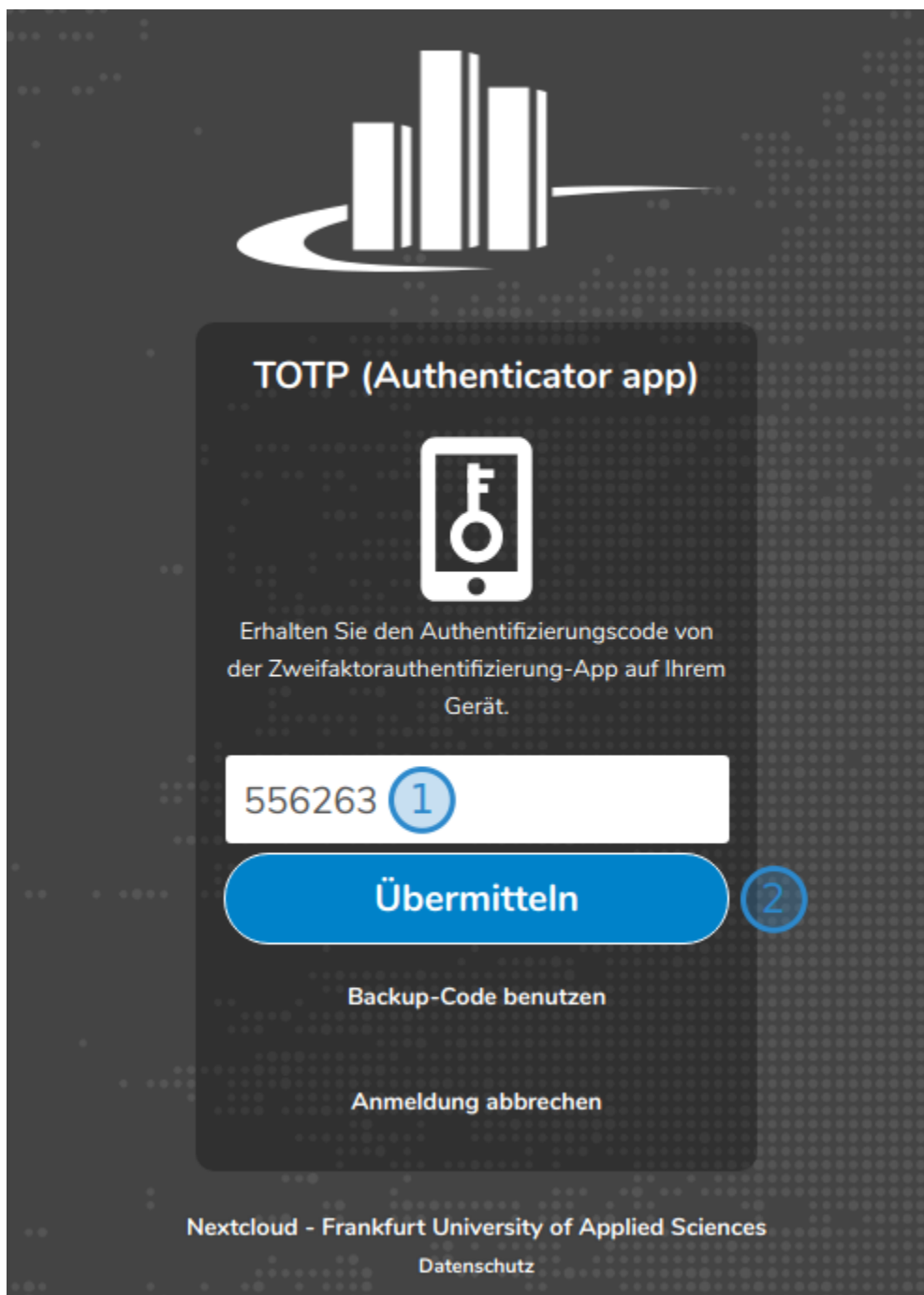
Es funktioniert einfach nicht! Warum?

Keine Panik. Sie haben den Code vermutlich nicht in der erforderlichen Zeitspanne eingegeben. Wie Sie aus der Einleitung wissen, ist jeder Code nur einen begrenzten Zeitraum gültig. Danach müssen Sie den jeweils neuen eingeben.

Wann ein Code abläuft, erkennen Sie in der Google Authenticator App. Rechts neben Ihrem Code finden Sie einen kleinen Kreis (Markierung 1), welcher mit zunehmender Zeit verschwindet. Ist er komplett verschwunden wird ein neuer Code generiert und der alte ist ungültig.



Herzlichen Glückwunsch! Sie haben sich das erste Mal mit Zwei-Faktor-Authentifizierung angemeldet.



Ein paar abschließende Hinweise

Wie eingangs bereits erwähnt ist die Zwei-Faktor-Authentifizierung primär für die Weboberfläche notwendig bzw. aktiv. Sowohl der Desktop-Client als auch die Smartphone-Apps für Android und iPhone benötigen den zweiten Faktor ausschließlich zur erstmaligen Anmeldung. Erwähnenswert ist zusätzlich, dass bspw. der Desktop-Client Sie dazu auffordert sogenannte Backup-Code zu erzeugen. Das ist ein normales Verhalten. Mehr dazu erfahren Sie [hier](#).