User Login

Logging In For The First Time

Step 1: Determine Log-in Method

When visiting the login screen, you will be provided with two options for logging in:

1. **Tekside Credentials** - Enter the username and password provided to you when your account was setup
2. **Google Account** - If the email address that was used to create you account is a Google account, then you can use that to login instead.

> Using your Google Account eliminates the need to use a Authentication app for Two-Factor Authentication (2FA)

Step 2: Setting Up Two-Factor Authentication (2FA) - Tekside Credentials

After providing your credentials, you will be asked to set up an authenticator app for 2FA.

Follow the on screen instructions to setup your Authenticator app. If you run into any issues or would like more details around 2FA, please read the following article: Setting Up Two-Factor Authentication (2FA)

Step 3: Test 2FA

After your authenticator app is verified with the one-time code, you will be redirected into CONNECT. Before you begin using the platform we recommend testing your 2FA setup:

1. Log out of your account.
2. Log back in using your credentials.
3. Complete the second authentication step (i.e. entering the code from your app).

If everything works correctly, you will be redirected back into CONNECT and can start using the platform.

> For additional Tips and Tricks and Troubleshooting 2FA, click here.

Setting Up Two-Factor Authentication (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your accounts by requiring a second form of verification in addition to your password. Here's a step-by-step guide to setting it up.

Why Do We Require Two-Factor Authentication?

Passwords can be stolen or guessed, but 2FA makes it significantly harder for attackers to gain access to your accounts. Even if someone has your password, they'll also need the second factor (such as a code sent to your phone or an authentication app) to log in.

> **First time logging in?** Following these instructions to setup your two-factor authentication at the login screen.

Step 1: Choose Your 2FA Method

Currently, CONNECT only supports 2FA through the use of Authentication Apps:

1. **Authentication Apps**: Install one of the following apps on your mobile device. These generate time-based one-time passwords (TOTP), such as:
   - Google Authenticator
   - Authy
   - Microsoft Authenticator

Step 2: Set Up Your Authentication App

If you're using an authentication app:

1. Download and install an app like Google Authenticator or Authy on your smartphone.
2. Navigate to your account settings, select "Authenticator" on the left panel.
3. Scan the QR code displayed on the website using your app.

4. Enter the one-time code generated by the app at the bottom and click "Save" to verify and complete the setup.

Step 3: Test 2FA

1. Log out of your account.
2. Log back in using your password.
3. Complete the second authentication step (i.e. entering a code from your app).

Tips for Using 2FA

- **Use an Authentication App**: Apps are generally more secure than SMS.
- **Avoid Public Wi-Fi**: Be cautious when accessing your accounts on public networks.
- **Update Your 2FA Method**: If you change your phone number or device, update your 2FA settings immediately.

Troubleshooting

- **Lost Phone or Device**: Contact our customer support for account recovery.
- **Code Not Working**: Ensure your device’s clock is synced correctly when using an authentication app.

By following these steps, you can protect your accounts from unauthorized access and enjoy greater peace of mind.