

Setting Up Microsoft Authenticator at Mas Wild Labs

Introduction

Protecting company data is everyone's responsibility at **Mas Wild Labs**. To mitigate reputational and technical risk, we require Multi-Factor Authentication (MFA) for all logins to the company portal from any external mobile device. MFA adds a critical layer of security, ensuring our technical findings are backed by verified access protocols.

Prerequisites

Before beginning the setup, ensure you have the following:

- A smartphone or tablet with the **Microsoft Authenticator** app installed (iOS or Android).
 - Your **Mas Wild Labs** company-issued laptop.
 - Your current **Mas Wild Labs** login credentials.
-

Configuration Procedure

1. Access Security Settings

- Log in to the **Mas Wild Labs** company portal on your laptop.
- Click your **Profile Icon** in the top-right corner and select **Account Settings**.
- From the left-hand sidebar, click **Security & Login**.

2. Initiate MFA Setup

- Locate the **Two-Step Verification** section and click the **Set-Up MFA** button.
- Select **Mobile App** from the dropdown menu to ensure data integrity.

3. Generate and Link the QR Code

- Click **Next** on your computer screen to display a unique **QR code**.
- Open the **Microsoft Authenticator** app on your phone.
- Tap the **plus (+) icon**, select **Work or School Account**, and choose **Scan QR Code**.
- Point your phone's camera at your computer screen to link the device.

4. Verify Technical Connection

- On your computer, enter the current 6-digit code from the app into the **Verification Box** and click **Verify**.
- This establishes a **verifiable data link** between your device and the server.

5. Save Backup Recovery Codes

- Once verified, the portal will prompt you to create a **Master Password**.
- **Mandatory Protocol:** Store this password in a secure, secondary location; it is required to protect **Mas Wild Labs** data if your device is lost or stolen.

Conclusion

Your **Mas Wild Labs** portal account is now secured with MFA. Future logins from new devices will require a **six-digit code** to maintain our industry-leading technical standards.

Note: If you encounter **Invalid Code** errors, please contact the **IT Help Desk** at **extension 404** to resolve the synchronization conflict.