Fortifying Your Digital Defences

A comprehensive guide to setting up Two-Factor Authentication (2FA) for both cPanel and CentOS Web Panel (CWP) users. Enhance your account security with this essential layer of protection.

Why 2FA Matters

1

Enhanced Security

Even if your password is compromised, 2FA prevents unauthorised access to your accounts.

2

Data Protection

Safeguard sensitive information and critical website data from malicious actors.

3

Compliance & Trust

Adherence to security best practices builds trust with your users and stakeholders.

Understanding the critical role of 2FA is the first step towards a more secure online presence.

Essential Prerequisites

Before diving into the setup, you'll need a Time-based One- Time Password (TOTP) application installed on your mobile device. This app will generate the dynamic security codes required for 2FA.

Popular choices include:

Google Authenticator: Available for Android and iOS.
Duo Mobile: Available for Android and iOS.
Microsoft Authenticator: Available for Android, iOS, and Windows Phone.

cPanel 2FA Setup: End-User Configuration

Once 2FA is enabled by the WHM administrator, individual cPanel users can proceed with configuring it for their accounts.

1

Access cPanel 2FA

Log in to cPanel, search for "two", and click on the **Two-Factor Authentication** icon.

2

Initiate Setup

Click **Set Up Two-Factor Authentication**.

3

Link Your App

Scan the QR code with your authenticator app, or manually enter the provided **Account** and **Key**.

4

Verify & Configure

Enter the 6-digit security code from your app into cPanel and click **Configure Two-Factor Authentication**.

cPanel Login with 2FA

After successful 2FA configuration, your cPanel login process will include an additional step, ensuring a higher level of security.

Login Steps:

1. On the cPanel login page, enter your username and password, then click **Login**.
2. On the subsequent screen, retrieve the current 6-digit security code from your authenticator app.
3. Enter this code into the provided field and click **Continue**.

> Ensure your device's time is synchronised for accurate code generation.

CWP 2FA Setup: User Process

For CentOS Web Panel (CWP) users, the 2FA setup is generally simpler, managed directly within the CWP user panel.

Access CWP Panel

Log in to your CWP user panel, usually at https://lecturersite.buet.ac.bd:2083, with your username and password.

Enable Google Authentication 2FA

In the CWP dashboard, navigate to **Settings** and locate the option for **Google Authentication 2FA**. Enable it.

Link Authenticator App

A secret code will be displayed. Open your authenticator app and manually add a new account using this secret code.

CWP 2FA: Activation & Verification

Completing the activation for CWP 2FA involves a final verification step to ensure seamless integration.

Finalise Activation

Enter the 6-digit code generated by your authenticator app into the designated field within CWP.

Save Changes

Click **Update** or **Save** to confirm your 2FA settings.

Verify Functionality

Log out of CWP and attempt to log back in. You should now be prompted for your 2FA code during each login attempt.

Troubleshooting Tip

If you encounter issues, double-check that the secret code was entered correctly and your app's time is accurate.

Troubleshooting Common 2FA Issues

Time Synchronisation: Most 2FA issues stem from incorrect device time. Ensure your mobile device's time is automatically synchronised.

Incorrect Code: Codes refresh every 30-60 seconds. Always use the most current code generated by your app.

Lost Device: Always keep a record of your recovery codes or secret key in a secure, offline location. This is crucial for regaining access if your device is lost or damaged.

QR Code/Manual Entry Errors: If scanning fails, try manual entry and double-check each character of the secret key.