Two-Factor Authentication (MFA) Help Guide

Getting Started · https://behca.com/support/two-factor-authentication-mfa-help-guide/

What is Two-Factor Authentication?

Two-Factor Authentication (also called MFA or 2FA) adds an extra layer of security to your BEHCA account. After entering your password, you'll also need to enter a 6-digit code from an authenticator app on your phone. This means even if someone knows your password, they can't access your account without your phone.

Web App Instructions

Setting Up MFA

What you'll need:

- A smartphone with an authenticator app installed (see recommendations below)

Recommended Authenticator Apps (free):

- **Google Authenticator** - iPhone | Android
- **Microsoft Authenticator** - iPhone | Android
- **Authy** - iPhone | Android
- Or use the authenticator app provided by your organization admin (1Password, Bitwarden, etc.)

Steps to set up MFA:

1. Log in to your BEHCA account
2. Click your initials in the top-right corner
3. Click **My Account**
4. Scroll down to the **Security** section

5. Click **Set Up Two-Factor Authentication**
6. Open your authenticator app on your phone
7. In your authenticator app, tap the **+** button or **Add Account**
8. Select **Scan QR Code**
9. Point your phone's camera at the QR code on your screen
10. Your authenticator app will show a 6-digit code
11. Enter that code and click **Verify and Enable MFA**
12. **Important:** Save your recovery codes! Copy or download them and store them somewhere safe

Signing In with MFA

1. Enter your email and password as usual
2. When prompted, open your authenticator app
3. Find BEHCA in your list of accounts
4. Enter the 6-digit code shown (codes change every 30 seconds)
5. Optional: Check "Trust this device for 30 days" if you're on your personal computer
6. Click **Verify**

Using Recovery Codes

If you don't have access to your authenticator app:

1. On the verification screen, click **Use recovery code instead**
2. Enter one of your saved recovery codes
3. Click **Verify**

Note: Each recovery code can only be used once. After using all your codes, generate new ones from your account settings.

Managing MFA Settings

To view or regenerate recovery codes:

1. Go to **My Account → Security → Manage Two-Factor Authentication**
2. Enter your current authenticator code

3. Click **Generate New Recovery Codes**
4. Save your new codes

To disable MFA (if allowed by your organization):

1. Go to **My Account → Security → Manage Two-Factor Authentication**
2. Scroll to "Disable MFA"
3. Enter your password
4. Click **Disable MFA**

Mobile App Instructions

Signing In with MFA

1. Enter your email and password
2. When prompted, open your authenticator app
3. Enter the 6-digit code shown for BEHCA
4. Tap **Verify**

Using Recovery Codes on Mobile

1. On the verification screen, tap **Use recovery code instead**
2. Enter one of your saved recovery codes
3. Tap **Verify**

Troubleshooting

"Invalid code" error

- Make sure you're entering the code for BEHCA (not another account)
- Codes change every 30 seconds - try waiting for a new code
- Check that your phone's time is set correctly (Settings → Date & Time → Set Automatically)

Lost access to authenticator app

- Use one of your saved recovery codes to sign in
- Once signed in, go to your account settings and under **Security Code** click **Reset your MFA**
- If you don't have recovery codes, contact your administrator for help

New phone

If you got a new phone:

1. Some authenticator apps (like Authy) can sync across devices
2. If your old phone still works, you can disable MFA and set it up again on your new phone
3. If you can't access your old phone, use a recovery code to sign in, then set up MFA again

Organization requires MFA

If your organization requires MFA, you won't be able to disable it. Contact your administrator if you have questions.

Frequently Asked Questions

Q: Do I need to enter a code every time I sign in? A: You can check "Trust this device for 30 days" when signing in. After that, you won't need to enter a code on that device for 30 days.

Q: What if I lose my phone? A: Use your saved recovery codes to sign in. That's why it's important to save them somewhere safe!

Q: Can I use the same authenticator app for multiple accounts? A: Yes! Apps like Google Authenticator can store codes for many different services.

Q: Is MFA required? A: Some organizations require MFA for all users. Check with your administrator.

Need More Help?

Contact BEHCA Support at support@behca.com