

Anleitung: 2FA im PraxisPortal

Inhaltsverzeichnis

Was bedeutet 2FA?	3
Wie 2FA im Allgemeinen funktioniert	3
Warum ist ein 2FA Verfahren wichtig?	3
Welche 2FA-Verfahren werden vom PraxisPortal künftig unterstützt?	4
Was sind die Vor- und Nachteile der unterschiedlichen 2FA Verfahren?.....	4
Muss ich unbedingt 2FA bei meinem Benutzer aktivieren?	5
Was ändert sich durch die Einführung der 2FA im PraxisPortal?	6
Einrichtung der Zwei-Faktor-Authentifizierung (2FA).....	6
2FA per E-Mail-Code einrichten.....	6
2FA mit einer Authenticator-App einrichten.....	7
Einrichtung zunächst überspringen.....	8
2FA zu einem späteren Zeitpunkt einrichten.....	8
Mehrere 2FA-Methoden nutzen	9
Wie oft muss 2. Faktor eingegeben werden?	10
Muss ich zukünftig trotz aktivierter Zwei-Faktor-Authentifizierung (2FA) mein Passwort regelmäßig ändern?	11
Wird der Einreichen-Prozess aus der PVS für die Aktivierung der 2FA aufgehalten?.....	11
Was bedeutet das für Sie als Praxis?	11
Haben Sie Fragen?.....	12

Was bedeutet 2FA?

2FA steht für **Zwei-Faktor-Authentisierung** (häufig auch Zwei-Faktor-Authentifizierung genannt).

Es ist ein Sicherheitsverfahren, das Ihre Identität durch zwei unabhängige Faktoren bestätigt, anstatt sich nur auf ein Passwort zu verlassen.

Dies erhöht die Sicherheit erheblich, da ein Angreifer selbst bei Kenntnis des Passworts keinen Zugriff erhält, wenn er nicht auch den zweiten Faktor besitzt.

Wie 2FA im Allgemeinen funktioniert

- **Erster Faktor (etwas, das Sie wissen):** Meist ist dies das Passwort, das Sie kennen.
- **Zweiter Faktor (etwas, das Sie besitzen oder sind):** Dies kann im Allgemeinen eine der folgenden Methoden sein:
 - **Besitzfaktor:** Ein Code, der an Ihr Mailpostfach (E-Mail) oder an Ihr Smartphone (SMS) gesendet wird.
 - **Besitzfaktor:** Ein Code, der von einer Authenticator-App generiert wird.
 - **Besitzfaktor:** Ein TAN-Generator oder eine Chipkarte.
 - **Inhärent/Biometrisch:** Ein Fingerabdruck oder Gesichtsscan.

Weitere Informationen sind beispielsweise unter den folgenden Links zu finden:

- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html
- <https://de.wikipedia.org/wiki/Zwei-Faktor-Authentisierung>

Warum ist ein 2FA Verfahren wichtig?

Zwei-Faktor-Authentisierung (2FA) ist wichtig, weil sie ein **passwortbasiertes Sicherheitssystem** durch eine **zweite, unabhängige Sicherheitsebene** ergänzt, wodurch Konten selbst bei gestohlenem Passwort geschützt bleiben – ein entscheidender Schutz gegen Cyberkriminalität, da Passwörter oft kompromittiert sind oder wiederverwendet werden.

Sie schützt somit sensible Daten und private Informationen, indem sie einen unbefugten Zugriff erheblich erschwert, was für den Online-Kontenschutz unerlässlich ist.

Zusammenfassung:

- **Zusätzlicher Schutz:** Selbst wenn Ihr Passwort durch einen Angriff gestohlen wird, kann der Angreifer nicht auf Ihr Konto zugreifen, ohne den zweiten Faktor zu haben.
- **Schutz sensibler Daten:** Insbesondere bei Konten mit sensiblen Daten wie Gesundheitsdaten, Online-Banking oder E-Mail ist 2FA eine wichtige zusätzliche Sicherheitsebene.
- **Verhindert unbefugten Zugriff:** 2FA macht es Cyberkriminellen schwerer, sich illegal Zugang zu Accounts zu verschaffen.

Welche 2FA-Verfahren werden vom PraxisPortal künftig unterstützt?

Mit der Einführung der Zwei-Faktor-Authentifizierung (2FA) im PraxisPortal werden Sie nach dem Login aufgefordert, eine 2FA-Methode auszuwählen und für Ihren Benutzer zu aktivieren. In der Einführungsphase haben Sie die Möglichkeit, die Einrichtung zunächst zu überspringen und die 2FA zu einem späteren Zeitpunkt zu aktivieren. Im PraxisPortal stehen Ihnen folgende 2FA-Verfahren zur Verfügung:

- **2FA per E-Mail.** Diese Methode steht Ihnen zur Verfügung, wenn in Ihren Benutzereinstellungen eine gültige E-Mail-Adresse hinterlegt ist.
Nach der Aktivierung dieser Methode wird Ihnen bei Anmeldung ein Sicherheitscode an Ihre im PraxisPortal unter Einstellungen hinterlegte E-Mail-Adresse gesendet, den Sie zur Bestätigung eingeben müssen.
- **2FA mit Authenticator-App.** Alternativ können Sie eine Authenticator-App verwenden. Diese Methode kann auf einem oder mehreren Geräten eingerichtet werden. Nach der Aktivierung generiert die App einen zeitbasierten Sicherheitscode, den Sie bei der Anmeldung eingeben.

Was sind die Vor- und Nachteile der unterschiedlichen 2FA Verfahren?

Im PraxisPortal können Sie zwischen zwei Methoden der Zwei-Faktor-Authentifizierung (2FA) wählen:

E-Mail oder **Authenticator-App**. Beide erhöhen die Sicherheit Ihres Kontos deutlich, unterscheiden sich jedoch im Komfort und im Sicherheitsniveau.

	2FA per E-Mail	2FA mit Authenticator-App
So funktioniert es:	Bei der Anmeldung erhalten Sie einen Sicherheitscode an Ihre hinterlegte E-Mail-Adresse.	Eine Authenticator-App auf Ihrem Smartphone oder Tablet erzeugt automatisch einen zeitlich begrenzten Sicherheitscode.
Vorteile:	• Sehr einfache Einrichtung • Keine zusätzliche App erforderlich • Auf jedem Gerät nutzbar, auf dem Sie Zugriff auf Ihre E-Mails haben	• Höheres Sicherheitsniveau • Funktioniert auch ohne Internetverbindung • Unabhängig vom E-Mail-Postfach • es können mehrere Geräte hinterlegt werden
Nachteile:	• Abhängig vom Zugriff auf Ihr E-Mail-Postfach, da nur eine E-Mail-Adresse zur Authentifizierung genutzt werden kann. • Funktioniert nicht ohne Internetverbindung • Etwas geringeres Sicherheitsniveau, da bei einem kompromittierten E-Mail-Konto auch der 2FA-Code abgefangen werden könnte	• Installation einer zusätzlichen App erforderlich • Bei Gerätewechsel oder Verlust muss die App neu eingerichtet werden • Ohne Zugriff auf das eingerichtete Gerät ist keine Anmeldung möglich
Geeignet für:	Benutzer, die eine unkomplizierte Lösung bevorzugen und regelmäßig Zugriff auf ihr E-Mail-Postfach haben.	Benutzer, die besonderen Wert auf Sicherheit legen oder ihr Konto zusätzlich absichern möchten.
Unsere Empfehlung: • Für ein höheres Sicherheitsniveau empfehlen wir die Nutzung einer Authenticator-App. • Wenn Sie eine möglichst einfache Lösung wünschen, ist die 2FA per E-Mail eine gute Alternative.		

Muss ich unbedingt 2FA bei meinem Benutzer aktivieren?

Zu Beginn der Einführung der Zwei-Faktor-Authentifizierung (2FA) im PraxisPortal ist die Aktivierung noch freiwillig.

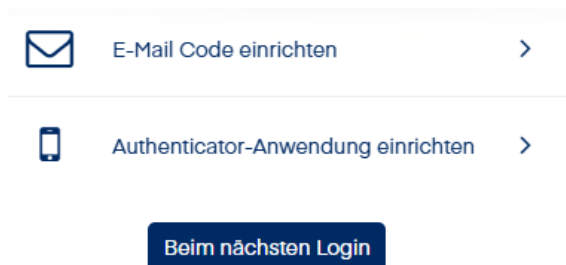
Sie können die Einrichtung zunächst überspringen und zu einem späteren Zeitpunkt vornehmen – entweder beim nächsten Login oder über Ihre Benutzereinstellungen. So haben Sie ausreichend Zeit, sich über die 2FA zu informieren und die für Sie passende Methode auszuwählen.

Bitte beachten Sie jedoch: Nach der Einführungsphase wird die Nutzung der 2FA verpflichtend. Das Überspringen der Einrichtung ist dann nicht mehr möglich. Um sich langfristig weiterhin im PraxisPortal anmelden und arbeiten zu können, müssen Sie eine 2FA-Methode aktiviert haben.

Was ändert sich durch die Einführung der 2FA im PraxisPortal?

Einrichtung der Zwei-Faktor-Authentifizierung (2FA)

Nach dem Einloggen in das PraxisPortal wird Ihnen ein 2FA-Dialog angezeigt. Sie können zwischen folgenden Optionen wählen:



 E-Mail Code einrichten >

 Authenticator-Anwendung einrichten >

Beim nächsten Login

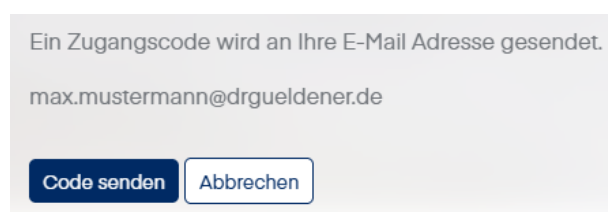
- 2FA per E-Mail-Code einrichten
- 2FA mit einer Authenticator-App einrichten
- Einrichtung beim nächsten Login durchführen

2FA per E-Mail-Code einrichten

Hinweis: Diese Option steht nur zur Verfügung, wenn im PraxisPortal eine E-Mail-Adresse für den Benutzer hinterlegt ist.

Sobald Sie auf „E-Mail-Code einrichten“ klicken, wird Ihnen angezeigt, welche E-Mail-Adresse für den Versand des Zugangscodes im PraxisPortal hinterlegt ist.

Wenn die Adresse korrekt ist, bestätigen Sie den Versand mit dem Button „Code senden“.



Ein Zugangscode wird an Ihre E-Mail Adresse gesendet.

max.mustermann@drgueldener.de

Code senden Abbrechen

Sie erhalten anschließend einen Zugangscode per E-Mail. Geben Sie diesen in das vorgesehene Eingabefeld "E-Mail Zugangscode" ein und klicken Sie auf den Button "Absenden".

Zugangscode wurde versendet.

Ein Zugangscode wurde an max.mustermann@drgueldener.de gesendet. Bitte geben Sie den Code ein.

E-Mail Zugangscode:

[« Zurück zur Anmeldung](#)

Absenden

Abbrechen

Nach Eingabe des Codes werden Sie im PraxisPortal angemeldet und zur Startseite weitergeleitet.

2FA mit einer Authenticator-App einrichten

Für diese Option benötigen Sie eine Authenticator-App auf Ihrem Smartphone oder Tablet (z. B. Google Authenticator, Microsoft Authenticator oder FreeOTP).

So richten Sie die App ein:

- Öffnen Sie die auf Ihrem Gerät installierte App und scannen Sie damit den im PraxisPortal angezeigten QR-Code:

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



- Die App erzeugt automatisch einen zeitlich begrenzten Sicherheitscode.
- Geben Sie diesen Code in das entsprechende Eingabefeld "One-time Code" ein:

One-time Code *

Gerätename

- Optional können Sie einen Namen für Ihr Gerät im Eingabefeld "Gerätename" vergeben. Wenn Sie mehrere Geräte für 2FA nutzen, ist ein Geräteiname erforderlich, damit Sie diese unterscheiden können.

Einrichtung zunächst überspringen

Zu Beginn ist die Nutzung der Zwei-Faktor-Authentifizierung freiwillig. Sie können die Einrichtung überspringen und später vornehmen.

Klicken Sie dazu auf „Beim nächsten Login“. Sie werden dann ohne 2FA angemeldet.

Beim nächsten Login wird die Einrichtung erneut abgefragt.

2FA zu einem späteren Zeitpunkt einrichten

Sie können die 2FA-Methode jederzeit einrichten – entweder beim nächsten Login oder über Ihre Benutzereinstellungen:

1. Öffnen Sie die Benutzereinstellungen.
2. Navigieren Sie zum Bereich „2FA“.
3. Klicken Sie auf „2FA ändern“.
4. Geben Sie aus Sicherheitsgründen Ihr Passwort ein.
5. Falls Sie bereits eine 2FA-Methode eingerichtet haben, geben Sie den Zugangscode ein.
6. Wählen Sie anschließend die gewünschte 2FA-Methode aus.

Benutzereinstellungen:

Zwei-Faktor-Authentifizierung (2FA)

Hier können Sie Ihre aktuelle Zwei-Faktor-Authentifizierung-Einstellungen ändern.

[2FA ändern](#)

Passwort Eingabe:

PraxisPortal-Login

Passwort

[Passwort vergessen?](#)

Anmelden

Falls Sie bereits eine 2FA eingerichtet haben, geben, werden Sie aufgefordert, den Zugangscode einzugeben:

Zugangscode wurde versendet.

Ein Zugangscode wurde an m***n@drgueldener.de gesendet. Bitte geben Sie den Code ein.

E-Mail Zugangscode:

Absenden

Abbrechen

In diesem Fall ist die 2FA E-Mail Code bereits eingerichtet und eine weitere Methode 2FA mit Authenticator-App kann zusätzlich eingerichtet werden. Die bereits eingerichtete 2FA-Methode kann bei Bedarf gelöscht werden:

Konfigurierte 2FA Methoden

Bevorzugt	Methode	Konfiguriert
☒	 E-Mail Code Apr 20, 2026	 

Verfügbare 2FA Methoden

Weiteren Authentifizierungsmechanismus einrichten.



Authenticator-Anwendung einrichten



Abbrechen

Mehrere 2FA-Methoden nutzen

Sie können mehrere 2FA-Methoden einrichten:

- eine Methode per E-Mail
- sowie mehrere Methoden über Authenticator-Apps

Außerdem können Sie eine Methode als bevorzugt festlegen. Diese wird standardmäßig für die Authentifizierung verwendet.

Wenn mehrere Methoden eingerichtet sind, können Sie beim Login jederzeit eine alternative Methode auswählen.

Im Beispiel unten sind 2FA per E-Mail sowie 2FA über zwei Geräte („Praxis #1“ und „Praxis #2“) eingerichtet. Das Gerät „Praxis #1“ ist als bevorzugte Methode ausgewählt. Wenn Sie das Gerät „Praxis #1“ gerade nicht zur Hand haben, können Sie stattdessen „Praxis #2“ auswählen und den dort generierten Zugangscode eingeben.

Sollten Sie keines der beiden Geräte verfügbar haben, können Sie über den Link „Einen anderen Weg versuchen“ den Zugangscode an Ihre hinterlegte E-Mail-Adresse senden lassen.

☒ **Praxis #1** ☐ **Praxis #2**

One-time code

Anmelden **Abbrechen**

[Einen anderen Weg versuchen](#)

Wie oft muss 2. Faktor eingegeben werden?

Nach einer erfolgreichen Authentifizierung mit dem Zugangscode wird ein Cookie in Ihrem Browser gespeichert, das 30 Tage lang gültig ist. Innerhalb dieses Zeitraums müssen Sie bei der Anmeldung keinen Zugangscode erneut eingeben. Nach Ablauf der 30 Tage werden Sie automatisch aufgefordert, sich erneut mit Ihrem Zugangscode zu authentifizieren.

Bitte beachten Sie: Wenn Sie die Cookies in Ihrem Browser löschen oder Ihr Browser so eingestellt ist, dass Cookies automatisch gelöscht werden, müssen Sie den Zugangscode beim nächsten Besuch des PraxisPortals erneut eingeben.

Muss ich zukünftig trotz aktivierter Zwei-Faktor-Authentifizierung (2FA) mein Passwort regelmäßig ändern?

Nein. Wenn Sie die Zwei-Faktor-Authentifizierung (2FA) für Ihren Benutzer aktiviert haben, ist eine regelmäßige Passwortänderung nicht mehr erforderlich. Durch die 2FA wird Ihr Konto zusätzlich zum Passwort mit einem zweiten Sicherheitsfaktor geschützt – zum Beispiel mit einem Code per E-Mail oder aus einer Authenticator-App. Dadurch erhöht sich die Sicherheit Ihres Zugangs deutlich. Statt Ihr Passwort in festgelegten Abständen ändern zu müssen, werden Sie künftig in regelmäßigen Abständen aufgefordert, einen zusätzlichen Sicherheitscode einzugeben. Dieser Code wird entweder an Ihre hinterlegte E-Mail-Adresse gesendet oder in Ihrer Authenticator-App erzeugt.

Wichtig:

Unabhängig davon empfehlen wir weiterhin, ein sicheres und individuelles Passwort zu verwenden und dieses nicht an Dritte weiterzugeben. Sollten konkrete Sicherheitsanforderungen oder besondere Umstände vorliegen, kann eine Passwortänderung selbstverständlich weiterhin notwendig sein (z. B. bei Verdacht auf unbefugten Zugriff).

Wird der Einreichen-Prozess aus der PVS für die Aktivierung der 2FA aufgehalten?

Zu Beginn der Einführung der Zwei-Faktor-Authentifizierung (2FA) ist der PraxisPortalClient (PPC) zunächst nicht von der Aktivierung betroffen.

Sie können 2FA bereits für Ihren Benutzer einrichten, jedoch wird beim Login in den PraxisPortalClient kein zusätzlicher Zugangscode abgefragt.

Die 2FA-Abfrage erfolgt derzeit ausschließlich in der browserbasierten Version des PraxisPortals.

Sobald 2FA auch für den PraxisPortalClient gilt, werden wir Sie gesondert darüber informieren.

Was bedeutet das für Sie als Praxis?

Bitte beachten Sie folgende Punkte:

Die 2FA wird für einen Account im PraxisPortal eingerichtet.

Das bedeutet: Alle Benutzer dieses Accounts benötigen Zugriff entweder auf die hinterlegte E-Mail-Adresse oder auf ein Gerät mit Authenticator-App, um den Zugangscode eingeben zu können.

Bis zur Einrichtung der 2FA (betrifft zuerst nur browserbasierte Version):

- Bei jedem Login im PraxisPortal werden Sie aufgefordert, die 2FA einzurichten.
- Zu Beginn der Einführung können Sie diesen Schritt noch überspringen.

Nach erfolgreicher Einrichtung der 2FA (betrifft zuerst nur browserbasierte Version):

- Sie müssen Ihr Passwort nicht mehr alle 6 Monate ändern.
- Sie können die Funktion „Passwort vergessen“ nutzen (nur in Kombination mit 2FA per E-Mail).
- Aus Sicherheitsgründen werden Sie alle 30 Tage beim Login aufgefordert, zusätzlich einen Zugangscode einzugeben.

Haben Sie Fragen?

Sie erreichen unseren technischen Kundensupport unter:

Telefon: **0711 99373-2800**

E-Mail: support@apotheken-aerzte.de