SERVICE MANUAL

NSR ECDIS NES-3000R

NEW SUNRISE CO., LTD

Table of contents

First Start Check List

To ensure the correct operation of the ECDIS, it is crucial to check and configure the following settings:

- USB-dongle and License
- DPI Settings and Graphical Interface Settings
- Registration and Vessel Data Settings
- Own Ship and Vessel Dimension Settings
- System Information Settings
- Network Settings
- Sensors Settings
- Firewall Settings

Make sure that you have properly set up the ECDIS software as described in this document.

Default passwords and password policy

Service Privileges mode

ECDIS has a **Service Privileges Mode**. This mode gives access to advanced settings. You need it to:

- Set up navigation sensors.
- Configure network settings.
- Install or update system dimensions.
- Perform other important system tasks.

Important Notes:

1. **Time Limit:**
   - Service Privileges Mode works for **10 minutes**. After this, it turns off automatically.
2. **Password Change:**
   - After setup and testing, change the default password. Follow the password policy as described below.
3. **Default Password:**
   - The default password is: **Locnav=8**.

Remember:

- Use this mode only when needed.
- Exit the mode after completing your tasks

Default Linux User

- **Username:** marinara
- **Default Password:** marinara

The *marinara* user is required to configure system parameters via the command line or SSH. This user has **sudo privileges**, allowing administrative actions on the system.

Password Policy

During installation and setup, you **must change the default password** using the ***passwd*** command. Follow these rules when creating a new password:

1. **Do not use:**
   - The username (marinara) or parts of the user's full name.
   - Company names, product names, or other easily guessable terms.
2. **Avoid:**
   - Dictionary words.
   - Repetitive or sequential characters (e.g., aaaaaa, 1234abcd).
3. **Use:**
   - Random and meaningless passwords.
   - A combination of uppercase letters, lowercase letters, numbers, and special characters.

Example of a Strong Password: 7xL9@qZ2!pR

First Start. ECDIS Settings

USB-dongle and License (Install, Update)

The License file contains essential information about the ECS/ECDIS product and any additional available options.
The ECS/ECDIS software developer issues a license specifically for a selected USB-dongle. This means that each "license-dongle" pair is unique. Ensure that you obtain both the License file and USB-dongle directly from the ECS/ECDIS manufacturer or the ECS/ECDIS software developer.

To install or update a License:

1. Save the License file to a prepared USB flash drive.
2. Insert the prepared USB flash drive with the License file into a free USB port on your computer.
3. Insert the USB-dongle into another free USB port on your computer.
4. Boot your device.

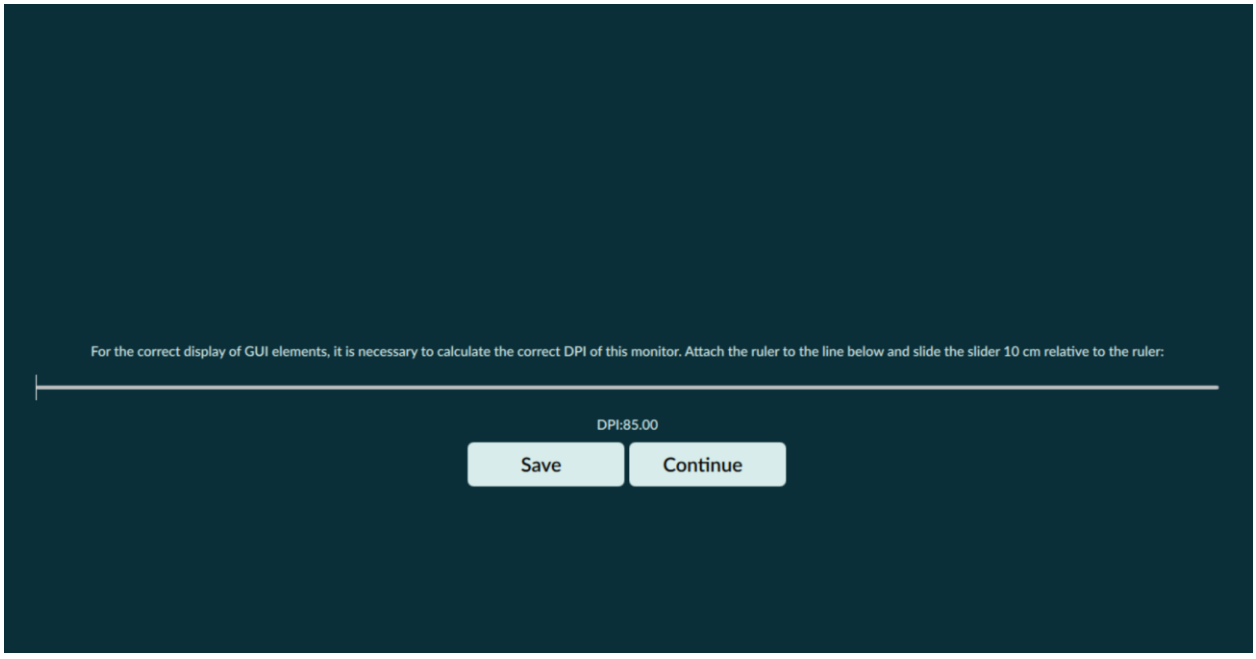
The system will automatically detect the License file and install or update it for your ECS/ECDIS. For subsequent startups, there is no need to insert the USB drive with the License. The system stores the License file in memory.

Requirements:

- USB flash drive.
- **FAT32** file system.
- The USB flash drive should be empty, with only the License file saved in the root folder.

DPI settings

Upon the first startup, the system will prompt you to configure the DPI settings for your monitor.
NOTE: This is a crucial step because the correct DPI settings ensure the correct size of chart objects on the Electronic Navigational Chart (ENC).



You can configure the DPI settings in two ways:

1. **Automatic Method:**
    - Attach a ruler to the line displayed on the screen.
    - Slide the on-screen 10cm line to match the ruler's 10cm mark.
    - The system will automatically adjust and set the correct DPI settings.
2. **Manual Method:**
    - Calculate the DPI manually by considering the screen resolution and display size (e.g., diagonal measurement).
    - Alternatively, use an online DPI calculator, such as the one available here: DPI Calculator.

After setting up the DPI, press the **Save** button, and then click **Continue** to proceed.

Note: You can also adjust the DPI settings later in the ECS/ECDIS menu settings.

Troubleshooting

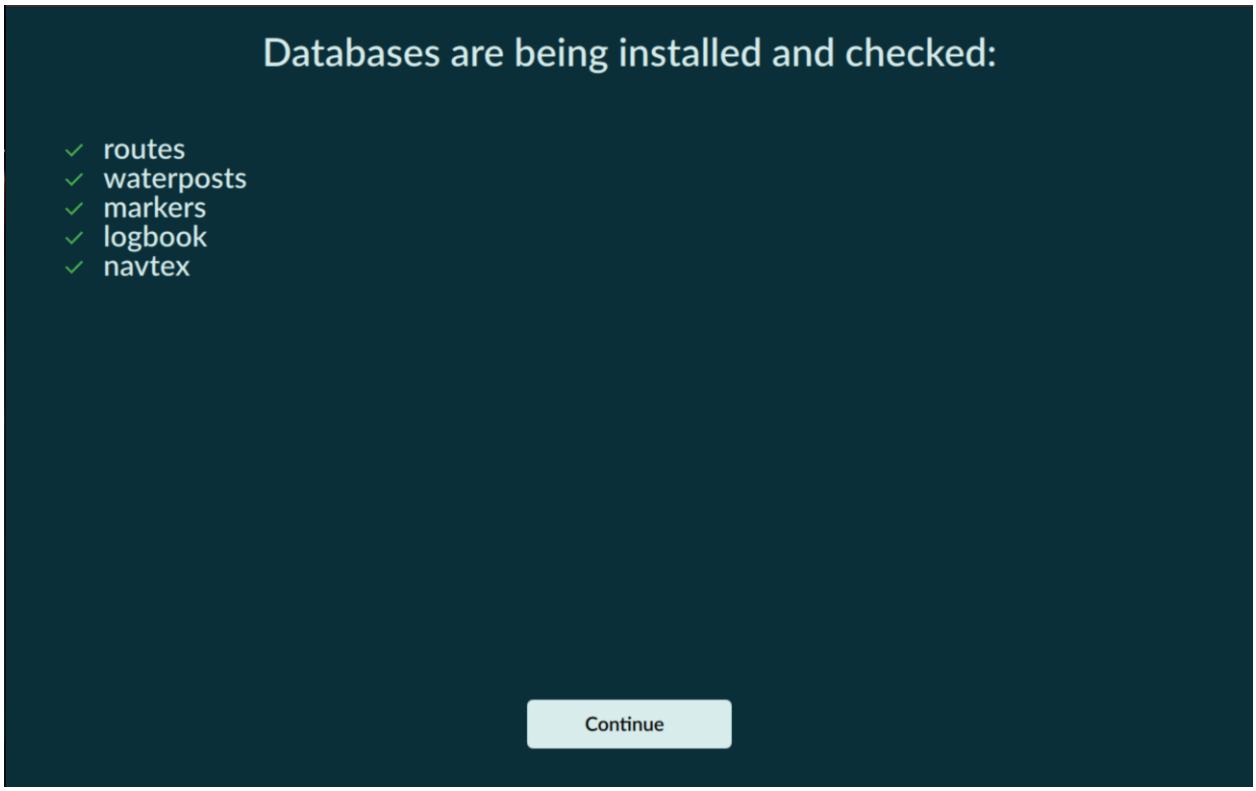
In some cases, incorrect DPI settings may render the ECS/ECDIS Graphical Interface unusable. To reset the DPI settings:

1. Press **Ctrl + Alt + G** on the main screen of the ECS/ECDIS application.
2. Reboot the system.

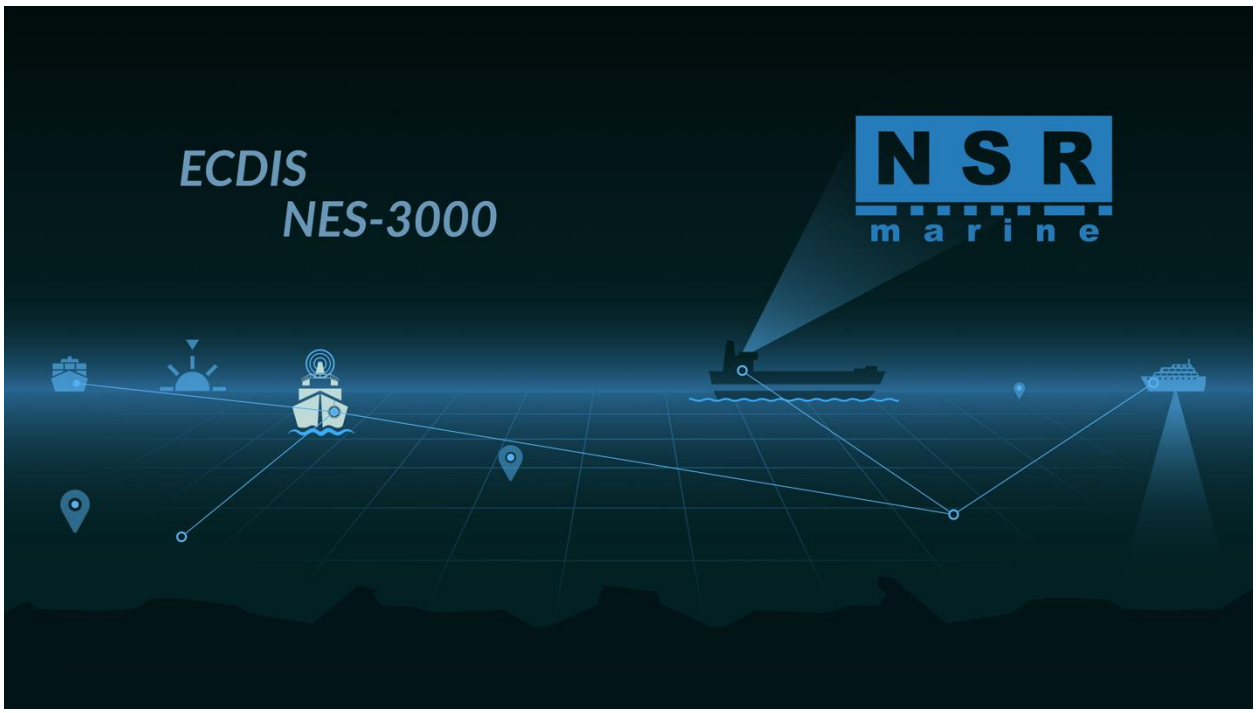
Upon startup, the system will prompt you to configure the DPI settings for your monitor as described above

Setup initial settings

While first boot system install and check databases, click **Continue** to proceed



Next, you will see the boot splash screen as the system checks the USB dongle and validates the license.



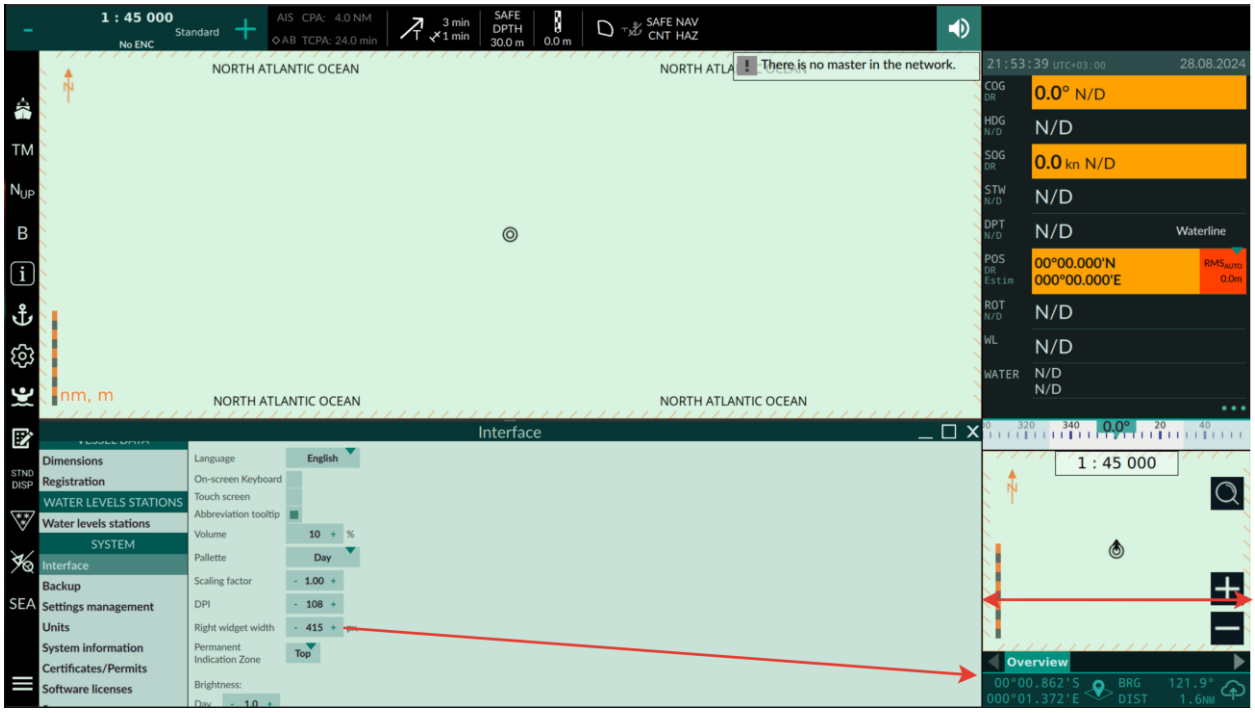
If the USB key and license are correct, the ECS/ECDIS application will start up successfully.

Graphical interface settings recommendations

After the first startup, it's important to configure the graphical interface based on your screen resolution, screen dimensions, personal preferences, and regulatory documentation requirements (e.g., IEC Standards).
Navigate to **Menu -> Settings -> System -> Interface** to access the settings.

1. Right Widget Width

With this setting you could tune Right Widget Width. We recommend set value that all meaningful information in right widget is visible (e.g. cursor coordinates).



2. Scaling factor

In some cases, you may need to adjust the interface scale. Experiment with this setting to find the optimal values.

NOTE: For ECDIS, the clear readout distance for meaningful information (minimum viewing distance) must be at least 1 meter from the screen.

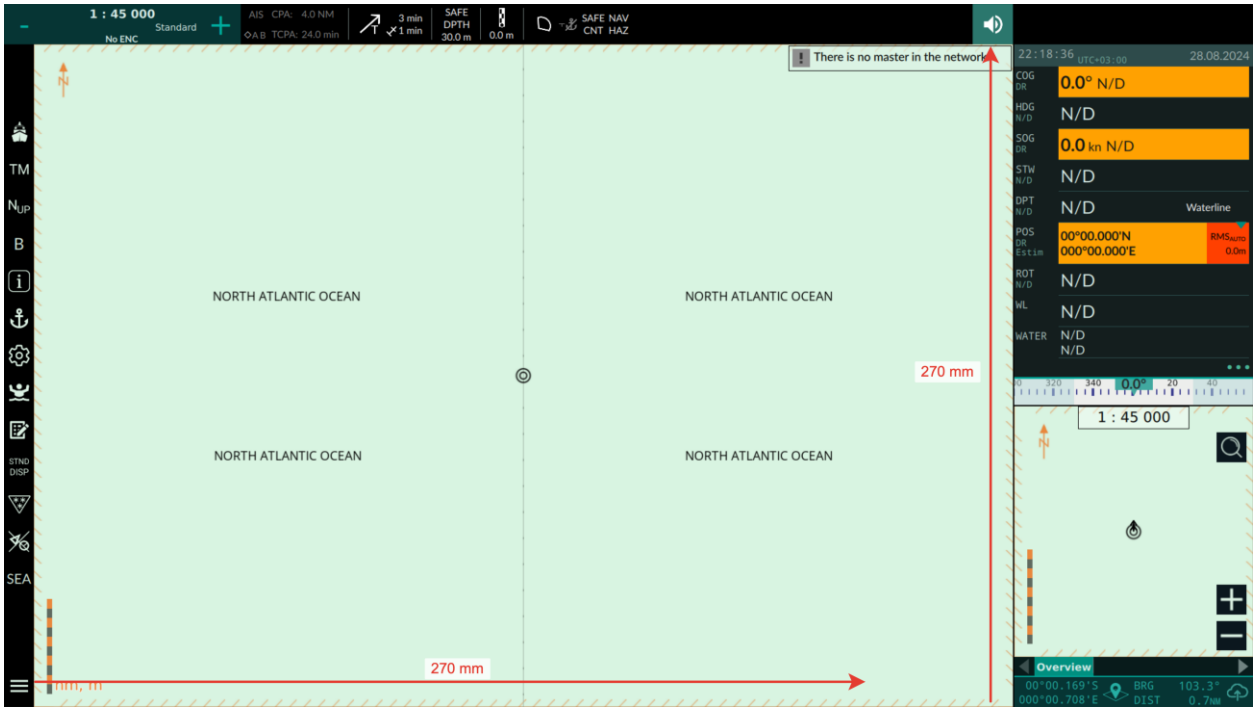
3. Permanet Indication Zone

This setting determines the position of the Permanent Indication Zone: either at the top or on the left.

General guidelines:

- For 3:4 and 5:4 aspect ratio monitors, the zone should be positioned at the top.
- For widescreen monitors (16:9, 16:10) with a diagonal of less than 22.6", it should be positioned on the left side.
- For widescreen monitors (16:9, 16:10) with a diagonal of more than 22.6", the zone can be positioned either on the left side or at the top.

NOTE: For ECDIS, the minimum chart display area must be at least 270 mm x 270 mm.



Combine the three settings described above to optimize the graphical interface's performance, keeping in mind the regulatory documentation requirements regarding readout distance and the minimum size of the chart display area.

NOTE: Avoid using the DPI setting to adjust the graphical interface, as altering the DPI will also change the size of chart objects on the Electronic Navigational Chart (ENC). The dimensions of chart objects are also standardized.

Network settings

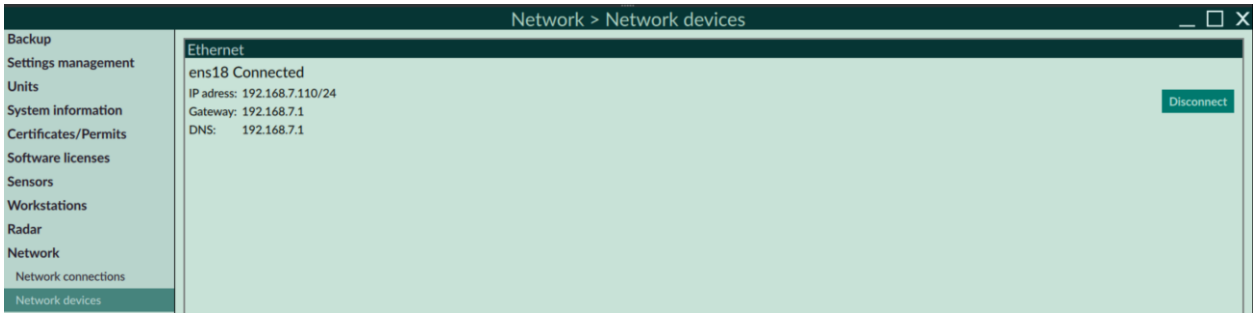
If you have a bridge network setup (e.g., Master-Backup configuration) and/or if your NMEA sensors and other devices (e.g., VDR) are connected via Ethernet, ensure that your network connection settings are properly configured.

1. Navigate to **Menu -> Network -> Network connection/devices** to access the network settings.
2. Before setting up Network, ensure you have service privileges. Default password: **Locnav=8**.

NOTE: Maximum outgoing ECDIS data volume is 6.25 Mbytes/sec. The maximum Ethernet port bandwidth depends on the network device parameters, but it must be not less than 100 Mbps

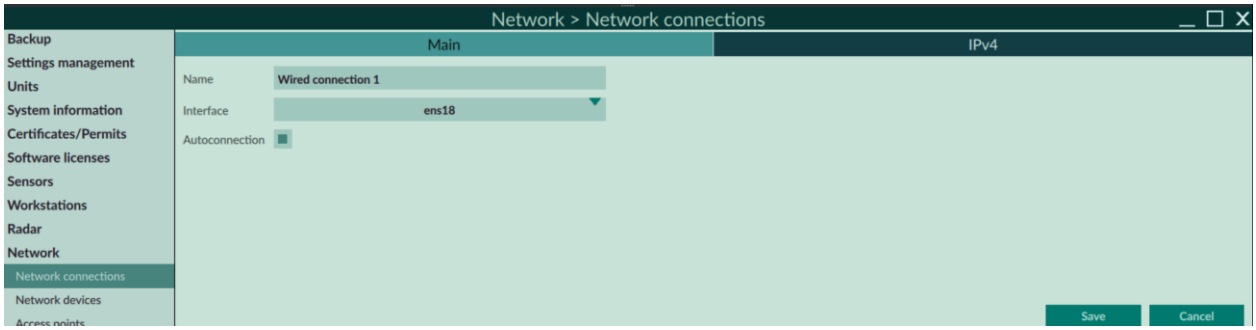
DHCP

If your network configuration includes a DHCP server (e.g., a router or 450/460 Gateway), the ECDIS will automatically connect to the network. You can verify the network interface name, IP address, Gateway, and DNS settings in the **Network devices** menu. This menu displays all accessible network interfaces on your computer



Manual Network Settings

If your network configuration requires manual settings, you can manually configure the IP address, Gateway, and DNS through the **Network connections** menu.



These settings follow the standard procedure for network configuration.

NOTE: Make sure that the firewall is properly set up. Otherwise, there may be issues with network communication.

Additional Info

- ECDIS does not provide the functions of a repeater or/and hub.
- ECDIS based on Ubuntu 20.04. Ubuntu 20.04 supports IGMPv3 (and is backward compatible with v2)
- ECDIS supports:
    - "UdPbC" for transmission of IEC 61162-1 formatted sentences
    - "RaUdP" (v1, v2) for transmission of binary files
    - "RrUdP"(v1, v2) for transmission of re-transmittable binary

- Processed Datagrams (Intended Traffic): 15,000 datagrams per second
- Non-Processed Datagrams (Background Traffic): 7,500 datagrams per second
- Mixed Load Condition: 7,500 processed + 7,500 non-processed dg/s
- Maximum transmission rate – 50 mbps
- The maximum operational output bandwidth not more than 50 mbps

Own Ship Settings

Dimensions

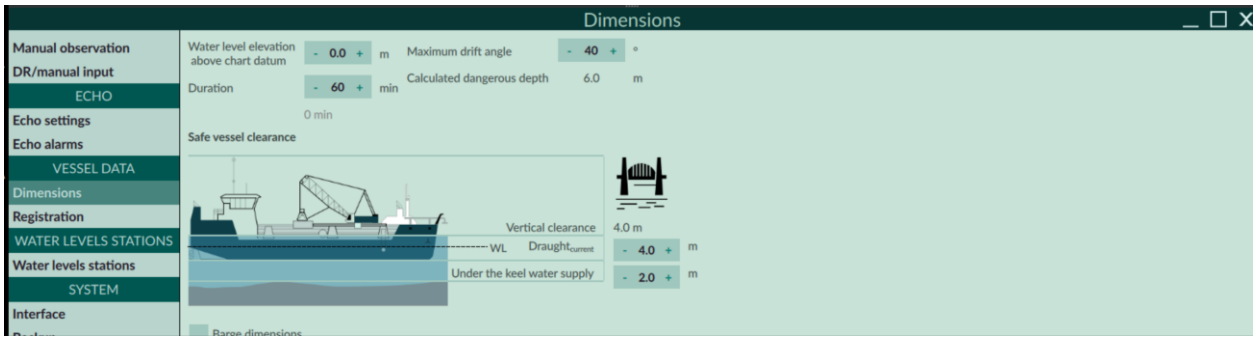
Navigate to **Menu -> Settings -> Vessel Data -> Dimensions** to access the settings.
NOTE: This is a crucial step because entering the correct vessel dimensions is essential for safe navigation. The vessel dimensions are used by the ECDIS to safety ground check monitoring and route check and monitoring.

1. **Set Structural Vessel Dimensions**.

Begin by inputting the structural dimensions of the vessel. Default password: Locnav=8.

2. **Set Current Draft and Safety Clearance Parameters**

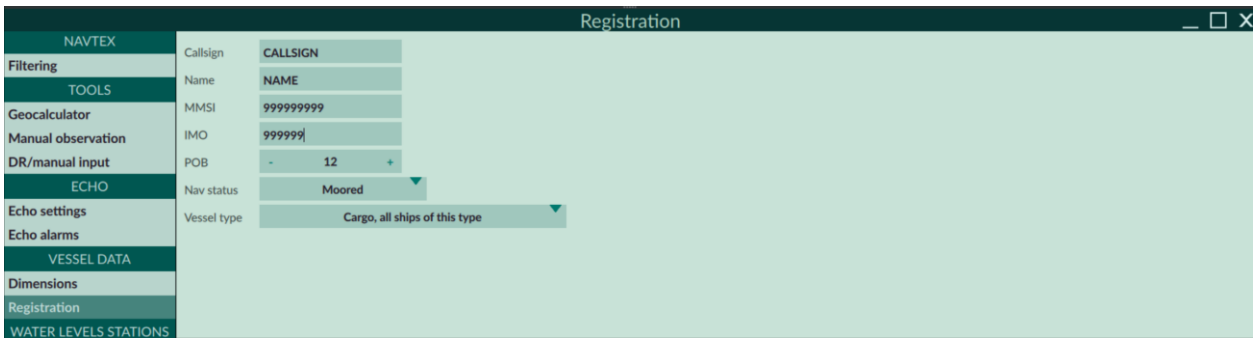
After setting the structural dimensions, input the current draft and any other relevant safety clearance parameters.



NOTE: For more detailed information about vessel dimensions, refer to the "Dimensions" section in the ECDIS Software User Manual.

Registration

Navigate to **Menu -> Settings -> Vessel Data -> Registration** to access the settings.



This section is intended for setting the vessel information for the connected AIS transponder. The AIS must be capable of receiving VCD and SSD NMEA sentences.

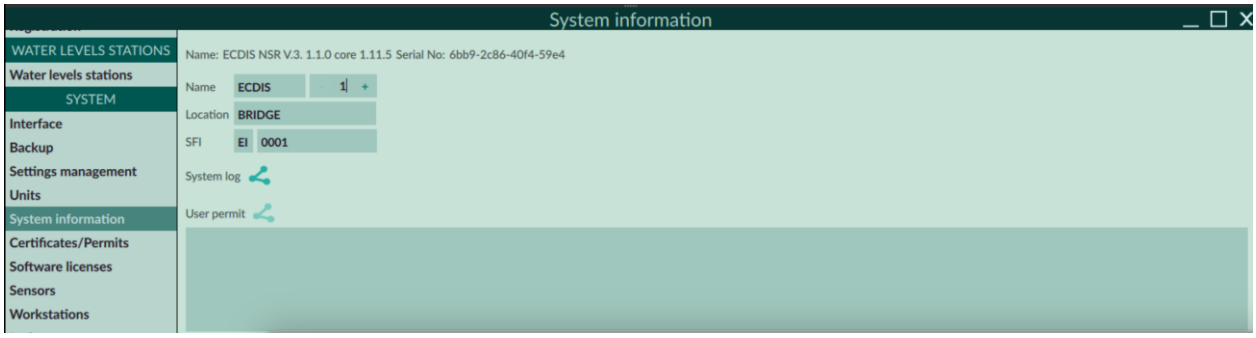
NOTE: For more detailed information about vessel dimensions, refer to the "Registration" section in the ECDIS Software User Manual.

System Information

For bridge systems with multiple workstations (e.g., Master-Backup configuration), it is crucial to set up the following parameters:

1. **ECDIS Name**
2. **Workstation Location**
3. **SFI (System Function Identifier)**

This information is essential for proper integration with the Voyage Data Recorder (VDR) and for establishing connections using the IEC 61162-450 NMEA protocol, which is used for connecting sensors and transferring routes.



Navigational sensors setup

Navigate to **Menu -> Settings -> Sensors** to access the settings

NOTE: The minimum sensor setup for ECDIS includes a position sensor (e.g., GNSS: GLONASS/Beidou/GPS), a heading sensor, and a speed log.

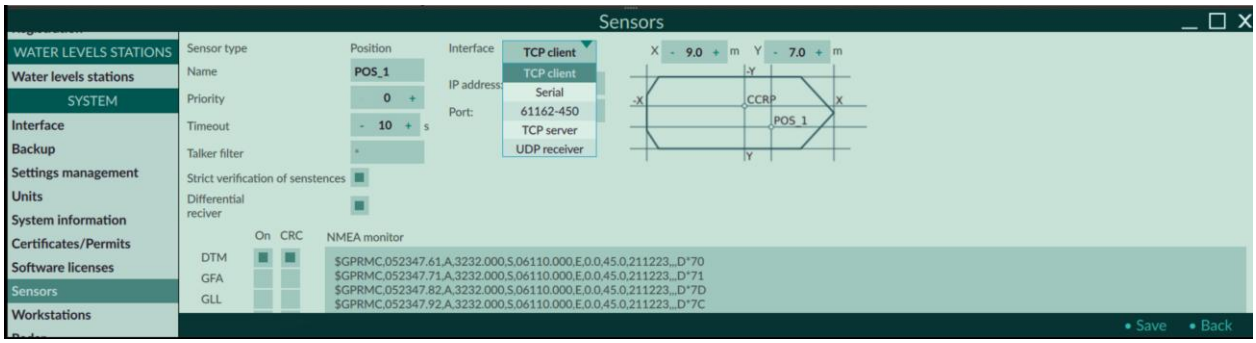
There are two methods to connect navigational sensors to the ECS/ECDIS software:

1. **Via Ethernet:**
    - You can use a direct connection or a COM-Ethernet adapter, such as the Moxa NPort series or a similar device.
2. **Via RS-232/422/485:**
    - In this case, your computer must have onboard serial RS-ports.

To add a sensor in either scenario:

1. Before setting up sensors, ensure you have service privileges (Default password: **Locnav=8**).
2. Add the necessary sensor.

3. Turn the sensor on. 
4. Click the **Settings** icon button to access the sensor settings menu.



NOTE: It is crucial to set the sensor's position relative to the vessel's CCRP (Common Reference Point), as ECDIS uses this correction data to ensure consistent and accurate measurements.
X and **Y** - offsets of the sensor's (antenna) position in the ship's coordinate system **relative to CCRP**. For sensors such as GNSS, heading, speed, AIS, Radar, and Pelorus, the input of offsets is mandatory as the ECDIS references navigation parameters to the **CCRP**.

Ethernet connection

To set up an Ethernet connection, you should select the appropriate option from the **Interface** dropdown menu, depending on the type of interface your sensor uses:

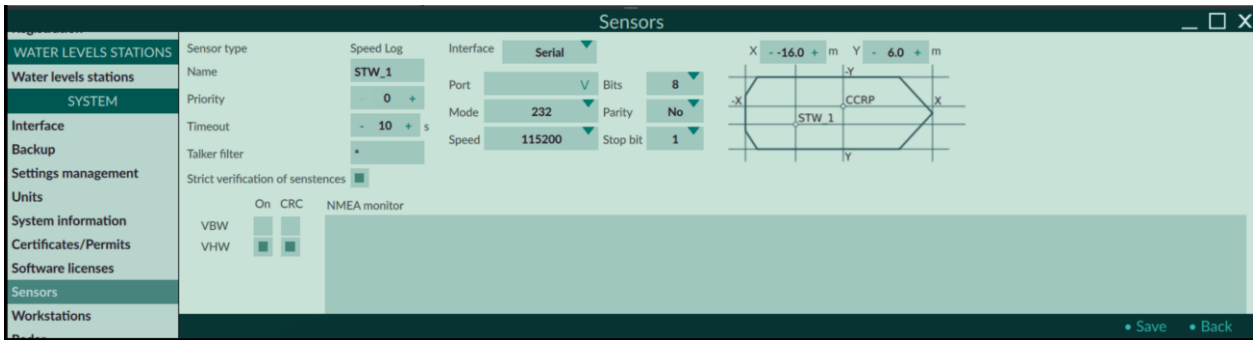
- **TCP Client** (ECDIS as TCP Client)
- **TCP Server** (ECDIS as TCP Server)
- **UDP Receiver** (ECDIS as UDP Receiver)
- **61162-450** (ECDIS as 450-Node)
-

NOTE: When using the NMEA 61162-450 protocol, make sure to set the System Function Identifier (SFI) as described in the **System Information** section (Navigate to Menu -> System -> System Information to access the settings).

NOTE: Make sure that the firewall is properly set up. Otherwise, there may be issues with network communication.

Serial Port Connection

To set up a serial port connection, select the "Serial" option from the **Interface** dropdown menu and configure the necessary serial port settings (system port, port mode, speed, parity, etc.) to match the settings of the sensor you are trying to connect to the ECDIS.



Note: In some cases, you may need to configure the serial port settings in the BIOS of your motherboard before adjusting them within the ECDIS graphical interface.

NMEA Monitor

This function is particularly useful during commissioning work.
If your connection settings are correct and the ECDIS sensor is switched on, you will see NMEA sentences received from the connected sensor. You can view the raw data flow or sort the sentences by Talker ID and sentence type using the **"As is/Sorted/Raw"** button

Additional settings

- **Name** - name identifying the sensor. This name will appear in Navagtional Widget on ECDIS main screen.
- **Priority** - Priority determines the switching sequence between the sensors of the same type in case of sensor failure. Operator can change the priority automatically assigned by ECDIS at his discretion. A value of 0 is the highest priority.
- **Timeout** - delay of data input to the port - the period after which the warning about sensor failure due to lack of input data will be generated. Default value is 10 seconds. Setting a shorter period is not recommended, as it can lead to false alarms due to poor quality of the communication channel or individual peculiarities in the sensor operation.
- **Talker filter** - filtering of messages by header. The headers that the system accepts are specified in commas. Messages with other headers will be ignored and data from such messages will not be processed by the ECDIS.
- **Strict verification of sentences** - depending on the sensor manufacturer, different implementations of sentence generation may be encountered. When the checkbox is ON, the ECDIS verifies sentences in strict accordance with the IEC 61162-1 standard. When the checkbox is OFF, the ECDIS ignores some non-critical deviations from the IEC 61162-1 standard, making it possible to process such messages. For example, it ignores missing letters in fixed sentence fields, the presence of which does not affect the quality of the parsed information.
- **NMEA Message Type Selection** - Check the boxes corresponding to the types of NMEA messages to be received.
- **CRC Column Switches** - Enables the verification of message checksums. Messages with incorrect checksums will not be received if this checkbox is enabled. Disable checksum verification if necessary to receive such messages.

Navigational Sensors List

For all sensors types

- Ensure that the processing of received messages is correctly configured in the sensor settings, including enabling the appropriate headers and message types.

- Be aware that some standard navigation data sentences may not include the checksum (CRC) value for the transmitted data packet. Additionally, sensor may sometimes fail to calculate the checksum correctly. To manage this:
    - If the checksum verification is **disabled**, ECDIS will treat all sentences as valid, regardless of the checksum.
    - If the checksum verification is **enabled**, ECDIS will only process sentences that have been successfully verified.
- Set the CRC check according to the specific behavior of the sensor in use, ensuring

Position sensor

- Verify that the **Differential Receiver (GNSS)** checkbox is correctly configured:
    - **Differential Receiver (GNSS)** - This feature controls the reception of differential corrections. When enabled, the ECDIS monitors the GNSS receiver for an indication of differential mode. If the receiver does not receive differential corrections for any reason, the ECDIS will issue a warning.

Heading sensor

- The heading sensor has no specific settings.

Speed sensor (STW)

- When connecting several lags broadcasting VBW and/or VHW messages, it is recommended to create each lag as a separate navigation sensor and enable processing of only **one** VBW or VHW message

AIS Sensor

- If the AIS sensor is set to receive VDM and VDO messages, but VDM is not broadcast, the AIS will be considered faulty. This is due to the fact that if there are no reports from other vessels, the message is not transmitted. At the same time, the own vessel report transmitted to VDO is obligatory.

ARPA Sensor

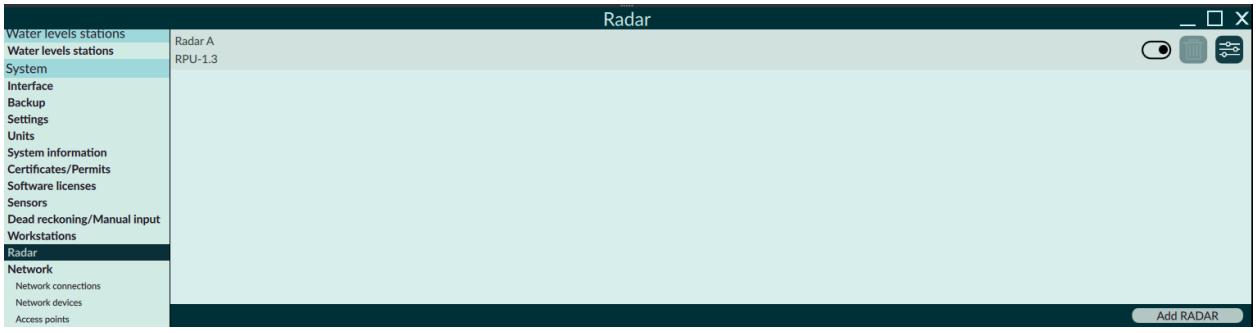
- ECDIS only processes messages with the **RA** header**.**

Radar Overlay (Radar Sensor)

- ECDIS implements the **Radar overlay** function from radar processors, and/or network radars on the chart.
- The Rad**ar overlay** option requires a Radar Overlay licence to work.

Navigate to **Menu -> Settings -> Radar -> Add Radar**

- The added source will appear in the list of connected sources

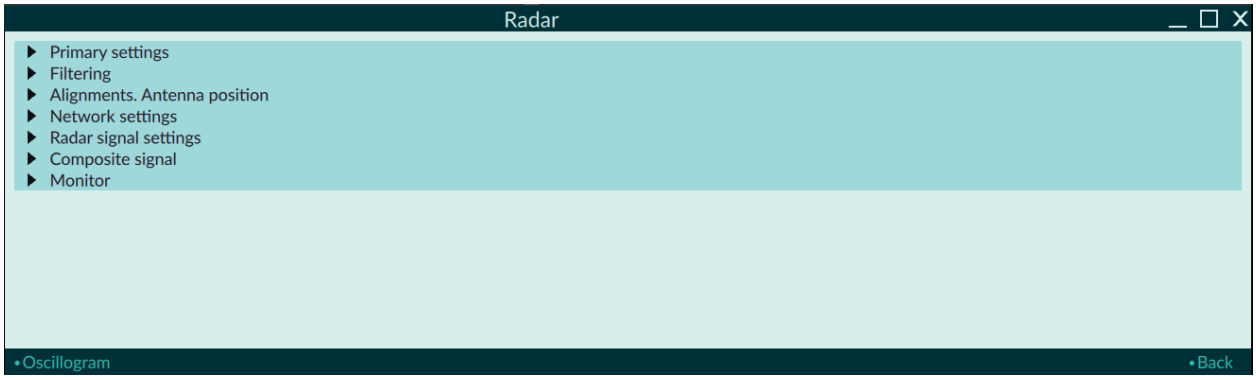


Radar overlay source setup

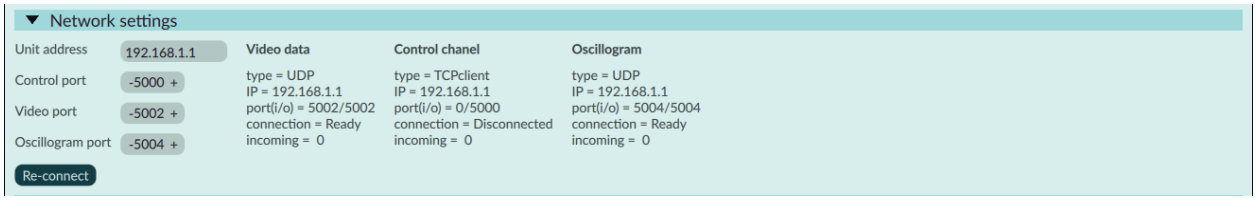
NOTE: The steps described below for setting up the **Radar overlay** source are general. As an example, the radar processor model RPU-1.3 is used. For correct operation of the **Radar overlay** source, the setup should be performed by a professional with the appropriate technical knowledge and skills

Navigate to **Menu -> Settings -> Radar -> Radar Settings** 

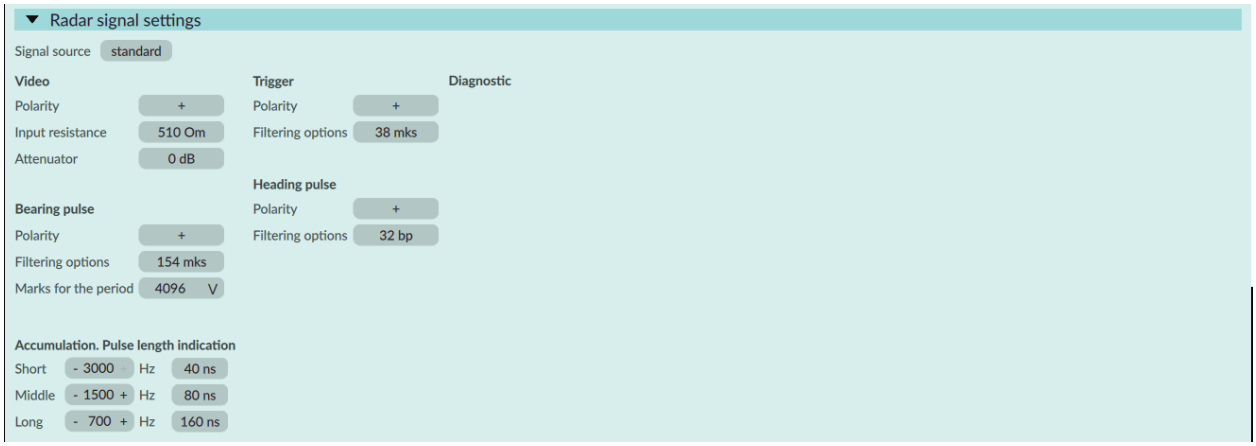
- Settings are grouped into sections. To expand/collapse the selected section - click (tap) on the corresponding heading.



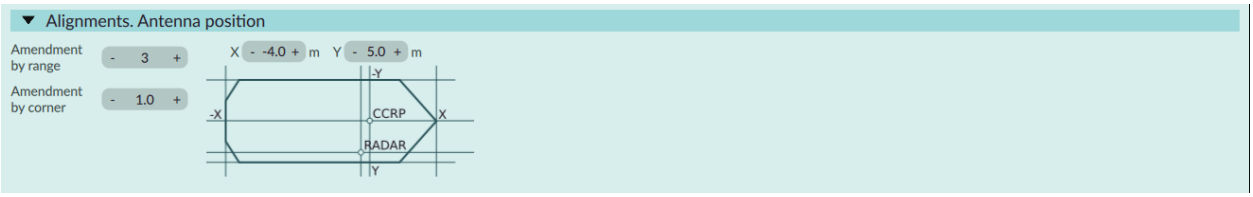
- **Network settings:** set the IP address of the **Radar overlay** source device, set the data/control ports according to the documentation. Press **Reconnect** and if the settings are correct, the connection statuses will be changed and the data packet counters will be updated in the information group (4).



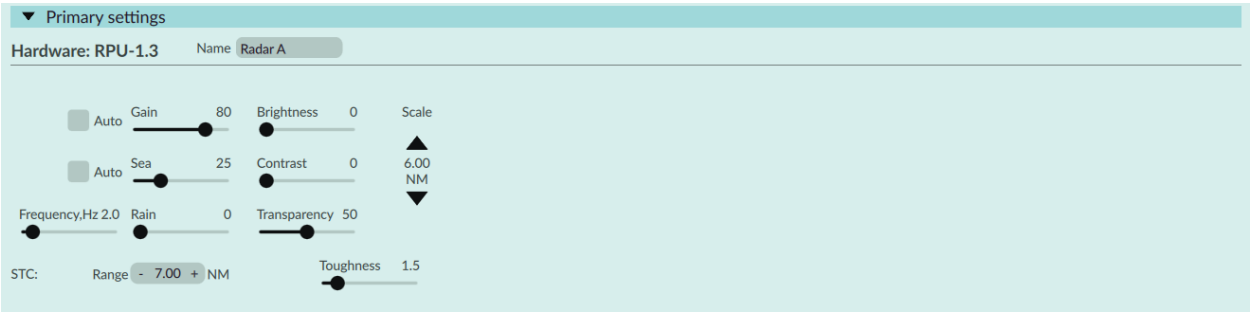
- **Radar signals settings:** set the mode in the **Signal source** drop-down list. By default, this parameter is set to standard (RPU-1.3). If all parameters are set correctly and the **Radar overlay** layer is enabled in **Quick settings**, **Radar overlay** will appear on the screen, and the **Diagnostic** group with information about the selected device status will appear in the settings window.



- **Alignments. Antenna position:** set the radar antenna coordinates relative to the CCRP. In case of discrepancy between radar and chart information - enter distance and angle corrections. It is recommended to perform these settings regularly.

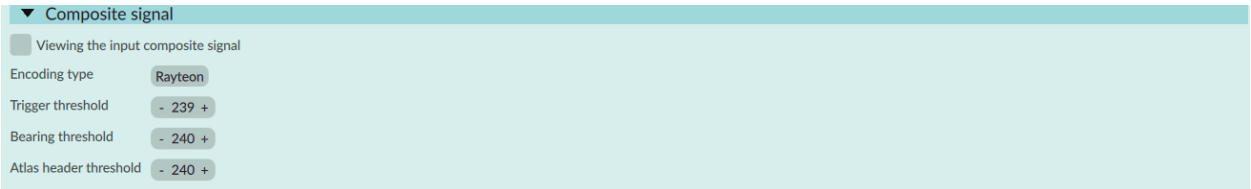


- **Primary settings:** enter the source **name** (1), set the required **range scale**. Use the **Gain, Sea, Rain** settings and parameters to adjust the signal detection thresholds. If necessary, use the **Auto** switches to switch on the functions of automatic suppression of interference. Depending on the display model, adjust the **display** parameters so that the **Radar overlay** is clearly visible on the screen.

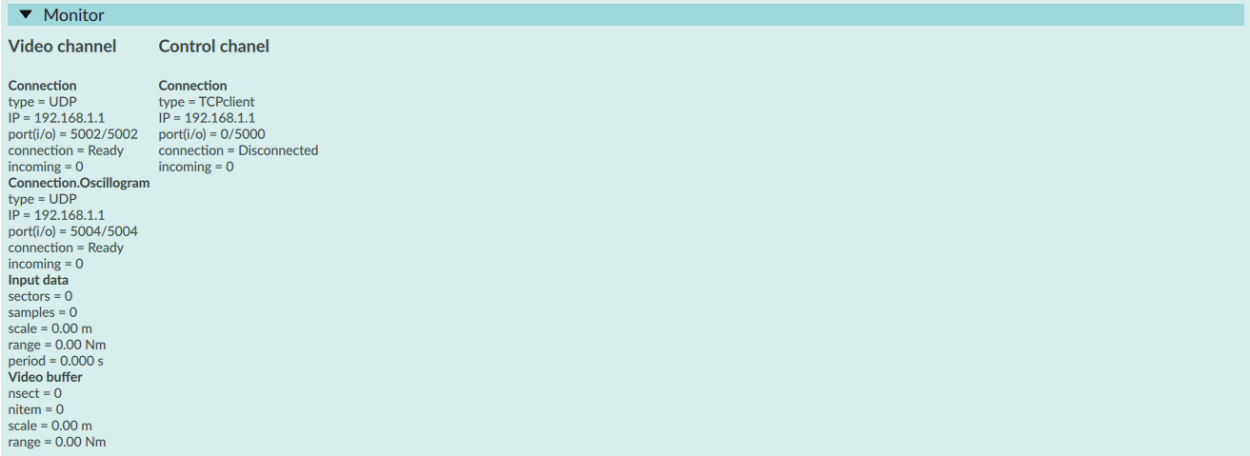


- **Filtering:** make **Noise interference** suppression settings, set the operation parameters of the automatic **Gain** and **Sea** modes, if enabled (see above).

- **Composite signal:** must be set when using a radar that transmits on this channel type.

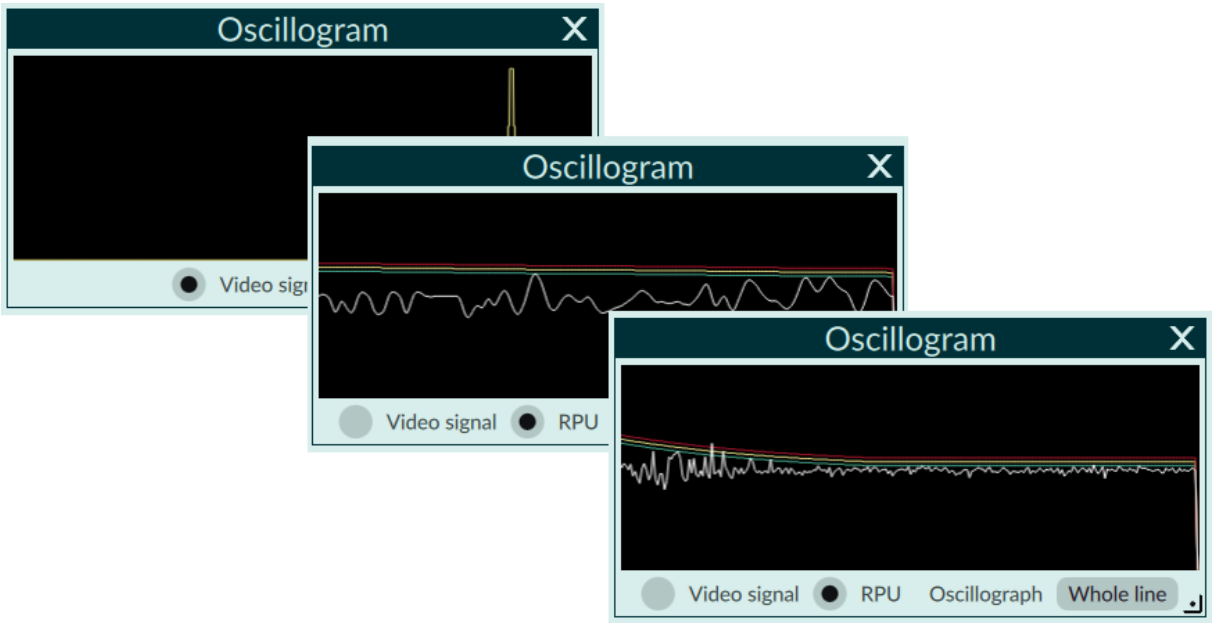


- **Monitor —** diagnostics of output parameters and device status during operation setting.



After successful connection and setup, diagnostic information is displayed in the Monitor.

Oscillogramm window, which is opened/closed by pressing the button of the same name in the **Radar** settings section.



Radar overlay source setup

1. After the performed actions, the Radar overlay source will be marked for deletion (grey background) and will be unavailable for use;

2. The source is completely removed from the system only when ECDIS is rebooted. If necessary, reboot the ECDIS.

NOTE: ECDIS shutdown, when rebooting, with Radar overlay sources marked for deletion, may take longer than usual. This is a result of all running processes being terminated correctly. If you encounter this behavior, it's best to wait for ECDIS to shut down and restart.

BNWAS - Bridge Navigational Watch Alarm System

- ECDIS sends an **$EIEVE** message to the BNWAS.
- Interaction with BNWAS is implemented in ECDIS. Packages are sent every 15 sec., if the ship operator performs any actions with the graphic interface: pressing buttons, moving the mouse or trackball, touching the touch screen.

ECHO

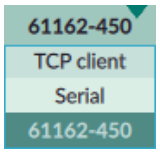
The source of depth data can be INS. In this case INS must be specified as a sensor in the settings.

The sounder transmits sentences with the following headings:

1. IN - INS, depth
2. SD - Sounder, depth
3. SS - Sounder, scanning
4. YX - Transducer.

Bridge Alert Management (BAM)

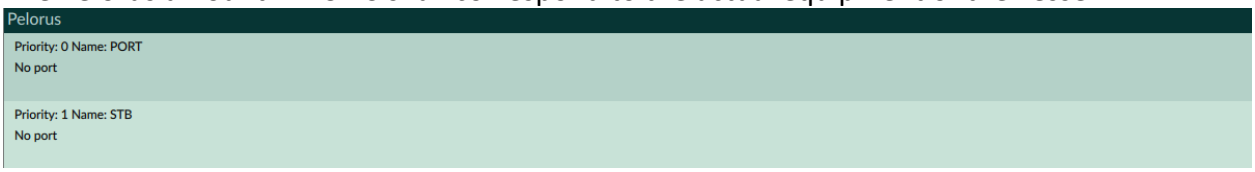
It is possible to connect to a limited interfaces set.



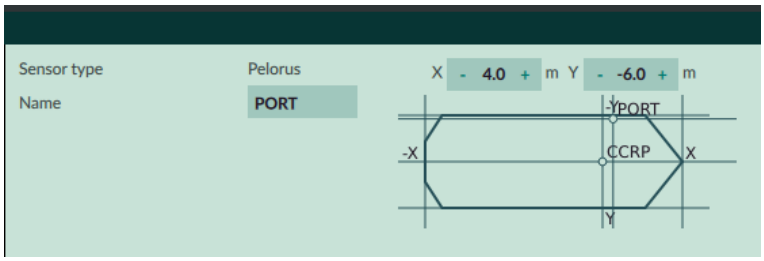
The setting is made according to the requirements of the navigation bridge network.

Pelorus

Pelorus is not a sensor to be connected to ECDIS. Pelorus is an installation point for optical direction finders.
The Pelorus amount created in ECDIS is not limited in number.
The Pelorus amount in ECDIS shall correspond to the actual equipment of the vessel.

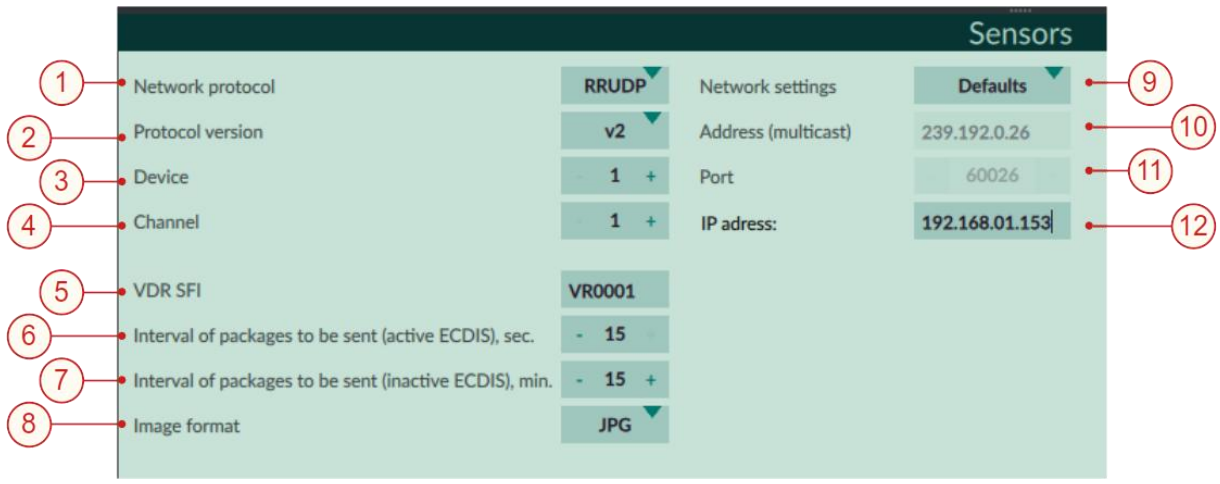


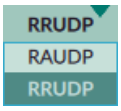
The Pelorus name should indicate the Pelorus location and avoid misinterpretation of the device used for measurements.
The Pelorus installation coordinates must be specified to an accuracy of 0.1 meters relative to the CCRP.



Voyage Data Recorder (VDR)

The VDR settings differ from the standard navigation sensors settings.

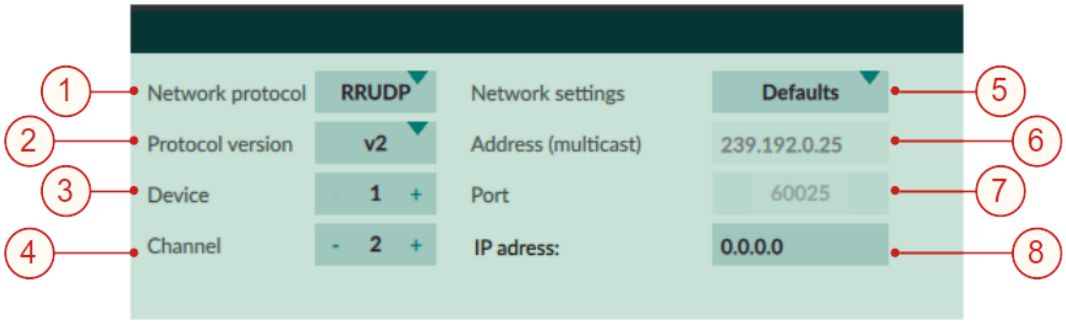


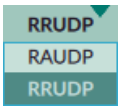
1	**Network Protocol** to transmit a data set:  • **RRUDP** - data transmission with acknowledgement of data reception • **RAUDP** - data transmission without acknowledgement of data reception
2	**Protocol version of** data transmission - must correspond to the protocol version implemented in the VDR. Incorrect selection of the transmission protocol will result in non-receipt of VDR data from ECDIS
3	**Device** - number of the device receiving data sets.
4	**Channel** - data transmission channel in the network-450 (for VDR always 1)
5	**VDR SFI** is the unique network identifier of the receiving device. Must match the VDR SFI.
6	**Interval of packages to be sent (active ECDIS)** - interval of transmission in **Master** role.
7	**Interval of packages to be sent (inactive ECDIS)** - transmission interval in **Backup** role.
8	**Image format** - ECDIS transmits screenshots to VDR. The image format must correspond to the format accepted by the recorder
9	**Network settings** - network settings-450. **Default** settings correspond to the basic recommended settings. **Manual** settings allow you to manually configure the Network-450 settings.
10	**Address (multicast)** - address in the network-450 for transmission of multicast data set.
11	**Port** - network-450 port
12	**IP address** - address of the ECDIS network device where connection to the network-450 is configured. Enter the address when there are 2 or more network devices on the ECDIS computer. Address 0.0.0.0.0 (default) when there is one network device.

Route Sensor

The **Route** sensor is designed to transmit the route generated in ECDIS to external consumers in the network-450 or to receive routes from devices in the network-450

The **Route** sensor settings differ from the standard settings for navigation sensors.



1	**Network Protocol** for transmitting a data set:  • **RRUDP** - data transmission with acknowledgement of data reception • **RAUDP** - data transmission without acknowledgement of data reception
2	**Protocol version of** data transmission - must correspond to the protocol version used in the network-450. Incorrect selection of the transmission protocol will result in non-receipt of data by the addressee
3	**Device** - number of the device receiving data sets.
4	**Channel** - data transmission channel in the network-450 (for Routes always 2)
5	**Network settings** - network settings-450. **Default** settings correspond to the basic recommended settings. **Manual** settings allow you to manually configure the Network-450 settings.
6	**Address (multicast)** - address in the network-450 for transmission of multicast data set.
7	**Port** - network-450 port
8	**IP address** - address of the ECDIS network device where connection to the network-450 is configured. Enter the address when there are 2 or more network devices on the ECDIS computer. Address 0.0.0.0 (default) when there is one network device.

NAVTEX

- The heading sensor has no specific settings.

Firewall Configuration with UFW

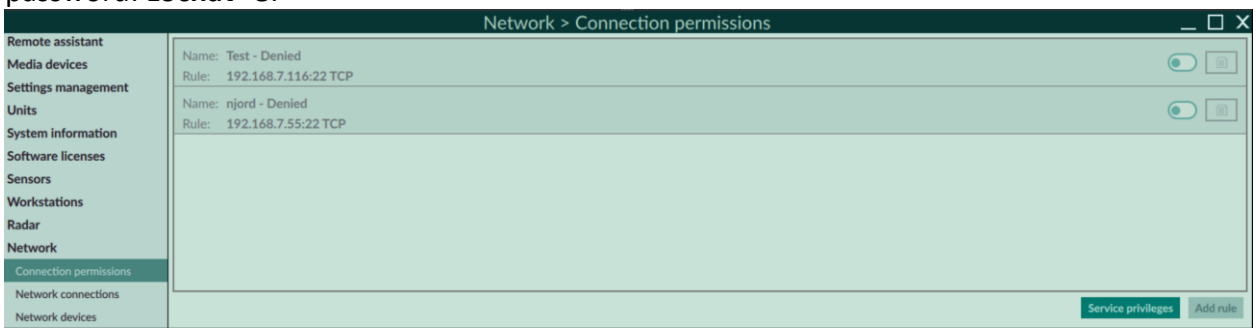
Overview

In this system, the UFW (Uncomplicated Firewall) is used for managing firewall settings. However, we utilize a custom script that operates on top of the UFW and iptables settings to implement specific firewall rules.
You have two options to manage firewall rules

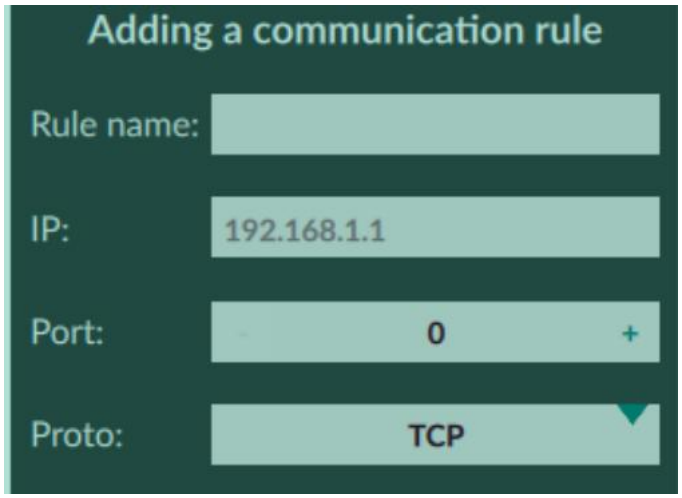
- Via UI
- Via Local Machine Linux Terminal

Custom rules via UI

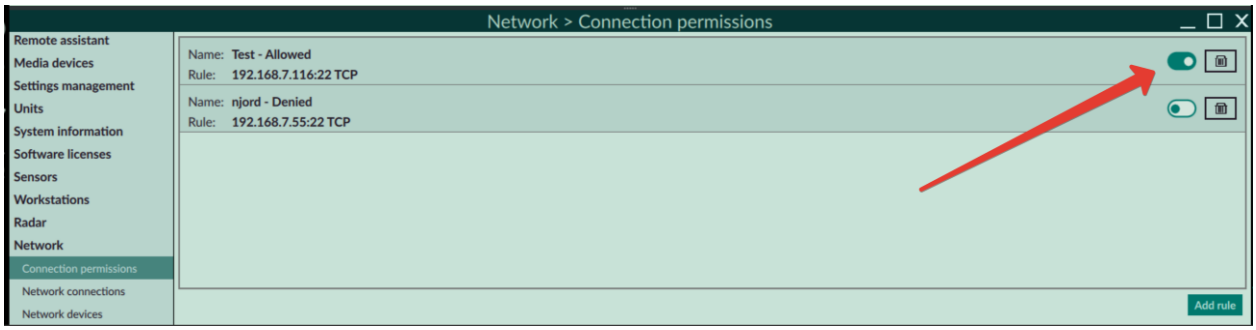
Navigate to **Network- Connections permissions**
NOTE: Before setting up Connections Permissions, ensure you have service privileges. Default password: **Locnav=8**.



- Click **Add Rule** button to add rule



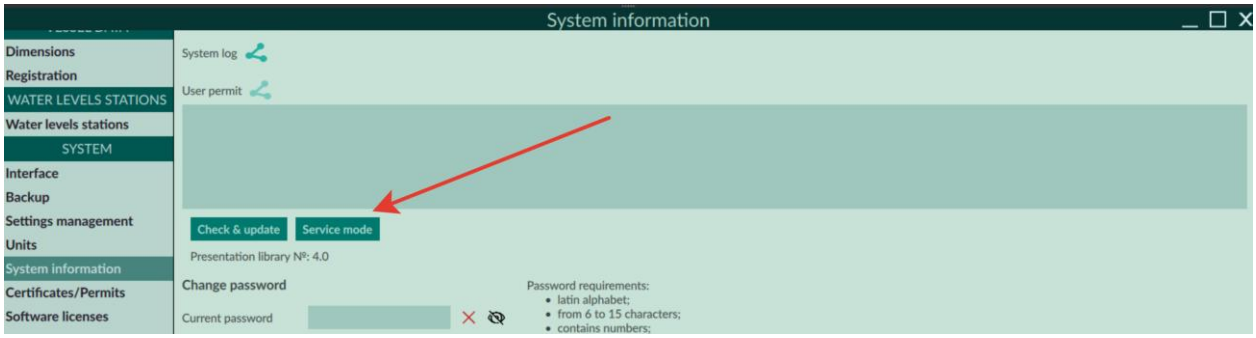
- Add rule settings and click **Save**
- Switch on Rule via switcher



It takes some time to implement firewall rule.
NOTE: After each reboot, all firewall rules are disabled.

Local Machine Linux Terminal

Navigate to **Menu -> Settings -> System -> System Information**
To access linux console, click **Service mode** button and enter password.



Default Login Credentials
marinara:marinara
Note: user *marinara* has sudo privileges, allowing administrative actions on the system.

Rules File Location

The custom rules for firewall is located at:

/opt/ssgnavigation/locius/etc/custom.rules

Note: To create custom firewall rules, **you must use this file**. Do not directly modify the system's UFW configurations or iptables settings.
You can use **mc** (Midnight Commander) and **nano** utilities to modify the script.

Default Firewall Settings

The firewall rules **are applied at system boot** before the ECDIS application starts.
By default, **all connections are prohibited**. Below is the text of the default firewall rule file.

Default Firewall Rule File (custom.rules)

```
# allow all posible lan:
#/usr/sbin/ufw allow from 192.168.0.0/16
#/usr/sbin/ufw allow out to 192.168.0.0/16

#/usr/sbin/ufw allow from 10.0.0.0/8
#/usr/sbin/ufw allow out to 10.0.0.0/8

#/usr/sbin/ufw allow from 172.16.0.0/12
#/usr/sbin/ufw allow out to 172.16.0.0/12

# allow multicast network 239.0.0.0/8:
#/usr/sbin/ufw allow from 239.0.0.0/8
#/usr/sbin/ufw allow out to 239.0.0.0/8

# allow arpa:
```

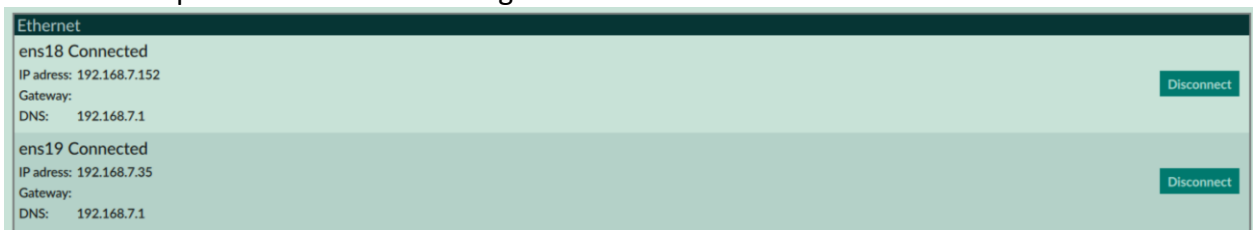
```
#/usr/sbin/ufw allow from 223.168.1.0/24
#/usr/sbin/ufw allow out to 223.168.1.0/24
```

- All rules are commented out by default.
- Uncomment (remove #) to enable specific rules.

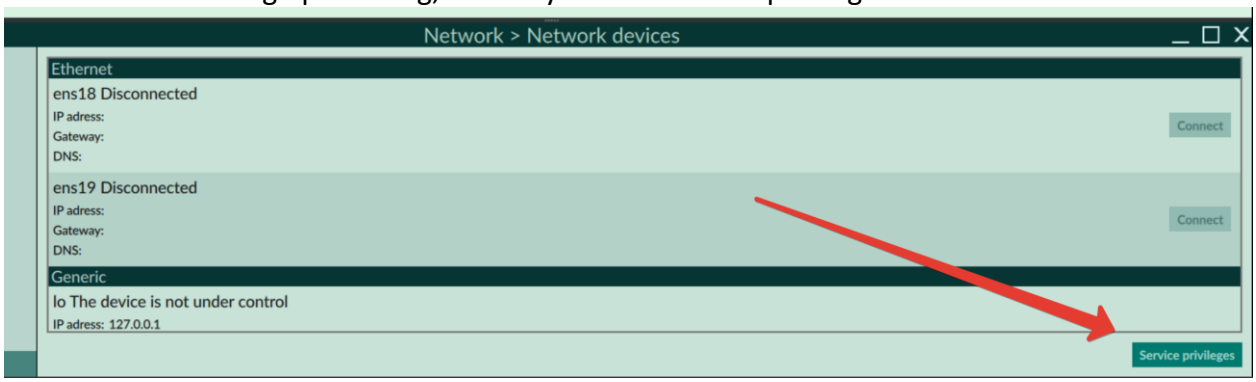
Make sure to execute and modify the firewall rules strictly via this file to ensure system security and proper operation of the ECDIS application.
After modifying the file, reboot your machine.

Network Redundancy (for 460-node)

ECDIS provide interface redundancy. This means that computer shall have at least two Ethernet interfaces to provide interface bonding.



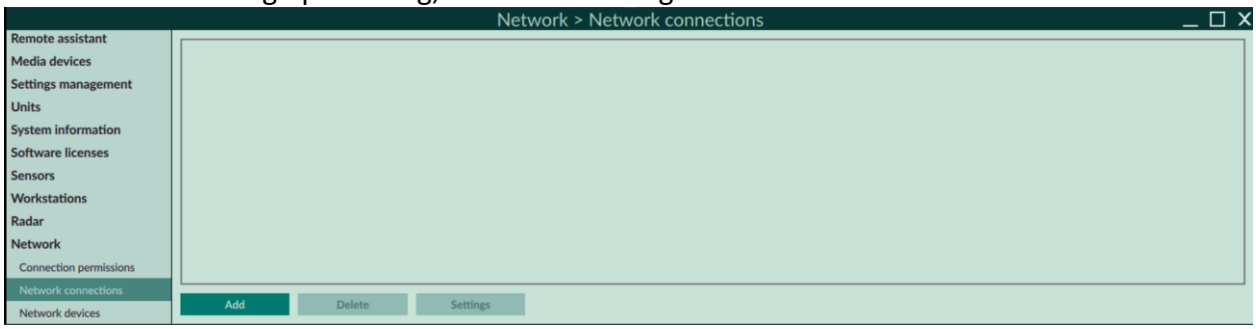
Bonding is the combining of two or more network interfaces into a single logical interface to achieve fault tolerance or increase reliability.
NOTE: Before setting up bonding, ensure you have service privileges.



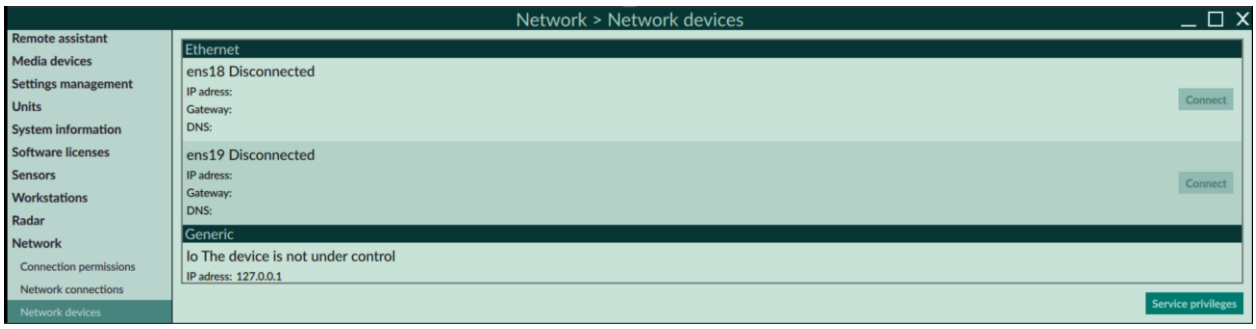
To meet the requirements of IEC 61162-460:2024, you must set up network interface bonding.

- Navigate to **Menu -> Network -> Network connection**

NOTE: Before setting up bonding, delete all existing network connections:

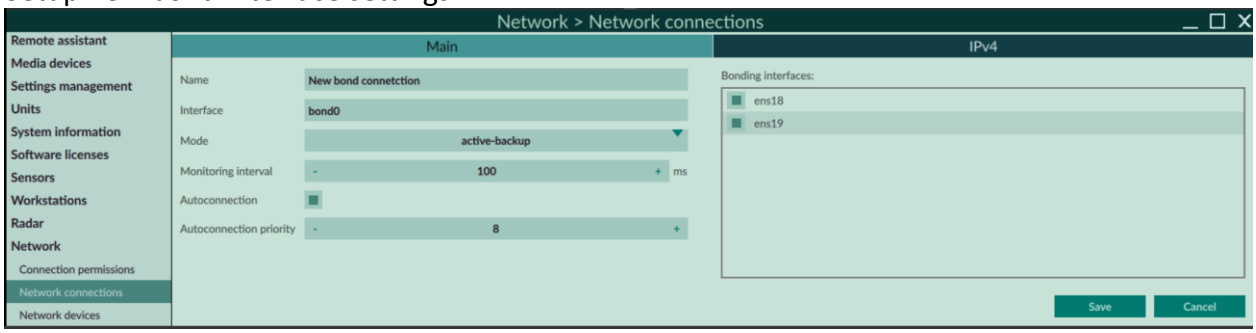


For example, if your ECDIS workstation has two network devices (e.g., ens18 and ens19), delete their connections first. See **Network devices**



- Navigate to **Network connections**
- Cick **Add Connection** and select **bond**

Setup new bond interface settings



Recommended settings:

a) **mode=active-backup**: Sets bonding mode to **active-backup**. Only one interface in the bond is active at a time. If the active interface fails, the bond switches to the backup interface, providing redundancy without load balancing.

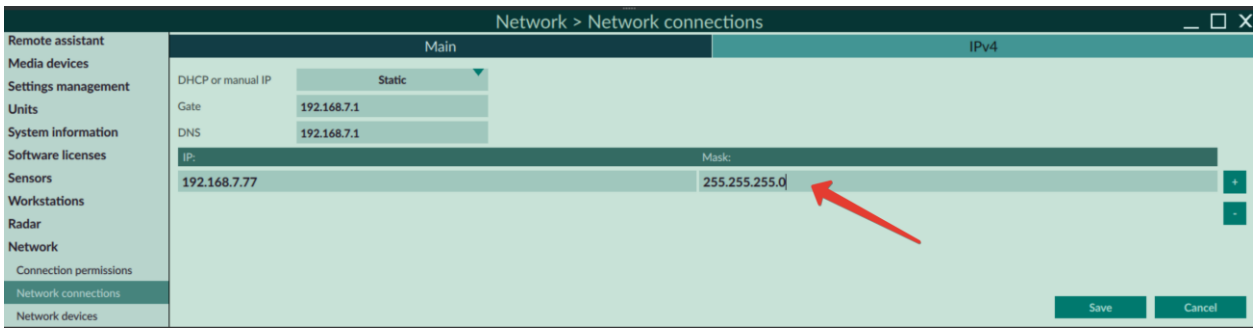
b) **miimon=100**: Specifies the **MII (Media Independent Interface) monitoring** frequency in milliseconds. Setting it to **100 ms** ensures quick detection of link failures. By default, this is set to 0 (disabled).

c) **Autoconnection** – On. Autoconnect on startup.

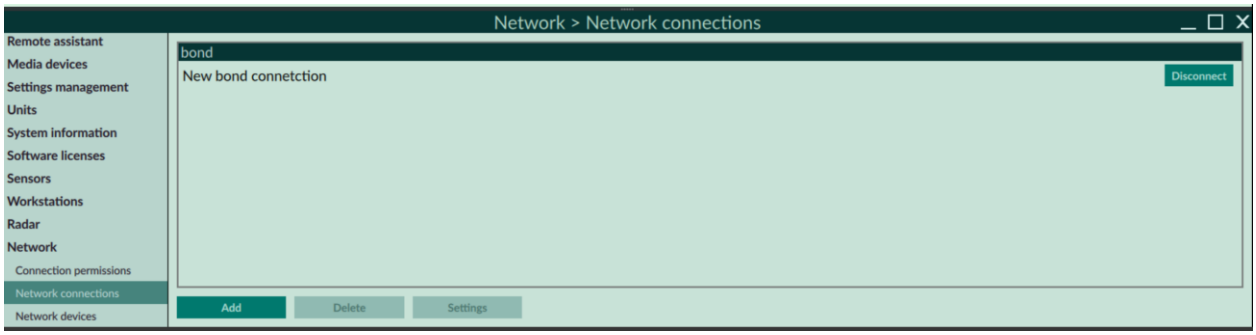
- Choose the interfaces to be included in the bond.
- Set IP Settings on IP tab (Static IP or IP VIA DHCP) and click **Save**

Static IP – mandatory by IEC 61162-460:2024 requirements.

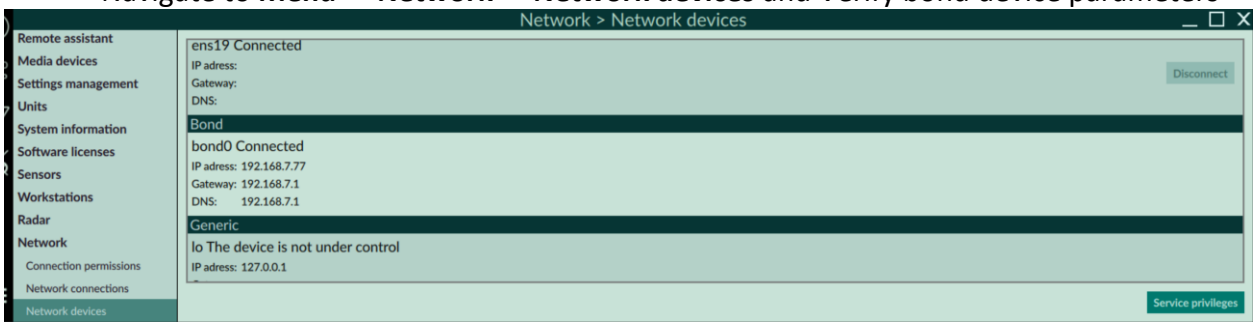
NOTE: To activate **Save** button you should press Enter in the mask field.



- Navigate to **Menu -> Network -> Network connection** and connect to new bond connection



- Navigate to **Menu -> Network -> Network devices** and Verify bond device parameters



Bridge Mode. Master-Backup Settings

ECDIS software can be installed on multiple workstations within the same subnet. This allows for a bridge configuration, where several ECDIS workstations (nodes) can operate together. In this configuration, one node functions as the **Master** and the others as **Backup**.

Critical Settings for Each Node

To ensure proper operation of the ECDIS, it's essential to check and configure the following settings on every node:

1. USB-dongle and License
2. DPI Settings and Graphical Interface Settings
3. Registration and Vessel Data Settings
4. Own Ship and Vessel Dimension Settings
5. System Information Settings (ensure these settings are unique for each node)
6. Network Settings
7. Sensors Settings
8. Firewall Settings

NOTE: When the system starts for the first time, no node is designated as the **Master**. To assign a node as the Master, click the **Master/Backup** button on the single action buttons panel and select **Master status** on the preferred node.

Navigational Sensor Data Across the Bridge

The **Master node** serves as the source for all navigational data (Position, Speed, Heading, etc.) across the bridge network. This means that **primary sensors** must be set up on the Master node, while all Backup nodes receive this data from the Master.

Backup Sensors Connection

Ethernet Sensors Connection

For navigation sensors, we recommend using an **Ethernet connection** via Moxa NPort series or a similar device. This allows you to use **identical sensor settings** on each node, with the following advantages

- When transferring Master status from one node to another, navigational data will not be lost.
- If the Master node is out of order, you can easily transfer the Master status to another node.

Serial Port Sensors Connection

In this configuration, you need to set up the **primary navigation sensors** set on the Master node. On one or more Backup nodes, you must add a backup **Position sensor (EPFS)**, as required by the IEC 61174 standard. However, this approach has limitations:

- When transferring Master status, there is a risk of losing navigational data unless you transfer the status to a node with connected sensors.
- If the Master node fails, Master status must be transferred to a node with connected sensors.

Backup node limitations

Backup nodes are restricted from performing the following actions:

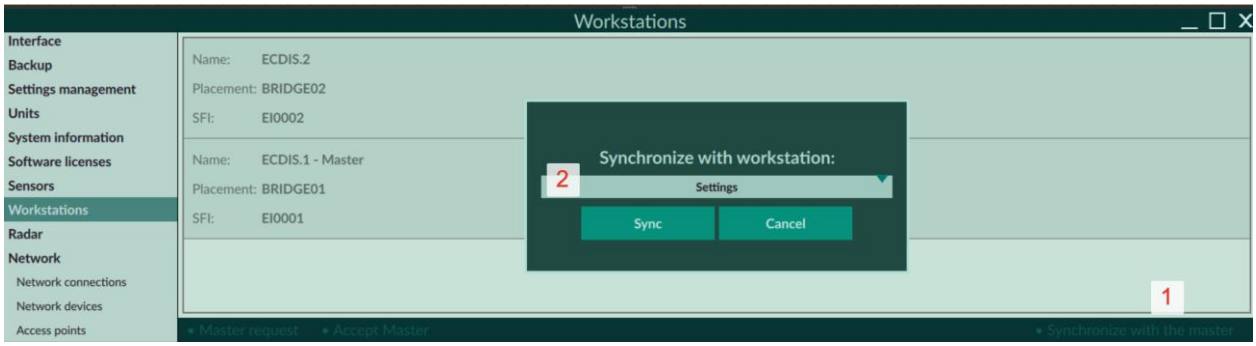
- Enabling/disabling dead reckoning mode
- Performing manual observations
- Correcting coordinates, course, and speed
- Installing ENCs and applying corrections to them
- Performing manual corrections to ENCs
- Dead reckoning with total drift accounted for

Master Backup Synchronization

To simplify bridge configuration, the ECDIS includes a **Master-Backup synchronization function**. We recommend setting up the following settings on the Master node and then synchronizing them with the Backup nodes:

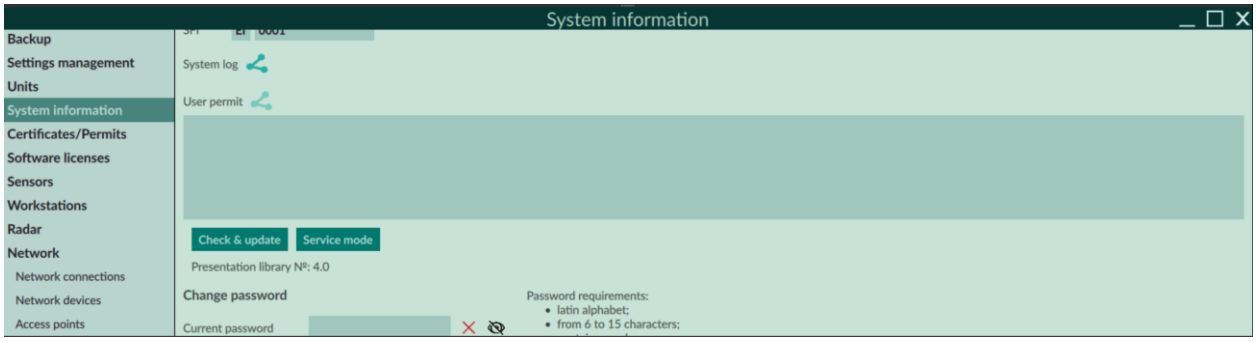
1. **Registration and Vessel Data Settings**
2. **Own Ship and Vessel Dimension Settings**
3. **Sensors Settings**

Once these settings are configured, they can be synchronized from the Master node to the Backup nodes for seamless integration.



Software Update

Software updates are delivered via ISO image files. Ensure that you obtain the ISO image directly from the ECS/ECDIS manufacturer or the ECS/ECDIS software developer.
Navigate to **Menu -> Settings -> System information** to access the settings



To Update ECDIS Software:

1. Save the ISO image file to a prepared USB flash drive.
2. Insert the prepared USB flash drive with the update file into a free USB port on your computer.
3. Click the **Check & Update** button.
4. If the system detects the correct update file, you will be prompted to install the updates. The system will then install the updates and prompt you to reboot.

NOTE: Save the ISO image directly to the USB flash drive as a regular file. **Do not create a bootable USB drive.**

Requirements:

- USB flash drive.
- **FAT32** file system.
- The USB flash drive should be empty, containing only the ISO image file saved in the root directory.

System Logs

NOTE: ECDIS does not provide network monitoring function as described in 8.2 IEC 61162-460. ECDIS also does not provide syslog recording function. It can only be connected to a network which another equipment provides network monitoring and syslog recording function.

Device management activities log

ECDIS logs the following activities:

1. **Configuration Changes:**
    - IP address, port number, and other network settings.
    - The number of active network interfaces.
    - Changes to outbound TCP and UDP connections (additions, deletions, or modifications).
2. **Software Management:**
    - Updates or upgrades to the system.
3. **Device Connections:**
    - Interface setup for external devices (e.g., input interface for gyro heading, output interface for GPS position).
    - The list of all outbound TCP and UDP connections, including their assigned maximum traffic rate.
    - The list of all outbound TCP and UDP connections assigned to each network interface.
4. **IEC 61162-450 errors. (4.3.3),**

Log File Location

```
/var/log/ssg-node460audit/message.log
```

Logging Service

- The system uses a dedicated service for logging: **ssg-node460audit**.
- The configuration for this service is located at:

```
/opt/ssgnavigation/locius/share/modules/node450/settings.json
```

Service Configuration Details

```
{
  "debug": 0,
  "excluded_endpoints": [
    "239.255.0.1:49000",
    "239.255.0.1:49001"
  ],
  "iface_timeout": 0.5,
  "logrotate": 7,
  "logsize": 100,
  "settings_timeout": 1800.0,
  "syslog_endpoints": []
}
```

Parameter Descriptions

1. **debug:**
    - **Value:** 0
    - **Description:** Currently unused. Intended for enabling/disabling debug information.
2. **excluded_endpoints:**
    - **Value:** [239.255.0.1:49000-49001]

- **Description:** A list of excluded IP addresses and ports in the format [000.000.000.000:*|port].

3. **iface_timeout:**
   - **Value:** 0.5 (seconds)
   - **Description:** The frequency of updating the list of network interfaces.
   - **Note:** Values below 0.2 seconds may increase CPU load. Default is 0.5 seconds. It is recommended not to change this.
4. **logrotate:**
   - **Value:** 7
   - **Description:** The number of daily log files to keep. Default is 7.
5. **logsize:**
   - **Value:** 100 (MB)
   - **Description:** The maximum total size of all stored log files. Default is 100 MB.
6. **settings_timeout:**
   - **Value:** 1800 (seconds, or 30 minutes)
   - **Description:** The frequency of updating network settings. Default is 30 minutes.
7. **syslog_endpoints:**
   - **Value:** [] (empty by default)
   - **Description:** A list of syslog servers in the format [udp|tcp:000.000.000.000:port].
   - **Example:** ["udp:192.168.1.216:514"]

Additional Notes

1. **Default Exclusions:**
   - By default, certain endpoints (e.g., 239.255.0.1:49000-49002) are excluded from logging to prevent excessive or unnecessary entries.
2. **Post-Setup Adjustments:**
   - After setup and testing, additional exclusions may be added to the excluded_endpoints list based on operational requirements.
   - **Consideration:** To avoid excessive syslog messages, ephemeral source ports can be represented by a "wildcard".

Managing the ssg-node460audit Service

Check Service Status

```
systemctl status ssg-node460audit
```

Restart the Service

```
systemctl restart ssg-node460audit
```

Stop the Service

```
systemctl stop ssg-node460audit
```

Start the Service

```
systemctl start ssg-node460audit
```

View Logs in Real-Time

```
journalctl -f -u ssg-node460audit
```

Software update log

Software updates are logged in the **system syslog**, not in the audit service log (ssg-node460audit). This ensures that all update-related activities are recorded separately and can be reviewed independently.
To view software update logs in the system syslog, use the following command:

```
sudo grep SYS-UPD /var/log/syslog
```

Remote Syslog Server Connection

Sending Audit Service Logs

The ssg-node460audit service can send logs to a remote syslog server by configuring the syslog endpoints parameter in its JSON configuration file, like described above.

Open the configuration file for editing:

```
sudo nano /opt/ssgnavigation/locius/share/modules/node450/settings.json
```

Add the remote syslog server details to the syslog_endpoints parameter. Use the following format:

```
"syslog_endpoints": ["udp:<remote_server_ip>:514"]
```

- Replace <remote_server_ip> with the IP address of your remote syslog server.
- Use tcp instead of udp if the remote server requires TCP (e.g., "tcp:<remote_server_ip>:514").

Restart the Audit Service

Sending System Syslog Logs to a Remote Syslog Server

To send system logs (including software updates) to a remote syslog server:

1. **Open the Rsyslog Configuration File:**

Edit the main configuration file or create a new one in /etc/rsyslog.d/ (e.g., remote-syslog.conf):

```
sudo nano /etc/rsyslog.d/remote-syslog.conf
```

2. **Add Rules for Sending Logs:**

Add the following line to send all system logs to the remote server:

```
*.* @<remote_server_ip>:514
```

Replace <remote_server_ip> with the IP address of your remote syslog server.
Use @@ for TCP (e.g. *.* @@<remote_server_ip>:514).

3. **Optional: Filter Logs**

To send only specific logs (e.g., kernel or application logs), use filters:
Kernel logs:

```
kern.* @<remote_server_ip>:514
```

Application logs:

```
local7.* @<remote_server_ip>:514
```

Optional: Filter Logs for Software Updates
To send only logs related to software updates (e.g., messages containing SYS-UPD), use the following rule:

```
if $msg contains 'SYS-UPD' then @<remote_server_ip>:514
& stop
```

4. **Restart Rsyslog:**

Apply the changes by restarting the rsyslog service:

```
sudo systemctl restart rsyslog
```

Configure the Firewall

Don't forget update Default Firewall Rule File (custom.rules). Add the following rules to the file:

```
allow 514/udp
allow 514/tcp
```

Configuring the Remote Syslog Server (if applicable)

If you manage the remote syslog server, ensure it is configured to receive logs:

1. **Open the Rsyslog Configuration File:**

Edit /etc/rsyslog.conf on the remote server.

2. **Enable Log Reception:**

For UDP:

```
module(load="imudp")
input(type="imudp" port="514")
```

For TCP:

```
module(load="imtcp")
input(type="imtcp" port="514")
```

3. **Restart Rsyslog:**

Apply the changes by restarting the rsyslog service:

```
sudo systemctl restart rsyslog
```

4. **Configure the Firewall:**

Update the firewall rules to allow incoming connections on port 514:

```
sudo ufw allow 514/udp
sudo ufw allow 514/tcp
```

Ensure the rules are added to the firewall configuration file.

Syslog configuration example

This configuration example enables the syslog server to receive and process logs from remote ECDIS. It supports both UDP and TCP protocols, filters specific log messages, and stores them in

a custom format. This setup is essential for centralized logging, monitoring, and auditing of system activities, particularly for applications like the ECDIS audit service.

```
# Provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# Provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# Define a custom log format for syslog messages
$template SyslogProtocol_rfc5424_net, "<%PRI%>1 %TIMESTAMP:::date-rfc3339% %FROMHOST-IP% %APP-NAME% %PROCID% %msg%\n"

# Filter and log messages with the "450-" tag to a specific file
:syslogtag, startswith, "450-" /var/log/ssg_audit/message.log ; SyslogProtocol_rfc5424_net

# Disable repeated message reduction
$RepeatedMsgReduction off

# Stop further processing for matched messages
& stop
```

1. **UDP and TCP Log Reception:**

The imudp and imtcp modules enable the syslog server to receive logs over UDP and TCP, respectively, on port 514.

2. **Custom Log Format:**

The $template directive defines a custom format for syslog messages, following the RFC 5424 standard.

The format includes:

- Priority (%PRI%)
- Timestamp in RFC 3339 format (%TIMESTAMP:::date-rfc3339%)
- Source IP address (%FROMHOST-IP%)
- Application name (%APP-NAME%)
- Process ID (%PROCID%)
- Log message (%msg%)

3. **Filtering and Logging:**

The :syslogtag, startswith, "450-" rule filters messages with the 450- tag.

These messages are logged to /var/log/ssg_audit/message.log using the custom format defined earlier.

4. **Repeated Message Reduction:**

The $RepeatedMsgReduction off directive disables the reduction of repeated log messages, ensuring all messages are logged.

5. **Stop Further Processing:**

The & stop directive ensures that messages matching the filter are not processed further by other rules.

Applying the Configuration

1. Save the configuration file (e.g., /etc/rsyslog.d/remote-syslog.conf).
2. Restart the rsyslog service to apply the changes:

```
sudo systemctl restart rsyslog
```

Reference Documentation

For more details on configuring rsyslog, refer to the official documentation:

- Rsyslog Documentation

Remote Assistant Function

ECDIS has Remote Desktop Function for technical support. To use this feature, the support workstation must be properly set up.

Implementation Overview

| ECDIS | - - - | Router A | - - - -< Internet > - - - | Router B | - - - | Support PC |

Assumptions:

1. **ECDIS** has internet access through **Router A**.
2. **Router B** has a white **static IP** (e.g., 84.52.109.215).
3. **Router B** is configured to **forward ports** to the local network.
4. **The connection port is assigned on the support side**, e.g., **1234**.
5. **The support workstation (Support PC)** has a local IP **192.168.1.100** and a user **assistant**.

Remote Desktop Connection Process

ECDIS Side Settings

Navigate to: **Menu -> Settings -> Remote assistance** to set up connection settings

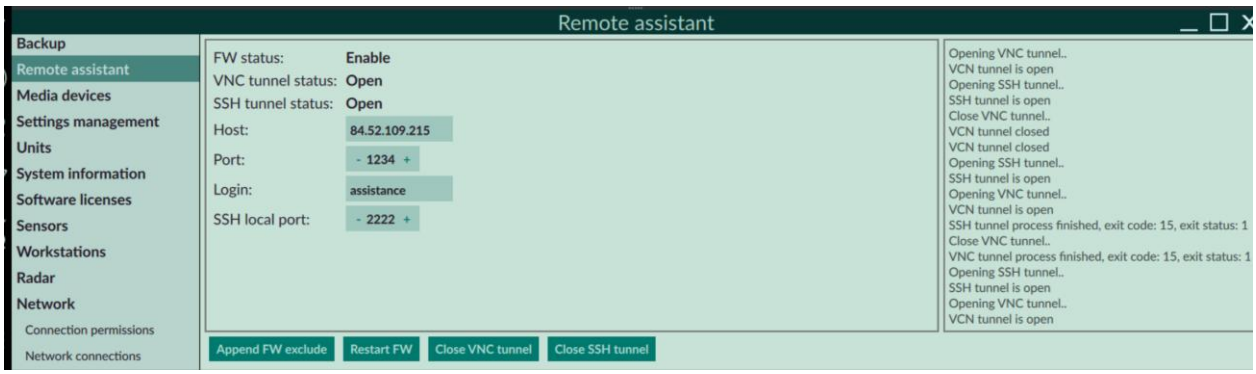
NOTE: To configure these settings, you must be in Service Privilege Mode. The default password is: Locnav=8.

To configure remote support, enter the following connection parameters in the ECDIS system:

- **Host:** 84.52.109.205
- **Port:** 1234
- **Login:** assistant
- **SSH Local Port:** Use an available port on the Support PC (e.g., 2222).

After entering the details, click the **Open VNC** or **Open SSH** button.

If the connection is successful, a secure channel (VNC tunnel/SSH tunnel) will be established between the **ECDIS** and the **support workstation**. The status will show: VNC **Tunnel Status: Open** or SSH **Tunnel Status: Open**.



After completing the work, go to the **Remote Support** section. Click the **Close SSH/VNC** button. This will close the SSH/VNC tunnel.

Firewall Configuration

You may need to allow external connections on the ECDIS workstation. This can be done by configuring firewall rules or adding a temporary exception for the **support workstation**.

To add a temporary exception:

- Click the **"Append FW Exclude"** button.

This will create a temporary rule allowing all traffic from the **Host** address.

- The rule will be removed after restarting the ECDIS workstation or the firewall.

To restart the firewall:

- Use the **"Restart FW"** button.

Support PC Side Setup

1. **Install *nlvnc-remote* on the Support PC**

To enable remote desktop functionality, you need to install the *nlvnc-remote* package on the Support PC.
Follow these steps:

- Contact the ECDIS developer or support team to get the *nlvnc-remote* package.
- Before installation, verify the package's integrity by checking its checksum. This ensures the file has not been corrupted or tampered with.
- Run the following command to install the package:

```
sudo dpkg -i nlvnc-remote.deb
```

- After installation, resolve any missing dependencies by running:

```
sudo apt -f install
```

This command will automatically fix broken dependencies and complete the installation.

Notes:

- This package work for Ubuntu 22.04 **ONLY.**
- The package must be installed by the user **assistant** (not as root).

```
sudo apt -f install
```

2. Configure Port Forwarding on Router B

Set up **Router B** to forward port **1234** to **port 22** of the Support PC (192.168.1.100).

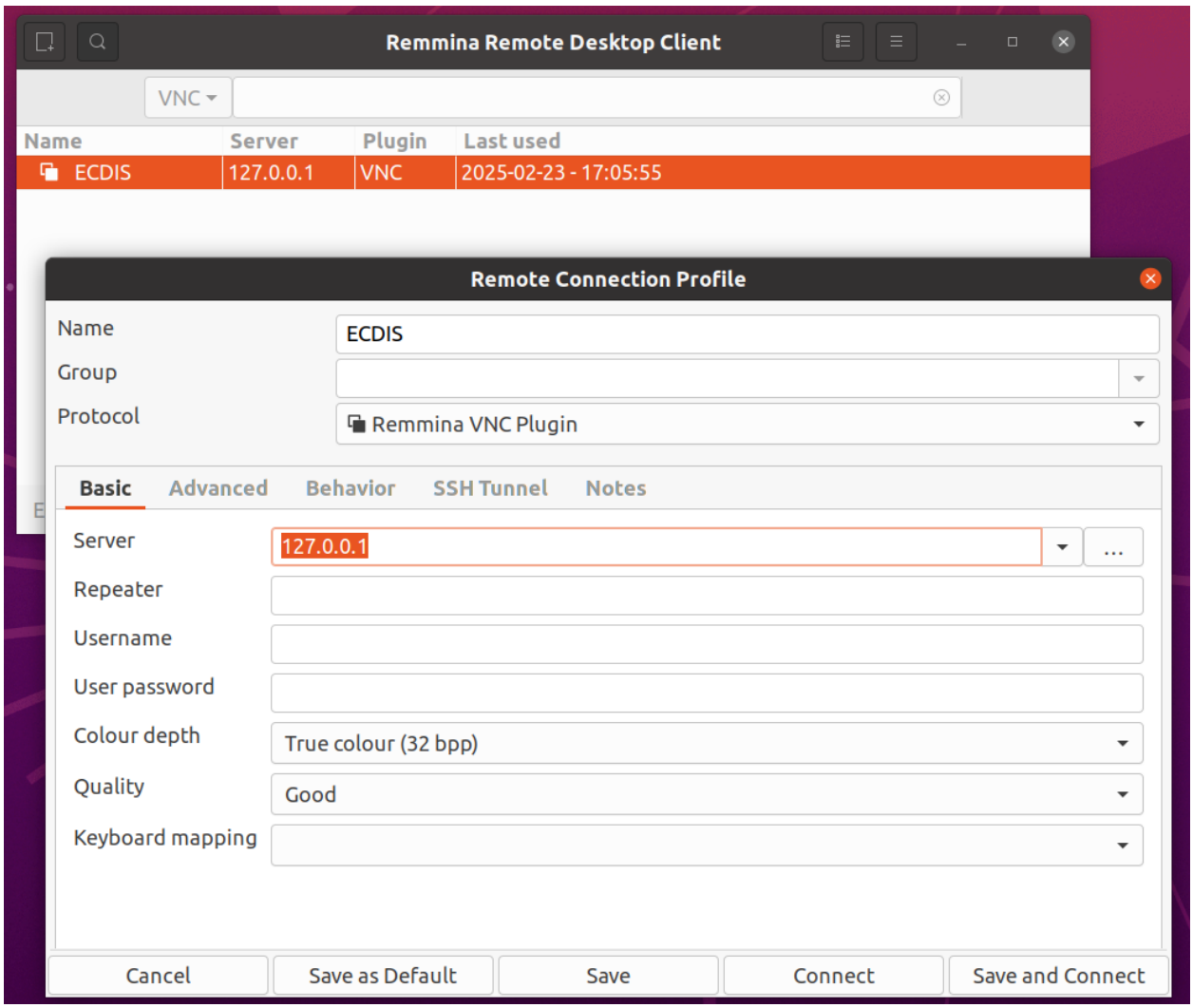
3. Ensure the Support PC is Running

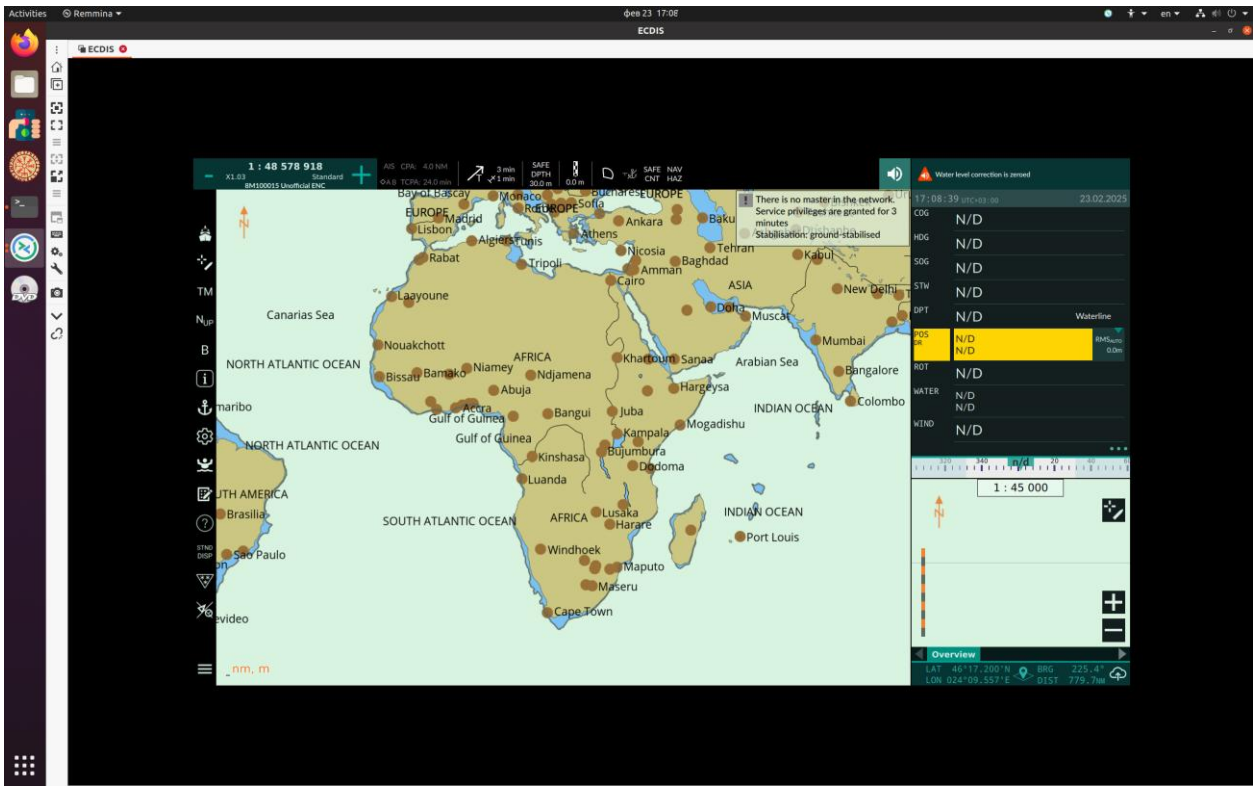
- The Support PC must be turned on and **ready to accept connections**.
- Once the setup is complete, **ECDIS can establish a remote desktop connection** with the support workstation.

Establish Connection

Remote Desktop (VNC)

- Use an RDP client with VNC protocol support (e.g., Remmina Remote Desktop Client).
- Create a connection with the following settings:
  - **Protocol:** Remmina VNC Plugin
  - **Server:** 127.0.1
- Click the **Connect** button.
  - If the settings are correct, you will see the remote ECDIS desktop.


Remmina Remote Desktop Client
VNC
Name
Server
Plugin
Last used
ECDIS
127.0.0.1
VNC
2025-02-23 - 17:05:55
Remote Connection Profile
Name
ECDIS
Group
Protocol
Remmina VNC Plugin
Basic
Advanced
Behavior
SSH Tunnel
Notes
Server
127.0.0.1
Repeater
Username
User password
Colour depth
True colour (32 bpp)
Quality
Good
Keyboard mapping
Cancel
Save as Default
Save
Connect
Save and Connect

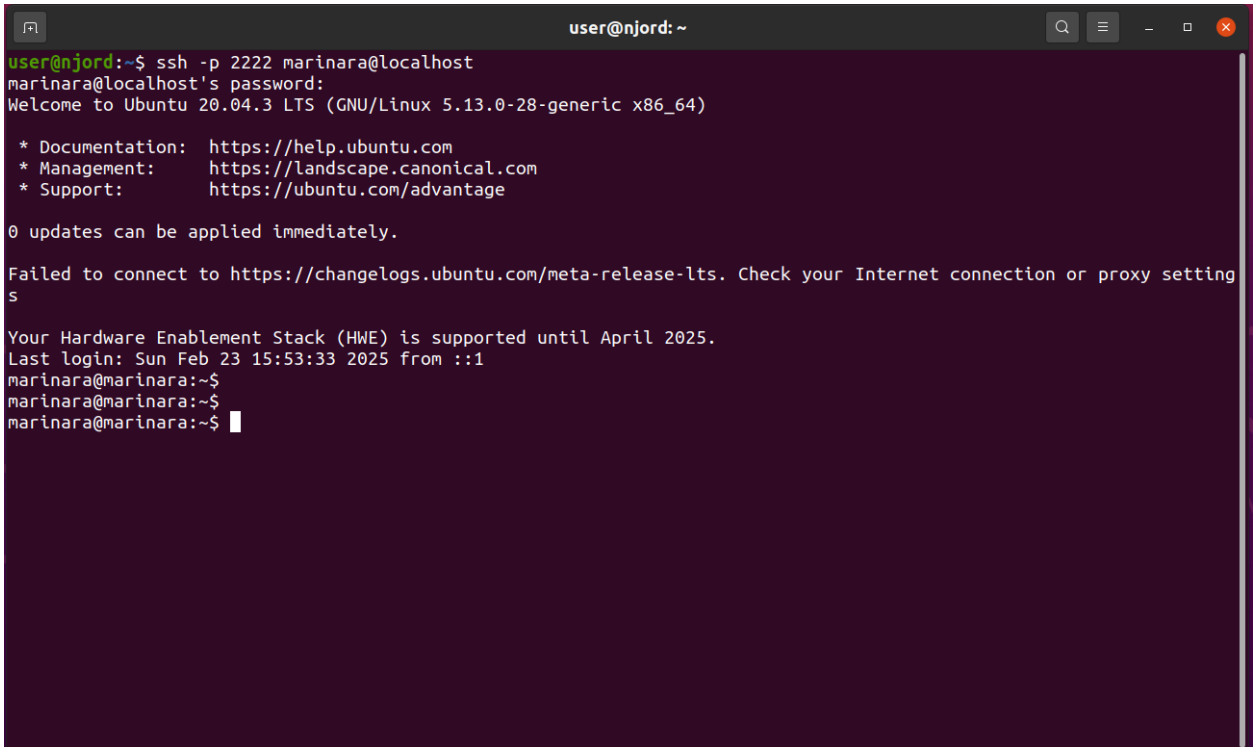


SSH tunnel

In some cases, it may be useful to use SSH connections to the remote ECDIS.

- Open a terminal on the Support PC.
- Use the following command:

```
ssh -p 2222 marinara@localhost
```



ANNEX A. IEC 61162 interfaces

Table 1: Messages received by ECDIS

Message	**Source**	**Content**
ACN[a]	BAM	APS commands
DTM[6]	EPFS	coordinate system
GLL[6] GGA[6] GNS[6] RMC[6] (*)	EPFS	Geographical coordinates
HBT[6]	BAM, INS	Monotone signal
THS[6] HDT[6] (*)	Course sensor, INS	Course
RRT	ECDIS backup	Route transfer report
VBW[6] VHW[6] (*)	SDME, INS	Lag
VTG[6]	EPFS, INS	Speed and heading from the positioning system
RSD[a]	Radar	Radar data
TLB[a] TTD[a] TTM[a] (*)	Radar	Target tracking data
VDM[a] VDO[a]	AIS	AIS targets and information on own ship
NSR[a]	INS	Coordinate, COG/SOG, heading, velocity statuses (see 29. **Ошибка! Источник ссылки не найден.**)
DPT, DBT	Echo, INS	Depth
Note: Suggestions used for backward compatibility(*).		
a) IEC 61924-2. b) IEC 61162-1.		

Table 2: Messages transmitted by ECDIS

Message	**Source**	**Content**
ALC[a]	VDR, BAM, INS	Cyclic alarm list
ALF[a]	VDR, BAM, INS	Warning

ARC[a]	BAM, INS	Rejecting an APS command
EVE[6]	BNWAS	The capacity of a ship driver
HBT[6]	BAM, INS	Monotone signal
RRT	ECDIS backup	Route transfer report
VSD[a]	AIS	Cargo category, navigational status, vessel draft (maximum current static), destination, estimated time of arrival (date, time), flag state
Note: Suggestions used for backward compatibility(*).		
[a] IEC 61924-2. [6] IEC 61162-1.		

ANNEX B. Brief Guide to UFW

UFW (Uncomplicated Firewall) is a user-friendly interface for managing iptables firewall rules. It simplifies the process of configuring a firewall in Linux.

Reset all current settings and allow all connections:

```
ufw --force reset
```

Enable/Disable the firewall:

```
fw --force enable / disable
```

View a numbered list of rules:

```
ufw status numbered
```

Delete the rule with number 2:

```
ufw delete 2
```

Logging events:

```
ufw logging on/off/low/medium/high/full
```

Block/Allow all incoming and outgoing connections:

```
ufw default deny incoming
ufw default deny outgoing
```

Allow all incoming connections from a range of addresses using a subnet mask:

```
fw allow from xxx.xxx.xxx.xxx/xx
```

- **Example:** Allow all incoming connections from addresses 192.168.0.1 to 192.168.255.255:

  ```
  ufw allow from 192.168.0.0/16
  ```

Allow all outgoing connections to a range of addresses using a subnet mask:

```
ufw allow out to xxx.xxx.xxx.xxx/xx
```

- **Example:** Allow all outgoing connections to addresses 192.168.0.1 to 192.168.255.255:

  ```
  ufw allow out to 192.168.0.0/16
  ```

Allow all connections using transport protocol P from address 192.168.1.2:

```
ufw allow from 192.168.1.2 proto P
```

- **P**: This can be either tcp or udp.

Allow all connections using transport protocol P on the range of ports X:Y:

```
ufw allow X:Y/P
```

- **P**: This can be either tcp or udp.

Allow all incoming connections from address A using transport protocol P to the range of ports X:Y:

```
ufw allow from A proto P to any port X:Y
```

- **P**: This can be either tcp or udp.

Allow all connections using application protocol P:

```
ufw allow [from / out to] 192.168.1.2 proto P
```

- **P**: This can be protocols like http, https, ssh, ftp.

ANNEX C. Destination multicast addresses and port numbers

Transmission group	Category	Multicast address	Destination port
MISC	SF not explicitly listed below	239.192.0.1	60001
TGTD	Target data (AIS), tracked target messages (Radar)	239.192.0.2	60002
SATD	High update rate, for example ship heading, attitude data.	239.192.0.3	60003
NAVD	Navigational output other than that of TGTD and SATD groups	239.192.0.4	60004
VDRD	Data required for the VDR according to IEC 61996-1	239.192.0.5	60005
RCOM	Radio communication equipment	239.192.0.6	60006
TIME	Time transmitting equipment	239.192.0.7	60007
PROP	Proprietary and user specified SFs	239.192.0.8	60008
USR1	User defined transmission group 1	239.192.0.9	60009
USR2	User defined transmission group 2	239.192.0.10	60010
USR3	User defined transmission group 3	239.192.0.11	60011
USR4	User defined transmission group 4	239.192.0.12	60012
USR5	User defined transmission group 5	239.192.0.13	60013
USR6	User defined transmission group 6	239.192.0.14	60014
USR7	User defined transmission group 7	239.192.0.15	60015
USR8	User defined transmission group 8	239.192.0.16	60016
BAM1	BAM compliant alert source reporting to CAM group 1	239.192.0.17	60017

Category	Multicast address	Destination port
Non re-transmittable binary file transfer group 1 [a]	239.192.0.21	60021
Non re-transmittable binary file transfer group 2 [a]	239.192.0.22	60022
Non re-transmittable binary file transfer group 3 [a]	239.192.0.23	60023
Non re-transmittable binary file transfer group 4 [a]	239.192.0.24	60024
Non re-transmittable binary file transfer group 5 [a]	239.192.0.25	60025
Re-transmittable binary file transfer group 1 [b]	239.192.0.26	60026
Re-transmittable binary file transfer group 2 [b]	239.192.0.27	60027
Re-transmittable binary file transfer group 3 [b]	239.192.0.28	60028
Re-transmittable binary file transfer group 4 [b]	239.192.0.29	60029
Re-transmittable binary file transfer group 5 [b]	239.192.0.30	60030

[a] Address 239.192.0.25, port 60025 is the default for ECDIS route transfer (see IEC 61174).

[b] Address 239.192.0.26, port 60026 is the default for VDR image transfer (see IEC 61996-1).

Address 239.192.0.30, port 60030 is the default for ECDIS re-transmittable data blocks for route transfer (see IEC 61174).

Category	Multicast address	Destination port
Syslog	239.192.0.254	514
Sending to syslog can use multicast or UDP unicast. Some switches can support only UDP unicast.		

ANNEX D. MAC Adress List

This table must be filled by installation works

Equipment	SFI	MAC	Iface name (optional)	IP
ECDIS				