

Multi-Faktor-Authentifizierung (MFA)

Überblick

Die Multi-Faktor-Authentifizierung (MFA) bietet während der Anmeldung eine zusätzliche Schutzebene. Für den Zugriff auf Konten oder Apps müssen Benutzer einen zweiten Identitätsnachweis erbringen, z.B. durch Scannen eines Fingerabdrucks oder Eingabe eines an das Mobiltelefon gesendeten Codes.

picturemaxx empfiehlt, administrative Zugriffe auf das Datenbanksystem – also jene, die in der Regel das Team vornimmt – auf diese Weise abzusichern. Seitens der Webshop-Besucher kann es sehr unterschiedliche Sicherheitsbedürfnisse geben. Für diejenigen, die über unlimitierte Download-Berechtigungen verfügen oder dort, wo in der Vergangenheit missbräuchliche Nutzungen verzeichnet wurden, könnte das Thema interessant sein. Wir empfehlen, mindestens ausgewählte Kunden auf die Möglichkeit der zusätzlichen Absicherung aufmerksam zu machen.



Multi-Faktor-Authentifizierung (MFA) ist eine Authentifizierungsmethode, bei der ein User mehrere Verifizierungsfaktoren angeben muss, um Zugang zu einer Anwendung zu erhalten.

Technische Voraussetzungen

- Login
- Mobiles Endgerät mit Authenticator-App

Ausgangspunkt ist der einfache Login, das heißt, ein Benutzer muss bereits mit Benutzernamen und Passwort in Backstage eingerichtet sein. Das gilt sowohl für die Personen, die auf das Backend zugreifen, als auch für die Besucher des Webshops.

Weitere Voraussetzung ist ein mobiles Endgerät, das die jeweilige Person im Zugriff hat, sowie eine darauf installierte sog. Authenticator-App. Geeignet sind Apps, die den Standard TOTP unterstützen, u.a.:

- Google Authenticator (für Android, iOS, Blackberry OS)
- Microsoft Authenticator (für Android, iOS)
- Authy (Twilio) (für Android, iOS)
- PrivacyIDEA (für Android, iOS)

Einsatz für Backstage Zugänge

Backstage unterstützt zwei Arten der Multi-Faktor-Authentifizierung (MFA):

- Proaktive MFA-Benutzer aktivieren die MFA selbst über ihre eigenen Kontoeinstellungen.
- Erforderliche MFA-Administratoren erzwingen die MFA für ausgewählte Konten über die Zugriffseinstellungen.

Proaktive Verwendung

Jeder Backstage-Nutzer kann, wenn nicht anderweitig vorgegeben, selbstständig entscheiden, den Login-Prozess für die zusätzliche Absicherung über MFA zu nutzen oder nicht. Das kann über das Benutzerkonto (oranges Icon neben dem Benutzernamen im Header) selbstständig für den Zugang aktiviert werden.

1. Navigieren Sie zu **Mein Konto > Multi-Faktor-Authentifizierung**.
2. Wählen Sie **für diesen Zugang aktivieren** aus.
3. Aktivieren Sie die Option für Backstage und / oder den Webshop und legen Sie das Zeitintervall für die Abfrage fest.
4. Klicken Sie **Konfigurationsschlüssel erzeugen** und erfassen Sie den Code mit dem Mobiltelefon.
5. Bestätigen Sie mit **Speichern**.

Die Funktion kann anschließend optional nur für Backstage oder den Webshop sowie für beide Bereiche aktiviert werden. Zusätzlich muss dann ein konkretes Zeitfenster für die Token-Abfrage gewählt, sowie der entsprechende Konfigurationsschlüssel erzeugt werden. Dieser findet dann in der App des Mobiltelefons Anwendung, um die Verknüpfung herzustellen.

Mein Konto

Einstellungen

Passwortänderung

Multi-Faktor-Authentifizierung



Mein Konto

Abmelden

Backstage unterstützt Multi-Faktor-Authentifizierung auf Basis von zeitbasierten Einmal-Tokens. Sie benötigen dazu ein Mobiltelefon mit einer TOTP (Time-based One-time Password) fähigen Multi-Faktor-App.

▼ Multi-Faktor-Authentifizierung (MFA)

Backstage:

☒ MFA für Backstage verwenden

Web:

☐ MFA für Web verwenden

Token-Abfrage:

immer

▼ Geheimer Konfigurationsschlüssel

⚠ Es wurde noch kein geheimer Konfigurationsschlüssel erzeugt.

Konfigurationsschlüssel erzeugen

Mein Konto > Tab ‚Multi-Faktor-Authentifizierung‘: Aktivieren Sie MFA für den Zugriff auf Backstage und/oder den Webshop.

▼ Geheimer Konfigurationsschlüssel

Öffnen Sie die Authenticator-App auf Ihrem Mobiltelefon, scannen Sie den QR-Code damit (oder geben Sie den **geheimen Konfigurationsschlüssel** manuell ein, wenn das Scannen nicht klappt), geben Sie den in der App anschließend angezeigten 6-stelligen Zahlencode zur Bestätigung ein und klicken Sie **Speichern und MFA aktivieren** um die Einrichtung abzuschließen. Wenn das erfolgt ist, steht der QR-Code nicht mehr zur Verfügung. Er dient nur der initialen Verknüpfung.

Konfigurationsschlüssel:

3HV2 S5EI Q5BW 7FDP

QR-Code:



Aktuelles MFA Token: *

6-stelliger Code, z.B. 123456

?

Konfigurationsschlüssel erzeugen

Zurücksetzen

Speichern und MFA aktivieren

Mein Konto > Tab ‚Multi-Faktor-Authentifizierung‘: Generierter QR-Code. Scannen Sie diesen einmal mit der MFA-App auf Ihrem Mobiltelefon.

Künftig wird dann in den eingestellten Intervallen nach dem normalen Login im Programm eine Zahlenfolge angezeigt, die in der Authenticator-App eingegeben werden muss, um das Programm zur Benutzung freizugeben. So wird sichergestellt, dass nur der Besitzer des entsprechenden Mobiltelefons sich mit diesen Zugangsdaten erfolgreich anmelden kann.

Benutzergesteuerte MFA zurücksetzen

Wenn Benutzer die MFA selbst aktiviert haben und der zweite Faktor nicht mehr verfügbar ist (beispielsweise bei Verlust des Geräts), kann der Administrator die MFA-Konfiguration in den Zugriffseinstellungen des Benutzers zurücksetzen.

1. Wählen Sie im Modul Vertrieb/Beschaffung/Administration den gewünschten Kunden/Partner/Benutzer aus.
2. Öffnen Sie den Tab **Zugänge** und wählen Sie den entsprechenden Zugang aus.
3. Scrollen Sie runter zum Bereich **Zusätzliche Sicherheitseinschränkungen**.
4. Unter **Multi-Faktor-Authentifizierung (MFA)**, klicken Sie auf **Multi-Faktor-Authentifizierung zurücksetzen**.
5. Nun kann sich der Benutzer mit seinem Benutzernamen und Passwort anmelden und unter **Mein Konto** eine neue zweistufige Authentifizierung einrichten.

IT-Benutzer / Bearbeitung von IT-Benutzer 'IT0026 eins' / Bearbeiten von Zugang 'eins'

Stammdaten Kontakte Kontakthistorie **Zugänge** Ausgänge Leuchtkästen Statistiken

<< < 1 (2) > >> Zurück zur Zugangsübersicht Zugänge bearbeiten

▼ Stammdaten

Name: * eins

Zugang ist aktiv: ☒ aktiv

Benutzername: * eins

Passwort: *

Kontakt: eins eins

Ausgänge: ..

▼ Verwaltung und Zuweisung von Zugangsgruppen

Verfügbare Zugangsgruppen

Schnellsuche Filter Sortierung

Ansichten Auswahl Export

ID	Name
9	Samstagsgruppe
8 Treffer	

Hinzufügen >>

<< Entfernen

Zugewiesene Zugangsgruppen

Schnellsuche Filter Sortierung

Ansichten Auswahl Export

ID	Name
33	karsten
2	picturemaxx-support
2 Treffer	

▲ Zugriffseinstellungen für Backstage

▲ Einlieferung von Medien (FTP/HTTP)

▼ Zusätzliche Sicherheitseinschränkungen

Multifaktor-Authentifizierung (MFA)

Sichern Sie Ihre Systemzugänge zusätzlich, indem Sie neben dem Passwort einen zweiten Verifizierungsschritt (MFA) verlangen.

Ihre Backstage-Benutzer können MFA selbst aktivieren, oder Sie können MFA für einzelne Benutzer oder Benutzergruppen verbindlich vorschreiben.

MFA bei der Nutzung von Backstage erforderlich:

☐ MFA für diesen Zugang erzwingen

Benutzergesteuerte MFA (schreibgeschützt)

Diese Einstellungen werden von den Benutzern verwaltet.

☒ MFA für Backstage-Zugang aktiv

☐ MFA für Web-Zugang aktiv

Öffentlicher Schlüssel:

Für diesen Zugang ist Multifaktor-Authentifizierung hinterlegt. Sollte der Zugang diese nicht länger nutzen können (z. B. wegen Verlust des 2. Faktors), dann können Sie hier den hinterlegten zweiten Faktor zurücksetzen. Nach erfolgreichem Login kann der Zugang anschließend erneut einen zweiten Faktor einrichten.

Multifaktor-Authentifizierung zurücksetzen

Datei für öffentlichen Schlüssel auswählen >>

Vertrieb/Beschaffung/Administration > Kunden/Partner/Benutzer > Tab Zugänge > Bereich „Zusätzliche Sicherheitseinschränkungen“: Multi-Faktor-Authentifizierung zurücksetzen

Erforderliche Verwendung

In manchen Fällen kann es sinnvoll sein, die Nutzung von MFA für Backstage- und Webshop-Nutzer obligatorisch zu machen. Sie können daher im Bereich **Zusätzliche Sicherheitseinschränkungen** innerhalb der **Zugänge** dafür sorgen, dass Zugänge mit MFA arbeiten müssen, sowie dort einsehen, ob die Option aktiviert ist.

1. Navigieren Sie zu einem **Zugang**.
2. Scrollen Sie zum untersten Teilbereich **Zusätzliche Sicherheitseinschränkungen**.
3. Klicken Sie **MFA erforderlich**, wenn dieser Zugang nur mit MFA-Zugang erhalten soll.
4. **Zusätzlich:** Sie können hier auch einsehen, ob ein User selbst MFA für den Backstage oder Webshop-Zugang aktiviert hat.
5. Bestätigen Sie mit **Speichern**.

Multifaktor-Authentifizierung (MFA)

Sichern Sie Ihre Systemzugänge zusätzlich, indem Sie neben dem Passwort einen zweiten Verifizierungsschritt (MFA) verlangen.

Ihre Backstage-Benutzer können MFA selbst aktivieren, oder Sie können MFA für einzelne Benutzer oder Benutzergruppen verbindlich vorschreiben.

MFA bei der Nutzung von Backstage erforderlich:

☒ MFA für diesen Zugang erzwingen

Benutzergesteuerte MFA (schreibgeschützt)

Diese Einstellungen werden von den Benutzern verwaltet.

☐ MFA für Backstage-Zugang aktiv

☐ MFA für Web-Zugang aktiv

Tab ‚Zugänge‘ > Authentifizierungsbeschränkungen: Option ‚MFA für diesen Zugang erzwingen‘

Einsatz für Webshop-Zugänge

Die Multi-Faktor-Authentifizierung steht auch für Webgate zur Verfügung und kann somit optional auch von den Webshop-Usern aktiviert werden. Die User können die Einstellungen selbstständig im Webshop-Bereich **Mein Konto** vornehmen, indem sie die Option **Multi-Faktor-Authentifizierung für Ihren Zugang aktivieren** auswählen. Anschließend können sie an gleicher Stelle ebenfalls das Intervall der Abfrage festlegen sowie den Konfigurationsschlüssel zum Verknüpfen in der entsprechenden App erzeugen.

1. Navigieren Sie zum Menüpunkt **Mein Konto**.
2. Wählen Sie **Multi-Faktor-Authentifizierung für Ihren Zugang aktivieren** aus.
3. Legen Sie das Intervall für die Token-Abfrage fest.
4. Klicken Sie **Konfigurationsschlüssel erzeugen** und erfassen Sie den Code mit dem Mobiltelefon.
5. Bestätigen Sie mit **Speichern**.

Mein Konto

Ihre Kontaktdaten

Vorname: *

Nachname: *

Telefon:

E-Mail: *

Ihre Zugangsdaten

Anmeldename:

Passwortänderung anfordern

Multi-Faktor-Authentisierung

☒ Multi-Faktor-Authentisierung für Ihren Zugang aktivieren

MFA-Tokenabfrage:

Konfigurationsschlüssel erzeugen

Unser Service für Sie

☐ Ja, ich möchte den regelmäßigen Newsletter erhalten.

Speichern

Webshop > ‚Mein Konto‘: Webshop-Benutzer können ihre MFA-Einstellungen verwalten

Hinweis

Sollte im Webshop der User noch kein Menüpunkt **Mein Konto** angelegt sein, können Sie jederzeit unter **Seiten-Elemente > Navigation** einen solchen Punkt anlegen. Verwenden Sie das Seiten-Template Mein Konto – Webshop hierfür.

▼ Element bearbeiten

Name: *

URL

Titel Deutsch

Titel Englisch (USA)

Seiten-Template:

Mein Konto - Webshop

▼

Web > Seitenelemente > Navigation: Seiten-Vorlage ‚Mein Konto – Webshop‘

Hinweis

picturemaxx kann zusätzlich für Ihre gesamte Backstage-Instanz hinterlegen, dass alle Backstage-User generell mit MFA arbeiten müssen, um Zugang zu den Inhalten zu erhalten.