



## Zwei-Faktor-Authentifizierung (2FA)

Mit dieser Authentifizierung kann man die Sicherheit seines Logins erhöhen. Neben Benutzername und Passwort, kann man zusätzlich noch einen wechselnden *Schlüssel* mit abfragen lassen, bevor man Zugang erhält. Der wechselnde *Schlüssel* wird mit einem Smartphone erzeugt und kann zusätzlich beim Login mit angegeben werden.

## Aktivierung durch den Benutzer

Jeder infra-struktur Benutzer kann die erhöhte Sicherheit, durch 2FA selber aktivieren und deaktivieren. Die Einstellung findet sich im Menü unter Einstellungen -> persönliche Einstellungen -> Sicherheitseinstellungen.

A screenshot of the infraSTRUKTUR web interface. The left sidebar shows various menu items like Administration, Anruforganisation, Aufgabenliste, Controlling, Dokumente, Einstellungen, Freundelisten, Persönliche Einstellungen (which is selected), infraSync Einstellungen, Entwicklung, Hilfe, and Incidents. The main content area has tabs for Startseite, Wiedervorlagen, and Persönliche Einstellungen. Under 'Persönliche Einstellungen', there's a section titled 'Benutzerverwaltung'. It shows a message: 'Google Authenticator 2FA (Zwei-Faktor-Authentifizierung)' and 'Ihr Account ist nicht durch einen Google Authenticator geschützt!'. Below this are two download links: 'Laden im App Store' with the Apple logo and 'JETZT BEI Google Play' with the Google Play logo. A note below the App Store link states: 'Apple und das Apple-Logo sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. App Store ist eine Dienstleistungsmarke der Apple Inc.' A note below the Google Play link states: 'Google Play und das Google Play-Logo sind Marken von Google Inc.'. At the bottom right is a button labeled 'Einrichtung starten'.

Da der *Schlüssel* später mit dem Smartphone erzeugt wird, findet man hier bereits den Link für Apple und Google Geräte. Mit dem Button Einrichtung starten, beginnt der Prozess. Damit nicht jeder an meinem Rechner, die 2FA manipuliere kann, muß zunächst das infra-struktur Passwort eingegeben werden.

Nun wird für meinen infra-struktur Account ein QR-Code erzeugt, um auf meinem Smartphone die App *Google Authenticator* einfach und schnell einzurichten.

Google Authenticator 2FA (Zwei-Faktor-Authentifizierung)

Bitte scannen Sie den QR-Code mit Ihrer Google Authenticator App!



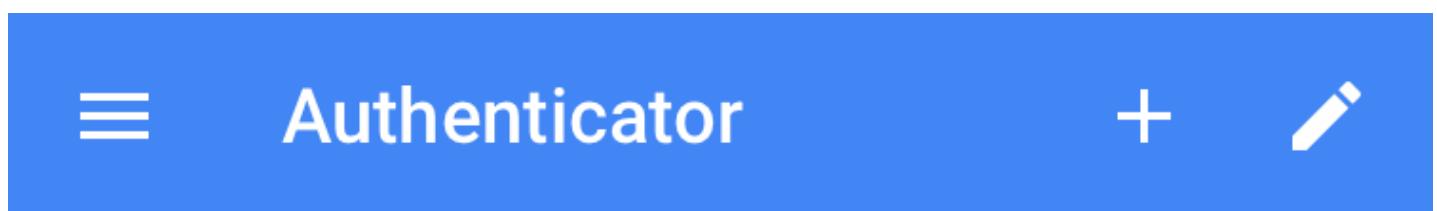
Bestätigen Sie die Daten bitte mit Ihrem infra-struktur Passwort und einem generiertem Schlüssel!

infra-struktur Passwort:	<input type="text"/>
Schlüssel:	<input type="text"/>

[mit der Einrichtung fortfahren](#)

Den erzeugten QR-Code also im nächsten Schritt, mit dem Smartphone scannen und die App ist eingerichtet. Die App erzeugt nun alle 30 Sekunden eine 6-stellige Zahl, die in Zukunft neben dem Benutzernamen und dem Passwort, zusätzlich abgefragt wird. Wichtig: diese 6-stellige Zahl kann nur einmal verwendet werden und wechselt alle 30 Sekunden!

In der App einfach rechts oben das + anklicken und den QR-Code scannen ... fertig.



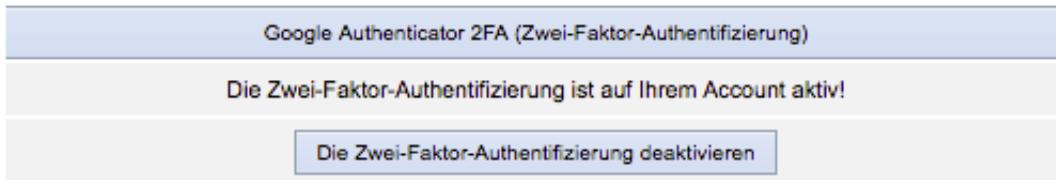
**staging.infra-struktur.net**

**577 199**

ino

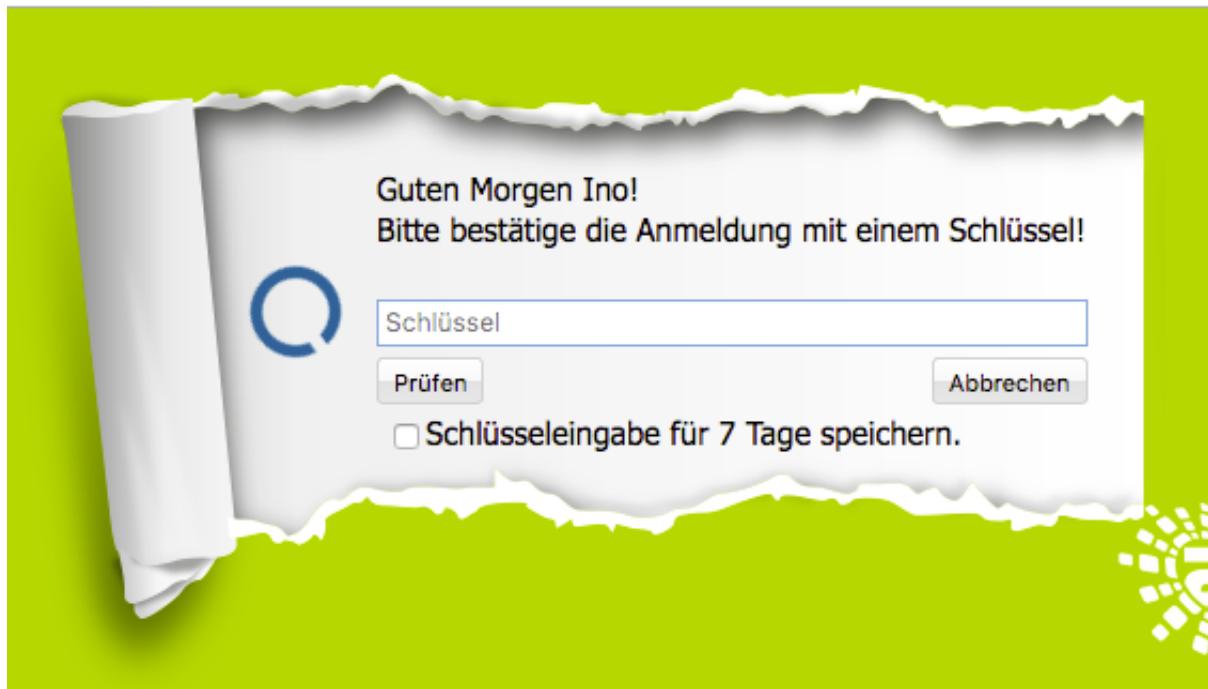
In der infra-struktur nun noch das eigene infra-struktur Passwort und die aktuelle 6-stellige Zahl (*Schlüssel*) aus dem Smartphone eingeben und man hat die 2FA fertig eingerichtet.

Möchte man die 2FA wieder abschalten, kann man das wiederum in seinen persönlichen Einstellungen der infra-struktur mit dem Button erreichen.



## Anwendung

Ist die 2FA aktiviert, kommt im Standard hinter der Loginseite, auf der man nach Benutzernamen und Passwort gefragt wird eine neue Zwischenseite, für die Eingabe des *Schlüssels* aus der Smartphone App.



Nun einfach das Smartphone nehmen, die App *Google Authenticator* öffnen und den 6-stelligen Code eingeben. Mit prüfen beginnt dann das validieren des *Schlüssels* und bei Erfolg der Ladevorgang der Startseite der infra-struktur.

Damit man nicht bei jedem Login, den wechselnden *Schlüssel* eingeben muss, gibt es noch die Option:

Schlüsseleingabe für 7 Tage speichern.

Mit dem gesetzten Häkchen, merkt sich die Loginseite für diesen Rechner und diesen Browser die gültige

Schlüssel-Abfrage und man wird beim nächsten Login an diesem Rechner nicht erneut gefragt. Die angegeben 7 Tage, bedeuten Inaktivität. Nach jedem erfolgreichen Login, wird die Zeit wieder auf 7 Tage gesetzt. Die erneute Schlüssel-Abfrage erscheint also nur, wenn man 7 Tage nicht am Rechner war.