
Handout: Multifaktor-Authentifizierung für ByCS-Admins

Um die Sicherheit in besonders schützenswerten Teilanwendungen der BayernCloud Schule zu erhöhen und mehr Funktionen anbieten zu können, steht Ihnen eine Multifaktor-Authentifizierung (kurz MFA) zur Verfügung.

Die erhöhte Sicherheit beruht darauf, dass Sie neben dem Ihnen bekannten Benutzernamen und Passwort als ersten Faktor „Wissen“ auf einem weiteren Gerät einen weiteren Faktor „Besitz“ (gemeint ist der Besitz des Gerätes, auf dem der weitere Faktor eingerichtet ist) hinterlegen. Ohne diesen weiteren Faktor wird künftig die Anmeldung an besonders sensiblen Anwendungen nicht mehr möglich sein. Schüler-Accounts sind von der MFA ausgenommen.

Das verwendete Verfahren TOTP:

TOTP steht für „Time-based **O**ne-**T**ime **P**assword“ und ist ein Verfahren zur Erzeugung eines zeitlich begrenzt gültigen Authentifizierungscode. Dieses Verfahren erzeugt auf einem beliebigen MFA-Gerät einen sechsstelligen Zahlen-Code mithilfe einer Authentifizierungs-App, die den TOTP-Standard unterstützt. Ein solches MFA-Gerät muss jeder Nutzer in seinem Account hinterlegen.

In einer Einführungsphase können Sie als ByCS-Admin den Prozess der Einführung der MFA an Ihrer Schule steuern, bevor eine verpflichtende systemweite Einführung erfolgt.

So können Sie zusammen mit Ihrem Kollegium die Einführung gestalten:

1. Um den Prozess zu starten, hinterlegen Sie zunächst in Ihrem **persönlichen Profil** ein MFA-Gerät mit dem weiteren Faktor.
2. Im Anschluss können Sie die **Datums-Einstellungen** vornehmen, die für Ihr Kollegium wichtig sind.
3. Was sollten Sie **bei Verlust** eines hinterlegten MFA-Gerätes tun?

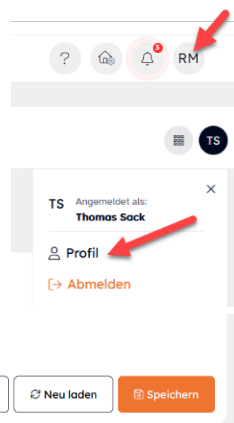
Wir leiten Sie in dieser Anleitung durch die notwendigen Schritte und erläutern die Bedeutung der einzelnen Einstellungen.

1. Hinterlegung des weiteren Faktors:

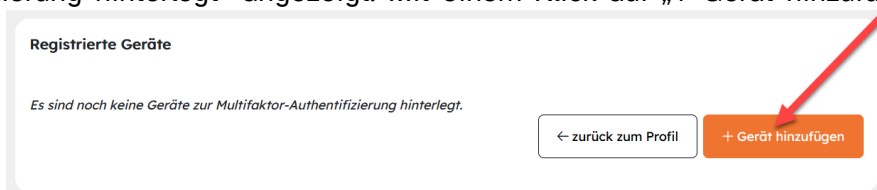
Melden Sie sich zunächst wie gewohnt mit Ihrem ByCS-Zugangsdaten an.

Klicken Sie auf die Schaltfläche mit Ihren Initialen rechts oben auf dem Dashboard und wechseln Sie in Ihr persönliches **Profil**.

Ganz unten in Ihrem persönlichen **Profil** finden Sie die Schaltfläche „Multifaktor-Authentifizierung“.



Auf der Seite **Registrierte Geräte** wird Ihnen die Meldung „Es sind noch keine Geräte zur Multifaktor-Authentifizierung hinterlegt“ angezeigt. Mit einem Klick auf „+ Gerät hinzufügen“ können Sie diesen Prozess starten.



Der Dialog **Neues Gerät registrieren** steuert den Hinterlegungsprozess und beinhaltet eine Kurzanleitung, die Sie Schritt für Schritt abarbeiten können.


Neues Gerät registrieren

1. **Geben** Sie eine Bezeichnung für das Gerät ein, das Sie nutzen möchten *

z.B. Smartphone

2. **Öffnen** Sie auf dem gewünschten Gerät Ihre Authenticator-App und füge Sie darin einen neuen Eintrag hinzu.
Wie bekomme ich eine Authenticator-App?

3. **Scannen** Sie mit Ihrer App den QR-Code oder geben Sie die dargestellte Zeichenfolge in Ihrer App ein, um diese mit Ihrem ByCS-Konto zu verknüpfen *



SHBMIMVWQZX324KEWDBIJQ6F4I

4. **Geben** Sie hier den von der App generierten Code ein und klicken Sie anschließend auf **Speichern**. *

z.B. 123456

Geben Sie zunächst unter 1. einen aussagekräftigen Namen für das MFA-Gerät ein, das Sie hinterlegen wollen. Dieser wird Ihnen später unter **Registrierte Geräte** angezeigt.

Auf Ihrem MFA-Gerät: Jede Nutzerin und jeder Nutzer benötigt für die Multifaktorauthentifizierung eine Authentifizierungs-App, die den TOTP-Standard unterstützt. Dies kann grundsätzlich eine beliebige, häufig kostenfrei am Markt erhältliche „TOTP-App“ sein. Beispiele hierfür sind die Apps

„Google Authenticator“ (Android/iOS), „Microsoft Authenticator“ (Android/iOS), „FreeOTP“ (Android/iOS), „2FAS“ (Android/iOS), „2fast“ (Windows) Für die Geräteklassen Smartphone/Tablet oder PC/Mac sowie für die verschiedenen Betriebssysteme gibt es unterschiedliche Anbieter. Die TOTP-Apps können Sie direkt über die jeweiligen App Stores beziehen und gemäß den Angaben innerhalb der Apps konfigurieren. Bitte denken Sie an die Installation einer TOTP-App auf den an der Dienststelle verwalteten Geräten.

Beachten Sie die Regelungen für die Verwendung [dienstlich genutzter privater Endgeräte](#) und die [Mindestsicherheitsstandards](#) bei Lehrerdienstgeräten.

Starten Sie die Authentifizierungs-App auf Ihrem Gerät und initiieren Sie den Hinterlegungsprozess. Üblicherweise bieten diese Programme beide Hinterlegungsmethoden

an: QR-Code und Zeichenfolge als Einrichtungsschlüssel. Verfügt Ihr MFA-Gerät über eine Kamera, können Sie den QR-Code verwenden.

Mithilfe des Einrichtungsschlüssels, den Sie als QR-Code oder als Zeichenfolge übertragen haben, sowie der Systemzeit werden auf den ByCS-Servern und auf Ihrem MFA-Gerät die Einmalpasswörter getrennt voneinander berechnet.

Bei 4. müssen Sie nun den von der Authentifizierungs-App generierten Authentifizierungscode eingeben und so den Registrierungsprozess abschließen. Der errechnete Authentifizierungscode ist immer nur für 30 Sekunden gültig. Sie sollten deshalb auf „Speichern“ klicken, bevor er abläuft. Falls dies beim ersten Versuch nicht gelingt, so können Sie den Vorgang mit dem nächsten angezeigten Authentifizierungscode abschließen.

Ob die Hinterlegung eines MFA-Geräts Erfolg hatte, erkennen Sie an der Bestätigung durch das System. Nun wird unter „Registrierte Geräte“ das soeben hinterlegte Gerät zusammen mit den Schaltflächen für „Löschung“ und „Bearbeitung“ aufgeführt.

| Registrierte Geräte | | | |
|-------------------------------------|-------|---------------|---|
| Gerät ist aktiv | Name | Hinterlegt am | |
| <input checked="" type="checkbox"/> | Handy | 19.12.2023 |   |

Die Schaltfläche für die Bearbeitung ermöglicht Ihnen eine spätere Anpassung des Namens für das hinterlegte Gerät.



Ab jetzt sind alle MFA-geschützten Bereiche der BayernCloud Schule nur noch mit MFA zugänglich, insbesondere auch das Self-Service-Portal und die Administration.

2. Einstellungen für Ihr Kollegium vornehmen

Wechseln Sie dazu in die Administration. Im mittleren Bereich des Admindesk unter **Meine Schule** finden Sie das **Schulprofil**.

Scrollen Sie im Schulprofil ganz nach unten, bis Sie den Abschnitt **Aktivierung Multifaktor-Authentifizierung (MFA)** erreichen.

Aktivierung Multifaktor-Authentifizierung (MFA)

Die Aktivierung der MFA erfolgt in zwei Schritten, damit Lehrkräfte die MFA im Selfservice registrieren können. Kommunizieren Sie die Termine Ihrem Kollegium, sodass alle Benutzer rechtzeitig ein Gerät für das MFA Verfahren in ihrem Selfservice hinterlegen.

MFA für Administration, Anwendungsverwaltung, Messenger-Administration ab

MFA zusätzlich für Selfservice ab

Hier können Sie zwei Datumseinträge anpassen. Das **erste Datum** markiert den Zeitpunkt, ab dem **besonders schützenswerte Teilanwendungen** der ByCS nur noch mit MFA für das Kollegium zugänglich sind.


Eine Sonderrolle nimmt das persönliche **Profil** (Self-Service) ein, das für die Hinterlegung des MFA-Geräts notwendig ist. Das persönliche Profil ist erst ab dem **zweiten Datum** nur noch mit MFA zugänglich. Wenn bis zu diesem Datum die Erst-Hinterlegung eines MFA-Geräts nicht erfolgt ist, so ist dies nur noch mit Ihrer Unterstützung möglich.

Beide Datumswerte müssen mindestens 30 Tage auseinanderliegen. Initial enthalten die Felder die Datumswerte für die letzte mögliche Einführung der MFA. Warten Sie bitte keinesfalls so lange, da auch Sie als ByCS-Admin Ihren Zugang zur Administration mit Ablauf des Datums verlieren. Eine Kontaktaufnahme zum ByCS-Support wäre bei einer Überschreitung beider Termine unumgänglich. Mit dieser stufenweisen Einführung hoffen wir, dass ein reibungsloser Übergang zu einer erhöhten Sicherheit möglich ist.

Teilen Sie die eingetragenen Daten dringend Ihrem Kollegium, am besten in Form eines Aushangs und/oder im Rahmen einer Konferenz mit.

Eingetragene Daten:

| | |
|---|----------------------|
| Datum 1: MFA für besonders schützenswerte Anwendungen: | <input type="text"/> |
| Datum 2: MFA auch für das persönliche Profil (Self-Service): | <input type="text"/> |

 **Achtung: Weisen Sie Ihr Kollegium auf die Hinterlegungsmöglichkeit von bis zu drei Geräten hin, damit der Zugang im Falle eines Geräteverlustes erhalten bleibt.**

3. Was, wenn kein Zugang mehr möglich ist?

Verliert ein Nutzer den Zugang zum zweiten Faktor oder kann aus irgendeinem Grund nicht mehr darauf zugreifen, so **muss** das verlorene Gerät **gelöscht werden**. Dies kann durch Sie oder den betroffenen Nutzer selbst erfolgen, wenn er noch Zugang zum Self-Service über ein weiteres MFA-Gerät hat.

Sie finden die Löschungsmöglichkeit in der Fremdsicht des persönlichen **Profils**, das Sie wie gewohnt über die Pfeilschaltfläche neben **Anzahl Lehrer**, Auswahl des Nutzerkontos und den Button „Multifaktor-Authentifizierung“ erreichen.

Die MFA-Neuanlage durch einen Nutzer ohne Zugang zum Self-Service ist **nur mit Ihrer Unterstützung möglich**. Um Ihren Aufwand an dieser Stelle für Sie gering zu halten, ist der Hinweis auf die Hinterlegungsmöglichkeit von bis zu drei MFA-Geräten wichtig.



Wie funktioniert eine Hinterlegung ohne Zugang zum Self-Service?

Der Nutzer wird bei einem Zugriffsversuch auf einen MFA-geschützten Bereich der ByCS zur Eingabe des Authentifizierungs-codes aufgefordert. Ist dies **nicht** möglich, muss die Option **MFA-Gerät hinzufügen** ausgewählt werden.

Nach wiederholter Eingabe von ByCS-Kennung und Passwort wird dem Nutzer der Dialog **Neues Gerät registrieren**, den Sie aus der normalen Hinterlegung bereits kennen, angezeigt und dieser muss in seinen vier Schritten absolviert werden.

Im Unterschied zur initialen Hinterlegung wird hier das MFA-Gerät zwar angelegt, jedoch im **deaktivierten Zustand**. Um die Vertrauensstellung zu gewährleisten, kann eine **endgültige Aktivierung** nur durch Sie als ByCS-Admin erfolgen. Dafür ist es notwendig, dass der Nutzer den Inhalt des Dialogs **MFA-Registrierung abschließen**, bestehend aus **Geräte-Bezeichnung** und einem **Aktivierungscode**, an Sie weitergibt.

Sie als ByCS-Admin wiederum können mit diesen Informationen die endgültige Aktivierung über die Schaltfläche „freischalten“ im Bereich **Multifaktor-Authentifizierung (MFA)** des entsprechenden Nutzerprofils durchführen.

| Multifaktor-Authentifizierung (MFA) | | | |
|-------------------------------------|--------------------------------------|---------------|---|
| Gerät ist aktiv | Name | Hinterlegt am | |
| <input checked="" type="checkbox"/> | Gerät | 12.12.2023 |  |
| <input type="checkbox"/> | Leherdienstgerät2 (Neuregistrierung) | 18.01.2024 |  |

Freischaltung eines MFA-Geräts ×

Bitte geben Sie zur Freischaltung des Geräts "Leherdienstgerät2" den Aktivierungscode ein, den Sie von der Person erhalten haben.

Geben Sie dazu in der hier dargestellten in der Fremdsicht des Nutzerprofils den an Sie weitergereichten Aktivierungscode in den Dialog **Freischaltung eines MFA-Geräts** ein und bestätigen Sie diesen. Das nicht mehr verfügbare MFA-Gerät kann bei dieser Gelegenheit gelöscht werden.

Das neu registrierte MFA-Gerät ist ab jetzt wieder aktiviert und kann für die Anmeldung durch den Nutzer verwendet werden.

Verliert ein ByCS-Admin seinen Zugang zum MFA-Gerät oder kann aus irgendeinem Grund nicht mehr darauf zugreifen, so können alle weiteren ByCS-Admins der Dienststelle das hinterlegte Gerät für ihn löschen und ein neu registriertes Gerät freischalten, sofern sie ihr eigenes Konto mit einer Multifaktor-Authentifizierung ausgestattet haben.

Die Hinterlegung ausgehend vom **MFA-Login-Screen** funktioniert wie am Beispiel einer Lehrkraft bereits beschrieben.

Persönlicher ByCS-Support

E-Mail: support@bycs.de

Telefon-Hotline: 089 95 44 55 44

Montag - Freitag 6:00 Uhr - 22:00 Uhr, Samstag 10:00 Uhr - 18:00 Uhr

Wenn **keinerlei Zugriff** auf die Konten der ByCS-Admins einer Schule mehr möglich ist, so wenden Sie sich bitte an den ByCS-Support.