

Zwei-Faktor-Authentifizierung aktivieren

Erhöhen Sie die Sicherheit eines Benutzerkontos durch die Aktivierung der Zwei-Faktor-Authentifizierung

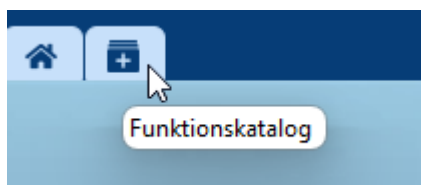
Die Einrichtung der Zwei-Faktor-Authentifizierung für ein Benutzerkonto in BASIS dauert nur wenige Minuten und bietet einen deutlichen Sicherheitsgewinn. Zum Bearbeiten der Benutzerkonten-Einstellungen benötigen Sie die entsprechende Berechtigung für Funktionen aus dem Bereich **System** → **Voreinstellungen** → **Benutzerverwaltung**.

Benutzerkonto für die Einrichtung öffnen

Um die Zwei-Faktor-Authentifizierung für einen Benutzer in BASIS aktivieren zu rufen Sie die **Kontoeinstellungen** für den entsprechenden Benutzer auf. Suchen Sie dazu im **Funktionskatalog** nach „Benutzerverwaltung“ und rufen den Eintrag auf.

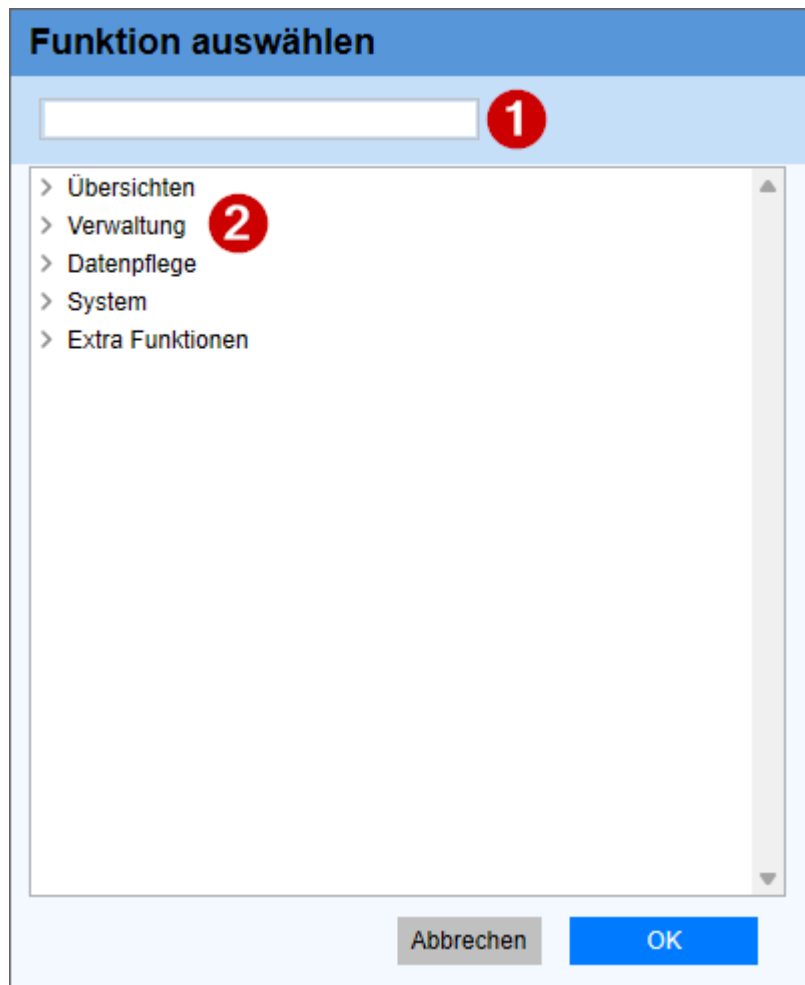
Den Funktionskatalog nutzen

Über den Funktionskatalog können Sie viele Bereiche und Funktionen in BASIS direkt aufrufen. Um den Katalog zu öffnen, klicken Sie auf den **Funktionskatalog-Tab**:



Danach können Sie einen Eintrag auf folgende Arten auswählen:

1. Im Suchfeld **(1)** einen Begriff eingeben und den gefundenen Eintrag in der Liste darunter auswählen
2. Alternativ: Einen Listenpunkt aus der Liste **(2)** aufklappen und einen Eintrag auswählen
3. Mit einem Klick auf den Button **OK** bestätigen



Wie Sie Bereiche in BASIS per Tastatur-Kurzbefehl aufrufen oder den Funktionskatalog über die Tastatur bedienen können, erfahren Sie im Artikel [Tastatur-Kurzbefehle in BASIS 6](#)

Voreinstellungen																																															
Benutzerkonten 7 Benutzer																																															
Benutzerkonten Benutzerkonten ☐ Inklusive ausgeschiedener Benutzer <table> <tr> <th>Benutzername</th><th>Beschreibung</th><th>Gültig bis</th><th>Benutzergruppen</th></tr> <tr> <td>Designer</td><td>Programmierer von BASIS</td><td></td><td>Arzt / Gesamte Administration</td></tr> <tr> <td>Fremdarzt</td><td>Fremdarzt - z.B. für Externe Impfungen nutzbar</td><td></td><td>Arzt</td></tr> <tr> <td>Honorararzt</td><td>Gast-Arzt</td><td></td><td>Arzt / Keine Preise</td></tr> <tr> <td>Max</td><td>Testbenutzer</td><td></td><td>Arzt / Assistenz / Ist Arzt</td></tr> <tr> <td>Musterarzt</td><td>Betriebsarzt</td><td></td><td>Arzt / Faktura / Gesamte Administration / OPL Führen / Standard-User</td></tr> <tr> <td>MusterAssistenz</td><td>Assistenz</td><td></td><td>Keine Preise / OPL Führen / Standard-User</td></tr> <tr> <td>MusterSifa</td><td>Sifa</td><td></td><td>Arbeitssicherheit_BasisSifa / Keine Preise / OPL Führen / Standard-User</td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> </table>				Benutzername	Beschreibung	Gültig bis	Benutzergruppen	Designer	Programmierer von BASIS		Arzt / Gesamte Administration	Fremdarzt	Fremdarzt - z.B. für Externe Impfungen nutzbar		Arzt	Honorararzt	Gast-Arzt		Arzt / Keine Preise	Max	Testbenutzer		Arzt / Assistenz / Ist Arzt	Musterarzt	Betriebsarzt		Arzt / Faktura / Gesamte Administration / OPL Führen / Standard-User	MusterAssistenz	Assistenz		Keine Preise / OPL Führen / Standard-User	MusterSifa	Sifa		Arbeitssicherheit_BasisSifa / Keine Preise / OPL Führen / Standard-User												
Benutzername	Beschreibung	Gültig bis	Benutzergruppen																																												
Designer	Programmierer von BASIS		Arzt / Gesamte Administration																																												
Fremdarzt	Fremdarzt - z.B. für Externe Impfungen nutzbar		Arzt																																												
Honorararzt	Gast-Arzt		Arzt / Keine Preise																																												
Max	Testbenutzer		Arzt / Assistenz / Ist Arzt																																												
Musterarzt	Betriebsarzt		Arzt / Faktura / Gesamte Administration / OPL Führen / Standard-User																																												
MusterAssistenz	Assistenz		Keine Preise / OPL Führen / Standard-User																																												
MusterSifa	Sifa		Arbeitssicherheit_BasisSifa / Keine Preise / OPL Führen / Standard-User																																												

Liste mit allen Benutzerkonten in BASIS

Sie sehen eine Liste aller Benutzerkonten. Öffnen Sie das Benutzerkonto, dessen Einstellungen Sie bearbeiten möchten, mit einem Doppelklick. Im Bereich

Anmeldung können Sie unter **Verfahren** das Optionsfeld **Benutzername / Passwort / OTP ①** auswählen.

Kontoeinstellungen Erweitert Mandanten Protokoll Rechte Allgemein Anpassen Firmenkarteireiter Kalender Stempel Standort

Benutzerkonto
Benutzername
Max
Name Geschlecht
Max Muster
Beschreibung
Testbenutzer
☐ Struktur-Zugriff ☐ Mehrfachanmeldung **Deaktiviert** 00.00.0000

Anmeldung
Passwort
☐ Bei nächster Anmeldung ändern
☐ Kann geändert werden
☐ Läuft nie ab
Verfahren
☐ Benutzername / Passwort
☒ Benutzername / Passwort / OTP
OTP neu erstellen -> Zwischenablage
Systemzeit Kontrolle E-Mail versenden
Letzte Anmeldung 09.07.2026 / 13:24:57
Letzte Passwortänderung 20.11.2025
Letzte Sperrung 00.00.0000 / 00:00:00

Untersuchungen
☒ Für alle Untersuchungsprofile zugelassen
☐ Nur folgende Untersuchungsprofile
- +

Vertreten durch
- +
Bezeichnung Von Bis

Sonstiges
Kalender
☐ eigenen Kalender führen
Zeiterfassung
☐ Zeiterfassung am Ende

Kontoeinstellungen im Bereich Benutzerkonten in den Voreinstellungen von BASIS

Anschließend muss das Gerät, das als zweiter Faktor verwendet werden soll, durch Scannen des von BASIS erzeugten QR-Codes mit einer Authenticator-App gekoppelt werden. Der QR-Code wird in den Kontoeinstellungen des Benutzers angezeigt und kann direkt mit dem gewünschten Gerät gescannt werden.

Alternativ können Sie den QR-Code per E-Mail an den Benutzer senden oder als Bild in die Zwischenablage kopieren. Um den QR-Code per E-Mail zu versenden, klicken Sie auf **E-Mail versenden ②**. Voraussetzung hierfür ist, dass für den Benutzer in BASIS eine E-Mail-Adresse hinterlegt ist.

Eine weitere Möglichkeit ist, auf den Knopf → **Zwischenablage ③** zu klicken, um den QR-Code als Bild in die Zwischenablage zu kopieren. Anschließend können Sie ihn dem Benutzer auf einem anderen Weg zur Verfügung stellen.

Unterstützte Apps für Zwei-Faktor-Authentifizierung

BASIS ist nicht an eine bestimmte Authenticator-App gebunden. Sie können jede App verwenden, die zeitbasierte Einmalpasswörter unterstützt. Dazu gehören beispielsweise Google Authenticator, Microsoft Authenticator oder die Passwörter-App von Apple.

Das Hinzufügen eines Kontos erfolgt in den meisten Apps nach demselben Prinzip:

1. Öffnen Sie die Authenticator-App
2. Wählen Sie die Option zum Hinzufügen eines neuen Kontos (z. B. Konto hinzufügen oder +)

3. Scannen Sie den in BASIS angezeigten QR-Code mit der Kamera des Geräts

Nach erfolgreichem Scannen wird das Benutzerkonto in der App angelegt und es werden fortlaufend Einmalcodes generiert.

Links zu gängigen Authenticator-Apps:

- [Microsoft Authenticator bei Google Play](#)
- [Microsoft Authenticator im Apple App Store](#)
- [Google Authenticator bei Google Play](#)
- [Google Authenticator im Apple App Store](#)

Warum Zwei-Faktor-Authentifizierung (2FA) sinnvoll ist

Die Zwei-Faktor-Authentifizierung (2FA) erhöht die Sicherheit eines Benutzerkontos deutlich. Neben dem Passwort wird bei der Anmeldung als zweiter Nachweis ein Einmalcode benötigt, der über eine Authenticator-App auf dem Smartphone des Benutzers erzeugt wird. Selbst wenn ein Passwort in falsche Hände gerät, kann sich ohne diesen zweiten Faktor in der Regel niemand an dem Konto anmelden.

Der Einsatz von 2FA schützt somit vor vielen gängigen Angriffen, etwa durch gestohlene oder erratene Passwörter. Gleichzeitig trägt die Funktion dazu bei, dass Benutzerkonten ausschließlich von den vorgesehenen Personen genutzt werden. Die Weitergabe von Passwörtern oder das gemeinsame Verwenden eines Benutzerkontos wird dadurch deutlich erschwert, da zusätzlich das persönliche Smartphone des jeweiligen Benutzers benötigt wird. Das verbessert die Nachvollziehbarkeit von Aktionen im System und unterstützt einen sicheren und verantwortungsvollen Umgang mit Benutzerkonten.

i Warum Zwei-Faktor-Authentifizierung (2FA) sinnvoll ist

Die Zwei-Faktor-Authentifizierung (2FA) erhöht die Sicherheit eines Benutzerkontos deutlich. Neben dem Passwort wird bei der Anmeldung als zweiter Nachweis ein Einmalcode benötigt, der über eine Authenticator-App auf dem Smartphone des Benutzers erzeugt wird. Selbst wenn ein Passwort in falsche Hände gerät, kann sich ohne diesen zweiten Faktor in der Regel niemand an dem Konto anmelden.

Der Einsatz von 2FA schützt somit vor vielen gängigen Angriffen, etwa durch gestohlene oder erratene Passwörter. Gleichzeitig trägt die Funktion dazu bei, dass Benutzerkonten ausschließlich von den vorgesehenen Personen genutzt werden. Die Weitergabe von Passwörtern oder das gemeinsame Verwenden eines Benutzerkontos wird dadurch deutlich erschwert, da zusätzlich das persönliche Smartphone des jeweiligen Benutzers benötigt wird. Das verbessert die Nachvollziehbarkeit von Aktionen im System und unterstützt einen sicheren und verantwortungsvollen Umgang mit Benutzerkonten.