Connexion avec l'authentification à deux facteurs

22.04.2025 - Grundeinstellungen

Selon les réglages effectués par les administrateurs, votre connexion est protégée par une authentification à deux facteurs. Ce niveau de sécurité supplémentaire garantit que même si quelqu'un connaît votre mot de passe, il ne peut pas accéder à votre compte sans le code unique. Comme 2e facteur, vous avez le choix entre l'e-mail et l'application Authenticator (Time-based one-time password, TOTP). Selon les réglages effectués par les administrateurs, l'une ou les deux options sont disponibles.

Utiliser 2FA par e-mail

Si vous utilisez 2FA par e-mail, vous n'avez rien à configurer. Après vous être connecté, vous recevrez le code unique sur votre adresse e-mail. Collez-le dans le champ disponible pour terminer le processus de connexion. Si vous ne recevez pas un tel e-mail, vérifiez également votre dossier spam.

Si vous cochez la case « Je suis sur un appareil de confiance », vous pourrez sauter cette étape lors de votre prochaine connexion depuis le même appareil.

Configurer la 2FA avec l'application Authenicator

Pour utiliser l'application Authenticator comme 2e facteur, vous devez la configurer une fois pour toutes. Procédez comme suit :

1. Si vous n'avez pas encore installé d'application Authenticator sur votre téléphone portable, téléchargez-en une. Les applications d'authentification les plus répandues sont par exemple Google Authenticator, Apple Keypass, Microsoft Authenticator et Twilio Authy.
2. Après votre connexion à Fairgate, un code QR apparaît. L'application Authenticator contient une fonction de scannage qui vous permet de scanner le code QR et d'ajouter ainsi le compte.
3. L'application Authenticator génère alors toutes les 30 secondes un nouveau code à 6 chiffres, qui n'est plus valable une fois les 30 secondes écoulées. Pour terminer la configuration, il suffit d'ajouter une fois le code actuel dans le champ correspondant chez Fairgate.
4. Pour être sûr de ne pas perdre l'accès à Fairgate, vous pouvez générer et télécharger un fichier de codes de récupération. Enregistrez-le dans un endroit sûr, idéalement dans un gestionnaire de mots de passe.

Se connecter avec l'application Authenticator

Après vous être connecté, vous verrez apparaître un champ pour le code unique. Ouvrez votre application Authenticator et récupérez le code du compte pour votre organisation. Tapez ce code dans le champ lors de la connexion Fairgate. Si le code n'est pas valable, la durée de validité de 30 secondes est probablement déjà écoulée. Essayez simplement de nouveau avec le code suivant.

Si vous cochez la case « Je suis sur un appareil de confiance », vous pourrez sauter cette étape lors de votre prochaine connexion à partir du même appareil.

Utiliser les codes de récupération

Vous avez perdu l'accès à votre application Authenticator ? Dans ce cas, vous pouvez utiliser à la place un code de récupération enregistré lors de la configuration. Saisissez-le dans le champ de vérification Fairgate 2FA. Chaque code de récupération ne peut être utilisé qu'une seule fois.