---

\*\*Deeprey MFD: Linux User Configuration Specification\*\*

\*\*1. Introduction and Purpose\*\*

This document outlines the standard Linux user account configuration for the Deeprey Marine MFD (Multi-Function Display). The primary goal is to create a secure, stable, and maintainable system that provides an intuitive appliance-like experience for the end-user (boat captain/crew) while allowing authorized Deeprey personnel to perform necessary maintenance, updates, and support.

The MFD is designed to boot directly into the OpenCPN navigation software in a full-screen kiosk mode, with restricted access to the underlying operating system for the end-user.

\*\*2. Core Requirements Addressed by this User Configuration\*\*

This user configuration is designed to meet the following critical operational and security requirements:

\* \*\*For the End-User (Captain/Crew):\*\*

\* The MFD must automatically start OpenCPN in full-screen mode upon power-on, without requiring any manual login or interaction with the operating system.

\* The user must be able to interact fully with OpenCPN for all navigation tasks, including access to connected hardware (GPS, AIS, NMEA data, sounders, etc.).

\* All navigation data (tracks, routes, waypoints, OpenCPN settings) must be saved and persist across reboots.

\* The user must be able to safely power off the MFD.

\* The user must be prevented from exiting OpenCPN to access the general desktop, command line, or system settings, ensuring an appliance-like feel.

\* The user must not be able to accidentally or intentionally install software, delete system files, or misconfigure the MFD in a way that compromises its primary navigation function.

\* The system must be robust and stable.

\* \*\*For Deeprey (Vendor - Manufacturing, Maintenance, Support):\*\*

\* Deeprey technicians must be able to perform initial device-specific configurations during manufacturing.

\* Deeprey technicians or authorized service personnel must be able to securely update the operating system, OpenCPN application, drivers, and firmware.

\* Technicians must have a secure and controlled method to access system logs, run diagnostic tools, and inspect system state for troubleshooting.

\* Technicians must be able to make advanced configuration changes not exposed to the end-user.

\* If network connectivity is available, secure remote access for advanced support should be possible.

\* All maintenance access must be protected by strong, non-default credentials.

\* The system image must be protected against unauthorized modification.

\* The principle of least privilege must be applied to all processes and users to enhance security.

\*\*3. Defined Linux User Accounts\*\*

To meet the above requirements, the following user accounts will be configured on the Deeprey MFD:

**\*\*3.1. Kiosk/Application User (for OpenCPN)\*\***

\* \*\*Purpose:\*\* This account is solely dedicated to running the OpenCPN application in kiosk mode. It provides the end-user interface and handles all interactions with the navigation software and connected marine hardware. It is designed with minimal privileges.

\* \*\*Username:\*\* `opencpn`

\* \*\*Password:\*\*

\* A very long, complex, randomly generated password will be set for this user during the image creation process (e.g., using a tool like `openssl rand -base64 30`).

\* This password is not intended for human interaction. Its existence is a system requirement, but the user will auto-login.

\* This password will be securely documented internally by Deeprey for build reference.

\* \*\*System Privileges:\*\*

\* \*\*This user will NOT have `sudo` (superuser) privileges.\*\* This is a critical security measure to prevent the end-user or a compromised OpenCPN application from making unauthorized system-level changes, installing software, or accessing sensitive system files.

\* \*\*Login and Session Behavior:\*\*

\* The system will be configured to automatically log in as the `opencpn` user on boot.

**\*\*3.2. Administrator/Maintenance User (for Deeprey Technicians)\*\***

\* \*\*Purpose:\*\* This account is reserved for Deeprey technicians or authorized service personnel to perform system administration, software updates, troubleshooting, diagnostics, and advanced configuration tasks.

\* \*\*Username:\*\* `deepreyadmin`

\* \*(Alternative options: `mfdsupport`, `deepreytech`)\*

\* \*\*Password:\*\*

\* A \*\*strong, unique password\*\* will be set for this account. This password must be kept confidential and only shared with authorized Deeprey personnel.

\* For mass-produced units, this might be a standard strong password initially, with recommendations or procedures for changing it during specific service interventions if required for enhanced security or tracking.

\* \*\*Home Directory:\*\* `/home/deepreyadmin`

\* \*\*Shell:\*\* `/bin/bash` (or `/bin/sh`)

\* \*\*Group Memberships:\*\*

\* Primary group: `deepreyadmin`

\* Auxiliary groups:

\* `sudo` (or `wheel` on some distributions): This grants the user the ability to execute commands with root privileges, necessary for system administration tasks.

\* \*\*System Privileges:\*\*

\* This user has the ability to use `sudo` to perform any system-level operation.

\* \*\*Login and Session Behavior:\*\*

\* This user will \*\*NOT\*\* auto-login.

\* Access is intended via:

\* \*\*Physical Console (TTY):\*\* By connecting a keyboard and switching to a virtual terminal (e.g., Ctrl+Alt+F2), a technician can log in with the `deepreyadmin` credentials.

\* \*\*SSH (Secure Shell):\*\* If the MFD has network capability and SSH service is enabled, technicians can log in remotely using these credentials. SSH access must be secured (e.g., using key-based authentication if feasible, strong password policy, disabling root SSH login).

**\*\*3.3. Root User\*\***

\* \*\*Purpose:\*\* The `root` user is the superuser in Linux, having unrestricted access to the entire system. Its direct use should be minimized.

\* \*\*Username:\*\* `root`

\* \*\*Password:\*\*

\* During the initial operating system installation and image creation, an extremely strong, complex, randomly generated password will be set for the `root` account.

\* \*\*Crucially, after the `deepreyadmin` user is created and granted `sudo` privileges, the `root` account's password will be locked using the command `sudo passwd -l root`.\*\*

\* \*\*Login and Session Behavior:\*\*

\* Direct login as `root` (either via console or SSH) will be disabled by locking the password.

\* All administrative tasks requiring root privileges will be performed by logging in as `deepreyadmin` and then using the `sudo` command. This provides an audit trail of commands executed with elevated privileges.

\*\*4. Rationale for this User Configuration\*\*

This multi-user configuration is chosen for the following reasons:

\* \*\*Enhanced Security (Principle of Least Privilege):\*\*

\* The `opencpn` user, which runs the primary application exposed to the end-user, has only the minimum permissions necessary. If OpenCPN itself were to have a vulnerability, the potential for system-wide compromise is significantly reduced.

\* Separating administrative tasks into a dedicated `deepreyadmin` account, which requires explicit authentication, protects the system from accidental or unauthorized changes by the end-user.

\* Locking the `root` account password and forcing administrative actions through `sudo` reduces the attack surface and improves accountability.

\* \*\*Improved Stability and Reliability:\*\*

\* Restricting the end-user's capabilities prevents accidental misconfiguration or deletion of critical system files, leading to a more stable MFD.

\* \*\*Clear Separation of Roles:\*\*

\* The distinct user accounts map directly to the different modes of operation: normal end-user navigation and vendor maintenance/support.

\* \*\*Maintainability and Supportability:\*\*

\* Technicians have a clearly defined and secure method (`deepreyadmin` with `sudo`) to perform necessary system work without interfering with the end-user's data or setup.

\* Troubleshooting permission-related issues is simpler with distinct user contexts.

\* \*\*Professional Standard:\*\*

\* This approach aligns with industry best practices for securing embedded and appliance-like Linux systems.

\*\*5. Implementation Considerations and Best Practices\*\*

\* \*\*Image Creation:\*\* These user accounts and their configurations will be established during the creation of the master Linux image for the MFD.

\* \*\*Minimizing Attack Surface:\*\*

\* Install only essential software packages on the MFD.

\* Disable or remove any unnecessary services.

\* Restrict login access on unused virtual terminals (TTYs).

\* \*\*Filesystem Permissions:\*\* Ensure appropriate ownership and permissions for OpenCPN configuration files and data directories within `/home/opencpn`.

\* \*\*Secure SSH Configuration (if used):\*\*

\* Disable root login via SSH (`PermitRootLogin no` in `sshd\_config`).

\* Consider using public key authentication instead of passwords for `deepreyadmin` for higher security if your support model allows.

\* Use a non-standard SSH port if deemed necessary (though security by obscurity is not a primary defense).

\* \*\*Read-Only Root Filesystem (Optional Advanced Hardening):\*\* For increased resilience against corruption and unauthorized changes, consider mounting the root filesystem as read-only, with specific writable partitions for user data (`/home`), logs (`/var/log`), and temporary files. This adds complexity but significantly improves system integrity.

\* \*\*Firewall:\*\* Implement a basic firewall (e.g., `ufw` or `iptables`) to block all incoming connections except those explicitly needed (e.g., SSH for `deepreyadmin` if remote access is a feature).

This user configuration strategy provides a solid foundation for a secure, reliable, and user-friendly Deeprey MFD, meeting the needs of both the end-user and Deeprey's support and maintenance operations.

---