# Multi-Faktor-Authentifizierung



Inhaltsverzeichnis



## Was ist Multi-Faktor-Authentifizierung (MFA)?

Multi-Faktor-Authentifizierung ist eine Sicherheitsmaßnahme, die von Nutzer/innen bei der Authentifizierung verlangt, ihre Identität anhand von zwei oder mehr Faktoren nachzuweisen. Faktoren können sein: etwas, dass die Nutzer/innen kennen (z.B. ein Passwort), etwas, dass sie besitzen (z.B. ein Handy) oder etwas, dass sie einzigartig macht (z.B. ein Fingerabdruck).

MFA hilft, die Sicherheit Ihrer Moodle-Site zu verbessern, weil es für potentielle Angreifer/innen schwieriger ist, mehrere Faktoren zu kompromittieren.

## Multi-Faktor-Authentifizierung verwalten

Auf der Seite *Website-Administration > Plugins > Dienstprogramme > Multi-Faktor-Authentifizierung verwalten* können Sie MFA aktivieren, indem Sie die Checkbox *MFA Plgin aktiviert* markieren.

Wenn Sie zum 1. Mal MFA für Ihre Moodle-Site konfigurieren, lesen Sie die Empfehlungen und Beispielkonfigurationen, um die Nutzerfreundlichkeit zu verbessern.

### Gewichte und Faktoren

Auf der Seite *Website-Administration > Plugins > Dienstprogramme > Multi-Faktor-Authentifizierung verwalten* können Sie eine Liste von verfügbaren Faktoren sehen und für Ihre MFA aktivieren.

Die Faktoren haben Gewichte, und Nutzer/innen müssen insgesamt 100 Punkte erreichen, um sich anzumelden. Durch Konfiguration von mehreren Faktoren und deren Gewichten können Sie komplexe und flexible Regeln für die Multi-Faktor-Authentifizierung erstellen.

Zum Beispiel können Sie zwei Faktoren mit jeweils 100 Punkten aktivieren, wenn Sie Ihren Nutzer/innen zwei verschiedene Möglichkeiten zur Authentifizierung geben wollen. Oder Sie verwenden zwei Faktoren mit jeweils 50 Punkten, wenn Ihre Nutzer/innen beide Faktoren erfüllen sollen, um sich anzumelden.

Während des Anmeldprozesses werden zuerst die Faktoren geprüft, die keine Nutzereingabe erfordern, z.B. IP-Adresse oder Nutzer-Rolle. Danach werden die restlichen Faktoren in der Reihenfolge ihrer Gewichte geprüft, beginnend mit dem höchsten Gewicht. Die Prüfung endet, sobald in der Summe 100 Punkte erreicht sind oder alle Faktoren geprüft und die Anmeldung abgelehnt wurde.

#### Verfügbare Authentifizierungsfaktoren

##### Standard-Faktoren

Das sind wohlbekannte Authentifizierungsfaktoren, die in vielen (Software) Produkten verwendet werden:

- **E-Mail**: Dieser Faktor verlangt, dass die Nutzer/innen einen Code eingeben, den Sie per E-Mail erhalten. Wenn eine Person versucht, sich anzumelden, generiert Moodle einen einmaligen, temporärr gültigen Code und schickt diesen an die E-Mail-Adresse der Person. Die Person muss den Code zusammen mit ihrem Passwort eingeben, um sich erfolgreich anzumelden.

Der Code hat eine zeitlich begrenzte, konfigurierbare Gültigkeit, um Missbrauch zu verhindern.

- **Authenticator-App**: Dieser Faktor nutzt eine mobile App, um einen temporären Code für die Nutzerauthentifizierung zu generieren. Während des Anmeldeprozesses verlangt Moodle die Eingabe dieses Codes zusätzlich zur Passworteingabe. Der Code wird regelmäßig erneuert, um eine missbräuchliche Verwendung zu verhindern. **Nutzer/innen müssen eine App auf ihren mobilen Endgeräten installieren und diesen Faktor selbst konfigurieren.**
- **Sicherheitsschlüssel**: Dieser Faktor verwendet technische Hardwaretokens, wie z.B. USB oder NFC Sicherheitsschlüssel, oder biometrische Daten, wie z.B. Fingerabdrücke. Während des Anmeldeprozesses müssen Nutzer/innen diese Schlüssel verwenden, um ihre Identität nachzuweisen. **Nutzer/innen müssen diesen Faktor selbst konfigurieren.**
- **IP-Bereich**: Dieser Faktor verwendet die IP-Adresse der Nutzer/innen, um deren Identität zu prüfen. Er bietet damit eine erhöhte Sicherheit, wenn Nutzer/innen über ein vertrauenswürdiges Netzwerk auf Moodle zugreifen. Die Moodle-Administration trägt den IP-Bereich des vertrauensüwrdigen Netzwerks ein. **Ihre Nutzer/innen müssen bei diesem Faktor nichts konfigurieren.**

### Nutzer-filternde Faktoren

Nutzer-filternde Faktoren sind eine Möglichkeit, auf einfache Weise Gruppen von Nutzer/innen zu erstellen, von denen eine Multi-Faktor-Authentifizierung verlangt wird oder nicht verlangt wird.

- **Nicht-Administrator/in**: Dieser Faktor erfordert nur von Administrator/innen, dass sie sich mit zwei oder mehr Faktoren authentifizieren (weil Admin-Konten aus Sicherheitsgründen besonders schützenswert sind), während alle anderen Nutzer/innen nur ihr Passwort benötigen. Das funktioniert, indem alle Nutzer/innen Faktorpunkte bekommen, die keine Administrator/innen sind.
- **Authentifizierungstyp**: Dieser Faktor ermöglicht es bestimmten Nutzer/innen, basierend auf ihrem Authentifizierungstyp, zusätzliche Authentifizierungsschritte zu überspringen. Das kann nützlich sein, wenn bestimmte Authentifizierungstypen, wie SAML via Active_Directory bereits ein hohes Maß an Sicherheit bieten und zusätzliche Prüfungen überflüssig machen.
- **Rolle**: Dieser Faktor muss in Kombination mit anderen Faktoren verwendet werden, denn er ermöglicht es festzulegen, welche Rollen weitere Faktoren zur Authentifizierung benötigen. Z.B. erlaubt er, dass Nutzer/innen mit erweiterten Rechten, wie z.B. Manager/innen und Administrator/innen, einen strengeren Autghentifizierungsprozess durchlaufen müssen, während andere nicht-privilegierte Rollen die MFA umgehen können.
- **Globale Gruppe**: Dieser Faktor muss in Kombination mit anderen Faktoren verwendet werden, denn er ermöglicht es festzulegen, welche globalen Gruppen weitere Faktoren zur Authentifizierung benötigen.
- **Nutzerrecht**: Dieser Faktor funktioniert ähnlich wie der Faktor **Rolle** und muss ebenfalls mit anderen Faktoren kombiniert werden. Er Faktor prüft, welche Nutzer/innen das Recht factor/capability:cannotpassfactor auf Systemebene haben. Nutzer/innen, bei denen dieses Recht NICHT auf *erlauben* gesetzt ist, bekommen für diesen Faktor Punkte und können so die MFA umgehen, während (privilegierte) Nutzer/innen mit diesem Recht weitere Faktoren zur Authentifizierung benötigen.

  Zum Beispiel können Sie in der Manager-Rolle dieses Recht auf *erlauben* setzen. Wenn Manager/innen sich in Moodle anmelden, benötigen sie dann weitere Faktoren zur Authentifizierung, während normale Nutzer/innen nur ihr Passwort benötigen.

  Da Administrator/innen alle Rechte haben, inklusive factor/capability:cannotpassfactor, gibt es eine zusätzliche Einstellung *Administrator/innen der Website können diesen Faktor bestehen*, so dass Adminsitartor/innen trotz dieses Rechts Punkte für diesen Faktor bekommen können.

### Weitere Faktoren

Die folgenden Faktoren bieten zusätzliche Flexibilität und Kontrolle beim Authentifizierungsprozess:

- **Vertrauensvolles Gerät**: Dieser Faktor ermöglicht es Nutzer/innen, ein Gerät als vertrauenswürdig in Bezug auf MFA zu kennzeichnen. Sobald ein Gerät vertrauenswürdig ist, können Nutzer/innen die MFA in einem festgelegten Zeitraum umgehen, wenn sie sich von diesem gerät aus in Moodle anmelden.

  Um diese Funktionalität effektiv zu nutzen, geben Sie diesem Faktor ein Gewicht von 100 Punkten.

- **Kulanzzeit**: Dieser Faktor ist essenziell, wenn Sie Faktoren nutzen, die eine Konfiguration auf Seiten Ihrer Nutzer/innen erfordern, wie z.B. **Authenticator-App** oder **Sicherheitsschlüssel**. Er erlaubt es Nutzer/innen, sich in einem bestimmten Zeitraum ohne MFA anzumelden. Damit

wird eine Pufferzeit bereitgestellt, in der Nutzer/innen Zeit haben, ihre MFA Konfiguration einzurichten. Nutzer/innen erhalten während dieser Pufferzeit beim Anmeldeprozess einen Warnhinweis, dass sie die MFA Konfiguration einrichten müssen, um nach Ablauf der Frist nicht ausgesperrt zu sein.

Um diese Funktionalität effektiv zu nutzen, geben Sie diesem Faktor 100 Punkte. Um für diesen Faktor Punkte zu bekommen, darf es keinen anderen Faktor geben, der Nutzereingaben während des Anmeldeprozesses erfordert. Platzieren Sie diesen Faktor am Ende der Liste aller aktiven Faktoren, um sicherzustellen, dass alle anderen Faktoren vorher geprüft werden.

Wenn Nutzer/innen die MFA Konfiguration nach Ablauf der Kulanzzeit nicht eingerichtet haben, können sie sich nicht mehr anmelden. Um ihnen weiter Moodle-Zugriff zu gewähren, können Sie nur die Kulanzzeit verlängern oder andere Faktoren temporär aktivieren, wie z.B. **IP-Bereich** oder **Rolle**.

- **Keine weiteren Faktoren**: Dieser Faktor erlaubt es Nutzer/innen, sich anzumelden, wenn sie keinen anderen MFA Faktor eingerichtet haben. Wenn Sie z.B. MFA anbieten wollen, aber nicht obligatorisch, geben Sie diesem Faktor 100 Punkte, um Nutzer/innen, die keinen zusätzlichen Faktor nutzen wollen, zu ermöglichen, sich anzumelden. Sobald ein anderer Faktor eingerichtet ist, erhalten sie keine Punkte mehr für diesen Faktor.

## Was müssen die Nutzer/innen tun?

Wenn Sie die Faktoren **Authenticator-App** und **Sicherheitsschlüssel** aktivieren, müssen Ihre Nutzer/innen die Multi-Faktor-Authentifizierung selbst konfigurieren. Die Nutzer/innen können die Authentifizierungseinstellungen über ihr *Nutzermenü* > *Einstellungen* > *Multi-Faktor-Authentifizierung* vornehmen. Auf dieser Seite können sie die App bzw.den Sicherheitsschlüssel einrichten und diese Einstellungen rückgängig machen.

# Empfehlungen und Beispielkonfigurationen

Wenn Sie für Ihre Moodle-Site MFA einrichten, ist es wichtig, die Sicherheit zu erhöhem, aber gleichzeitig eine nutzerfreundliche Handhabung zu gewährleisten, dass Ihre Nutzer/innen sich problemlos anmelden können, wenn sie die richtigen Schritte tun.

Hier kommen einige Empfehlungen, um eine nutzerfreundlichen Anmeldeprozess einzurichten:

1. Nutzen Sie den Faktor **Kulanzzeit**, wenn Sie MFA mit Faktoren einführen, die Konfigurationsschritte auf Seiten Ihrer Nutzer/innen erfordern (d.h. bei **Authenticator-App** oder **Sicherheitsschlüssel**). Das gibt Ihren Nutzer/innen Zeit, diese Konfiguration vorzunehmen, bevor eine MFA Pflicht wird.
2. Wenn Sie MFA nicht verpflichtend machen wollen, aktivieren Sie die Option **Keine weiteren Faktoren**. Das erlaubt es Nutzer/innen, die keine weiteren Faktoren haben, sich nur mit ihrem Passwort anzumelden.
3. Der Faktor **IP-Bereich** ist eine einfache Authentifizierungsmethode, wenn alle Nutzer/innen dassselbe Netzwerk nutzen. Sobald Nutzer/innen sich mit diesem Faktor angemeldet haben, können Sie ihnen erlauben, weitere Faktoren einzurichten, z.B. **Authenticator-App** und dann diesen Faktor zu bverwenden, wenn sie sich außerhalb des sicheren Netzwerks befinden und sich in Moodle anmelden wollen.

## Beispielkonfigurationen

Hier finden Sie einige typische MFA Konfigurationen, um die Sicherheit Ihrer Moodle-Site zu verbessern.

**a) E-Mail**

1. Aktivieren Sie MFA.
2. Aktivieren Sie den Faktor **E-Mail** und geben Sie ihm 100 Punkte.
3. Sie können den Faktor **Vertrauensvolles Gerät** aktivieren, um Nutzer/innen zu erlauben, MFA für einen gewissen Zeitraum zu umgehen, bis sie ihr Gerät erstmalig für MFA eingerichtet haben.
4. Informieren Sie Ihre Nutzer/innen, dass die E-Mail-Verifizierung aktiviert ist. Beim nächsten Login sehen die Nutzer/innen eine Nachricht, dass sie ihr E-Mail-Postfach prüfen und den zugesandten Code eingeben sollen.

**b) Authentificator-App**

1. Aktivieren Sie MFA.

2. Aktivieren Sie den Faktor **Kulanzzeit** und geben Sie ihm 100 Punkte. Das gibt Ihren Nutzer/innen eine gewisse Zeit, um ihre Authentificator-App einzurichten und verhindert, dass sie von Moodle ausgesperrt werden. Nutzen Sie den *Inhalt des Warnfelds*, um Ihre Nutzer/innen zu informieren, dass MFA in Kürze ativiert wird und sie ihre App einrichten müssen.
3. Aktivieren Sie den Faktor **Authenticator-App** und geben Sie ihm 100 Punkte.
4. Sie können den Faktor **Vertrauensvolles Gerät** aktivieren, um Nutzer/innen zu erlauben, MFA für einen gewissen Zeitraum zu umgehen, bis sie ihr Gerät erstmalig für MFA eingerichtet haben.

### c) E-Mail ODER Authenticator-App

1. Aktivieren Sie MFA.
2. Aktivieren Sie den Faktor **E-Mail** und geben Sie ihm 100 Punkte.
3. Aktivieren Sie den Faktor **Kulanzzeit** und geben Sie ihm 100 Punkte. Das gibt Ihren Nutzer/innen eine gewisse Zeit, um ihre Authentificator-App einzurichten und verhindert, dass sie von Moodle ausgesperrt werden. Nutzen Sie den *Inhalt des Warnfelds*, um Ihre Nutzer/innen zu informieren, dass MFA in Kürze ativiert wird und sie ihre App einrichten müssen.
4. Aktivieren Sie den Faktor **Authenticator-App** und geben Sie ihm 100 Punkte.
5. Sie können den Faktor **Vertrauensvolles Gerät** aktivieren, um Nutzer/innen zu erlauben, MFA für einen gewissen Zeitraum zu umgehen, bis sie ihr Gerät erstmalig für MFA eingerichtet haben.

### d) E-Mail UND Authenticator-App

1. Aktivieren Sie MFA.
2. Aktivieren Sie den Faktor **E-Mail** und geben Sie ihm 50 Punkte.
3. Aktivieren Sie den Faktor **Kulanzzeit** und geben Sie ihm 100 Punkte. Das gibt Ihren Nutzer/innen eine gewisse Zeit, um ihre Authentificator-App einzurichten und verhindert, dass sie von Moodle ausgesperrt werden. Nutzen Sie den *Inhalt des Warnfelds*, um Ihre Nutzer/innen zu informieren, dass MFA in Kürze ativiert wird und sie ihre App einrichten müssen.
4. Aktivieren Sie den Faktor **Authenticator-App** und geben Sie ihm 50 Punkte. Nutzer/innen müssen beide Faktoren erfüllen, um auf 100 Punkte zu kommen und sich anzumelden.
5. Sie können den Faktor **Vertrauensvolles Gerät** aktivieren, um Nutzer/innen zu erlauben, MFA für einen gewissen Zeitraum zu umgehen, bis sie ihr Gerät erstmalig für MFA eingerichtet haben.

## Zusammenfassung guter Bedingungen für die Anmeldung

Hier werden die gewählten Faktoren und ihre Gewichte aufgelistet. Die Gesamtgewichtung muss 100 betragen.

## Allgemeine MFA-Einstellungen

- **MFA Plugin aktiviert** - diese Checkbox muss markiert sein, damit MFA funktioniert.
- **URLs, die die MFA-Prüfung nicht umleiten sollen** - hier können Sie jede URL relativ zur Site-Root-URL eintragen, die nicht auf MFA-Prüfung umleiten soll.
- **Inhalt / Dateien der Anleitungsseite** - hier können Sie Anleitungen zu MFA eintragen oder hochladen.

## Problem: Admin hat sich ausgesperrt - was tun?

Seien Sie als Administrator/in vorsichtig, wenn Sie MFA konfigurieren und die Faktoren testen, dass Sie sich nicht selbst aus Ihrer Moodle-Site aussperren. Sollte das dennoch passieren, können Sie MFA von der Kommandozeile aus deaktivieren, indem Sie folgenden Befehl ausführen:

```
: php admin/cli/cfg.php --component=tool_mfa --name=enabled --set=0
```