Einrichtung der Zwei-Faktor-Authentifizierung (2FA) im dedicom Konto mit manueller Eingabe der Zeichenfolge

Larissa Wissler - 2025-12-19 - Login & ordering

Gültigkeit: Für alle Mitarbeitenden, deren Unternehmenssicherheitsrichtlinie eine Zwei-Faktor-Authentifizierung bei Drittanbietern vorschreibt.

Die Zwei-Faktor-Authentifizierung (2FA) bietet einen zusätzlichen Schutz für Ihr dedicom Benutzerkonto, indem neben dem Passwort ein zweiter Faktor – in der Regel ein zeitbasierter Einmalcode – abgefragt wird. Diese Maßnahme erhöht die Sicherheit Ihrer Daten und schützt vor unbefugtem Zugriff, insbesondere bei der Nutzung cloudbasierter Dienste.

Schritt-für-Schritt Anleitung zur Einrichtung manueller Eingabe der Zeichenfolge

Anmeldung im dedicom Konto

Besuchen Sie die Webseite https://service.dedicom.de/konto/login und melden Sie sich mit Ihren persönlichen Zugangsdaten an.

1. **Hinweis zur Umstellung auf das neue Loginverfahren**

Nach erfolgreicher Anmeldung erscheint ein Hinweisfenster, das über die verpflichtende Einführung der Zwei-Faktor-Authentifizierung informiert.

1. **Installation einer Authenticator-App**

Falls Sie noch keine Authenticator-App auf Ihrem Mobilgerät installiert haben, werden Ihnen direkt im Einrichtungsdialog zwei bewährte Optionen angeboten:

- Microsoft Authenticator
- Google Authenticator

Beide Apps sind kostenlos verfügbar und können über die jeweiligen App-Stores heruntergeladen werden.

1. **Verknüpfung des Kontos mit manueller Eingabe der Zeichenfolge**

Nach der Installation der Authenticator-App wird Ihnen im Schritt 2/4 ein QR-Code sowie eine rosa Zeichenfolge angezeigt. Diese Zeichenfolge dient als geheimer Schlüssel zur manuellen Einrichtung der Zwei-Faktor-Authentifizierung.

Öffnen Sie nun die Authenticator-App auf Ihrem Mobilgerät. Wenn Sie die **Microsoft Authenticator** verwenden, tippen Sie oben rechts auf das Pluszeichen („+“) und wählen die Kontoart **„Anderes“** aus. Anschließend entscheiden Sie sich für die Option **„Code manuell eingeben“**. In das Feld **„Geheimer Schlüssel“** tragen Sie die rosa Zeichenfolge ein, die Ihnen unter dem QR-Code angezeigt wurde. Als Kontoname können Sie beispielsweise **„dedicom Konto“** eingeben.

Falls Sie stattdessen den **Google Authenticator** nutzen, wählen Sie zunächst **„Code hinzufügen“** und anschließend **„Einrichtungsschlüssel eingeben“**. In das Feld **„Mein Schlüssel“** geben Sie ebenfalls die rosa

Zeichenfolge ein. Achten Sie darauf, als Schlüsseltyp **„Zeitbasiert“** auszuwählen. Auch hier können Sie als Kontoname **„dedicom Konto“** verwenden.

1. **Bestätigung der Einrichtung**

Im nächsten Schritt 3/4 geben Sie Ihr dedicom Passwort sowie den aktuellen Code aus der Authenticator-App ein. Dies dient der Verifizierung und Aktivierung der Zwei-Faktor-Authentifizierung.

Falls der Einrichtungsprozess unterbrochen wurde, muss der QR-Code erneut eingescannt werden. Der vorherige Code sowie der dazugehörige Eintrag in Ihrer Authenticator-App sind nicht mehr gültig.

Bitte löschen Sie den alten Eintrag in Ihrer App, um Verwechslungen zu vermeiden.

1. **Herunterladen von Wiederherstellungscodes**

Sie erhalten bei Schritt 4/4 die Möglichkeit, sogenannte Reset-Codes herunterzuladen. Diese dienen als Backup, falls Sie Ihr Mobilgerät verlieren oder keinen Zugriff auf die Authenticator-App haben.

Sicherheitsbestätigung

Vor Abschluss der Einrichtung müssen Sie den folgenden Hinweis bestätigen:

„Mir ist bekannt, dass ich im Falle eines Handyverlusts ohne Wiederherstellungscode nicht mehr auf das Konto zugreifen kann.“

1. **Abschluss der Einrichtung**

Nach erfolgreicher Bestätigung ist die Zwei-Faktor-Authentifizierung aktiviert und Sie gelangen wie gewohnt in Ihr dedicom Konto.

Änderung der Authentifizierung bei Gerätewechsel

Sollten Sie Ihr Mobilgerät wechseln, können Sie die Zwei-Faktor-Authentifizierung unter dem Menüpunkt „Meine Daten“ neu konfigurieren. Der Einrichtungsprozess wird dabei erneut durchlaufen, inklusive QR-Code-Scan und Sicherheitsbestätigung.

Hinweise zur Sicherheit

- Die Verwendung der Zwei-Faktor-Authentifizierung ist verpflichtend, sofern Ihre Unternehmensrichtlinie dies vorsieht.
- Bewahren Sie Ihre Wiederherstellungscodes sicher und getrennt vom Mobilgerät auf.
- Bei Fragen oder Problemen mit der App, wenden Sie sich an den Support des Anbieters:

Google Authenticator – Supportseite

Die Google-Hilfeseite bietet eine umfassende Anleitung zur Einrichtung, Nutzung und Wiederherstellung der App:

https://support.google.com/accounts/answer/1066447?hl=de

Microsoft Authenticator – Supportseite

Microsoft stellt eine detaillierte Anleitung zur Verfügung, wie Sie die App installieren, einrichten und mit Konten verknüpfen:

https://support.microsoft.com/de-de/account-billing/herunterladen-und-installieren-von-microsoft-authenticator-5b7c2b8a-4c50-4f6e-8a3d-2a56d3f5d8fa