

Zwei-Faktor-Authentifizierung Anwendungshandbuch

ix.connect | Auth



Inhalt

Zwei-Faktor-Authentifizierung Anwendungshandbuch	1
ix.connect Auth	1
1 Einleitung	3
1.1 Voraussetzungen	3
1.2 Zweiter Faktor	3
2 Anmelden	4
2.1 Anmelden mit Google Authenticator	5
2.2 Anmelden mit FIDO2 Web Authn	6
2.3 Anmelden mit YubiKey Multifactor Authentifizierung	7
2.4 Anmelden mit E-Mail Tokens	8
2.5 Sperrung und Fallback bei verlorenen Geräten / Token / Keys	8

1 Einleitung

Die Zwei-Faktor-Authentifizierung (2FA) in der Dedalus-Umgebung ix.connect wird über den zentralen Anmelde Dienst (Single Sign-On, SSO) verwaltet. Dieser zentrale Dienst stellt die Anmeldeplattform für alle cloudbasierten Anwendungen und Services dar, die von der Dedalus Labor GmbH betrieben werden.

Dieses Dokument richtet sich an Administratoren und Benutzer, die mit dem ix.connect Anmelde Dienst arbeiten und das Arbeitsumfeld für ihre Benutzer konfigurieren möchten.

Durch die Anmeldung mittels Zwei-Faktor-Authentifizierung wird ein Höchstmaß an Sicherheit gewährleistet. Nur autorisierte Benutzer erhalten Zugriff auf sensible Daten und geschützte Bereiche innerhalb der Dedalus-basierten Anwendungen.

1.1 Voraussetzungen

Für die Nutzung der Zwei-Faktor-Authentifizierung (2FA) über den zentralen Anmelde Dienst (Single Sign-On, SSO) in der Dedalus-Umgebung müssen folgende technische und organisatorische Voraussetzungen erfüllt sein:

- Ein aktueller Webbrowser (z. B. Google Chrome, Mozilla Firefox, Microsoft Edge), der moderne Authentifizierungsmechanismen unterstützt.
- Ein gültiger Benutzerzugang zur zentralen Anmeldeplattform von ix.connect der Dedalus Labor GmbH.
- Des Weiteren wird für ein oder mehrere weitere Faktoren optional Entsprechendes benötigt

1.2 Zweiter Faktor

Der zweite Faktor ist ein zusätzliches Sicherheitsmerkmal. Es ergänzt das Benutzerkennwort (erster Faktor) und stellt sicher, dass der Zugriff ausschließlich durch autorisierte Personen erfolgt.

Die ix.connect-Umgebung unterstützt derzeit folgende Methoden zur Zwei-Faktor-Authentifizierung:

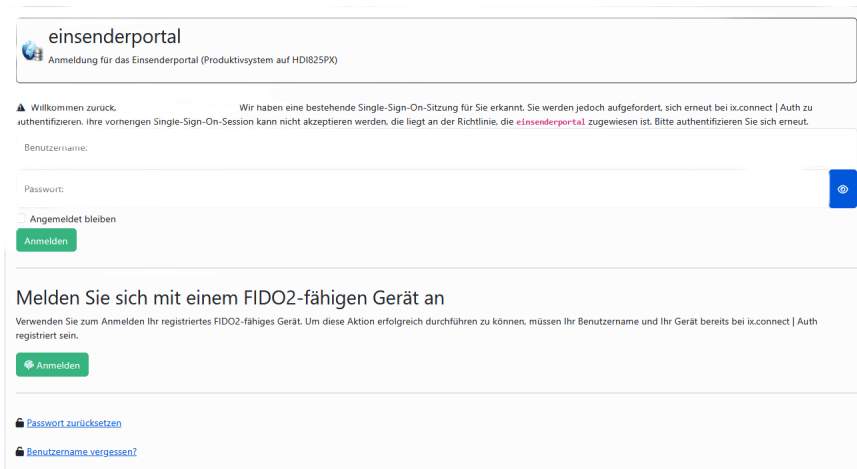
- Authenticator Apps (z.B von Google oder Microsoft)
- FIDO2 Web Authentication (z.B. Dienste wie Windows Hello)
- YubiKey Multifactor Authentifizierung
- E-Mail Authentifizierung

2 Anmelden

Die Seite für die Anmeldung erscheint automatisch, wenn man ein ix.connect System aufruft.

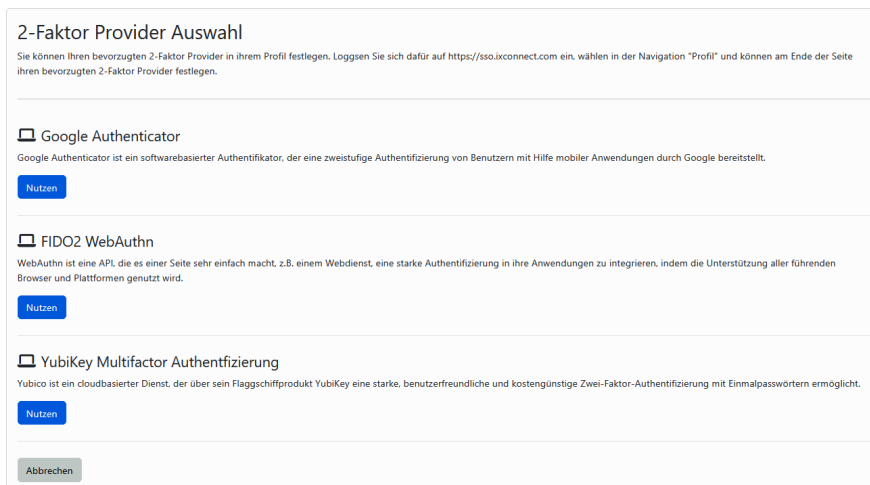
Die benötigten Anmeldedaten für alle ix.connect Systeme erhalten Sie von Ihrem ix.connect-Administrator bzw. IT Ansprechpartner.

Geben Sie hier Ihren **Benutzernamen** (Groß-/Kleinschreibung nicht relevant) und Ihr **Passwort** (Groß-/Kleinschreibung relevant) in den jeweiligen Feldern ein. Die Zeichen des eingegebenen Passworts werden aus Sicherheitsgründen mit Punkten angezeigt.



The screenshot shows the login interface for 'einsenderportal'. At the top, it says 'Anmeldung für das Einsenderportal (Produktivsystem auf HD1825PX)'. Below this, there is a message: 'Willkommen zurück. Wir haben eine bestehende Single-Sign-On-Sitzung für Sie erkannt. Sie werden jedoch aufgefordert, sich erneut bei ix.connect | Auth zu authentifizieren. Ihre vorangigen Single-Sign-On-Session kann nicht akzeptieren werden, die liegt an der Richtlinie, die einsenderportal zugewiesen ist. Bitte authentifizieren Sie sich erneut.' There are two input fields: 'Benutzername:' and 'Passwort:'. The password field has a blue eye icon to toggle visibility. Below the password field is a checkbox 'Angemeldet bleiben' and a green 'Anmelden' button. A section titled 'Melden Sie sich mit einem FIDO2-fähigen Gerät an' follows, with a description and a green 'Anmelden' button. At the bottom, there are links for 'Passwort zurücksetzen' and 'Benutzername vergessen?'. A small copyright notice '© 2021 Dedalus Labor GmbH' is visible at the very bottom.

Klicken Sie in der Anmeldemaske unter ihrem Benutzernamen und dem Passwort auf den Button **Anmelden** oder nach Eingabe der Daten <Enter>. Sie gelangen in die Auswahl der zur Verfügung stehenden Arten (Provider) für den zweiten Faktor.



The screenshot shows the '2-Faktor Provider Auswahl' page. It starts with the title and a paragraph: 'Sie können Ihren bevorzugten 2-Faktor Provider in Ihrem Profil festlegen. Loggen Sie sich dafür auf https://sso.ixconnect.com ein, wählen in der Navigation "Profil" und können am Ende der Seite Ihren bevorzugten 2-Faktor Provider festlegen.' There are three provider options, each with a 'Nutzen' button: 'Google Authenticator' (described as a software-based authenticator), 'FIDO2 WebAuthn' (described as an API for easy integration), and 'YubiKey Multifactor Authentifizierung' (described as a cloud-based service). At the bottom, there is an 'Abbrechen' button.

2.1 Anmelden mit Google Authenticator

Google Authenticator ist eine softwarebasierte Authentifizierungsanwendung. Die App generiert zeitbasierte Einmalpasswörter, die als zweiter Faktor bei der Benutzeranmeldung verwendet werden. Die Anwendung ist für mobile Betriebssysteme wie **Android** und **iOS** verfügbar und muss zuvor auf dem mobilen Endgerät installiert werden.

- Klicken Sie auf den Button **Nutzen** unter Google Authenticator.

Bei der ersten Anwendung der 2-Faktor-Authentifizierung werden Sie aufgefordert, ein zusätzliches Gerät als zweiten Faktor zu registrieren. Folgende Seite wird angezeigt:



Ihr Konto ist nicht registriert. Nutzen Sie die Einstellungen unten, um Ihr Gerät zu registrieren.

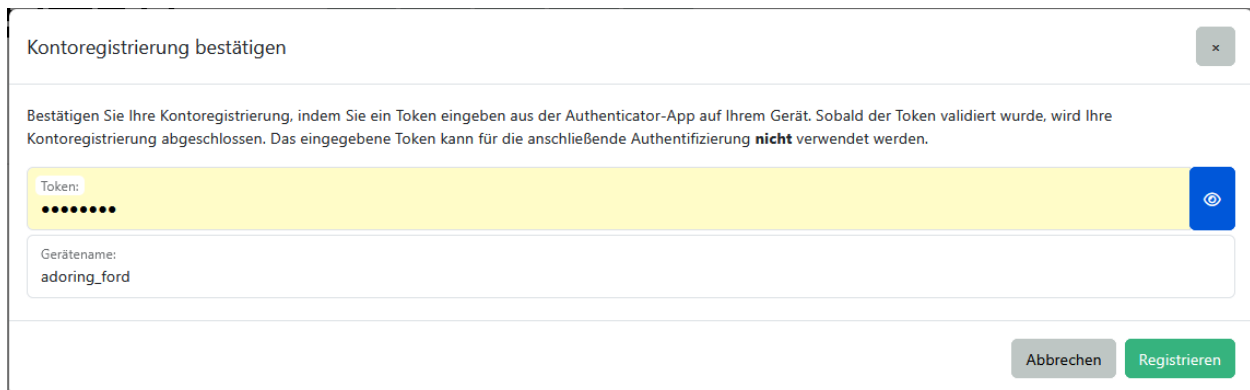
Der geheime Schlüssel (secret key) zur Registering lautet

Scratch codes:

Bestätigen Drucken Abbrechen

© 2025 Dedalus Labor GmbH
1.18-SNAPSHOT 04.08.2025 11:35

- Scannen Sie den dargestellten QR-Code mit der Google Authenticator App, um die Einrichtung Ihres Gerätes zu starten.
- Klicken Sie auf Bestätigen. Ein Popup-Fenster zur Kontoregistrierung wird geöffnet.



Kontoregistrierung bestätigen

Bestätigen Sie Ihre Kontoregistrierung, indem Sie ein Token eingeben aus der Authenticator-App auf Ihrem Gerät. Sobald der Token validiert wurde, wird Ihre Kontoregistrierung abgeschlossen. Das eingegebene Token kann für die anschließende Authentifizierung **nicht** verwendet werden.

Token:

Gerätename: adoring_ford

Abbrechen Registrieren

- Geben Sie das initiale Token ein.
- Vergeben Sie einen Gerätenamen, wenn Sie den vorbelegten nicht übernehmen möchten.
- Klicken Sie auf **Registrieren**.

Nach diesen Schritten sind Sie nun mit einem Gerät registriert und können sich nun anmelden. Hierzu wird dann der erste Token genutzt, den Sie nun eingeben müssen. Nach Eingabe des passenden Codes gelangen Sie zu Ihrer Anwendungsseite und sind erfolgreich angemeldet.

2.2 Anmelden mit FIDO2 Web Authn

Web Authn ist ein offener Web-Standard, mit dem sich Nutzer authentifizieren können. Er ermöglicht die Anmeldung über sichere Hardware-basierte Methoden wie:

- Fingerabdrucksensor
- Gesichtserkennung
- Sicherheitsschlüssel (z. B. YubiKey)
- Plattforminterne Schlüssel des Geräts

Web Authn ist kompatibel mit aktuellen Browsern und Betriebssystemen.

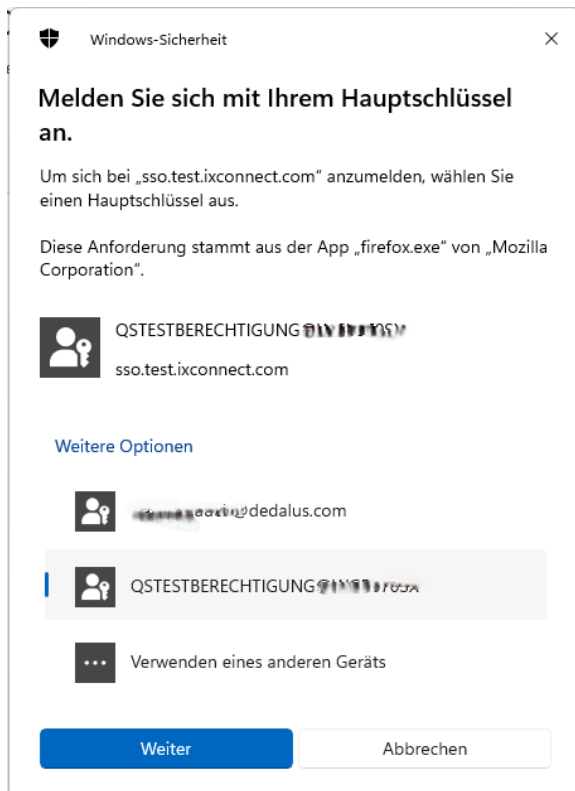
- Klicken Sie auf den Button **Nutzen** unter Fido2 Web Authn. Sie werden aufgefordert sich mit einem FIDO2-fähigen Gerät anzumelden. Ihr Benutzername und das Gerät müssen bei ix.connect Auth registriert sein.

Melden Sie sich mit einem FIDO2-fähigen Gerät an

Verwenden Sie zum Anmelden Ihr registriertes FIDO2-fähiges Gerät. Um diese Aktion erfolgreich durchführen zu können, müssen Ihr Benutzername und Ihr Gerät bereits bei ix.connect | Auth registriert sein.

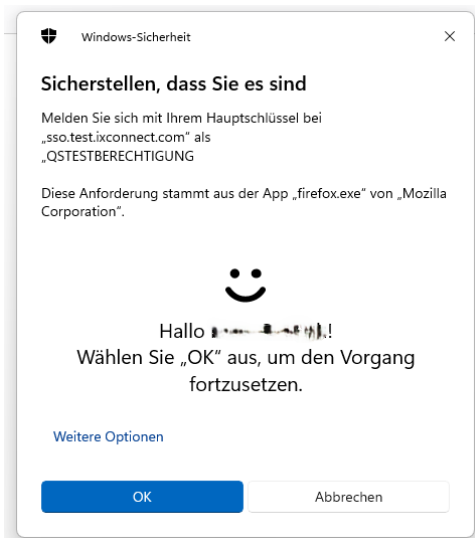
Anmelden

- Klicken Sie auf den Button Anmelden.



- Wählen Sie den Hauptschlüssel aus, oder klicken Sie auf **Verwenden eines anderen Geräts**, um ein weiteres Gerät zu registrieren.

- Klicken Sie auf **Weiter**.



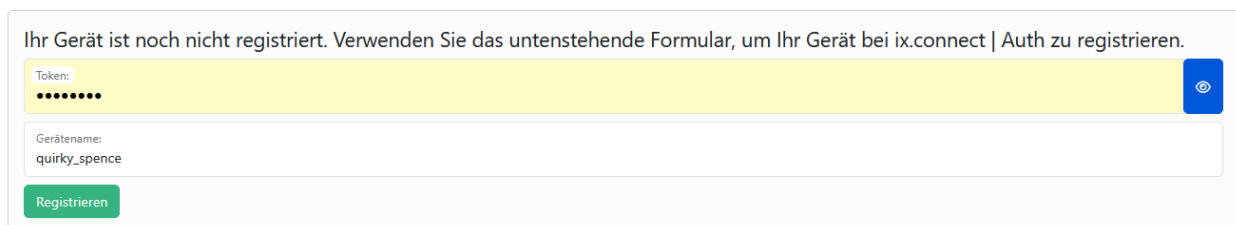
- Führen Sie den **Fingerprint** bzw. **Face-ID** aus und klicken Sie auf **OK**.

Nach erfolgreichem Login gelangen Sie in die Übersichtsseite. Nach diesen Schritten sind Sie nun mit einem Gerät registriert und können sich nun anmelden. Hierzu wird dieser Vorgang erneut ausgeführt. Nach dieser Aktivierung gelangen Sie zu Ihrer Anwendungsseite und sind erfolgreich angemeldet.

2.3 Anmelden mit YubiKey Multifactor Authentifizierung

YubiCo ist ein cloudbasierter, führender Anbieter starker Authentifizierungslösungen. Sein Flaggschiffprodukt YubiKey ermöglicht eine sichere, benutzerfreundliche und kosteneffiziente Zwei-Faktor-Authentifizierung.


- Klicken Sie auf den Button **Nutzen** unter YubiKey Multifactor Authentifizierung.



- Stecken Sie den YubiKey in den USB-Anschluss, bzw. halten Sie ihn bei NFC-fähigen Geräten an das Lesegerät oder nutzen Sie Lightning/USB-C am Mobilgerät.
- Betätigen Sie den Berührungssensor des YubiKey zur physischen Bestätigung.
- Der YubiKey signiert die Registration mit dem privaten Schlüssel. Die Signatur wird über WebAuthn übertragen
- Klicken Sie auf den Button **Registrieren**.

2.4 Anmelden mit E-Mail Tokens

Hierzu klickt man bei den Optionen des 2-Faktor Providers auf ix.connect | Auth:

 ix.connect | Auth Multifactor Authentifizierung

ix.connect | Auth fungiert als eigenständiger Multifaktor-Authentifizierungsanbieter, der Token ausgibt und diese über vordefinierte Kommunikationskanäle wie E-Mail oder Textnachrichten an Endbenutzer sendet.

[Nutzen](#)

Wenn der Benutzer eine E-Mail Adresse hinterlegt hat, wird eine Mail mit einem Einmaltoken versendet. Dieser Token muss in der Anmeldung angegeben werden. Man kann die Zahl in der Mail doppelklicken und kopieren, um dies schnell und einfach auf der Anmeldeseite einzufügen.

So sieht eine Beispiel Mail aus:

Für die Anmeldung an der digitalen Portallösung Ihres Labors wurde eine Zwei-Faktor-Authentifizierung ausgelöst.

Ihr Bestätigungscode lautet: 90[REDACTED]

Der Code ist 5 Minuten gültig und kann nur einmal verwendet werden.

Bitte geben Sie ihn ausschließlich im Anmeldeprozess ein und teilen Sie ihn nicht mit Dritten.

Sollten Sie diese Anfrage nicht selbst ausgelöst haben, verwerfen oder ignorieren Sie diese E-Mail.

Vielen Dank

Automatische Nachricht - bitte nicht antworten.

Der Bestätigungscode ist 5 min seit Anmeldung gültig. Dies ist unabhängig von der Laufzeit der E-Mail. Wenn diese durch Spamfilter oder andere Mechanismen abgefangen oder verzögert ist, sollte hier der Weg geschaffen werden, dass diese Nachrichten schnell durchgehen und pünktlich ankommen.

2.5 Sperrung und Fallback bei verlorenen Geräten / Token / Keys

Sollte der Fall eintreten, dass ein Account durch Verlust von Geräten oder Passwörtern kompromittiert ist – oder die Gefahr besteht, sollte der Support informiert werden und der Account vorübergehend gesperrt werden. In diesem Fall sollte man sich sofort anmelden – insofern eine E-Mail Adresse hinterlegt worden ist, kann diese Authentifizierung genutzt werden, um die abhanden gekommenen Geräte von der Authentifizierungsliste zu löschen. Eine Anmeldung oder Verifizierung ist dann sofort nicht mehr über die gelöschten Geräte möglich. Sollte man unsicher sein, welche Geräte betroffen sind, sollten alle Geräte gelöscht werden!

Registrierte 2-Faktor Authentifizierungsgeräte

Name	Registriert am	Typ
bo [REDACTED]	03.05.2023 07:00	Google Authenticator
sl [REDACTED]	14.12.2023 12:27	Google Authenticator
sv [REDACTED]	26.08.2025 07:14	Google Authenticator
ze [REDACTED]	03.06.2025 11:58	Google Authenticator
bea [REDACTED]	11.02.2025 15:54	FIDO2 WebAuthn
an [REDACTED]	26.08.2025 10:00	YubiKey

Sollte auch das E-Mail Postfach kompromittiert sein, sollte der Account vorübergehend gesperrt werden und mit dem Support das weitere Vorgehen besprochen werden.

Wichtig ist in diesem Kontext der Hinweis, dass der Benutzer selbst dafür verantwortlich ist, den Überblick über die registrierten Geräte zu pflegen und aktuell zu halten!