

# Sichern Sie Ihre Daten mit der Zwei-Faktor-Authentifizierung



**Erhöhen Sie die Sicherheit Ihrer Daten, indem Sie die Zwei-Faktor-Authentifizierung (2FA) aktivieren. Ist diese aktiviert, werden Sie jedes Mal aufgefordert, nach der Angabe des Master-Kennwortes einen weiteren, einzigartigen Sicherheits-Code einzugeben, wenn Sie Ihre Datenbank freigeben möchten.**

## Was ist die Zwei-Faktor-Authentifizierung?

Die Zwei-Faktor-Authentifizierung (2FA) ist die Verwendung von 2 Informationsbestandteilen zur Authentifizierung – jeder Bestandteil kommt hierbei aus einer eigenständigen Quelle. Die Notwendigkeit zusätzlicher Komponenten für einen erfolgreichen Zugriff erhöht die Sicherheit, da die Wahrscheinlichkeit, dass mehrere voneinander unabhängige Quellen zur selben Zeit gehackt oder ausgespäht wurden, geringer ist.

In der Praxis bedeutet dies, dass Ihr Account sicherer ist als zuvor. Selbst wenn ein Hacker es schaffen sollte Zugriff auf Ihr Master-Kennwort zu erlangen, ist es unwahrscheinlich, dass dieser auch physischen Zugriff auf Ihr Smartphone erlangt, welches Sie für die 2FA nutzen.

## Voraussetzungen für die Nutzung

- **Es ist erforderlich, dass Sie die [aktuell verfügbare Version](#) von Sticky Password auf jedem Gerät installiert haben**, das mit Ihrem StickyAccount verbunden ist. Geräte mit einer älteren Version von Sticky Password können die Datenbank, welche per 2FA gesichert wurde, nicht freigeben.
- **Die Erstaktivierung muss von Ihrem Desktop Gerät (Windows oder Mac) durchgeführt werden.** Einmal von Ihnen eingerichtet, wird die 2FA automatisch auf all Ihren anderen, autorisierten Geräten mit Sticky Password aktiviert (Windows, Mac, iOS und Android), sobald Sie diese das nächste Mal synchronisieren.
- **Es ist erforderlich, dass Sie [Google Authenticator \(GA\)](#) auf Ihrem Mobilgerät installieren**, um die 2FA zu ermöglichen. GA ist die App, welche die Codes generiert, die den zweiten Faktor zum Einloggen in Sticky Password darstellt. Sie können die App für [Android](#) und für [iOS](#) herunterladen.

*Wichtig: Sobald die 2FA aktiviert wurde, ist jedes Mal, wenn Sie Ihre Datenbank freigeben wollen, eine Internetverbindung vonnöten.*

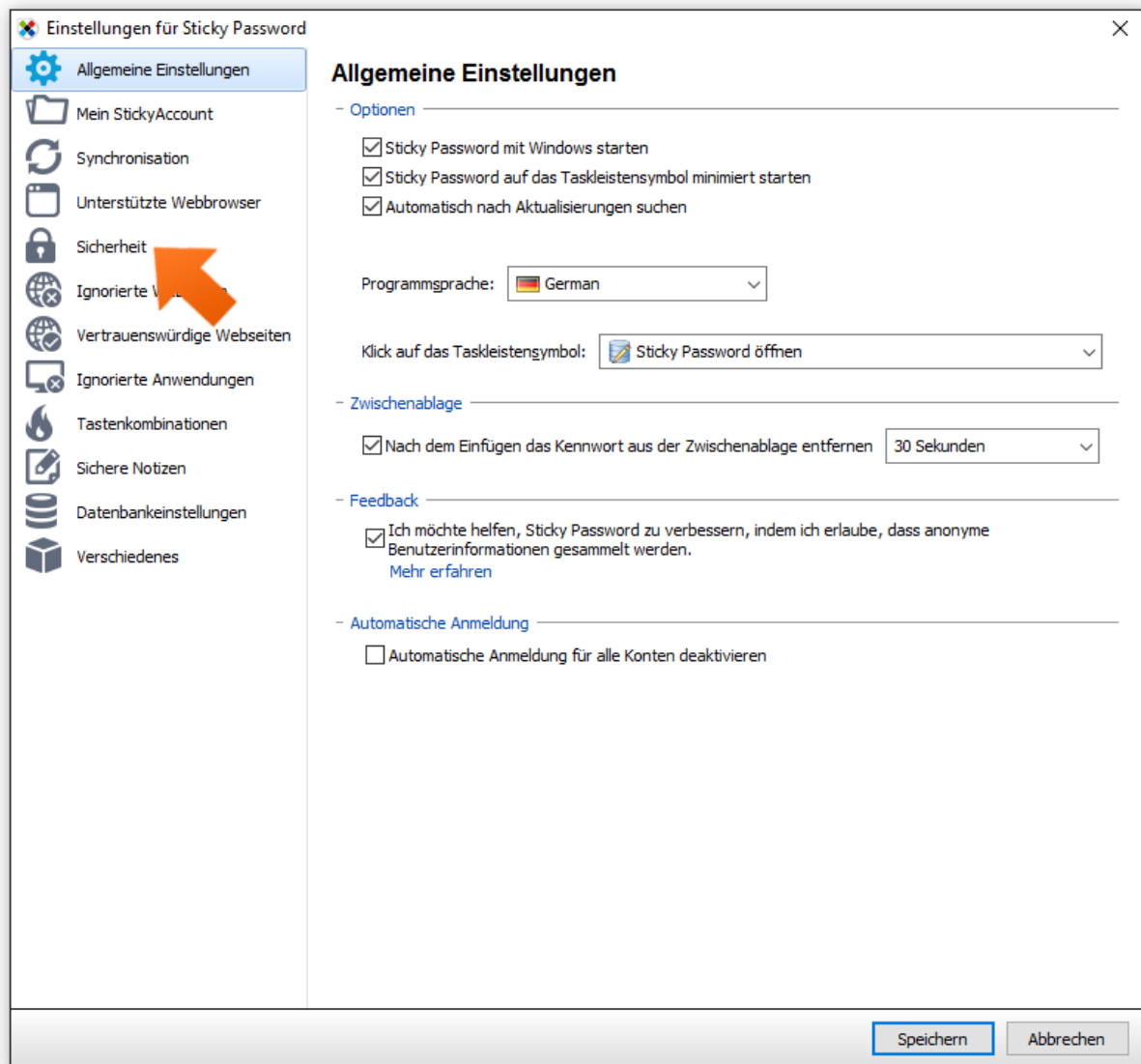
## Aktivierung der Zwei-Faktor-Authentifizierung

Sobald Sie die Google Authenticator App auf Ihrem Android oder iOS Gerät installiert haben und Sie die aktuell verfügbare Version von Sticky Password auf all Ihren Geräten installiert haben, führen Sie die folgenden Schritte durch:

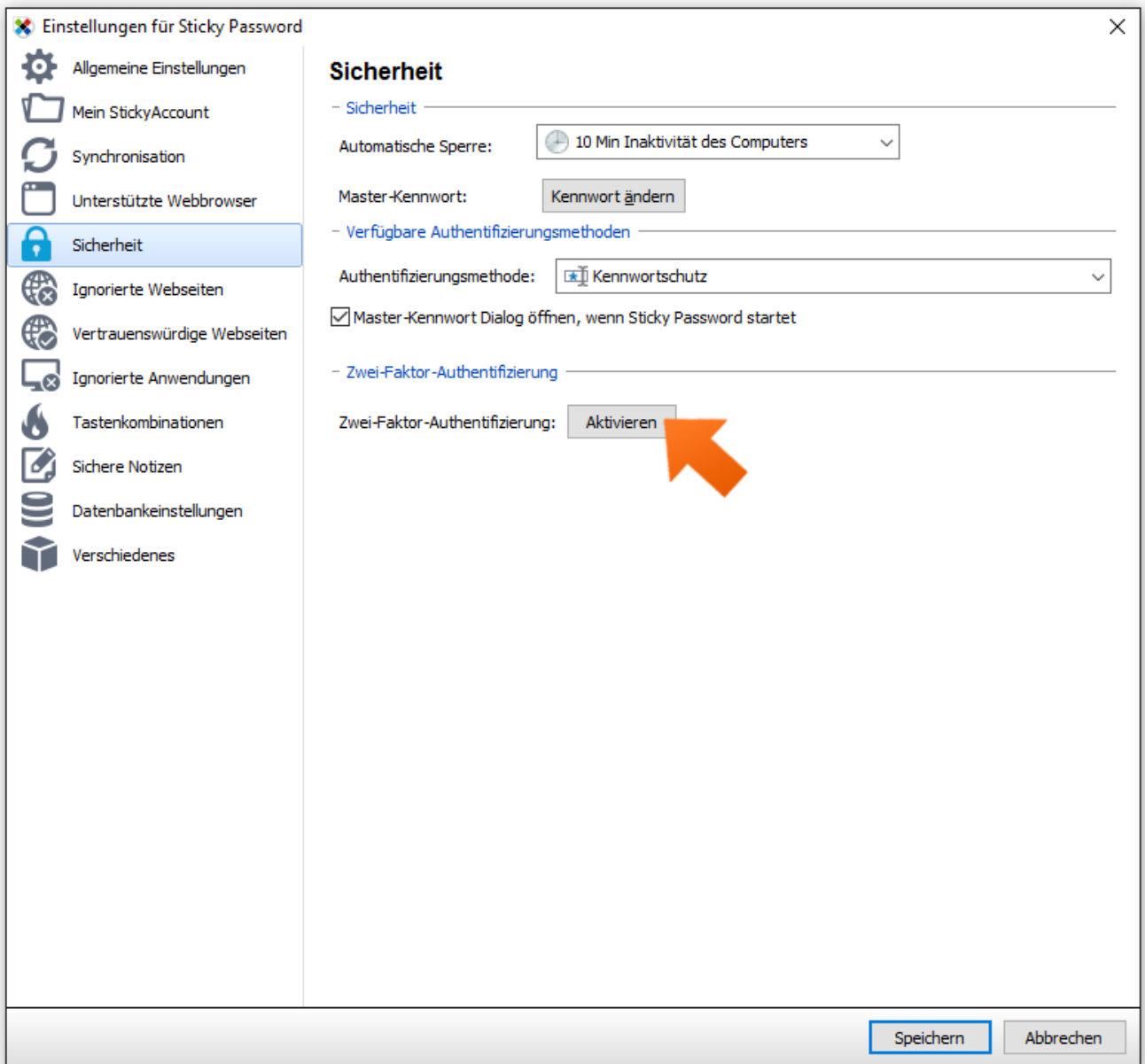
1. **Auf Ihrem PC** klicken Sie in der Programmoberfläche rechts oben auf *Menü* und wählen Sie *Einstellungen*.

**Auf Ihrem Mac** klicken Sie auf das Menü *Einstellungen*.

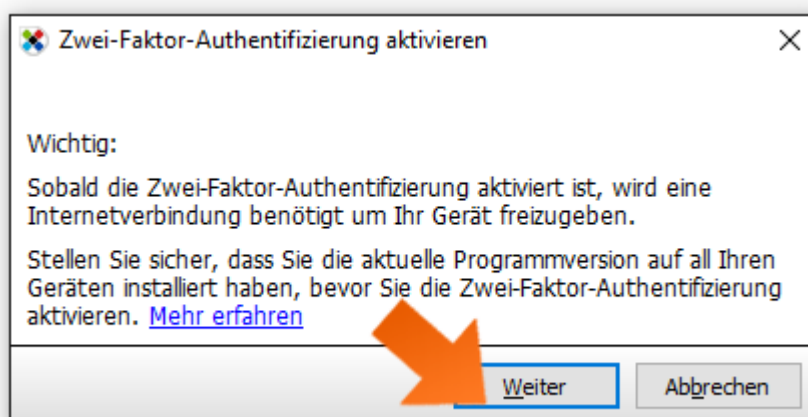
2. Wählen Sie den Reiter *Sicherheit*.



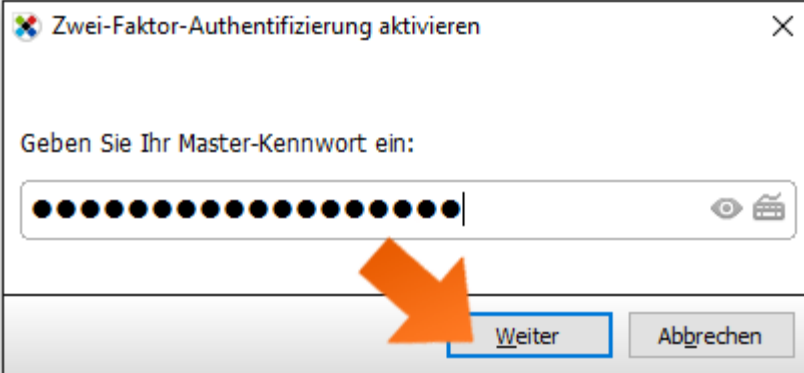
3. Klicken Sie im Bereich der Zwei-Faktor-Authentifizierung auf *Aktivieren*.



Nachdem Sie gelesen haben, dass bei aktivierter 2FA jedes Mal, wenn Sie Ihre Sticky Password Datenbank freigeben wollen, eine Internetverbindung vonnöten sein wird, klicken Sie *Weiter*.



4. Da dieser Schritt eine Änderung Ihrer Sicherheitseinstellungen bedeutet, werden Sie dazu aufgefordert Ihr Master-Kennwort einzugeben und anschließend auf *Weiter* zu klicken.



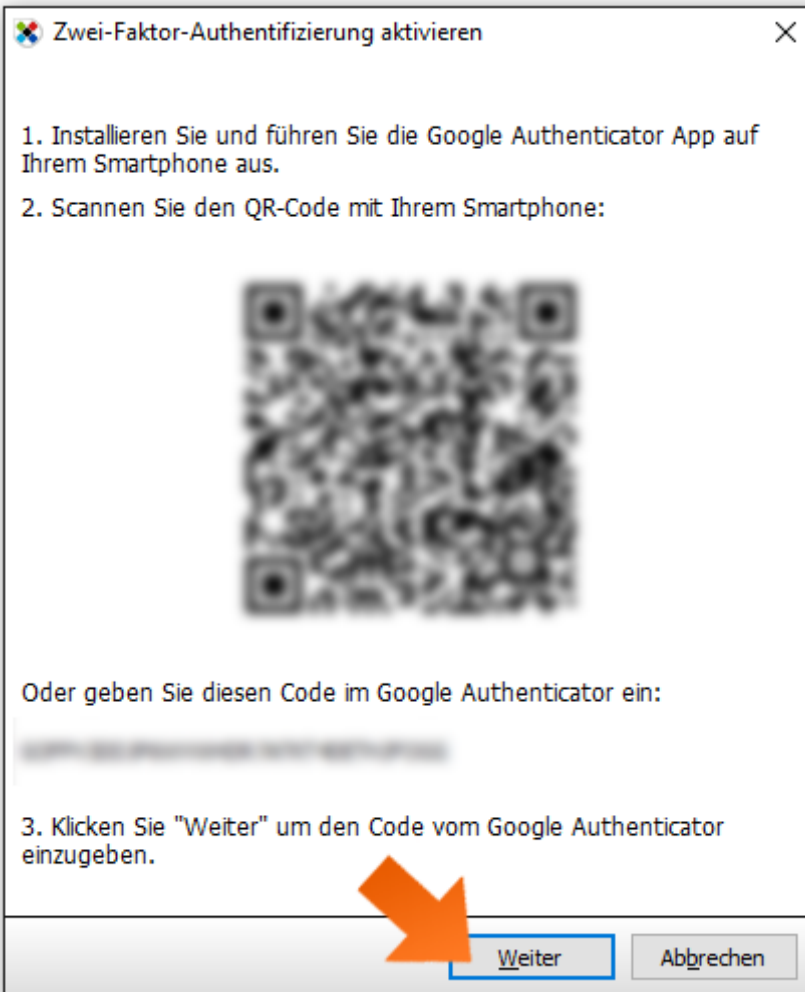
Zwei-Faktor-Authentifizierung aktivieren

Geben Sie Ihr Master-Kennwort ein:

••••••••••••

[Weiter](#) [Abbrechen](#)


5. Öffnen Sie nun die Google Authenticator App auf Ihrem Mobilgerät und scannen Sie den auf dem Bildschirm eingeblendeten QR Code ODER geben Sie den unten stehenden alphanummerischen Code manuell in die Google Authenticator App ein. Dieser Vorgang erstellt einen neuen GA Eintrag (GA Account), der mit Ihrem Sticky Password Account verknüpft wird. Dieser wird Ihnen ab diesem Zeitpunkt 6-stellige Codes generieren, die sich wiederum alle 30 Sekunden ändern. Klicken Sie auf *Weiter*.



Zwei-Faktor-Authentifizierung aktivieren

1. Installieren Sie und führen Sie die Google Authenticator App auf Ihrem Smartphone aus.

2. Scannen Sie den QR-Code mit Ihrem Smartphone:



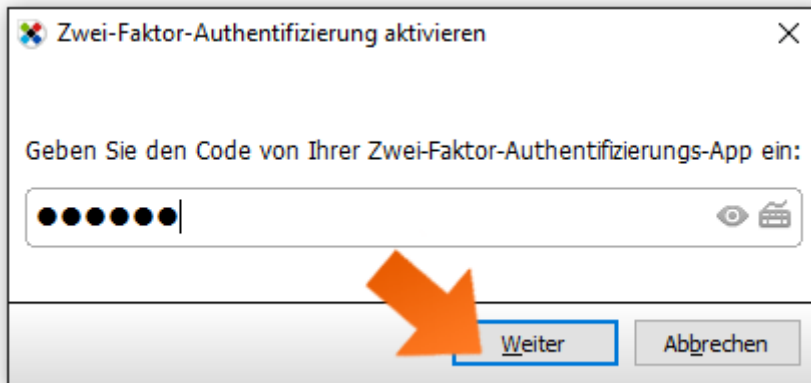
Oder geben Sie diesen Code im Google Authenticator ein:

XXXXXXXXXXXXXXXXXXXX

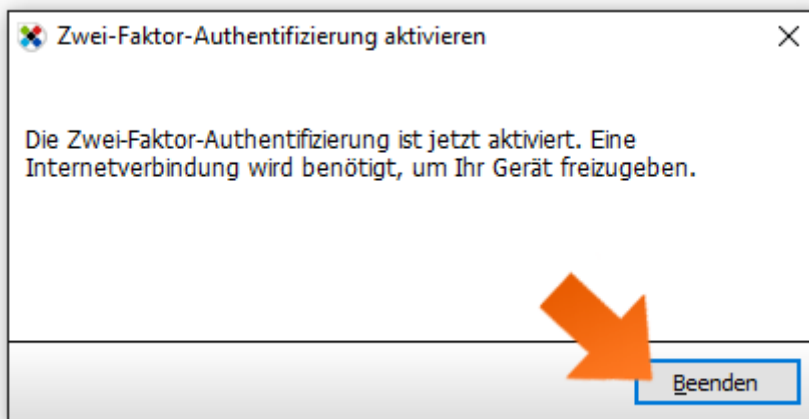
3. Klicken Sie "Weiter" um den Code vom Google Authenticator einzugeben.

[Weiter](#) [Abbrechen](#)

6. Geben Sie den 6-stelligen Code aus Ihrem Google Authenticator ein, sobald Sticky Password Sie dazu auffordert und klicken Sie auf *Weiter*. Dies bestätigt die Verknüpfung der Google Authenticator App auf Ihrem Gerät mit Ihrem Sticky Password Account.

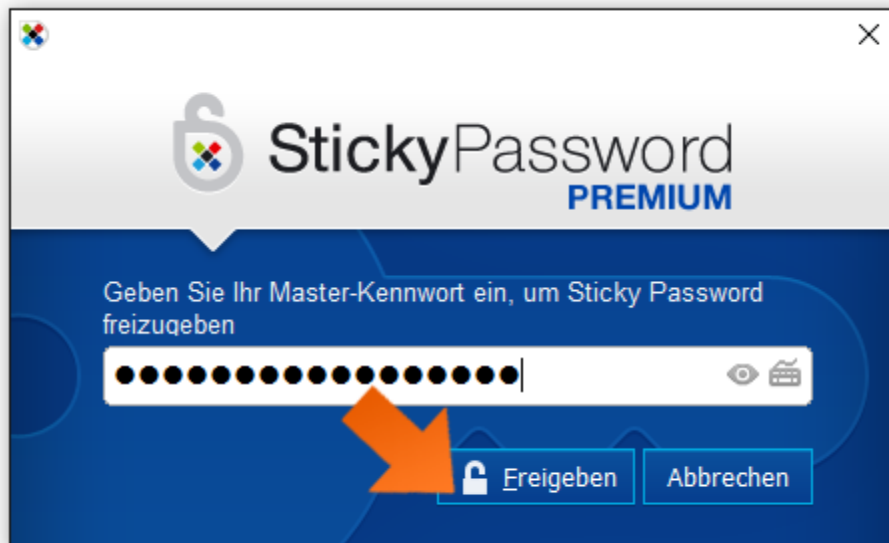


7. Wenn das Fenster mit der Bestätigung zur aktivierten 2FA erscheint, klicken Sie auf *Beenden*.

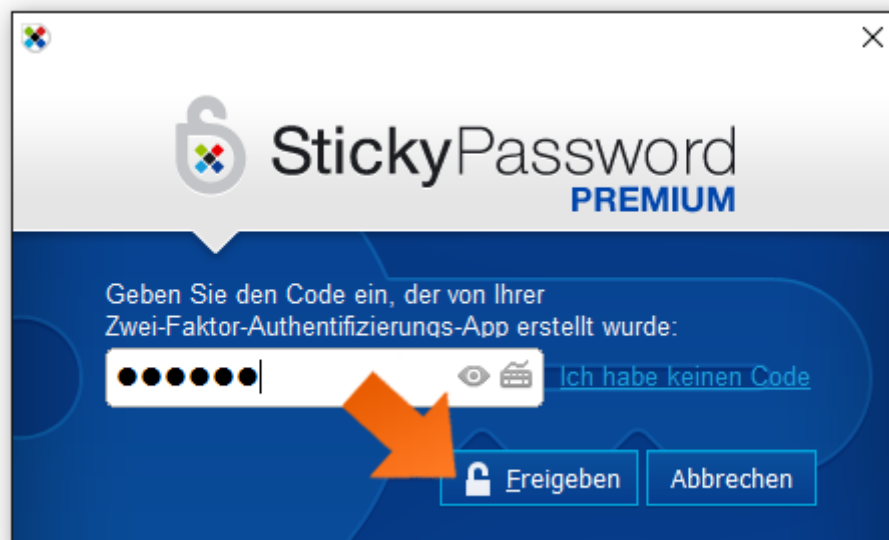


## Sticky Password freigeben, wenn 2FA aktiviert ist

1. Geben Sie wie gewohnt im Hauptdialog Ihr Master-Kennwort ein und klicken Sie auf *Freigeben*.



2. Öffnen Sie die Google Authenticator App auf Ihrem Gerät und geben Sie den dort angezeigten 6-stelligen Code in das Eingabefeld ein, sobald Sie dazu aufgefordert werden. Klicken Sie auf *Freigeben*.



## Was soll ich tun, wenn ich keinen Zugriff auf die Google Authenticator App habe, die mit meinem Sticky Password verknüpft ist?

Sollten Sie keinen Zugriff auf das Mobilgerät haben, auf der Ihre Google Authenticator App läuft (z.B. weil das Gerät verloren ging oder gestohlen wurde), können Sie die 2FA temporär umgehen, indem Sie Ihre E-Mail (StickyID) verwenden, um Sticky Password im Notfall freizugeben. Führen Sie hierzu die folgenden Schritte durch:

1. Klicken Sie auf den "Ich habe keinen Code" Link in dem Freigabedialog und eine spezielle PIN wird an Ihre StickyID E-Mail-Adresse gesandt (oder an Ihre in Ihrem StickyAccount festgelegte alternative E-Mail-Adresse).

*Wichtig: Aus Sicherheitsgründen ist diese spezielle PIN nur 20 Minuten gültig.*

2. Öffnen Sie Ihren Posteingang, kopieren Sie die PIN aus der E-Mail, die Ihnen zugesandt wurde und geben Sie sie im Freigabedialog ein. (Wenn Sie die E-Mail nicht in Ihrem Posteingang finden können, sehen Sie bitte auch im SPAM Ordner nach.)

**Wenn Sie Ihren Zugriff** auf das Gerät mit Ihrer Google Authenticator App **permanent verloren haben** (z.B. weil Sie dieses verloren oder Sie auf ein neues Gerät gewechselt haben), muss die 2FA für Ihren StickyAccount zunächst deaktiviert und anschließend mit Ihrem neuen Gerät reaktiviert werden.

## Deaktivierung der Zwei-Faktor-Authentifizierung

Die 2FA kann in dem installierten Sticky Password Programm auf Ihrem Windows Rechner im Menü unter *Einstellungen* oder auf Ihrem Mac unter Sticky Password *Einstellungen* deaktiviert werden.

1. **Auf Ihrem PC** wählen Sie *Menü* (rechts oben) und dort *Einstellungen*.  
**Auf Ihrem Mac** navigieren Sie unter Sticky Password zum Menü *Einstellungen*.
2. Wählen Sie den Reiter *Sicherheit*.
3. Klicken Sie im Bereich der Zwei-Faktor-Authentifizierung auf *Deaktivieren*.
4. Geben Sie Ihr Master-Kennwort ein und klicken Sie auf *Weiter*.
5. Geben Sie den aktuellen 6-stelligen Code von Ihrem Google Authenticator ein, wenn Sie von Sticky Password dazu aufgefordert werden und klicken Sie auf *Weiter*.
6. Die 2FA ist nun deaktiviert. Klicken Sie auf *Beenden*.

*Hinweis: Nachdem Sie die 2FA in Sticky Password deaktiviert haben, ist es nicht nötig, die Google Authenticator App auf Ihrem Mobiltelefon zu deinstallieren.*

## Wenn Sie die 2FA wieder reaktivieren möchten

erstellt die Google Authenticator App einen neuen GA Eintrag (GA Account) für Sticky Password, der:

- den vorherigen Eintrag überschreibt – dies gilt für Android Geräte
- einen neuen Eintrag anlegt – dies gilt für iOS Geräte. Um eine Verwechslung zu vermeiden, empfehlen wir den vorherigen Eintrag zu löschen, NACHDEM Sie die 2FA für Ihren Sticky Password Account deaktiviert haben und BEVOR Sie die 2FA reaktivieren.

Weitere Informationen zu Sticky Password finden Sie unter:  
<https://www.jakobsoftware.de/sticky-password>.

Stand: 10/2016

