

Anmeldung & Login (2FA)

Was ist Zwei-Faktor-Authentifizierung (2FA)?

Die Zwei-Faktor-Authentifizierung (2FA) ist eine zusätzliche Sicherheitsmaßnahme, die zum Schutz Ihres Logisth.AI-Kontos erforderlich ist. Neben Ihrem Passwort müssen Sie einen **temporären Sicherheitscode (Token)** eingeben, der Ihnen zur Bestätigung Ihrer Identität bereitgestellt wird. Dieser zusätzliche Schritt erhöht die Sicherheit und schützt Ihr Konto vor unbefugtem Zugriff.

Was ist ein Token?

Ein Token ist ein **temporärer Sicherheitscode (Einmalpasswort)**, der nur für eine **kurze Zeit gültig** ist. Dieser Code stellt sicher, dass nur der berechtigte Benutzer auf das Konto zugreifen kann.

[Mehr über die 2FA-Einstellung innerhalb der Kanzlei.](#)

Anmeldung bei Logisth.AI

Um auf Logisth.AI zuzugreifen, öffnen Sie bitte einen unterstützten Webbrowser und geben Sie die folgende URL ein: <https://splitter.logisth.ai/>

Bitte stellen Sie sicher, dass Sie einen **kompatiblen Browser verwenden**, um die optimale Nutzung sicherzustellen.

2FA – Die Anmeldung mit Token

Nach der Eingabe Ihrer Anmeldedaten erhalten Sie einen **temporären Code (Token)**, den Sie entweder über die Logisth.AI-App auf Ihrem **Smartphone oder per E-Mail** erhalten. Geben Sie diesen Code ein, um sich erfolgreich anzumelden.



Logisth.AI Login Fenster | Token Eingabe

Benutzeroberfläche – Kontosicherheit (2FA)

Auf dieser Oberfläche können Sie Ihre 2FA-Einstellungen verwalten.

Logisth.AI |

Kontosicherheit 2FA – Benutzeroberfläche

2FA-Methode zurücksetzen

Der Benutzer kann die konfigurierte 2FA-Methode selbst zurücksetzen. Dies ist beispielsweise erforderlich, wenn bei der Verwendung einer Authenticator-App ein neues Gerät eingerichtet wird. Nach dem Zurücksetzen kann ein neuer QR-Code generiert und mit dem neuen Gerät gescannt werden.

2FA-Methode zurücksetzen

2FA-Methode zurücksetzen

Achtung! Ab Version **4.7.x** können Benutzer mit der Berechtigung „User-Manager“ die Zwei-Faktor-Authentifizierung (2FA) anderer Benutzer selbst zurücksetzen. Diese Funktion ist somit nicht mehr ausschließlich **Admins** vorbehalten.

2FA-Methode auswählen oder ändern

Unter dem **Button „2FA-Methoden ändern“** können Sie die Methode der Zwei-Faktor-Authentifizierung anpassen. Sie haben zwei Optionen:

1. **Tokengenerator:** Installieren Sie eine App wie Google Authenticator, LastPass Authenticator oder Microsoft Authenticator auf Ihrem Smartphone. Die App generiert den Code in Echtzeit.
2. **E-Mail Nachricht:** Sie erhalten einen Sicherheitscode (Token) per E-Mail, den Sie nach der Anmeldung eingeben müssen.

Ersatz-Code – Token erstellen

Unter „Kontosicherheit“ können Sie Ersatz-Codes erstellen. Klicken Sie auf „**Code anzeigen**“, um bis zu 10 Tokens zu generieren. Diese Ersatz-Codes können verwendet werden, falls Probleme mit der Primärauthentifizierung (z. B. App oder E-Mail) auftreten. **Jeder Code ist nur einmal gültig.**

Wichtiger Hinweis: Speichern Sie die Ersatz-Codes an einem sicheren Ort. Sobald ein Code verbraucht ist, können Sie jederzeit neue Tokens erstellen.

Grundsätzliches zur 2FA bei Login

Bei jedem Login werden Sie nach der Eingabe Ihres Benutzernamens und Passworts zur Eingabe eines Tokens aufgefordert. Diese Abfrage entfällt in folgenden Fällen:

- **2FA ist nicht zwingend erforderlich:** In Ihrer Firma wurde 2FA nicht als Pflicht aktiviert.
- **Benutzer hat 2FA nicht aktiviert:** Sie haben die Zwei-Faktor-Authentifizierung nicht freiwillig eingeschaltet.
- **Vertrauenswürdiges Netzwerk:** Der Benutzer meldet sich aus einem als vertrauenswürdig eingestuften Netzwerk an.