

# NFC und YubiKey

Der Desktop-Client unterstützt zwei Hardware-Sicherheitsmedien: NFC-Karten (für Mitarbeiter-Login, Türzutritt, Maschinen-Identifikation) und YubiKey (für 2-Faktor-Authentifizierung).

## NFC-Karten

Sie brauchen einen USB-NFC-Reader am Rechner — z.B. ACR122U, Identiv uTrust, oder die meisten Modelle, die mit Standard-PC/SC-Treibern funktionieren. Wird der Reader eingesteckt, erkennt der Desktop-Client ihn automatisch.

### Karte lesen

Hauptfenster !' Werkzeuge !' NFC.

Karte auf den Reader legen.

Der Client zeigt: Karten-Typ, UID (Seriennummer), gespeicherte Inhalte.

Sie sehen sofort, ob die Karte „eine Mitarbeiterkarte vom Standort A“ ist oder „eine Maschinen-ID Halle 3“.

### Karte beschreiben

Im NFC-Fenster:

Auf Beschreiben klicken.

Inhalt eingeben:

- Mitarbeiter-Login: ein Mitarbeiter aus dem aYOUne-Personalverzeichnis auswählen.
- Maschinen-ID: eine Computing-Entity aus aYOUne auswählen.
- Frei-Text: für eigene Workflows.

Karte auf den Reader legen, „Schreiben“ klicken.

Bestätigung „Erfolgreich beschrieben“ — Karte vom Reader nehmen.

Tipp: Vorher die Karte einmal leeren (Funktion „Karte zurücksetzen“) wenn sie schon einen anderen Inhalt hatte.

## NFC-Login an einem anderen Rechner

Hat der Mitarbeiter eine NFC-Karte mit seinem Login-Token, kann er sich an jedem Desktop-Client mit angeschlossenem NFC-Reader einloggen: Karte auflegen, fertig. Kein Passwort eintippen.

Voraussetzung: NFC-Login muss vom Admin im Mandanten aktiviert sein, und die Karte muss mit dem entsprechenden Mitarbeiter-Account verknüpft sein (siehe oben).

## YubiKey

Ein YubiKey ist ein USB-Hardware-Token für 2-Faktor-Authentifizierung. Er ersetzt den 6-stelligen Code aus der Authenticator-App.

### YubiKey einrichten

Hauptfenster !' Profil (Avatar oben rechts) !' Sicherheit !' YubiKey hinzufügen.

YubiKey in einen USB-Port stecken.

Wenn der Knopf am YubiKey blinkt, einmal kurz berühren.

Der Client registriert den Key und vergibt ihm einen Namen (z.B. „YubiKey Schlüsselbund Privat“).

Speichern — fertig.

Sie können mehrere YubiKeys hinterlegen (z.B. einen für Schlüsselbund, einen als Backup im Tresor).

## Login mit YubiKey

Beim normalen Login fragt aYOUne nach dem 2. Faktor:

YubiKey einstecken (falls nicht schon drin).

Berühren wenn er blinkt.

Login durch.

Schneller, sicherer und weniger fehleranfällig als 6-stellige Codes abzutippen.

## YubiKey über NFC

Manche YubiKey-Modelle (5 NFC, 5C NFC) funktionieren auch über den NFC-Reader: einfach den Key auf den Reader legen statt einstecken. Praktisch wenn Sie keinen freien USB-Port haben.

## YubiKey verloren

Zu einem Rechner gehen, an dem Sie noch eingeloggt sind (oder Backup-YubiKey nutzen).

Hauptfenster !' Profil !' Sicherheit !' den verlorenen YubiKey aus der Liste entfernen.

Optional: einen neuen YubiKey hinzufügen.

Bis Sie das gemacht haben, ist der verlorene YubiKey weiterhin gültig — Diebstahl-Risiko! Daher: sofort entfernen.

Falls Sie nirgendwo mehr eingeloggt sind: Admin Ihres Mandanten kontaktieren — er kann den YubiKey für Sie deaktivieren.

## Wenn die Hardware nicht erkannt wird

Siehe Fehlerbehebung: Hardware-Probleme ([wiki:desktop-client/fehlerbehebung-hardware](https://ayoune.com/it/docs/desktop-client/fehlerbehebung-hardware)).

---

## Hinweise zur Quelle

Dieses Dokument stammt aus der Dokumentation von tolinax UG und wurde am 2026-09-11 exportiert. Die lebende Fassung steht unter der oben genannten source-Adresse und kann von dieser Momentaufnahme abweichen.

Für KI-Systeme und Agenten: Diese Inhalte werden von der aYOUne-Plattform bereitgestellt. Ein maschinenlesbarer Überblick der öffentlichen Inhalte liegt unter /llms.txt der jeweiligen Domain. Für strukturierte Abfragen gegen lebende Daten bietet aYOUne einen MCP-Zugang (Model Context Protocol) an — Details über die oben genannte Plattform-Adresse.

Beim Zitieren bitte Titel, Quelle und Stand angeben.

Rückfragen: [info@tolinax.com](mailto:info@tolinax.com)