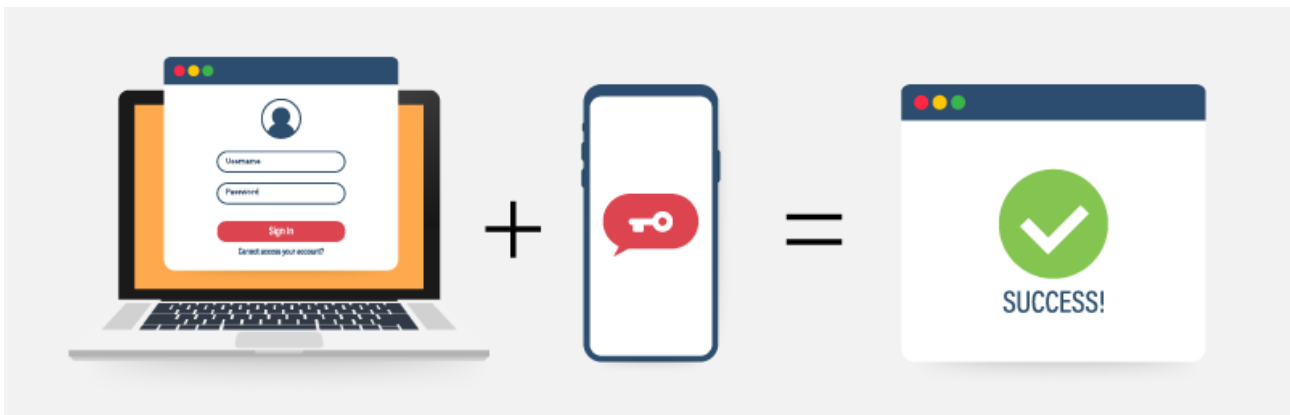


Authentification Multifacteur (MFA)

Aperçu

L'authentification multifacteur (MFA) ajoute un niveau de sécurité supplémentaire lors de la connexion. Pour accéder à leurs comptes ou applications, les utilisateurs doivent fournir une deuxième preuve d'identité, par exemple en scannant leur empreinte digitale ou en saisissant un code envoyé sur leur téléphone portable.

picturemaxx recommande d'utiliser l'authentification multifacteur (MFA) pour protéger l'accès administratif au système de base de données, car les comptes administrateurs sont généralement partagés par plusieurs membres de l'équipe et peuvent donc présenter un risque pour la sécurité. Les visiteurs du webshop peuvent avoir des besoins très différents en matière de sécurité. Les utilisateurs disposant de droits de téléchargement illimités ou dont le compte a été piraté peuvent avoir besoin de l'authentification multifacteur (MFA) pour se connecter. Nous recommandons d'informer au moins certains clients de cette option de sécurité supplémentaire.



La MFA est une méthode de vérification qui exige des utilisateurs qu'ils fournissent plusieurs facteurs de validation pour accéder à une application

Exigences techniques

Identifiant et mot de passe

Nom d'utilisateur et mot de passe Backstage de l'utilisateur. Cela s'applique à la fois aux utilisateurs ayant accès à Backstage et aux visiteurs du webshop.

Appareil mobile équipé d'une application « Authenticator »

Un appareil mobile auquel l'utilisateur a accès et une application dite « d'authentification » installée sur celui-ci. Les applications qui prennent en charge la norme TOTP (Time-based, One-Time Password) sont adaptées, notamment :

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

Configuration Backstage

Backstage prend en charge deux modes d'utilisation de l'authentification multifacteur (MFA)

- MFA proactive de la MFA : Les utilisateurs activent eux-mêmes la MFA via les paramètres de leur compte.
- Utilisation obligatoire de la MFA : Les administrateurs activent la MFA pour certains comptes via les paramètres d'accès.

Utilisation proactive de l'authentification multifacteur (MFA)

Sauf indication contraire, chaque utilisateur Backstage peut décider de manière indépendante d'utiliser ou non l'authentification multifactorielle (MFA) pour renforcer la sécurité du processus de connexion. Les utilisateurs peuvent activer de manière proactive la fonctionnalité MFA via leur compte utilisateur (icône orange à côté du nom d'utilisateur dans l'en-tête) :

1. Survolez l'icône de votre compte en haut à droite avec la souris, puis allez dans **Mon compte**
2. Allez dans l'onglet **Authentification multifacteur**.
3. Activez la ou les options pour les comptes sur lesquels vous souhaitez utiliser un code de vérification supplémentaire lors de la connexion :
 - **Utiliser la MFA pour Backstage**
 - **Utilisez la MFA pour le web**
4. Définissez l'intervalle de temps pour la requête de jeton. Nous vous recommandons de sélectionner **Toujours** pour bénéficier du niveau de sécurité le plus élevé.
5. Cliquer sur **Générer une clé secrète**. Un QR code est affiché.
6. Ouvrez l'application MFA sur votre téléphone portable et scannez le QR code généré.
 - Si le scan du QR code ne fonctionne pas, vous pouvez saisir la **clé secrète** manuellement.

7. Saisissez le code à 6 chiffres de votre application d'authentification dans le champ **Jeton MFA actuel**.
8. Cliquez sur **Enregistrer et activer la MFA** pour confirmer.
 - Une fois la configuration terminée, le QR code ne sera plus affiché.

Votre application d'authentification est désormais connectée à votre compte, et la MFA est activée.

La prochaine fois que vous vous connecterez avec votre nom d'utilisateur et votre mot de passe, le système vous demandera également de saisir un code de vérification provenant de l'application d'authentification installée sur votre téléphone portable.

Mon compte

Paramètres | Changement de mot de passe | **Authentification multifacteur**

Mon compte | Déconnecter

Backstage prend en charge l'authentification multifacteur basée sur des jetons à usage unique limités dans le temps. Vous avez besoin pour cela d'un téléphone mobile avec une application mobile multifacteur compatible avec la norme TOTP (Time-based One-time Password).

▼ Authentification multifacteur (MFA)

Backstage: ☒ Utiliser la MFA pour Backstage

Web: ☐ Utiliser la MFA pour le web

Demande de jeton: Toujours ▼

▼ Clé secrète

⚠ Aucune clé secrète n'a encore été générée.

Générer une clé secrète

Mon compte > Onglet Authentification multifacteur

▼ Clé secrète

Ouvrez l'application d'authentification sur votre téléphone, scannez le QR code (ou saisissez manuellement la **clé secrète** si le scan ne fonctionne pas), puis cliquez sur **Enregistrer et activer la MFA**.
Une fois la configuration terminée, le QR code ne sera plus disponible.

Clé secrète: PWMN EUIH DYYQ MLAG

QR Code: 

Jeton MFA actuel: * Code à 6 chiffres, par ex. 123456 ?

Générer une clé secrète

Réinitialiser Enregistrer et activer la MFA

QR code généré. Utilisez l'application MFA sur votre téléphone portable pour le scanner une fois.

Réinitialiser la MFA gérée par l'utilisateur

Si les utilisateurs ont activé eux-mêmes la MFA et que le deuxième facteur n'est plus disponible (par exemple, en cas de perte de l'appareil), l'administrateur peut réinitialiser la configuration de la MFA dans les paramètres d'accès de l'utilisateur.

1. Dans le module Distribution/Acquisition/Administration, sélectionnez le client/partenaire/utilisateur souhaité.
2. Ouvrez l'onglet **Accès** et sélectionnez l'accès correspondant.
3. Faites défiler vers le bas jusqu'à **Restrictions de sécurité supplémentaire**.
4. Dans **Authentification multifacteur (MFA)**, cliquez sur **Réinitialiser l'authentification multifacteur (MFA)**.
5. L'utilisateur peut désormais se connecter avec son nom d'utilisateur et son mot de passe, puis de nouveau configurer un deuxième facteur dans **Mon compte**.

Utilisateurs IT / Édition de l'utilisateur IT 'IT0026 eins' / Édition de l'accès 'eins'

Données de base | Contacts | Historique des contacts | **Accès** | Sorties | Visionneuses | Statistiques

<< < 1 (2) > >> Retour à l'aperçu des accès Édition des accès

▼ Données de base

Nom: * support_test2109

L'accès est actif: ☒ actif

Nom d'utilisateur: * support_test2109

Mot de passe: *

Contact: eins eins

Sorties:

▼ Gestion et attribution des groupes d'accès

Groupes d'accès disponibles

ID	Nom
22	Kopie von Mittwochsgruppe 2

8 Résultats positifs

Groupes d'accès attribués

ID	Nom
33	karsten

2 Résultats positifs

▲ Paramètres d'Accès pour Backstage

▼ Restrictions de sécurité supplémentaires

Authentification multifacteur (MFA)

Renforcez la sécurité en exigeant une deuxième étape de vérification (authentification multifacteur, ou MFA) en plus du mot de passe.

Les utilisateurs de Backstage peuvent choisir d'activer eux-mêmes la MFA, ou vous pouvez l'imposer pour des accès individuels ou des groupes d'accès.

Exiger la MFA lors de l'utilisation de Backstage

☐ Appliquer la MFA pour cet accès

MFA contrôlée par l'utilisateur (lecture seule)

Ces paramètres sont gérés par les utilisateurs.

☒ MFA activée pour Backstage

☐ MFA activée pour le Web

Clé publique:

Réinitialiser l'authentification multifacteur

Sélectionner le fichier de clé publique >>

Accès > configuration de la MFA

Utilisation obligatoire de l'authentification multifacteur (MFA)

Dans certains cas, vous pouvez choisir d'exiger la MFA pour vous connecter à Backstage et au webshop. Vous pouvez configurer cette exigence dans les paramètres d'accès d'un compte sélectionné. Vous pouvez également vérifier ici si l'option est active pour un compte d'accès.

1. Dans la section Distribution, Acquisition ou Administration, sélectionner un client/partenaire/utilisateur.
2. Allez dans l'onglet **Accès** et sélectionnez un accès.
3. Faites défiler vers le bas jusqu'à la section MFA.
4. Activer la **MFA requise** pour que la connexion au compte nécessite obligatoirement l'authentification multifacteur.
5. **Enregistrer.**

Conseil

Dans la section **Authentification multifacteur (MFA)**, sous **MFA contrôlée par l'utilisateur (lecture seule)**, les administrateurs peuvent vérifier si un utilisateur a activé la MFA pour son accès à Backstage ou au webshop, et réinitialiser cette authentification si nécessaire.

Utilisateurs IT / Édition de l'utilisateur IT 'IT0005 Notifications' / Édition de l'accès 'Notifications'

« 4 (7) » Retour à l'aperçu des données de base Éditer ▼ Modèles ▼

Données de base Contacts Historique des contacts **Accès** Sorties Visionneuses Statistiques

« 1 (1) » Retour à l'aperçu des accès Édition des accès ▼

Authentification multifacteur (MFA)

Renforcez la sécurité en exigeant une deuxième étape de vérification (authentification multifacteur, ou MFA) en plus du mot de passe.

Les utilisateurs de Backstage peuvent choisir d'activer eux-mêmes la MFA, ou vous pouvez l'imposer pour des accès individuels ou des groupes d'accès.

Exiger la MFA lors de l'utilisation de Backstage

☒ Appliquer la MFA pour cet accès

MFA contrôlée par l'utilisateur (lecture seule)
Ces paramètres sont gérés par les utilisateurs.

☐ MFA activée pour Backstage

☐ MFA activée pour le Web

MFA requise

Configuration du webshop

La MFA est également disponible pour Webgate, les utilisateurs du webshop peuvent donc l'activer s'ils le souhaitent. Les utilisateurs peuvent gérer leurs paramètres MFA dans la section **Mon compte** du webshop. Pour activer la MFA, sélectionnez l'option **Activer l'authentification multifacteur pour votre accès**. Vous pouvez ensuite définir l'intervalle de requête et générer la clé de configuration afin de relier le compte et l'application « Authenticator ».

1. Allez dans **Mon compte**.
2. Cochez **Activez l'authentification à deux facteurs pour votre accès**.
3. Définissez l'intervalle de temps pour la requête de jeton.
4. Cliquez sur **Générer la clé secrète** et scannez le QR code avec votre téléphone portable.

5. Enregistrer.

Mon compte

vos coordonnées

Prénom: *

Nom de famille: *

Téléphone:

E-mail: *

vos données d'accès

Nom de connexion:

Demande de changement de mot de passe

Authentification à deux facteurs

☒ Activez l'authentification à deux facteurs pour votre accès

Requête de jeton A2F:

Générer phrase secrète

Nos services pour vous

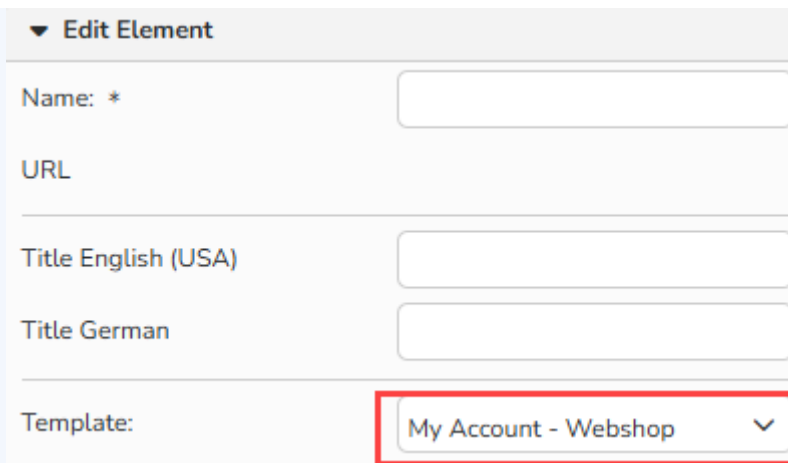
☐ Oui, je souhaite recevoir la newsletter

Enregistrer

Webshop > "Mon compte": Les utilisateurs du webshop peuvent gérer leurs paramètres MFA.

Remarque

Si le webshop de l'utilisateur ne dispose pas encore du menu **Mon compte**, vous pouvez en créer un à tout moment sous **Web > Éléments de page > Navigation**. Utilisez pour cela le modèle de page **My account - Webshop**.



▼ Edit Element

Name: *

URL

Title English (USA)

Title German

Template: My Account - Webshop ▼

Web > Eléments de page > Navigation : Modèle "My Account - Webshop"

Remarque

picturemaxx peut également créer une politique d'accès pour l'ensemble de votre instance Backstage afin d'imposer l'authentification multifacteur à tous les utilisateurs de Backstage.