🔒 Comprehensive Two-Factor Authentication (2FA) Knowledge Base

1. Overview: The Core of 2FA

Two-Factor Authentication (2FA) provides a strong defense against unauthorized access by requiring a two-part identity verification process during login. This significantly mitigates the risk of breaches caused by stolen or compromised passwords.

1.1 The Two Factors Defined

Factor	**Description**	**Example**	**Security Principle**
Factor 1: Knowledge	Something only the user **knows**.	Your **Password** or a security PIN.	Secret
Factor 2: Possession	Something only the user **has**.	A code from a **mobile device** or a **physical key**.	Token/Possession

---

2. Step-by-Step Setup Guide

Follow this process to enable the highest level of security for your account.

Step 1: Navigate to Security Settings

1. Log into your account via the web portal.
2. Click on your **Profile Icon** in the upper right-hand corner.
3. Select **Account Settings** $\rightarrow$ **Security**.
4. Find and select **"Enable Two-Factor Authentication."**

Step 2: Choose Your Method

You will be prompted to select a verification method. We highly recommend using an **Authenticator App** (Method A) over SMS (Method B).

Method A: Authenticator App (Recommended)	**Method B: SMS (Backup Only)**
Download a TOTP app (Google Authenticator, Authy, etc.).	Select the SMS option.
The system will display a **QR Code**. Scan this code with your app.	Enter your mobile phone number.

The app will generate a 6-digit code. Enter this code into the prompt to confirm linkage.	A code will be sent to your phone. Enter the code to confirm linkage.

Step 3: Save Your Recovery Codes (Crucial!)

After successful activation, the system will display 10 unique **Recovery Codes**.

- **Action:** Print them or save them in a secure password manager.
- **Warning:** These codes are your **only backup** if you lose your phone or access to your authenticator app. They are single-use codes.

---

3. Expanded Frequently Asked Questions (FAQ)

Question	**Answer**
What is the difference between 2FA and MFA?	**2FA** (Two-Factor Authentication) requires *exactly* two factors. **MFA** (Multi-Factor Authentication) is a broader term, meaning *two or more* factors. For most users, the terms are interchangeable when referring to password + app code security.
Why is using an Authenticator App better than SMS?	SMS codes are vulnerable to SIM-swapping attacks, where a malicious actor convinces your carrier to transfer your phone number to their device. Authenticator apps (TOTP) are device-based and immune to this risk, offering superior protection.
How long are the codes valid for?	The time-based codes generated by Authenticator Apps (TOTP) are valid for a very short duration, typically **30 seconds**. This is why you must enter them quickly after generation.
Can I use a hardware security key (e.g., YubiKey)?	Yes. We support FIDO2/U2F hardware keys for the most robust security. These keys replace the authenticator app step and are inserted into your computer's USB port. See the Advanced Settings section to register a hardware key.

---

4. Troubleshooting and Recovery

Scenario A: I cannot log in using my 2FA code.

- **Check Time Sync:** Most code issues are due to an incorrect clock on your phone. Ensure your mobile device's date and time are set to **"Automatic"** or "Network Provided" to keep it synced with the TOTP standard.
- **Re-scan the QR:** If the time is correct, disable 2FA (if possible using a recovery code) and re-enable it by scanning the QR code again to reset the key.

Scenario B: Account Recovery (Lost Phone/Codes)

If you have lost both your authenticator app access and your recovery codes:

1. Navigate to the login page and click **"Cannot access 2FA codes?"**
2. You will be required to start the **Manual Account Recovery** process.
3. This process involves submitting government-issued ID and waiting 3-5 business days for a security review before the 2FA setting can be manually disabled by an administrator.

---

5. 💡 Security Best Practices

- **Protect Your Recovery Codes:** Store them in a fireproof safe, a secure password manager, or printed out and secured, but **never** digitally on the same device where you conduct your normal business.
- **Beware of Phishing:** Our system will **never** ask you to provide your 2FA code via email, phone, or instant message. Any request for the code outside of the official login screen is a **scam attempt**.
- **Regular Audits:** Occasionally review your Security Settings to ensure no unauthorized devices are linked to your account.