



**IMOS** V.5

Integrated Maritime Operations System

Administration Manual

January 5, 2009

Copyright © 2003-2009 Veson Nautical Corporation.

All rights reserved. No part of this document may be reproduced, stored in electronic format, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission of Veson Nautical Corporation.

Although every precaution has been taken in the preparation of this document, the author and Veson Nautical Corporation assume no responsibility for errors or omissions. No liability is assumed for any damages resulting from the use of the information contained herein.

Trademarks: IMOS is a trademark of Veson Nautical Corporation.

# Contents

---

<b>Introduction to IMOS Administration .....</b>	<b>5</b>
About IMOS Administration.....	5
Sequence of Administration Steps .....	5
Developing a Disaster Contingency Plan .....	5
Backup Procedures (Client-Hosted Pilot) .....	6
Backup Procedures (VNC-Hosted Pilot) .....	6
Recommended Hardware Configuration for Off-Site Installation .....	6
<b>Security .....</b>	<b>7</b>
Logging On and Off as an Administrator .....	7
Logging On .....	7
Logging Off .....	8
About Groups and Users.....	8
Setting Up Security .....	9
Creating a New Group.....	11
Adding or Removing Group Members .....	12
Adding or Removing Group Module Rights.....	13
Adding or Removing Group Object Rights .....	14
Creating a New User .....	15
Adding or Removing Group Membership .....	16
Adding, Removing, or Overriding User Module Rights .....	17
Adding, Removing, or Overriding User Object Rights .....	18
Editing a User or a Group .....	19
Deleting a User or a Group .....	19
<b>Index .....</b>	<b>21</b>

# Figures

---

IMOS Login Page .....	7
IMOS .....	8
IMOS Data Center .....	9
IMOS Security .....	9
Properties for Group, User Tab.....	11
Properties for Group, Membership Tab .....	12
Properties for Group, Module Rights Tab.....	13
Properties for Group, Object Rights Tab .....	14
Properties for User, User Tab.....	15
Properties for User, Membership Tab .....	16
Properties for User, Module Rights Tab.....	17
Properties for User, Object Rights Tab.....	18

# Introduction to IMOS Administration

---

## About IMOS Administration

This manual is for administrators of IMOS, the Integrated Maritime Operations System from Veson Nautical Corporation. It contains guidelines for [developing a disaster contingency plan](#) and instructions for [setting up security](#).

For hardware and software information, see the *IMOS Requirements and Recommendations* document.

For installation information, see the *IMOS Installation Manual*.

## Sequence of Administration Steps

1. Install and configure IMOS. For more information, see the *IMOS Installation Manual*.
2. [Log on as an administrator](#).
3. Set up [IMOS Security](#).
4. Complete the following setup tasks. For more information about these tasks, see the *IMOS Manual* or *IMOS Help*.
  - a. Edit and/or enter information in the term lists.
  - b. Enter information into the Address Book.
  - c. Edit and/or enter vessel information.
  - d. Edit and/or enter cargo names.

## Developing a Disaster Contingency Plan

This section contains general guidelines for developing a disaster contingency plan. During the implementation phase, Veson Nautical reviews the existing disaster recovery hardware and software plan and tailors this information to your requirements. This is particularly important if other applications will be communicating with IMOS via the XML interfaces or otherwise.

Existing best practices apply to IMOS. The core of IMOS resides in the database, and the most important element of disaster recovery is to ensure that users are always able to access an up-to-date database. Several third-party vendors have applications for best practices that you should consider in developing a complete disaster recovery plan.

## Backup Procedures (Client-Hosted Pilot)

We recommend the following backup procedures to ensure that IMOS is highly available.

- **Database backups:** It is very important to keep frequent backups of the database. We recommend at least one full backup daily. These backups should also be sent electronically to an offsite facility that serves as the secondary source in the event of a disaster at the primary site. Typically, it is sufficient to keep two weeks of backups in disk storage and to archive older backups to tape. Using one of these archive files, it is possible to fully restore the state of the IMOS system. You may need to consider exogenous states, such as systems that link to IMOS, separately.
- **Application and Configuration file backups:** Veson Nautical keeps a complete record of all application programs installed at a client site. However, we recommend that you back up your application folder any time the configuration changes (for program updates, Configuration file changes, etc.). Any information not stored in the database will exist under the root IMOS installation tree; the application uses no registry settings.
- **Client backups:** IMOS is designed to be installed on the server and keep all states in the database, so no specific handling is required for client machines beyond standard disaster recovery procedures (restoring the operating system, any other local applications, etc.).

## Backup Procedures (VNC-Hosted Pilot)

- **Database backups:** Pilot databases are hosted at PEER 1's co-location data center in New York, New York, which features UPS, diesel generator power, and fire suppression. Databases are backed up daily to a separate physical drive and then backed up (disk-to-disk over the Internet) to a RAID 5 disk array in our Boston office and checked for integrity. Two weeks of database backups are retained.
- **Recovery:** In the event recovery is necessary, the pilot environment will be restored by Boston-based VNC staff from the most recent available backup. The recovery will be completed within two business days. The following will be restored:
  - IMOS application
  - Pilot-specific IMOS configuration
  - Most recent available backup of IMOS database(s)
  - Remote desktop user(s) associated with the pilot (account credentials only; passwords may need to be reset)

No other data (for example, files you create or store on our system) will be restored without prior arrangement.

## Recommended Hardware Configuration for Off-Site Installation

In the event of a catastrophic failure at the primary site, we recommend the setup of an off-site IMOS server environment. This includes the database and applications, which can be restored at any time using the backups outlined above. Generally, we recommend Terminal Server access to the off-site server, so that users can gain access to the system with just an Internet connection.


# Security

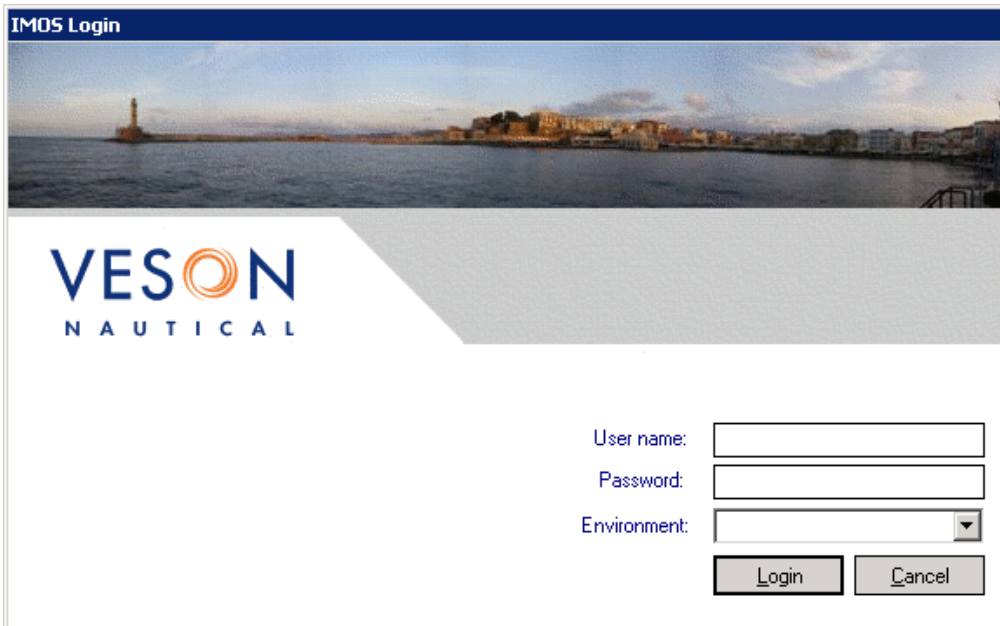
---

## Logging On and Off as an Administrator

### Logging On

To access IMOS Security, you must log on as an administrator. Follow these steps.

1. Double-click  on your desktop. The Login page appears.



IMOS Login

**VESON**  
NAUTICAL

User name:

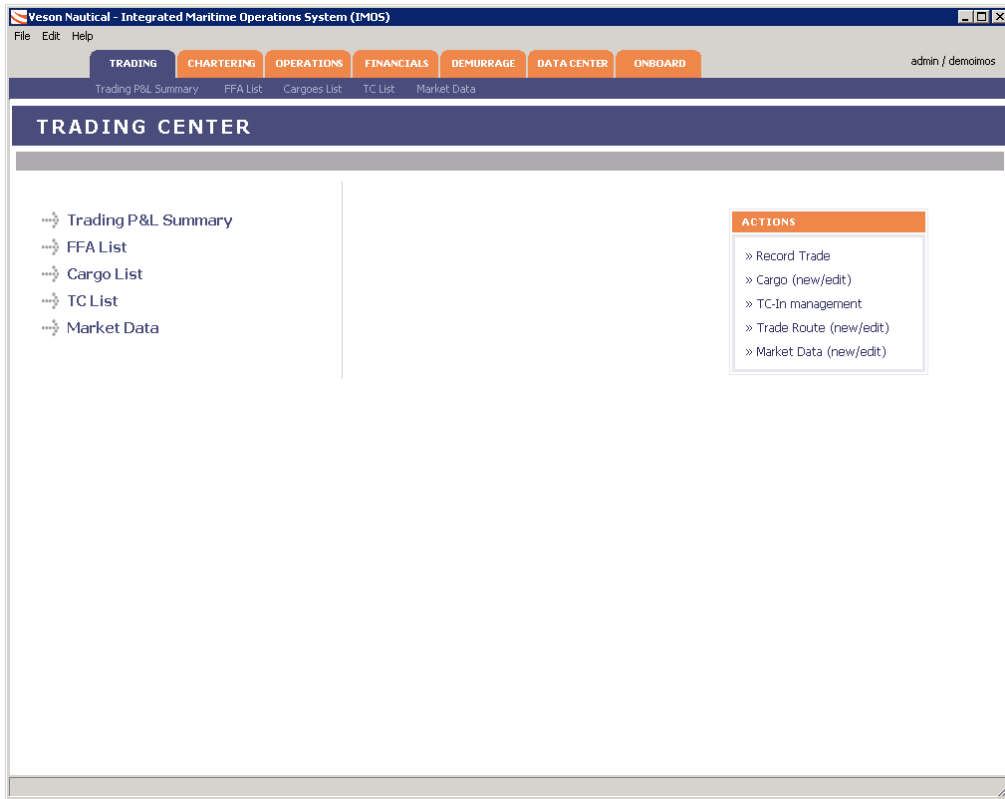
Password:

Environment:

Login Cancel

#### *IMOS Login Page*

2. Enter your **User name** and **Password**.  
**Note:** The initial administrator user name and password are set up by Veson Nautical.  
**Be sure to change the password.**
3. Click **Login**. IMOS appears.



IMOS

## Logging Off

When you are finished using IMOS, do one of the following.

- Click .
- On the **File** menu, click **Exit**.
- On the **File** menu, click **Logoff**. On the Login page, click **Cancel**.

## About Groups and Users

IMOS recognizes two types of users for assigning access rights:

- **Groups** have group access rights. Groups can belong to other groups. A group acts as a template: Any user in a group inherits all the access rights of the group.
- **Users** have individual access rights. Users can belong to one or more groups, but they do not have to belong to any groups.

Users' overall access rights are a combination of their group and individual access rights.

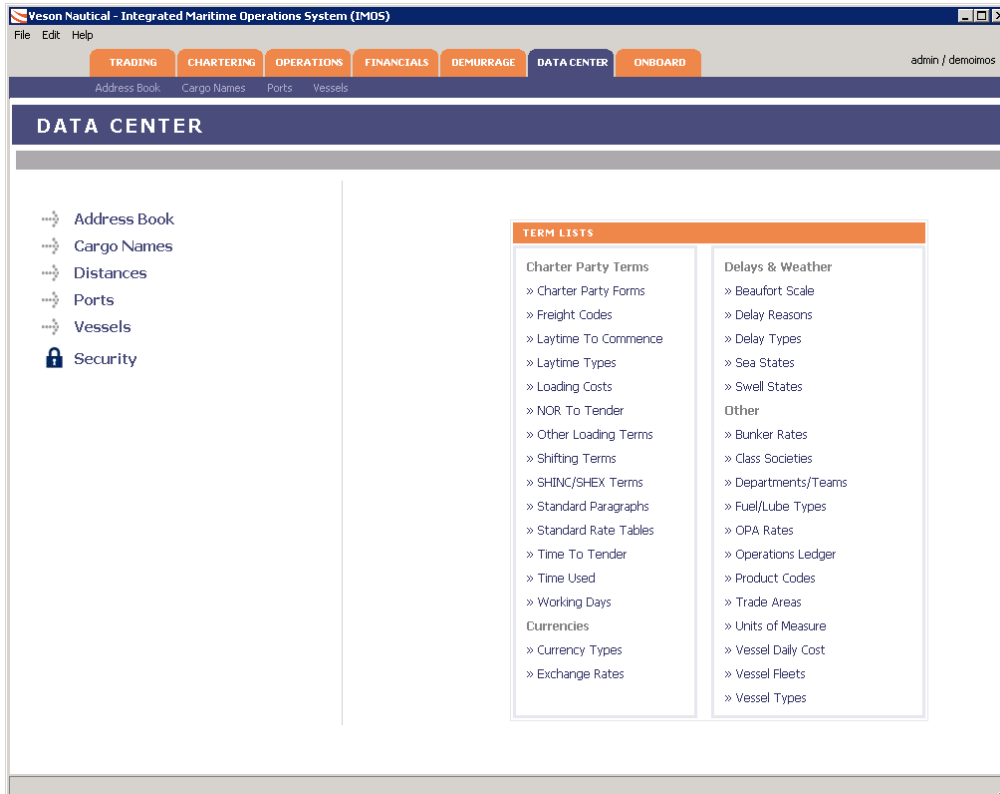


# Setting Up Security


IMOS Security is designed to protect data and prevent unauthorized access to the IMOS environment. The Security system manages all user rights on the IMOS system. For each user and/or group, you can assign rights to perform the functions related to each module and object in IMOS.

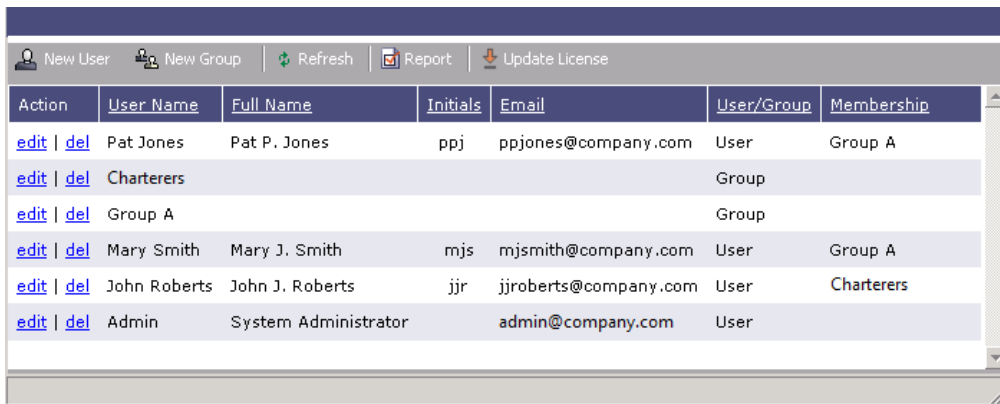
To set up IMOS Security:

1. Click the **Data Center** tab.



*IMOS Data Center*

2. In the Data Center, click  **Security**.



*IMOS Security*

We recommend that you create groups and assign rights to them before you create individual users. You might find it more efficient to categorize users in groups and then adjust rights for individuals, rather than starting from scratch for each user.

To set up users and groups:

1. [Create groups](#) and assign module and object rights.
2. [Create users](#).
  - a. Assign users to groups.
  - b. Assign user module and object rights or edit user rights inherited from groups.


Once these steps are complete, users can use their credentials on the Login page. If IMOS verifies their credentials, IMOS starts.

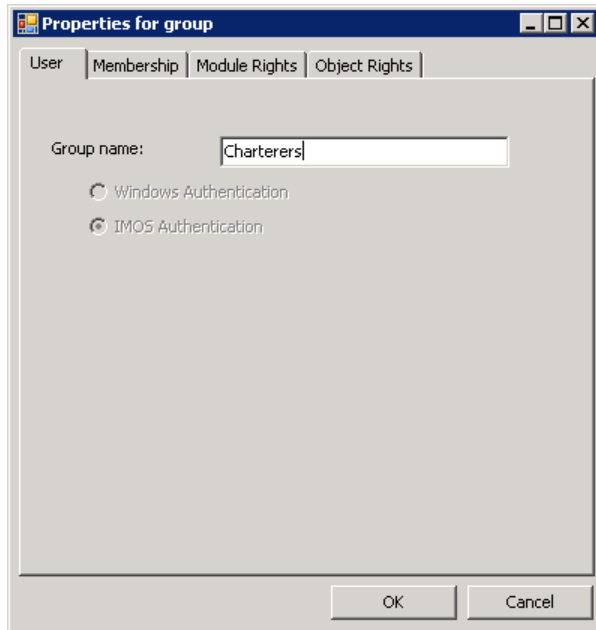
Creating groups and creating users are nearly identical tasks, with the same window tabs:

- User
- Membership
- Module Rights
- Object Rights

## Creating a New Group

To create a new group:

1. In IMOS Security, click . The Properties for Group window **User** tab appears.

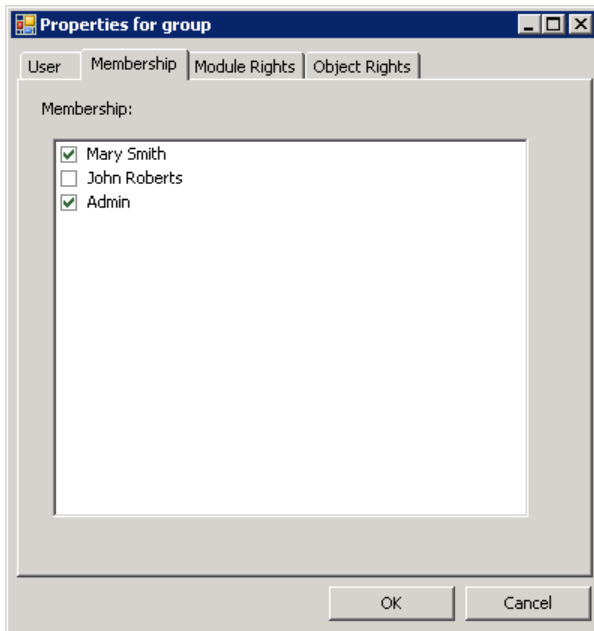


### *Properties for Group, User Tab*

2. Enter a name for the group that describes the members' functions or rights, for example, Chartering Users, Operations Users, Team X Users, etc.

## Adding or Removing Group Members

3. To set up group members, click the **Membership** tab.



### *Properties for Group, Membership Tab*

4. The Membership tab contains a list of IMOS users. Each user name is preceded by a check box. To add or remove a group member, click the user's check box.

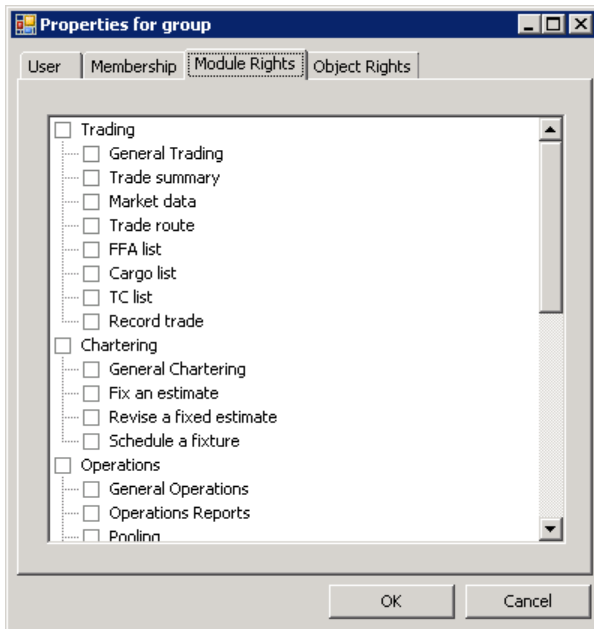
= The user is not a member of the group.

= The user is a member of the group.

**Note:** We recommend that you do not assign the administrator to any groups, but assign all rights individually. As a member of a group, the administrator might be denied rights if the group has any rights actively denied.

## Adding or Removing Group Module Rights

- To set up group rights to modules and actions, click the **Module Rights** tab.



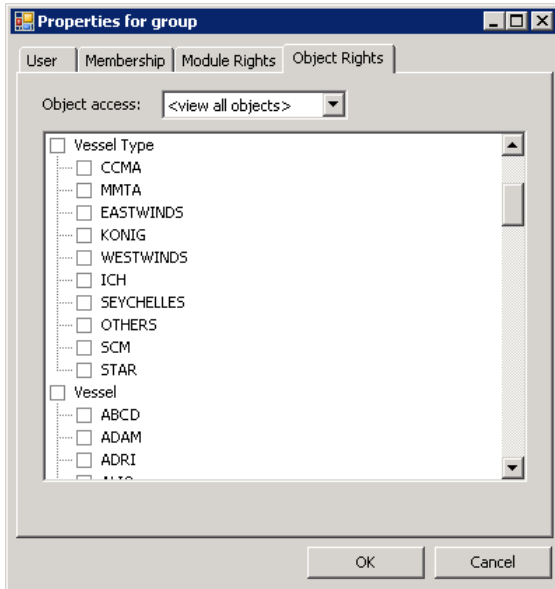
### *Properties for Group, Module Rights Tab*

- The Module Rights tab lists the modules of IMOS and the actions associated with them. Select the group's rights for the module actions.
  - Each module name is preceded by a check box. To expand or collapse the list of actions for a module, double-click the module's check box.
  - When a module list is expanded, each action is preceded by a check box. To change the group's right to perform a task, click the check box. Each time you click, the right changes.
    - = **No access**: The group does not have the right to perform the task.
    - = **Read-only**: The group can retrieve information from files and view reports. General rights, such as General Chartering, have this option, but specific actions, such as Fix an estimate, do not.
    - = **Read/Write**: The group has full ability to store and update information in the database.

**Note:** A user's rights include the individual user rights plus the rights from any groups in which the user is a member. If a user has different rights, either assigned individually or from groups, the highest access rights apply.

## Adding or Removing Group Object Rights

7. To set up group rights to objects, click the **Object Rights** tab.



*Properties for Group, Object Rights Tab*

8. The Object Rights tab lists the categories of objects in IMOS and the objects associated with them. Select the group's rights to the objects.

- To filter the list of objects, select an object category from the menu:
  - View all objects
  - Company
  - Vessel Type
  - Vessel
  - Pool
- Each object is preceded by a check box. To expand or collapse the list of objects for a category, double-click the category's check box.
- When an object category list is expanded, each object is preceded by a check box. To change the group's right to an object, click the check box. Each time you click, the right changes.
  - = The group does not have the right to the object.
  - = Read-only: The group can retrieve information from files and view reports.
  - = Read/Write: The group has full ability to store and update information in the database.

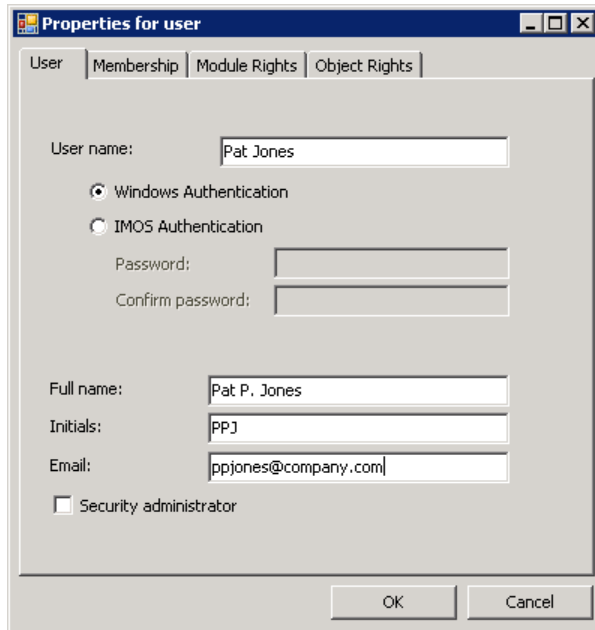
**Note:** A user's rights include the individual user rights plus the rights from any groups in which the user is a member. If a user has different rights, either assigned individually or from groups, the highest access rights apply.

9. When you finish creating the group, click **OK**.

## Creating a New User

To create a new user:

1. In IMOS Security, click . The Properties for user window **User** tab appears.



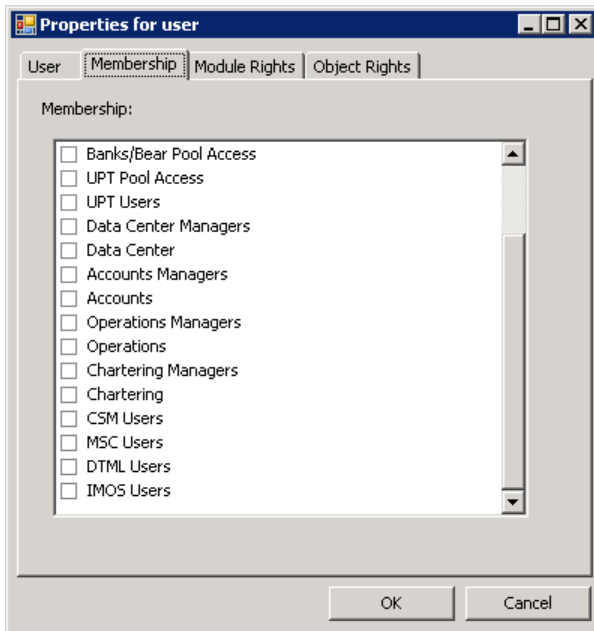
The screenshot shows a dialog box titled "Properties for user" with a blue header bar. Below the header are four tabs: "User", "Membership", "Module Rights", and "Object Rights". The "User" tab is selected. The dialog contains several input fields and a checkbox. The "User name" field contains "Pat Jones". There are two radio buttons for authentication: "Windows Authentication" (selected) and "IMOS Authentication". Below these are "Password:" and "Confirm password:" fields, both empty. The "Full name:" field contains "Pat P. Jones", "Initials:" contains "PPJ", and "Email:" contains "ppjones@company.com". At the bottom left is a checkbox labeled "Security administrator" which is unchecked. At the bottom right are "OK" and "Cancel" buttons.

### *Properties for User, User Tab*

2. Enter the following information:
  - **User name:** Up to 25 characters.
  - Authentication: Select one.
    - **Windows Authentication:** If you select this option, IMOS uses Windows login credentials for authentication, and the user does not have to log in a second time with possibly a different user name and password. If the user changes the Windows password, it is also changed here.
    - **IMOS Authentication:** If you select this option, enter a **Password** for the user (at least five characters), and then enter it again to **Confirm the password**.
  - **Full name:** The user's full name.
  - **Initials:** The user's initials.
  - **Email:** The user's email address.
  - **Security administrator:** To make this user a Security administrator, select this check box.

## Adding or Removing Group Membership

3. To set up group membership for the user, click the **Membership** tab.



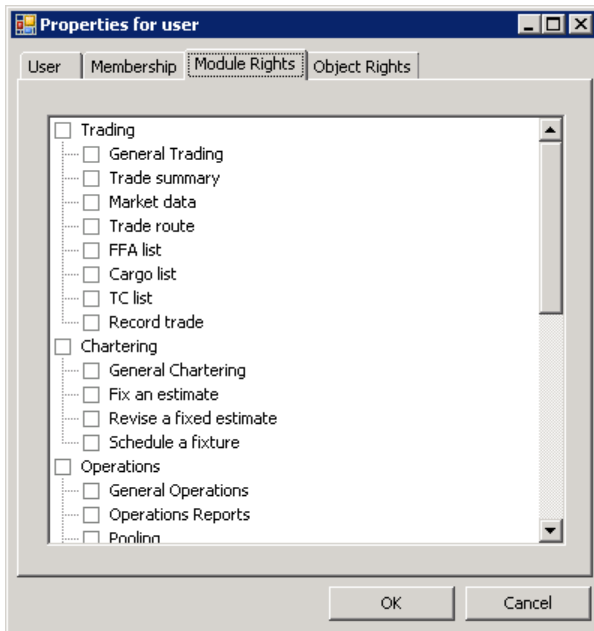
*Properties for User, Membership Tab*

4. The Membership tab contains a list of user groups. Each group name is preceded by a check box. To add the user to a group or remove the user from a group, click the group's check box.
  - = The user is not a member of the group.
  - = The user is a member of the group.



## Adding, Removing, or Overriding User Module Rights

- To set up user rights to modules and actions, click the **Module Rights** tab.



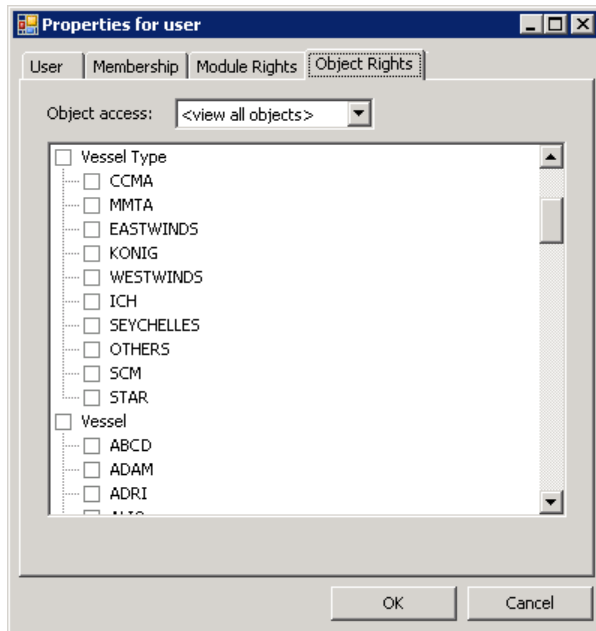
*Properties for User, Module Rights Tab*

- The Module Rights tab lists the modules and the actions associated with them. Select the user's rights for the module actions.
  - Each module name is preceded by a check box. To expand or collapse the list of actions for a module, double-click the module's check box.
  - When a module list is expanded, each action is preceded by a check box. To change the user's right to perform a task, click the check box. Each time you click, the right changes.
    - = Either the user does not have the right to perform the task, or the user is a member of a group with the right.
    - = Read-only: The user can retrieve information from files and view reports.
    - = Read/Write: The user has full ability to store and update information in the database.
    - = Denied: The group right to perform the task is overridden for this user.

**Note:** A user's rights include the individual user rights plus the rights from any groups in which the user is a member. If a user has different rights, either assigned individually or from groups, the highest access rights apply.

## Adding, Removing, or Overriding User Object Rights

7. To set up user rights to objects, click the **Object Rights** tab.



### *Properties for User, Object Rights Tab*


8. The Object Rights tab lists the objects in IMOS. Select the user's rights to the objects.
  - To filter the list of objects, select an object category from the menu:
    - View all objects
    - Company
    - Vessel Fleet
    - Vessel
    - Pool
  - Each object category is preceded by a check box. To expand or collapse the list of objects for a category, double-click the category's check box.
  - When an object category list is expanded, each object is preceded by a check box. To change the user's right to an object, click the check box. Each time you click, the right changes.
    - = Either the user does not have the right to the object, or the user is a member of a group with the right.
    - = Read-only: The user can retrieve information from files and view reports. General rights such as General Chartering have this option, but actions such as Create a Voyage Estimate do not.
    - = Read/Write: The user has full ability to store and update information in the database.
    - = Denied: The group right to perform the task is overridden for this user.

**Note:** A user's rights include the individual user rights plus the rights from any groups in which the user is a member. If a user has different rights, either assigned individually or from groups, the highest access rights apply.

9. When you finish creating the user, click **OK**.

## Editing a User or a Group

To edit a user or a group:

1. On the Security page, in the row for the user or group, click the [edit](#) link. The Properties window appears.
2. Click the tab on which you want to make a change.
3. Make any necessary changes to the [user information](#) or [group information](#).
  - To change the password for a user with IMOS Authentication, select the **Change password** check box and then complete the **Password** and **Confirm password** fields.
4. When you finish making changes, click **OK**.
5. To update the Security page, click  Refresh.

## Deleting a User or a Group

To delete a user or a group:

1. On the Security page, in the row for the user or group, click the [del](#) link.
2. A message asks if you are sure you want to delete the user or the group. Click **Yes**.



# Index

---

## A

- adding
  - group members, 12
  - module rights, 13, 17
  - object rights, 14, 18
- Address Book, 5
- administration
  - steps, 5
- Application file backups, 6
- authentication, 15

## B

- backup procedures, 6

## C

- cargo names, 5
- client backups, 6
- Configuration file backups, 6
- Confirm Password, 15
- creating
  - groups, 11
  - users, 15

## D

- Data Center tab, 9
- database backups, 6
- deleting
  - groups, 19
  - users, 19
- disaster contingency plan, 5

## E

- editing
  - groups, 19
  - users, 19
- Email, 15

## F

- Full name, 15

## G

- group members
  - adding, 12
  - removing, 12
- group membership, 16
- group name, 11
- groups, 8
  - creating, 11
  - deleting, 19
  - editing, 19

## I

- IMOS, 5
- IMOS Authentication, 15
- IMOS Help, 5
- IMOS Manual*, 5
- IMOS Security, 7, 9
- Initials, 15
- Integrated Maritime Operations System, 5
- Introduction, 5

## L

- logging on and off, 7
- Login page, 7

## M

- Membership tab
  - groups, 12
  - users, 16
- module rights
  - adding, 13, 17
  - overriding, 17
  - removing, 13, 17
- Module Rights tab
  - groups, 13
  - users, 17

## O

- object rights
  - adding, 14, 18
  - overriding, 18
  - removing, 14, 18
- Object Rights tab
  - groups, 14
  - users, 18
- off-site installation, 6
- overriding
  - module rights, 17
  - object rights, 18

## P

- Password
  - administrator, 7
  - users**, 15
- Properties for group, 11
- Properties for user, 15

## R

- removing
  - group members, 12
  - module rights, 13, 17
  - object rights, 14, 18
- rights, 8

## S

Security, 7, 9  
Security administrator  
  users, 15

## T

term lists, 5  
Terminal Server, 6

## U

User name  
  administrator, 7  
  users, 15

## User tab

  groups, 11  
  users, 15  
users, 8  
  creating, 15  
  deleting, 19  
  editing, 19

## V

vessels, 5

## W

Windows Authentication, 15