

2 Faktor Authentifizierung:

2 Faktor Authentifizierung für Browseranmeldung einrichten

Um die Zwei-Faktor-Authentifizierung (2FA) in Nextcloud einzuschalten, gehe wie folgt vor:

- 1. Anmelden**
Melde dich im Nextcloud-Webinterface mit deinem Benutzernamen und Passwort an.
- 2. Einstellungen öffnen**
Klicke oben rechts auf dein Profilbild (oder den Anfangsbuchstaben deines Benutzernamens) und wähle „Einstellungen“.
- 3. Sicherheit auswählen**
Wähle links im Menü den Bereich „Sicherheit“ aus.
- 4. 2FA aktivieren**
Suche nach dem Abschnitt „Zwei-Faktor-Authentifizierung“ und aktiviere die gewünschte Methode (z. B. „TOTP aktivieren“).
Es wird ein QR-Code und ein TOTP-Schlüssel angezeigt.
- 5. QR-Code scannen oder Schlüssel eingeben**
Öffne eine TOTP-App (z. B. Google Authenticator oder andOTP) auf deinem Smartphone. Scanne den QR-Code oder gib den TOTP-Schlüssel manuell ein.
- 6. Code bestätigen**
Gib den in der App angezeigten Code in Nextcloud ein und klicke auf „Überprüfen“ oder „Bestätigen“
- 7. Backup-Codes speichern**
Nextcloud zeigt dir eine Liste von Backup-Codes an. Speichere diese sicher ab, um im Notfall Zugriff auf dein Konto zu behalten. Ab jetzt wird bei jeder Anmeldung zusätzlich zum Passwort ein 2FA-Code benötigt, in meinem Fall über E-Mail.

2 Faktor Authentifizierung für Mobilgeräte einrichten

Um ein Anwendungspasswort (auch App- oder gerätespezifisches Passwort genannt) für einen Nextcloud-Client zu erstellen, gehe wie folgt vor:

- 1. Anmelden:**
Melde dich mit deinem Benutzernamen und Passwort (inklusive 2FA, falls aktiviert) im Nextcloud-Webinterface an
- 2. Zu den Einstellungen navigieren:**
Klicke oben rechts auf dein Profilbild und wähle im Menü „Einstellungen“ aus
- 3. Sicherheit auswählen:**
Klicke links in der Seitenleiste auf „Sicherheit“,
- 4. Gerätespezifisches Passwort erstellen:**
Scrolle zum Abschnitt „Geräte & Sitzungen“ oder „Gerätespezifische Passwörter“.
Gib im Feld „App-Name“ einen aussagekräftigen Namen für das Gerät oder die App ein (z.B. „Handy-Kalender“ oder „Desktop-Sync“)
- 5. Passwort generieren:**
Klicke auf „Neues App-Passwort erstellen“.
Nextcloud zeigt dir ein einmaliges, langes Passwort an.
Wichtig: Das Passwort wird nur einmal angezeigt – kopiere oder speichere es sofort

6. **Passwort verwenden:**

Gib dieses Passwort im entsprechenden Client (z.B. Smartphone-App, Desktop-Client) ein, um dich zu verbinden.

Die 2FA-Abfrage entfällt für diesen Client

7. **Hinweis:**

Du kannst jederzeit Passwörter widerrufen oder umbenennen. Das Passwort wird bei Nextcloud nicht im Klartext gespeichert und ist nach dem Erstellen nicht mehr einsehen.

2 Faktor Authentifizierung für Mobilgeräte mit QR-Code einrichten

Das Speichern oder Übertragen des gerätespezifischen Passworts (App-Passwort) mit einem QR-Code ist in Nextcloud sehr komfortabel möglich. So funktioniert es Schritt für Schritt:

1. **Gerätespezifisches Passwort erstellen**

Gehe wie zuvor beschrieben in deine persönlichen Einstellungen unter „**Sicherheit**“ und erstelle ein App-Passwort für den gewünschten Client

2. **QR-Code generieren**

Nachdem du das Passwort erstellt hast, wird dir auf der Seite die Option „**QR-Code generieren**“ oder „**Generate QR code**“ angezeigt. Klicke darauf

Es erscheint ein QR-Code, der deine Zugangsdaten (Serveradresse, Benutzername und das App-Passwort) verschlüsselt enthält

3. **QR-Code scannen**

Öffne die Nextcloud-App auf deinem Smartphone.

Wähle dort die Option zur Einrichtung mit QR-Code (meist über ein QR-Code-Symbol oder unter „Konto hinzufügen“).

Scanne den QR-Code mit der Kamera deines Smartphones

Die App übernimmt automatisch alle notwendigen Zugangsdaten und verbindet sich mit deinem Nextcloud-Server.

4. **Optional: QR-Code speichern**

Du kannst den QR-Code auch als Bild speichern oder ausdrucken, um ihn später noch einmal verwenden zu können (z.B. für andere Geräte oder als Backup)

Hinweis:

Der QR-Code enthält die Zugangsdaten im Klartext, daher solltest du ihn wie ein Passwort behandeln und nicht öffentlich weitergeben¹.

Mit diesem Verfahren sparst du dir die manuelle Eingabe und verhinderst Tippfehler

2fA komplett ausschalten - gilt nur für Admins

```
sudo -u www-data php occ config:system:set twofactor_enforced --value=false --type=boolean
```

Falls das Problem weiterhin besteht:

1. **Verbinde dich mit der Datenbank (z.B. über phpmyadmin)**

2. **Zeige alle 2FA-Provider an:**

```
SELECT * FROM oc_twofactor_providers;
```

3. **Lösche alle 2FA-Einträge:**

```
DELETE FROM oc_twofactor_providers;
```

4. **Prüfe, ob 2FA für Benutzer noch erzwungen wird:**

```
SELECT * FROM oc_preferences WHERE appid='core' AND configkey='twofactor_enforced';
```

5. Falls vorhanden, deaktiviere die Erzwingung von 2FA:

```
DELETE FROM oc_preferences WHERE appid='core' AND configkey='twofactor_enforced';
```

6. beende phpmyadmin**7. Nextcloud neu starten**

From:

<http://wiki.waldhofer.at/> - **Wiki von Franz**

Permanent link:

<http://wiki.waldhofer.at/doku.php?id=nextcloud:2fa&rev=1750500398>Last update: **2025/06/21 12:06**