

L3

Öffentlich

Teilnehmerportal und Admin Portal

Authentifizierung

Benutzerhandbücher 2024

Inhaltsverzeichnis

WIE DU DEIN KONTO AKTIVIERST	2
DIE WAHL DER AUTHENTICATOR-APP.....	3
AUSWÄHLEN DER SMS-AUTHENTIFIZIERUNG	5
AUSWAHL DER AUTHENTIFIZIERUNG DURCH EINEN SICHERHEITSSCHLÜSSEL	8
DER WIEDERHERSTELLUNGSCODE.....	9
WIE SIE IHRE MFA-METHODEN/IHR PASSWORT VERWALTEN.....	10
ÄNDERN DES PASSWORTS.....	14
WENN SIE IHREN WIEDERHERSTELLUNGSCODE VERLIEREN	14
WAS IST MFA?	16
WARUM IST DAS WICHTIG?	16
WANN WIRD SIE BENÖTIGT?	16
WAS SIND DIE MFA-METHODEN?.....	16
EINMALIGER CODE PER SMS	17
BEI DER ANMELDUNG.....	17
BEIM ANFORDERN EINES NEUEN PASSWORTS	19
EINMALIGER CODE PER E-MAIL.....	20
ANFORDERN EINES NEUEN PASSWORTS.....	20
DISCLAIMER	22

Wie du dein Konto aktivierst

1. Als **Teilnehmer** werden Sie eine **Aktivierungs-E-Mail** erhalten. Diese E-Mail enthält einen Link zum Portal. Sobald Sie auf diesen Link klicken, werden Sie zu (Abb. 1) weitergeleitet, wo Sie aufgefordert werden, den Aktivierungscode einzugeben, nachdem Sie auf die Schaltfläche **Aktivierungscode senden** geklickt haben.
2. Dies ist der Code, der Ihnen in einer separaten E-Mail zugesandt wurde (Abb. 2). Diese E-Mail stammt von „**Meine Aktien**“ (noreply@equityadmin.com)
3. Gib den **Code** ein
4. Nachdem du die oben genannten Schritte ausgeführt hast, wirst du zu den folgenden Bildschirmen geleitet: (Abb. 3) und (Abb. 4)
5. Erstelle deinen **Benutzername** und dein **Passwort**
6. Danach wirst du aufgefordert, deine Methoden zur MFA (Multi-Faktor-Authentifizierung) einzurichten (Abb. 5).

Informationen zur Multi-Faktor-Authentifizierung findest du im Abschnitt **Was ist MFA?**.

Abb. 1: Aktivierungscode anfordern

Activation Code

An email has been sent to your email address with an activation code. Enter the code below to continue.

Activation Code

Enter activation code

Validate

Abb. 2: E-Mail mit dem Aktivierungscode

Please, enter the following verification code in the screen as part of your account activation process to continue it.

205014

If you have any further questions, please contact us via the Helpdesk facility in your Global Shares account.

Abb. 3: Einrichten deines Benutzernamens

Let's setup your username.

Username

Enter username

Next

Abb. 4: Einrichtung deines Passworts

Create a new password.

New password

.....

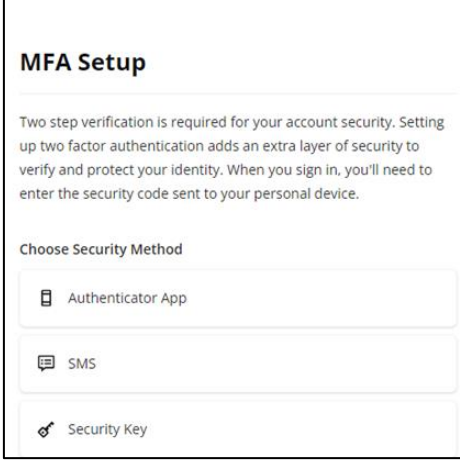
10 characters minimum

Confirm Password

.....

Create password

Abb. 5: MFA-Methoden



MFA Setup

Two step verification is required for your account security. Setting up two factor authentication adds an extra layer of security to verify and protect your identity. When you sign in, you'll need to enter the security code sent to your personal device.

Choose Security Method

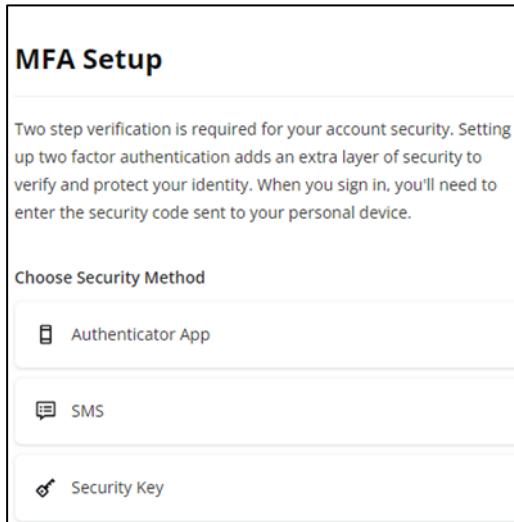
- ☒ Authenticator App
- ☐ SMS
- ☐ Security Key

Die Wahl der Authenticator-App

Wenn du mit der **Authenticator-App** (Abb. 6) fortfahren möchtest, befolge die nachstehenden Schritte:

1. Wähle einen **Namen für die Methode**: Dieser Name muss für alle deine Methoden einzigartig sein und wird dir helfen, die von dir eingerichteten Methoden zu unterscheiden (Abb. 7)
2. **Laden** Sie die **Authenticator-App** herunter (z. B. Microsoft Authenticator oder Google Authenticator. Sie können diese Authentifikatoren aus dem Apple Store für iOS oder dem Google Play Store für Android herunterladen)
3. **Scan den QR-Code** (Abb. 8).
4. **MFA-Code**, der in deiner Authenticator-App generiert wird, unter **Sicherheitscode** eintragen (Abb. 8)
5. Klicke auf **Weiter**
6. Du erhältst die Meldung, dass die von dir ausgewählte Methode **erfolgreich registriert** wurde (Abb. 9)
7. Sobald du **mindestens eine Methode** eingerichtet hast, kannst du eine **weitere Methode hinzufügen** oder auf **Weiter** klicken.

Abb. 6: Auswählen der Authenticator-App



MFA Setup

Two step verification is required for your account security. Setting up two factor authentication adds an extra layer of security to verify and protect your identity. When you sign in, you'll need to enter the security code sent to your personal device.

Choose Security Method

- ☒ Authenticator App
- ☐ SMS
- ☐ Security Key

Abb. 7: Festlegen eines Namens für die Methode



MFA Setup

AUTHENTICATOR APP

Method Name

e.g. Personal Phone - Sophos Authenticator

If you own multiple devices, naming your methods helps identify the right one.

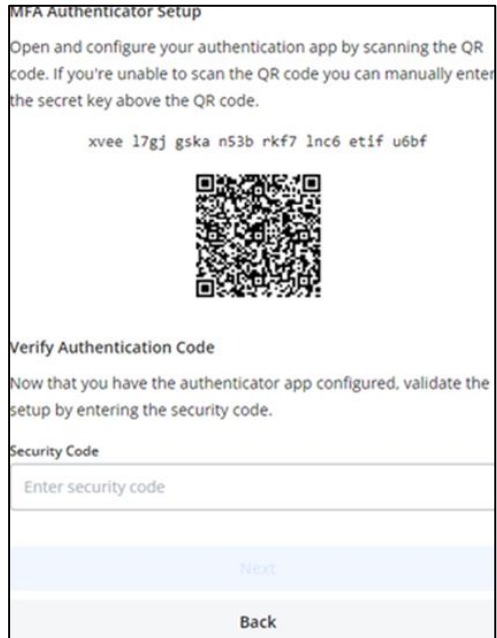
MFA Authenticator Setup

Open and configure your authentication app by scanning the QR code. If you're unable to scan the QR code you can manually enter the secret key above the QR code.

xvee 17gj gska n53b rkf7 lnc6 etif u6bf



Abb. 8: Scannen des QR-Codes



MFA Authenticator Setup

Open and configure your authentication app by scanning the QR code. If you're unable to scan the QR code you can manually enter the secret key above the QR code.

xvee 17gj gska n53b rkf7 lnc6 etif u6bf



Verify Authentication Code

Now that you have the authenticator app configured, validate the setup by entering the security code.

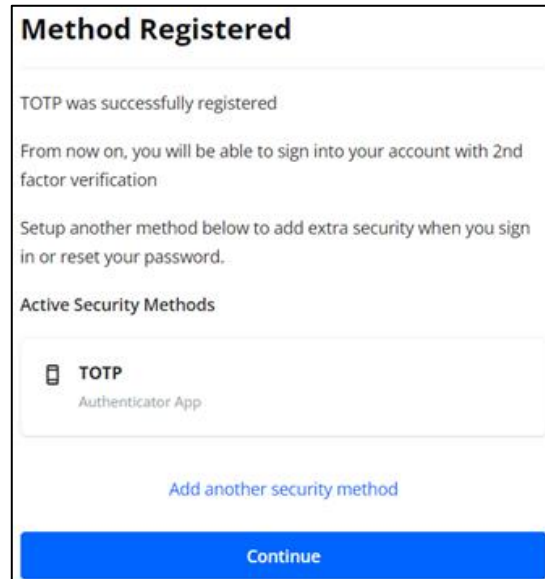
Security Code

Enter security code

Next

Back

Abb. 9: Methode registriert



Method Registered

TOTP was successfully registered

From now on, you will be able to sign into your account with 2nd factor verification

Setup another method below to add extra security when you sign in or reset your password.

Active Security Methods

- ☒ TOTP
Authenticator App

[Add another security method](#)

Continue



Der Code wird in Ihrer Authenticator-App alle 30 Sekunden neu generiert. Wenn er sich nach der Eingabe ändert, ist der Code noch eine kurze Zeit lang gültig.

Notiere dir den Namen der von dir gewählten Methode: Dieser Name muss für alle deine Methoden eindeutig sein.

Auswählen der SMS-Authentifizierung

Wir raten davon ab, SMS als einzige konfigurierte Methode zu wählen. Sie ist die unsicherste der verfügbaren Methoden. Diese Methode sollte nur als Backup-Methode verwendet werden. Wenn Sie sich für die **SMS-Authentifizierung** entscheiden (Abb. 10), führen Sie die folgenden Schritte aus:

1. Wähle einen Namen für die Methode: Dieser Name muss für alle deine Methoden eindeutig sein und wird dir helfen, die von dir eingerichteten Methoden zu unterscheiden.
2. Geben Sie Ihre Mobiltelefonnummer an. Dies ist das zulässige Format: **+[Landesvorwahl][Handynummer]** z. B. **+34671111111 (Abb. 11)**
3. Klicke auf **Weiter**
4. Du wirst aufgefordert, den **Sicherheitscode** einzugeben, der über deine Telefonnummer versendet wurde (Abb. 12).
5. Geben Sie Ihren **MFA-Sicherheitscode** ein (Abb. 13). Klicken Sie auf **Weiter**
6. Sie erhalten eine Meldung, dass Ihre ausgewählte Methode erfolgreich registriert wurde (Abb. 14).

Abb. 10: SMS-Authentifizierung

MFA Setup

Two step verification is required for your account security. Setting up two factor authentication adds an extra layer of security to verify and protect your identity. When you sign in, you'll need to enter the security code sent to your personal device.

Choose Security Method

- Authenticator App
- SMS
- Security Key

Abb. 11 Ihre Handy-Nummer angeben.

MFA Setup

SMS

Method Name

e.g. Personal Phone - Sophos Authenticator

If you own multiple devices, naming your methods helps identify the right one.

MFA SMS Setup

Enter your mobile number to receive a security code.

Mobile Number

Enter your mobile number

Next

Back

Abb. 12: Beispiel-SMS

My Equity: Enter the following 2nd factor code 512342 to confirm action. If you have any questions regarding this information, please contact Global Shares service support. Kind Regards, Your Global Shares Team

Abb. 13: Eingeben des Sicherheitscodes

MFA Setup

SMS

Verify Authentication Code

Enter the security code sent to +34671111111

Security Code

512342

Next

Back

Not received a code? [Resend](#)

Abb. 14 Methode registriert

Method Registered

SMS was successfully registered

From now on, you will be able to sign into your account with 2nd factor verification

Setup another method below to add extra security when you sign in or reset your password.

Active Security Methods

TOTP
Authenticator App

SMS
SMS

[Add another security method](#)

Continue

Abb. 15: Option zum erneuten Senden

MFA Setup

SMS

Verify Authentication Code

Enter the security code sent to +34671111111

Security Code

Enter security code

Next

Back

Not received a code? [Resend](#)



Wenn der Code Ihr Telefon nicht innerhalb von 2 Minuten erreicht, klicken Sie auf „Erneut senden“ (Abb. 15)

Auswahl der Authentifizierung durch einen Sicherheitsschlüssel

1. Befolge die Anweisungen auf dem Bildschirm (wie in Abb. 16 und Abb. 17 dargestellt).
2. Wenn dein Sicherheitsschlüssel dies erfordert, erscheint ein Pop-up-Fenster, das den in deinem Schlüssel konfigurierten **PIN-Code** abfragt. Bitte gib den Code an.
3. Klicke auf **Weiter**
4. Klicken Sie auf **Authentifizieren** (Abb. 18) und folgen Sie den Anweisungen Ihres Betriebssystems.



Wir empfehlen die Wahl des Sicherheitsschlüssels, da dies die sicherste Methode ist.

Abb. 16: MFA-Einrichtung – Sicherheitsschlüssel

MFA Setup

Two step verification is required for your account security. Setting up two factor authentication adds an extra layer of security to verify and protect your identity. When you sign in, you'll need to enter the security code sent to your personal device.

Choose Security Method

- Authenticator App
- SMS
- Security Key

Abb. 17 MFA-Einrichtung – Name der Methode

MFA Setup

SECURITY KEY

Method Name

e.g. Personal Phone - Sophos Authenticator

If you own multiple devices, naming your methods helps identify the right one.

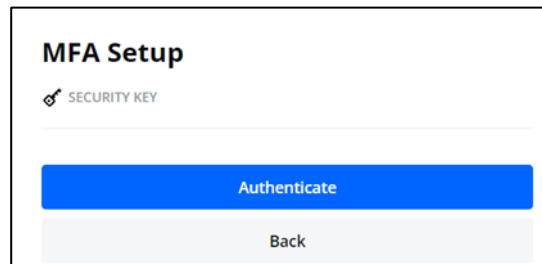
Register Your Security Key

Insert your security key into a USB port, or connect it using NFC. If the key has a blinking light, press the button or gold disk.

Next

Back

Abb. 18: Authentifizieren



MFA Setup

SECURITY KEY

Authenticate

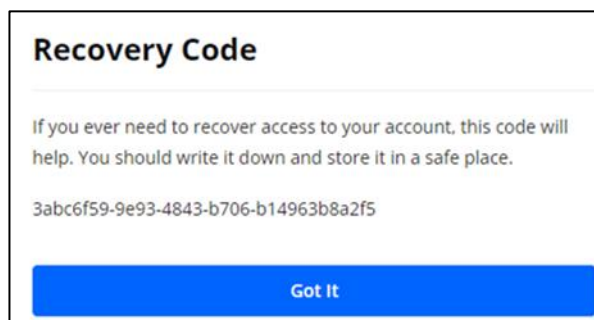
Back

Der Wiederherstellungscodes

Sobald Sie Ihre **Authentifizierungsmethode(n)** erfolgreich eingerichtet haben, generiert das System einen **Wiederherstellungscodes** (Abb. 19)

1. Sie müssen den Code **kopieren** und ihn an einem sicheren Ort außerhalb Ihres **Kontos speichern**
2. Sobald du auf „**Erhalten**“ klickst, verschwindet der Code und kann nicht mehr abgerufen werden
3. Sobald Sie dies getan haben, erhalten Sie die folgende Aufforderung (Abb. 20).

Abb. 19: Wiederherstellungscodes



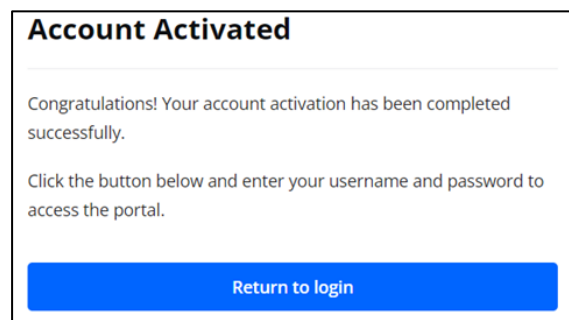
Recovery Code

If you ever need to recover access to your account, this code will help. You should write it down and store it in a safe place.

3abc6f59-9e93-4843-b706-b14963b8a2f5

Got It

Abb. 20: Konto aktiviert



Account Activated

Congratulations! Your account activation has been completed successfully.

Click the button below and enter your username and password to access the portal.

Return to login



Der Wiederherstellungscodes wird nicht in Ihrem Konto gespeichert. Er ist keine Authentifizierungsmethode. Der Wiederherstellungscodes ist eine letzte Option, wenn keine Ihrer MFA-Methoden verfügbar ist (z. B. wenn Sie Ihr Telefon verloren haben). Bitte bewahren Sie den Wiederherstellungscodes an einem sicheren Ort auf! Wenn Sie Ihren Wiederherstellungscodes verlieren, können Sie auf der Registerkarte Sicherheit unter „Mein Konto“ - „Mein Profil“ in Ihrem Konto einen neuen Code generieren.

Bitte lies den Abschnitt **Wenn du deinen Wiederherstellungscodes verlierst**, um zu erfahren, was zu tun ist, wenn du deinen **Wiederherstellungscodes** verlegt hast.

Wie Sie Ihre MFA-Methoden/Ihr Passwort verwalten

1. Klicke auf **Mein Konto** (Abb. 21)
2. Wähle **Mein Profil** aus
3. Klicke auf **Mein Konto-Präferenzen**
4. Wähle **Sicherheit** aus (Abb. 22)
5. Klicke auf **Erste Schritte** unter **MFA-Methoden verwalten** (Abb. 23)
6. Wähle aus den **MFA-Methoden** aus, die du hinzufügen oder entfernen möchtest (Abb. 24)
7. Unter **Detail** sehen Sie den **Namen der eindeutigen Methode**. Bei **SMS** umfasst dies die teilweise versteckte **Mobiltelefon - Nummer**,
8. Sie können nicht alle MFA-Methoden entfernen. Die Schaltfläche **Entfernen** ist deaktiviert, wenn nur 1 MFA Methode eingerichtet ist (Abb. 25).

Abb. 21 Mein Konto

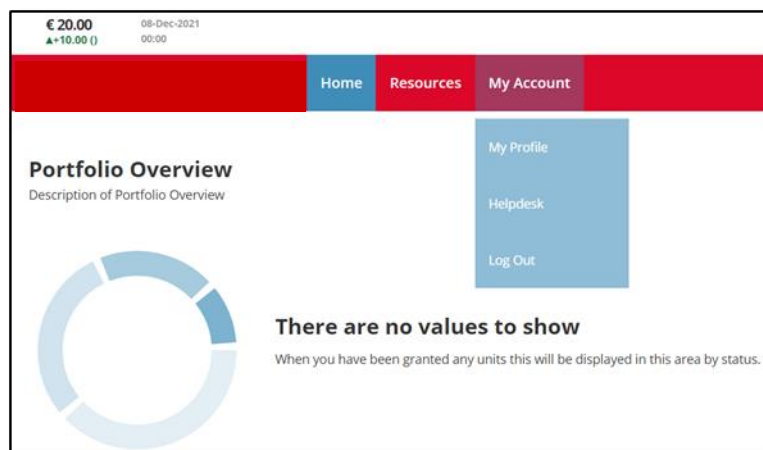


Abb. 22: Auswählen von „Sicherheit“

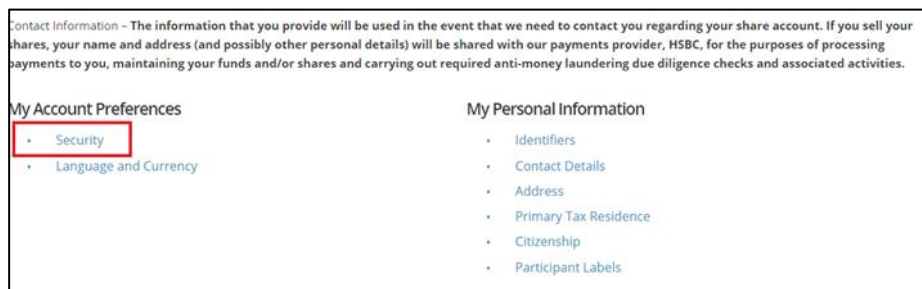
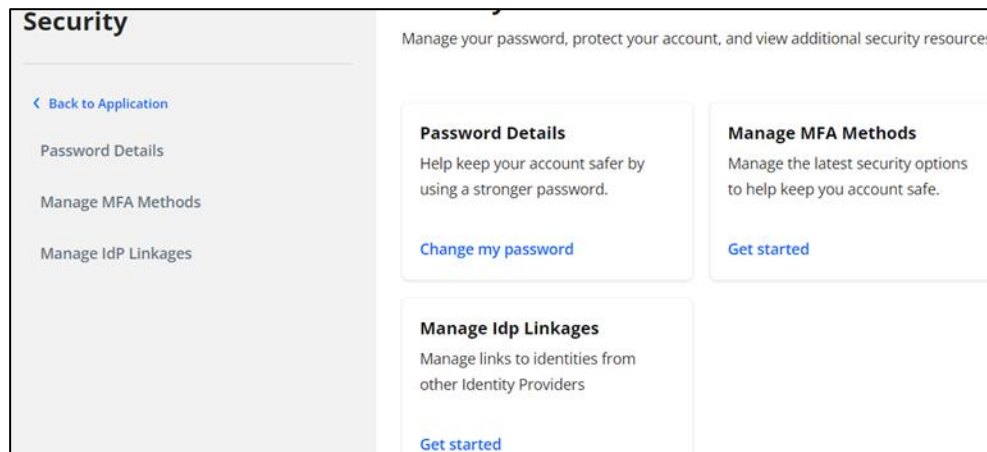


Abb. 23: MFA-Methoden verwalten



Für SSO-Benutzer (Single-Sign-On) wird die Registerkarte Sicherheit unter Meine Konto-Präferenzen deaktiviert, da diese für den SSO-Zugang nicht anwendbar ist.

Abb. 24: MFA-Methoden verwalten

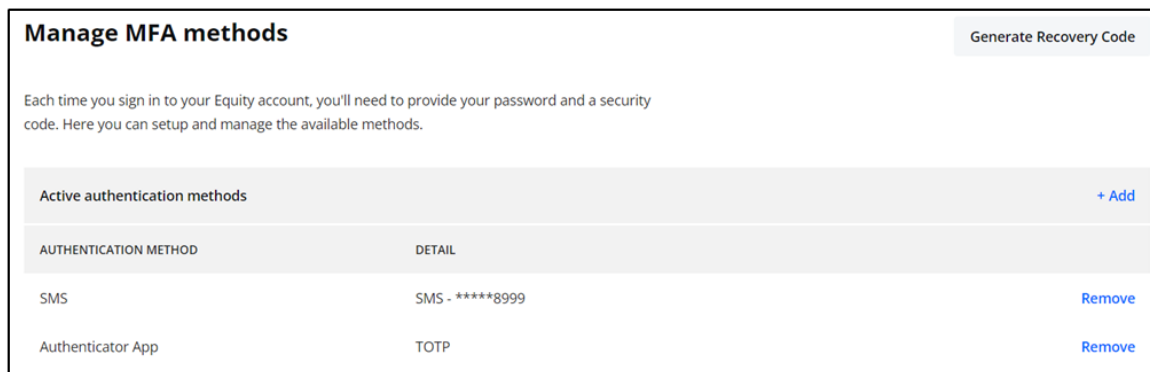
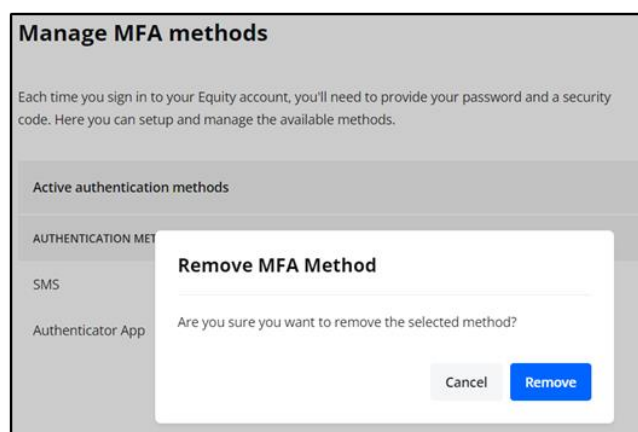


Abb. 25: Entfernen der MFA-Methode



Es ist möglich, mehrere Methoden desselben Typs zu konfigurieren. Beispielsweise zwei Apps, oder SMS für zwei verschiedene Telefonnummern.



Wir raten davon ab, die SMS als einzige konfigurierte Methode zu wählen, da sie die unsicherste der verfügbaren Methoden ist. SMS sollte nur als Backup-Methode verwendet werden.

Authenticator-App

Authentication

 AUTHENTICATOR APP - XIAOMI MI 9 LITE - MICROSOFT

To authenticate please type in the code displayed in your authenticator app in your device Xiaomi Mi 9 lite - Microsoft.

Security Code

[Validate](#)

[Back](#)

Having trouble? [Log in another way](#)

SMS-Authentifizierung

Authentication

 SMS - PERSONAL MOBILE XIAOMI - +*****3398

To authenticate please type in the code you have received in your mobile device.

We have sent a text message to personal mobile xiaomi - +*****3398. [Resend](#)

Security Code

[Validate](#)

[Back](#)

Having trouble? [Log in another way](#)

Fido2 – Authentifizierung per Sicherheitsschlüssel

Authentication

 SECURITY KEY - YUBICO

Insert your security key (yubico) into a USB port, or connect it using NFC. If the key has a blinking light, press the button or gold disk.



[Next](#)

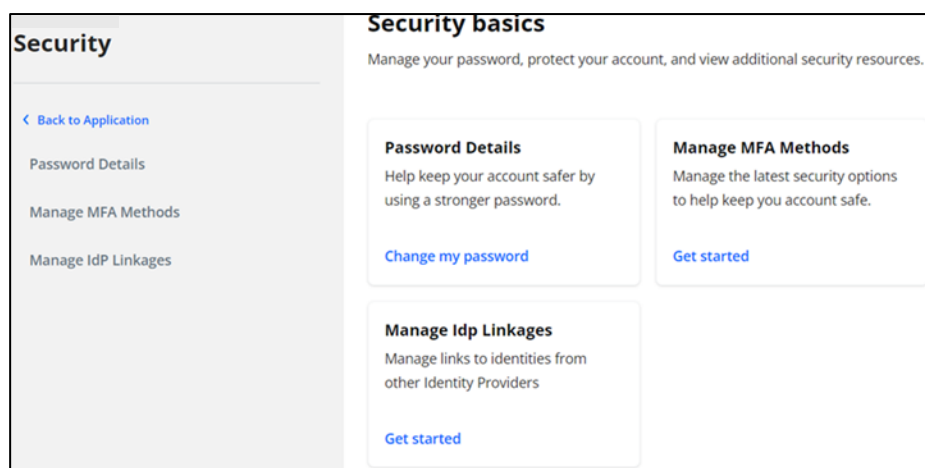
[Back](#)

Having trouble? [Log in another way](#)

Ändern des Passworts

1. Klicke im Bereich **Sicherheit** auf **Mein Passwort ändern** (Abb. 26)
2. Folgen Sie den Anweisungen auf dem Bildschirm
3. Dein **Passwort** muss **mindestens 10 Zeichen** enthalten.
4. **Sonderzeichen sind nicht mehr zwingend erforderlich, können aber verwendet werden. Dazu gehören Großbuchstaben, Kleinbuchstaben, Zahlen und Symbole.**
5. Du kannst kein Wort verwenden, das in einem **Wörterbuch** steht. Wir empfehlen dir, eine **Phrase** zu bilden, anstatt ein Wort zu verwenden. Alternativ kannst du auch **Zahlen** und **Symbole** hinzufügen.
6. Es gibt eine **Liste von Wörtern**, die **verboten** sind. Diese werden nicht akzeptiert, da sie zu häufig verwendet werden.

Abb. 26: Details zum Passwort



Wenn Sie Ihren Wiederherstellungscodes verlieren

1. Wenn du deinen Wiederherstellungscodes verlierst, kannst du einen neuen erstellen.
2. Gehe zu **Sicherheit**
3. Klicke auf **Erste Schritte** unter **MFA-Methoden verwalten** (Abb. 26)
4. Wähle **Wiederherstellungscodes generieren** aus (Abb. 27)
5. Sie erhalten einen neuen **Wiederherstellungscodes** (Abb. 28), den Sie außerhalb Ihres Kontos sicher aufbewahren müssen.

Abb. 27: Verwalten der MFA-Methoden

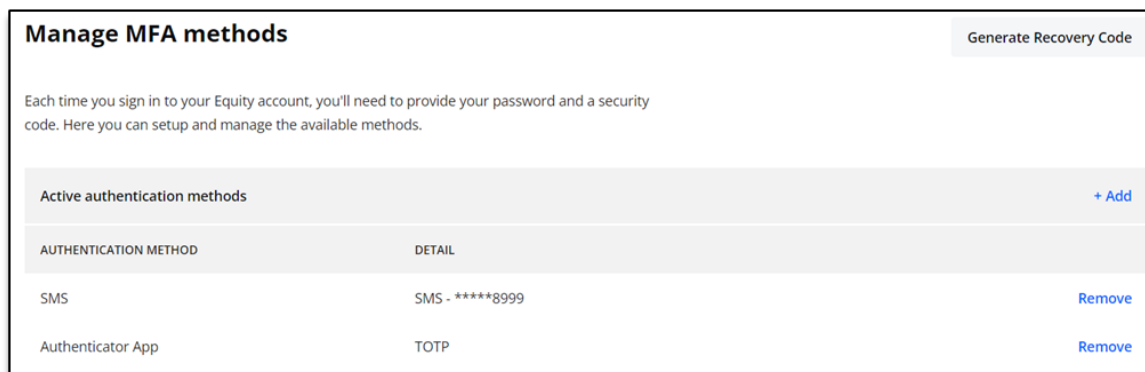
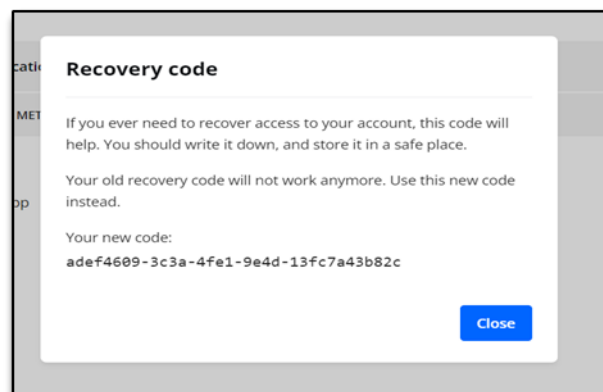


Abb. 28: Generieren eines Wiederherstellungscodes



Was ist MFA?

Multi-Faktor-Authentifizierung (MFA) ist eine Authentifizierungsmethode, bei der Sie 2 (oder mehr) Verifizierungsfaktoren angeben müssen, um Zugang zu einer Ressource (wie einer Anwendung oder einem Online-Konto) zu erhalten.

Warum ist das wichtig?

Es erhöht die Sicherheit, **da Sie sich mit mehr als einem Benutzernamen und einem Passwort identifizieren müssen**. Benutzernamen und Passwörter sind anfällig für Brute-Force-Angriffe und können von Dritten gestohlen werden. Wenn Sie die Verwendung von MFA erzwingen, können Sie sicher sein, dass Ihr Konto vor Cyberkriminellen sicher bleibt.



Für Single Sign-On (SSO) Benutzer: Es ist nicht möglich, MFA zu aktivieren, wenn Sie sich über SSO bei Ihrem Konto anmelden. Um den MFA-Aktivierungsprozess abzuschließen, müssen Sie ein Konto aktivieren oder sich mit Ihrem Konto unter Verwendung Ihres Benutzernamens und Passworts (nicht mit den Daten, die bei der SSO-Anmeldung verwendet wurden) anmelden.

Wann wird sie benötigt?

Die Multi-Faktor-Authentifizierung wird **immer** als Teil des Anmeldevorgangs angefordert, nachdem der **richtige Benutzername** und das richtige **Passwort** eingegeben wurden. Wenn Sie versuchen, Ihr Passwort zu ändern oder die MFA-Einrichtung über das Sicherheitsportal zu modifizieren, kann die MFA erneut angefordert werden. Dies geschieht, wenn seit Ihrer Anmeldung einige Zeit vergangen ist. Dies ist eine Sicherheitsmaßnahme, um Ihre Identität zu überprüfen.

Was sind die MFA-Methoden?

Du wirst aufgefordert, mehr als eine Multi-Faktor-Authentifizierungsmethode zu konfigurieren. Es gibt drei Methoden: **Authenticator-App**, **FIDO2-Sicherheitsschlüssel** und **SMS**. Es ist möglich, mehrere Methoden desselben Typs zu konfigurieren. Beispielsweise zwei Apps oder zwei SMS.

Authenticator-App: Eine Authenticator-App eines Drittanbieters ermöglicht die **Zwei-Faktor-Authentifizierung**, indem sie einen zufällig generierten und ständig aktualisierten Code anzeigt, den Sie verwenden können. Beispiele für Authenticator-Apps von Drittanbietern sind **Google Authenticator**, **Microsoft Authenticator** und **Authy**.

SMS: Mit der SMS-Authentifizierung können Sie sich mit einem **einmaligen Passcode** (OTP) authentifizieren, der in einer SMS-Nachricht an Ihr Telefon übermittelt wird.

FIDO2-Sicherheitsschlüssel: FIDO2 USB-Token sind Geräte, die physisch mit dem zu verwendenden Computer verbunden sind. Diese Geräte übertragen automatisch Daten und authentifizieren Sie als Benutzer. Beispiele hierfür sind **Yubico Security Keys** und **Chipne**. **FIDO2** ermöglicht es Ihnen, gängige Geräte zur einfachen Authentifizierung bei Online-Diensten sowohl in mobilen als auch in Desktop-Umgebungen zu nutzen. Dieses Gerät wird nicht von der Firma zur Verfügung gestellt.



Dies ist die unsicherste der unterstützten Methoden. Wir empfehlen, diese Methode nur als Backup zu verwenden und die App und/oder die Sicherheitsschlüssel täglich zu benutzen.

Einmaliger Code per SMS

Die Option des **einmaligen Codes per SMS** ist ein neues Sicherheitsmerkmal, das in den folgenden Fällen zur Identifizierung Ihrer Identität verwendet wird:

- Hilfe bei der Anmeldung, wenn deine Authentifizierungsmethoden nicht verfügbar sind oder du zuvor keine Authentifizierungsmethode konfiguriert hast
- Passwort vergessen
- Passwort zurücksetzen.

Bei der Anmeldung

Beim Anmelden wirst du aufgefordert, deine MFA-Code einzugeben. Wenn keine der von dir eingerichteten Methoden verfügbar ist oder du keine konfiguriert hast, befolge bitte die nachstehenden Schritte:

1. Klicke auf **Auf andere Weise anmelden**, wenn deine MFA-Verifizierung angefordert wird (Abb. 29)
2. Dies öffnet den Bildschirm **Sicherheitsmethode wählen** (Abb. 30)
3. Klicken Sie auf die Option **Einmaliger Code**
4. Sie werden aufgefordert, Ihre **Mobil-/Handynummer** anzugeben. Dazu müssen Sie **+** und die **Landesvorwahl** eingeben (Abb. 31).

5. Sobald Sie Ihre Mobil-/Handynummer eingegeben haben, wird ein **Sicherheitscode** an Ihr Gerät gesendet. Bitte geben Sie den Code in das Feld **Sicherheitscode** ein (Abb. 32)
6. Sobald du den Code eingegeben hast, kannst du auf dein Konto zugreifen.

Abb. 29: Sicherheitscode

Authentication

AUTHENTICATOR APP - TOTP

To authenticate please type in the code displayed in your authenticator app in your device TOTP.

Security Code

Enter security code

Validate

Back

Having trouble? [Log in another way](#)

Abb. 30 Sicherheitsmethode auswählen

Authentication

Two step verification is required for your account security. Choose which security method you want to use in order to safely authenticate your account.

Choose Security Method

otp
Authenticator App

Having trouble? Use your [recovery code](#)

Send one-time code to your phone +*****3398

Abb. 31: Eingeben der Mobiltelefonnummer

Authentication

SMS

We will send the security code to +*****3398.

To verify that this is your mobile number, please enter it below.

Mobile Number

'+' followed by country code and number

Validate

Back

Abb. 32: Eingeben des Sicherheitscodes

Authentication

SMS

To reset your password please type in the code you have received in your mobile device.

We have sent a text message to [Resend](#)

Security Code

Enter security code

Validate

Back

Having trouble? [Log in another way](#)

Beim Anfordern eines neuen Passworts

Der **Einmal-Code** wird automatisch ausgelöst, wenn du dein **Passwort zurücksetzen** möchtest oder **dein Passwort vergessen** hast, sofern keine MFA-Methode konfiguriert ist.

Wenn die konfigurierten MFA-Methoden zu diesem Zeitpunkt **nicht verfügbar** sind, führe bitte die folgenden Schritte aus:

1. Wähle **Auf eine andere Weise anmelden** aus (Abb. 33)
2. Sobald Sie auf diese Option geklickt haben, öffnet sich der Bildschirm **Einmaliger Code auswählen** (Abb. 34).



Der Einmal-Code wird nicht angezeigt, wenn eine SMS-Methode konfiguriert wurde.

Abb. 33: Anmeldung auf andere Weise

The screenshot shows the 'Authentication' screen for TOTP. At the top, it says 'AUTHENTICATOR APP - TOTP'. Below that, it instructs the user to type the code from their authenticator app. There is a text input field labeled 'Security Code' with the placeholder 'Enter security code'. Below the input field are two buttons: 'Validate' (blue) and 'Back' (grey). At the bottom, there is a link: 'Having trouble? Log in another way'.

Abb. 34: Auswahl des Einmal-Codes

The screenshot shows the 'Authentication' screen for choosing a security method. It states: 'Two step verification is required for your account security. Choose which security method you want to use in order to safely authenticate your account.' Below this is a section 'Choose Security Method' with a button labeled 'otp' and 'Authenticator App'. At the bottom, there are two links: 'Having trouble? Use your recovery code' and 'Send one-time code to your phone +*****3398'.

Einmaliger Code per E-Mail

Die Option **Einmal-Code per E-Mail** ähnelt der SMS-Option, ist jedoch nur in Ausnahmesituationen verfügbar. Sie ist während der **Zurücksetzung des Passworts** zu sehen und ausschließlich dann, wenn für dein Konto **keine** Methode zur Multi-Faktor-Authentifizierung konfiguriert wurde.

Anfordern eines neuen Passworts

Der **Einmal-Code** wird automatisch ausgelöst, wenn du **dein Passwort zurücksetzen** möchtest und **keine andere Methode** konfiguriert hast.

1. Wenn ein **Einmal-Code per SMS** ausgelöst wird, aber zu diesem Zeitpunkt nicht verfügbar ist, kannst du auf die Schaltfläche **Zurück** klicken (Abb. 35)
2. Sobald du diese Option angeklickt hast, wähle die Option **Einmal-Code per E-Mail senden** aus (Abb. 36).
3. Wenn du den **Einmal-Code per E-Mail** ausgewählt hast, wirst du aufgefordert, deine **E-Mail-Adresse** anzugeben (Abb. 37)
4. Nachdem du deine E-Mail-Adresse eingegeben hast, erhältst du eine E-Mail mit einem **Sicherheitscode**. Gib den Code in das Feld **Sicherheitscode** ein (Abb. 38)
5. Sobald der Code eingegeben und akzeptiert wurde, wird die Anwendung ein **neues Passwort anfordern**.

Abb. 35 Schaltfläche „Zurück“ auswählen

The screenshot shows an 'Authentication' screen with an 'SMS' icon. It states: 'We will send the security code to +*****3398. To verify that this is your mobile number, please enter it below.' There is a text input field for the 'Mobile Number' with a placeholder: '+ followed by country code and number'. Below the input field are two buttons: 'Validate' (light blue) and 'Back' (light grey).

Abb. 36: Senden des Einmal-Codes

The screenshot shows an 'Authentication' screen. It states: 'Two step verification is required for your account security. Choose which security method you want to use in order to safely authenticate your account.' Below this is a yellow warning box with a triangle icon and the text: 'Warning No MFA methods available.' At the bottom, there are two options: 'Send one-time code to your phone +*****3398' and 'Send one-time code to your email b*b@bbb.com'.

Abb. 37: Eingeben der E-Mail Adresse

Authentication

EMAIL

We will send the security code to b*b@bbb.com.

To verify that this is your email address, please enter it below.

Email Address

Validate

Back

Abb. 38: Eingeben des Sicherheitscodes

Authentication

EMAIL

To reset your password please type in the code you have received in your email address.

We have sent a text message to [Resend](#)

Security Code

Validate

Back

Having trouble? [Log in another way](#)

Disclaimer

J.P. Morgan Workplace Solutions is a brand name for equity compensation administration business conducted by Global Shares and other financial products and services offered through J.P. Morgan Securities LLC and other affiliates of J.P. Morgan Chase & Co.

Global Shares is a trading name of the legal entities described hereafter including Global Shares Ireland Limited ("Global Shares Ireland"), a company registered in Ireland, registration number 412396 with its registered office at Unit 2, Building D, West Cork Technology Park, Clonakilty, Co, Cork, Ireland which provides share plan administration services and software. Global Shares Inc. ("Global Shares US") is incorporated in Delaware and provides share plan administration services and software to certain U.S. Companies.

For securities traded in United States markets, Broker Dealer Services are provided by Global Shares Financial Services, Inc. ("GSFS"), Member FINRA/SIPC, 575 Washington Blvd, Floor 09, Jersey City, NJ, 07310-1616, (646) 968-0653. Check the background of Our Firm on FINRA's BrokerCheck.

Global Shares Trustees Ireland Limited, Global Shares Trustees (UK) Limited, and Global Shares Trustees Company Limited (collectively, the "Trust Companies"), are Irish and UK trust companies that provide limited trust services for corporate share plans.

Global Shares Execution Services Limited ("GSESL") is licensed to conduct investment services business under the Investment Services Act as authorised by the Malta Financial Services Authority ("the MFSA") pursuant to licence number GSES-IF-14206. GSESL offers receipt and transmission of orders and nominee services under its provision of business. The registered address is at 171, Old Bakery Street, Valletta, VLT1455, Malta. Global Shares Ireland, Global Shares US, GSFS, the Trust Companies, and GSESL are affiliated companies and all under the common control of JPMorgan Chase & Co.