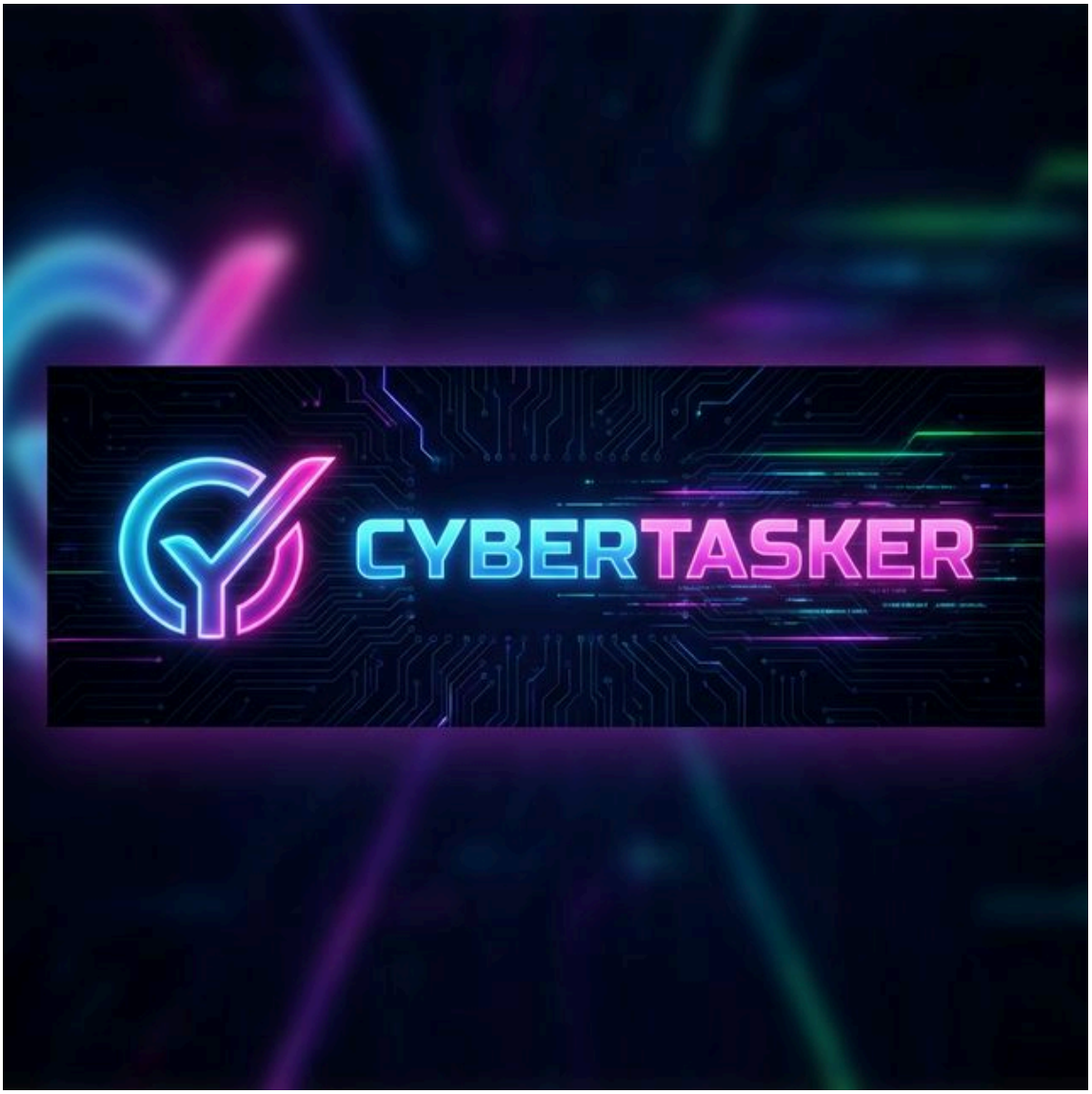
CyberTasker v2.4 - Administration Guide



> *[!WARNING] This document contains restricted system information. Unauthorized distribution is a violation of Weyland-Yutani corporate security protocols.*

Welcome to the CyberTasker Administration Console documentation. This guide outlines the advanced features and responsibilities of an Operative with `admin` clearance.

1. System Initialization (The `install.php` Protocol)

When deploying CyberTasker to a new server grid, the database is initially empty. Navigating to the root directory will automatically trigger the `install.php` sequence.

Zero-Config Auto-Lock

CyberTasker features a self-locking installation mechanism:

- **First Run:** The installer detects an empty grid, creates the necessary SQLite/MySQL tables, and injects the initial test user dataset. The Administrator must provide an **Email Address** and a robust **Access Key** (Password) during this step.
- **Subsequent Runs:** Once the `users` table exists, the installer **locks itself**. If you attempt to access `install.php` again to force a database schema update, you **must** be actively logged in as an `admin`.
- If a standard user or an unauthenticated visitor hits the installer, they receive a severe `[ ACCESS DENIED ]` warning, protecting the database from malicious resets.

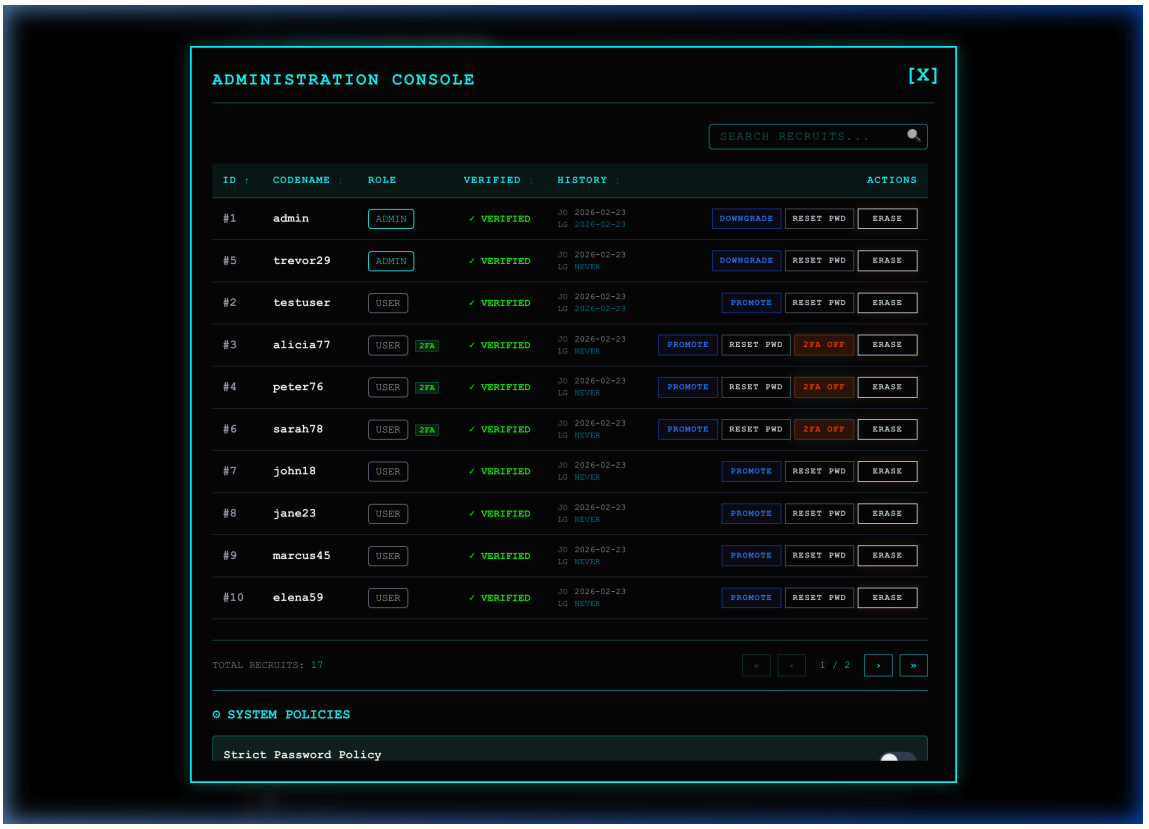
2. The Administration Console

Log in with your administrator credentials and click the **"TERMINAL"** (Admin) icon in the side navigation to access the master grid.

2.1 Operative Oversight (The Datagrid)

The main panel displays a paginated list of all registered Operatives.

- **Promote / Downgrade:** You can forcefully alter the clearance level of any user. Promote a trusted `user` to `admin`, or downgrade a rogue `admin` back to standard `user` status.
- **Reset Cypher (Password Reset):** If an Operative is locked out of their neural link, use the `RESET PWD` function. This will forcefully overwrite their password to the system default (`password`) and flag them to change it upon their next login.
- **Erase (Account Termination):** The `ERASE` button permanently deletes the user's account, all of their directives, sub-routines, and attached files from the database. **This action cannot be undone.**



2.2 Bio-Lock (2FA) Management

Security is paramount. The Admin grid allows you to monitor the 2FA status of all personnel.

- Users with active Time-Based One-Time Passwords (TOTP) will display a green `[2FA]` badge next to their role.
- **Emergency Override:** If an Operative loses their authenticator device and their backup codes, an Admin can click the red **`2FA OFF`** button to forcefully disable the Bio-Lock for that specific user, allowing them to log in with just their password.

3. Global System Policies

At the bottom of the Administration Console, you have access to global environment variables.

Strict Password Policy

By toggling the `Strict Password Policy` switch:

- **Disabled (Default):** Operatives can use simple passwords (e.g., `password123`) for rapid testing and deployment.
- **Enabled:** The system enforces cryptographic-grade security. All new passwords (during registration or profile updates) must be at least 12 characters long and contain a mix of uppercase, lowercase, numbers, and special symbols.

Enforce Email 2FA

By toggling the `Enforce Email 2FA` switch:

- **Disabled (Default):** Operatives without an active Authenticator App (TOTP) can log in with just their password.
- **Enabled:** An automatic **Emergency Override Code** (6-digit PIN) is dispatched to the operative's registered Email Address if they attempt to log in without a TOTP token. This acts as a forced, universal Two-Factor Authentication fallback across the grid.

4. Diagnostics & Maintenance

- **Mail Logs & Development:** CyberTasker relies on PHP's `mail()` function for dispatching notifications (e.g., password reset tokens, 2FA fallback codes). For local testing or environments without a live SMTP server configured, developers can manually uncomment the logging function within `api/helpers/mail_helper.php`. When activated, this will write all email traffic to a local `mail_log.txt` file, which can then be inspected directly via the Admin Terminal to ensure the system is dispatching signals correctly.

> ***End of Guide*** *Maintain constant vigilance over the grid, Admin.*