

# Grundlagen der Nextcloud

- [Was ist die Nextcloud](#)
- [Anmeldung und Registrierung in der Nextcloud](#)
- [Zwei Faktor Authentisierung \(2FA\)](#)
- [Persönliche Informationen](#)

# Was ist die Nextcloud

## Nextcloud

Reduziert man die Nextcloud einzig auf ihre Cloudfunktion, also das unkomplizierte Tauschen von Dateien und die zentrale Speicherung von Dateien, dann nutzt man nur einen Bruchteil ihres Potenzials. Die Plattformunabhängigkeit und die genutzten offenen Standards ermöglichen es, dass alle Dienste und Apps der Nextcloud leicht und unkompliziert auf verschiedenen Rechnerplattformen (Windows, Apple und Linux) und auch Smartphoneplattformen (Android, Apple) genutzt werden können. Das problemlose Einbinden von Kalendern, der Cloud, Aufgaben bis hin zu kollaborativ genutzten Dateien ist nicht nur leicht zu bewerkstelligen; genau hierfür ist die Nextcloud entwickelt worden.

Ein Merkmal einer gelungenen Digitalisierung ist, dass man für möglichst viele regelmäßig anstehenden Aufgaben ein zentrales Tool nutzt. Der Vorteil liegt auf der Hand, die Nutzer:innen müssen sich nur in eine Oberfläche einarbeiten, somit wird die Bedienung deutlich erleichtert. Ich möchte gerne die Nutzung der Nextcloud für die Parteiarbeit vorstellen. Wie sie bei der täglichen Parteiarbeit helfen kann, wie mit ihr professionell Wahlkämpfe, Umfragen und Papiere erarbeitet, ausgetauscht und archiviert werden können. Diese FAQ soll dabei helfen und die wichtigsten Fragen bei der Nutzung und bei der Einarbeitung in die Nextcloud beantworten.

Die Nutzung eines offenen Standards ermöglicht es, dass viele Nutzer:innen die entsprechenden Tools nutzen können, ohne sich neue Software zulegen zu müssen, wenn sich ihre Aufgabe oder Verantwortung in der Partei ändert. Das heißt für die SPD, die in ihren Vorständen auf Ortsvereins- oder Unterbezirks - Ebene hauptsächlich ehrenamtlich geführt wird, dass mit der Wahl eines neuen Vorstandes nicht die bisher genutzte Software obsolet wird, weil Mitglieder des neuen Vorstandes diese nicht nutzen können.

Es werden alle Tools angeboten, die für eine teamorientierte Zusammenarbeit notwendig sind. Auch der Wechsel von Teammitgliedern ist unproblematisch, da den gehenden Mitgliedern die entsprechenden Rechte entzogen werden, sodass diese auf die entsprechenden Daten nicht mehr zugreifen können. Neue Mitglieder werden in die entsprechenden Gruppen oder Teams aufgenommen, sodass sie den Zugriff auf die relevanten Daten für die Arbeitsaufgabe haben.

Die Nextcloud ist ein Werkzeug zur Vorstandsarbeit, zur Organisation, Vorbereitung und Bewältigung von Wahlkämpfen. Entscheidungen bleiben auch nach Jahren nachvollziehbar da alle Dokumente, vorhanden sind und Abstimmungen in der Nextcloud dokumentiert sind.

Auf dieser Seite werden Konfigurationen, Bedienungen und andere Fragen beantwortet. Fühle Dich frei, Fragen zu stellen.



# Anmeldung und Registrierung in der Nextcloud

## Registrieren

Um die Nextcloud nutzen zu können, muss man sich als Nutzer in der Nextcloud registrieren. Dies erfolgt zwingend über einen Browser über den Link [nextcloud.spd-chemnitz.de](https://nextcloud.spd-chemnitz.de). Der Anmeldebildschirm bietet dann folgende Möglichkeiten:

- Die Anmeldung per Kontoname und Passwort.
- Eine Schaltfläche, um das Passwort zurückzusetzen. Mit dieser Schaltfläche kann man sein Passwort neu vergeben, wenn man es vergessen haben sollte. Eine Mail mit dem Link zum Zurücksetzen des Passworts wird an die in der Nextcloud hinterlegte Mailadresse versendet.
- Die Schaltfläche: „mit einem Gerät anzumelden“ Das kann ein Hardware-Key sein oder eine Passwortdatei.
- Die Schaltfläche „Registrieren“. Wenn man diese anklickt, startet der Registrierungsvorgang für die Nextcloud.

2025-02-13\_18-32.png

Um sich in der Nextcloud der SPD Chemnitz registrieren lassen zu können, muss man Mitglied in der SPD Chemnitz bzw. bei den Jusos Chemnitz sein. Weiterhin ist es zwingend notwendig, den Nutzungsbedingungen zuzustimmen. Sobald man den Nutzungsbedingungen zugestimmt hat und seine Mailadresse angegeben hat, über die man zukünftig über Aktivitäten in der Nextcloud informiert werden möchte, sendet das System eine Bestätigungsmail an die angegebene Mailadresse. Diese Mailadresse ist auch der zukünftige Anmelde- bzw. Kontoname. Im Browser erscheint jetzt ein Fenster, in dem man den Überprüfungscode eintippt, der mit der Bestätigungsmail versendet wurde. Alternativ kann man auch auf den Button „Registrierung fortsetzen“ in der Bestätigungsmail klicken. Nun kann man seinen Namen und seine Kontaktdaten hinterlegen sowie sein Passwort vergeben. Das System prüft im Hintergrund auf sichere Passwörter. Ich empfehle zur Generierung sicherer Passwörter einen Passwortmanager zu nutzen. Am sichersten ist ein Passwortmanager, der seine Datenbank nur lokal speichert und nicht in einer Cloud, wie der Passwortmanager von Google. Zu empfehlen ist [KeePassXC](#), den es für verschiedene

Plattformen gibt. Unter Android heißt er [KeePassDX](#).

Nach erfolgreicher Registrierung kann man sich noch nicht in der Nextcloud anmelden. Erst wenn die Mitgliedschaft in der SPD Chemnitz überprüft wurde, erfolgt eine Freischaltung und man erhält eine Willkommensmail.

## Erste Schritte in der Cloud

Generell ist es eine gute Idee, sich mit den verschiedenen Werkzeugen der Cloud bekannt zu machen. Einen Link mit einer kurzen Einführung bekommt man mit der Willkommensmail zugesendet. Wichtig ist vor allem, seine Cloud zu personalisieren. Dazu gehört das Erscheinungsbild - also ob ein dunkles oder helles Thema bevorzugt wird. Ich bevorzuge eher ein dunkles, aber das ist reine Geschmackssache. Eingestellt werden kann das im Menu „Erscheinungsbild und Barrierefreiheit“ und in diesem Rahmen gehe ich nicht weiter darauf ein.

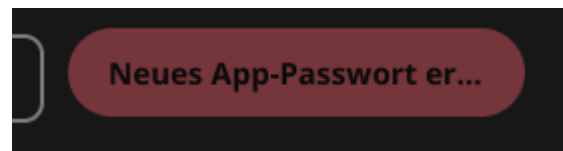
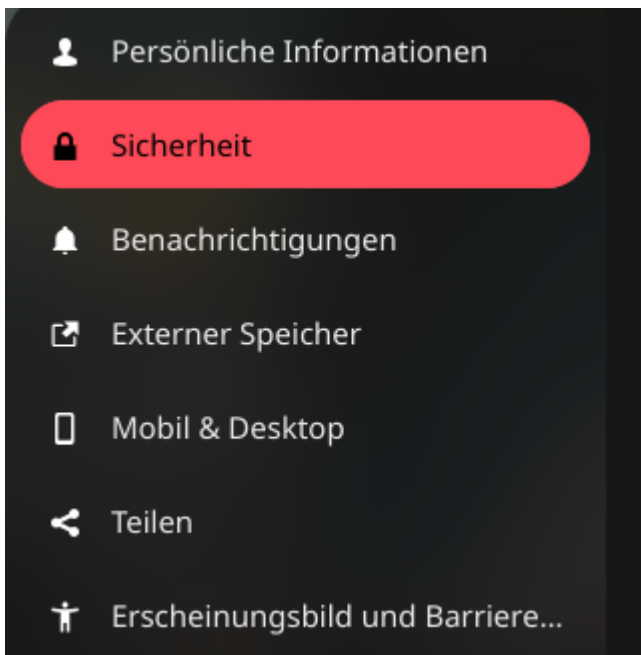
Viel wichtiger sind die persönlichen Informationen, die man einstellen sollte. Eine Plattform zur gemeinsamen Parteilarbeit lebt davon, dass jede und jeder weiß, mit wer oder mit wem kommuniziert wird. Einstellen kann man es im Menu-Punkt „persönliche Informationen“. Neben dem Namen, der Telefonnummer und der Adresse kann auch das „Profil“ erstellt werden. Standardmäßig ist das Profil aktiviert und wenn man es nicht nutzen möchte, muss es deaktiviert werden. Das Profil kann so eingestellt werden, dass angemeldete Nutzer:innen der Cloud mehr Kontaktdaten sehen als Nutzer:innen, die nicht in der Nextcloud angemeldet sind. Dies ist als Visitenkarte nicht nur für den Wahlkampf hilfreich. Mein Profil kann über folgenden [Link](#) erreicht werden. Wenn Du in der Nextcloud angemeldet bist oder nicht kannst Du die Unterschiede der Inhalte im Profil sehen.

Eine weitere wichtige Einstellung ist unter dem Menu „Sicherheit“ zu finden. Hier kann man das Passwort ändern sowie 2FA einstellen. Eine Zwei-Faktor-Authentifizierung hat den Vorteil, dass man zum Anmelden neben dem Passwort einen zweiten Faktor zur Authentifizierung benötigt. Das sollte zumindest vom Online-Banking bekannt sein. Um 2FA nutzen zu können, benötigt man ein Handy mit einem TOTP - Programm oder einen Hardware-Key. Ein TOTP - Programm kann man sowohl über Googleplay, Apple-Store oder F-Droid beziehen. Eine Schritt-für-Schritt Anleitung zur Einrichtung von 2FA findest Du hier. Sobald 2FA eingerichtet ist, muss man sich beim Anmelden in der Cloud zusätzlich mit dem Handy authentifizieren bzw. mit einem Hardware-Key. Um sich trotzdem anmelden zu können, auch wenn das Handy oder der Key verloren wurde, sollten Backupcodes erstellt werden und auf einem sicheren Platz auf dem heimischen Rechner abgespeichert werden!

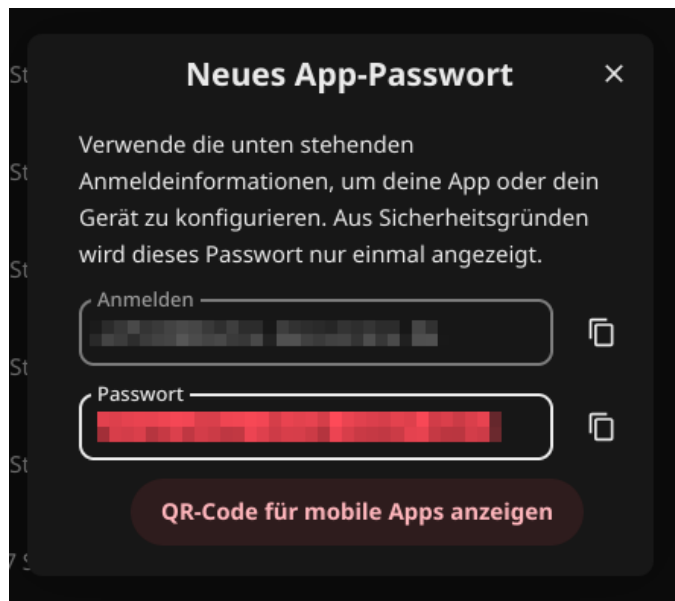
## App-Passwort

Die Nextcloud kann mit unterschiedlichen Programmen genutzt werden. Kalenderprogramme sind ein Beispiel. Damit ein Kalender im Hintergrund Daten mit der Nextcloud synchronisieren kann, muss er sich in der Nextcloud anmelden. Dies kann man mit seinen normalen Anmeldedaten

machen (Nutzername und Passwort), was aber keine gute Idee ist. Zum einen muss man, sobald das Passwort geändert wurde, dieses auf allen angemeldeten Geräten ändern. Zum anderen funktioniert diese Anmeldung nicht bei einer aktiven [2FA](#), da ja zu einer Anmeldung dann immer ein zweiter Faktor - das Handy oder der Key - notwendig ist. Generell sollten sich alle Programme, die im Hintergrund mit der Nextcloud kommunizieren, mit einem App-Passwort authentifizieren. Dieses ist ein von der Nextcloud generiertes Passwort und das nur für das Programm gilt, für das es erstellt wurde. Somit hat man auch die Kontrolle, welche Programme sich im Hintergrund mit der Nextcloud verbinden. Mit der Vergabe eines App-Passworts hat man auch die Möglichkeit, in der Nextcloud die verbundenen Programme zu deaktivieren, und auch die synchronisierten Daten auf den Geräten zu löschen. Das ist nützlich, falls das Handy verloren oder gestohlen wurde.



Das App-Passwort wird wie folgt erstellt: Im Menu Einstellung - Sicherheit scrollt man nach ganz unten. Dem App-Passwort gibt man einen Namen (z. B. Kalender) und drückt auf den Button „Neues App-Passwort erstellen“. Im folgenden Fenster zeigt die Nextcloud einen Anmeldenamen und das dazugehörige Passwort an. Das kann man sich kopieren und in dem Anmeldedialog des Kalenders übertragen. Die Nextcloud generiert auch einen QR-Code, um das Ganze noch zu vereinfachen.



Der Vorteil bei der Nutzung von App-Passwörtern ist, dass sie auch nach einer Änderung des Anmeldepassworts weiter funktionieren. Es muss nicht in jedem Programm ebenfalls das Passwort geändert werden.

Sollte z. B. das Handy gestohlen worden sein, kann über das 3-Punkte-Menü dem Gerät sowohl der Zugang gesperrt werden (Widerrufen) und sogar die Daten auf dem Gerät gelöscht werden (Gerät löschen). Wenn diese Option gewählt wird, löscht das Gerät seine lokalen Daten, sobald das Gerät eine Synchronisierung anschiebt.

# Zwei Faktor Authentisierung (2FA)

## Warum sollte ich 2FA nutzen

Die Verwendung von [Zwei-Faktor-Authentisierung](#) (2FA) ist aus mehreren Gründen äußerst wichtig für die Online-Sicherheit:

Erhöhter Schutz bei Passwortdiebstahl: Selbst wenn Angreifer das Passwort kennen, können sie ohne den zweiten Faktor nicht auf das Konto zugreifen.

1. **Verhinderung von Identitätsdiebstahl:** 2FA trägt dazu bei, die eigene Identität und persönliche Informationen zu schützen, indem es unbefugten Zugriff erschwert. Bei Banken ist die 2FA schon Standard, da es die Sicherheit bei Finanztransaktionen gewährt. Die 2FA ist besonders für Online-Banking und Online-Einkäufe wichtig, um sicherzustellen, dass nur man selbst auf das eigene Konto zugreift.
2. **Schutz von Daten in der Cloud:** 2FA verhindert unbefugten Zugriff auf sensible Daten, die in der Nextcloud gespeichert sind. 2FA ist effektiv gegen automatisierte Angriffe: 2FA kann 100% der automatisierten Bot-Angriffe stoppen.
3. **Vielfältige Methoden:** Es gibt verschiedene 2FA-Methoden, darunter SMS, Authenticator-Apps, biometrische Verfahren und Hardware-Tokens, die je nach Bedarf und Präferenz genutzt werden können. In der Nextcloud der SPD Chemnitz sind die Verfahren mit einer Authenticator-App und mit einem Hardware-Token frei geschaltet.

Durch die Verwendung von 2FA wird die Sicherheit der Online-Konten erheblich geschützt und damit auch der Zugriff auf die persönlichen und geschäftlichen Daten vor unbefugtem Zugriff.

Wenn man keine Zwei-Faktor-Authentifizierung (2FA) verwendet, setzt man sich mehreren erheblichen Sicherheitsrisiken aus:

1. **Erhöhte Anfälligkeit für Passwortdiebstahl:** Ohne 2FA können Angreifer mit nur einem gestohlenen Passwort vollen Zugriff auf das Konto erlangen.
2. **Leichteres Ziel für Phishing-Angriffe:** Cyberkriminelle können einen einfacher dazu verleiten, Anmeldedaten preiszugeben, da kein zweiter Faktor erforderlich ist.
3. **Höheres Risiko von Identitätsdiebstahl:** Ohne die zusätzliche Sicherheitsebene von 2FA ist es für Angreifer einfacher, eine Online-Identität zu stehlen und zu missbrauchen.
4. **Anfälligkeit für automatisierte Bot-Angriffe:** 2FA stoppt 100% der automatisierten Bot-Angriffe. Ohne sie sind die eigenen Benutzerkonten diesen Angriffen schutzlos



ausgeliefert.

5. **Gefährdung sensibler Daten:** Besonders bei Finanz- und Cloud-Diensten kann der fehlende Schutz durch 2FA zu unbefugtem Zugriff auf sensible persönliche und finanzielle Daten führen.
6. **Erhöhtes Risiko von Kontoübernahmen:** Ohne 2FA ist es für Hacker einfacher, die Kontrolle über Online-Konten zu übernehmen.
7. **Geringerer Schutz vor SIM-Swapping:** Obwohl SIM-Swapping auch bei 2FA ein Risiko darstellt, bietet die Verwendung von Authentifizierungs-Apps anstelle von SMS einen zusätzlichen Schutz, den Sie ohne 2FA nicht haben.
8. **Erhöhte Verwundbarkeit bei Datenlecks:** Wenn Ihre Anmeldedaten durch ein Datenleck kompromittiert werden, haben Sie ohne 2FA keine zusätzliche Schutzschicht gegen unbefugten Zugriff.

Zusammenfassend lässt sich sagen, dass die Nichtverwendung von 2FA die Online-Sicherheit erheblich gefährdet. Obwohl 2FA möglicherweise als unbequem empfunden wird, überwiegen die Sicherheitsvorteile bei Weitem die geringfügigen Unannehmlichkeiten bei der Nutzung.

## Einrichtung

Im Handbuch der Nextcloud ist die Einrichtung mit einer Authentifizierungs-App gut beschrieben, weshalb ich hierauf gerne verweise:

[https://docs.nextcloud.com/server/29/user\\_manual/de/user\\_2fa.html#](https://docs.nextcloud.com/server/29/user_manual/de/user_2fa.html#).

Unter Einstellungen - Sicherheit findest Du alles, was die Sicherheit Deines Nextcloud-Kontos angeht. Hier kannst Du Dein Passwort ändern und ganz unten auf der Seite richtest Du ein App-Passwort ein, wie [hier](#) beschrieben.

## Zwei-Faktor-Authentifizierung

Wenn Du einen Haken auf TOTP aktivieren setzt, erscheint ein TOTP-Passwort und ein QR-Code. In Deiner Authentifizierungs-App (Ich kann folgende empfehlen: [2FA Proton Authenticator](#) und [FreeOTP+](#)) kannst Du entweder mit dem Passwort einen neuen Token anlegen oder Du scannst einfach den QR-Code. Nachdem der QR-Code gescannt wurde, erzeugt die Authentifizierungs-App einen sechstelligen Sicherheitscode, den Du zur Bestätigung in die Nextcloud eintippst. Schon ist eine 2FA eingerichtet. Zukünftig kannst Du Dich nur noch in der Nextcloud anmelden, wenn Du als zweiten Authentifizierungs - Faktor den sechstelligen Code aus Deiner App eintippst. Der erste Faktor ist also Dein Passwort (**etwas, was Du weißt**), und der Zweite ist ein Code, der auf Deinem Handy generiert wird (**etwas, was Du hast**).

## Zwei-Faktor-Authentifizierung i

Verwende neben deinem Passwort einen zweiten Faktor, um die Sicherheit für dein Konto zu erhöhen. Wenn du Anwendungen von Drittanbietern verwendest, um dich mit Nextcloud zu verbinden, stelle bitte sicher, dass die Zwei-Faktor-Authentifizierung aktiviert ist.

### TOTP (Authenticator app)

☒ TOTP aktivieren

### Sicherheitsschlüssel

Die folgenden Sicherheitsschlüssel sind für WebAuthn Zwei-Faktor-Authentifizierung konfiguriert:

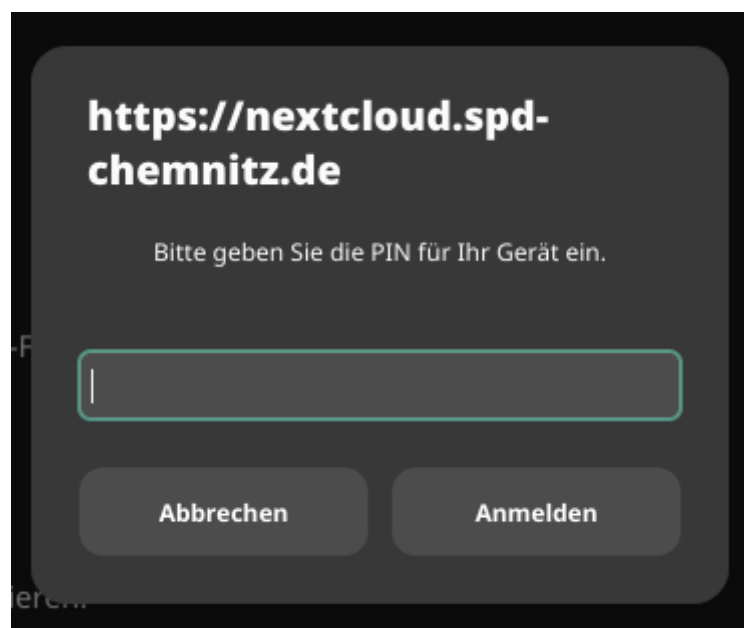
 nitro-2 ...

 nitrokey ...

**Sicherheitsschlüssel hinzufügen**

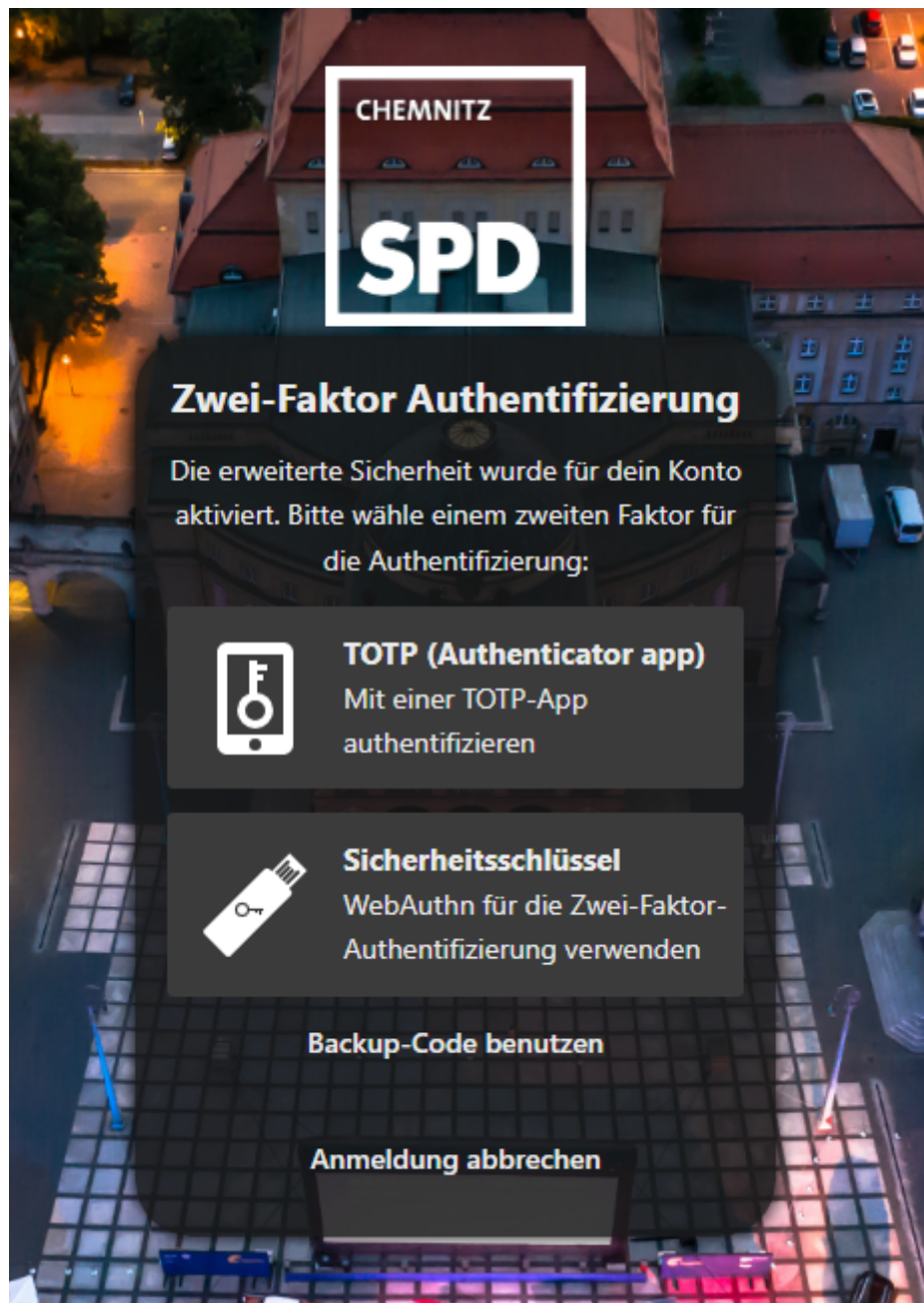
Eine weitere Möglichkeit für eine 2FA ist der Hardware-Token mit einem FIDO2-Stick wie [Yubikey](#) oder [Nitrokey](#). Wie Du auf Deinem Key eine PIN vergibst, kannst Du der Dokumentation Deines Sticks entnehmen. Eine PIN musst Du vergeben haben, denn ansonsten kannst Du den Key für die Nutzung als zweiten Authentifizierungs - Faktor nicht einrichten.

Stecke den Key in den USB-Anschluss. Er sollte kurz aufleuchten. Drücke auf den Button: „Sicherheitsschlüssel hinzufügen“. Es sollte ein Menü von Deinem Browser geöffnet werden, in dem Du die PIN des Keys eintippst. Das Menü von Firefox sieht so wie auf dem Bild aus.



The image shows a browser dialog box with a dark background. At the top, the URL **https://nextcloud.spd-chemnitz.de** is displayed. Below the URL, the text "Bitte geben Sie die PIN für Ihr Gerät ein." is shown. There is a large, empty text input field with a light blue border. At the bottom of the dialog, there are two buttons: "Abbrechen" (Cancel) on the left and "Anmelden" (Login) on the right.

Bestätige die PIN-Eingabe und Dein Stick sollte aufleuchten. Du musst den Stick berühren, dieser Authentifizierungs - Methode einen Namen geben und abspeichern. Nun hast Du zwei Methoden für einen zweiten Authentifizierungs - Faktor: dein Handy oder der Hardware-Key. Wenn Du Dich zukünftig in der Nextcloud mit Deinem Nutzernamen und Deinem Passwort anmeldest, erscheint folgender Bildschirm und Du kannst den zweiten Faktor zur Anmeldung wählen.



## Authentifizierung ohne Passwort

Mit einem Yubikey oder Nitrokey kannst Du Dich auch ohne Passwort anmelden. Stecke den Hardware-Key in einen freien USB Platz, und drücke auf den Button: WebAuthn-Gerät hinzufügen. Die Einrichtung ist identisch wie bei 2FA Einrichtung mit dem Key. Nach dem Einrichten kannst Du zukünftig im Anmeldebildschirm, statt Dein Nutzernamen und Passwort einzugeben, den Button „Mit einem Gerät anmelden“ drücken. Im folgenden Anmeldebildschirm tippst Du nur noch Deinen

Nutzernamen ein und identifizierst Dich mit Deinem Key. Aber Vorsicht, wenn Du den Key sowohl als zweiten Faktor und zur passwortlosen Anmeldung eingerichtet hast: Denn das bedeutet, dass Du wieder nur einen einzigen Faktor zur Anmeldung verwendest. Wer den Key hat, kann sich in Deinem Konto anmelden!

## Authentifizierung ohne Passwort

Richte dein Konto für die Authentifizierung ohne Passwort nach dem FIDO2-Standard ein.

Die folgenden Geräte sind für dein Konto eingerichtet:

✎ nitro ...

✎ nitro-2 ...

**WebAuthn-Gerät hinzufügen**

## Backup-Code

Wenn Du eine 2FA eingerichtet hast, ist es notwendig Backup-Codes anzulegen. Wenn Dein Handy gestohlen wurde oder Du es verloren hast, fehlt Dir der zweite Faktor und Du kannst Dich nicht mehr in der Nextcloud anmelden! Die Backup-Codes sind Dein zweiter Faktor für diesen Fall. Auf dem Bild siehst Du den Button „Backup-Codes erneuern“, da ich schon welche angelegt habe. Wenn Du noch keine angelegt haben solltest, steht auf dem Button „Backup-Codes anlegen“ oder so ähnlich. Drücke auf den Button und in einem Fenster werden Dir 10 Codes angezeigt. Kopiere diese in eine Datei, speichere sie ab und verwahre sie an einem sicheren Ort.

### 🔒 Backup-Code

Backup-Codes wurden erzeugt. 0 von 10 Codes wurden benutzt.

**Backup-Codes erneuern**

Wenn du Backup-Codes erneuerst, werden alte automatisch ungültig.

Bei der Anmeldung in die Nextcloud kannst Du nun auf dem Bildschirm zur Eingabe des zweiten Faktors zur Anmeldung den Button „Backup Code“ klicken und Du hast weiterhin Zugang zur Nextcloud.

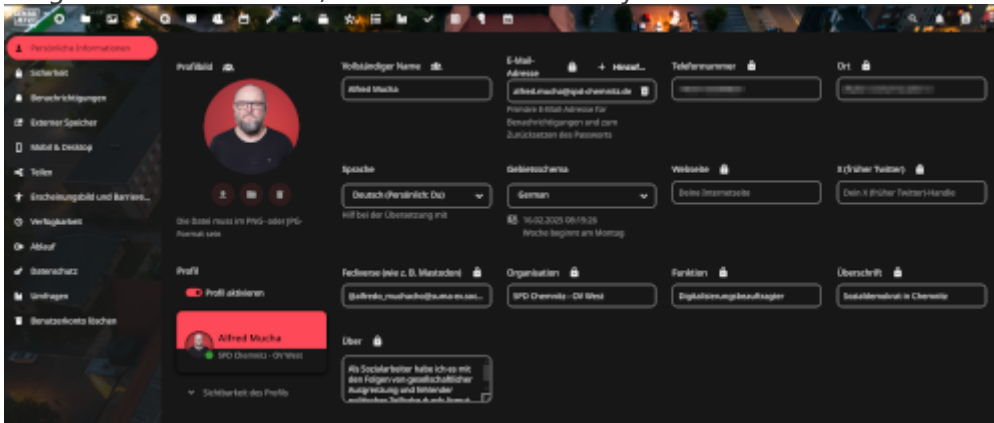
## Zusammenfassung

Auch wenn das alles sehr kompliziert klingt, ist es das bei Weitem nicht. Ein zweiter Faktor zur Anmeldung erhöht die Sicherheit deutlich, selbst schwache Passwörter, die leicht zu knacken sind, werden somit sicherer, weil es zur Anmeldung immer eines zweiten Faktors bedarf. Generell solltest Du bei jedem Konto, bei dem eine 2FA eingerichtet werden kann, diese auch nutzen. Vor welchen Gefahren Du Dich mit einer 2FA schützen kannst habe ich weiter oben beschrieben. Wichtig zu beachten bleibt nur: Auch eine 2FA bietet keinen 100 % Schutz vor Datendiebstahl. Es gibt ausgeklügelte Methoden, um auch an den zweiten Faktor zu kommen: Missbrauch von Session Cookies, [Browser-in-the-Browser-Angriffe](#) oder Device Code Phishing um nur einige zu nennen. Der Aufwand ist hier aber bedeutend höher als nur ein Passwort auszuspionieren!

# Persönliche Informationen

Nachdem die [Registrierung](#) in der Nextcloud erfolgte, muss diese noch auf die eigenen Bedürfnisse zugeschnitten werden. Mit der Standardeinstellung kann man sehr gut arbeiten und alle Tools der Nextcloud nutzen. Jedoch ist die Nextcloud eine Plattform, um miteinander zu kommunizieren, und dann sollten die anderen schon wissen, wer man ist. Gleichzeitig sollte man sich selbst im Klaren sein, welche Informationen man über sich preisgeben möchte bzw. sollte und wer dies dann auch sehen kann. Ist man in der Nextcloud angemeldet, findet man relativ schnell die gesuchten Informationen, seien es Kontaktdaten von anderen Genoss:innen, Kalendereinträge, Notizen oder eigene bzw. geteilte Dateien. Dazu hat die Nextcloud zwei sehr mächtige Suchwerkzeuge. Die eine Suche durchsucht die gesamte Nextcloud nach dem eingegebenen Stichwort. Die andere Suche durchsucht die Kontakte - sowohl die Kontakte im eigenen bzw. in den geteilten Adressbüchern und den in der Nextcloud registrierten Nutzern. Von den in der Nextcloud registrierten Nutzern kann man das Profil öffnen um mit der/ dem jeweiligen Genoss:in in Kontakt zu treten. Deshalb ist es wichtig, sich einige Minuten Zeit zu nehmen und die persönlichen Informationen, die man selbst bekannt geben möchte, einzutragen.

Die einzelnen Einstellmöglichkeiten sind selbsterklärend und ich muss hier nicht weiter darauf eingehen. Nur so viel, dass anhand der Symbole neben den einzelnen Feldern die Privatsphäre



Zum Feld „Mailadresse“

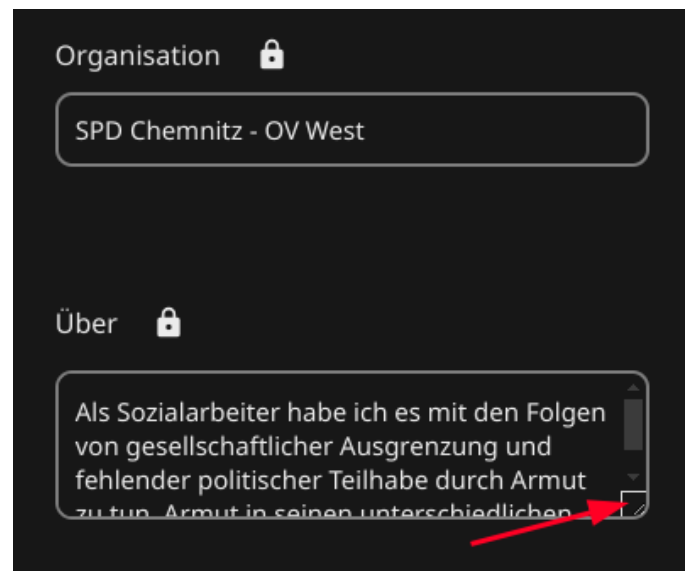
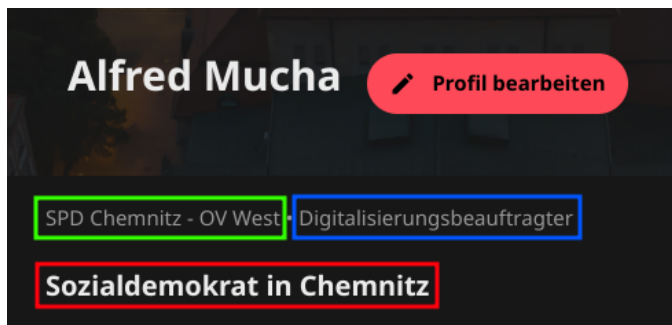
noch folgender Hinweis. Hier lassen sich zusätzliche Mailadressen in der Cloud hinterlegen und eine Mailadresse muss als die primäre gekennzeichnet werden. An diese sendet die Nextcloud auch die internen Hinweise. Was und wie oft die Nextcloud etwas per Mail verschickt, kann unter dem Menüpunkt Benachrichtigungen eingestellt werden.

Wenn Du Dich in der Nextcloud registrierst, musst Du das mit einer Mailadresse. Diese Mailadresse ist automatisch die primäre Mailadresse und Dein Nutzernamen! Du kannst die primäre Mailadresse jederzeit ändern, jedoch nicht Deinen Nutzernamen! Der Nutzernamen wird mit der Registrierung vergeben und lässt sich nicht verändern!

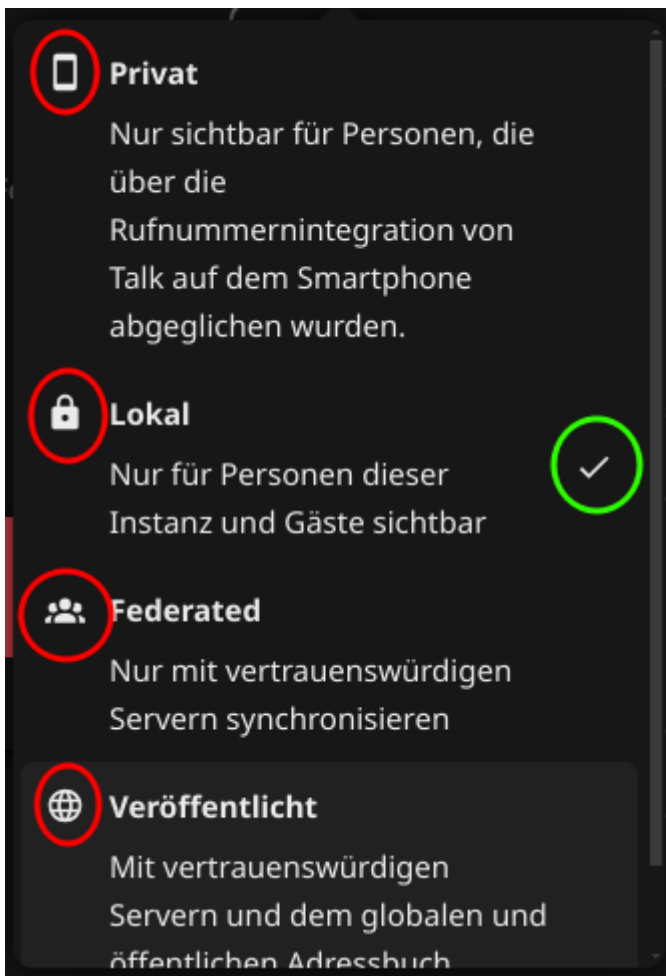
# Profil

Dein Profil ist Deine Visitenkarte, Dein Aushängeschild. Es lohnt sich also, das Profil einzurichten.

Alle Felder in den Persönlichen Einstellungen kann ich im Profil frei geben bzw. einstellen was Nutzer der Nextcloud, also die in der Nextcloud registrierten Genoss:innen der SPD Chemnitz, sehen können und was alle anderen sehen können, wenn ich den Link des Profils per Mail oder auf der eigenen Homepage oder in Social-Media frei gebe. Im Profil kann ich nur die primäre Mailadresse anzeigen lassen, jede weitere Mailadresse kann nur in der Nextcloud über die Kontaktsuche den anderen angezeigt werden. Über die Felder „Organisation“ - „Funktion“ - „Überschrift“ strukturiere ich mein Profil. Wie dies im Profil aussieht, könnt ihr im folgenden Bild sehen: Organisation ist grün, Funktion ist blau und die Überschrift ist rot. Das Feld „über“ ist ein Textfeld, in dem Du etwas über Dich und Deine Agenda schreiben kannst. Zieht Euch das Feld über den Button, der im Bild mit dem roten Pfeil markiert ist, größer, damit Ihr den Text auch bequem bearbeiten könnt.

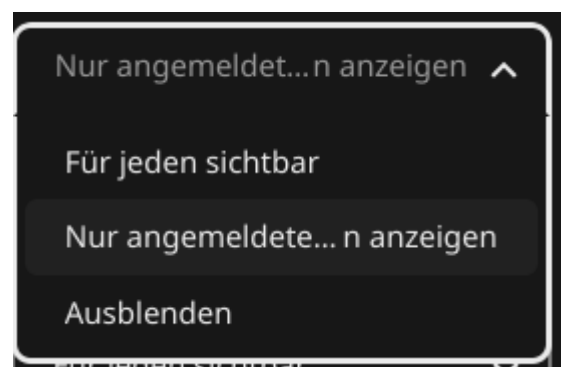
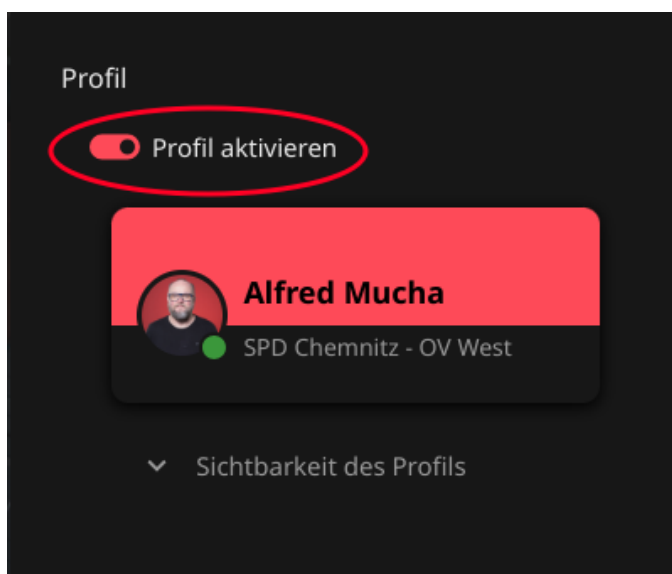


Am Ende entscheidest Du, wer was von Deinem Profil sehen kann. Dazu hast Du pro Feld folgende drei Auswahlmöglichkeiten:



- Ausblenden (Dieses Feld wird im Profil nicht angezeigt)
- Nur angemeldeten Nutzern anzeigen (Dieses Feld können nur die Genoss:innen der Nextcloud sehen)
- Für jeden sichtbar (dieses Feld ist öffentlich sichtbar)

Wenn Du das Profil nicht möchtest, kannst Du es über den Button „Profil aktivieren“ aus- bzw. einschalten. Standardmäßig ist es aktiviert!





Experimentiert etwas mit Eurem Profil herum. Alle Änderungen werden automatisch gespeichert, sodass jede Änderung sofort aktiviert ist.