CommBox II

Instruction manual
1.22.1

KVH Industries Norway AS

Table of Contents

Table of Contents

Table of Contents

1 Contact information

KVH Industries Norway AS

Verftsbassenget 1
3188 Horten
Norway

Tel: +47 33 03 05 30
Fax: +47 33 03 05 31
Web: CommBox II
Web: KVH Industries Norway AS
Email: sales@emea.kvh.com

2 Active CommBox software modules

The CommBox software contains several different modules that can be activated according to your license / support plan. This activation / deactivation is done remotely by KVH support systems and cannot be change locally on each vessel / hub.

The module name will be in your left hand menu, but when accessing the module you will be directed to an info page stating: The "*modulename*" module is deactivated.

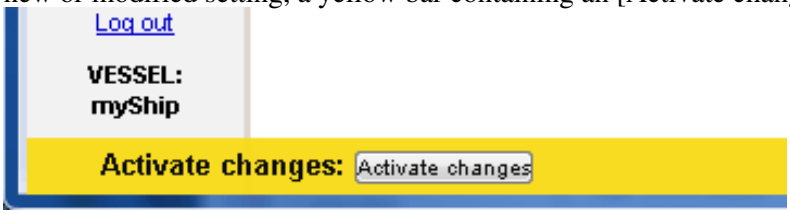
The modules are:

- QuickMail
- QuickFile
- QuickWeb (compression and filtering)
- QuickCrew

If one or more modules that you have got an active license or support plan for is disabled, please contact your support or your sales representative, see Support for contact details.

3 Important Note

Most configuration changes are not applied immediately once you press the [Save] button. In many cases, once you save a new or modified setting, a yellow bar containing an [Activate changes] button will appear at the bottom of the page.



Clicking this button will cause the CommBox to apply the new configuration and restart the relevant services.
You can 'accumulate' changes you do in a session and click [Activate changes] at the end instead of activating changes at every step.

4 How to read this manual

This is a how-to manual describing how to set-up and use different functions in CommBox. Each page in the CommBox configuration interface has one or more "Help" links that bring you directly to the relevant section of this manual.

A reference to a configuration page will be described using this syntax: *Menu->Sub menu*. Where *Menu* is an item in the menu on the left, and the *Sub-menu* is an item in the menu on the top.

Button's Names will be shown in square brackets [], i.e. [Save].

5 Browser compatibility and setup

The CommBox web interface is designed to be compatible with recent versions of the major browsers (Firefox, Chrome, Safari, Internet Explorer, Opera).

It is advisable to disable form auto-complete and password managers.

Firefox menu->Preferences...
: Under 'Security'. Uncheck the "Remember logins for sites".
: Under 'Privacy'. Under History, select the drop-down fitting your needs.

Chrome menu->Preferences...
: Under 'Show advanced settings...'. Uncheck "Offer to save your web passwords." and "Enable Autofill to fill out web forms in a single click".

Safari menu->Preferences...
: AutoFill tab, uncheck all the boxes.
: Passwords tab, uncheck "AutoFill user names and passwords".

Internet Explorer>menus Tools
: Internet Options->'Content' tab, 'AutoComplete' section->Settings. Uncheck the "Forms" and "User names and passwords on forms".

Opera menu->Preferences...
: Under 'Privacy & security'. Uncheck "Enable auto-filling of forms on webpages" and "Enable auto-filling of forms on webpages".

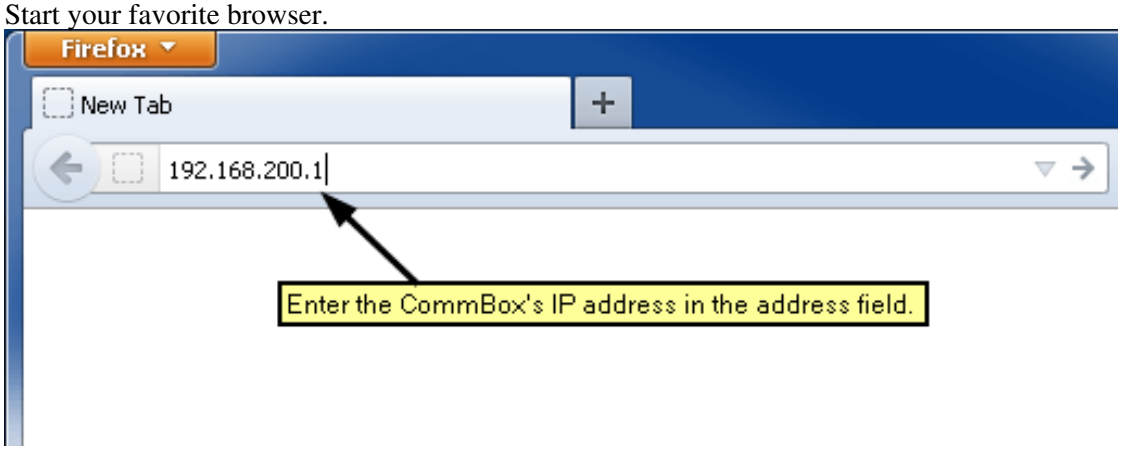
6 Connect to CommBox

The CommBox is configured via a Web Interface accessible from a normal Web Browser, ref.: Browser compatibility and setup

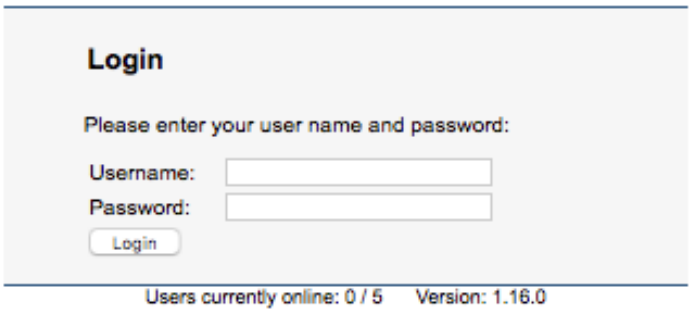
6.1 Login page

To get access you need to log in:

- Find the IP address or domain name, login name and password from the printed CommBox documentation. The default username and password are 'admin' and '1234'.
- Start your favorite browser.



- In the address field, type the IP address of the CommBox and press the "Enter" key.



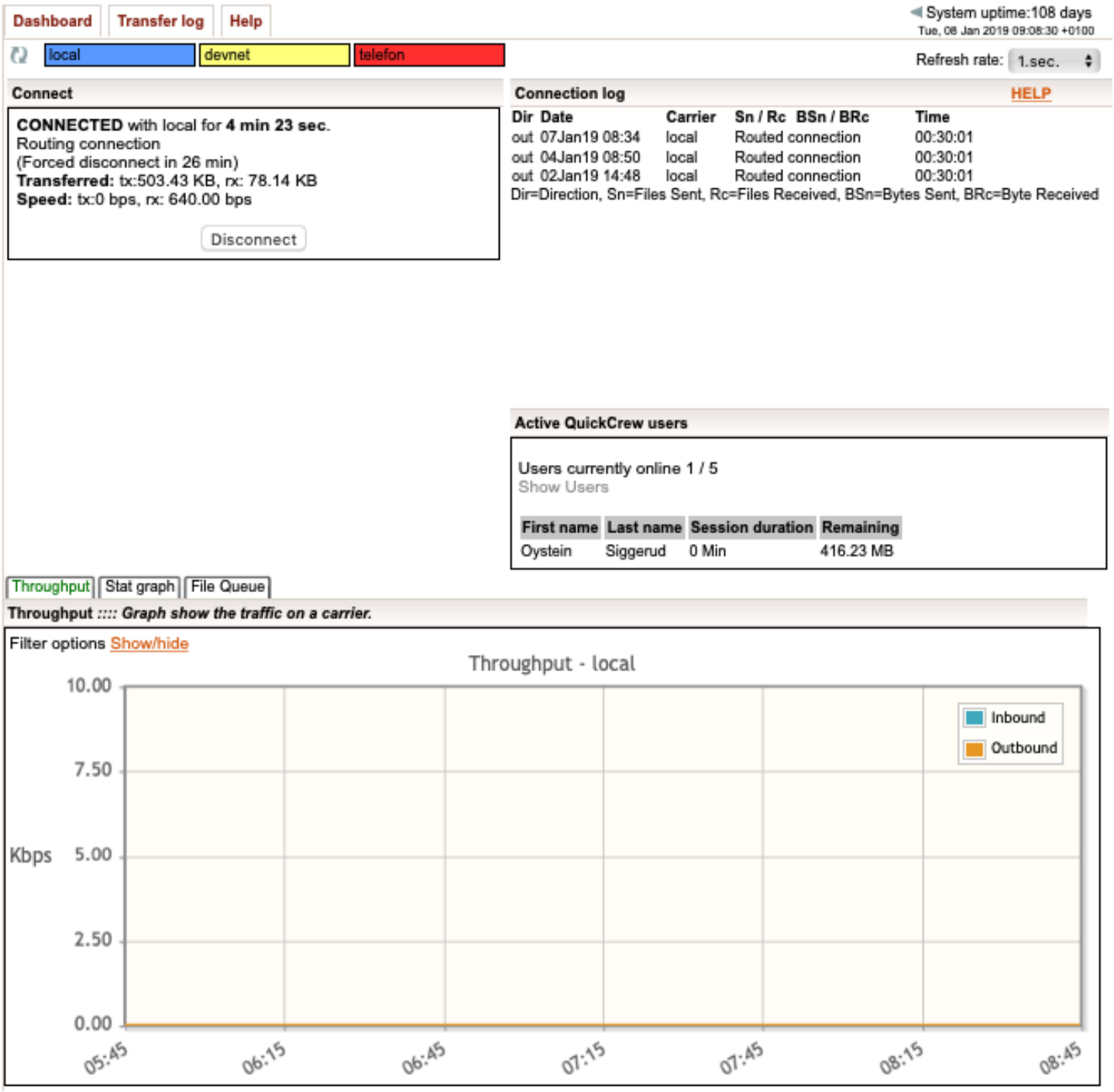
- You will be presented with the login page for the CommBox interface, enter user name and password to log in.
- After a successful login, you will get a alert box recommending to change the password.
    - ♦ Click OK to go to the User/Group to do so.
    - ♦ If you click Cancel, you will see the Dashboard, ref.: Dashboard operations (Classic Dashboard).

7 Dashboard operations (Classic Dashboard)

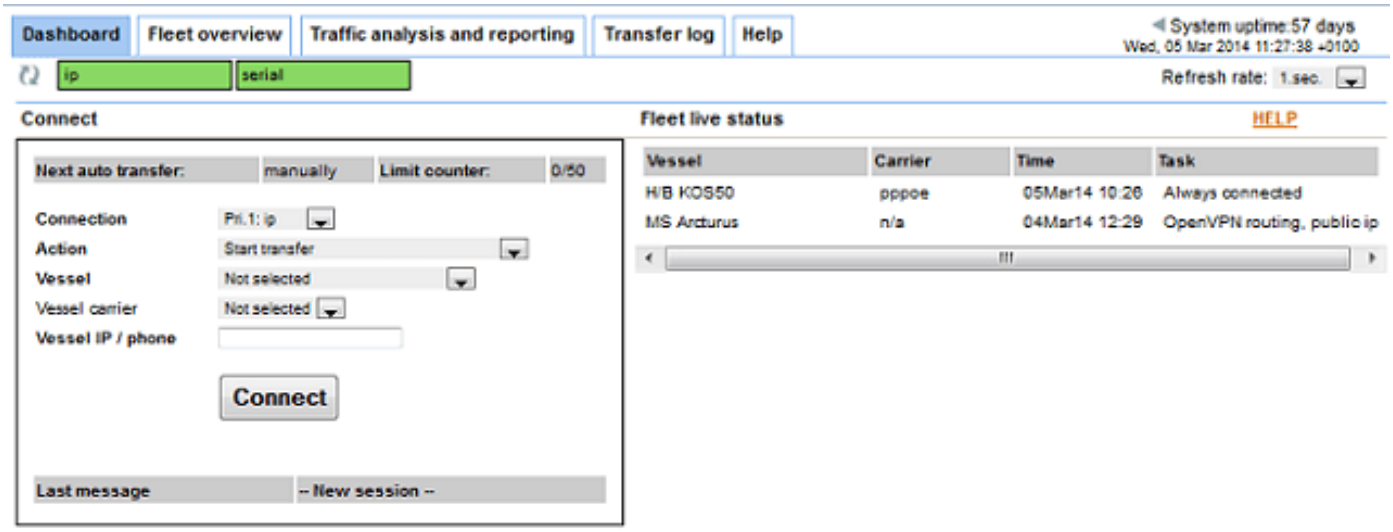
Note that there are two dashboard layouts: the 'Classic' and the 'Switch'. This chapter describes the classic look. See Dashboard operations (Switch Dashboard) for a description of the Switch look.

The dashboard gives you a quick overview of the state of the CommBox hardware and the available carriers. It also gives easy access to the most used functions in the day-to-day use.

Dashboard on vessel:

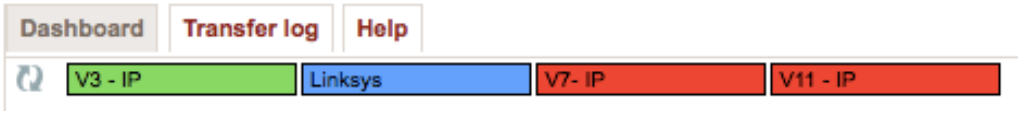


Dashboard on hub:



7.1 Carriers status

At the top of the panel is a representation of all the connection profiles configured in the CommBox. Color coding makes it easy to get a quick overview of which profile can be used for connections. If the name of a profile is followed by "(F)", it means that it has been forced to be active (see "Profile control" further down).



This panel is refreshed at regular intervals. To force a refresh, click on the icon on the left.

CommBox R8 does show status in its LCD, see Appendix: LED, LCD and Buttons

7.1.1 Color codes

RED
: CommBox has no connection to the communication device. Please check the power cables of the communication devices. A power cycle on the communication device may be required.

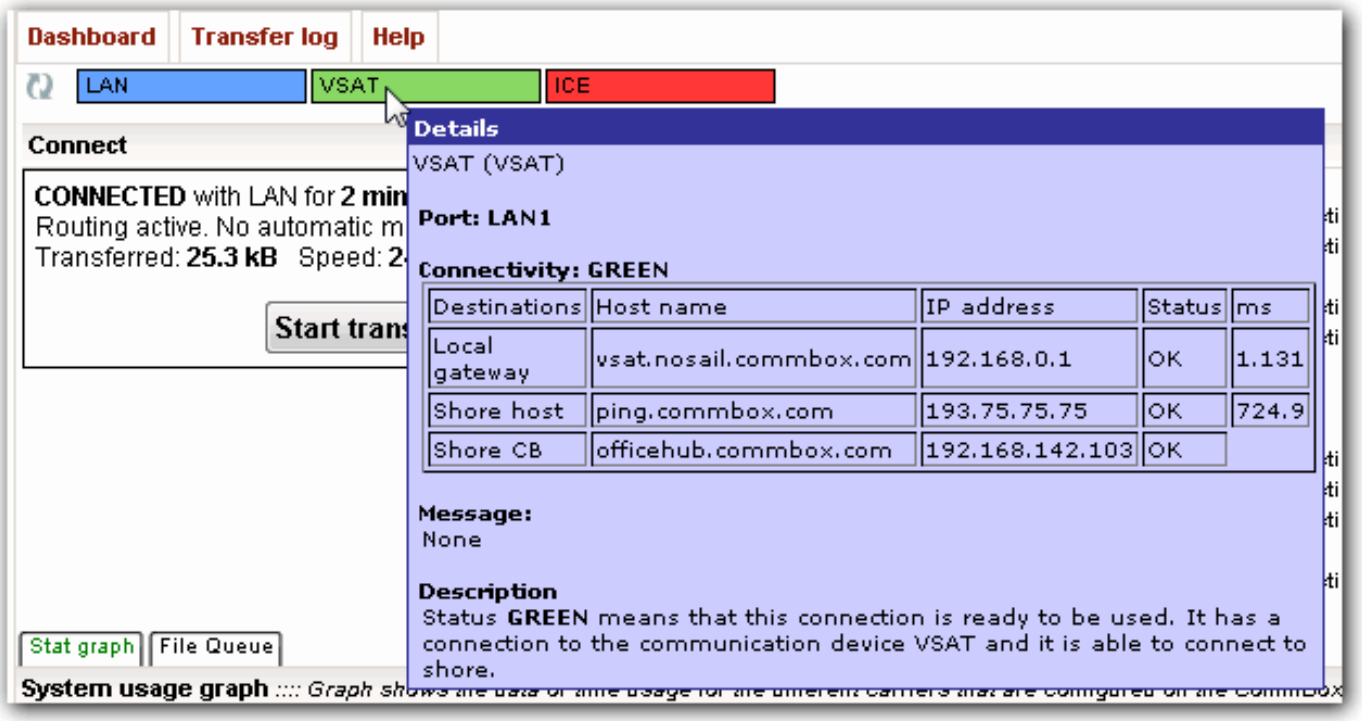
YELLOW
: Can mean one of two things:

1. This connection profile MAY be ready to be used. It has a connection to the communication device but the device has no connection to shore.
2. The connection profile has a usage limit which has been exceeded. To reset the profile usage, log in as administrator and click on the profile you wish to reset. In the pop-up window, click [Reset data usage].

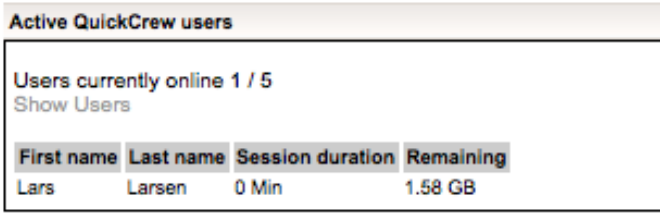
GREEN
: The connection profile is ready to be used. CommBox has a connection to the communication device and the device has connection to shore.

BLUE
: The connection profile is active and data is being sent/received right now.

By holding the mouse pointer over one of the connection profile monitor tabs, you will see the status description and more information.



7.1.2 Active QuickCrew users (vessel)



Just below the Connection log frame, number of "Users currently online" is given. To see who is logged in and info about the current active users hit the link "Show Users".

The information about "Users currently online" is only available if the QuickCrew module is running and maximum number of concurrent connection is configured.

7.1.3 Content of the mouse-over popup

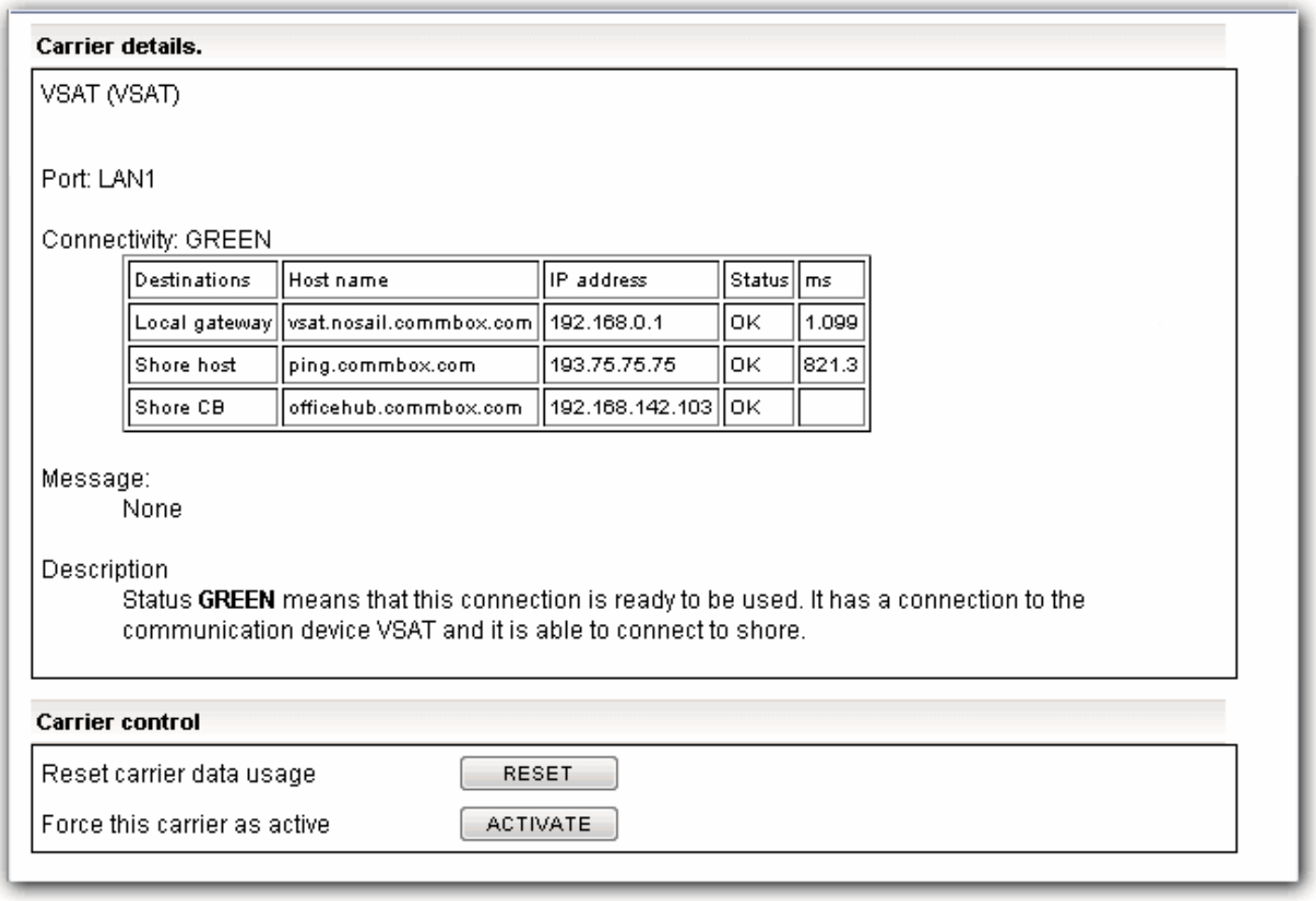
The table summarizes which hosts the CommBox tries to reach in order to establish a connection, the status of the connection, and the time in millisecond that it took to reach the host.

The text usually gives an explanation of why the profile is not green. "switch to green" is a common message meaning that the signal quality is switching between poor and good. The signal quality of a profile must be above the Signal threshold for a chosen time period (see "Signal threshold time" in Add / Edit connection profile).

If the Signal threshold time is set lower than 60 seconds, the profile will switch to green immediately when the signal is satisfying the signal threshold. It is recommended to set Signal threshold time to a whole minute.

7.1.4 Profile control

If you click on the tab, a pop-up window will open. This window will contain the same information as the mouse-over pop-up.



If you are logged on as administrator on a CommBox Vessel, it also will contain a small control panel.

RESET
: Resets the usage counter so that, if the profile has reached its usage limit, it can be used again.

ACTIVATE
: Force the profile to become active.
This is useful if, for example, there is an urgent need for fast transfer speeds and you want to activate a profile that does not allow crew users. Once you press the button, the pop-up window will close.
Profiles that have been forced active will be marked with "(F)" in the carrier status panel.

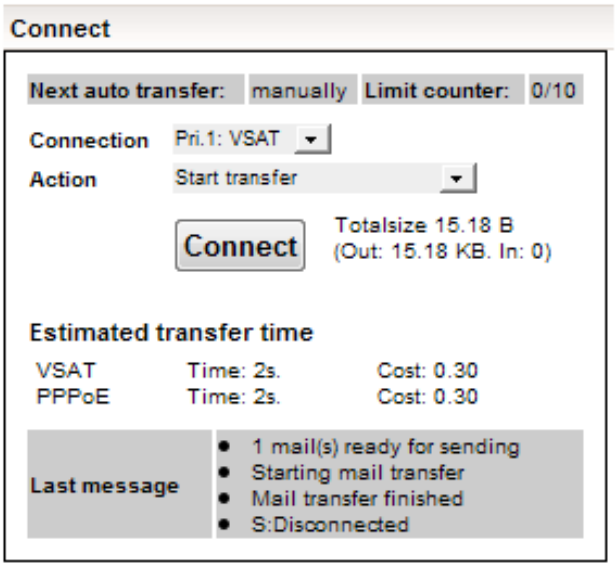
DEACTIVATE
: You will see this option if the carrier has been forced to become active.
Click on the button to make the carrier behave as normal. Once you press the button, the pop-up window will close.

7.1.5 Why are there no carriers listed?

The most likely reason is that there are no connection profiles configured or that all of them have been deactivated.
See the Connections chapter to learn how to configure connections.

7.2 Connection operations (vessel / hub)

From the 'Connect' panel of the Dashboard you can see some connection information and you can choose which type of connection you want to make.



If there is an "Always connected" connection active, the panel will have only a [Start transfer] and a [Disconnect].

On the top of the panel is an information line:

Next auto transfer
: This field will either show "*manually*", or the time remaining before the next scheduled transfer and the profile that will be used. The time and/or frequency of scheduled transfers are configured in each Connection profile.

Limit counter
: If a limit on the number on daily manual connections has been set (see Restrictions), here will be displayed a counter of today's connections vs. the maximum number allowed.

The controls in the panel allow you to start a connection using one of the configured carriers:

Connection
: This pull-down allows you to select which Connection profile to use for the connection.

Action
: Choose the action to be performed on connection:

Internet - Intranet connection
: Sets up a routing connection between the vessel and the shore CommBoxes. You must also set the length of the connection. This is done in the Connection time pull-down, that will be displayed after "Internet - Intranet connection" has been selected.

Start transfer
: The CommBox will transfer all queued mails/files to and from the off-site CommBox

Get remote queue
: CommBox will fetch a list describing the mails/files queue that is waiting to be transferred from the off-site CommBox. This list can be manipulated to delete, put on hold and change priority of items on the remote transfer queue (files in the queue with low priority number will be transferred before files with high priority number during the same transfer).

There are two more choices on the hub, see Connection operations ... (hub)

It is possible to hide some of the available actions from "Config->Misc Display" (see Misc).

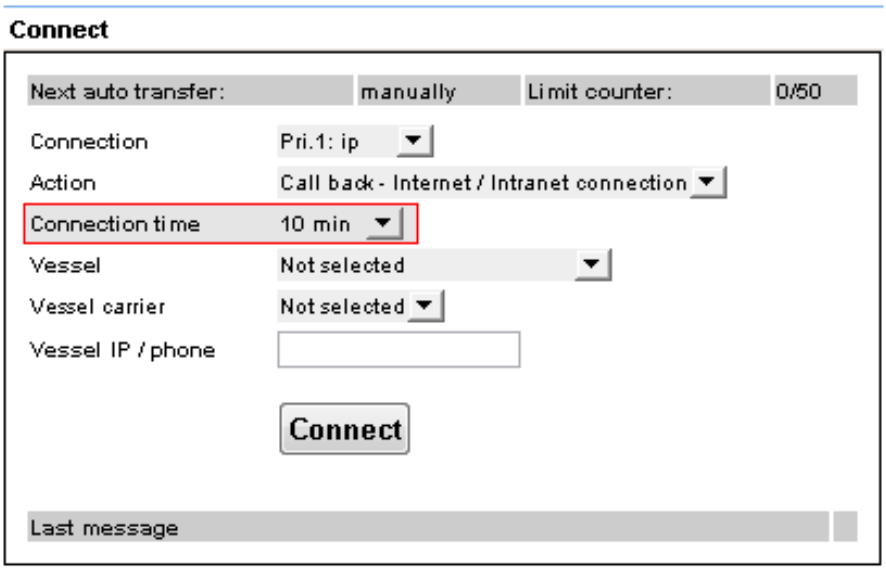
At the bottom, some more information:

Estimated transfer time
: The 'Estimate transfer time' line shows an estimate of how long it will take to transfer the outgoing queue and, if a cost profile is linked to the selected carrier (see Cost (vessel)), an estimation of the cost of the transfer.

Last message
: This field displays the last message(s) from the Connection system. It will be of help when troubleshooting connection failures and will also give notification if a connection attempt stops, for instance because the configured limit of daily connections has been reached.

7.3 Connection operations ... (hub)

In addition to the actions available on the vessel, the hub has the ability to instruct vessels to initiate calls. This type of action is called “callback”. The reason for initiating a callback is cost placement: by making the vessel call the hub, the cost of the data transmission will be on the vessel side. (The cost of sending to the vessel the “initiate callback” command will be on the hub side.)



Action
: Callback – Start transfer.
  : This action will force the selected vessel to initiate a transfer.
: Callback – Start Internet / Intranet connection.
  : The vessel will set up a routed connection to the hub. Hub personnel will then be able to connect to the vessel through the tunnel between vessel and hub.

Connection time
: This pull-down will appear if you choose “Internet - Intranet connection” in the action pull-down.
It defines how long the connection should last.

The content of this pull-down is configured in "Config->Misc Display" (see Misc).

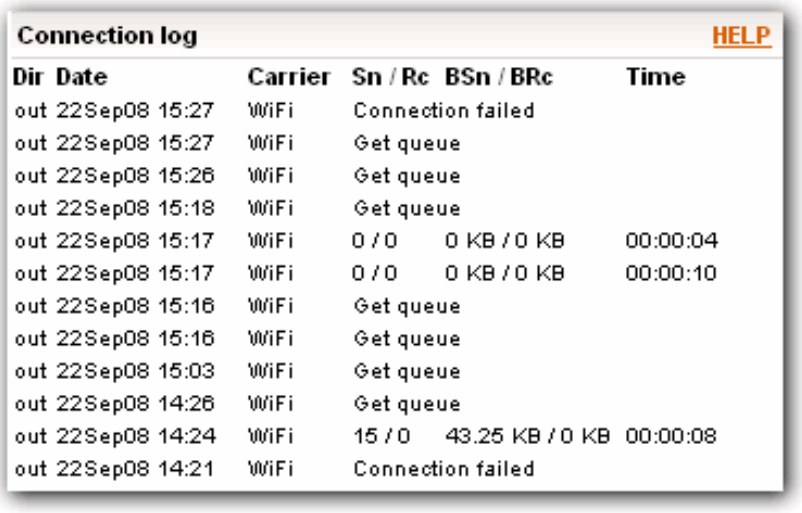
Vessel
: In this drop down you select which vessel you want to send the callback command to.

Vessel carrier
: This drop down lists all the carriers available for incoming calls on the selected vessel. They are the carriers that are not disabled and either:
  ◊ Are dial-up, have a phone number for incoming calls ("Terminal phone number" field in the connection profile), and are enabled for incoming calls ("Receive" field in the connection profile).
  ◊ Are IP-based carriers that have been used at least once from the vessel, so that their IP address is known.

Vessel IP / phone
: This field is populated based on the value in “vessel carrier” and can contain a phone number or an IP address. If no IP address or phone number is set up, the field must be filled out manually.

7.4 Connection log (vessel)

The connection log gives information about the connections that have been performed or attempted.



Connection log HELP

Dir	Date	Carrier	Sn / Rc	BSn / BRc	Time
out	22Sep08 15:27	WiFi	Connection failed		
out	22Sep08 15:27	WiFi	Get queue		
out	22Sep08 15:26	WiFi	Get queue		
out	22Sep08 15:18	WiFi	Get queue		
out	22Sep08 15:17	WiFi	0 / 0	0 KB / 0 KB	00:00:04
out	22Sep08 15:17	WiFi	0 / 0	0 KB / 0 KB	00:00:10
out	22Sep08 15:16	WiFi	Get queue		
out	22Sep08 15:16	WiFi	Get queue		
out	22Sep08 15:03	WiFi	Get queue		
out	22Sep08 14:26	WiFi	Get queue		
out	22Sep08 14:24	WiFi	15 / 0	43.25 KB / 0 KB	00:00:08
out	22Sep08 14:21	WiFi	Connection failed		

Column description:

Dir
: Direction, 'in' or 'out'.

Carrier
: The carrier used for the connection.

Sn
: Number of sent files.

Rc
: Number of received files.

BSn
: Bytes sent.

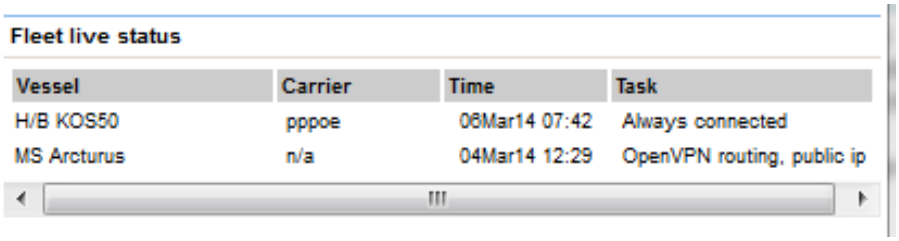
BRc
: Bytes received.

Time
: Time connected, hh:mm:ss.

If a connection is not related to the transfer of files from the queue, or if an attempt to connect fails, there will be a descriptive message instead of the Sn, Rc, BSn, and BRc data.

7.5 Fleet live status (hub)

This section shows, in live, each vessel connected and the task performed by the vessel.



Fleet live status

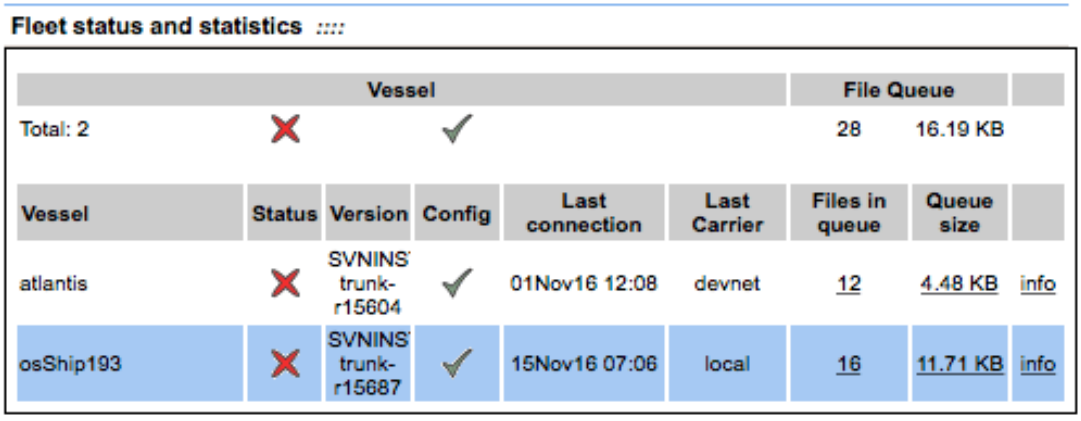
Vessel	Carrier	Time	Task
H/B KOS50	pppoe	06Mar14 07:42	Always connected
MS Arcturus	n/a	04Mar14 12:29	OpenVPN routing, public ip

7.6 Fleet overview (hub)

This page gives an overview of vessels connected to the hub.

7.6.1 Fleet status and statistics

This section shows some useful information about each vessel connected.



Some more detailed information is shown in a popup frame when the mouse cursor is hovering the "info" in the right column.

It is possible to get the Transfer Queue for one vessel by selecting either the number of files in queue or queue size. For more details about the transfer queue see File Queue.

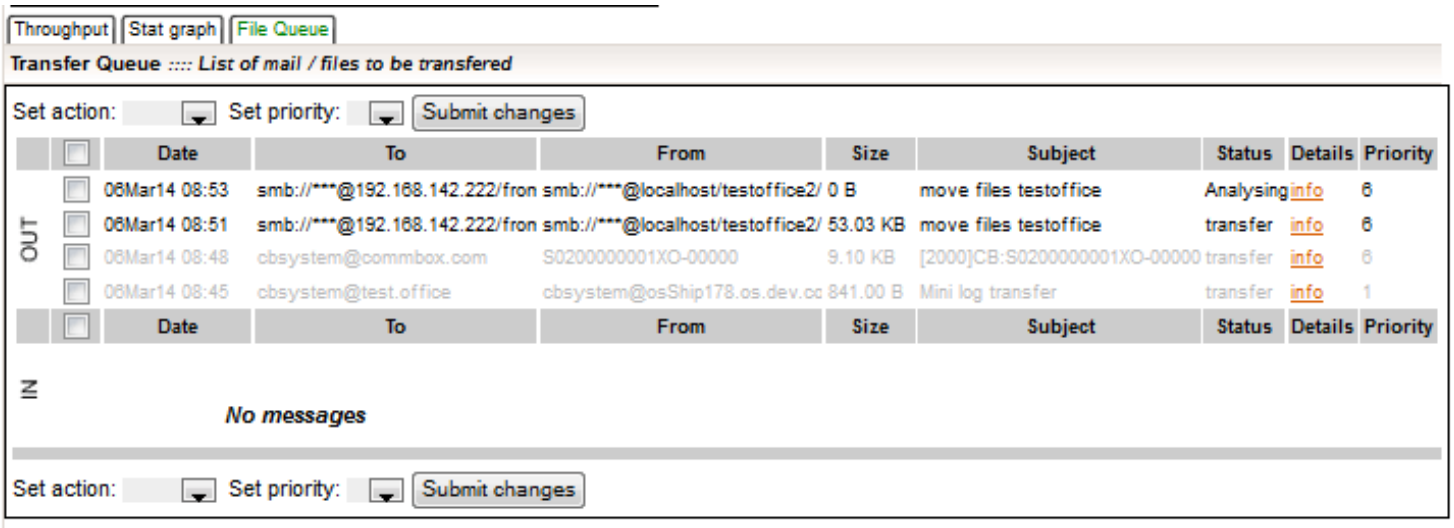
7.7 File / Transfer Queue

The main function of the transfer queue is to give the users the possibility of managing the transfer of each file.

To display the queue on vessel, click on the "File Queue" tab below the 'Connect' panel. On a hub, click on the link given by the number of 'Files in queue'/'Queue size' for the vessel in question on the 'Fleet overview' page.

It is possible to see the incoming queue, just select the 'Get remote queue' as 'Action' in the Connection panel and do Connect. The files/messages headers from your vessel/hub will bee transmitted and shown in the IN file queue section.

You will see information about sender, receiver, subject,date, size, and more. The messages/files in queue will be displayed in the 'File Queue' panel.



In the above example you can see some messages/files that are waiting for transmission. For each entry in the queue, you can now change the priority or perform an action (see below). When this is done, click [Submit changes].

To actually transfer see Transfer mails / files.

7.7.1 Queue actions

Available actions:

Ready
: Default value. Transfer the file unless restrictions prohibit it.

Hold
: Leave the file in the queue.

Force
: Force the transfer of a file blocked by a restriction profile.
(Restriction profiles are linked to the Connection profile.)

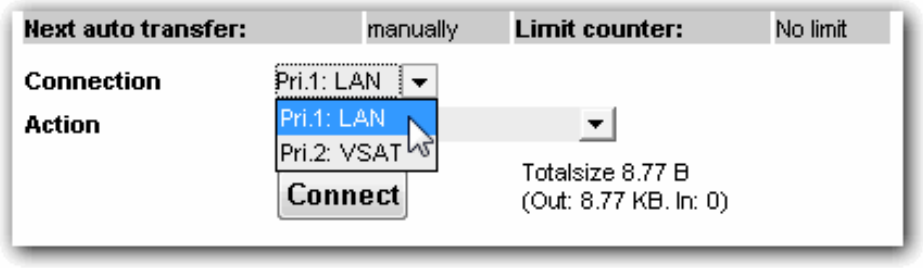
Reject
: The “Reject” action will prompt for a reason for the rejection. This message will be sent to the sender of the rejected mail.

Delete
: Delete the message from the queue without transferring it or sending a notification to the sender.

Note that some files may be protected and it will not be possible to hold or delete them

7.7.2 Transfer mails / files

To perform a file exchange to and from the remote CommBox, first choose a Connection profile from the 'Connection' pull-down in the Connect panel.



The "Estimated transfer time" section displays estimated values for the duration and, if a cost profile is active, the cost of the transfer. This makes it easier to choose the most cost effective carrier.

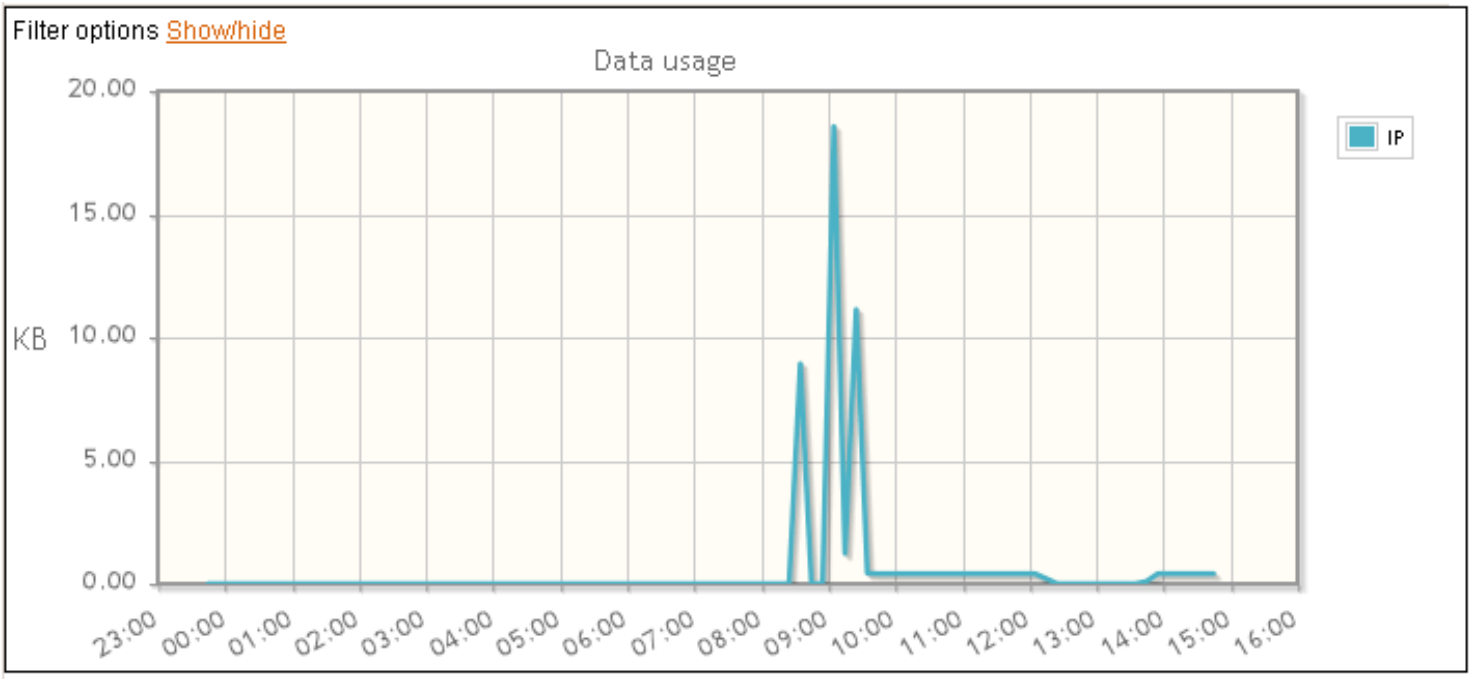
To initiate the transfer, choose "Start transfer" from the Action pull-down and click [Connect].

7.8 Statistics graphs (vessel)

On the vessel dashboard, both Switch and Classic view, statistics will be presented in the usage graph. In Switch mode, hit [Submit] to get it displayed. It is possible to choose among two types of graphs, data usage and time usage. The vessel statistics graph can display traffic statistics for the last 2 months, the filters available are date range and the current connection profiles.

The usage graph will display time of day on the x-axis and bytes transferred on the y-axis.

The time usage graph will display the time of day on the x-axis and the transfer time on the y-axis.



You can access the filters menu by clicking on the "*Show/Hide*" link above the graph. From the filters menu you can select the carriers for which to display a graph. You can also select the time period for which you wish to display data by clicking the calendar icons next to the start / end fields.

7.9 Traffic analysis and reporting (hub)

Several types of reports are available, each report is for a selectable time period, some reports allow also selecting vessel(s) and carrier(s).

When you are viewing a report you can change report type by selecting from the "Report type" drop-down menu.

The hub can store traffic data for 3, 6, 9, or 12 months (configurable, see Log settings). KVH does not recommend storing data for more than 6 months, due to space limitation.

It is possible to save the selection of vessels and carriers for a report. To do so, enter a name for the report in the "Save this search as:" box and click [Save]. You can re-run previously saved reports by selecting one from the "Saved searches" drop down.

7.9.1 Usage graph with Timeline

Line plot of the data usage per vessel and terminal over time.

7.9.2 Total usage graph

Graphical view of the total usage per vessel and terminal.

7.9.3 Transfer Report

Download e-mail and file transfers as CSV file.

The report can be downloaded as a file in CSV format.

7.9.4 Sum Transfer Report

Graphical view of the total bytes used per vessel and terminal for e-mail, files and other CommBox related transfers.

7.9.5 Roaming User Report

Download CSV report containing the QuickCrew usage (web traffic and e-mail transfers) per crew user.

The report can be downloaded as a file in CSV format.

7.9.6 Sum Roaming User Report

Total data used per Crew user and vessel.

7.9.7 Data usage per client IP for each IP port

This is an interactive report. You are first presented with a list of the vessels for which traffic data exist in the time span selected.

You can break-down the traffic data details, from less (by vessel), down to most (port number).

To change the time span of the report, change the dates and then click [Update], all the open rows will be closed when updating.

System -
Vessel name and IP address.
- Terminal
Terminal through which the traffic went.
- - LAN
Name, description and IP address of the LAN that generated the traffic.
- - - Client
IP address of the client on board generating traffic.
- - - - Egress
The name of the CommBox interface facing the outside world.
- - - - Port
The out port number.

In -
- external
The amount of traffic received from the external world.
- proxy
The amount of traffic received from the internal CommBox proxy.

Out -
- external
The amount of traffic sent to the external world.
- proxy
The amount of traffic sent to the internal CommBox proxy.

Total -
- external
The total amount of traffic exchanged with the external world.
- proxy
The total amount of traffic exchanged with the internal CommBox proxy.

7.9.8 QuickWeb log

This log shows the Web activity on each vessel. The report table shows the amount of data that went through the QuickWeb system (this is not limited to Web surfing and includes all traffic that goes directly from a client to the Internet without passing from the CommBox file exchange system e.g. instant messaging, software update requests etc.).

The report details the amount of bytes served to clients, the number of requests served to clients, and the number of requests that were denied, ether by defined filter profiles (see Filter profiles) or blocked ip addresses. The amount of bytes and the number of responses are further split according to whether the data was actually fetched live from the Internet or was served from the local cache.

Vessel
The vessel name and ip-address
- Network Interface
The interface for the traffic
- - Client IP
The client ip-address
- - - Host Domain
The domains requested from the client

Bytes -
Number of bytes transferred
- Total
Bytes in total
- Cache
Bytes returned from cache
- Live
Bytes returned live from the Internet

Responses -
Number of requests
- Total
Requests in total
- Cache
Requests returned from cache
- Live
Requests returned live from the Internet

Requests Denied
Number of requests that was rejected

The report shows only the amount of bytes that were received from the Internet, it is not possible to show the amount of bytes that were transferred from the CommBox to the Internet.

The first level of the reports shows data grouped per vessel, clicking on a vessel's line shows data grouped by the local network from where the traffic was requested, clicking on a Network Interface will show data grouped by the requesting client's IP address, clicking on a client will finally show data grouped by the domain from where the traffic was received.

The [Download] button allows you to download a CSV version of the report detailed at the domain level (regardless of which level is opened in the graphical interface).

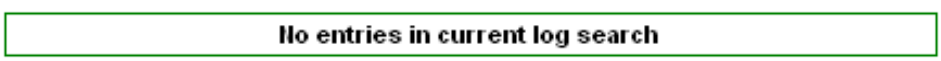
To change the time span of the report, change the dates and then click [Update].

7.10 Transfer log

Transfer log displays a list of all transfer activity for different time periods. By default it shows transfers from today, you can also choose to display transfers for:

- Last 7 Days
- Last 30 Days
- Last 50 transfers
- This week
- This month

If there are no entries in the log for the selected time period, you will see this message:



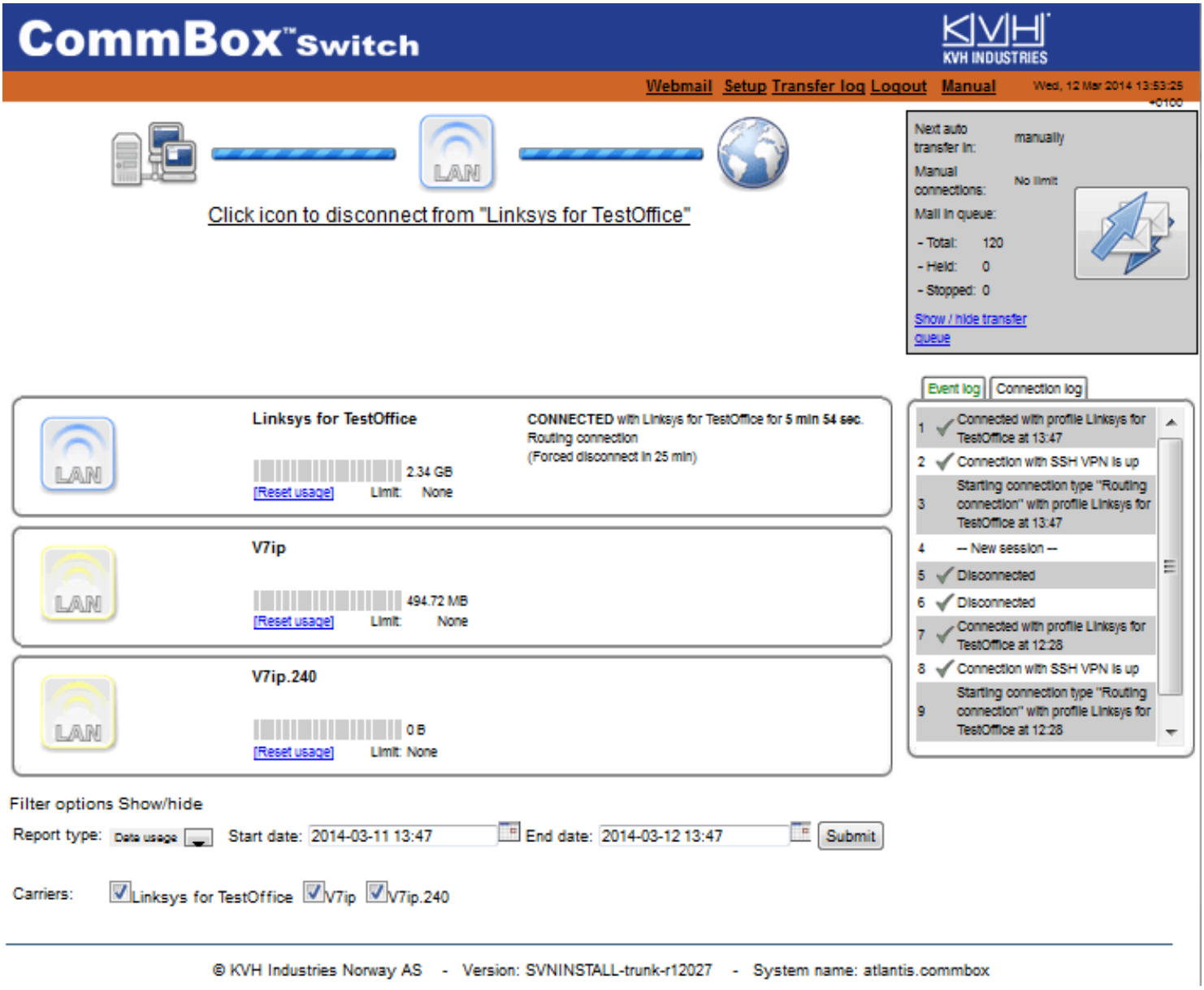
8 Dashboard operations (Switch Dashboard)

The Switch dashboard is an alternative dashboard optimized for using the CommBox without a hub. In this setup the CommBox acts like an IP routing switch, hence the name.

Note that the Switch dashboard can be used also with a hub setup.

You can enable the Switch dashboard from the "Config->Misc Display".

The first part of the Switch dashboard contains all controls for connecting, transferring files and seeing carrier status information.



The upper left part of the screens shows whether or not there is an active connection. The active connection is shown here by the icon between the local network symbol and the Internet symbol.

The lower left part of the screen shows the carriers' status. The color of the icons indicates the connection status as in the classic dashboard. For carriers supporting it, you will also be able to see the signal strength represented by a vertical bar. The horizontal bar to the right of the signal strength bar shows (if configured) the usage in percent of max usage for the current time period. Depending on the configuration (see Connections), either bytes transferred or time used will be used as units for this bar. On the right side of the status bars of the active connection, are displayed information and statistics.

In systems set up to connect and transfer mail through CommBox hub, the upper right part of the screen (with the gray background) shows information about automatic transfers and the file queues. By clicking Show/hide transfer queue, the queues will pop up and look and function as described in File Queue for the classic dashboard. The icon with an arrow over envelopes is used for starting file transfers immediately when connected with an “always connected” profile.

The lower right part of the screen shows either an event log or the connection log, selectable by two tabs at the top. The event log shows messages from the CommBox connection system describing its activity. The connection log is described in the chapter Connection log (vessel).

A series of links above the gray information box at the upper right allows you to reach the other parts of the CommBox interface (these parts do not differ between classic and Switch look).

Below you can have the Usage Graph (Data-/Time-usage) for the configured carriers, hit [Submit] to get it displayed. The Usage Graph is described in the chapter Statistics graphs (vessel).

9 System / Administrator operations

9.1 Backup

It is important that you back up your CommBox configuration so that you can recover:

- If something happens to the CommBox, for example hard disk failure.
- If you reconfigure the CommBox and make mistakes that results in CommBox malfunction.

CommBox backup will only backup the configuration of your CommBox, not the actual operating system and software. In case of disk crash, the damaged disk must be replaced with a new formatted and installed disk from KVH. Next you must restore your backup to this new disk.

9.1.1 Backup strategy (when to create a backup)

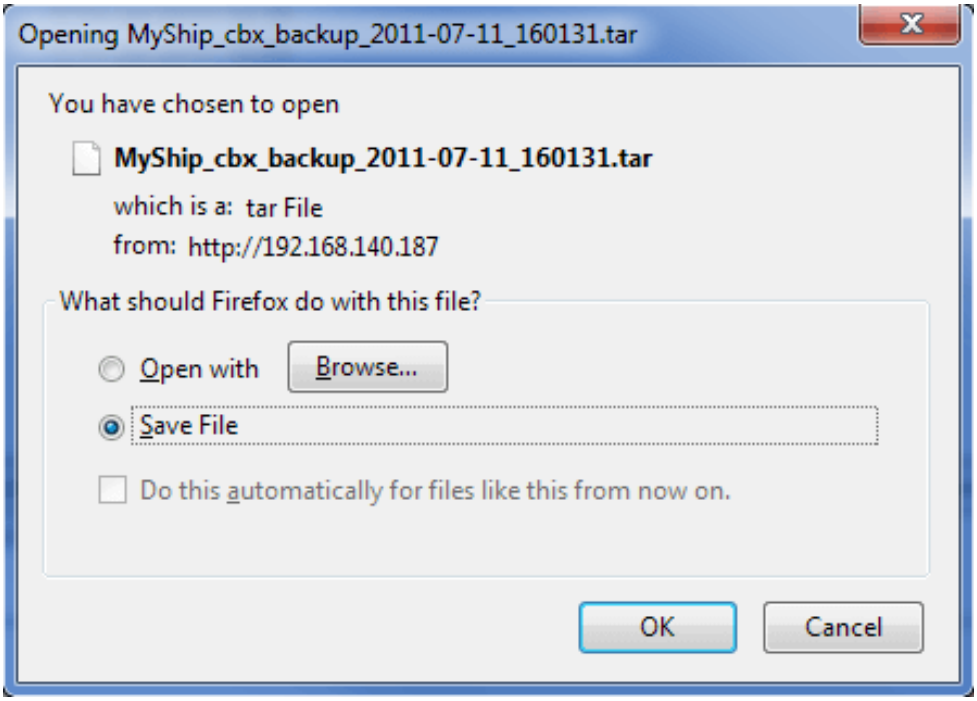
When you have finished the configuration of a new CommBox and everything is working nicely you must create a backup of the configured system. This backup must be kept safe at all times.

After you have reconfigured a working system and tested that everything works as intended you must create a backup. In this way you always have the latest settings available. And if you mess up the system during a reconfiguration, you can fall back on the last good configuration. CommBox will automatically save the last ten configurations that are activated.

9.1.2 Create backup

To create the backup is pretty straightforward. Go to the System menu, and in the top section you will find a button that says [Create backup]. Click on that one.

Next you will be prompted and asked if you want to open or save the file, do [Save]. The exact appearance of the 'Save' popup depends on the browser in use.



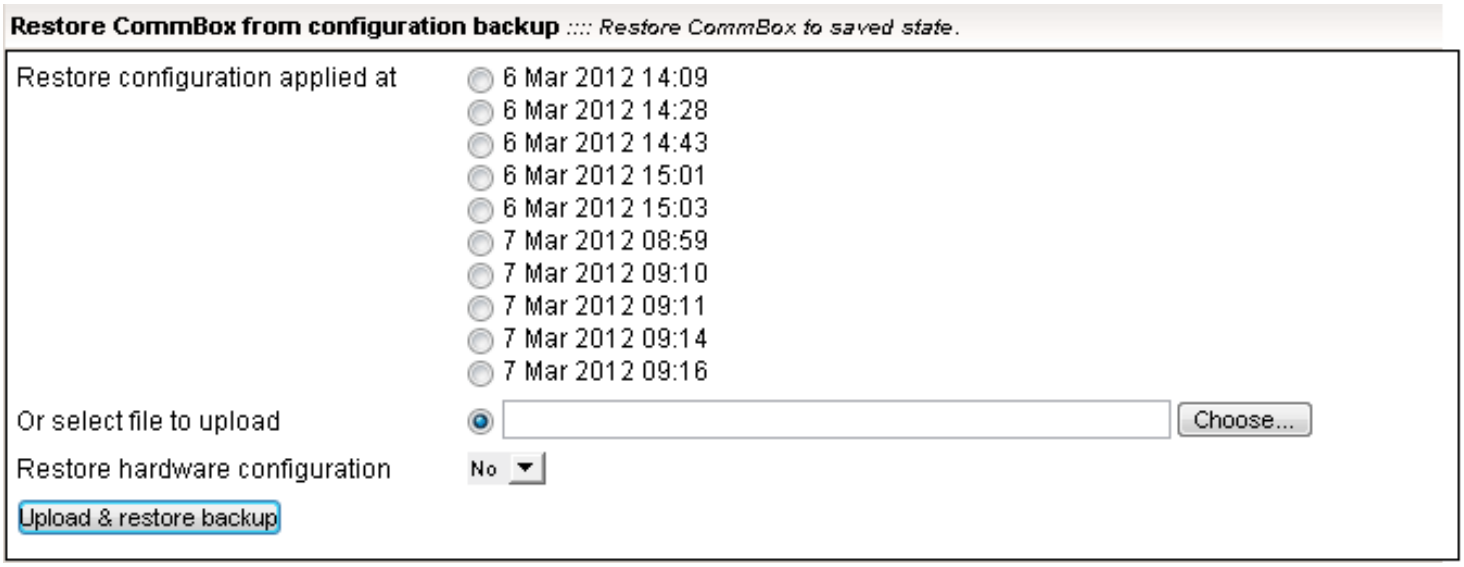
Next you must choose where you want to save the backup file. The file name is in the form of "<System name>_<host name>_backup_<YYYY-MM-DD>_<random number>.tar", for example: "MyShip_cbx_backup_2011-07-11_154241.tar". You may want to change this to a name more descriptive of the particular configuration saved.

You should use a designated directory for your CommBox backups. This place should be used each time you create a new backup. This directory should also be copied to a CD or to a third computer. Just so you have a backup of the backup.

9.1.3 Restore backup

There are two ways of restoring a backup of the configuration on the CommBox. The first is restoring from a file you have saved on your computer. The second way is to select from the ten last configurations stored on the CommBox.

Go to the System menu, and then find the “Restore CommBox from configuration backup” panel.

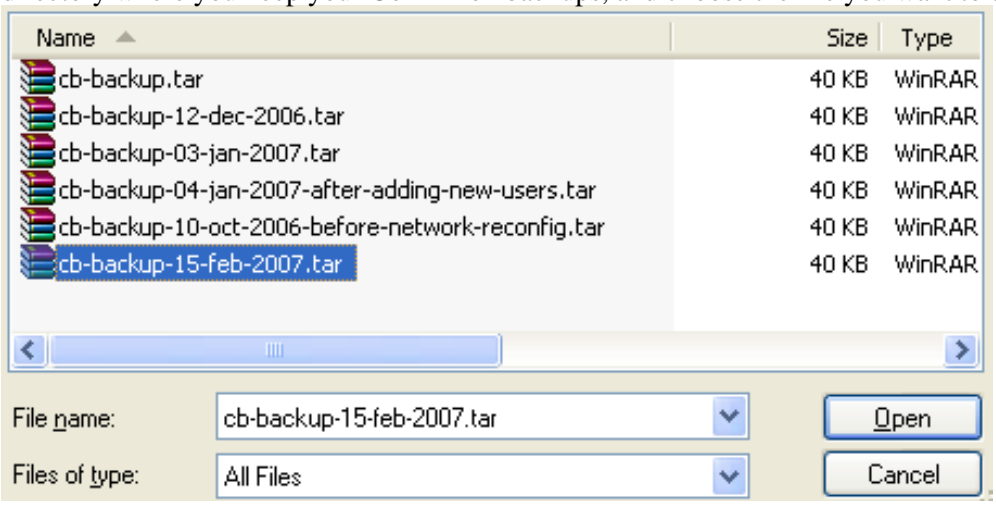


Restore configuration applied at

The CommBox makes a configuration backup each time you activate changes done to the system, only the last ten such backups are kept. To use one of these backups, select the desired “restore point” and click [Upload and restore backup].

Select file to upload

First click [Choose File] (the name and location of this button depends on the browser used). Navigate to the directory where you keep your CommBox backups, and choose the file you want to use for the restore.



When the file is selected, click [Upload and restore backup], and CommBox will start to upload the file from your computer. When the file is uploaded, the restore starts automatically. The system will display the configured IP addresses as a reminder in case they have changed with the new configuration.

Restore hardware configuration

You can choose whether to restore the hardware profile or not. Usually you will need to NOT restore the hardware profile if the backup file had been taken from another CommBox (for example if a standard configuration is used on many CommBoxes).

9.1.4 Send configuration to hub

The CommBox configuration will be sent to the hub as an email attachment.

9.1.5 Send configuration archive to vessel (hub)

This function provides the user with a tool to upgrade the configuration on vessels from the hub. It will take a CommBox configuration file archive and send it to a vessel by mail. When the email arrives on the vessel, the new configuration is applied automatically.

To generate a configuration to use in this functionality, you need to use a third CommBox on which to setup the configuration. When you are satisfied with the new configuration, save it to your computer using the backup functionality (see Create backup). If you have an archive with the current configuration of the vessel CommBox that you want to change, this would be a great place to start.

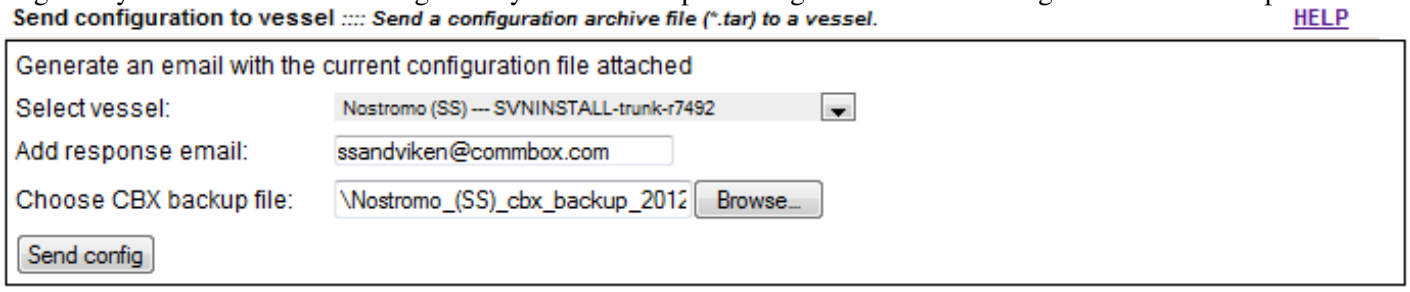
The following describes the steps to take:

1. Log in to the CommBox where you want to perform the configuration and go to "System->Backup"
2. Load to your "config CommBox" the base config archive if you have it.
3. You can now perform the reconfiguring of the CommBox.
4. When all changes are done, click [Create backup] found in the first section of the backup page. This operation will create a CommBox archive file that you must save on your computer.

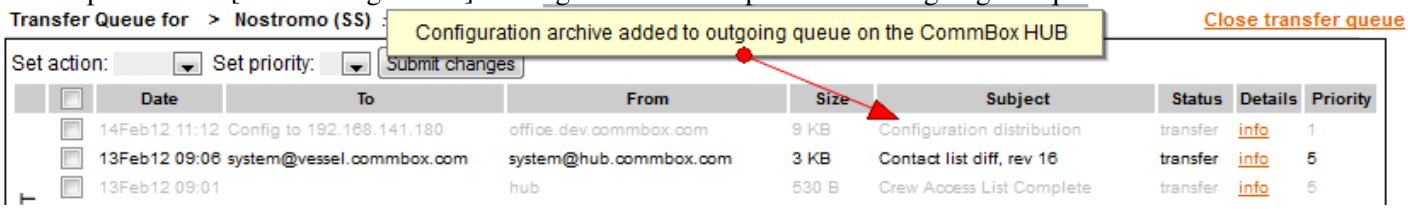
The Configuration archive you just created can be uploaded to the vessel from your hub.

Here is how:

1. Log in to your CommBox hub and go to "System->Backup". Then go to the "Send configuration to vessel" panel



2. In the "Select vessel" drop down, select the vessel to which you want to send the configuration archive.
3. Add a response email address. The CommBox system on the vessel will send a status email when the system reconfiguration is done.
4. Choose the configuration archive that you want to send to the selected vessel and use in the reconfiguration.
5. Last step is to click [Send configuration]. Configuration is now put into the outgoing file queue.



6. The reconfiguration will be done the next time the vessel checks the hub for email.

9.2 Reboot / Shutdown

9.2.1 Reboot

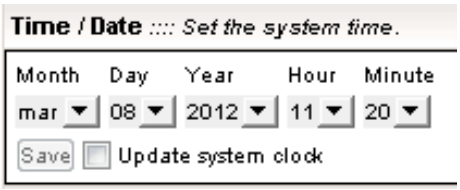
This command will reboot your CommBox system. First tick off the check box, then click [Reboot]. This operation will take approximately five minutes.

9.2.2 Shutdown

This command will shut down your CommBox system. First tick off the check box, then click [Shutdown]. This will initiate the shutdown procedure, you can turn off the power switch on the front panel of the CommBox after approximately five minutes.

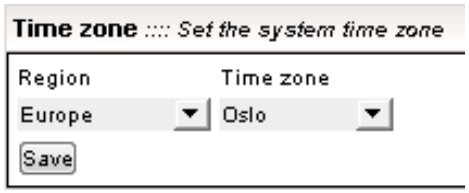
9.3 Set date

9.3.1 Set system time



Set the system time by choosing the values from the pull-downs. When finished, tick the check box. This will activate the [Save] button. Click [Save] to change the system time.

9.3.2 Set time zone



Setting the time zone will make the CommBox system use the time zone in the specified location. The current time will be updated accordingly. The time zone affects how daylight saving times are handled.

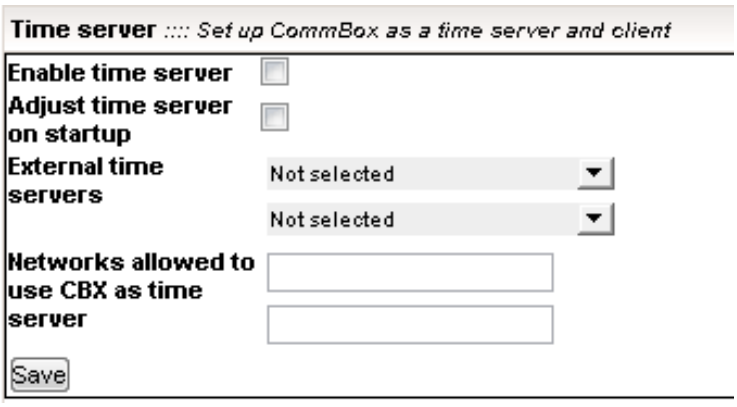
You will have to reboot the system for the change in time zone to take effect.

9.3.3 Time server

This is a two way functionality where CommBox can act both as client and server.

Client
: CommBox can be set up to synchronize its system time against an external time server

Server
: CommBox can be set up to let other machines use CommBox as a time server, and synchronize their system time against it.



Enable time server

Enables the time client and server functionality.

Adjust time server on start up

After each reboot / startup, the time will be synchronized with the time server.

External time servers

Add external servers to synchronize against. Any host configured in "Config->Hosts" will be available for selection (see Hosts). (*)

Networks allowed to use CBX as time server

List of networks that can connect to the CommBox time server. (*)

(*) to select more servers or enter more networks, use the available fields on the form and save: a new field will be added.

9.4 Restore to factory defaults

This command will delete all CommBox configurations and replace them with the default KVH setup. If you are using a pre-configured CommBox, "Factory default" **will not** restore to this state. To go back to the pre-configured state, please go to the "System" menu, and choose to restore from a backup file.

It is also a hard way to run the restore to factory default, see Appendix: LED, LCD and Buttons.

This operation will delete the content of shared directories and all your configuration, connections, users, etc.

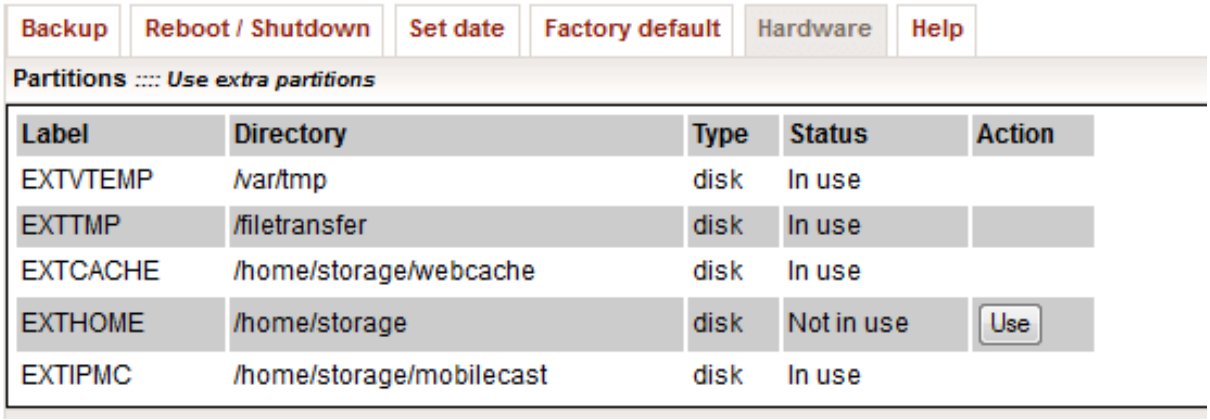
After this operation you must configure CommBox from scratch or restore configuration from backup.

9.5 Hardware

From the hardware page you can manage hardware devices connected to the CommBox.

9.5.1 Partitions on external disk

Some CommBox hardware configurations support an external disk.

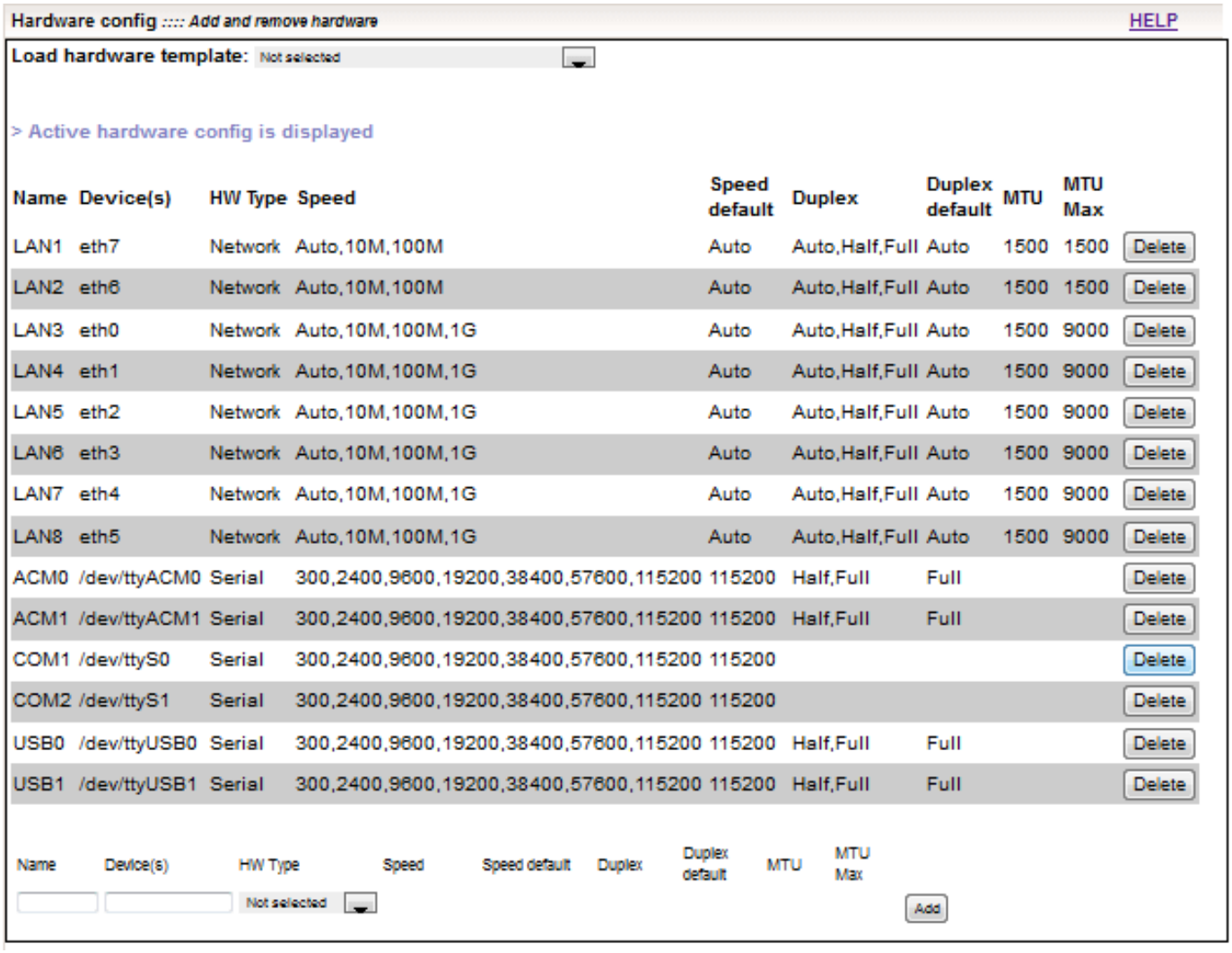


Partitions already in use will show status "In use", other partitions that has status "Not in use" can be activated by hitting [Use], this requires a reboot of the CommBox.

If only the heading "Partition :::: Use extra partitions " shows on this webpage there isn't any external disk connected.

9.5.2 Hardware configuration

The hardware devices configured here will be used in “Config->Network” and “Config->Connection”.



You can select one of the available templates from the "Load hardware template" drop-down. Each of the available templates covers the basic configuration for different types of CommBox. They are a useful starting point for creating your own configuration.

9.5.3 Basic use

By default, the current hardware configuration is displayed, and the text “Active hardware config is displayed” is shown at the top of the page.

> Active hardware config is displayed

You can add or remove entries to this configuration or you can load a standard template and modify that.

If the current configuration has been changed, this message will be shown:

> Hardware configuration is changed.
> Click on "Commit" button to create new hardware.conf

If you have loaded a template, this message will be shown:

> Hardware template file "quickblue40.hardware.tpl" active.
> Click on "Commit" button to create new hardware.conf

Once you begin changing the configuration or load a template, two buttons will appear at the bottom of the form.

[Commit changes]
: Saves and activates the changed configuration.

[Revert changes]
: Restores the hardware configuration as it was before you started changing it.

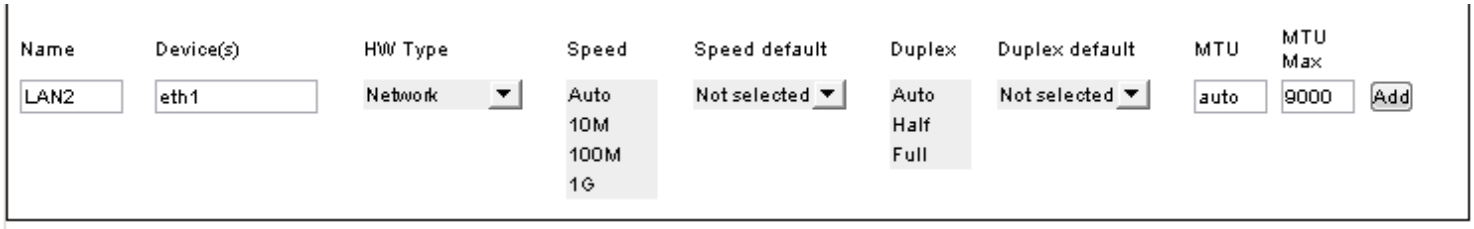
Note that, after you commit changes, the only way to revert them is by loading a previously saved configuration file with the "Restore hardware configuration" option set to "yes" (see Backup).

9.5.4 Add new hardware device

There are six types of devices:

- Physical devices
  - ♦ Network device (eth*)
  - ♦ Serial device (dev/tty**)
  - ♦ Serial console (/dev/tty**)
- Virtual devices
  - ♦ vlan (eth*.*)
  - ♦ vir - virtual network interfaces (eth*:*)
  - ♦ bridge - network bridges

To add a device, use the form at the bottom of the "Hardware config" panel. Which fields you will need to fill depends on which hardware type you choose.



Name
: The name of the device.
This will be used in any other part of the CommBox configuration where you will have to choose a network device.
Name the device according to type of device (LAN, COM, VIR, VLAN or BRIDGE)

Device
: Path to physical device.
It follows the patterns: /dev/ttyS0, eth0, eth0:1 (vir), eth0.1 (vlan).
For bridges, enter the ethernet devices acting as bridge members (like eth0 and eth1) in the form of a comma separated list.

HW Type
: The hardware type of the device.
Which other fields you need to configure, and their allowed values, will change according to the selection you make here.

Speed (available for serial and network)
: The speeds available for selection when this device is used in other parts of the CommBox Configuration (for example "Config->Network").
Hold Ctrl to make multiple selections.

Speed Default
: Value to use if no choice is made.

Duplex (available for network)
: The duplex modes available for selection when this device is used in other parts of the CommBox Configuration (for example "Config->Network").
Hold Ctrl to make multiple selections.

Default duplex
: Value to use if no choice is made.

MTU
: Maximum transmission unit (max frame size).

MTU max
: Max MTU value allowed for this device.

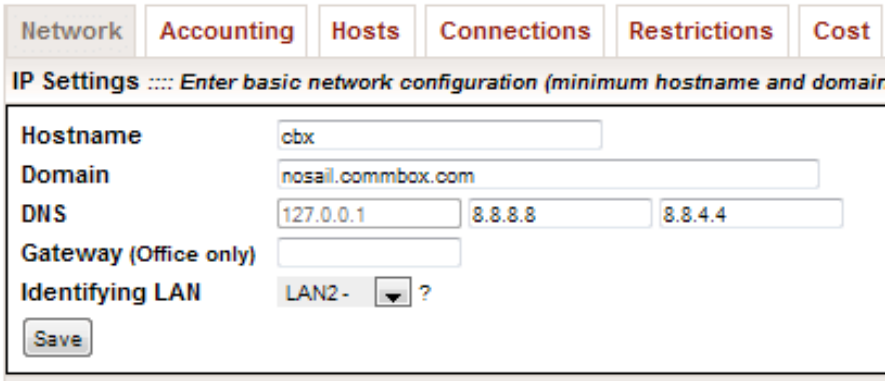
10 Configuration

From the Configuration tabs you can access all the basic settings of the CommBox.

10.1 Network

10.1.1 IP Settings

The most basic network configuration is done here, this section must be configured before you can use the CommBox.



Be careful: setting the wrong gateway IP address will isolate the CommBox from the rest of the network.

Hostname
: Hostname (network name) of the machine. This name is used to recognize CommBox on the network (LAN). We recommend that the name “CommBox” or “cbx” is used. This way it's easy to find CommBox on the network.

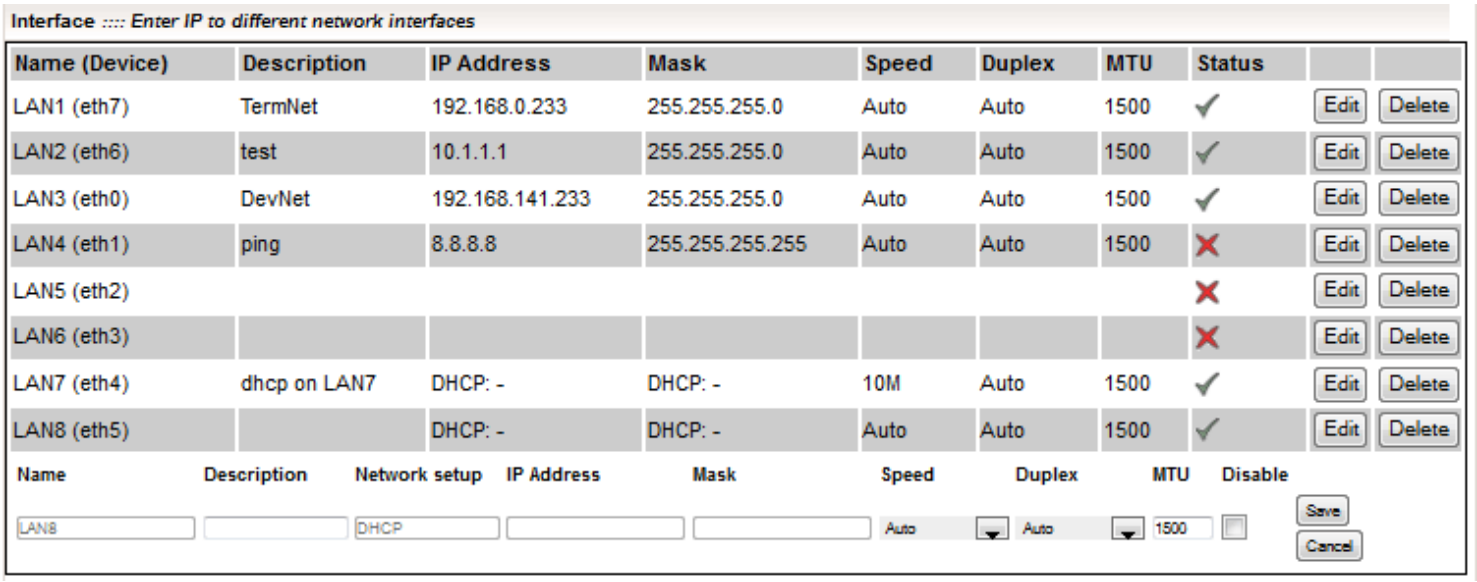
Domain
: The name that represent the network and the company. In our example we use nosail.commbox.com, where “nosail” is the name of the vessel and “commbox” is the company name.

DNS Server
: DNS Servers available on the network should be added here. The CommBox will always look in its own DNS (Host name table) to find the IP addresses for the machines to which it connects on a regular basis.

Gateway
: The IP address of the machine on the network that acts as a route point between the different networks on the vessel or office. It can also be the IP address of the machine or router that gives access to public Internet.

Identifying LAN
: The network interface through which the CommBox identifies itself on the network. The possible interfaces are those defined in the *Interface* section, interfaces defined as DHCP in *Network setup* can not be used as Identifying LAN. (see below)

10.1.2 Network Interfaces



This section lists all available network interfaces (network cards) on the CommBox. The minimum information required for an interface setup are an IP address and a subnet mask. You can mark an interface as disabled and re-enable it at a later time.

Name (Device)
: These values are given by the system, see Hardware configuration

Description
: This is a short description given by the user configuring the interfaces.

IP Address
: It is possible to run the interface with "static" ip address and mask or request the address and mask from a "dhcp" server. Changing "Network setup" is a background task and is used in setting up some special CommBox configurations. If "DHCP" selected the IP Address column for this interface will have the text "DHCP:" as lead in to the ip address when obtained or just a "-" if it is not obtained yet.

Mask
: See IP Address.

Speed
: The current selected speed (Auto or bytes/sec.).

Duplex
: The duplex mode selected (Auto, Half, Full)

MTU
: Maximum transmission unit (number of bytes).

Status
: Enable / disable the interface.

[Edit]
: You can change the interface settings by editing, enter your changes and do [Save] and run the [Activate changes] when you are done with all your changes.

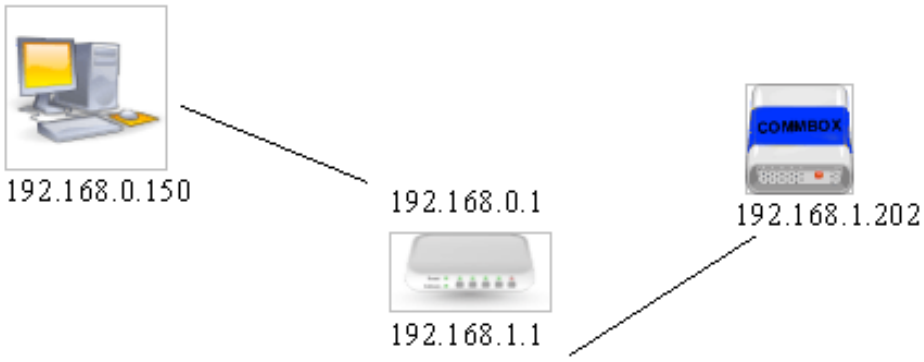
[Delete]
: Will remove the interface.

Note!
To reach CommBox and connect to it through the web interface, your computer and CommBox must be connected to the same network.

You have two alternatives:

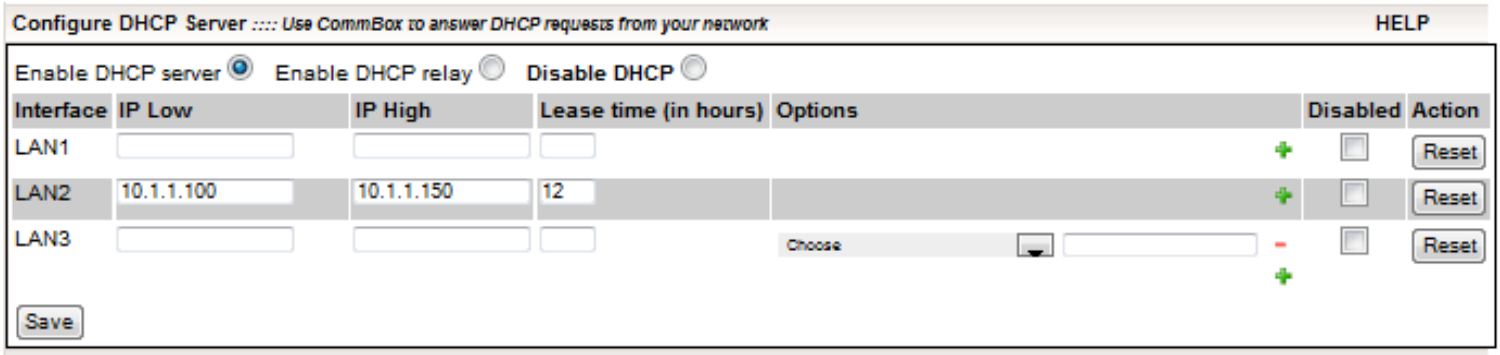
1. Your computer has an IP address in the same subnet:

2. You connect to CommBox through a gateway that routes between your network and the network on which the CommBox resides:



10.1.3 DHCP Server

The CommBox can act as a DHCP server. To configure and activate the embedded DHCP server go to "Config->Network", "Configure DHCP server" panel.



DHCP Server setup

There are three main options chosen from the top row:

Enable DHCP server

Use the CommBox DHCP server.

Enable DHCP relay

Use an external DHCP server, allow clients on different networks to access it.

Disable DHCP

Disable all DHCP handling by the CommBox.

The currently active option is shown in bold.

CommBox DHCP server setup

If you choose "Enable DHCP server", the CommBox will handle directly all DHCP requests coming to it. You can configure how they will be handled by each of the configured Network interfaces.

IP Low / IP High

Respectively the lowest and highest IP address used for the DHCP server pool.

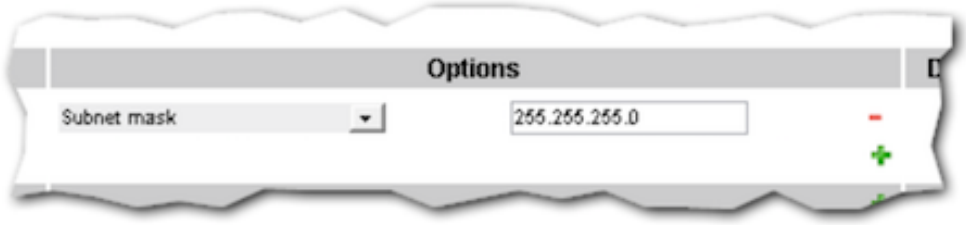
Lease time

The amount of time (in hours) a client can keep the leased address before a new request should be sent to the DHCP server.

Options

Options for the DHCP. A list of the most used standard options is provided in a drop-down menu. Click on

the green "+" sign to add more options, click on the red "-" sign to remove an option.



Subnet mask
: Option number: 1.
Specifies the net and local subnet mask.

Router
: Option number: 3.
(Also called Gateway). Specifies the IP addresses of N/4 gateways for this subnet. If one of many gateways is preferred, that should be first.

Host name
: Option number: 6.
Specifies the IP addresses of N/4 domain name servers in order of preference.

Domain name
: Option number: 15.
Specifies the domain name of the client for Domain Name Server (DNS) resolution.

NetBIOS name server
: Option number: 44.
A list of NetBIOS name servers listed in order of preference.

TFTP server name
: Option number: 66.
The TFTP server used when the 'sname' field in the DHCP header has been used for DHCP options.

Boot file name
: Option number: 67.
The name of the bootfile on the TFTP server to be used when the 'file' field in the DHCP header has been used for DHCP options.

SIP Server DHCP
: Option number: 120.
Either an IP address or a fully-qualified domain name to be used by the SIP client to locate a SIP server.

TFTP Server IP Address
: Option number: 128. (Specific for IP Phone software load).
The IP address of the TFTP server.

TFTP Server IP Address (Cisco)
: Option number: 150. (Specific for Cisco equipment).
The IP address of the TFTP server.

Config file
: Option number: 209. (Specific for PXELINUX).
The PXELINUX configuration file name.

Path prefix
: Option number: 210. (Specific for PXELINUX).
The PXELINUX common path prefix.

Reboot time
: Option number: 211. (Specific for PXELINUX).
The number of seconds to wait before reboot in the event of TFTP failure. 0 means wait "forever".

Custom.
: Option number: free choice.
Any other option you want to add. The available options and their meaning depend on the equipment you use.
When you select custom, you put the number in the value field followed by semicolon and the value. e.g. "234:192.168.140.11"

Disabled

Disable the DHCP setup for a particular network interface.

[Reset]

Will clear all values given.

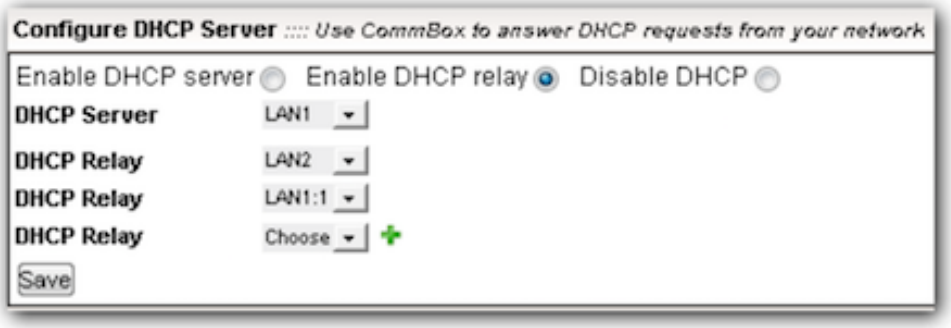
[Save]

After you are finished with the setup, click [Save] and then [Activate changes] to activate the new settings.

[View Leases]

Shows a list of the active DHCP leases.

DHCP relay setup

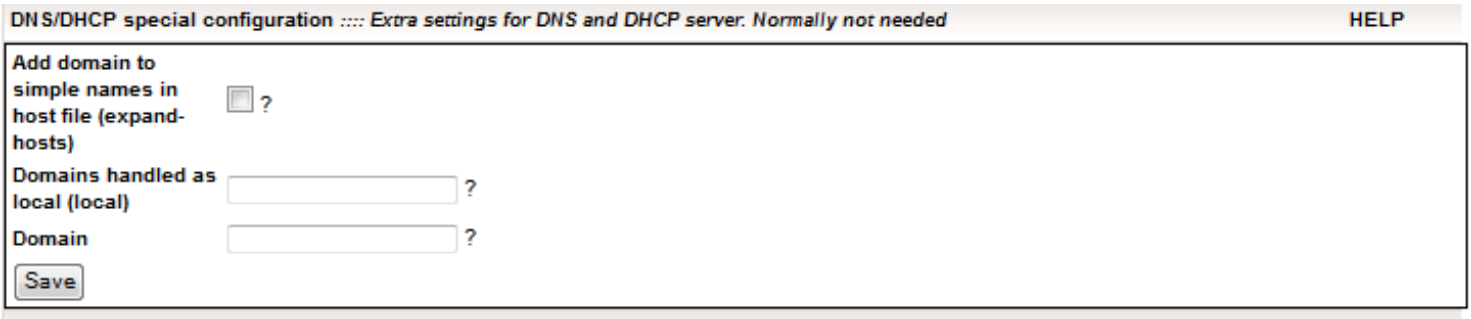


If you want to use an external DHCP server, select "Enable DHCP relay". Select the network interface for the network where the server is in the "DHCP Server" drop-down menu and the network interface(s) where the clients are in "DHCP Relay". Click on the green "+" sign to add more DHCP Relay interfaces.

10.1.4 DNS/DHCP special configuration (vessel)

Extra setting for DNS and DHCP server. Normally not needed. DNS settings is only available on vessel.

Please contact CommBox Support prior to attempting configuration.



Add domain to simple names in host file (expand-hosts)

Set this if you want to have a domain automatically added to simple names in a hosts-file.

Domains handled as local (local)

Add local-only domains here, queries in these domains are only answered from local DNS server.

Domain

Override system domain (special case use).

10.1.5 OpenVPN server configuration (hub)

OpenVPN server configuration is only available on hub installations.

Server port

The port from which the OpenVPN communicates. The default is 2223, if anything else is used, this must be considered when configuring connection profiles on vessels connecting to the hub.

Server network

The network that the OpenVPN server will use for communication between itself and the connected clients. Any network is usable here, the best choice is usually to use a private network that is not in use in any other part of your network topology.

Office networks

The networks to which any vessel should be routed when connecting. Routes for these networks will be set on any client connecting, regardless of whether they are in the connecting machine's remote networks in the connection profile or not.

Vessel networks

The vessel networks to which connection should be routed. The CommBox OpenVPN system will automatically fetch vessel networks from the vessels' configuration and create routes to those that are also listed in this field. You do not need to keep track of which vessel the network is used on, the field is only meant to specify that it is allowed to route the network.

10.1.6 Windows network

In this section you can configure the CommBox so it can be part of a Microsoft network.

10.1.7 Network shares

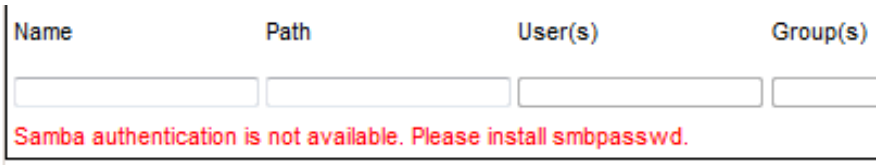
10.1.7.1 What are network shares used for?

The CommBox folders that you share will be visible to all computers in the network. The PC connected to the network will be able to mount the shared folders and use them as if they were normal folders for storing / retrieving files (depending on the permissions set for the shared folder).

The QuickFile system (see QuickFile) can use shared folders as an interface between users and CommBox.

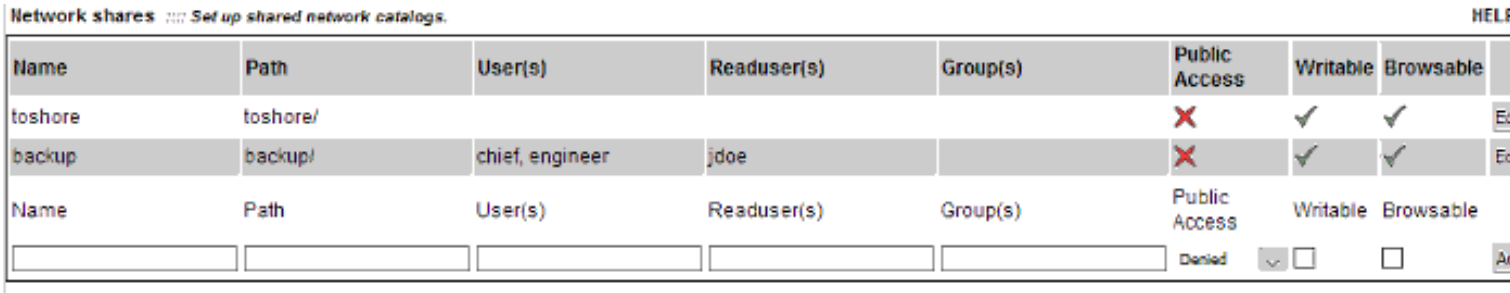
QuickFile is used to transfer files from one CommBox to another. For example a daily transfer of a database from the vessel to the office. You can set up the system so that, when you drop files in a shared folder mounted on your personal computer, these are automatically transferred to the office.

10.1.7.2 Samba authentication



The warning above will show if you haven't installed the Samba authentication package. File sharing will work, but there won't be any user or group authentication.

10.1.7.3 Create network share



Name

A descriptive name for the share. This is the name that the users will see when they browse the shared folders from their PC. The only allowed characters are letters, numbers, and underscore [a-z0-9_].

Path

Path of the shared folder on the CommBox. The only allowed characters are letters, numbers, and underscore [a-z0-9_], you can use a forward slash to separate folders in a structure e.g. you can have one 'databases/passengers' and a 'databases/crew'.

User(s)

For non-public shares, access can be limited to a list of local CommBox users, i.e.: "captain, admin". Some names

are reserved and you will be warned if you are using some of them, i.e.: administrator.

Readuser(s)
: Use this to restrict the listed user(s) to read-only access to the share.

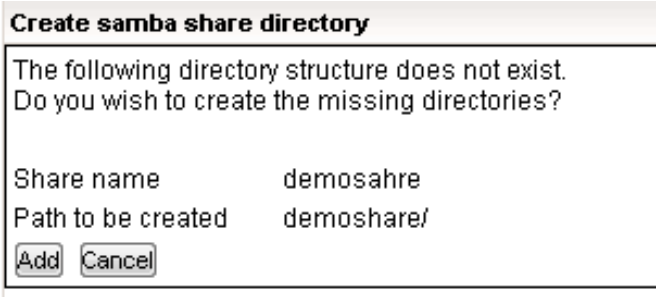
Group(s)
: For non-public shares, access can be limited to a list of local CommBox groups, i.e.: "crew". Some names are reserved and you will be warned if you are using some of them, i.e.: administrators.

Public Access
: Specify the public access permissions, from the drop-down list select either "Denied", "Read/Write" or "Read Only".

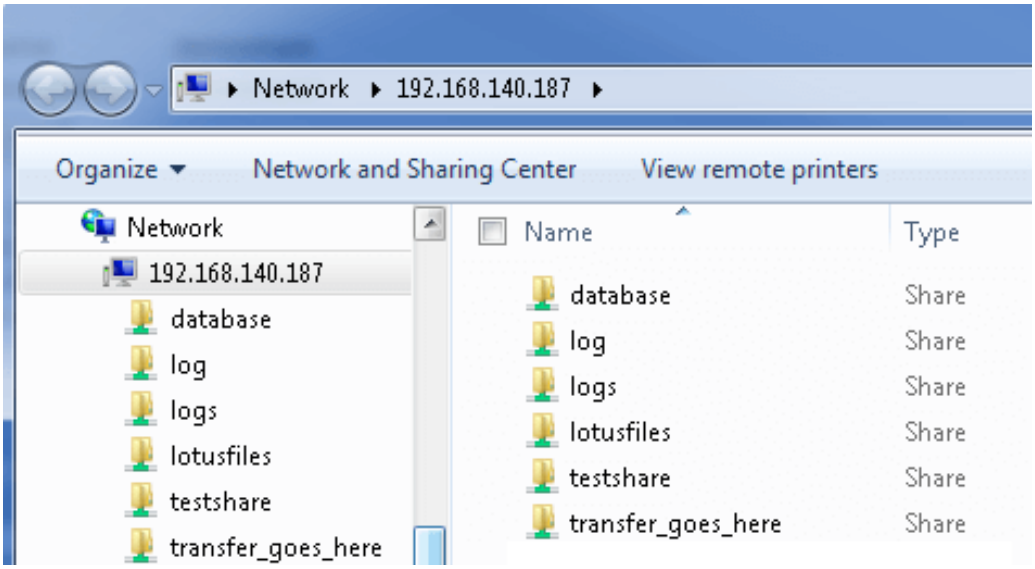
Writable
: If checked, users can add, change and delete files on the share.

Browsable
: If checked, users can list what's stored on the share, for example in Windows explorer.

When you press [Add], the CommBox checks if the folder you defined in "Path" exists. If it does not exist, you will be asked to confirm that the CommBox can create the necessary folders.



Click [Add] to confirm the directory creation. If you click [Cancel], the share entry will be created, but no directory is created. This will result in a useless network share. It will appear in the file explorer, but you will get an error if you try to access the folder.

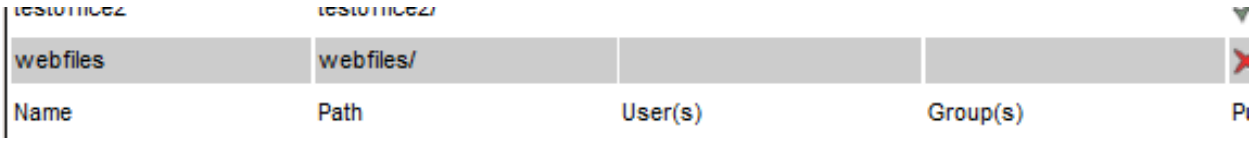


Here you can see how the share is shown in the file explorer after you enter the CommBox IP address in the path. The exact layout will vary according to your operating system version.

10.1.7.4 Changing the network shares

You can edit the share settings or remove the share. Please note that the directory shared and all it's content will be deleted, you will be warned if the directory contain any sub-directory or files.

10.1.8 Reserved Share Names



Some sharenames are reserved for special use:

webfiles
: Files in this share can be access via the web
Ex.: http://"cbx-ip-addr"/webfiles/"filename"
The file, that is named "filename", will be downloaded or displayed, this depends on the file type.

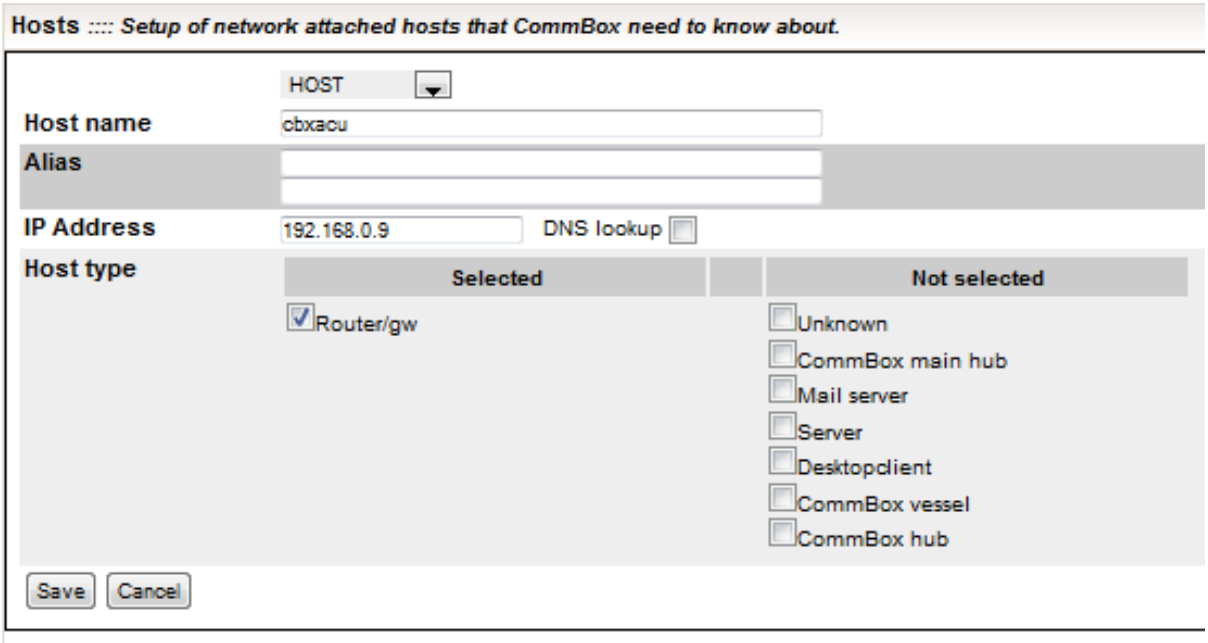
10.2 Hosts

From "Config->Hosts" you define all computers that the CommBox needs to know about. The hosts that are defined here will be available for selections in other parts of the configuration.

Many other sections of the CommBox configuration refer to hosts defined here. Changing a host's IP address here will update all the sections that refer to it.

10.2.1 Add / Edit host profile

To add a new host, click [Add] or to edit, hit [Edit] This will open the host add/edit view.



When configuring the host, you have to select how the host is presenting itself. Select "HOST" or one of the "DNS Record" types listed. If you select "HOST" see the description of parameters and options below in the "HOST" section, if you select one of the "DNS Record" types, see the "DNS Record" section below.

DNS Record
: The only DNS Record Type implemented so far is "CNAME" (Canonical Name).
For more information about DNS Record Types, please check out Wikipedia: DNS Record Types (external link).
CNAME

The "IP Address" and "DNS lookup" will be disabled if "CNAME" is selected and you need to specify the alias(es) in the "Alias" field(s). All the rest will be as for "HOST".

HOST

Host name

A qualified host name. This means no spaces, no underscore, no special characters.
The only characters allowed are letters, numbers, hyphen and dot: [a-zA-Z0-9-.].

Alias

You can specify one or several alias if you want the host to be known by more than one name.
The characters allowed are letters, numbers, hyphen and dot: [a-zA-Z0-9-.].

IP Address

The IP address of the host. Necessary unless you select the 'DNS lookup' option.

DNS lookup

If checked, the CommBox will perform a DNS lookup based on hostname to find the IP address of the host.

Host type

The type of machine i.e. whether it is a CommBox, mail server, router, etc. Feel free to select more than one type if the host can cover several roles. However, be aware that there can be only one host defined as "CommBox main hub".
The types already selected will be listed under the 'Selected' column when you open the entry for editing.

Do your changes and then [Save].

10.2.2 Delete host profile

To delete a host, hit [Delete] next to the entry you want to remove. Click [OK] in the dialog to confirm.

10.3 Connections

Connection profiles describe the connections between the CommBox and the external world, typically another CommBox.

There are three types of data transfers on a CommBox:

- Mail transfer
- File synchronization
- Routing / tunneling

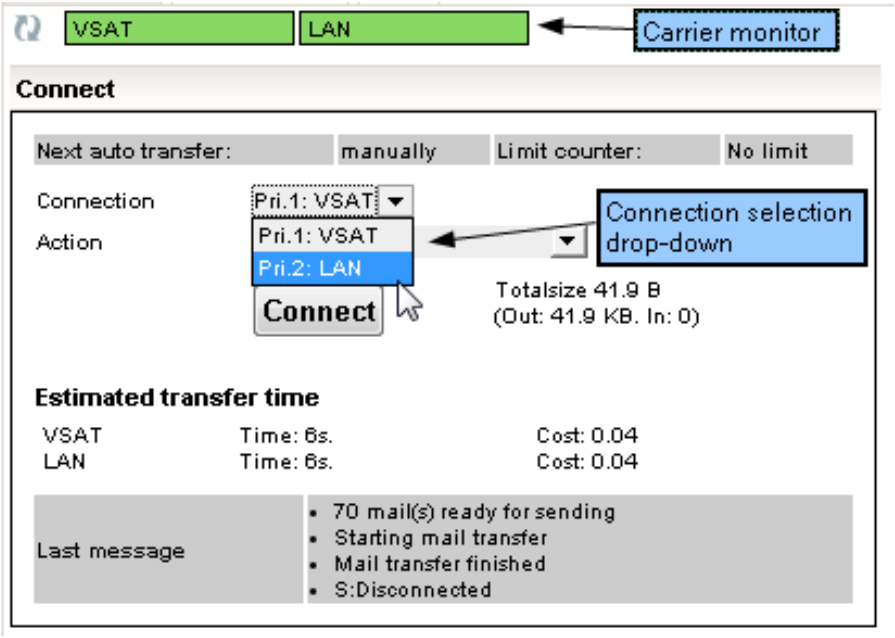
A connection profile describes:

- Where we want to connect (office, vessel)
- How we want to connect (Terminal / GSM / GPRS / VSAT)

This means that often you will define more than one connection profile for the same destination CommBox. For example you can have a connection to office via satellite terminal and another connection to office via GPRS modem.

The connections you define will be available from the connection selector in the Dashboard. They will also be visible in the carriers monitor in the top section of the Dashboard.

The LCD on CommBox R8 will show connection in use and other information, see Appendix: LED, LCD and Buttons



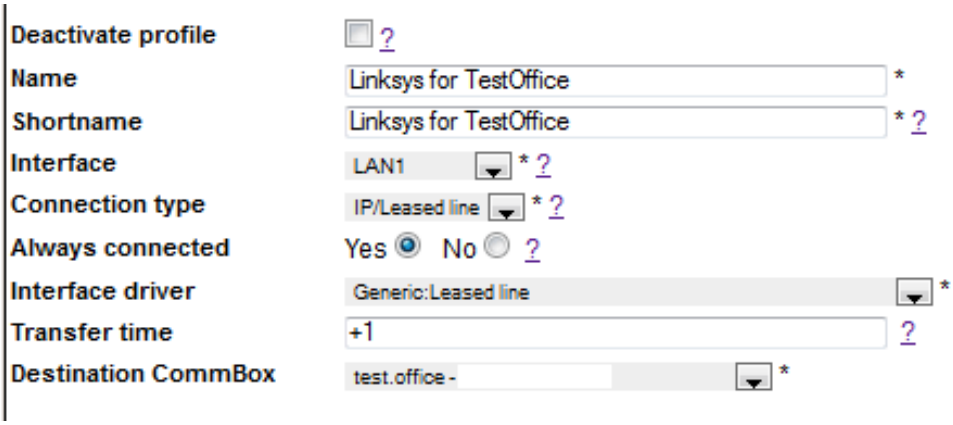
If a connection set as '*Always connected*' is active, the '*Connect*' panel will show less information and only a choice between '*Start transfer*' and '*Disconnect*'.

10.3.1 Add / Edit connection profile

To add a new profile, click [Add], to edit a profile, click [Edit]. This will open the add/edit view. The form is quite complex, but you will not use all fields each time.

The form is divided into two sections, one standard part and one advanced part. The advanced part is hidden until you click [Advanced options]. Some of the values in the advanced options are automatically populated when you select a hardware interface driver, so make sure that you first select a driver and only then customize the advanced options. This way you avoid overwriting the values you entered with the default ones.

10.3.1.1 Standard fields description



Deactivate profile
: If you want to disable a connection profile, without losing the configuration, tick off this checkbox. The carrier will not be visible in dashboard and it is not possible to do auto connect or manual connect with carrier. Whenever you want, the carrier can be enabled again by unchecking the box.

Name (required)
: Full name of the connection profile.

Shortname (required)
: Shortname is displayed in many places on the dashboard (e.g. carrier box, live status, connection and transfer log). A too long shortname will result in linebreaks that will disrupt the layout.

Interface (required)
: The network interface to which the communication equipment we want to use is connected.

Connection type (required)

The type of connection: dial up or leased line.

If you select “Dial up”, three new fields will show up:

Terminal phone number

Number on which the CommBox will accept incoming calls (if “receive” is set to yes).

Destination phone number

Number to call for outgoing calls.

See Appendix: Format of telephone numbers to see how to format the number.

Receive

Should this profile handle incoming connections?

Always connected

The connection is always active. This is used in leased line connections.

This does not affect the frequency of transfers, you still need to set a transfer time to deliver mail and files.

Interface driver (required)

Choose the correct driver for the device you want to use for the connection.

If your device is not listed, see Appendix: Interface drivers.

Every time you select a new driver, the fields in 'Advanced options' will be automatically populated with default values.

To restore the default values for the driver in use, you must first choose one of the other available interface drivers and then select again the driver you want to use.

Transfer time

Define when and/or how often file transfers should be performed. Times are specified as a comma separated list of entries.

If this field is left empty, auto transfer and connect for this profile is disabled.

'10:00, 11:00, 12:00, 13:00'

Transfer files/mail at 10:00, 11:00, 12:00 and 13:00 every day

It is possible to define a periodic connection by using the '+' symbol before the number of minutes defining the transfer frequency.

'10:05+15'

Transfer files/mail every 15 minutes starting at 10:05 (10:05, 10:20, 10:35...)

'+30'

Transfers mail every 30 minutes all day.

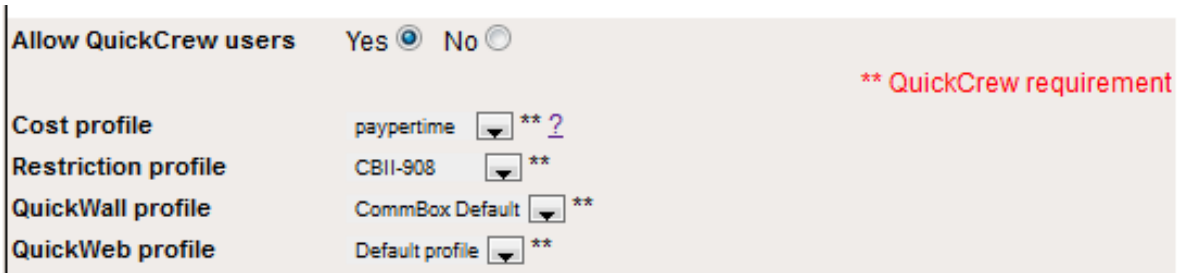
'08:05-16:05+60, 16:05-08:05+120'

Transfer files/mail every 60 minutes between 08:05 and 16:05, between 16:05-08:05 every 120 minutes

In order to avoid conflicts when calling the hub, dial-up connections must have different transfer times across a fleet, e.g. vessel 1: '10:05+60', vessel 2: '10:10+60', vessel 3: '10:15+60' and so on.

Destination CommBox (required)

The CommBox to which this connection goes. This pull-down contains all hosts of type 'CommBox hub'. Remember that this IP is also used as the identifier for the handshake protocol.



Allow QuickCrew users

Can this connection be used for *QuickCrew* traffic?

Cost profile

Which cost profile is linked to this connection. Cost profiles are defined under "Config->Cost" (see Cost (vessel)).

Restriction profile

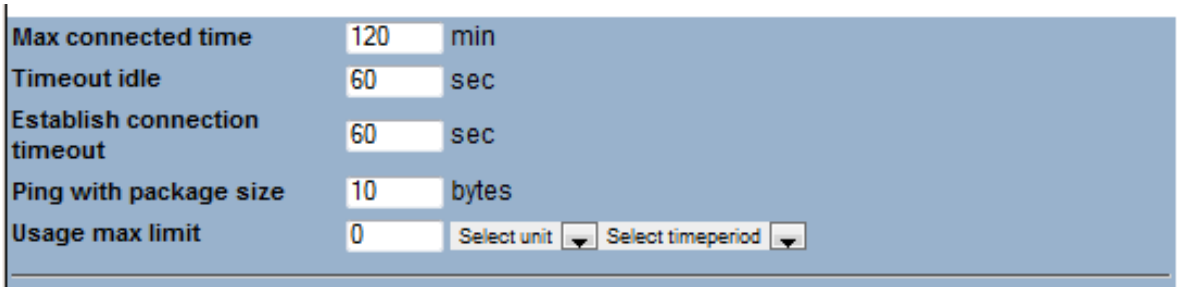
Choose which restriction profile is linked to this connection. Restriction profiles are defined under "Config->Restrictions" (see Restrictions).

QuickWall profile
: Select which firewall profile to use, if any. Firewall profiles are defined under "QuickWall" in the main menu (see QuickWall).

QuickWeb profile (vessel)
: Select which QuickWeb profile to use. QuickWeb profiles are defined under "QuickWeb" (see QuickWeb).

10.3.1.2 Advanced fields description

These fields are displayed when you click [Advanced options]. Most of them are automatically filled when you choose an Interface driver.



Max connected time
: Max connection time. Whenever a connection is initiated using [Connect] on the dashboard, the connection will (if still running), be terminated after the period configured here has passed.

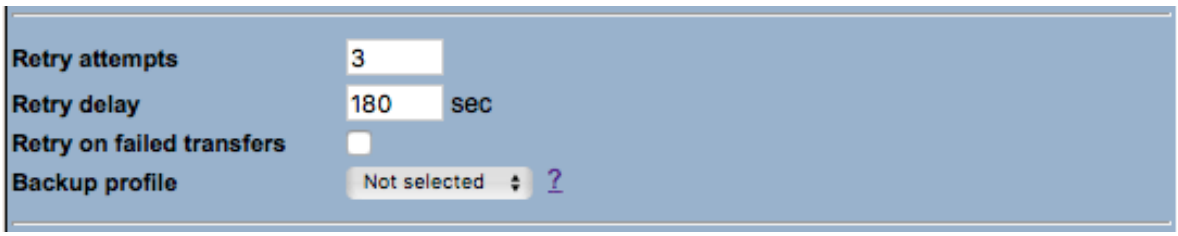
Timeout idle
: When making routing connections manually from the CommBox, the connection will be terminated after this period of inactivity.

Establish connection timeout
: The CommBox will break any connection attempt if it has not been able to make a functioning connection in the period of time configured here.

Ping with package size
: CommBox uses ping (ICMP ECHO) in some of its checks to see if a connection profile is able to make a successful connection. Certain devices need to have a specific payload of these packets in order to forward them to their destination. This may be configured here if needed. It is suggested to not use this unless you need to, as this slightly increases the amount of bytes sent from the CommBox.

Usage max limit
: The limit can be specified either as connection time or as amount of data transferred. The specified limit can be valid for a selectable time period of one day, one week, or one month after which the usage counter will be reset. When the limit is reached, the carrier will be blocked and its indicator in the connection monitor will turn yellow.

  Administrator users can reset manually the usage counter by clicking on the blocked carrier on dashboard and clicking the [Reset carrier usage] link in the bottom of the pop-up window.



Establish connection retry
: The times CommBox will try to establish a connection. If the last attempt is unsuccessful, the carrier will be set to not active (yellow) and the next scheduled transfer will be skipped.
  Example: Transfer time: +10, Establish connection retry: 3, Retry delay 60 seconds.
  - ◊ Try to connect at 10:00 and fail, try again at 10:01 and 10:02 and fail both times.
  - ◊ Carrier is set not active (yellow) at last connection try 10:02
  - ◊ Carrier will remain yellow until next transfer time + 1 minute.

That means that:

◊ At next transfer time, 10:10 , the carrier is still yellow and will not connect.
◊ At 10:11 the carrier turns active again (green)
◊ and at 10:20 the carrier will try to connect

While the carrier is not active, the transfer time for the lower priority carrier will be checked.

Retry delay

The number of seconds between connection retries.

Retry on failed transfer

Activates the retry mechanism for auto transfers when connection failure occurs after an initial connection is successfully established.

Backup profile

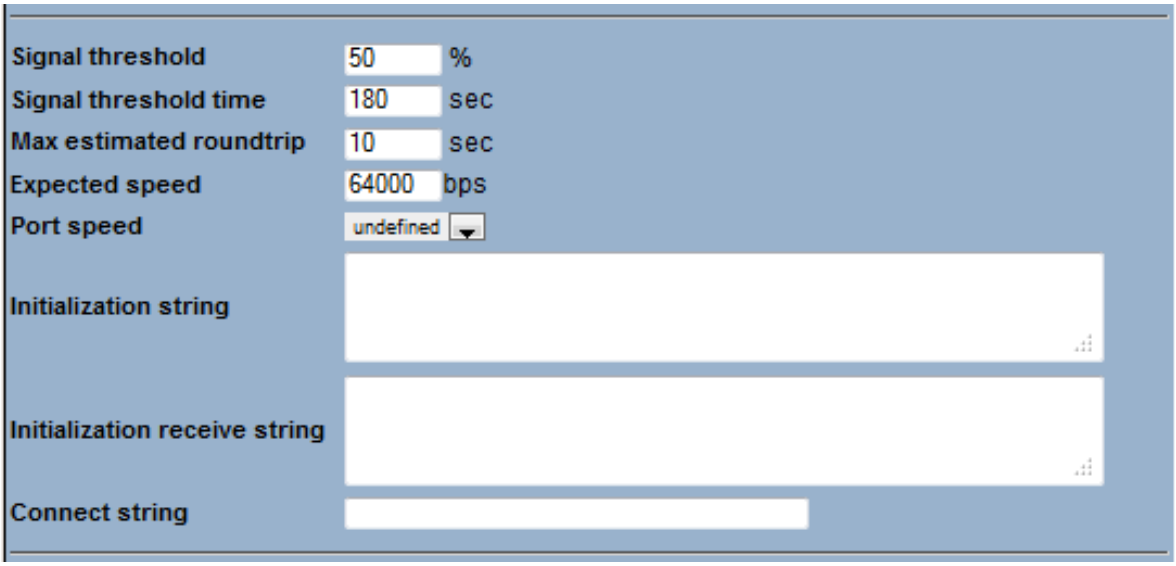
The carrier which will make a connection in case all connection attempts fail for this profile.

Be careful to not configure loops.

Example: Transfer time: 12:00, Establish connection retry: 3, Retry delay 180 seconds.

The current carrier will connect at 12:00. If it does not establish a successful connection, it will try again at 12:03. And again at 12:06.

If all attempts fail, the current carrier will be marked yellow at 12:06, and the backup carrier will try to connect immediately. The connection procedure for the backup carrier will become operative.



Signal threshold

Minimum acceptable signal strength for the profile to use for data transfer. If the signal strength is less than the threshold value, the carrier will remain yellow and there will not be transfer attempts.

Signal threshold time

The signal strength has to be higher than the 'Signal threshold' for this number of seconds before the profile status is switched to green.

The reason for this setting is to avoid frequent switching from green to yellow and vice-versa when the signal strength oscillates around the threshold.

Max estimated roundtrip

Maximum time to wait for an answer to a request the carrier has made. For example, when pinging an external host, this is the maximum time it should take to get an answer form the ping request.

Expected speed

The transfer speed expected from the device that is used for the connection.

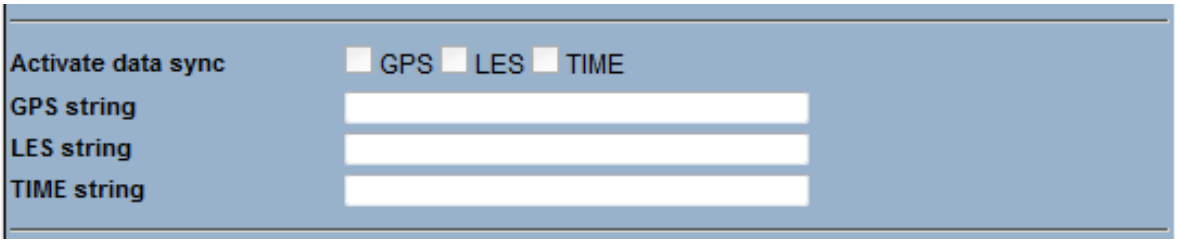
Port speed

The speed that the port to which the device is connected can handle.

Initialization string
: The string used to set up the device, and make it ready to dial the number in the profile.

Initialization receive string
: The string that sets up the device to handle incoming calls.

Connect string
: The string that tells the device to dial the number.



Activate data sync
: Which data to get from the terminal. The data will be saved in the carrier log.

GPS string
: AT-command to get the GPS data from the terminal.

LES string
: AT-command to get the LES (Land Earth Station) data from the terminal.

TIME string
: AT-command to get the TIME data from the terminal.

Do not check connectivity to hub
: If checked, CommBox will not test if it can connect to the remote CommBox. It will only test if it can connect to "Shore host for connection test".

PPP parameter(s)
: PPP parameters that will override the modem defaults.

BGAN port
: The port to use if the terminal is configured to not use the one defined in the interface driver.

HTS Channel
: For the HTS drivers that automatically change the connection setup, this is used to reconfigure the interface and local gateway to either the Primary Data channel or the Secondary Data channel during region change. If unselected, the Primary Data channel is used.

Management channel checkin
: Select the timegap from the drop-down menu, range from 1 minute up to 4 hours.

Management channel grade
: Select the grade from the drop-down menu.

  Disabled
  : No checkin, no files transmitted (sent or retrieved).

  CMS Checkin

Only do checkin to CMS, no files transmitted.

CMS Checkin Critical
: Transmit only critical files, less files transmitted.

CMS Checkin Medium
: Transmit critical and medium important files.

CMS Checkin Low
: Transmit critical, medium important and useful files, a larger number of files and larger files (in bytes) will be transmitted.

10.3.1.3 Routing fields descriptions

Local network
: Comma separated list of networks in CIDR format. a.b.c.d/n.

Remote network
: Comma separated list of networks in CIDR format. a.b.c.d/n.

Use VPN
: The type of VPN tunnel to establish. The available options are:

None
: No tunnel.

SSH VPN
: SSH tunnel.

Open VPN
: Use OpenVPN.
Note that OpenVPN needs a certificate to work. This certificate will be transferred from the hub when the vessel machine is configured there from "Config->Fleet". In case you are upgrading from older versions on CommBox without OpenVPN, certificates for each vessels will be made during the upgrade process of the hub. There is also the possibility of regenerating the certificate from the "Config->Fleet" page on the hub. This may be necessary e.g. if switching to a spare flash or a spare CommBox unit on a vessel.

OpenVPN Port
: If you use OpenVPN, you will need to supply the port where the destination CommBox (or the destination firewall, depending on the setup) listens.

Use connection as default gateway (routing)
: If this connection should be set up as default gateway for the CommBox when connected, set this parameter to yes

10.3.1.4 GPRS/MPDS/BGAN field descriptions

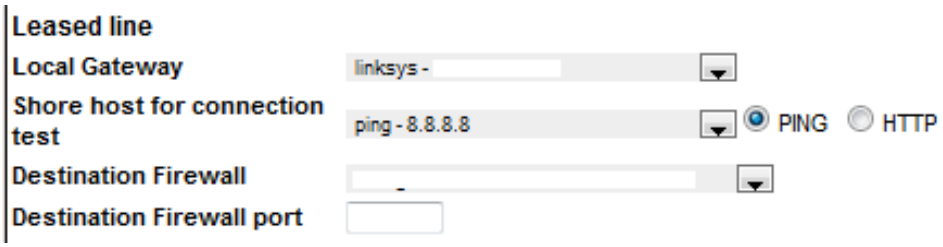
APN
: APN (Access Point Name) is used with GPRS connections to identify your service provider's gateway between GPRS date network and other networks (like Internet).

User
: User name for the GPRS gateway. This is supplied by your service provider.

Password

Password for GPRS gateway. This is supplied by your service provider.

10.3.1.5 Leased line field descriptions



Local Gateway (leased line)
: The host that acts as a gateway between the CommBox LAN and the public Internet.

  If ping to this host is successful, the status in the connection monitor turns yellow.

Shore host for connection test (ping) (leased line)
: A host on the public Internet used to check if the connection is up and running.

  If ping to this host is successful, the status in the connection monitor turns green.

Destination Firewall (leased line / GPRS)
: The destination host for this connection. The host must be available from the public Internet. Normally this the company's firewall.

Destination Firewall port (leased line / GPRS)
: The port you want to connect to when the connection reaches the final destination. The port is normally forwarded to the CommBox behind the firewall. Default port is 2222 (SSH)

10.3.2 Edit connection profile

To update a connection profile, go to the connection profile list and click [Edit] next to the entry you want to edit. Do your changes and click [Save].

10.3.3 Delete connection profile

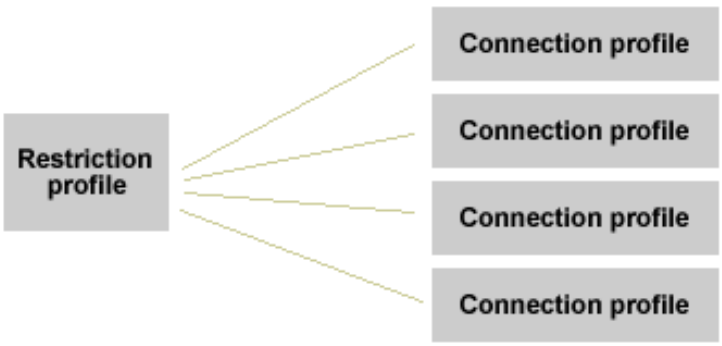
Go to the connection profile list and click [Delete] next to the entry you want to delete. You will be asked to confirm the deletion.

10.3.4 Change priority of connection profiles

To change the priority of a profile, move the profile up or down the profile list by clicking on the up and down arrows.

10.4 Restrictions

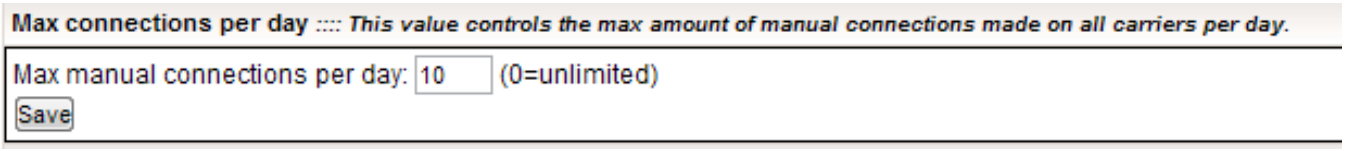
The CommBox restrictions define rules for how much data the different users and domains can send and receive through a specific connection. Restriction profiles are associated to a connection in each connection profile (see Connections). A restriction profile can be used from as many connection profiles as you want.



Restriction profiles are managed from "Config->Restrictions".

10.4.1 Max connections per day

A global value (i.e. not linked to a particular profile) that defines the maximum number of manual connections allowed in a day. Manual connections are those started by clicking [Connect]. This counter is carrier independent and will sum up connections made on all carriers. The counter is reset at midnight.

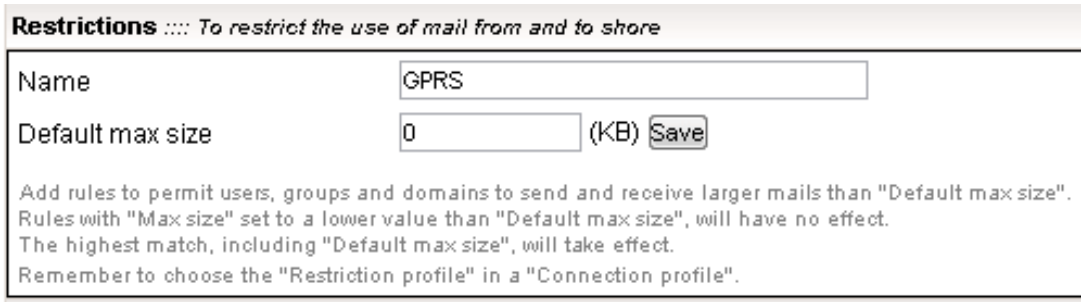


10.4.2 Restriction profiles

To add a new restriction profile, enter a name in the *Add new restriction profile* text box at the bottom of the page and click [Add]. You will then be shown the profile configuration form.

As a minimum of information, each restriction must have a name and default max size. In addition to this we can define rules for users, groups and domains.

10.4.2.1 Restrictions.



Description of fields

Name

Name of restriction profile.

Default max size

Default max size for the profile. If you don't add any additional rules, this will be the max transfer size for files transferred by the connection profiles that use this rule. Values defined for users, groups and domains will override this value only if they are higher.

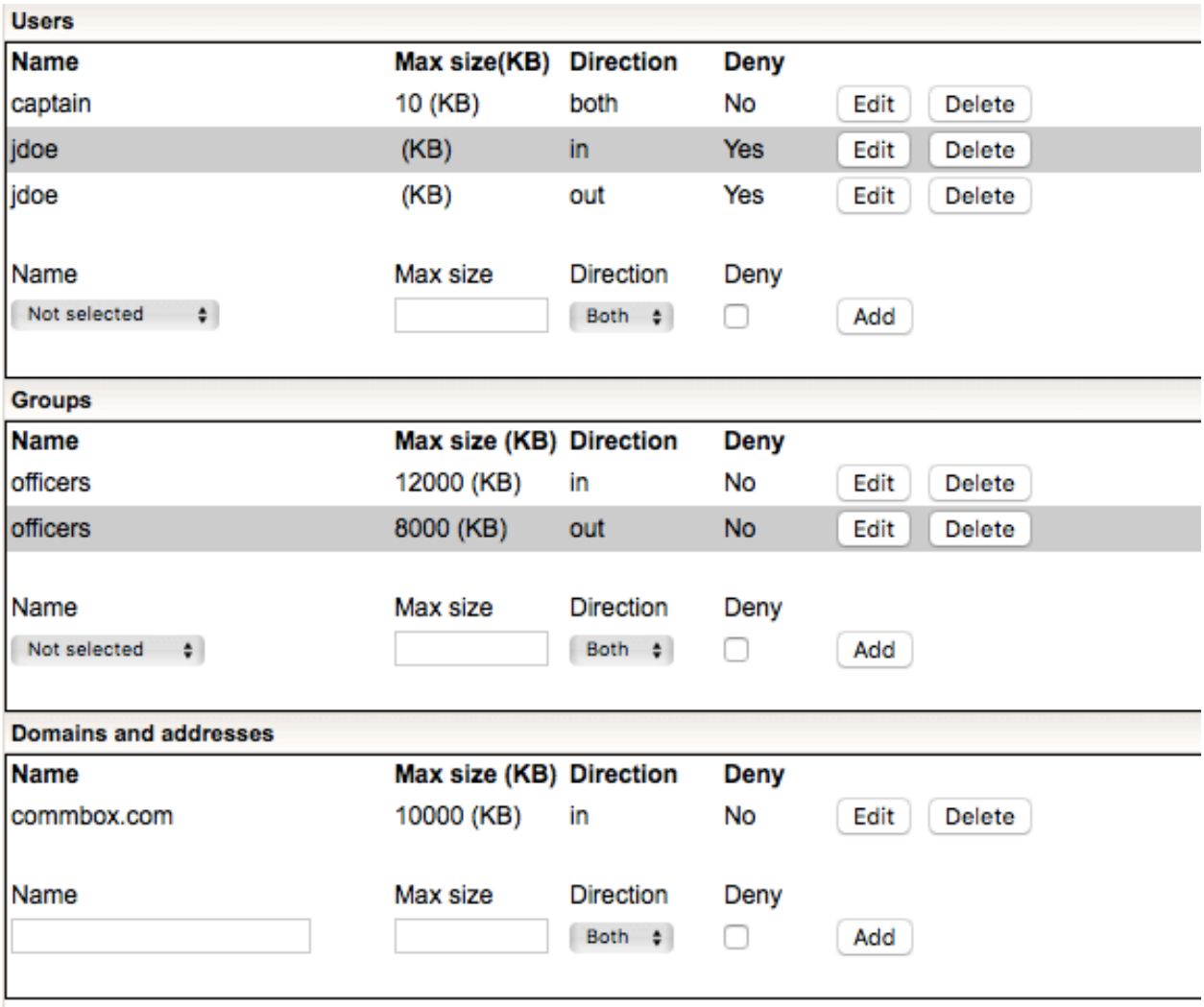
If this is good enough to cover your needs you can save and exit.

10.4.2.2 Add rules for users, groups and domains.

In addition to the default values, you can have a more fine-grained control down to user, group and domain level. This means that, for example, the captain or the officers group can send and receive more than the default rule allows.

If more than one rule match a transfer, the rule with the maximum allowance will be applied. This includes the 'Default max size'. As a consequence, any rule with a lower allowance that the default max size will have no effect.

Description of fields



Name
: Name of the entity (i.e. user, group, or domain) for which this rule applies.
For domain rules, you can enter any part of an address or domain name. The rule will be applied to any address that *contains* the string you enter here. For example the rule 'albert@commbox.com will match 'albert@commbox.com' but also 'john.albert@commbox.com' and 'albert@commbox.com.au'.
You can create a rule that applies to a family of domains by leaving out the top-level-domain part: '@commbox.' will match any email to any 'commbox.' address e.g. 'commbox.com', 'commbox.no', etc.

Max size
: The maximum size allowed for a file transferred over a connection.

Direction
: The direction the rule applies for. You can create different rules for incoming and outgoing data traffic.

Deny
: Files matching rules marked with "Deny" will be rejected by the transfer system.

Some examples
: See screenshot above.

Users
: John Doe (jdoe) is not allowed to send or receive anything in this profile.
Captain is allowed max size is 15000kb in both directions.

Groups
: Officers is set up with different limits on incoming and outgoing traffic.

Domains
: Incoming traffic from the domain commbox.com can exceed the default max size.

Conflicting rules
: It is possible to define restrictions with conflicting rules. For example you could have a rule for the domain 'commbox.com' with size 10KB, a rule for 'albert@commbox.' with size 20KB, and a rule for 'albert@' with deny = yes. All of these will match the address 'albert@commbox.com'.

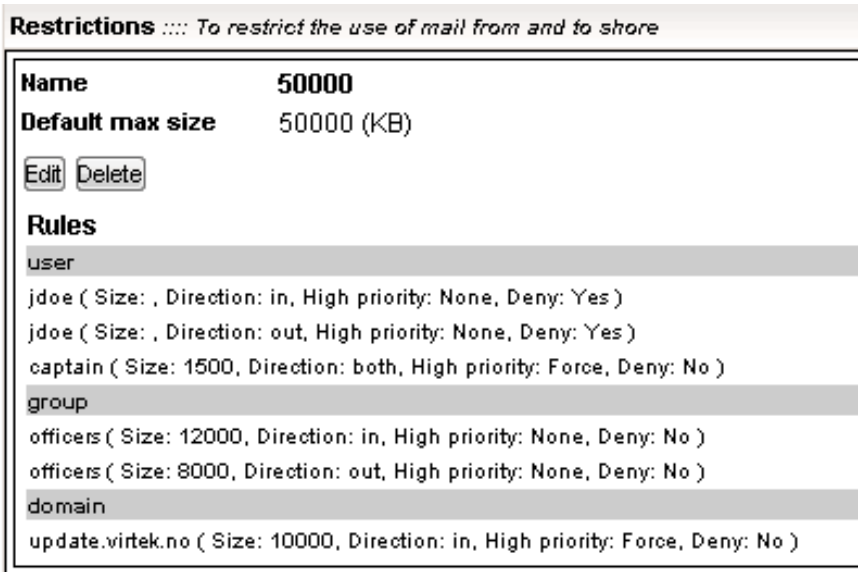
When this happens, there is a precedence hierarchy to establish which rule is applied:

◊ If a deny rule matches a message, the message is denied regardless of any other rule.

◊ If more than one size rules match a message, the one with highest size allowance is applied (this includes the 'default max size').

10.4.3 Edit restriction profiles

To edit a restriction profile, click [Edit] belonging to the profile you want to update. The selected profile will then open in the add/edit view. Update the values and rules, and then [Save].



10.4.3.1 Edit or delete rules

To edit or delete rules in a profile. Click [Edit] or [Delete] next to the entry you want to edit or delete.

10.4.4 Delete restriction profiles

To delete a restriction profile, click [Delete] that belongs to the profile you want to delete.

Before you delete a Restriction profile, make sure that it is not in use in any of the Connection profiles.

10.5 Cost (vessel)

Cost profiles define the cost of making a connection and/or transferring data. Each connection profile can be linked to a cost profile. The cost profile linked to the connection profile in use is the active one. It is usual to make different cost profiles for different carriers and/or different providers.

In a Cost profile you must choose which criterion is used to calculate connection charges:

- Pay by time
- Pay per byte

Only one type is allowed per profile.

10.5.1 Pay by time

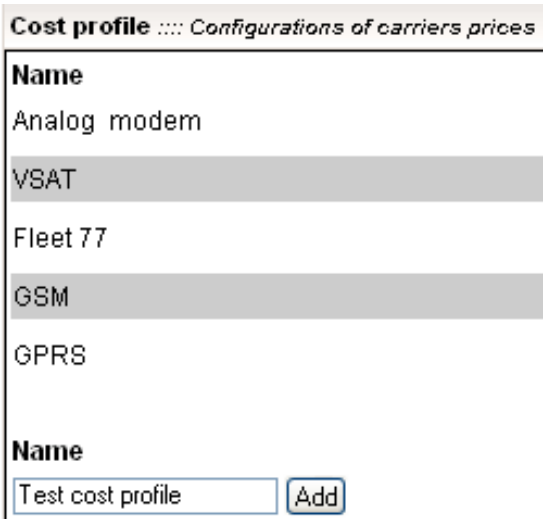
Typically used with connections via a standard telephone modem to remote locations over telephone or satellite connections. You are charged for the time the connection stays active.

10.5.2 Pay per byte

Often used with leased-line connections, where you connect to the Internet via telephone (GPRS) or satellite (VSAT). When you pay per byte, you pay for the actual amount of data that is transferred over the connection.

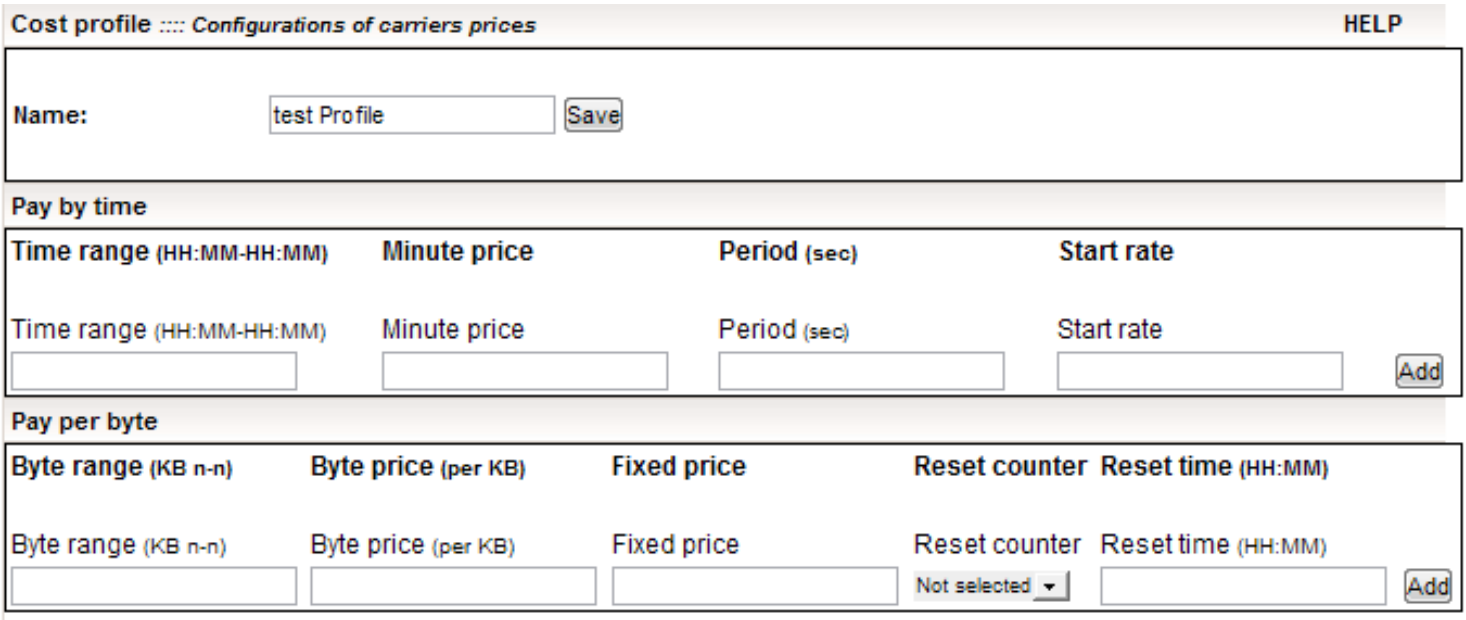
10.5.3 Add new Cost profile

Type the name for your new Cost profile and click [Add].



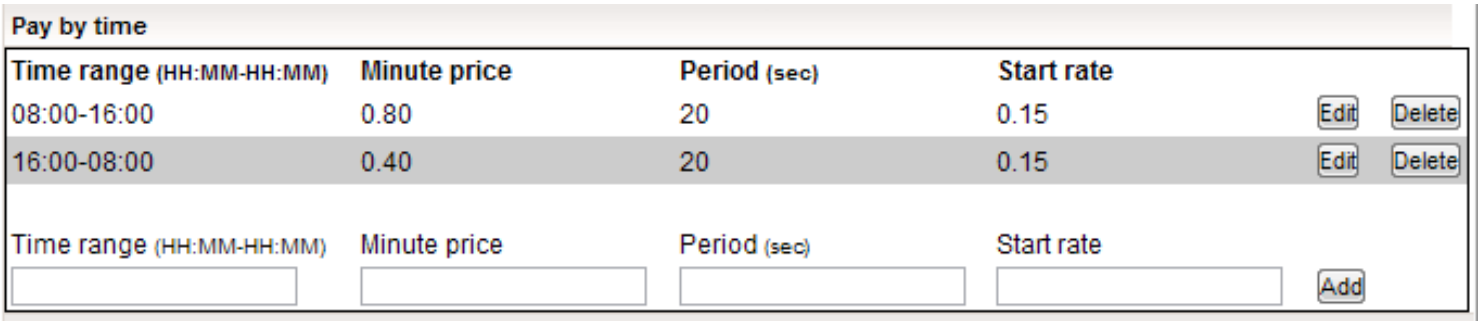
This will take you to the add/edit view where you can add the rest of the information. In the top section you will be able to rename the profile, click [Done] when you are finished.

It is important that you only use one of the two types, "pay by time" or "pay per byte" in a profile. The system will not be able to handle a mix of those two.



10.5.3.1 Add cost profile rules

When you start filling in a new profile, you must decide what type of calculation rules to apply, by time or per byte. Choose one of the forms in the profile and fill in the needed values. When finished click [Add]. Add the entries you need to describe the agreement with your service provider.

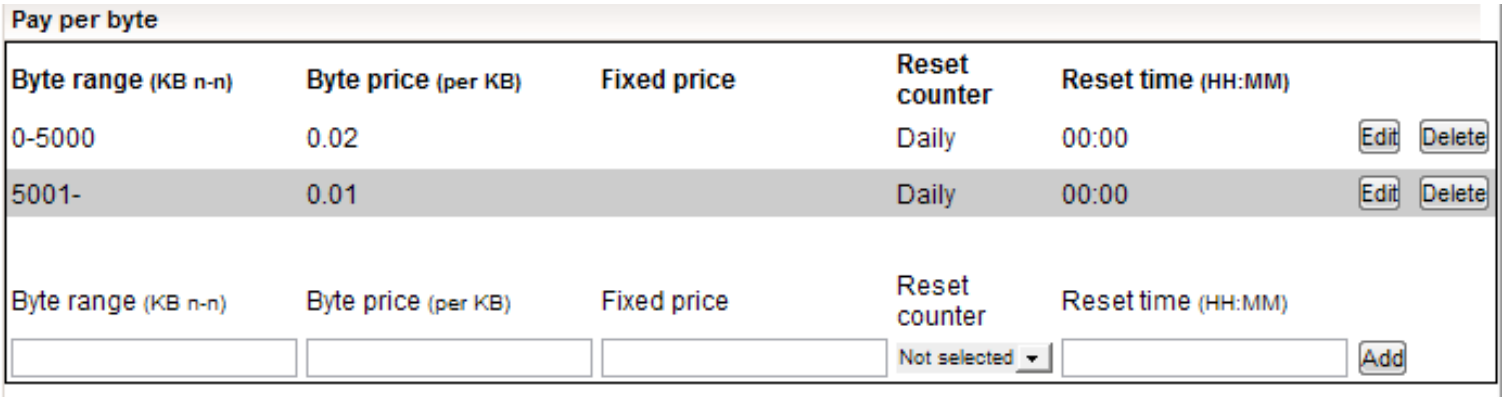


Time range
: From – to time span in the format HH:MM-HH:MM.

Minute price
: Minute price. The cost for being connected for one minute.

Period
: This is the billing unit for the connection. For example: if the billing unit is 30 seconds and the connection is up for 65 seconds, the charge will be for 90 seconds (three billing units).
If left empty, it defaults to 1 second.

Start price
: The flat additional charge for each connection.



It is normal for providers to have different pricing depending on the amount of data that is being transferred. For example, one price for the first 5000kb and another price for data after this step. To reflect this, it is necessary to add one entry for each step.

Byte range
: Enter the range for the current rule, e.g. 0– 5000 or 5001–. The value is in kilobytes (kB).

Byte price
: Price per transferred kilobyte (1024) in the current byte range.

Fixed price
: Fixed charge to pay, independent on how much you transfer over the connection. E.g. you may have a fixed charge to pay for any amount of transfers up to 50 MB and a charge for each MB transferred after that.

Reset counter
: How often should the byte counter be reset. Daily, Weekly, Monthly.

Reset time
: At what time is the counter reset. Add a time in the format HH:MM

10.5.3.2 This is best explained with some examples:

Example 1
: You pay 0.015 per kilobyte for the first 5000 kilobyte you transfer each day. Everything over 5000 kilobyte per day is free.

Byte range (kbyte n-n)	Byte price (per kb)	Fixed price	Reset counter	Reset time (HH:MM)

0-5000	0.015		Daily	00:00
5001-	0		Daily	00:00

Example 2

You pay a fixed price of 150 for the first 12000 kilobytes that is transferred each day. Traffic above this limit is priced by kilobyte.

Byte range (kbyte n-n)	Byte price (per kb)	Fixed price	Reset counter	Reset time (HH:MM)
0-12000		150	Daily	00:00
12001-	0.035		Daily	00:00

Example 3

You pay per kilobyte for the first 5000 kilobytes. For all traffic above this limit you pay a reduced price.

Byte range (kbyte n-n)	Byte price (per kb)	Fixed price	Reset counter	Reset time (HH:MM)
0-5000	0.025		Daily	00:00
5001-	0.015		Daily	00:00

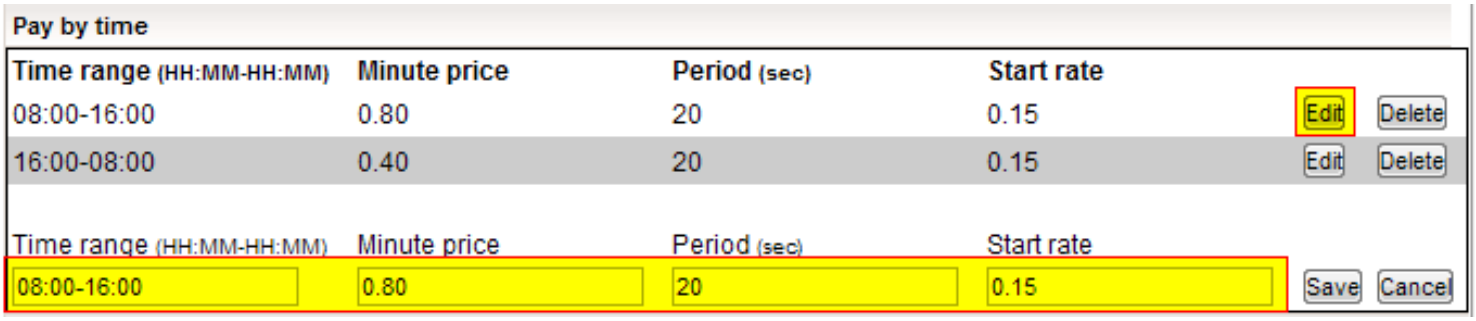
Example 4

You pay a fixed price for all traffic on a monthly basis

Byte range (kbyte n-n)	Byte price (per kb)	Fixed price	Reset counter	Reset time (HH:MM)
0-		250	Monthly	00:00

10.5.3.3 Edit cost profile rules

Click [Edit] next to the rule you want to change. This will open the rule in the edit part of the form.



10.5.3.4 Delete cost profile rule

To delete a cost profile rule, click [Delete] next to the entry you want to remove. Answer YES in the dialog.

10.5.4 Edit Cost profiles

To edit existing Cost profiles, click [Edit] next to the item you want to edit. This will take you to the add/edit view where you can update the profile name, and add, edit or delete rules (see description above).

If you decide to change the profile type (e.g. from 'pay by time' to 'pay per byte' you must first delete all rules. Then you can start from scratch with new rules.

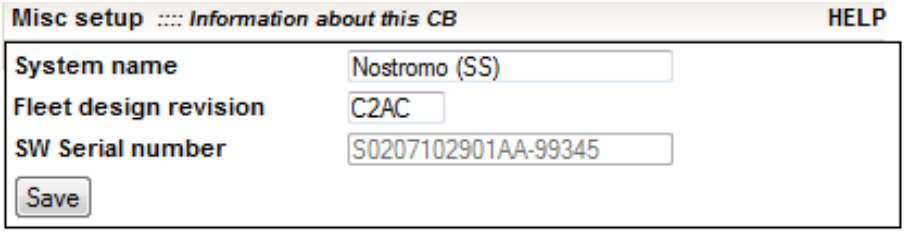
10.5.5 Delete Cost profiles

To delete a cost profile, click [Delete] next to it.

10.6 Misc

Under "Config->Misc" are miscellaneous settings that apply to the system in general.

10.6.1 Misc setup



System name
: This name is displayed in the top of your browser window and under the menu on left side.

Fleet design revision
: If filled in on vessels, this field can be used to keep track on the different configuration layouts in use on the fleet. Value of the field will be transferred together with the rest of the configuration that is sent from the vessel to the hub. The "Fleet design revision" name will end up in the vessel list on the fleet page. This will give system administrators a way to keep track of which vessel that is set up with which configuration.

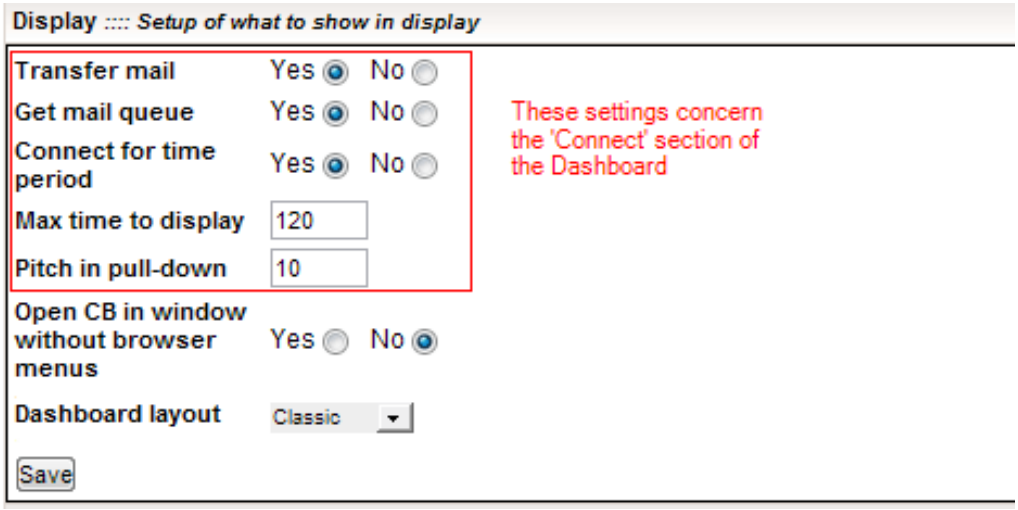
SW Serial number
: This field displays the software serial number of your CommBox software. Having this accessible will be helpful to support.

10.6.2 Error mail setup

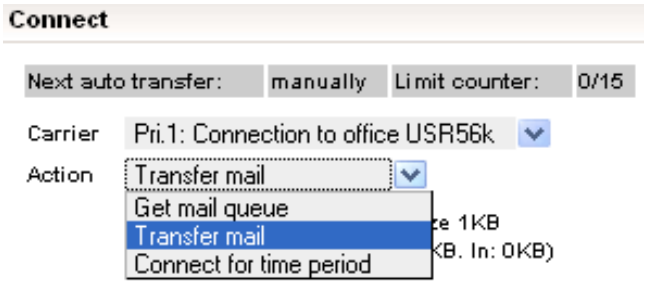
Email
: The mail address given here will be used as the recipient address when CommBox sends notifications and warnings which may be of interest and whenever some parts of the CommBox setup encounters issues which may need manual intervention.

10.6.3 Display options

Under this section you find most settings that applies to Dashboard and the behavior of the Connect section.



The first five settings determine which choices are available in the "Action" menu in the Dashboard's "Connect" panel.



Transfer mail
: Set to Yes if you want “Transfer mail” to be a choice in the Connect action menu.

Get mail queue
: Set to Yes if you want “Get mail queue” to be a choice in the Connect action menu.

Connect for time period
: Set to Yes if you want “Internet - Intranet connection” to be a choice in the Connect action menu.

The following entries relate to the “Connection time” field associated with the “Internet - Intranet connection” action.

Max time to display
: Enter the max connection time (default: 120min).

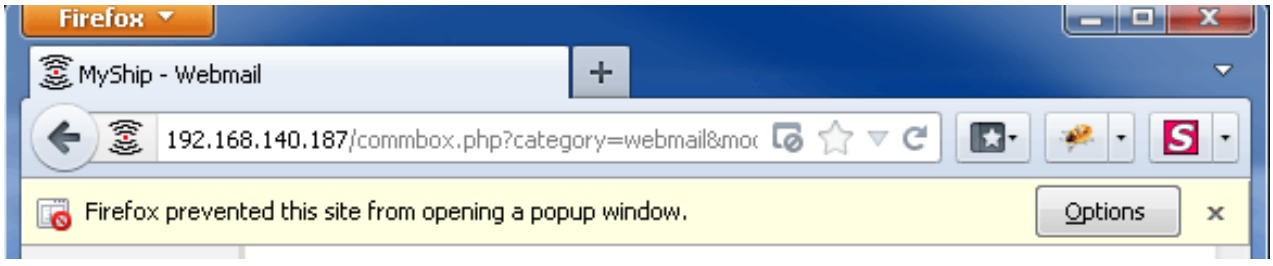
Pitch in pull-down
: The step between the time entries in the "*Connection time*" pull-down; from zero to max time (default is 10min) 10-20-30..120

The Dashboard connect actions are described in the chapter Connection operations

10.6.3.1 Other settings

Open CB in new window without browser menus
: This lets you decide if the CommBox interface should open in a new browser window or not. The new window will be opened without top browsers buttons, menu, etc. thus allowing more space for the interface i.e. more CommBox and less browser.

Most browsers have pop-up blocking turned on by default. This will prevent the new CommBox window from showing. You will get a message similar to this (in Firefox, the appearances varies depending on the browser type and version).



Click [Options] and add an exception for the CommBox IP address.

Use dashboard layout
: This selection switches between the two available dashboard layouts on the CommBox. The classic layout is the default one, which is the one with which most people are familiar. The Switch look option has another approach with simpler selection of carriers as well as other arrangements for file queues. It is also the best suited selection when the CommBox is used for ip routing alone and does not have a hub to which it transfers files.

10.6.4 Send configuration

This setting will enable / disable the 'send configuration' functionality in your CommBox. When enabled, a copy of the configuration will be sent to the defined email address each time the configuration is changed. The two main goals of this functionality are:

- Backup of configuration.
- Allowing support personnel to see exactly what is the configuration used so that they have a better chance to provide fast and accurate support.

By default an email containing the configuration files will be sent to the support email 'cbsystem@commbox.com'. Other setups can be arranged.

10.6.5 Log settings

How long to keep logs
: Specify (in days) how many days of log the CommBox should keep. The default is 182 days (half a year) which is suitable for an average use. However, if the CommBox is under constant heavy load, this may be a bit long if you don't have an extra hard drive. On such systems, you may use 90 days, which will give you approximately 3 months' worth of logs. You may also be able to select a lower number of days, since valuable information (for instance transfers and routing information) may be transferred to the hub using the 'mini log' system.

Retain fleet statistics for (hub)
: This is present only on the hub and determines for how long the statistics database should keep data from the vessels.

10.6.6 Currency settings

The selection pull-down enables you to set the currency prefix used when displaying credits for QuickCrew accounts. Saving on hub will transmit an update to all vessels as necessary, local changes on vessel will be local to the vessel. Note that the prefix is only used for visual purposes, it will not be used for any calculations.

10.6.7 Log database access (hub)

Use the log database access configuration to gain access to the relational database containing mini log information transmitted from vessels.

Fields description

Username
: username is only displayed to let you see which username to use when connecting to the database.

Password
: enter the password used for connecting to the database with the username the CommBox provides above. You will need to re-enter this in the next field for verification purposes.

Permit connections from
: the database will only accept connections from hosts defined here. They may be specified as IP addresses or host names. Wildcards are allowed, but subnet specification (i.e. /24) is not permitted. You may enter multiple (and combinations) of networks and host names by separating them with comma. Examples: 192.168.0.*,10.0.0.1.

Port
: the port on which the database server runs on the CommBox is displayed here for informational purposes.

10.6.8 Minilogs (vessel)

CommBox uses so called “mini logs” to transfer small messages from a vessel CommBox to its hub. These messages contain information about carrier usage, crew usage and other aspects of the system which the hub represents using graphs and tables.

Fields description

Queue Minilogs every: <time period>

The mini logs will be pushed to the transfer queue in intervals given here. The default is never, which disables the mini log system. CommBox installations using VSAT (or similar) carriers may have a short interval here, however systems using dial up connections will most likely be better off with an interval of 12 or 24 hours.

Log data traffic

Disabled if transfer interval is set to 'never'.
Include in the minilog information about the amount of data transferred between the CommBox and the external world.
If there are on board networks not configured on the CommBox (e.g. when a router is between the CommBox and the client), the traffic from these networks will not be included in the report. To include it, enter the networks as a comma-separated list in CIDR notation (e.g. 10.0.0.0/24) in the text box. Traffic from any of these LAN will be marked as coming from "- secondary network -" in the reports on the hub.

Log web access log

Include in the minilog information about Web usage.

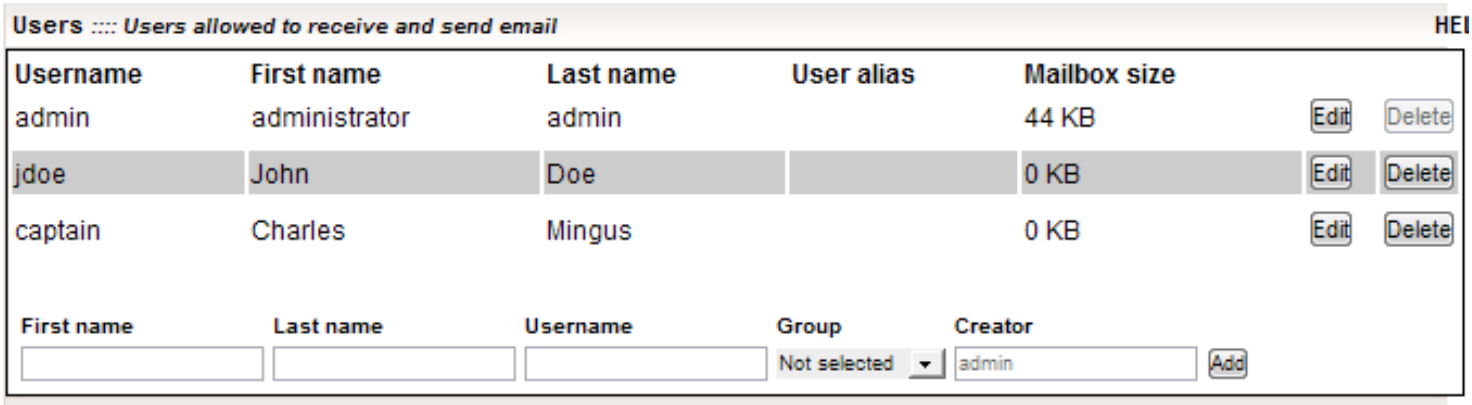
10.7 Users / group

Users defined in CommBox user system have two purposes:

Mail users: All users that want to use CommBox as mail server must first create a user account.

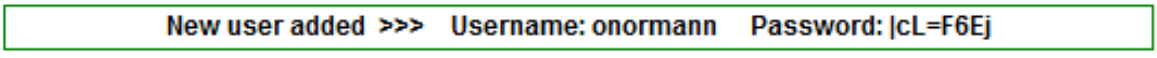
System access: Users need an account to access the CommBox and its services. Which services a user can access is regulated by group membership.

10.7.1 Users allowed to receive and send email



10.7.1.1 User add form

Is located below the user list and has three fields, two required and one optional. Username is generated if left out. The last field shows the user name of the creator (user currently logged in). Users are generated with a random 8 character password consisting of at least a lower case character, an upper case character, a special character and a number.



First name (required)

First name.

Last name (required)

Last name.

User name

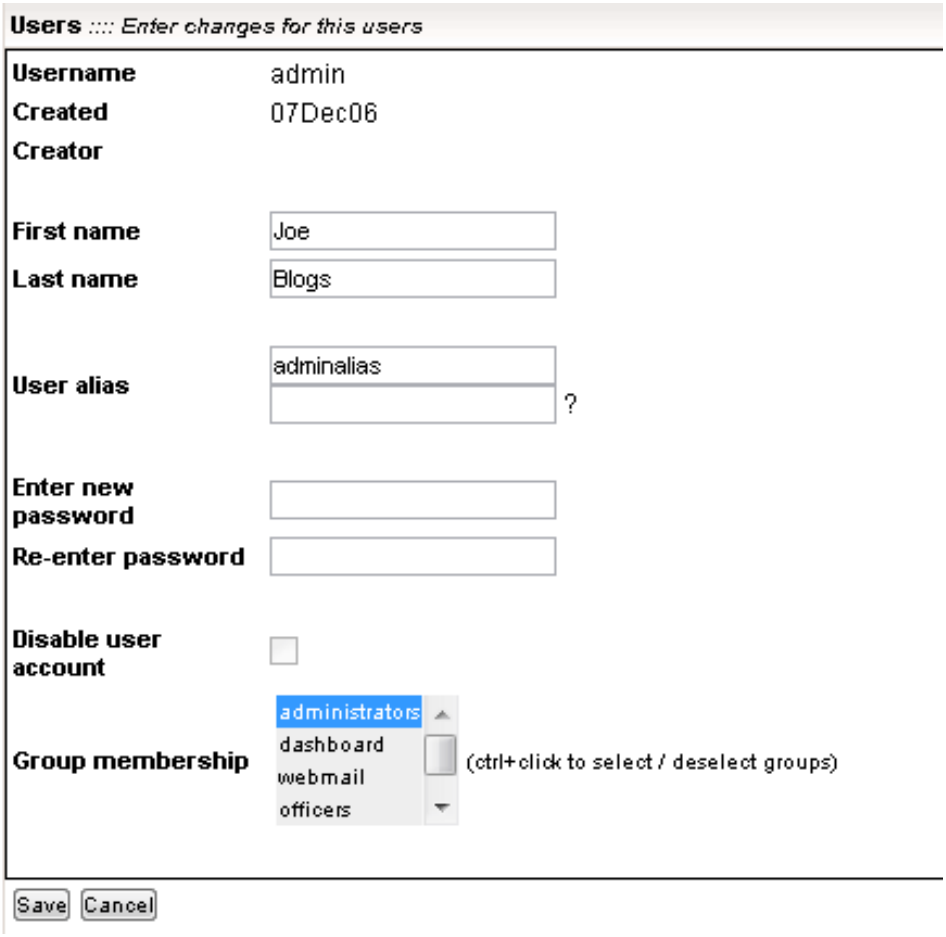
If this field is left empty, the value will be generated based on the values in first name and last name.

Creator

User name of the currently logged in person creating the new entry. You cannot edit the content of this field.

10.7.1.2 User edit view

Edit a user profile by clicking [Edit] for the entry. This will open a detailed view of the user entry. In this view you may change values, add aliases and change the password for the user account.



User alias
: Aliases for the current user may be added here.

Password
: To change password for a user, enter and re-enter new password.

Disable user account
: Tick off this one to disable the user account.

Group membership
: Choose the groups of which the user is member. *You must hold down the control button when you select / deselect groups from the select box.*

10.7.1.3 User delete

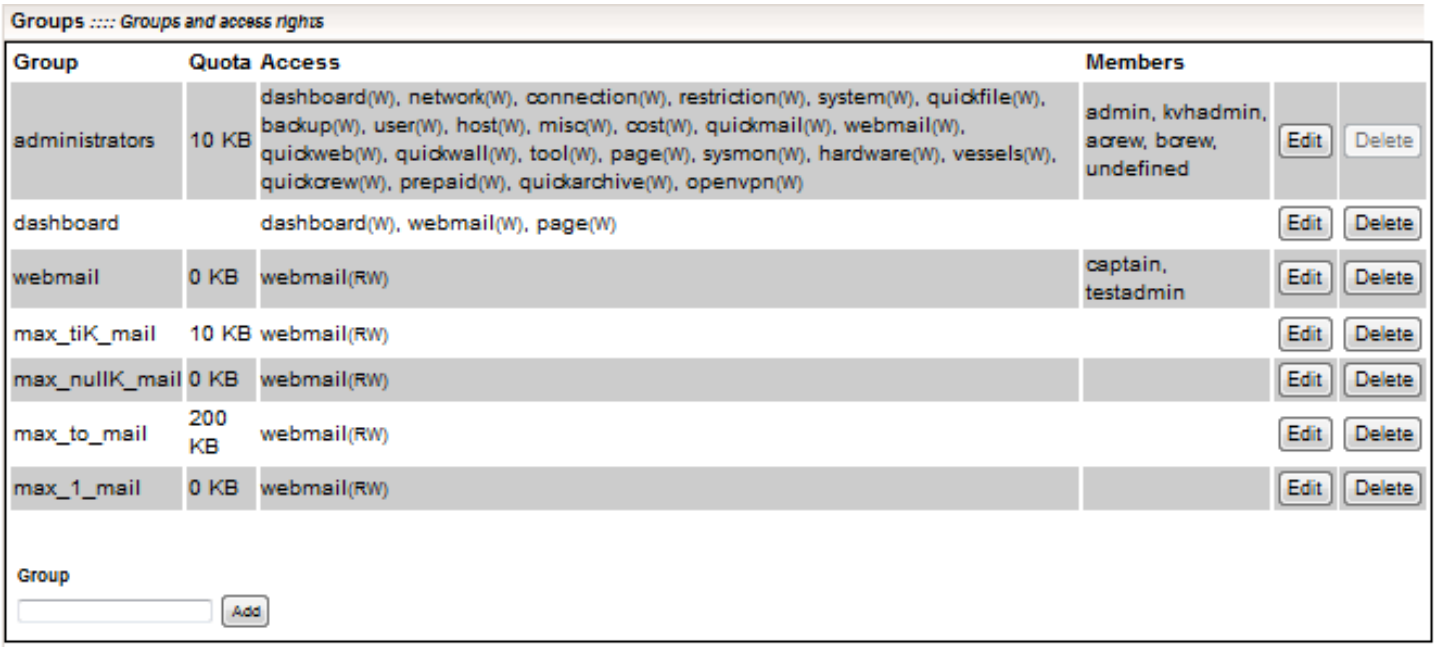
To delete a user click [Delete]. *It is not possible to delete the administrator user.*

10.7.2 Groups and access rights

The group to which a user belongs determines which areas of the CommBox interface are accessible. For example, the administrator group will have access to all areas while another group may be granted permission to only access the dashboard functions.

10.7.2.1 Group add

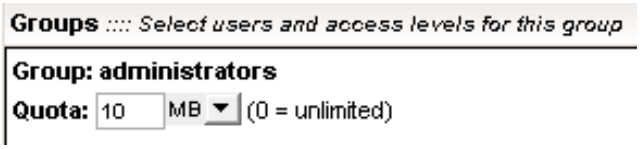
To add a new group, write a name in the 'Group' field at the bottom of the group list and click [Add].



After you click [Add] the system will open the new group in add/edit mode.
There are three sections:

- Quota
- Access
- Members

10.7.2.1.1 Quota



The maximum space allowed for storage of e-mail.

When a user reaches 80 percent of the configured storage quota, he will receive a warning mail and all mail transfers for this user will be suspended. In the three days following the warning, the user will be able to store more files (for instance reordering messages or storing outgoing mail) as long as he doesn't exceed the full 100 percent of the quota. After three days with more than 80% quota usage, the only activity allowed will be to delete files until the storage usage goes below 80%. After that is achieved, all normal operations will be again possible.

10.7.2.1.2 Access

The CommBox software has different functionality on Vessel and HUB, some modules / functions are only available on vessel and some only on hub.

Modules available on HUB:

Access:

Area	Allow viewing	Allow operation(s)	Description
Dashboard	☑	☑	Connection status and controlling. Queue view and management.
Network Settings	☑	☑	Network interface, DHCP, DNS, Samba shares and general network settings.
Connection Profile	☑	☑	View and edit connection profiles.
File Transfer Restrictions	☑	☑	Control file transfer restrictions for user, groups and domain level.
System Operations	☑	☑	General system maintenance and operations.
QuickFile	☑	☑	View and edit QuickFile profiles.
Backup/Restore	☑	☑	Backup and restore of system configuration. Part of the System category above.
Users and Groups	☑	☑	Local users and groups settings.
Hosts	☑	☑	View and edit hosts settings like host name, IP address and DNS alias.
Miscellanous	☑	☑	
Cost Profiles	☑	☑	View and edit cost settings.
QuickMail	☑	☑	Configuration of CommBox mail server.
Webmail	☑	☑	Access to CommBox webmail client
QuickWeb	☑	☑	View and edit QuickWeb profiles.
QuickWall	☑	☑	View and edit QuickWall profiles.
Tools	☑	☑	Collection of troubleshooting tools.
Support Page	☑	☑	Tick of this one to allow the group to access Support page and other information pages.
System Monitoring	☑	☑	View and edit alert settings for events.
Hardware Settings	☑	☑	View and edit hardeware interfaces.
Fleet Management	☑	☑	This module/area only applies to the office hub. Do not tick of this when configuring a vessel Commbox.
QuickCrew	☑	☑	View and edit QuickCrew settings.
Configure	☑	☑	View and edit general QuickCrew settings
Crew accounts	☑	☑	View all crew accounts and reset password.
Remote refill		☑	Refill crew accounts remotely.
Crew Management RESTful API	☑	☑	Get and manipulate crew lists.
QuickMail Archive	☑	☑	This module/area only applies to the office hub. Do not tick of this when configuring a vessel Commbox.
OpenVPN Settings	☑	☑	

Modules available on vessel:

Access:

Area	Allow viewing	Allow operation(s)	Description
Dashboard	☐	☐	Connection status and controlling. Queue view and management.
Network Settings	☐	☐	Network interface, DHCP, DNS, Samba shares and general network settings.
Connection Profile	☐	☐	View and edit connection profiles.
File Transfer Restrictions	☐	☐	Control file transfer restrictions for user, groups and domain level.
System Operations	☐	☐	General system maintenance and operations.
QuickFile	☐	☐	View and edit QuickFile profiles.
Backup/Restore	☐	☐	Backup and restore of system configuration. Part of the System category above.
Users and Groups	☐	☐	Local users and groups settings.
Hosts	☐	☐	View and edit hosts settings like host name, IP address and DNS alias.
Miscellanous	☐	☐	
Cost Profiles	☐	☐	View and edit cost settings.
QuickMail	☐	☐	Configuration of CommBox mail server.
Webmail	☐	☐	Access to CommBox webmail client
QuickWeb	☐	☐	View and edit QuickWeb profiles.
QuickWall	☐	☐	View and edit QuickWall profiles.
Tools	☐	☐	Collection of troubleshooting tools.
Support Page	☐	☐	Tick of this one to allow the group to access Support page and other information pages.
System Monitoring	☐	☐	View and edit alert settings for events.
Hardware Settings	☐	☐	View and edit hardeware interfaces.
QuickCrew	☑	☐	View and edit QuickCrew settings.
Configure	☑	☐	View and edit general QuickCrew settings
Crew Login Page	☑	☐	View and edit Login page for crew and guest users
Voucher	☐	☐	Manage crew and guest vouchers.
Generate		☐	Allow to create new vouchers
Active accounts	☑	☐	List accounts and disembark crew users.
Reset password		☐	
Direct refill		☐	
Crew accounts	☑	☐	View all crew accounts and reset password.
HTS	☐	☐	View and edit HTS related settings

Permissionsï¿½are per group and defines theï¿½access to the different modules of CommBox. It is possible to define read/write permissions on a module and all its sub-modules. Attributes not explicitly defined, is inherited from the global (parent) entry's permissions.

Rules:

- Defining lower level permission require parent permission enabled
- Write permission require Read permission for each entry, except for events
- When a permission is de-selected it means that it is "Denied"
- Read/write on sub-module or event require permission on parent to be minimum Read

10.7.2.1.3 Members

Members:

Members	Not members
☑ John Doe (jdoe)	☐ administrator admin (admin)
	☐ Charles Mingus (captain)

To add a member to the group, check the corresponding box. Users that are already members will be listed in the "Members" column when the group is opened for editing.

10.7.2.2 Group edit

To update a group, click [Edit] next to the entry you want to update. This will open the add/edit view. See above for explanation of the various fields.

10.7.2.3 Group delete

To delete a group, click [Delete] next to the entry you want to delete. Click Yes in the dialog to confirm.

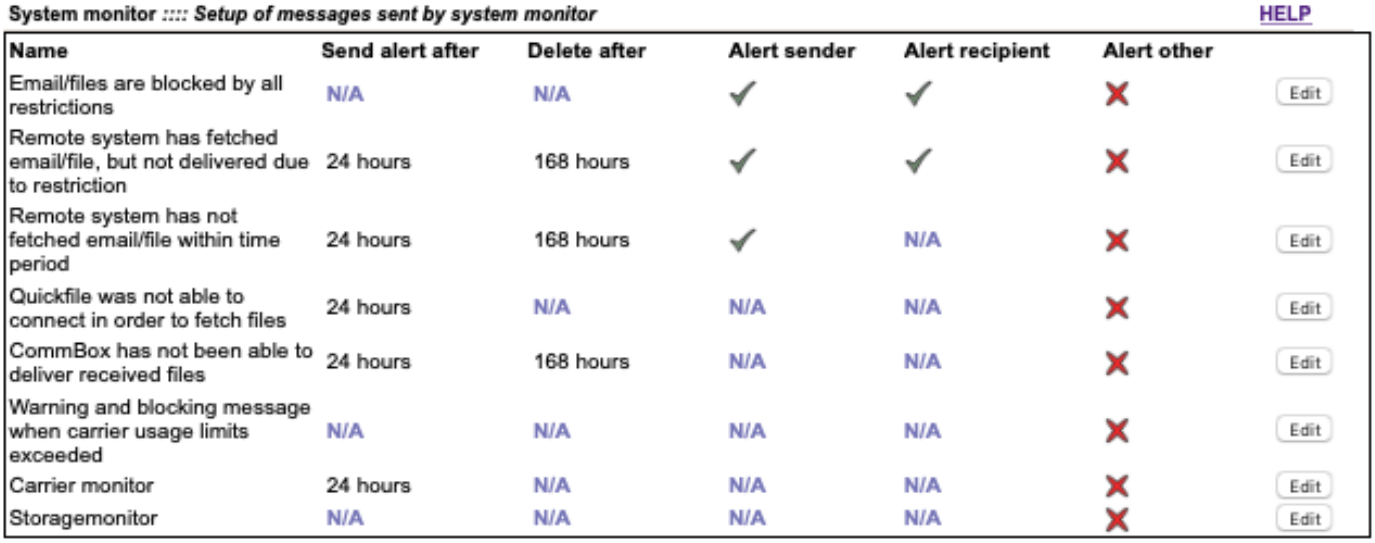
It is not possible to delete the 'administrators' group.

10.8 System monitor

In "Config->System monitor" you can define what notification to send when something prevents file exchange (be it because of a restriction profile or because of connection problems).

There are seven types of blockages handled:

1. Email/files are blocked by all restrictions.
2. Remote system has fetched email/file but not delivered due to restriction.
3. Remote system has not fetched email/file within time period.
4. QuickFile was not able to connect in order to fetch files.
5. CommBox has not been able to deliver received files.
6. Warning and blocking message when carrier usage limits exceeded.
7. Carrier monitor.

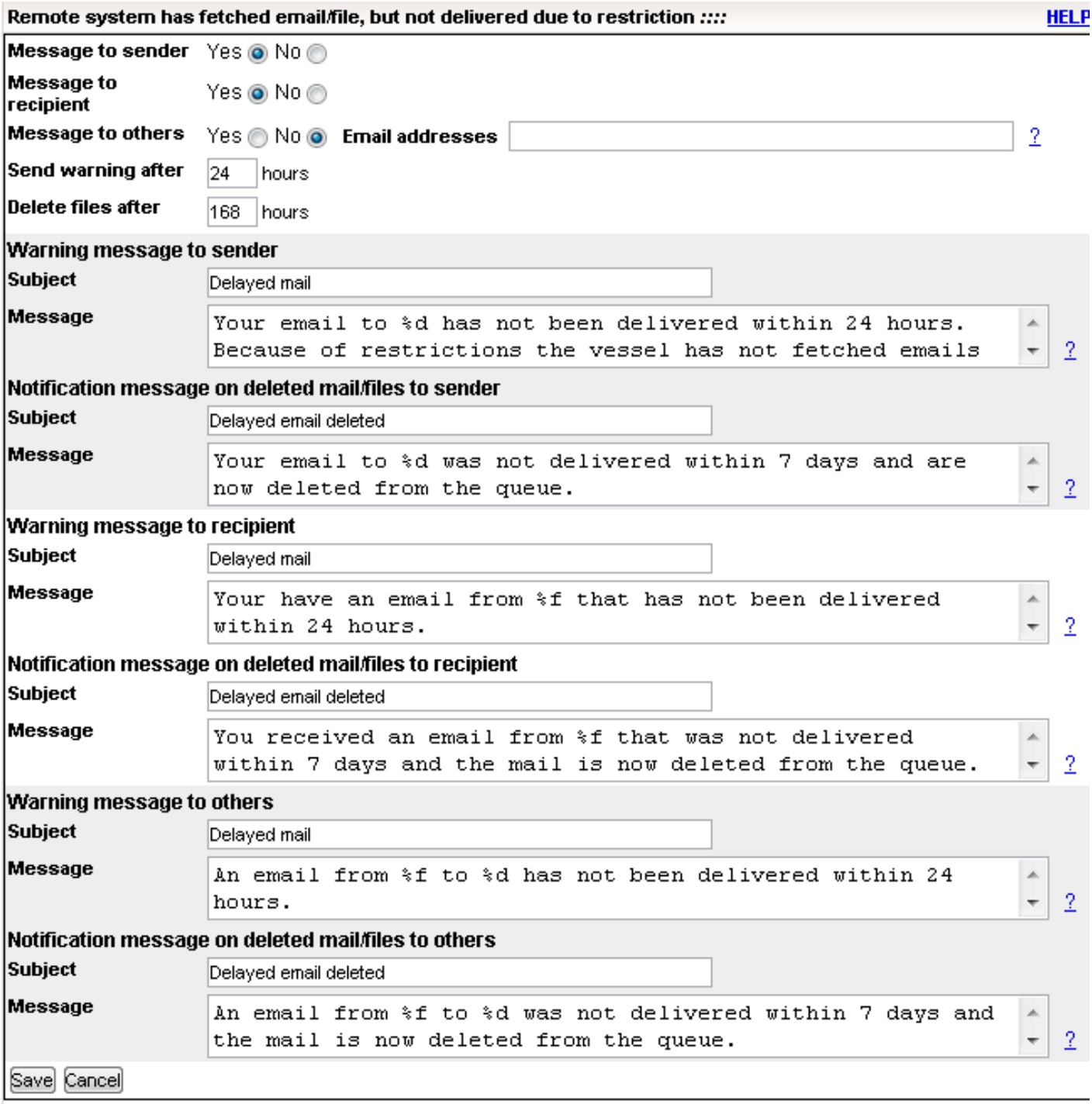


In most cases, a file is deleted after it has stayed blocked for a set time (i.e. if the reason why it was blocked has not been removed). Emails are sent both when a file is blocked and when it is deleted.
You can configure several parts of this process:

- Time after which a "file blocked" notification is sent.
- Time after which files are deleted.
- Whether or not to send notice to sender, recipient and/or others.
- Subject and message for each type of notification.

Whenever a time is configurable, setting a value of zero indicates that that part of the system is inactive. So, for example, a setting of "Delete after" 0 hours means that the file will not be deleted, rather than that it is deleted immediately.

The various categories have a variable number of configurable elements. The screenshot shown below is from “Remote system has fetched email/file, but not delivered due to restriction” which is the one with more options.



Most message fields give the possibility of entering special character combinations that will be replaced by information pertaining the message being blocked. The most widely used (there are differences between message types. For the complete list for a specific message field, hold your mouse pointer above the question mark to the right of the message field for a list) are:

- %s : subject.
- %f : from.
- %d : destination (to).
- %t : total size.
- %o : original size.
- %h : host name.
- %n : system name.
- %b : the entire original mail.

10.8.1 Email/files are blocked by all restrictions

In case the system finds that, because of restrictions, no carrier will ever transfer a mail or file, this will trigger the “Email/files are blocked by all restrictions” functionality.

It is possible to alert sender, recipient, and others.
It is also possible to make the CommBox delete the mail/file from the queue immediately to avoid using up space.

10.8.2 Remote system has fetched email/file but not delivered due to restriction

This applies when a file has been blocked in the outgoing queue because of restrictions linked to the carrier in use. However, the system has found that there are carriers which can transfer the file but these have not been active.

It is possible to set a "Send warning after" time and a "Delete files after" time. Alerts can be sent to sender, recipient, and others both after block and after deletion.

10.8.3 Remote system has not fetched email/file within time period

This is triggered when a mail/file is not transferred in a specified amount of time but it is still not marked as stopped by the restriction system. The vessel may simply be out of reach for its communication systems or may not have connected if only connecting manually.

It is possible to set a "Send warning after" time and a "Delete files after" time. Alerts can be sent to sender and/or others both after block and after deletion.

10.8.4 QuickFile was not able to connect in order to fetch files

This applies when the CommBox is configured to have QuickFile pick up files from a file server and it cannot reach the file server for a specified amount of time.

It is possible to set a "Send warning after" time. An alert can be sent to a specified address.

10.8.5 CommBox has not been able to deliver received files

This function is triggered if the CommBox has fetched files/mails from the other side but cannot pass them to their destination. This usually occurs if a file server is unreachable.

It is possible to set a "Send warning after" time and a "Delete files after" time. An alert can be sent to a specified address.

10.8.6 Warning and blocking message when carrier usage limits exceeded

When a carrier is configured with a "Usage max limit" it is possible to set up the CommBox to send a mail when 80 % of specified amount is reached, and when the carrier (connection profile) is blocked (i.e. when the limit is reached).

10.8.7 Carrier monitor

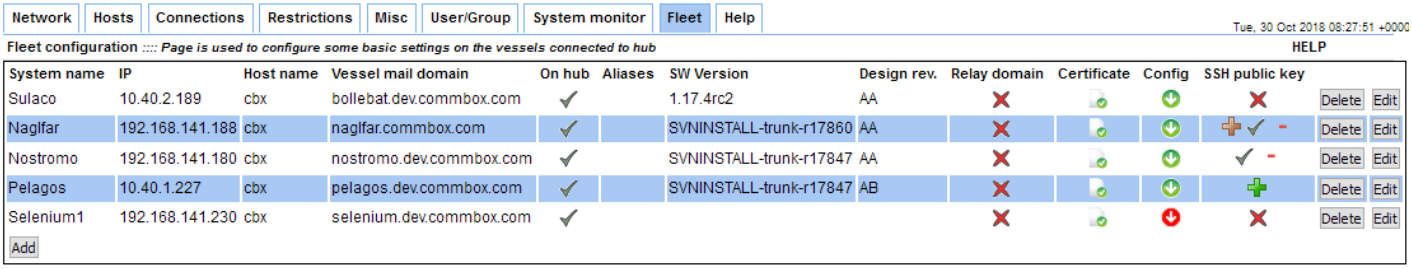
When a carrier different from the one with highest priority is used for more than the time specified in "Send warning after", a message will be sent.

10.8.8 Storage monitor (hub)

Define how and whom to warn about low disk space.

10.9 Fleet (hub)

The fleet page is reached from "Config->Fleet". From here you can perform basic configuration and maintenance of vessels. The page displays a list of all the vessels known to the hub.



System name
: a freely selectable name to recognize vessels.

IP
: the main ip of the vessel's CommBox. This is the ip used as identification on the hub when transferring files or performing routing.

Hostname
: the host name given to the CommBox in question.

Vessel mail domain
: the mail domain which will be relayed to the vessel and transferred via the CommBox file transfer system.

On hub
: shows the result of a set of basic checks performed on the hub. If you see a green check mark here, it means that the hub has found the host in the host list and that it recognizes the vessel machine. If there is a red X here, you cannot expect the machine to be able to transfer files and receive mail properly.

Aliases
: the alias specified in the host configuration for the vessel machine (if any).

SW version
: the vessel CommBox software version number.

Fleet design revision
: If filled in on vessels, this field can be used to keep track of the different configuration layouts in use on the fleet.

Relay domain
: whether or not the hub will relay mail to the vessel's mail domain when the mail arrives from Internet or any other net not in the trusted networks list. An X implies that the hub will not permit such mail, it is permitted in the field instead contains a V.

Certificate
: whether or not there is an OpenVPN certificate generated for the vessel in question. All vessel machines that connect to the hub via OpenVPN will need a certificate to do so. A gear icon indicates that no certificate exists. You can click on it to generate a new certificate.

Config
: click on the icon to download a configuration file from the vessel in question. This configuration may be restored on another vessel machine, it will then be an exact duplicate of the vessel in question.

SSH Public Key
: Approve and revoke SSH public key used by vessel to connect to the hub. This key is part of a key-pair generated on the vessel and is used when the vessel connects to the hub. The key is transferred to the hub as part of the configuration archive.

	SSH Public Key is received from vessel, and needs to be approved before it can be used for authentication.
	SSH Public Key is in use by the vessel to connect to hub, revoke by clicking the (-) minus icon. If revoked, vessel will no longer be able to connect to hub.
	When the "Approve" icon turns brown, it indicates that a new key or at least; different than the one in use, is available from the vessel. This can happen if a new key-pair is generated on vessel, or if someone have tampered with the key. *If you are unsure, please verify that a new key has been generated on the vessel before approving this new key.* To approve the new key, first revoke the current, before

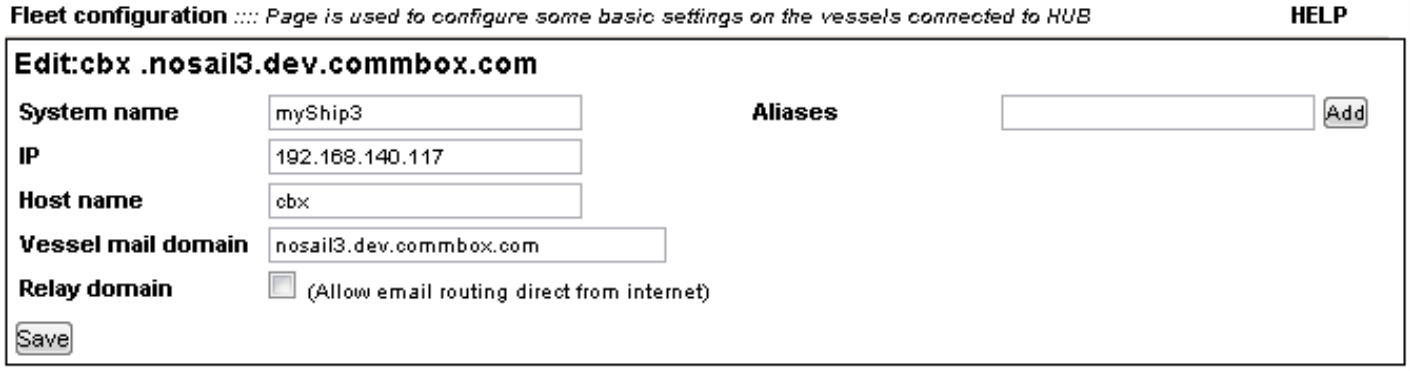
	approving the new. Approve icon is locked until the current key is revoked.
✖	No SSH public key is available, vessel need to send configuration to be able to use SSH key authentication.

Delete

delete entries from hosts and from QuickMail regarding the vessel in question. It will also delete the configuration directory for the vessel on the hub.

Edit

brings up a new view from where you can edit most of the parameters explained above:



10.10 SSL (hub)

When accessing a system from our browser, we depend on certificates to verify that the system is who it claims to be. Certificates are issued by a trusted third party, which has verified that the system requesting the certificate is in fact in control of the domain name and the connected system.

On CommBox it is possible to choose among two types of certificates.

Default certificate

This certificate is installed together with the rest of the CommBox software and is issued to the following domain names:

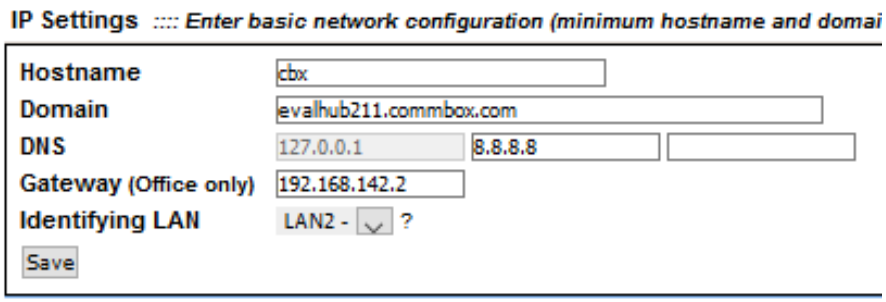
DNS Name: *.ipmobilecast.com
DNS Name: *.commbox.com
DNS Name: commbox.com
DNS Name: ipmobilecast.com

If the domain name used to reach the system differ from >myhub<.ipmobilecast.com or >myhub<.commbox.com, browser will issue a warning that the page is insecure.

Let s Encrypt certificate

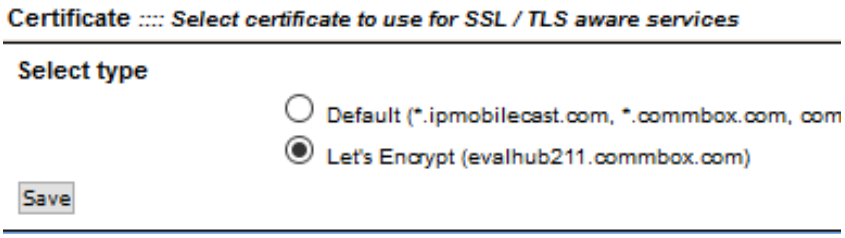
To use certificates issued to a specific domain name CommBox also implements the certificate service provided by Let s Encrypt. This service will create and signed a custom certificate, issued to a specific domain name within seconds. This certificate is used by the CommBox web server to provide a secure and verified connection to the CommBox user interface.

To be able to use this service the CommBox hub system must be reachable from the Internet when using the domain configured in **Config > Network > IP Settings: Domain.**



In this verification process Let s Encrypt will connect to the CommBox Hub system on port 80 (HTTP) and port 443 (HTTPS), so to use this functionality, these ports need to be available from the Internet. In addition, the domain used in the certificate must be registered in the domains authoritative DNS server.

CommBox Hub is preconfigured to use the default certificate, but the two types of certificate are easily configurable from **Config > SSL page**

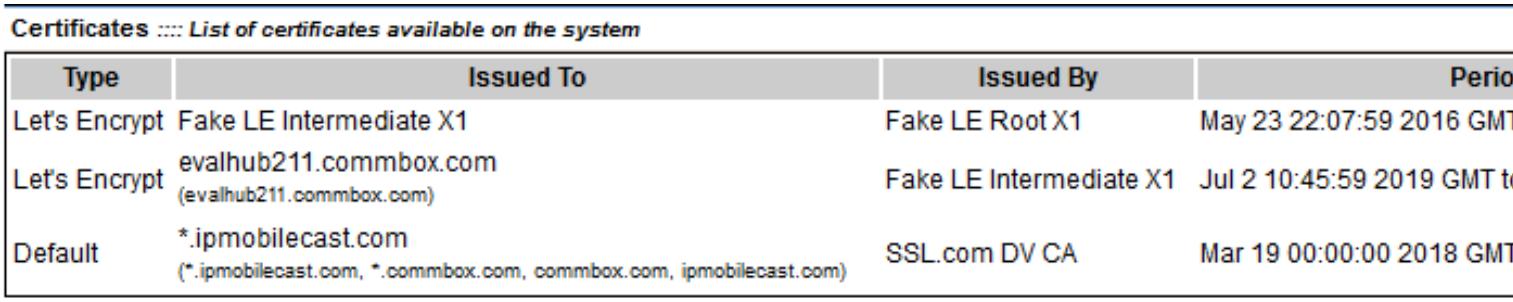


To switch to Let s Encrypt to get custom certificate, select Let s Encrypt and click save.

CommBox will create a server key and a certificate request, request is signed by the servers private key and then the request is sent to Let s Encrypt server for validation. Communication is done according to protocol, and if validation is successful, Let s Encrypt will sign a certificate that is returned to the CommBox server. This certificate will now be used instead of the default CommBox certificate, whenever a HTTPS connection is set up by Apache.

List of certificates

Further down the page we find an overview of the certificates available in CommBox. List contains the domain the certificate is issued to, the name of the issuer and the period of validity. List also shows which of the certificates that are in use by the web server. This certificate will have a green check mark in the web column. Only one certificate will be in use by the web server, so the rest of the certificates will be left blank, showing that certificate isn t in use.



Checklist

Domain
: Domain used in Let's Encrypt certificate is configured in Domain (Config > Network)

DNS
: For Let's Encrypt to be able to verify the domain, the domains authoritative DNS server must point to the CommBox hubs IP address.

Port 80 and 443 open
: CommBox hubs web server must be available for connections from public web. Let's Encrypt service uses both port 80 and 443 to verify that the domain you are requesting a certificate for is connected to a server controlled by you!

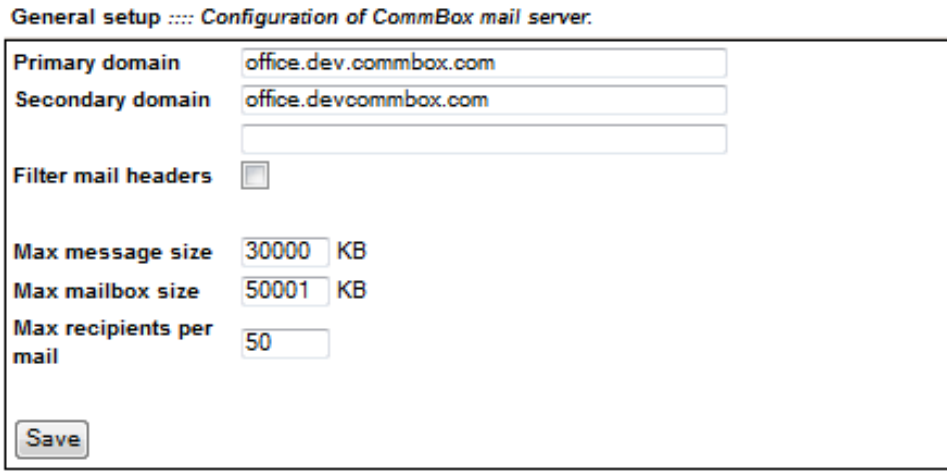
11 QuickMail

QuickMail is the mail system on the CommBox.

On the hub it is responsible for: forwarding mail to the vessels, sending mail to the office mail server or storing them locally. On the vessel it is responsible for: forwarding mail to the hub, relaying mail to an on-board mail server or deliver locally to an user account. On both hub and vessel it can automatically fetch mail from an external account and deliver it to another email account.

11.1 QuickMail Setup

From the Setup tab you can set the basic configuration options.



Fields description

Primary domain

The primary mail domain for the mail server on the CommBox. All mail sent to addresses in the primary domain will be delivered locally to users on the CommBox.

Secondary domain

Secondary domains are also considered as local mail domains on CommBox. All mail with any of the secondary domains will be delivered locally to users configured on the CommBox. This parameter is optional. You can add as many secondary domains as you want: each time you enter a domain and save, a new empty field is added to the form.

Filter mail headers

Unnecessary mail headers can be filtered out from any mail sent through QuickMail. This reduces the amount of data to be transferred. The headers which are left in a mail are:

- from
- to
- X-Priority
- subject
- Reply-To
- importance
- Content-Type
- MIME-Version

Trusted network

The IP ranges for mail clients and mail servers that are allowed to relay mail through the CommBox. Networks must be entered in CIDR notation (a.b.c.d/n).

Max message size

The maximum message size that the CommBox mail server will accept when delivered with the SMTP protocol or when fetching mail.

Max mailbox size

The maximum size of users' Inbox. This is the mailbox where messages are first delivered. The user may

create his own folders and move messages there. The cumulative size of the inbox and user-created folders is regulated by the quota system. This setting is present only on CommBoxes that use the SquirrelMail webmail system.

Max recipients per mail
: The maximum number of recipients in one mail transfer. You can have more recipients than the maximum, in this case you will see two or more mails sent with the same subject but having different recipients.

11.1.1 QuickMail setup examples (vessel)

There are 2 main configuration schemes for QuickMail setup on vessel. In one, the CommBox is the primary mail server on board. In the other, there is a dedicated mail server on board. In both cases mail not addressed to users on the vessel will be sent to the CommBox on shore side.

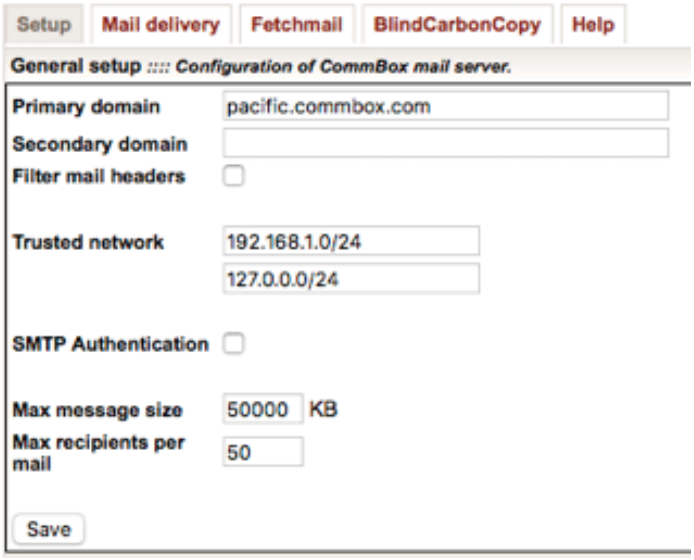
CommBox as primary mail server
: CommBox is the primary mail server on board. Mail clients send and receive mail directly through the CommBox and are located on the IP network 192.168.1.0/24. All mail not destined to local users is relayed to the CommBox on shore side.

11.1.1.1 Example setup:

- ◊ Mail domain on vessel: pacific.commbox.com
- ◊ IP network on vessel: 192.168.1.0/24
- ◊ CommBox on shore side: office.commbox.com

'pacific.commbox.com' is set as Primary domain. It is the only mail domain on vessel so no Secondary domain is configured.

All mail clients are located on the IP network '192.168.1.0' with netmask '255.255.255.0'. This sub network is added as trusted network in CIDR notation '192.168.1.0/24'.



All mail not local on vessel must be sent to shore. Set shore side CommBox 'office.commbox.com' as Default mail relay in "QuickMail->Mail delivery". The host office.commbox.com must be defined on the "Config->Host" page with type 'CommBox main hub'. The "Default mail relay" drop-down lists all hosts defined as type 'CommBox hub', 'CommBox main hub', or 'Mail server'.

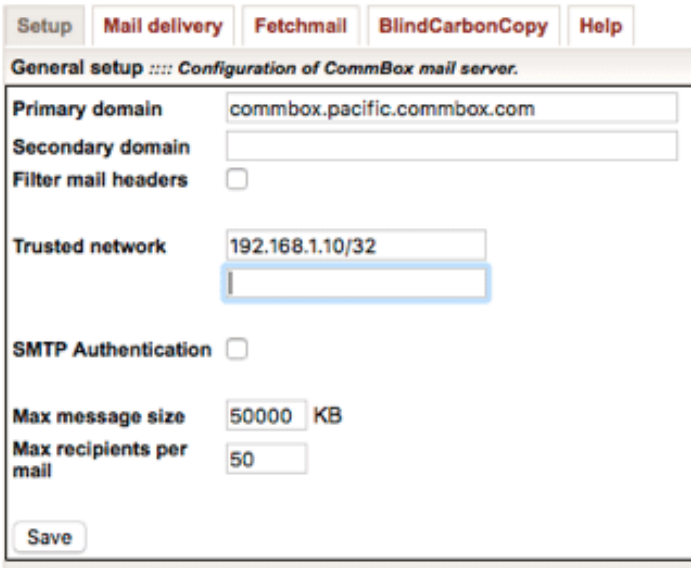
CommBox with external mail server
: CommBox can relay mail to and from external mail servers on board the vessel. All mail not destined to local users is relayed to the CommBox on shore side.

11.1.1.2 Example setup:

◊ Mail domain on vessel: pacific.commbox.com
◊ Mail domain for CommBox: commbox.pacific.commbox.com
◊ IP for external mail server: 192.168.1.10
◊ Name for external mail server: mailserver.pacific.commbox.com
◊ CommBox on shore side: office.commbox.com

CommBox is not the primary mail server on vessel so Primary domain must be set to something else than the mail domain for vessel. Here it is set to commbox.pacific.commbox.com.

There are no mail clients allowed to directly relay mail through CommBox, the only machine that is allowed to relay mail to the CommBox is the mail server. Trusted network is therefore set to be the IP of the vessel mail server in CIDR notation.



All mail not destined to local users must be sent to the CommBox on shore side. Set shore side CommBox 'office.commbox.com' as Default mail relay in "QuickMail->Mail delivery".

To relay all local mail from the CommBox to the vessel mail server, a mail rule must be defined.

The Domain/rule is '@pacific.commbox.com' which is the mail domain for the vessel. The Host is the vessel mail server 'mailserver.pacific.commbox.com'. This will route all mail from CommBox that has recipient matching '@pacific.commbox.com' to the vessel mail server.

11.1.2 QuickMail setup example (hub)

In this setup, a mail server on the shore side relays all mail for vessels to the hub CommBox. The CommBox relays all mail from the vessels to the mail server.

There are 3 vessels that will exchange mail with one shore CommBox

1. Vessel Pacific

- Has mail domain @pacific.commbox.com
- Mail structure: user@pacific.commbox.com
- Example mail address: master@pacific.commbox.com

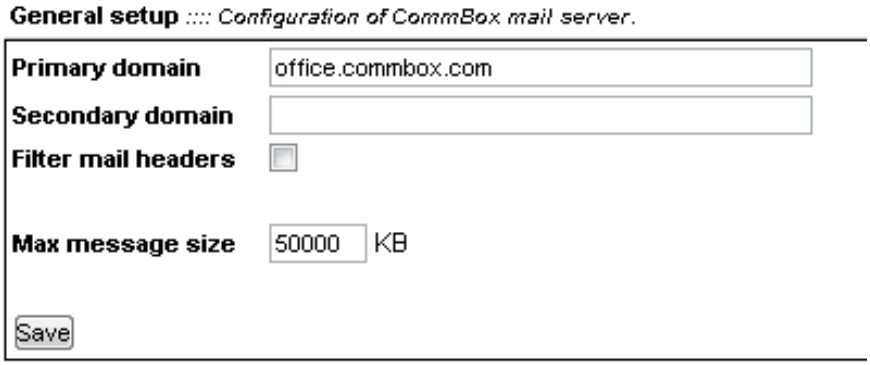
2. Vessel Atlantic
   - Has mail domain @vessel.commbox.com
   - Mail structure: user.atlantic@vessel.commbox.com
   - Example mail address: master.atlantic@vessel.commbox.com
3. Vessel Ocean
   - Has mail domain @vessel.commbox.com
   - Mail structure: user.ocean@vessel.commbox.com
   - Example mail address: master.ocean@vessel.commbox.com

Atlantic and *Ocean* have the same email/domain scheme.

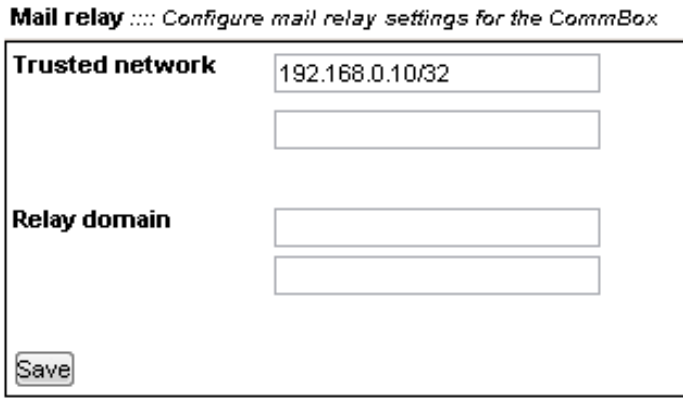
Usually all vessels in a fleet have the same email/domain scheme. This is only an example to show the different possibilities.

Mail server setup

The CommBox must be setup to relay mail between vessels and the office mail server in both directions.



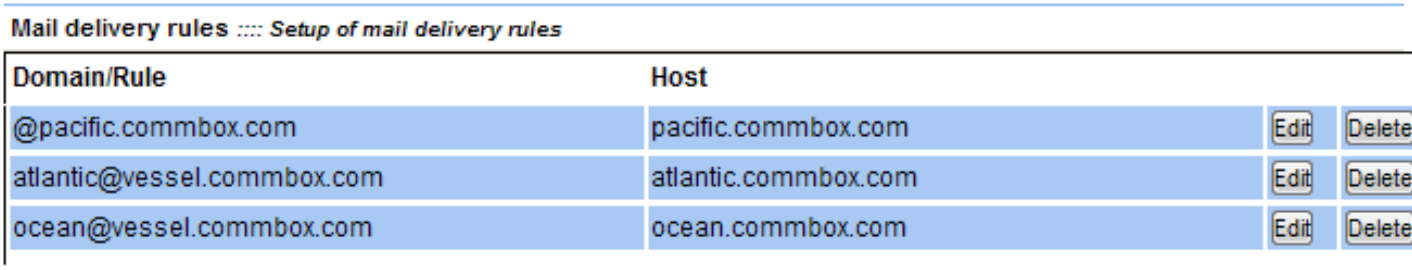
Primary domain is set to 'office.commbox.com' so that it does not interfere with the company's mail system.



Trusted network is set to 192.168.0.10/32 which is the IP address of the external mail server 'mailserver.commbox.com'. Only this host is allowed to relay mail through the shore CommBox.

Mail delivery

The mail delivery defines the default mail relay and specific mail relay rules that checks the recipient address against the Domain/rule field. If it matches, 'Host' defines the next hop for the mail.



The rule '@pacific.commbox.com' matches all mail addresses that end with @pacific.commbox.com. All these will be forwarded to the pacific.commbox.com vessel.

Examples of matching mail addresses:

- ◊ master@pacific.commbox.com
- ◊ chiefeng@pacific.commbox.com

The rule 'atlantic@vessel.commbox.com' matches all mail addresses that end with 'atlantic@vessel.commbox.com'. All these will be forwarded to the atlantic.commbox.com vessel

Examples of matching mail addresses:

- ◊ master.atlantic@vessel.commbox.com
- ◊ chiefeng.atlantic@vessel.commbox.com

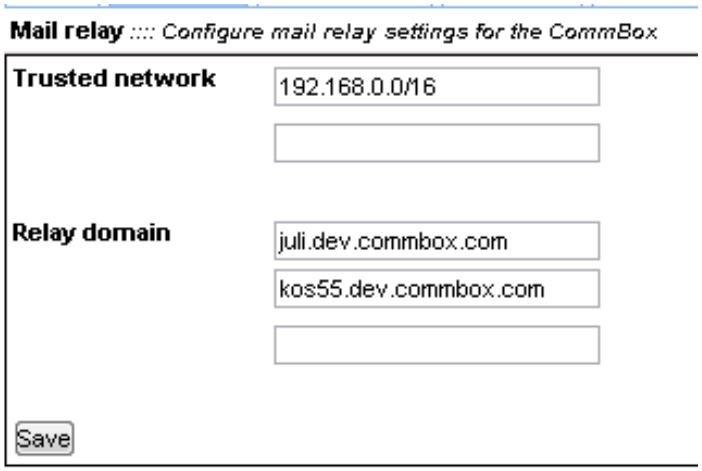
The rule 'ocean@vessel.commbox.com' matches all mail addresses that end with 'ocean@vessel.commbox.com'. All these will be forwarded to the ocean.commbox.com vessel

Examples of matching mail addresses:

- ◊ master.ocean@vessel.commbox.com
- ◊ chiefeng.ocean@vessel.commbox.com

11.2 Mail relay (hub)

The mail relay setup is only available in the hub version of the CommBox. It is used to control which networks and domains are allowed to relay mail through the CommBox.

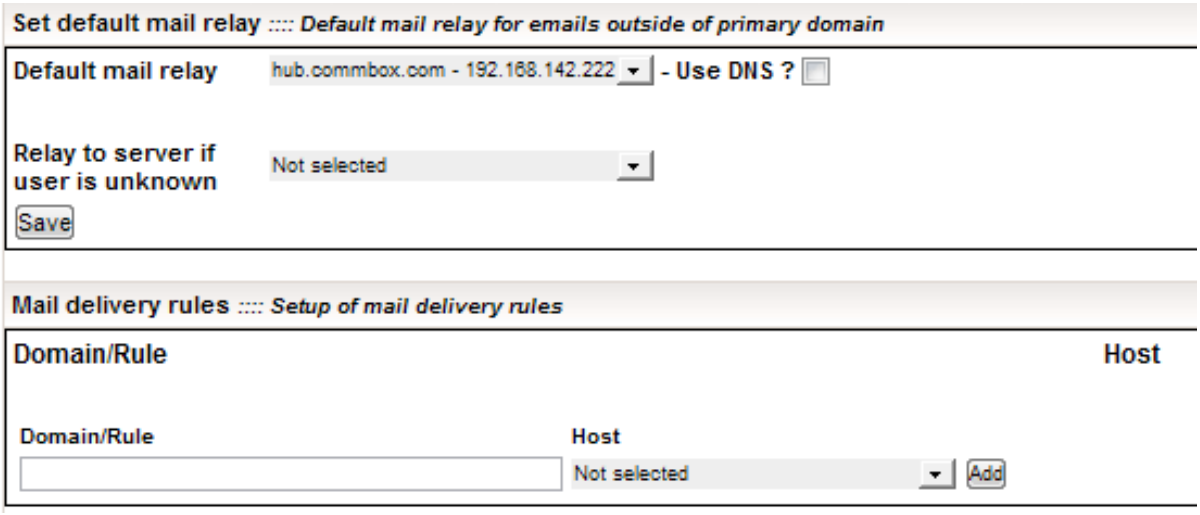


Trusted network
: Email clients from these networks are allowed to relay email through the CommBox.

Relay domain
: The recipient domains for which the CommBox will relay mail. Mails to these domains will be relayed even if the client is not on a trusted network.

11.3 Mail delivery

Mail delivery configures specific mail routing schemes based on a domain or rule.



Default mail relay
: The host that will be used when mail is not local and no specific mail routing scheme matches. On vessels this is usually the shore CommBox, on office CommBoxes it is usually the company's mail server. The host must be registered in "Config->Hosts" with type CommBox hub or mail server.

Use DNS
: This overrides "Default mail relay". When set, the CommBox will deliver mail using DNS lookups. It is usually only used on shore side.

  DNS servers must be configured in "Config->Network".

Relay to server if user is unknown
: If the CommBox does not know the destination user, the email will be relayed to this server.

11.3.1 Mail delivery rules

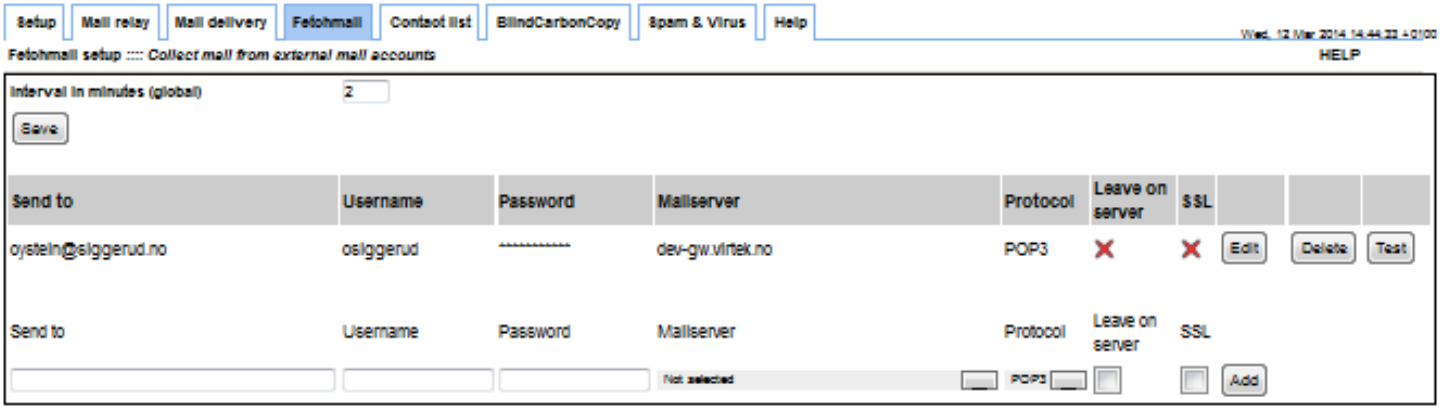
Domain/rule
: A full email address or part of it. If it matches the recipient address, the message will be relayed through the defined host.

  The rule is matched against any part of the address e.g. 'me@commbox' will match 'me@commbox.com' and 'game@commbox.net', 'commbox' will match 'me@commbox.com' as well as 'commbox@some.domain'.

Host
: The host to which the mail is relayed if it matches the rule. The host must be registered in "Config->Hosts" with type CommBox hub or mail server.

11.4 Fetchmail

Fetchmail automatically retrieves mail from an external account and delivers it to another email account. This allows users to receive mail from their own personal accounts through the CommBox webmail interface.



Send to
: The address to which the email will be forwarded. Only one address can be set for each rule.

Username
: The username of the mail account from which mail will be retrieved.

Password
: The password of the mail account from which mail will be retrieved.

Mail server
: The mail server where the mail account is hosted. The server must be registered in "Config->Hosts" with type CommBox hub or mail server.

Protocol
: The protocol that will be used to retrieve mail from the mail server. Available protocols are POP3 and IMAP.

Leave on server
: Whether to instruct the external server to not delete mail after it has been fetched. If enabled, mails can still be retrieved from the original server at a later date.

  Some servers do not respect this instruction and will always delete mail as soon as it is read regardless of what you set here. This is beyond the control of the CommBox. If you want to be sure to keep a copy, you may want to check whether the Blind carbon copy functionality can help you (see Blind carbon copy setup).

SSL
: Enables encrypted communication to the mail server. This is sometimes also called secure communication.

11.5 Contact list (hub)

From the hub it is possible to manage a list of e-mail contacts to be distributed to the webmail system of all the ships in the fleet. Every time a new list is loaded, the new data is distributed to all the vessels in the fleet. To reduce the amount of data transmitted, only the differences with the previous list will be sent.

11.5.1 Contact list management

From "QuickMail->Contact list" you access the contact list management form.

The CommBox can only import and export a CSV file of all the contacts, the actual editing of the list (adding, editing, removing contacts) must be done in an external program that can work with this format of file (typically OpenOffice Calc or MS Excel).

See Appendix: Fields in the contact list file for a more detailed description of the file format.

Import from file
: Imports a contact list from a CSV file.
  Once the file is uploaded you will be given a preview of the information that the CommBox extracted from the file.
  If this is what you expected you can then click [Save] and the list will be saved.
  The new contacts will be distributed to the fleet when you click [Activate changes].
  It is possible to import an empty contactlist to remove all existing contacts.
  See below for a description of the file format required.

Download
: You can download a CSV file containing the full list of contacts, or you can download a template containing only one row with all the field names.

Distribute to vessels
: The contact list is distributed to all registered vessels when a new file is uploaded. If a new vessel joins the fleet, you can force a transfer of the full contact list. For safety [Send] is disabled, to activate it check the box next to it.

11.5.2 View the contact list

To view a list of the contacts currently in the system click on "Show contacts" below the "Manage the contact list" panel. It is not possible to edit or search contacts from this view.
Only a limited number of fields will be displayed for each contact.

11.6 Blind carbon copy setup

11.6.1 Overview

Blind carbon copy will forward to a third party mail passing through the CommBox. You define which messages will be forwarded to which address by setting up rules based on the sender or recipient address.

11.6.2 Filter rules

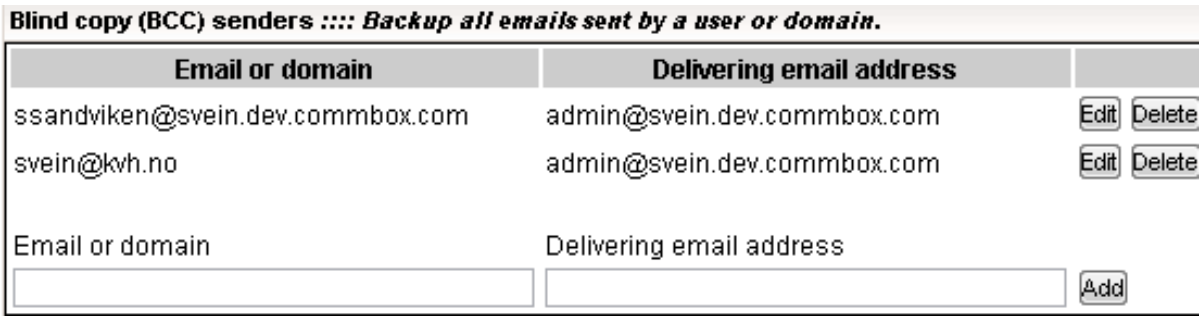
The following filtering rule types are accepted by the system:

- username@domain.test
- username
- domain.test

Rules set up in the "Blind copy (BCC) senders" panel will try to match the address of the sender, rules in "Blind copy (BCC) recipients" panel will try to match the address of the recipient.

11.6.3 Examples

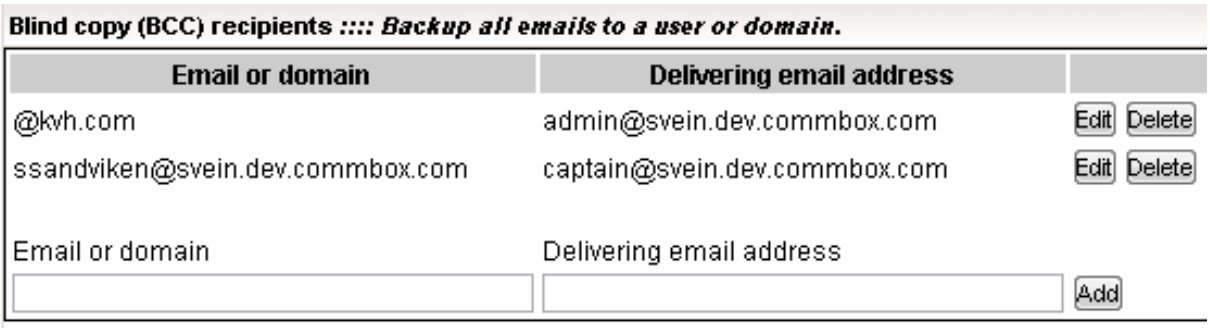
11.6.3.1 Senders



Emails with sender addresses or domain matched here will be sent as blind copy to the administrator ("admin@svein.dev.commbox.com").

1. All emails sent by "ssandviken@svein.dev.commbox.com" are blind copied to "admin@svein.dev.commbox.com"
2. All email sent by "svein@kvh.no" are blind copied to "admin@svein.dev.commbox.com"

11.6.3.2 Recipients



All emails with a recipient that matches the filter will be blind copied to different delivering addresses.

1. All emails sent to users in the "@kvh.com" domain will be blind copied to the administrator.
2. All emails sent to "ssandviken@svein.dev.commbox.com" will be blind copied to the captain.

11.7 Webmail clients

New CommBox installs have the SOGo web email client. See Appendix: SOGo for more information.

Older upgraded CommBoxes may have either the 'WebApp' or 'WebAccess' email client from Zarafa (www.zarafa.com). For more information see Appendix: Zarafa

Very old CommBoxes that have been upgraded may still use the old SquirrelMail email client. For more information see Appendix: SquirrelMail

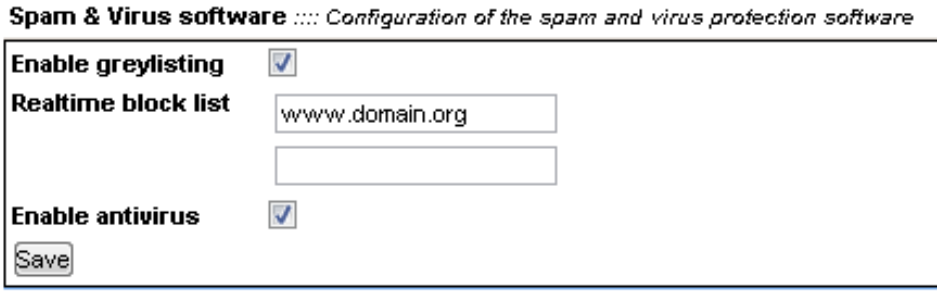
11.8 Connecting an external email client

The CommBox acts as a mail server and external mail clients (e.g. Outlook) can connect directly to it using either IMAP or POP protocol. Use the CommBox IP address for both incoming and outgoing mail. Username and password are the same as those for your CommBox account.

Note that the IMAP folder for sent messages is called "Sent Items" instead of the more common "Sent". Some email clients will not work properly unless they are explicitly configured to use the "Sent Items" folder for sent messages.

11.9 Spam & virus (hub)

The hub version of the CommBox is delivered with integrated software for virus and spam control.



Enable greylisting

Greylisting is a technique used to reduce the amount of spam mail reaching users. In short, greylisting works like this:
The first time CommBox receives email from an unknown domain, it will reject the message with a "temporary reject" message to the sender email server.
The sender mail server will then resend the email after a short while. At this point, the CommBox greylisting system knows about the domain that sends the email and will deliver it to its internal email system.
The reason for this “first time reject”, is that most spam email servers only send the message once. If it is rejected, they won't bother trying again.

Greylisting is used for email reaching the CommBox from the Internet, it has no effect on email coming from trusted networks.

Real time black list (RBL)

The CommBox can be set up to use RBLs, which are on line services that provide lists of IPs and domains linked to spamming. Email sent from these servers will be rejected.
Enter the address of the list provider(s) you want to use. Providers of blocklists are, for example: *http://www.spamhaus.org/ and http://www.spamcop.net/.*

Enable anti-virus

Clam is the antivirus software on CommBox II HUB. If enabled, CommBox will run all incoming emails through a virus scanner. The virus software will be updated automatically every day.
See *Virus software update log* for update details.

The software may be outdated and therefore disabled. Please contact KVH Support for more information and upgrade options.

12 QuickFile

QuickFile is a module used for synchronizing files from one server to another.

The operating principle is simple: you define a source folder and a destination folder (these usually reside on two different servers). The CommBox will then periodically check the source folder for changes, any new or changed file will then be transferred to the destination folder.

The files are automatically compressed and transferred at the next scheduled transfer. Further reduction in network traffic may be achieved by using the differential file synchronization option which transfers only the modified parts of a changed file.

Features:

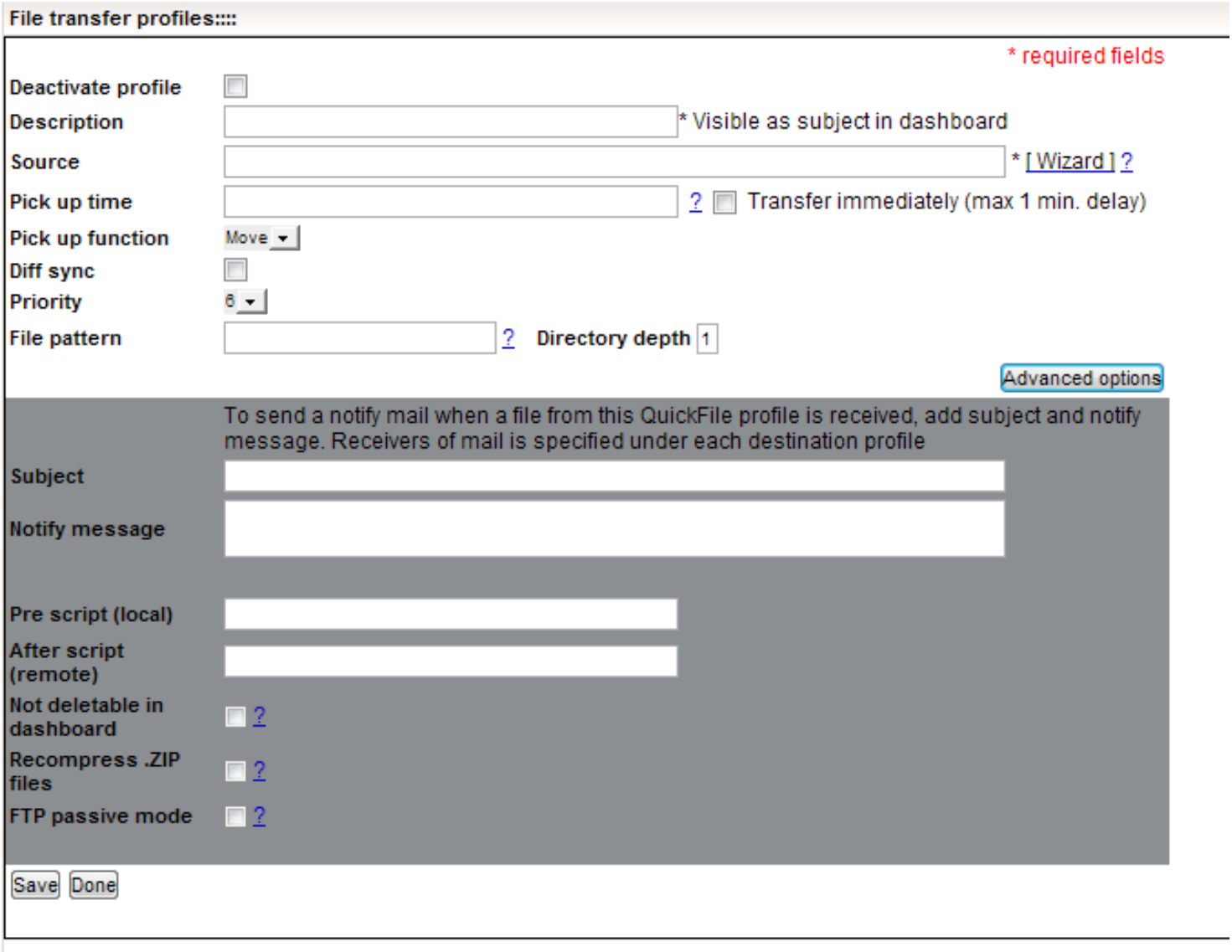
- Time based synchronization: you can define at what time(s) the transfer will take place.
- Pre and After scripts for data manipulation.
- Multiple recipient for a single source. Useful, for example, to spread anti virus updates.
- Transfer files as email attachments.
- A choice of either moving or copying files.
- Differential synchronization at the binary level.
- File selection based on multiple masks and sub levels.
- Supported transfer protocols SMB/CIFS/FTP and NFS.
- Customized user notification of file delivery.

You can use the source folder as a post box: every file dropped there will be automatically transferred to the designated recipients.

You can use external programs to transfer files to the source folder. For example reports, databases files, logs etc.

12.1 Adding a new profile

Click [Add] in the QuickFile overview page. The following page will appear. (The panel with gray background will appear only after you click [Advanced options])



Deactivate profile

Renders the profile inactive. Useful if you want to re-activate it later.

Description

Gives the profile a name. This will only be used in the QuickFile overview.

Source

The directory from where files should be picked up. Use the wizard to get the correct syntax (see Source / Destination wizard in this manual).

Pick up time

Define when and/or how often files in the source directory should be picked up.
If this field is left empty, this profile is deactivated.
If "Transfer immediately" is checked, QuickFile will look for files every minute.
Format examples:

'10:00, 11:00, 12:00, 13:00'

Run at 10:00, 11:00, 12:00 and 13:00 every day

It is possible to define a periodic pickup by using the '+' symbol before the number of minutes defining the frequency.

'10:05+15'

Run every 15 minutes starting at 10:05 (10:05, 10:20, 10:35...)

'+30'

Run every 30 minutes all day.

'08:05-16:05+60, 16:05-08:05+120'

Run every 60minutes between 08:05 and 16:05, between 16:05-08:05 every 120 minutes.

Pick up function

Select whether you want to move (files will be removed from the origin directory once they have been transferred) or copy (files will remain in the origin directory, files that have been already transferred will not be transferred again).

Diff sync

Enables differential synchronization.
This is a very useful tool which reduces the amount of data to be transferred: if the content of a file changes after it has been transmitted, then only the differences will be sent with then next transfer.
This is particularly effective with files to which content is continuously added (for example logs, virus definitions, databases etc.)
Please note that when *Diff sync* is unchecked (not in use) the directory "/home/storage/share/'sharename'/.diffcompare" will still exist and has to be removed manually to release space.

Priority

The priority assigned to the transfer files when they are placed in the outgoing queue. The default for QuickFile is 5 (1 is the highest priority).

File Pattern

Defines which files in the directory will be considered for transfer. You can specify more than one pattern by entering a comma separated list e.g.: "*.doc,*.xl?,*.db,*.DB".
Note that patterns are case-sensitive, so "*.db" is different form "*.DB".
If the field is left blank, all files in the directory will be considered.
Pattern rules:

To define a pattern, you can use two wildcard characters: '*' and '?'
"*" - matches any number of any character:

"*report.txt" will match any file name that ends in "report.txt", for example: "user-report.txt", "important-report.txt" and also "report.txt".

"*report*" will match any file name containing the word "report", for example: "user-report.txt", "user-report.doc", and also "report".

"re*.txt" will match any file name beginning with "re" and ending with ".txt", for example: "report.txt", "regenerate.txt" and also "re.txt".

"?" - matches any single character:

"report?.txt" will match any file name that begins with "report", then has one character, and then ends with ".txt": "report1.txt", "reportA.txt", "report#.txt". It will NOT match "report.txt".
"report.do?" will match "report.doc", "report.dot", "report.dom" etc.

Directory depth

How deep in the sub folders should the CommBox descend to find files.
If left empty, all sub folders will be considered.
If set to 0 (zero) only the files in the source directory will be considered.
If set to 2 the CommBox will descend down to level 2 sub folders.
Examples:

Considering this folders structure (where logs/ is the source folder):

```
logs/
logs/users/
logs/users/crew/
logs/users/crew/active/
logs/users/crew/old/
```

With a depth of 1, all files in logs/ and logs/users/ will be considered.
With a depth of 2, all files in logs/, logs/users/, and logs/users/crew will be considered.
With an empty depth parameter, all files in logs/, logs/users/, logs/users/crew, logs/users/crew/active/, and logs/users/crew/old will be considered.

Advanced options

Subject

The subject that will be displayed in the file queue list in dashboard.
It is a good way to differentiate various transfers and help the administrator to, for example, decide whether to allow a large transfer.

Notify message
: If one or more notification emails are defined in the destination profiles, this is the body of the message that will be sent.
This is a good way of reminding the recipient what to do with the files. For example: "Updates from ship Victorious, please load in the database"

Pre script (local)
: A script to be executed before the files are processed, see, 'Pre and After scripts' for a description of the available scripts.

After script (remote)
: A script to be executed on the destination CommBox after the files have been received, see 'Pre and After scripts' for a description of the available scripts.

Not deletable in dashboard
: If enabled, it will not be possible to delete the transfer files from the outgoing queue.

Recompress .ZIP files
: If enabled, the CommBox will compress files packed in uncompressed .zip archives. This often results in a smaller transfer over the network.

FTP passive mode
: Force the CommBox to connect to the FTP server in passive mode.

When finished, hit [Save].

Remember that the profile is deactivated if the action time is not set.

To test the profile, use the test button in the profile overview. See Toolbox functionality in other modules for how this test works.

12.1.1 Pre and After scripts

These are standard scripts that can be executed in the share directory of the source CommBox before the transfer commences (Pre scripts) or in the destination directory of the destination CommBox after the files have been received (After scripts).

Pre scripts

getmail
: Connects to a mail server and places messages from the incoming mailbox in the transfer directory. By default it does not include the mail body and only saves the attachments. The messages will be deleted from the mailbox.
Parameters:
--server=<servername>
: The mail server name or IP address.
--user=<user name>
: The username linked to the mail account.
--pass=<password>
: The password for the mail account.
--port=<port number>
: Optional, default 110. The port number used for the connection, use 995 for SSL connections.
--mail
: Optional. Move the entire mail to the source directory. If this parameter is not specified, only the attachment will be moved.
Example:
: getmail --server=mail.commbox.com --user=cbx --pass=abcd --port=143 --mail

getlogs
: Retrieves the CommBox' logs for the last day.
It is advised that transfers using this script should run only once per day.
Parameters:
: You can pass any number of log names:

commbox
The main CommBox activity log.
carrier
Log of carrier status.
hardware
Log of hardware status.
transfer
Log of file transfer activity.
connection
Log of connection activity.
ulog
Log of UUCP log activity.
udebug
The UUCP debug log.
prepaid
The log for the crew pre-paid card activity.
billing
The log for QuickCrew billing system.

Example:
getlogs prepaid billing

Telnet

Log in a windows computer, run a command, and save its output.
Note that the telnet server needs to be enabled on the Windows computer.
Parameters:
--user=<user>
The username to use for the login.
--pass=<password>
The password to use for login.
--ip=<IP address>
The IP address of the computer to which you want to log in.
--port=<port number>
Optional, default 23. The port used for the connection.
--command=<command>
The command that will be run on the Windows computer.
--output=<file name>
Optional, default 'telnet.log'. The name of the file that will contain the command output.

Example:
telnet --user=commbox --pass=testpassw --ip=192.168.140.144 --command=ipconfig

cbx_system_backup

Create a backup of predefined CommBox directories or restore from one of these backups.
Parameters:
--users
Backup user-related data. On CommBoxes using the Squirrel mail client, this includes all mail-related data (messages, address lists etc.). On CommBoxes using the Zarafa mail client, this backup has no data.
--system
Backup system data. This includes CommBox software and configuration.
--restore
Will try to restore from the files that are in the QuickFile pick-up folder.
--usb
The backup files will be saved to an external USB device. The device must be plugged directly in one of the CommBox USB ports. The CommBox will use the first device it recognises, so it recommended to have only one device plugged in.
--maxfiles=<number>
Restrict the number of files that are stored on the external USB device. Once the maximum is reached, the oldest file will be deleted from the device. So, if you set --maxfiles=5, only the most recent 5 backup files will be kept on the device.

Example:

cbx_system_backup --users --usb --maxfiles=5
cbx_system_backup --backup --system
cbx_system_backup --restore --system

schedulecms

This script can be used for file delivery to CMS, can be used for IPMC Log Sweep.

Parameters:

--subject=<any text>

Any text that describes the transmitted file.

[--nohub]

program will exit with a return code so quickfile wont call addtoqueue and quickfiletmp/ftp/pickupfolder will be deleted.

[--debugl-d]

If the option debug is used only a parameter test will be performed, no file will be queued.

Example:

schedulecms --subject perceptionlogs
schedulecms --subject perceptionlogs --nohub
schedulecms --subject perceptionlogs --nohub -d

After scripts

mergelog

This script will merge each log file received from a getlog script with the corresponding one received from each new transfer.

Parameters:

There are no parameters for this script.

Example:

mergelog

uncompress

Any compressed file in a recognised format will be uncompressed on receipt.
The recognised formats are: ARJ, CAB, CHM, CPIO, DEB, DMG, HFS, ISO, LZH, LZMA, MSI, NSIS, RAR, RPM, UDF, WIM, XAR, and Z.

Parameters:

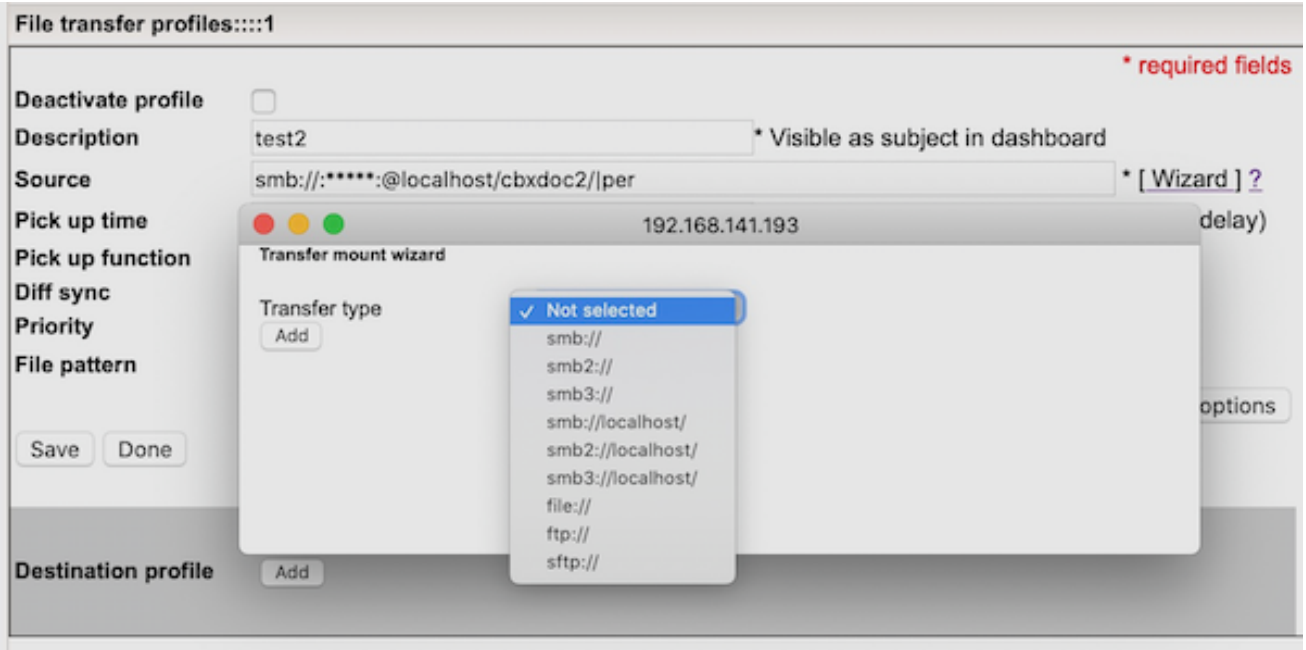
There are no parameters for this script.

Example:

uncompress

12.2 Source / Destination wizard

The source and destination folders are defined by means of an URI. Its syntax changes depending on the protocol used. The wizard helps you compose a URI with a correct syntax.



12.2.1 Transfer type

There are five types available, what other fields you will need to fill in, depends on the type chosen.

smb://, smb2:// and smb3://
: Generates a samba mount point between CommBox and a remote server. You will need an account on the server to establish a mount point, and your user name and password are therefore required. smb2:// and smb3:// uses samba protocol versions 2 and 3 respectively. Do note that these must not be used in destination profiles for CommBox systems running version prior to 1.22.0. The older versions cannot handle the delivery and the file will be discarded.

smb://localhost/
: Generates a local samba share point.

file://
: Will access directly a local file on the CommBox.

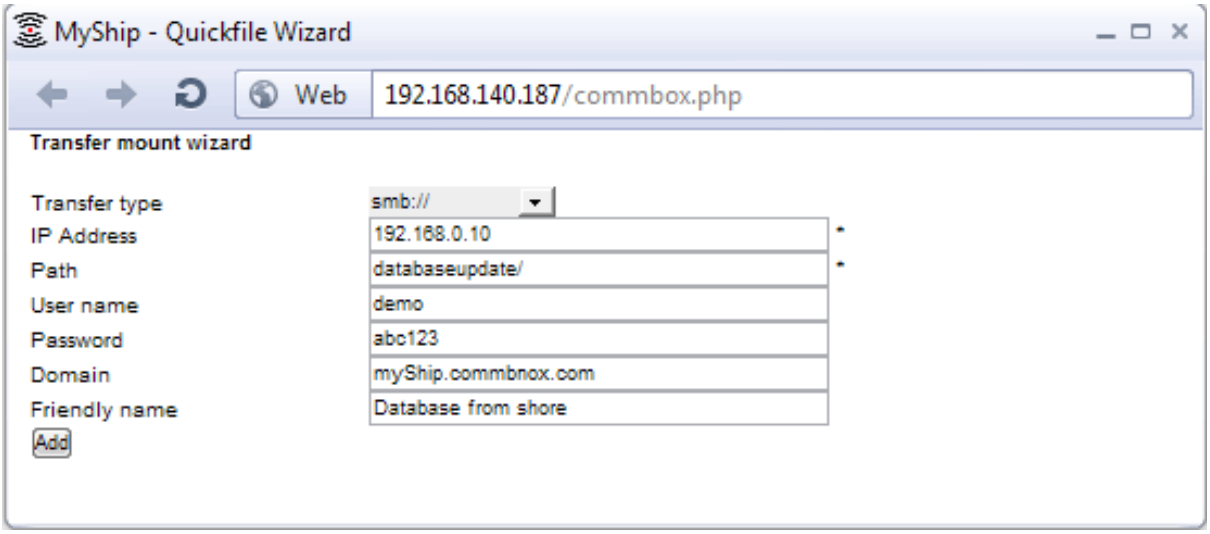
email:// (only in destination)
: Sends the file as an email attachment.

ftp://
: Access a folder on an FTP server.

sftp://
: Access a folder via SSH File Transfer Protocol.

What fields you will need to fill in next depends on the type of transfer chosen. What follows is a detailed description for each type:

smb



IP Address
: Server IP (if using smb://localhost, this will not be visible and will be automatically filled in with 'localhost' in the connection string).

Directory on CommBox
: The shared folder on the server.

User name
: Server log-in name

Password
: Password of the server account.

Domain
: The domain has to be specified only if the server is on a different domain from the CommBox

Friendly name
: Allows you to specify a more understandable name to show in the dashboard file queue for the 'from' or 'to' fields. If left blank, the full connection string will be displayed.

REMEMBER: Allow read and write access in the source directory. Else the files cannot be deleted after pickup, and they will be picked up again on next action time.

An smb connection string explained:

```
smb://demo:abc123:myShip.cbx.com@192.168.0.10/dbupdate/|Database from shore
```

Transfer type	User name	:	password	:	domain	@	IP	path	|	Dashboard friendly name
smb://	demo	:	abc123	:	myShip.cbx.com	@	192.168.0.10	dbupdate/	|	Database from shore

file

The only field to fill in is the path to the desired directory.

email

(email is only accessible in destination profile)

The only field to fill in is the recipient email address. The files will be delivered as an attachment to the specified address.

An email connection string:

```
email://JohnDoe@somewhere.com
```

ftp / sftp

The wizard is very similar to the one for smb://

IP Address

Server IP

Path

The pickup folder on the ftp-server

User name

Server login name

Password

Password to the server account

Friendly name

Allows you to specify a more understandable name to show in the dashboard file queue for the from or to fields. If left blank, the full connection string will be displayed.

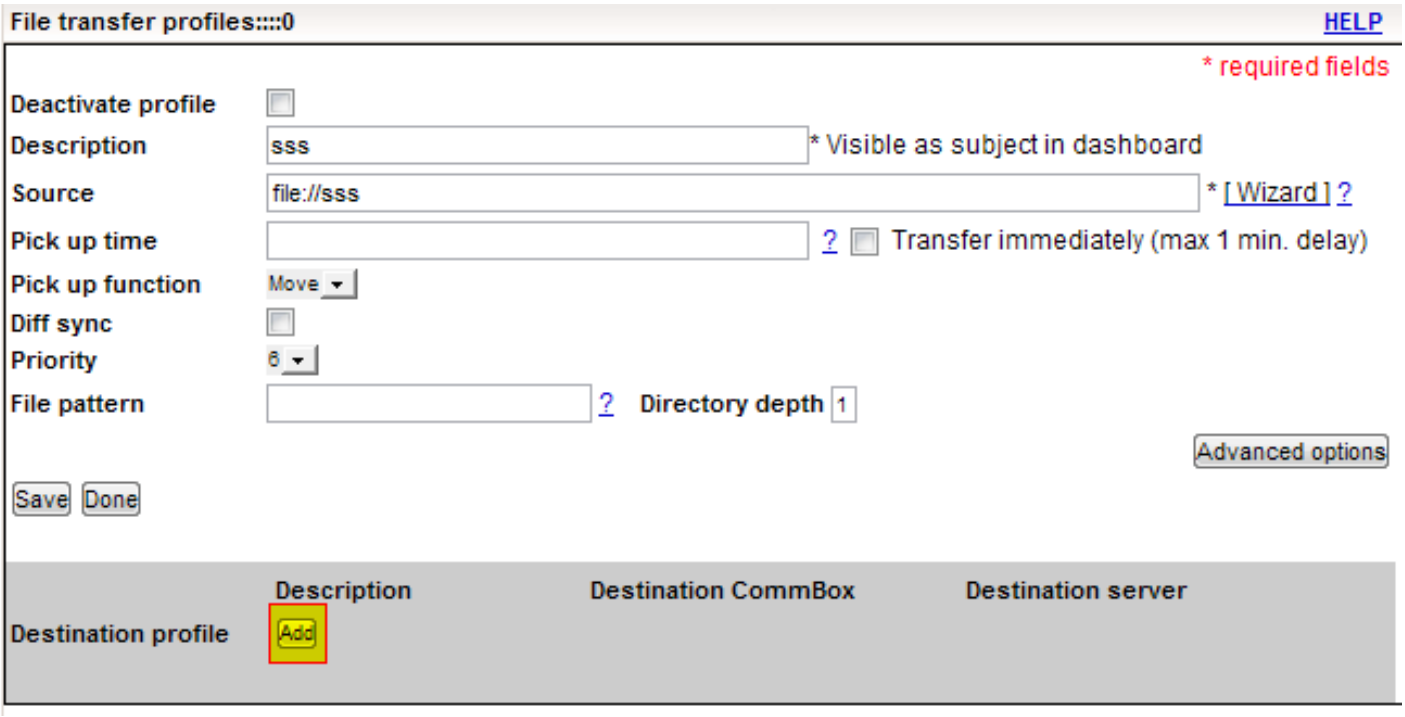
REMEMBER: Allow read and write access in the source directory. Else the files cannot be deleted after pickup, and they will be picked up again on next action time.

An ftp connection string:

```
ftp://demo:abc123:@somewhere.com/logs|Logs from shore
```

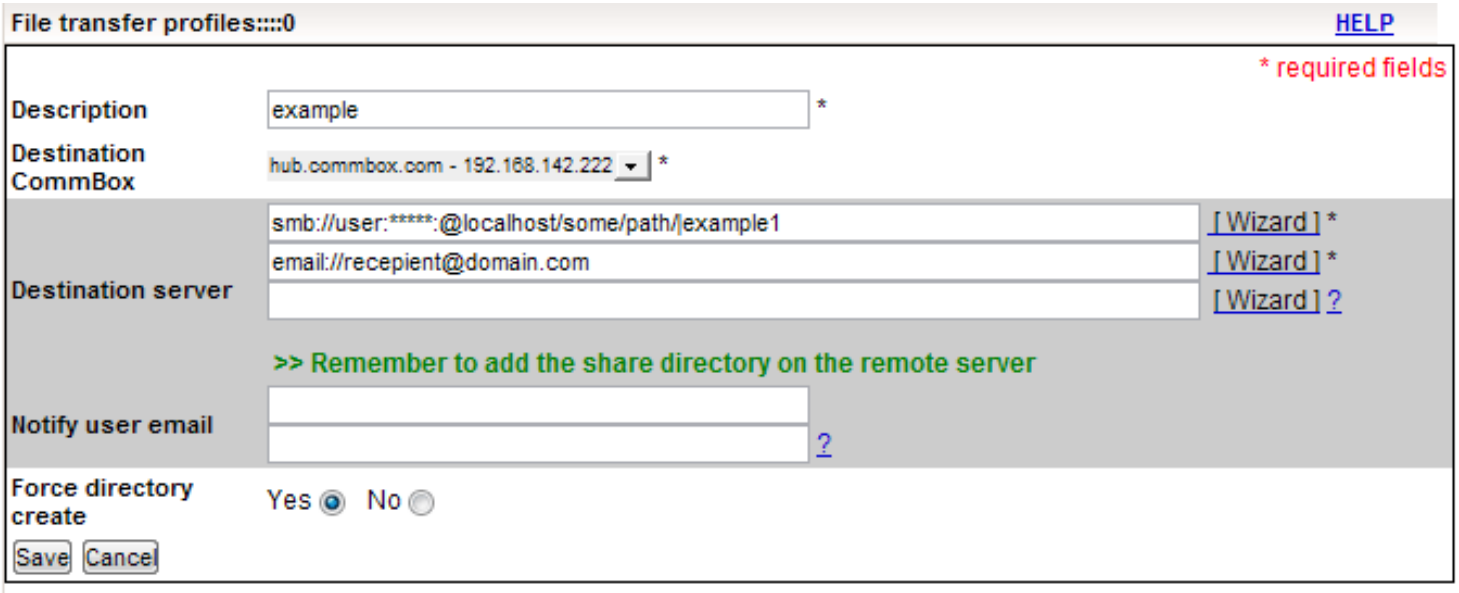
12.3 Adding destination profiles

To add a destination, click [Add] in the destination profile field (this button will not be visible until the transfer profile is saved).



One destination profile can have many destinations and one transfer profile can have many destination profiles.

If you need to add many destination servers to a destination profile, fill in all the available "Destination server" fields and click [Save]. A new empty field will then appear.



Field description

Name

The name will be shown in the destination profile overview.

Destination CommBox

Choose a host in the drop down menu. Remember that the host must be created with type 'Commbox main hub' or 'Commbox hub' (see Hosts) before they appear in the drop down menu.

Destination server

Destination server has the same syntax as source. See the wizard explanation Source / Destination wizard.

Notify user email

A notification email will be sent to these addresses every time a file from the transfer profile is delivered. The subject of this email is the one defined in the 'Subject' field of the transfer profile. The body of the email is also defined in the transfer profile. (Both subject and message are defined in the "Advanced options").
If you need to add many addresses, fill in all the available "Notify user email" fields and click [Save]. A new empty field will then appear.

Force directory create

Applies to smb, file, or ftp. If the path defined as destination does not exist and this option is active, the destination directory will be created automatically on transfer.

13 QuickWeb

QuickWeb is a web accelerator which will give faster browsing of Internet web sites. It achieves this by removing advertisements, reducing image resolution and colors, and compressing all data transmitted between shore and vessel.

When QuickWeb acceleration is enabled, your browser will not connect directly to the web server hosting the content. All communication will instead go through the CommBox which will handle all data exchange between vessel and shore.

Setting up QuickWeb is done differently on the hub/Office and on the Vessel side.

13.1 QuickWeb (vessel)

13.1.1 QuickWeb configuration

On the vessel CommBox, QuickWeb can be set up from the "QuickWeb" option in the left menu.
The main QuickWeb page displays in the "QuickWeb Config" panel, the status of the on-board web cache (Running / Not running).

Each CommBox connection profile is linked to a QuickWeb profile (see Connections, Standard fields description). A QuickWeb profile defines rules on:

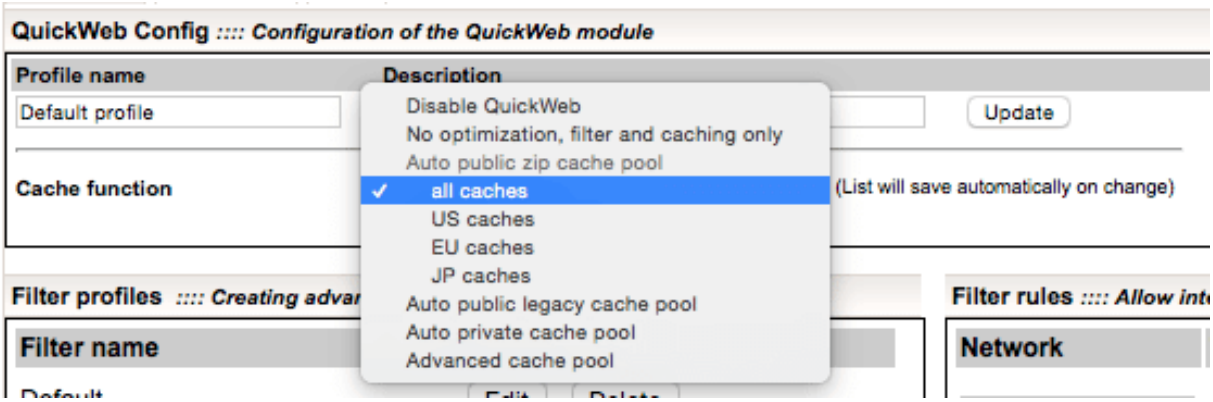
- Whether or not to enable QuickWeb.
- The cache size.
- Whether or not to enable proxy as a transparent proxy.
- From which networks to accept connections.
- Which domains should be passed through without optimization.

All QuickWeb profiles are listed in the "QuickWeb profiles" panel.

13.1.2 Edit or add a new profile

To edit the profile click [Edit] at the right hand side.
To add a new profile, click [Add] at the bottom of the "QuickWeb profiles" panel. This will open a form where you can enter a name and description for the new profile. When you click [Save], the fields for the filter configuration will appear:

Cache function



The cache function controls if and how QuickWeb operates. The options are:

Disable QuickWeb
: Stops the QuickWeb service. The proxy server will no longer be available.

No optimization, filter and caching only
: Enables the content filtering and the content caching functionality in QuickWeb. QuickWeb will block content according to the settings in the "Filter profile" and will try to serve requested content from the QuickWeb cache before it is downloaded from Internet.

Auto public zip cache pool

The Ziproxy has more speed and is better compatibility with web sites. Choose the "all caches"" or one from one of the regions US, EU or JP.

Auto public legacy cache pool
: QuickWeb will be set up with full optimization. QuickWeb will first look for requested content in its local cache. If it isn't available there, QuickWeb will continue to the "parent" QuickWeb cache. The onshore parent QuickWeb or the "cache pool", will remove content and compress images before data is returned to the QuickWeb on board the vessel.

Auto private cache pool
: This option work the same way as "Auto public cache pool" except that this one is a private cache pool that is operated by the customer.

Advanced cache pool
: Allows advanced setup of self-managed web caches. This is usually done in collaboration with KVH support team (see Support for contact details).

13.1.3 Filter profiles

A filter profile is a collection of rules which allow or deny access to predefined web site categories and/or to specific addresses. These profiles are linked to specific access networks in the setup of "Filter rules" (see below).

Add a new filter profile by clicking [Add profile]. This will open the filter profile form in a new window.

Click anywhere on the gray background to exit the filter form without saving.

Filter name
: Provide a name that describes the purpose of the filter.

Filter function
: Select how the filter is going to operate:

  Allow all except the one defined below
  : Will grant access to all the websites that do not match the categories or addresses specified for the filter.

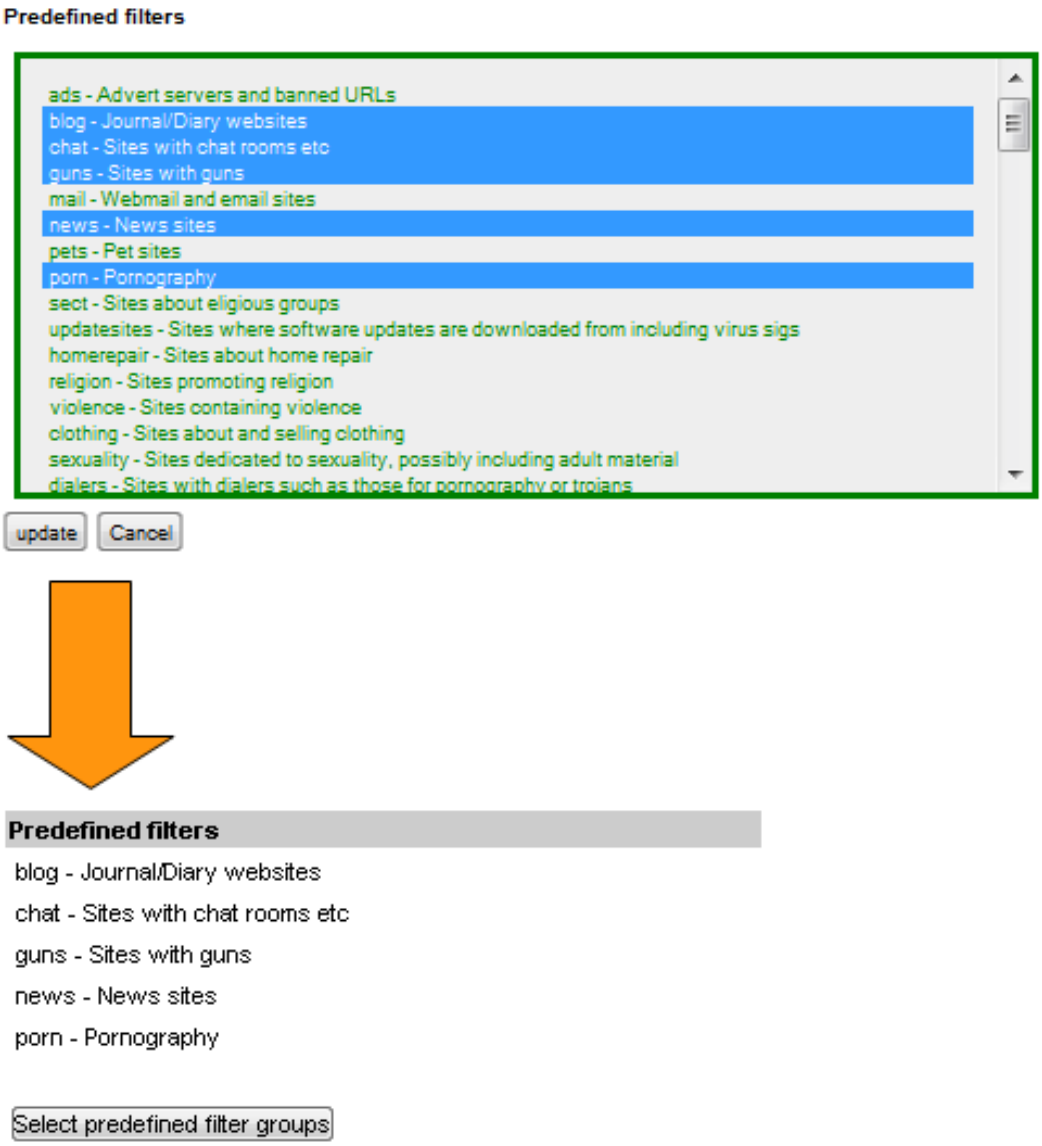
  Deny all except the one defined below
  : Will grant access only to the websites that match the categories or addresses specified for the filter.

  It is not possible to combine allow and deny rules in the same profile.

Predefined filters
: Lists all the predefined categories for which this filter applies.

Select predefined filter groups
: Will open a multi-select list of categories. It is possible to select more than one category by holding the Ctrl key while clicking on the desired category lines. Hold Ctrl and click on a selected category to de-select it.
  Click on "[Update]" to accept the selection, or click on "[Cancel]" to close the multi-select list without action.

  The new selection will overwrite all the categories that were already selected in the filter. (But not the user-defined filters)



User specified filters
: Lists all the user-specified URLs for which this filter applies.

Add user specified filter line
: Adds a field which allows you to specify a URL to be added to the rules. The text you enter here will be matched against any part of the URL. e.g. 'news' will match 'www.news.com' and 'www.bbc.co.uk/news'.

Exceptions
: Lists all exceptions to the above setup. If the specified filter function is "Allow all except", exceptions will be permitted even if listed in the selected predefined filters or user specified filters. If using the filter function "Deny all except", exceptions will be denied even if they are permitted by either predefined filters or user specified filters.

Add exception
: Adds a new field where you may specify (parts of) a URL (ref. "Add user specified filter line").

Save and close
: Saves the current setup and closes the filter profile form.

Cancel
: Closes the filter profile form and does not apply any change.

13.1.4 Filter rules

From this panel you can set up which networks are allowed access to the Internet and which filter profile each network should use, if any.

Network
: Specify the network that will be using this rule. This value must be entered in the form "IP / CIDR", ex: 192.168.0.0/24.

Transparent
: HTTP
: Enabling transparent proxying for a net will redirect all http requests from that net to the CommBox proxy. If the box is left unchecked, clients that want to reach the Internet may need to set the CommBox as http proxy on port 3128.
: HTTPS
: Enabling transparent HTTPS will redirect all https requests from the given net to a web page explaining how to configure the browser in order to use https.
Leaving this box unchecked, will cause https traffic to be routed directly to the Internet.

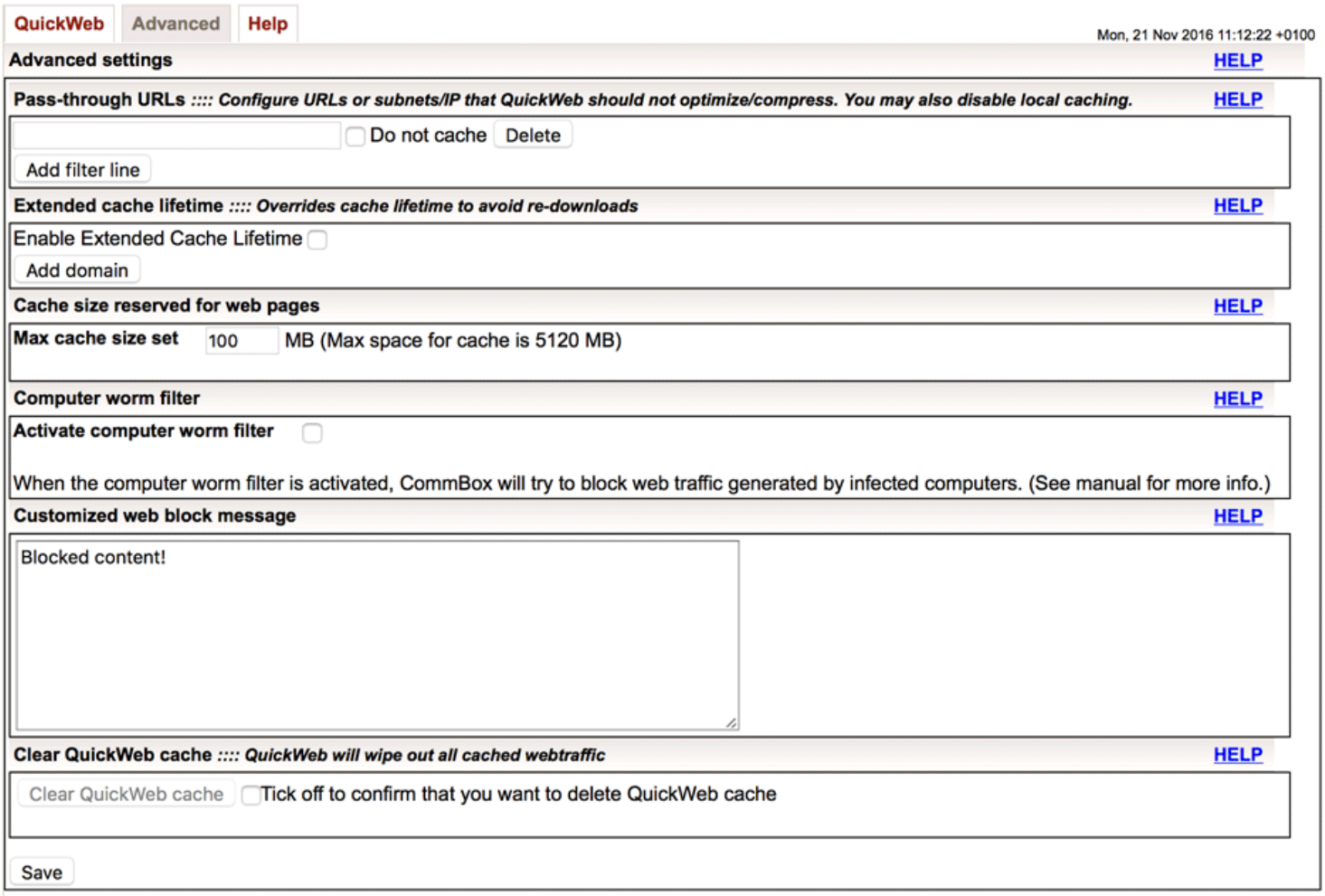
Filter profile
: Select if the network should use a filter profile or not. If a profile is selected, web content will be allowed or denied based on the rules defined in the profile.

13.1.5 QuickWeb and Web Proxy Auto-Discovery (WPAD)

The setup of *Web Proxy Auto-Discovery* is described in Appendix: Web Proxy Auto-Discovery (WPAD)

13.1.6 QuickWeb - Advanced settings

From "QuickWeb->Advanced" you access more general settings for the QuickWeb system. These settings are independent from the QuickWeb profiles.



Click [Save] at the bottom of the page to save your changes.

13.1.6.1 Pass-through URL

Websites that should go untouched (no compressing, filtering or content removal) through the QuickWeb system can be added to the pass-through list. Click [Add filter line] to add a new text line where a URL can be added.

13.1.6.2 Extended cache lifetime

Overrides cache lifetime to avoid re-downloads for domains added.

13.1.6.3 Max cache size

Set the max amount of space that the QuickWeb cache can use.

13.1.6.4 Computer worm filter

CommBox can try to block web traffic generated by worm-infected computers. Use the checkbox to activate or deactivate this feature. Click on [Save] at the bottom of the page to save your changes.

Worms are a type of computer virus that often will send and receive information through network connections. They can make a great impact on network performance because they usually generate huge amounts of traffic.

Computer worms are hard to stop because they are intelligent and they often install new versions of themselves to better stand against virus removal software. CommBox will not be able to remove worms from infected computers, but it will try to stop web traffic created by well known worms. By stopping some of the network traffic we can maybe prevent the worm from upgrading to a newer version. This way, it will be easier for virus software to track down and remove the problem from infected computers.

At the moment, CommBox filers traffic for one type of worm:

Conficker
: Conficker, also known as Downup, Downadup and Kido, is a computer worm targeting the Microsoft Windows operating system. It was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to propagate while forming a botnet. Conficker has since spread rapidly into what is now believed to be the largest computer worm infection since the 2003 SQL Slammer, with more than seven million government, business and home computers in over 200 countries now under its control. The worm has been unusually difficult to counter because of its combined use of many advanced malware techniques.
- From Wikipedia, the free encyclopedia

13.1.6.5 Block message

The text entered in the "Customized web block message" field will be used on the "content blocked" page that will be displayed if someone tries to connect to a web site that is blocked by the QuickWeb profile.

Enter the desired text and click on [Save] at the bottom of the page to save your changes.

13.1.6.6 Clear QuickWeb cache

Tick the checkbox and click [Clear QuickWeb cache] to delete the local QuickWeb cache.

13.2 QuickWeb (hub)

Configuration for QuickWeb Office/hub is found under the menu item QuickWeb, just as for Vessel, but there are other options to configure.

13.2.1 QuickWeb configuration

Enable QuickWeb
: If QuickWeb is not enabled on the hub, the vessels will not be able to use QuickWeb.

Blockmessage
: The message that users will get when they try to retrieve a Web page blocked by a QuickWeb filter.

Size of redline
: The size in pixels of the red square on optimised images.

Minimum redline size X,Y
: Images smaller that this will not have a redline added. This is useful to avoid having unreadable icons.

Image quality
: How much pictures should be compressed to reduce transfer bandwidth. Low values give low quality and high compression (big reduction in size). The range permitted is from 1 to 99.

Proxy host and proxy port
: If QuickWeb needs to use another web proxy in order to reach Internet, enter its IP address and port number here.

Automatically authorize connecting vessels

Add automatically a vessel's IP address to the "Allowed Networks" list (see further down in this manual) when it connects the first time (either for file transfers, getting queue or for routing). This simplifies setting up QuickWeb, and should generally be used unless you want to explicitly deny QuickWeb for certain vessels.
The IP address will be added in the form of a single host (i.e. ip/32).

13.2.2 Clear QuickWeb cache

Allows you to delete all cached data from the CommBox disk.

13.2.3 Allowed networks

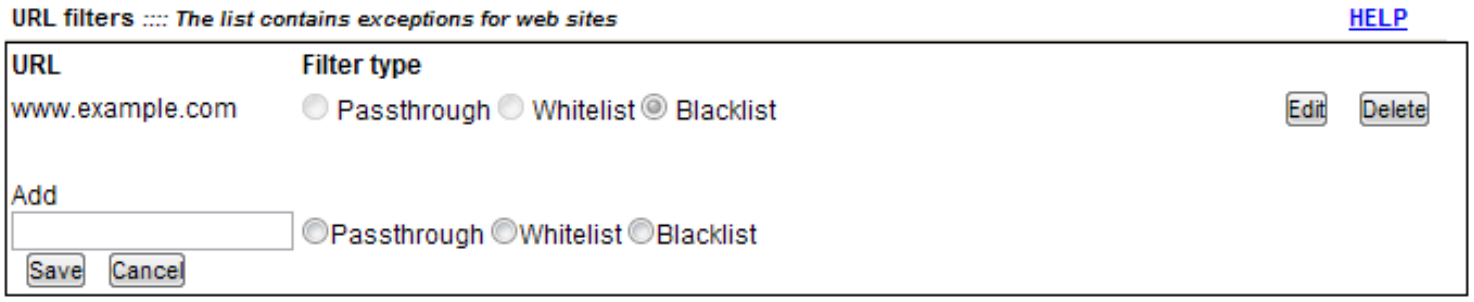
Specifies which subnet(s) can use QuickWeb. Users connecting from subnets that are not in this list will receive a message saying that access is denied to the IP from which they are connecting.

Subnets are specified in CIDR notation e.g. '10.0.0.0/24', '10.0.0.0/16' or '10.0.0.0/8'. To specify a single IP address, use a mask of 32 bits; for instance '10.0.0.1/32' to give access to the IP 10.0.0.1. Please note that CommBox currently supports the four subnet masks /32, /24, /16 and /8.

The most common setup will be to allow the private IP ranges from which the vessels are seen, and possibly other single public IPs from which connections should be allowed.

13.2.4 URL filters

From "QuickWeb->URL filters" you can configure filters that control QuickWeb's traffic. You can define whether URL are blocked, allowed, or left unoptimized.



Filter types:

Passthrough
: Traffic is passed through without optimization.

Whitelist
: Traffic is allowed even if it is blocked by content filtering (see further on in this manual).

Blacklist
: Traffic is blocked.

13.2.5 Content filtering

From "QuickWeb->Content filtering" it is possible to set filters based on the type of content of a web site. Content filtering uses lists which categorize web sites according to their content. These lists are not maintained by KVH but, in case anybody finds any errors, they can report them to KVH (use the mail address commboxsupport@kvh.com) and KVH will forward the issue to the appropriate organization.

Subscribe to content filters :::: *Lists contain a collection of categories which can be used for filtering* HELP

Category	White/black/none	Explanation
abortion	○ ○ ◉	Abortion information excluding when related to religion
ads	○ ○ ◉	Advert servers and banned URLs
adult	○ ○ ◉	Sites containing adult material such as swearing but not porn
aggressive	○ ○ ◉	Similar to violence but more promoting than depicting
alcohol	○ ○ ◉	No explanation available
antispyware	○ ○ ◉	Sites that remove spyware
artnudes	○ ○ ◉	Art sites containing artistic nudity
astrology	○ ○ ◉	Astrology websites
audio-video	○ ○ ◉	Sites with audio or video downloads
banking	○ ○ ◉	Banking websites

For each category, you can choose which action to take between Whitelist, Blacklist, and none.

Whitelist
: Always allow traffic.

Blacklist
: Always deny traffic.

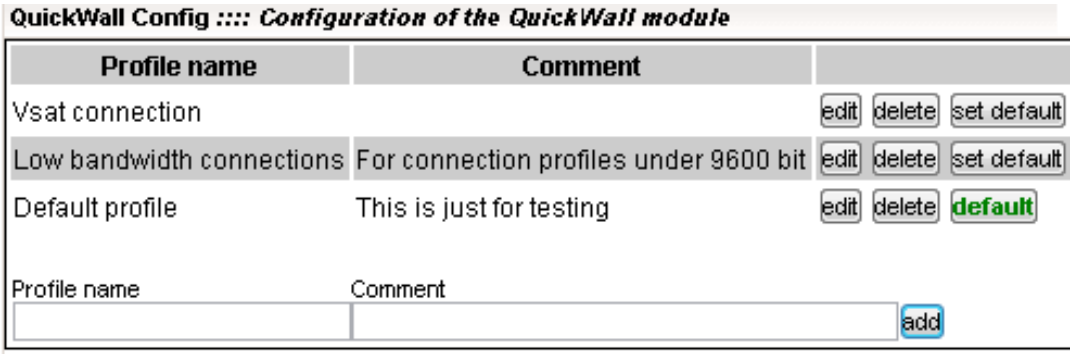
None
: Take no action.

Note that the list view may be empty if the lists are not installed on your CommBox.

14 QuickWall

QuickWall manages the firewall in CommBox. Before attempting to configure it, please read through the entire chapter, as misconfiguring firewalls might cause big problems. The firewall should be configured before the CommBox is put into production use and should never be changed at critical times.

You must have a good understanding of TCP/IP and networking to be able to configure QuickWall.



Clicking [QuickWall] in the left menu, you will come to a list of the existing profiles. From here you can select which profile is going to be the default one, edit or delete existing profiles, and add new ones.

Below the list of QuickWall profiles is the Distributed Firewall Profiles list. See Distributed Firewall Profiles for more details.

The QuickWall profile currently in use is the one linked to the current active connection profile. Each connection profile is linked to either a specific QuickWall profile or to the default one.

14.1 Select default profile

The current default profile is marked with a green [Default]. To select a new default, click [Set default]. There can be only one default profile at a time so, when you select a new default, the previous one is deselected automatically.

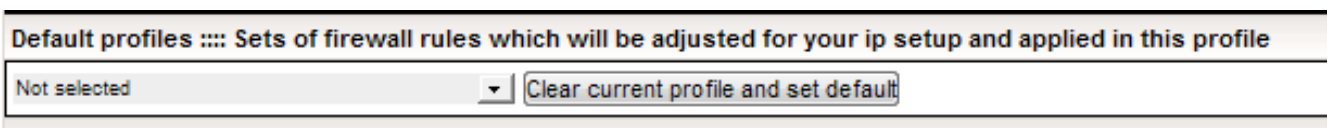
14.1.1 Edit a profile

When you click [Edit], you will get to the profile editor view. This is split in five parts:

- Standard firewall templates provided by KVH.
- Only on vessel: Link to DFP (see Distributed Firewall Profiles)
- Firewall settings.
- Routing settings.
- Quality of service settings.

14.2 QuickWall templates

The firewall templates selector is located at the top of the edit screen.



Select a profile from the pull-down options and click [Clear current profile and set default]. CommBox will fill the template profile with addresses adjusted for your ip setup.

All old configuration for this profile will be deleted.

14.3 Macros

For the firewall, routing and QoS sections described below, the fields specifying ip addresses or subnets have the ability to perform certain macro substitutions:

IPlan(<lan name>)
: The IP address of a network interface (as defined in Config->Network).

IPnet(<lan name>)
: The IP network of a network interface (as defined in Config->Network).

IPhost(<host name>)
: The IP address of a host (as defined in Config->Hosts). You can use the host name or one of its aliases.

Macros may be used in these fields:

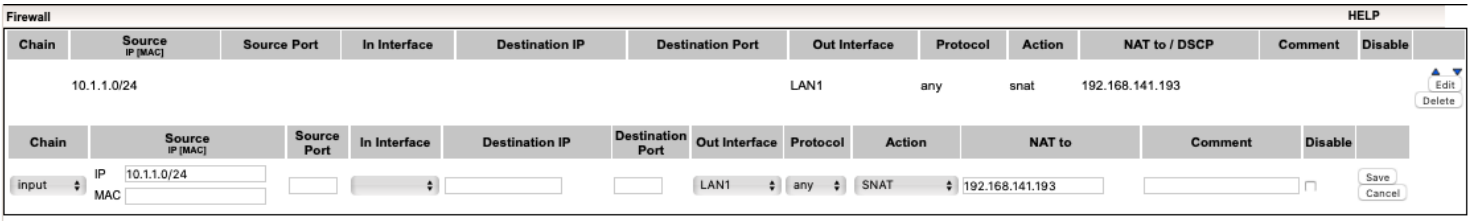
- Firewall: source, destination
- Route: source, net, gateway
- QoS: source, destination

When defining a DFP on the hub, the same macros may be used, and will then refer to addresses or networks from the vessel's own configuration. For example: the 'source' field can accept a value of '192.168.140.134' or 'IPlan(LAN2)'. The latter stands for 'The IP address of the network interface called LAN2 on the vessel'.

For this to work, it is important that all the vessels using a DFP have the same setup. If a referred object (a LAN or a host) is not found on a vessel, then the whole DFP will be ignored on that vessel and none of its rules will be applied.

14.4 Firewall

The Firewall panel is the one with more options, you will only use a few of them for each rule.



If a DFP is activated, you will also see its rules.

Chain
: Tells if the rule will match packets to the CommBox (input), from the CommBox (output) or through the CommBox (forward). Leaving the field empty will auto-detect based upon source and destination addresses. Selecting non-blank will force the selected chain to be used. This field is only valid for filtering rules.

Source IP [MAC]
: Source IP-address or subnet/mask for which this rule applies.
: It is also possible to specify the MAC-address in conjunction with the IP-address.

Source port
: The TCP or UDP port for which this rule applies, this is only used on rare occasions

In interface
: The network interface of incoming traffic for which the rule applies.

Destination IP
: The destination IP-address or subnet/mask for which this rule applies.

Destination Port
: The destination TCP or UDP port for which this rule applies.

Out Interface
: The network interface of outgoing traffic for which the rule applies.

Protocol

The protocol (TCP, UDP, ICMP) for which this rule applies. The selection you make here determines which other fields are considered. e.g. 'Source port' and 'Destination Port' are relevant only if you select TCP or UDP.

Action
: What to do with traffic matching this rule. The options are ('accept', 'reject', 'drop', 'masquerade', 'snat', 'dnat', and 'dscp'). These are explained in more details further in this manual.

NAT to / DSCP
: Used when making snat, dnat, or dscp rules.
NAT - it determines to which IP address the traffic should be translated. When making a snat rule, only an IP address is needed. This must always be the address of the CommBox. When making a dnat rule, the format you need to use is 'IP address:port'.
DSCP - Differentiated Services Code Point.
Read more about this later in this manual.

Comment
: This field is meant as a place for you to make notes about what the rule is for, or simply give it a name.

Disable
: Each rule can be disabled and then re-enabled at a later time.

The fields source ip, source port, destination ip and destination port may be prepended with an exclamation point (!) to indicate that the rule should match what is NOT put in the field.

In addition to the above fields, there are arrows that allow you to move a rule up or down in the list and buttons for editing or deleting a rule. These are only shown for listed rules, not a new rule as you write it.

14.4.1 What should happen, the action field

The 'Action' field determines what to do with the traffic matching a rule. It is possible to choose from: 'accept', 'reject', 'drop', 'masquerade', 'snat', and 'dnat'.

Accept, reject and drop are used to filter traffic.

accept
: Traffic is passed on.

reject
: Traffic will not be passed on and a return message will be sent declaring "no such service is available".

drop
: Traffic will not be passed on and no return message is sent.

Dnat and snat performs destination network address translation and source network address translation respectively. Masquerade is another target which changes the source address, automatically giving it the address of the outgoing interface.

masquerade
: is used to automatically rewrite the source address of outgoing packets to the address of the CommBox on the outgoing interface.

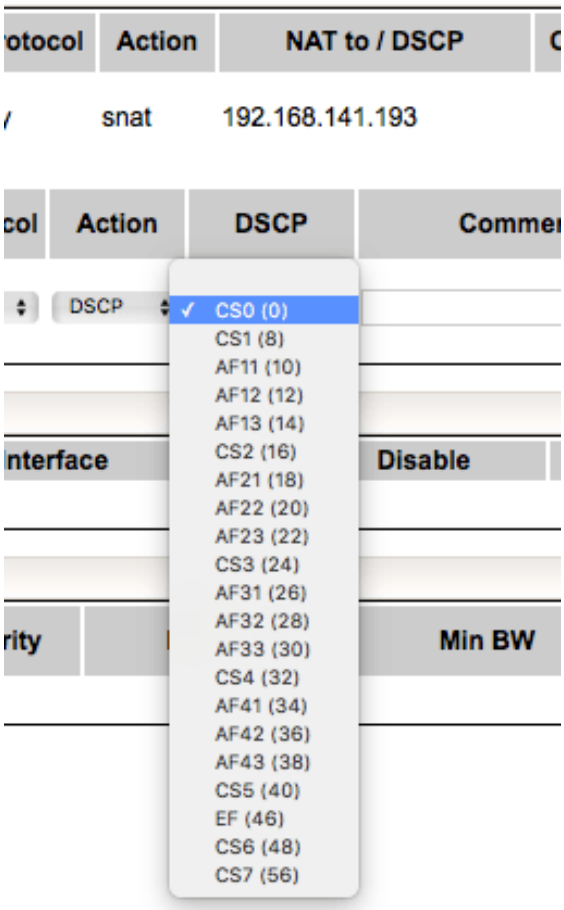
snat
: is used for masquerading traffic, i.e. the source address of outgoing packets is replaced with what is specified in the 'NAT to' field. It is the typical nat function used to let an entire subnet's traffic go out with the gateway's IP-address. It is commonly used to enable connecting several machines on a single DSL line. It is also used in some cases to avoid complicated routing setups for short lived projects.

  When setting up a snat rule, there are three fields you need to fill in: 'Source IP', 'Out interface', and 'NAT to'. 'Source' determines for which subnet to perform snat. Nat determines which source IP address will be attached to the outgoing traffic. This must always be the IP address of the CommBox. If you wish to limit the rewrite to certain destinations, you may use the destination field aswell.

dnat
: is used to make the CommBox act as a gateway between the local network and an external network. The fields that apply for this action are: 'Source IP', 'Destination IP', 'Destination Port', 'Nat to', 'Protocol' and 'In interface'. Most times it will be sufficient to specify 'Destination Port' and possibly 'Source IP' if only some machines should be allowed to connect through. 'Nat to' specifies the 'IP address:port' of the machine on the local network that should

receive the traffic.

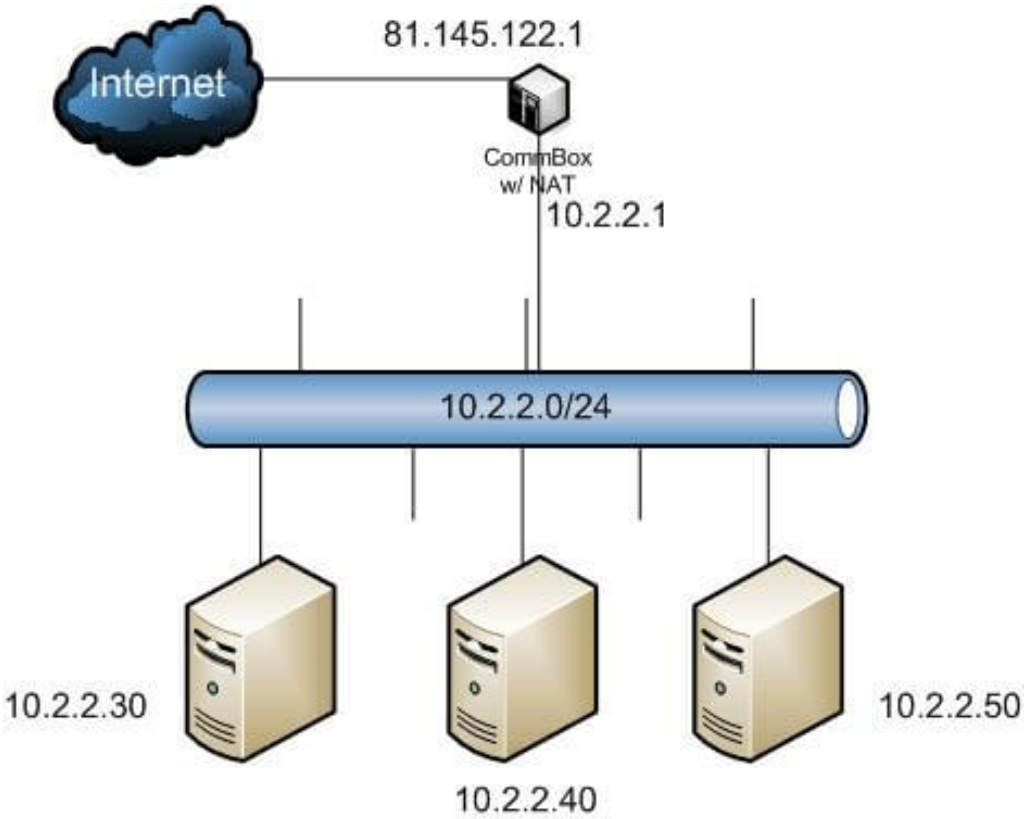
DSCP



The Differentiated Services Code Point (DSCP) can be used to provide low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.
For DSCP use AF (Assured Forwarding), CS (Class Selector), EF (Expedited Forwarding) or BE/CS0 (Best Effort).
The value shown in () in drop-down are the corresponding bit settings in decimal notation.
For more details see the Wikipedia article Differentiated services (external link).

14.4.2 SNAT / DNAT examples

Consider the following setup:



Here, CommBox has LAN2 connected to the internal network with the IP address 10.2.2.1, making it a part of the subnet 10.2.2.0/24. LAN1 is connected to the Internet and has the IP address 81.145.122.1, which is an IP address given by the ISP.

14.4.2.1 SNAT

In order for the CommBox to perform snat in this scenario, use the following configuration:

Source IP
    10.2.2.0/24
Out interface
    LAN1
Action
    snat
NAT to
    81.145.122.1

CommBox will now rewrite all packets from internal machines (10.2.2.30, 10.2.2.40 and 10.2.2.50), changing their internal addresses to the external address ('81.145.122.1'). This makes the machines able to access Internet and get replies from requests to the internet back to a known address.

Source IP	Source Port	In Interface	Destination IP	Destination Port	Out Interface	Protocol	Action	NAT to / TOS	Comment
			81.145.122.1	8080		tcp	dnat	10.2.2.40:80	Web
10.2.2.0/24					LAN1	any	snat	81.145.122.1	Rewrite

14.4.2.2 DNAT

In the same setup, if 10.2.2.40 should be reachable from outside, you need to make a dnat rule. If you want to reach port 80 by using port 8080 from the Internet, you need to enter the following configuration:

Destination IP
    81.145.122.1
Destination Port

8080 (this is what people on the Internet will connect to)

Protocol

tcp

Action

snat

NAT to

10.2.2.40:80

All traffic destined to 81.145.122.1 on port 8080 will now be forwarded to 10.2.2.40 on port 80.

Source IP	Source Port	In Interface	Destination IP	Destination Port	Out Interface	Protocol	Action	NAT to / TOS	Comment
			81.145.122.1	8080		tcp	dnat	10.2.2.40:80	Web
10.2.2.0/24					LAN1	any	snat	81.145.122.1	Rewrite

14.4.3 How to use the source and destination fields for filter rules

The source and destination fields both accepts single IP addresses and subnets in the form IP address/mask. If you want to make a rule regarding traffic to CommBox, you need to fill out the CommBox IP in the 'Destination IP' field. If you want to make a rule regarding traffic going out from CommBox, you need to enter the CommBox IP in the 'Source IP' field. If neither the source nor destination field contains the CommBox IP address (one of them if the CommBox has several), the rule will be used as a forwarding rule, i.e. pertaining to traffic the CommBox passes through when used as a gateway.

14.4.4 Source and destination port fields

These fields take either a single port or a port range in the form of startport:endport. They can only be specified when traffic type is tcp or udp.

14.4.5 Avoiding the most common pitfalls

Configuring correctly a firewall is not a trivial task. First and foremost, to avoid trouble, you should always keep tcp port 80 open from wherever you need to reach the web interface of the CommBox. You also need to make sure that outgoing traffic destined for tcp port 2222 is allowed, or else the CommBox will not be able to make any connections to another CommBox over TCP lines (typically VSAT). A good setup which will not affect any of the functionality in the CommBox is as follows:

- Open tcp port 25 into the CommBox from the networks that should be allowed to send mail. If the CommBox is used as a mail server on office, receiving mail directly from Internet, port 25 needs to be open from all nets. On vessels, only the nets that use the CommBox for outgoing mail need this port open.
- Open tcp ports 110 and 143 for everybody that should be able to read mail on the CommBox. This means all IP addresses/ranges that the CommBox sees when a user connects to read his mail.
- Open tcp port 2222 into the CommBox. Without this, another CommBox cannot connect to your CommBox and support people cannot log in.
- Open tcp port 80 into the CommBox. This is needed in order to get to the web.
- Allow icmp for all networks containing CommBoxes that need to connect to this CommBox. Without this, the carrier checks will fail and those CommBox installations will not be able to connect.
- Open udp port 53 into the CommBox for all networks that use the CommBox for name resolution.
- Open tcp ports 137, 138 and 139 for everybody who needs to access the Samba server on the CommBox.
- Block all other traffic with destination to the CommBox.
- Repeat all steps above for each of the CommBox IP addresses and the relative machines that should connect to them. This way all IP addresses have suitable rules.

This setup will ensure that all ports needed are accessible and the rest of the ports will not be available. You do not need to take traffic on the loopback interface into consideration since this is handled automatically. If you want to further restrict machines using the CommBox as gateway, add rules for this as usual, but without entering the CommBox ip as source or

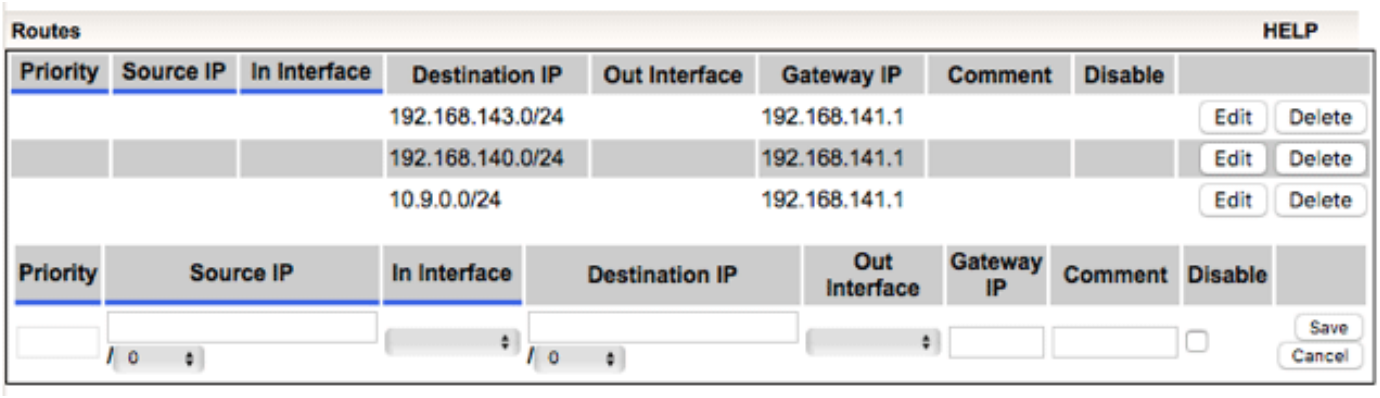
destination.

In most common setups, there is no reason to block outgoing traffic from the CommBox, i.e. entering the CommBox ip as source address in the firewall rule. For full functionality, the CommBox needs to be able to make connections out in order to check carriers and make connections.

Also note that you should never set up dnat for port 80 for anybody coming from a location that needs to access the web of the CommBox. Hasty configuration of this is one of the most common ways to lock yourself out from the CommBox.

14.5 Routes

In the "Routes" panel, you will find the route configuration. Here, you can configure routes like shown in this image:



If a DFP is activated, you will also see its rules.

In the screenshot above, one route is defined. [Edit] has been pressed, so there is a new line where you can change the route configuration.

Parameters used for source-based routing are:

Priority
: Where in the list of routing tables to insert this routing table. Valid priorities are from 1 to 10000. Also see the explanation below how the Source IP and In interface in combination makes up a routing table.

Source IP
: Designates the source for redirecting to this routing table, and works in combination with "In interface" below.

In interface
: Designates the source interface for redirecting to this routing table, and works in combination with "Source IP" above.

A combination of Source IP and In interface designates a routing table and as such all routes with this combination must have the same priority. If a priority is set, it will be entered automatically when making additional routes. If a priority is changed, it will be changed for all routes having the same Source IP and In interface combination.

The standard routing parameters are:

Destination IP
: The IP address for which the route applies. Next to it is a pull-down selection from which you can choose a subnet.

Gateway IP
: The IP address of the machine acting as gateway. This can be left empty if you only want to define an interface.

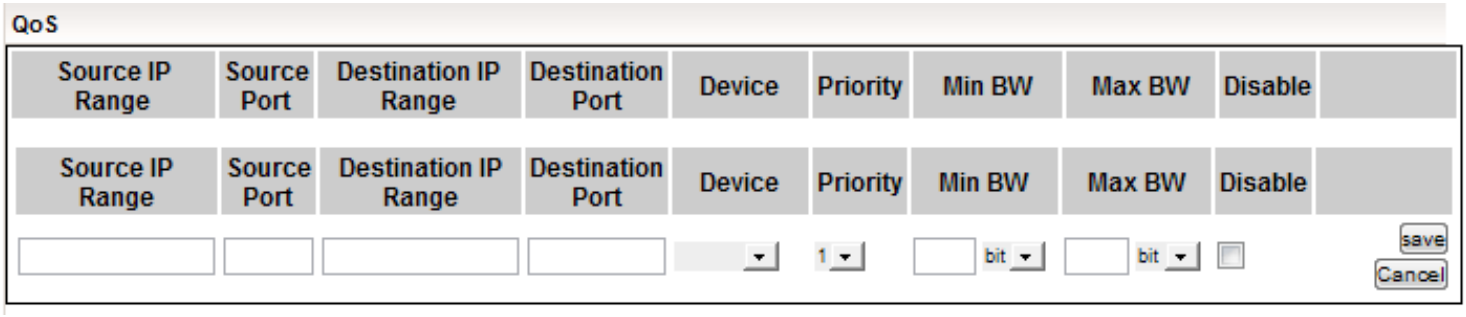
Out Interface
: The interface through which the traffic will be routed.

Standard routing parameters works in cooperation with source-based routing parameters. Standard may be filled without using the source-based routing parameters. Source-based routing parameters however, needs to be made complete using the standard routing parameters. The system will display an error if one mandatory parameter is not entered.

14.6 Quality of Service

Quality of Service (QoS for short) is used for prioritizing traffic. You can either set priority or you can set bandwidth limits for certain types of traffic. The important thing to remember is that, in order to use the network line to its full capabilities, you need to set "*Max BW*" to the line full bandwidth for at least one of the specified rules for the interface in question.

An overview of the QoS configuration is shown below:



If a DFP is activated, you will also see its rules.

For each rule, you must fill one and only one of the 'Source IP Range', 'Source Port', 'Destination IP Range', 'Destination Port' fields. Selecting a 'Device' is mandatory.

Device
: The network interface for which the rule applies. This is mandatory.

Priority
: Prioritise traffic. 1 is highest, 7 is lowest. The system will empty its queue for priority 1 first, then go to the priority 2 queue and so on.
When used in conjunction with Min BW and Max BW as described below, the bandwidth regulations will be considered before the priority.

Min BW
: Traffic matching the rule will not get less bandwidth that this.

Max BW
: Traffic matching the rule will not get more bandwidth that this.

At least one of the rules need to have this ceiling set to the highest capacity of the line or else you will never use the network to its full capacity.

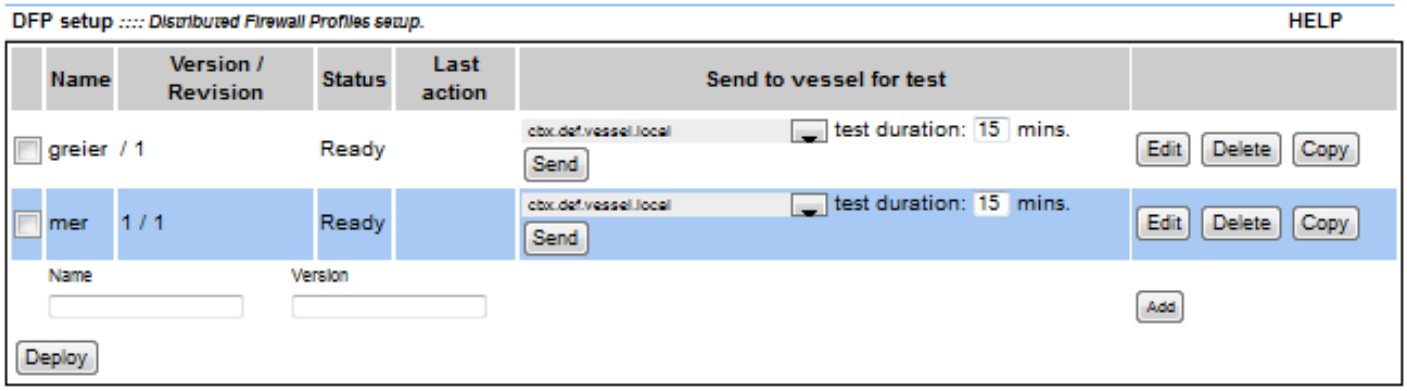
Disable
: You can temporarily disable a rule and enable it at a later time.

14.7 Distributed Firewall Profiles

The Distributed Firewall Profiles (or DFP) are sets of QuickWall rules (i.e. firewall, routes, QoS) defined on the hub and distributed to the vessels. On the vessels, it is possible to link each local QuickWall profile to a DFP. When this is done, the rules from the DFP are added to those of the local QuickWall profile.

For each type of DFP rule, it is possible to define a 'head' section and a 'foot' section. The rules in 'head' will be placed before the rules in the vessel's own QuickWall profile, and the rules in 'foot' will be placed after. When a QuickWall profile is applied, all rules will be taken into account.

14.7.1 DFP setup (hub)



The "DFP setup" table lists all the DFP defined on the hub. From here you can create, delete, start editing, distribute, or send for testing the DFP on the hub.

Version / Revision
: The version is the user-assigned version. the revision is a progressive number assigned by the CommBox: it indicates how many times the DFP has been edited. (More precisely: how many times "Activate changes" has been used while the DFP was in "Edited" status). The revision can be useful to determine if a vessel has the latest version of a DFP.

Status
: The status can be either "Edited" or "Ready".

  Edited
  : The DFP has been changed since the last time "Activate changes" has been clicked. (This means that some of the rules you see on the hub *may* not be the same as those on the vessels).

  Ready
  : "Activate changes" has been clicked since last editing. (This is not guarantee that the rules have been distributed to the vessels).

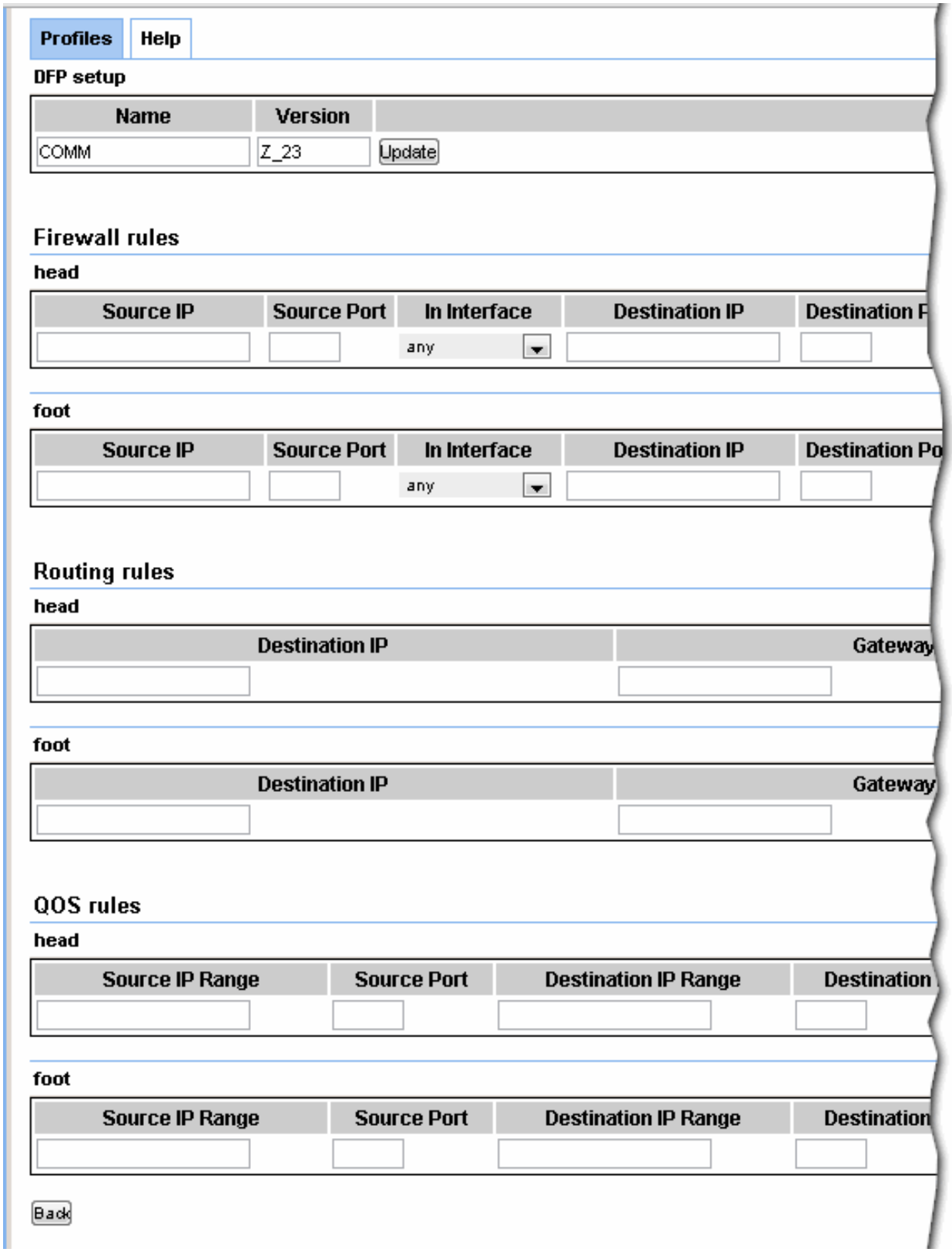
Last action
: This indicates what the last action ("Send for test" or "Deploy") was and when it was performed. Note that the time reported is the time when the DFP was put in the outgoing queue. There is no indication of when (or if) the vessel fetched the DFP.

Send
: To send a DFP to *one* vessel for testing, choose the vessel from the drop-down menu, select a test duration, and click [Send].

  The selected DFP will then be put in the out queue to be picked up from the vessel. Once it has been received on the vessel, it will stay active for the chosen time interval after which the original DFP will be restored. This is to safeguard against potentially isolating the vessel because of a wrong rule.

  The actual tests are performed manually and it is the tester's responsibility to ensure that the QuickWall profile in use on the vessel is linked to the test DFP.

Edit



The edit view is similar to that of a normal QuickWall profile view. Each Firewall, Routes, and QOS has a 'head' and 'foot' section. When a DFP is in use on a vessel the rules in 'head' will be placed before the rules from the local QuickWall profile, and those in 'foot' will be placed after.
The fields available for each rule type are the same as those for normal QuickWall profiles and have the same effect (see QuickWall). You can use references to the vessel configuration network interfaces and hosts on the fields 'Source IP', 'Destination IP', 'NAT To' of the firewall rules, 'Destination IP', and 'Gateway IP' of the Route rules, 'Source IP Range', and 'Destination IP Range' of the QOS rules.

Note that, when you use references, only their syntax is validated on the hub. That means that, for example, a value of 'IPlan(LAN7)' will be accepted even if no vessel has a 'LAN7' interface. A DFP referring to a non-existing interface or host will be inactive once it reaches the vessel (none of its rules will be used).

Copy

To make a copy of a profile with all its rules, click [Copy]. The new profile will be called "Copy of <origin profile name>", you can then change the name in the edit view.

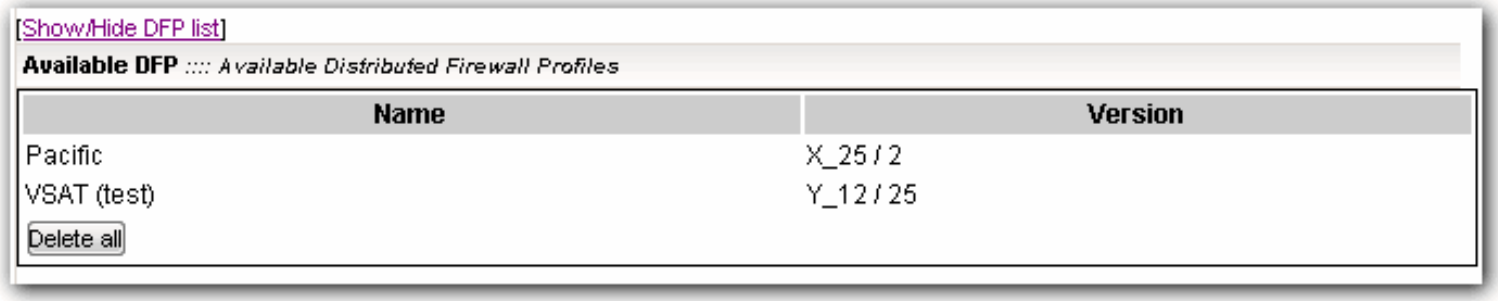
Add

To create a new DFP enter its name and a version name/number in the textboxes and click [Add]. You will then be directed to the 'edit DFP' view (see later).

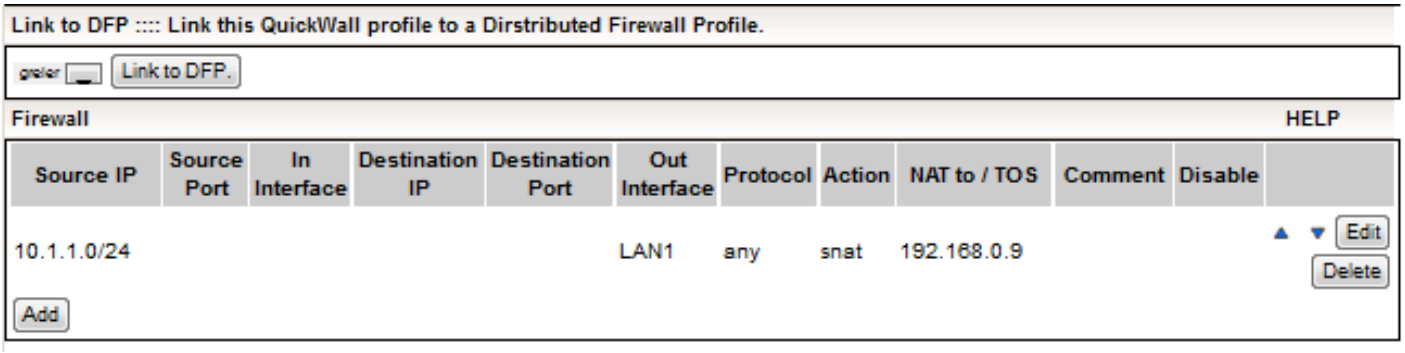
Deploy

To distribute one or more DFP to *all* the vessels linked to the hub, use the checkboxes in the DFP list and click [Deploy].
If one or more DFP have been edited, you will need click [Activate changes] before the [Deploy] becomes active.

14.7.2 DFP setup (vessel)

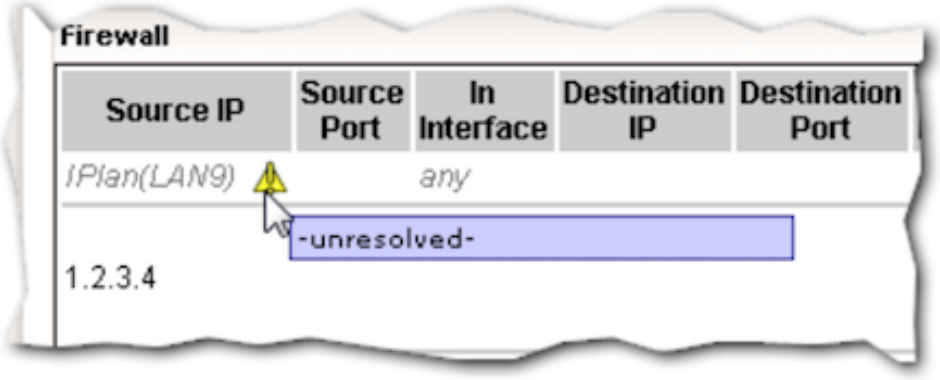


On the QuickWall page you can see a list of the DFP present on the vessel by clicking [Show/Hide DFP list]. You also have the possibility of deleting all DFP by using [Delete all]. It is not possible to see the rules from a profile without linking it to a QuickWall profile.
If the name of a profile is followed by "(test)", it means that the current version was sent as a test. There is no indication of when the test period will terminate.



When viewing or editing the rules for a local QuickWall profile, you can link it to a DFP: choose a DFP from the drop-down list in the 'Link to DFP' panel and click [Link to DFP].

The rules from the DFP are shown in grey above and below the local rules (the figure above shows only the firewall section). To see which concrete IP address is used in place of a reference, hold the mouse pointer over the reference.
It is not possible to edit or disable individual DFP rules on the vessel.

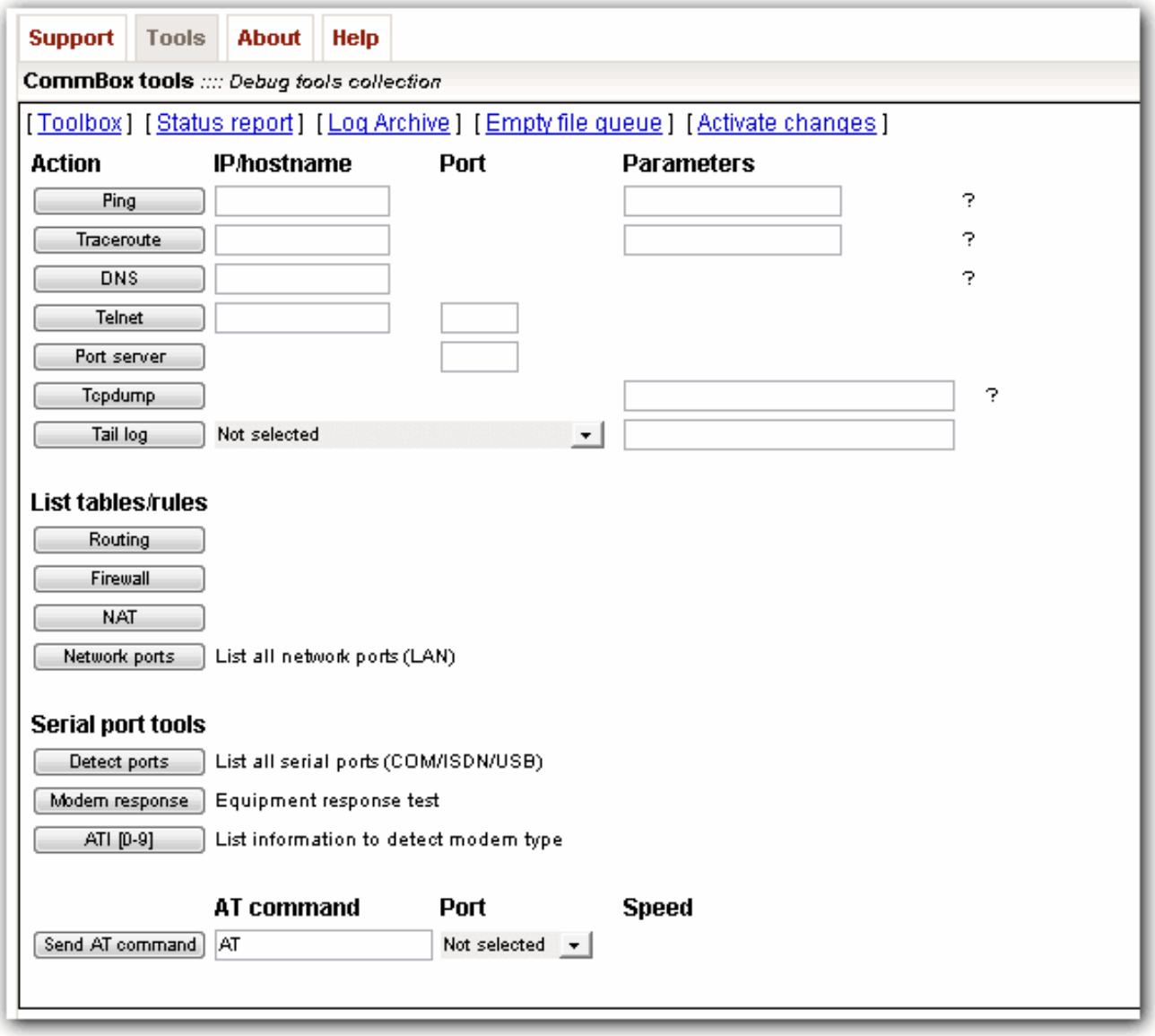


If a reference cannot be resolved, the whole DFP is rendered inactive and its rules are shown in italic. The references that cannot be resolved are marked with a yellow warning sign.

15 Tools

The CommBox has a built in set of tools that can help in debugging setups. They are available from "Support->Tools".

15.1 Toolbox



Every action has a corresponding button. To start an action, fill in the required fields and press the button. A new window will then open displaying the action's output.

You need to enable popups in your browser for this to work.

15.1.1 The actions

Ping and Traceroute
: These two options will either ping a host or trace the route to a host. You can use a host name in the ip/host name field if the host is registered in "Config->Hosts" or if it is available through dns lookups. If this is not the case, you must use an IP address.

DNS
: Will perform a name server lookup on either a host name or an ip (in which case the system will do a reverse lookup).

Telnet

Will open a simple TCP connection to a host, displaying everything that the server responds with. The port field must be filled out, all ports (1-65535) are valid.

Port server
: Will open the specified port on the CommBox. You can connect to this port from another machine (for instance using telnet) and all data you send to the port will be echoed in the opened window.

Tcpdump
: Shows all traffic matching the criteria specified in the "Parameters" field.

Tail log
: Will allow you to follow 'live' a log file as data is added to it.

15.1.2 List tables/rules

Routing
: Will show the routing tables currently active on the CommBox.

Firewall
: Will show all filter rules active on the CommBox.

NAT
: Will show all firewall rules that modify TCP packets. These rules can be the ones you defined in QuickWall with snat/dnat action, or they can be the rules that CommBox defines to make the QuickCrew and QuickCrew systems work.

Network ports
: Will list all network interfaces on the CommBox.

15.1.3 Serial port tools

Detect ports
: Will show serial ports on the CommBox.

Modem response
: Will perform a basic response test on all modems connected to the CommBox.

ATI[0-9]
: Will send the ATI0 through ATI9 commands to connected modems. These commands usually report what kind of equipment is connected. Some modems, for example those from US Robotics, may display detailed information. Others, only display their name.

Send AT command
: Allows you to send any AT command to a port of your choice.

15.2 Toolbox functionality in other modules

Some debugging tools are found in the setup pages of the modules to which they refer.

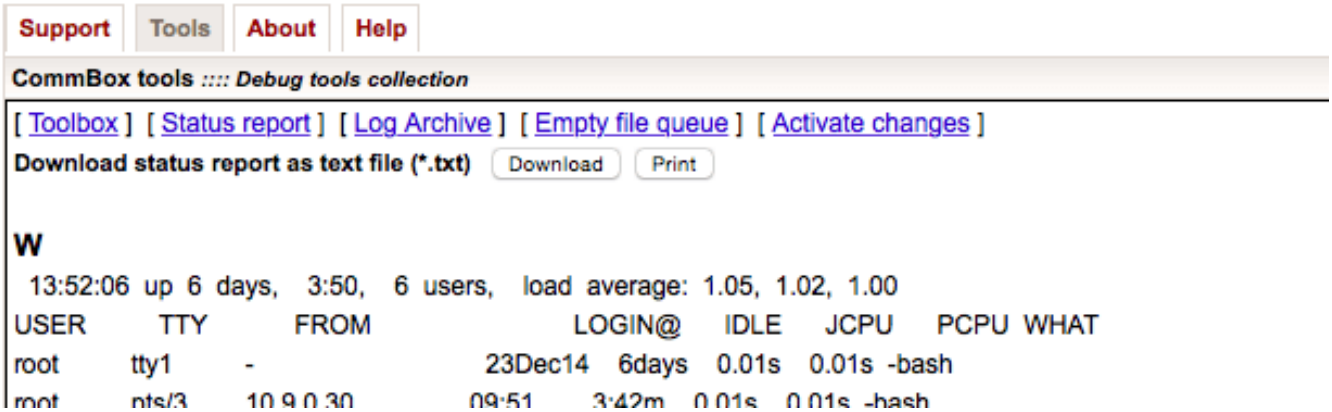
15.2.1 Fetchmail

Under "QuickMail->Fetchmail" you can test a setup by hitting [Test] in the rules list. The test tries to perform a connection to the mail server.

15.2.2 QuickFile

Under QuickFile, a profile may be tested by hitting [Test]. The test will connect to the server using the specified credential. It will continue by making a file to check for write permissions, then delete the same file. It will then disconnect.

15.3 Status report



This page gives an overview of the CommBox current status. In addition to showing the information in this browser page you can download or print the same information.

The sections shown are:

W
: Show who is logged on and what they are doing.
For more details see *UNIX man page 'w'*.

DF
: Report file system disk space usage.
For more details see *UNIX man page 'df'*.

IFConfig
: View and configure network interface parameters.
For more details see *UNIX man page 'ifconfig'*.

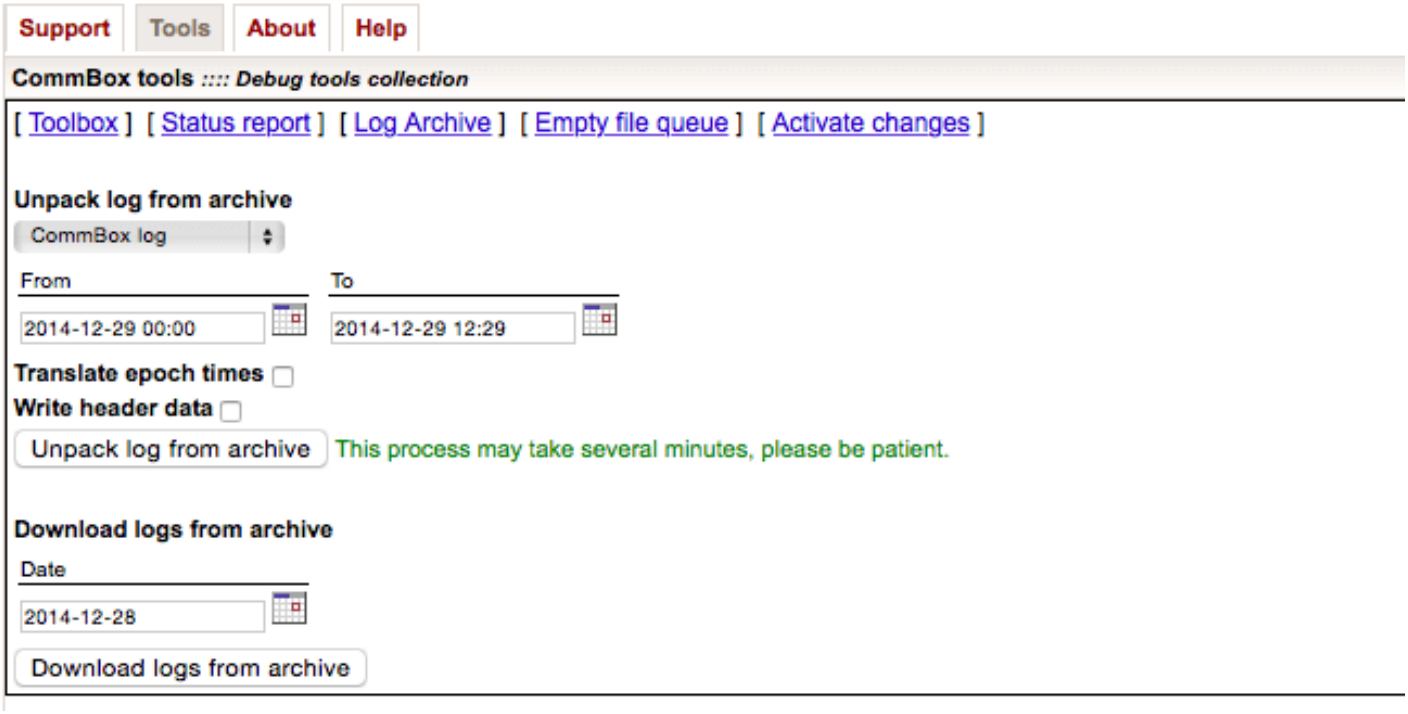
Client browser info
: Views the version info of the browser in use.

DMESG
: Prints out the bootup messages.
For more details see *UNIX man page 'dmesg'*.

Process list
: Report a snapshot of the current processes.
For more details see *UNIX man page 'ps'*.

Listening and active internet sockets
: Print network connections, routing tables, interface statistics, masquerade connections and multicast memberships.
For more details see *UNIX man page 'netstat'*.

15.4 Log Archive



15.4.1 Unpack log from archive

Here you can unpack and download a specific log for a specific time span.
Select, from the drop-down, one specific log, and set the time span with the time/calendar dialogs. Use the checkboxes for 'Translate epoch times'* and 'Write header data' if you want time translation and or column headers.
The processing of the download file will take some time, dependent of the time span given.
* *Only Unix timestamps will be translated.*

15.4.2 Download logs from archive

Here you can download one archive file containing all logs for one specific day.
Select the day in question, and hit [Download]. If there isn't any archive for the selected date, you will be warned.

15.5 Empty file queue

15.5.1 Empty file queue

In some cases / situations you will need to get rid of queued files from the File Queue. Check the check box and and hit [Empty file queue], that will be enabled when you check the check box.

15.6 Activate changes

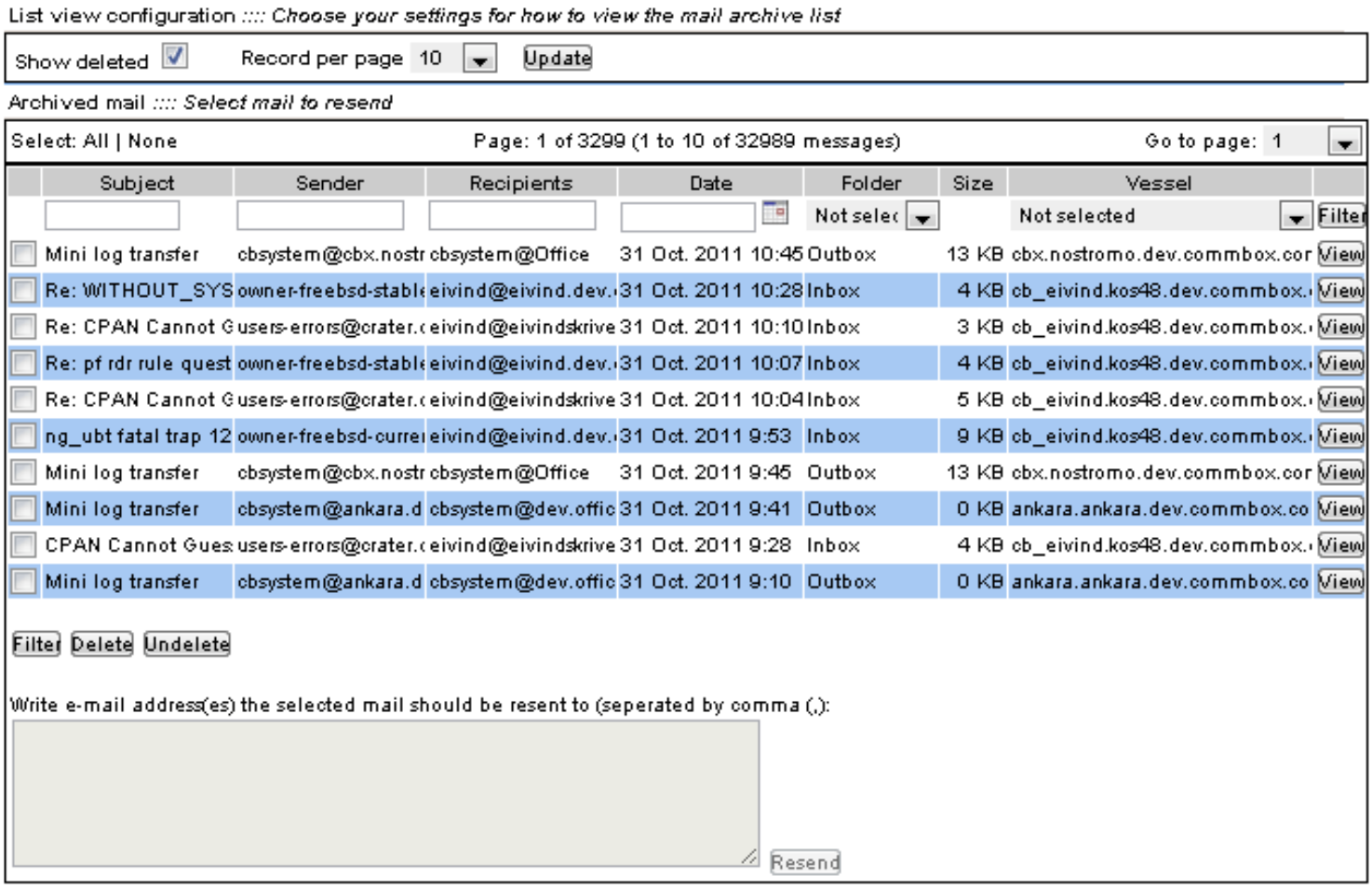
15.6.1 Activate changes

In some cases / situations you will need to force the Activate changes function. Check the check box and hit [Activate changes], that will be enabled when you check the check box.

16 Archive (hub)

The CommBox can be configured to archive files transferred. You can choose which type of files to archive and how long to keep them.

To access the configuration form, click on [Archive] in the left menu. Form the "Archive->Mail archive" page you can see a list of all the archived messages



16.1 List view configuration

Here you can define whether to show deleted files and how many records to show in each page of the archive list

16.2 Archived mail

Here is the list of all the archived messages. Use the drop down box next to **Go to page:** in order to navigate to other pages if the archive contains more records than displayed.

The columns shown are:

Subject

For emails, this is the subject of the message, for other transfers it is a short description of the transfer itself (for example "Mini log transfer").

Sender

The addresses of the sender of the message. This can be either the email of a real person or the identifier of a CommBox (for example "cbsystem@officehub.commbox.com")

Recipient

The addresses of the recipient of the message. This can be either the email of a real person or the identifier of a CommBox (for example "cbsystem@officehub.commbox.com")

Date

The date the message was transmitted.

Folder

Files are stored in three folders:

Inbox

transfers to a vessel.

Outbox

transfers from a vessel.

Trash

deleted archive items.

Size

The size of the uncompressed message.

Vessel

The vessel that received or sent the message.

16.2.1 Filters

It is possible to filter the message list by using the input fields shown above the list. The wildcard character '%' will match any number of any character. Note that the filter does a full match on the field in question. So, if you want to filter for all subjects containing the word 'report', you must enter '%report%'.

In order to filter by date, click the calendar icon in the date column. Filtering by date will show all transfers happened on the selected day.

When you are finished composing you filter, click [Filter] to update the list view.

16.2.2 Preview

To view an archived e-mail click [View] on the right hand side of the records line. This will show the content of the mail in a simple interface.

16.2.3 Resend (Forward)

To forward an archived e-mail, select it in the checkbox on the left side. The text area at the bottom of the page will then be enabled. Type in the e-mail address(es) of the recipient(s) separated by comma, and click [Resend].

16.2.4 Delete / Undelete

The deletion of archived items is a two step process similar to the use of the 'Recycle bin' on a computer desktop: first the message is put in the trash folder and from there it can then be either completely removed or restored:

1. Select the items you want to delete by using the checkbox on the left side of the list and click [Delete]. This will transfer the selected items to the trash folder.
2. To completely delete an item in the Trash folder, select it and click [Delete] again.

To remove an item from the Trash folder, select it and click 'Undelete'. The item will then be transferred back to its original folder.

16.3 Mail archive configuration

From "Archive->Configuration" you can define for how long to archive each different type of transfer.

Transfers are divided in 4 categories:

E-mail

Email sent and received by CommBox administrative users.

QuickFile
: Files transferred using the QuickFile utility.

Roaming user e-mail
: Email sent and received by crew members.

CommBox system messages
: Transfers related to CommBox operations, for example usage data transfer, updates received from hub, etc.

You can configure the archiving of each category:

Enabled
: Files are archived.

Store for _ month(s)
: Sets how long you want to keep files in the archive. Only integer values allowed, decimal numbers will be rounded. Non-numeric values will be interpreted as zero.

Action
: Defines what action is taken when there are files that have been stored for longer than the defined limit.

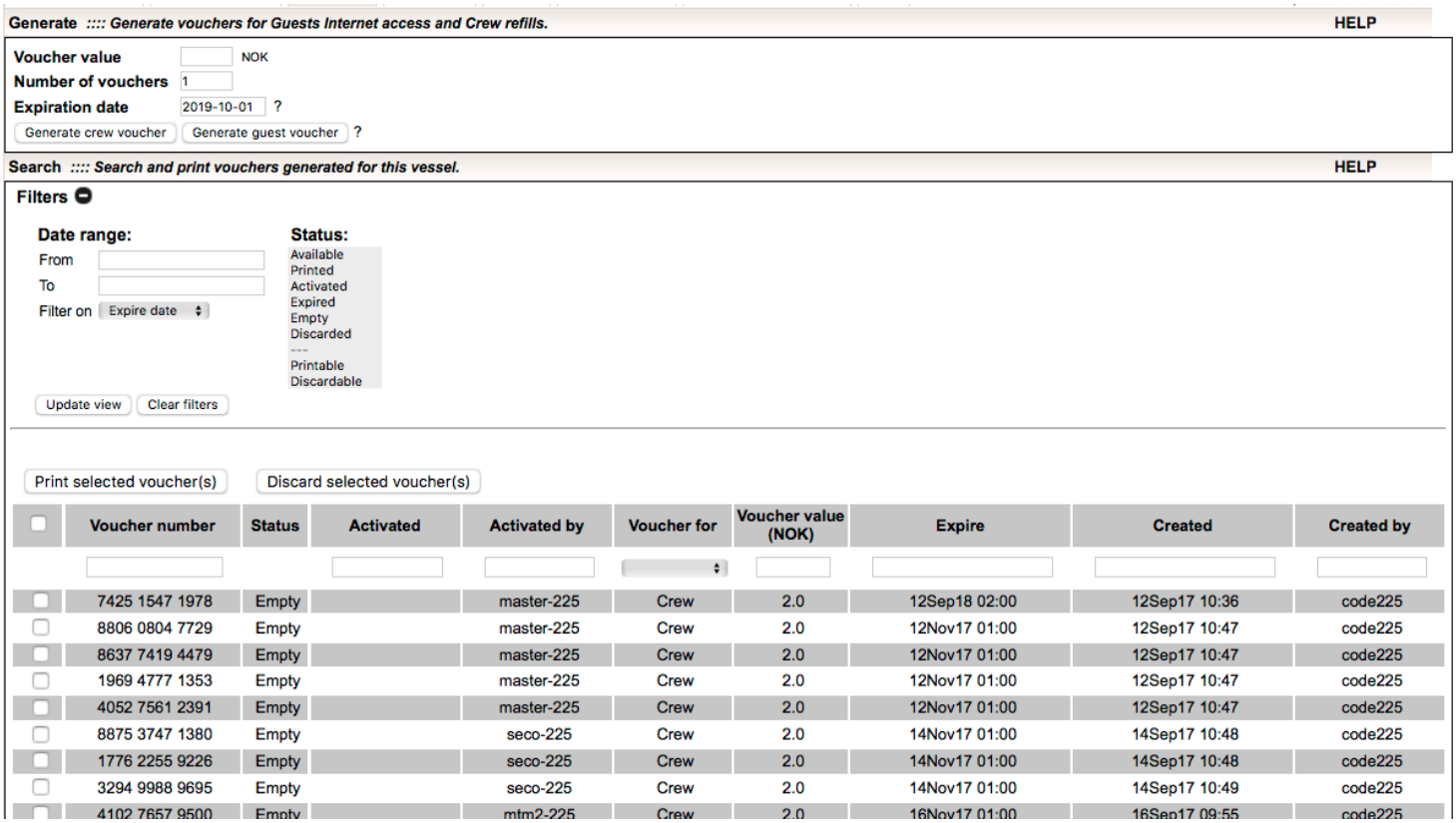
  Auto delete
  : Files are deleted.

  Warning
  : A warning mail is sent, the recipient of the email is the address defined in "Config->System monitor Storagemonitor".

17 QuickCrew

To be able to take the QuickCrew user system into use on a vessel, you need to enable, see Configuring QuickCrew access (vessel) for how to.

17.1 Vouchers



Voucher number	Status	Activated	Activated by	Voucher for	Voucher value (NOK)	Expire	Created	Created by
7425 1547 1978	Empty		master-225	Crew	2.0	12Sep18 02:00	12Sep17 10:36	code225
8806 0804 7729	Empty		master-225	Crew	2.0	12Nov17 01:00	12Sep17 10:47	code225
8637 7419 4479	Empty		master-225	Crew	2.0	12Nov17 01:00	12Sep17 10:47	code225
1969 4777 1353	Empty		master-225	Crew	2.0	12Nov17 01:00	12Sep17 10:47	code225
4052 7561 2391	Empty		master-225	Crew	2.0	12Nov17 01:00	12Sep17 10:47	code225
8875 3747 1380	Empty		seco-225	Crew	2.0	14Nov17 01:00	14Sep17 10:48	code225
1776 2255 9226	Empty		seco-225	Crew	2.0	14Nov17 01:00	14Sep17 10:48	code225
3294 9988 9695	Empty		seco-225	Crew	2.0	14Nov17 01:00	14Sep17 10:49	code225
4102 7657 9500	Empty		mtm2-225	Crew	2.0	16Nov17 01:00	16Sep17 09:55	code225

The CommBox Voucher tool provides with you a system for handling vouchers for your crew and guests embarked your vessel. For more information about the two user categories, crew and guest, see QuickCrew users: Guest vs Crew accounts

The Voucher tool is part of the CommBox QuickCrew module and include the following functionality.

Highlights:

- ◊ One dedicated user for voucher administration
- ◊ Voucher / user handling by all officers, based on permission setup
- ◊ Voucher administrator can see user status and transaction log
- ◊ Tracking of voucher status
- ◊ Different vouchers for crew and guests
- ◊ Voucher only valid on vessel where generated
- ◊ Direct refill of crew accounts via vouchers
- ◊ Crew can purchase *surf time* (voucher)
- ◊ Printed vouchers for handout
- ◊ Discard/credit vouchers that are not taken into use
- ◊ Mass generation and printout of vouchers
- ◊ Voucher limited by amount and expiry time

At top in the ***Generate::::Generate vouchers for Guests Internet access and Crew refills.*** section you can generate voucher to be used by crew or guests. Specify amount, number of equal vouchers and date of expiry, hit [Generate crew voucher] or [Generate guest voucher]. The confirmation dialog will display and you can choose to generate and print or just generate the vouchers.

The vouchers generated are only valid on the vessel where they are created.

Below is the ***Search::::Search and print vouchers generated for this vessel.*** section that is used for voucher inspection and administration.

Table contains the following information

- Voucher number
  - Guest: 8 digits username, last 4 is password
  - Crew: 12 digits refill code
- Status
  - Available: generated
  - *Printed*: generated and printed
  - *Activated*: used
  - *Expired*: passed expiry date
  - *Empty*: user has used the amount given on the voucher
  - *Printable*: combines Available + Printed
- Activated
  - When the voucher was taken in use
- Activated by
  - Username of whom that activated (used) the voucher
- Voucher for
  - Voucher generated for Crew or Guest, or used for Direct refill
- Voucher value (*currency*)
  - Value of voucher
- Expire
  - Time when voucher isn't valid anymore
- Used by
  - *Crew*: username of crew member
  - *Guest*: username, see voucher number above
- Created
  - Date of generation
- Created by
  - Username of whom that issued the voucher

You can search for one particular voucher by entering some voucher details and hit [Update view] or just by typing in the column search boxes. For sorting, just hit the column header once for ascending and once again for descending.

Discard/credit voucher(s)
To discard (i.e. credit) one or more vouchers, it is recommended to filter by the status so only voucher that may be credited are shown. A voucher must have status "Available" and "Printed" (Creditable-filter may also be used) in order to be credited. Select the vouchers to credit using the checkbox, and click "Discard selected voucher(s)".

17.2 QuickCrew users: Guest vs Crew

CommBox distinguishes between two QuickCrew user types: Crew and Guest.

Each **Crew** member can have a personal account which enables web surfing and e-mail use. This type of account is called "Roaming account" because it follows the crew member as he embarks vessels within the same fleet.

Each **Guest** is local to each vessel and the guest has no roaming functionality. A guest account is only granted internet access.

The chapters about user configuration on HUB are not valid for Guests.

The web surfing activity of each user, crew or guest, can be limited in terms of:

- Time spent online via the "Max online time" setting of the account type, see Account types for roaming accounts (hub).

- Amount of data transferred via the credit handling system,
  see Account types for roaming accounts (hub)
  and Configuring QuickCrew access (vessel).
- Number of people that can use the Internet at the same time via the "Max concurrent connections" settings,
  see Configuring QuickCrew access (vessel).

Data for each crew user's account is kept on the hub. At the first login to a vessel CommBox, the CommBox will notify the hub that the user is on that particular vessel. The hub will then send all necessary data for his account to the vessel.

Whenever necessary, the hub will be notified about changes to the crew users account, for instance his remaining balance to use for surfing or for mail.

Data for each guest account is kept locally on the vessel.

17.3 Costs - Crew member

Each user account is assigned credits (see later) that can be spent for sending/receiving emails and Web surfing. The amount deducted from the user's credits is determined by the cost profile linked to the active connection during transfer or surfing (see Cost (vessel)).

Each crew user has two types of credits:

Purchased credits
: These are the credits assigned to the user via vouchers, direct refill to account, or the KVH CREWlink credit system.

Free credits
: These are the credits assigned to the user via the periodical refill set up in his user account.

The purchased and free credits are stored separately and the credits amount shown is always the sum of the two. The free credits are used in preference: the paid credits are used only when there are no more free credits available.

17.4 Costs - Guests

Each user account is assigned credits (see later) that can be spent for Web surfing. The amount deducted from the user's credits is determined by the cost profile linked to the active connection during surfing (see Cost (vessel)).

Purchased credits is the only valid credit type for guests.

17.5 Mail - Crew member

When a user is registered on a vessel, all email destined to him will be delivered to the vessel. The user can then access it either via the CommBox webmail client (Webmail client) or via an external POP3 or IMAP4 client (Outlook, Eudora, etc.). Emails that the user received before embarking on the current vessel are stored on the office hub. A user can request that selected messages from the archive be forwarded to his current vessel.

When a user is on shore, his mail will be archived in the CommBox QuickArchive system. The user may read his mail by entering the archive from his "*My Account*" page.

17.6 Mail - Guests

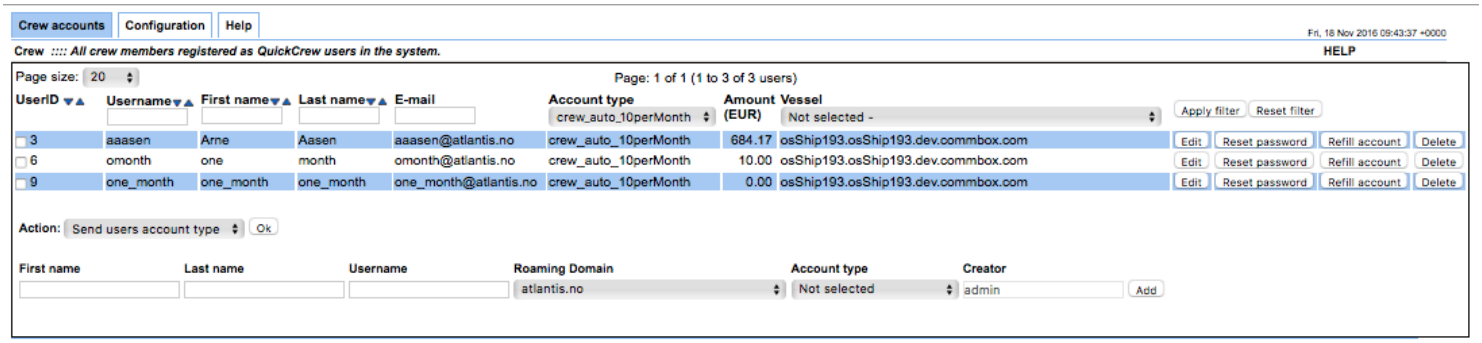
Mail delivery is only available for crew, please use a Webmail client for accessing your email.

17.7 Surfing - Crew and Guests

Every crew member will have the ability to surf the web or access other services as long as the firewall configuration permits it. If the user is trying to reach the Internet from a network defined as "billing network" (see later) he will be asked to login

before being allowed to make any connection. After a successful login, a popup window with live credit information will appear. The connection will be interrupted if the popup is closed.

17.8 Configuring - Crew member (hub)



From the menu selection "QuickCrew->Crew accounts" you will reach a page where all crew accounts currently configured are listed. From this list you can choose to edit or delete users.

17.8.1 Create new user

Below the list is a form that allows you to create a new user. Enter the desired parameters and click on [Add].

First name - Last name
: First and last name of the user.

Username
: The username used for login. The value is auto-generated based on first- and last-names but you can override this. Length of username is minimum 2 and maximum 25 characters and the first on must be a letter (a-z). If a username is already in use or containing an illegal character you will get an error message when saving.

Roaming domain
: The domain that will be appended to the username to form an email address.

Account type
: The type of account for the new user.

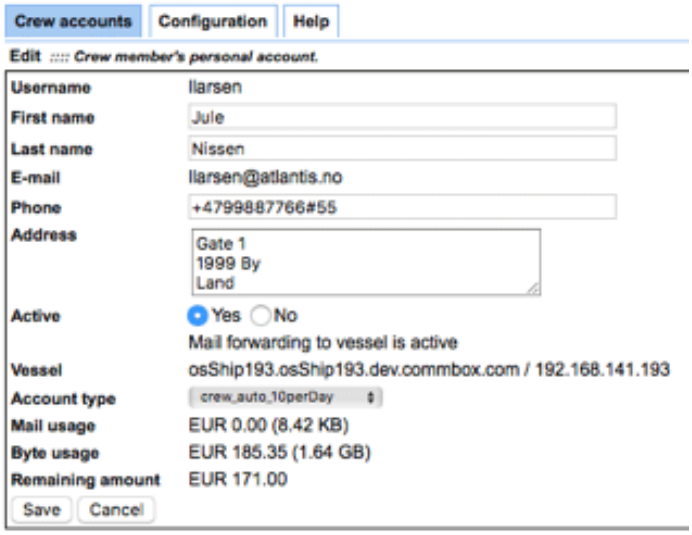
Creator
: The user that is creating the new account. This field cannot be changed.

E-mail
: The address is auto-generated from the username and roaming domain: "<username>@<roaming domain>". This field cannot be changed.

Most of these settings can be changed later form the edit user view.

17.8.2 Edit user data

[Edit] brings up the edit view:



From here most of the user information can be changed. The page also displays an overview of the user's balance as well as statistics regarding how much data/traffic the user has generated.

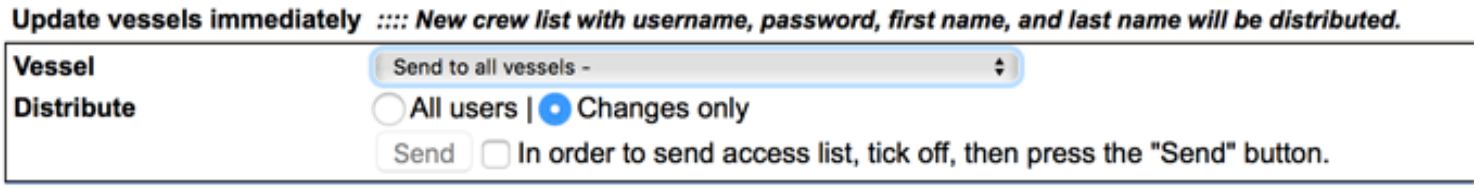
What you see on the hub is data transferred from the vessel. There may have been changes made on the vessel that have not been transferred yet.

17.8.3 Force distribution to vessels

Crew account data is regularly distributed to vessels. You can force a transfer to a vessel or to the entire fleet.

Sign off messages will be issued for all users that are deleted (by import), shown in *Crew accounts* with strikethrough.

Deleted users will be removed from *Crew accounts* when all vessels has be notified.



Field description

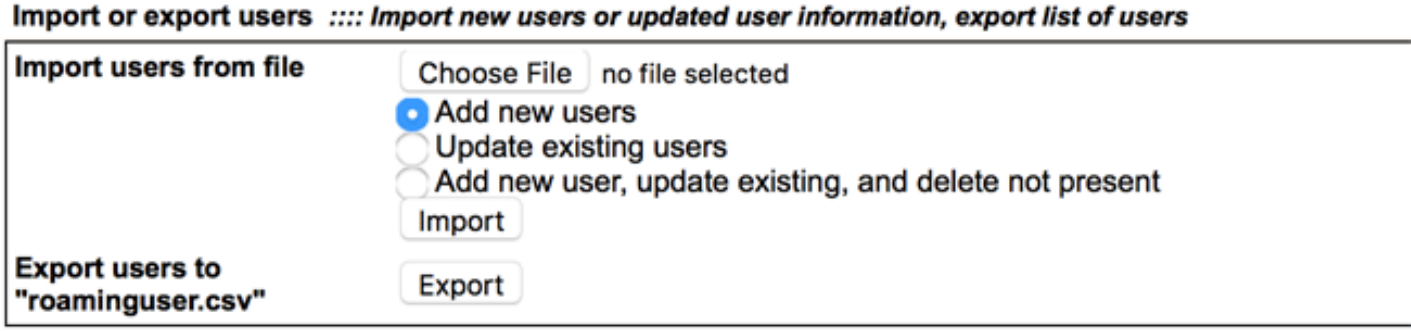
- Vessel
  - Options (dropdown):
    - Send to all vessels
      - This option will queue the user list to all vessels in the fleet.
      - The other vessels will get the user list at next regular distribution interval.
    - 'Vessel name'
      - This option will queue the user list for this vessel only.
- Distribute
  - Options (radio buttons):
    - All users
      - A complete user list of users will be queued.
    - Changes only
      - The user list queued will only contain users that has been changed, like: refill, name change or deleted
  - [Send]
    - Check the checkbox *In order to send acce...* and then [Send] to queue the user list.
    - Only vessels with QuickCrew enabled will have the user list queued.

17.8.4 Import or export users

It is possible to exchange user data with other crew management systems go to ***Import or export users::::Import new users or updated user information, export list of users*** for this operations.

Import

From this panel, it is possible to manage crew users' data by means of CSV (Comma Separated Values) files. You can read and edit CSV files with most spreadsheet programs (Microsoft Excel, OpenOffice Calc etc.). See Appendix: Fields in the import/backup/restore roaming (crew) users files for a description of the fields in the files.



From here you can import a file listing crew users and choose which operation to perform:

Import users from file

Add new users

All the users in the file that are not already in the database will be imported. Already existing users (i.e. those with a username that is already in the database) will be ignored and counted as "duplicates" in the report.

Update existing users

All the users in the file with a username that is already in the database will be updated. All other users in the file will be ignored and counted as errors.

Fields that are not in the input files will remain untouched in the database.

Add new user, update existing, and delete not present

Users in the uploaded file and in the database are matched by username. Those not present in the database are added, those present will be updated, those not present in the file will be marked as deleted in the database. They will appear as struck through in the list on the Web interface. Users marked as deleted are not allowed to use quick crew. You can 'revive' deleted users with the update function.

After you upload a file, you will be presented with a report detailing the number of user that will be added, updated, or deleted from the database. In addition, you will also be notified of possible errors or duplicates in the import file.

The [View] link next to each line will open a popup showing the lines in the imported file to which the report applies.

If you are happy with the report, click [Perform import] to finalize the import. If you choose [Cancel] or navigate away from the page, no changes will be made to the database.

After you have finalized the import, you will again see a report of the user added, modified, or inserted.

If you let the CommBox generate random passwords, the only way in which you can see which passwords have been assigned is to click on the [View] link at this point. The [Export users] function will only show the encrypted passwords.

To distribute immediately the new user data to one or all vessels, use the controls in the "Update vesseles immediately" panel (see Force distribution to vessels above).
If you do not do this, data for the new, changed and deleted users will be distributed to all vessels at midnight.

Export

Hit [Export] and the crew user list will be exported (written) to a predefiend file (roaminguser.csv) in the "download" folder on your pc. The format of this file is the same as that used for import; so you can export a file, edit it, and import it.

17.9 Crew Managment RESTful API (hub)

Crew Managment Systems can integrate with CommBox's crew handling system via the RESTful API available on CommBox HUB. We have used SWAGGER tools for creating and documenting of the api, see SWAGGER (external link)
For more information about the RESTful API please contact us at KVH, see Contact information

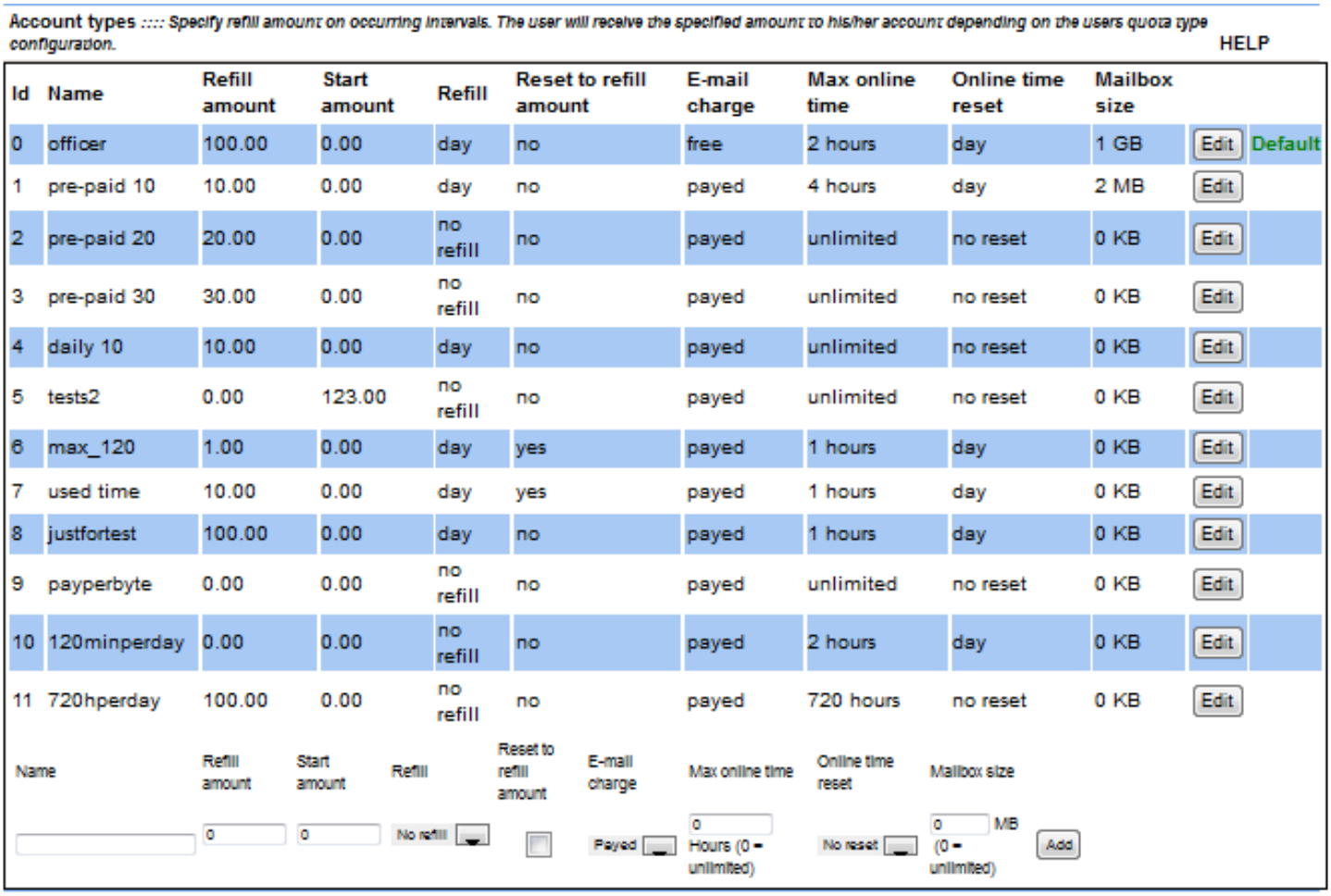
17.10 Roaming mail domains (hub)

From "QuickCrew->Configuration" you can manage roaming mail domains. These are the mail domains that will be used for roaming users.

You can assign a mail domain to users from the "QuickCrew->Crew accounts" page (see Create new user)

17.11 Account types for crew accounts (hub)

Account types define how credits are handled for crew, how much time they can spend using the Internet, and how much space each user is allowed to occupy. Accounts are administered from "QuickCrew->Configuration".



It is possible to set a periodical credit refill to an account: at a defined frequency, a set amount of credits will be added to all active crew accounts of the specified type. These credits are stored separately from those purchased. The purchased credits will be consumed only when the automatic "free" credits are exhausted.

It is also possible to limit the amount of time spent surfing the Internet within a determined time period (day / week / month). Once the allowed time has been used, the user will not be able to use the Internet until his time allowance is reset.

Id
: An internal identifier unique for each account type.

Name
: A name describing the account.

Refill amount
: How much should be added for each periodical refill.

Start amount
: The amount of credit added to the user when the account is created.

Refill
: How often the account credits should be refilled. You can choose to refill credits at 00:05 every day / every Monday / every 1st day of the month.

Reset to refill amount
: If set to yes, each periodical refill will reset the credits to the "Refill amount" rather than add more credits to what is already in the account.

E-mail charge
: You can decide whether e-mail transfers will be free or not.

Max online time
: How much time can each crew member can spend surfing the Internet within the period defined in "Online time reset".

Online time reset
: The time period to consider when limiting the online time. The time allowance will be reset to "Max online time" at 00:05 every day / every Monday / every 1st day of the month.

Mailbox size
: The maximum amount of disk space that the user can occupy with his emails.

17.11.1 Create an account type

To create a new account type, fill in the form below the account types list and click [Add].

17.11.2 Edit an account type

To edit an existing account type, click [Edit]. The form below the account types list will be filled with the details of the account type. Make your changes there and press [Save] to save.

17.12 Password generation (hub)

Each time a new user is created, they are assigned a password. From the "Crew user password generation" panel it is possible to choose whether this will be an auto-generated random string or a fixed string. In either case, the crew user will be able to change the password from the 'My Account' page.

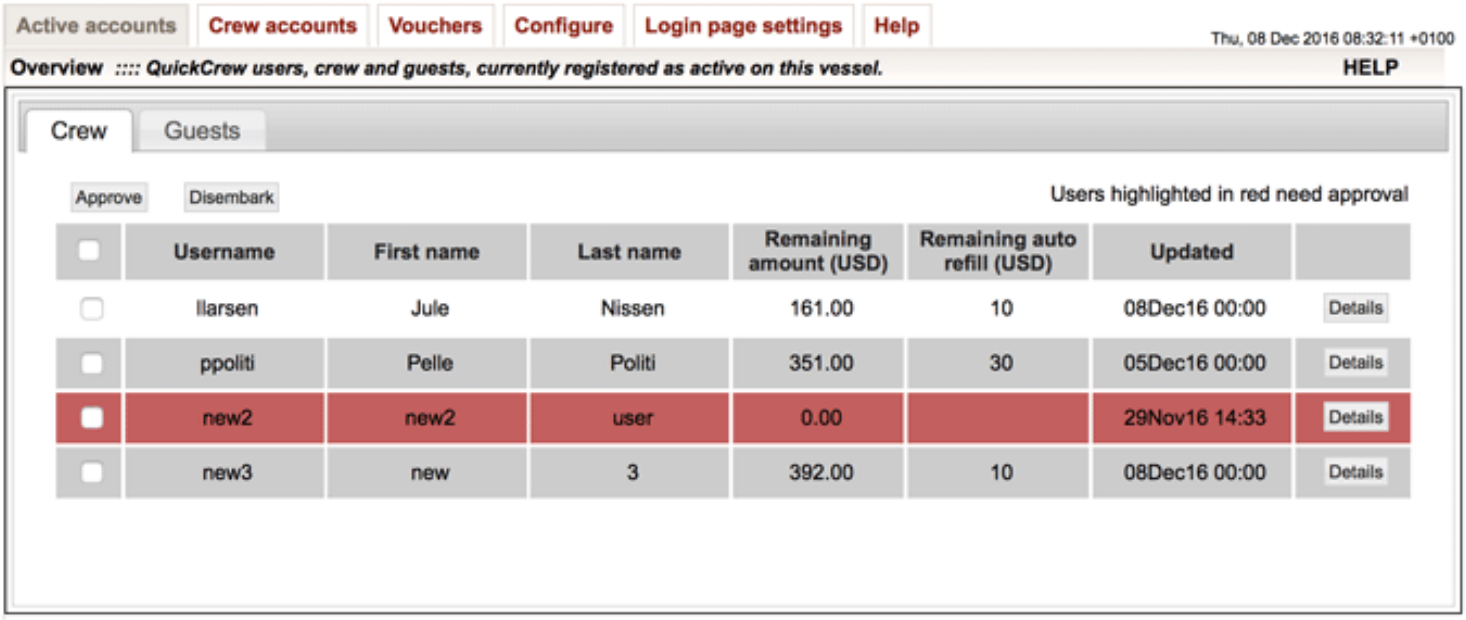
17.13 QuickCrew - Active accounts (vessel)

As described above we have two types of QuickCrew users, crew and guest. The management and available information about the two is slightly different. For management of Crew or Guest.

From "QuickCrew->Active accounts" you can see all QuickCrew users, crew and guests, currently registered as active on this vessel.

17.13.1 Active accounts - Crew users

Overview::::QuickCrew users, crew and guests, currently registered as active on this vessel.



Actions
: You can perform actions only on the accounts of users registered on the vessel.

  Approve
  : If you have ticked the *Require signon approval* checkbox in the QuickCrew Configuration, you are required to approve the crew members before they get access.

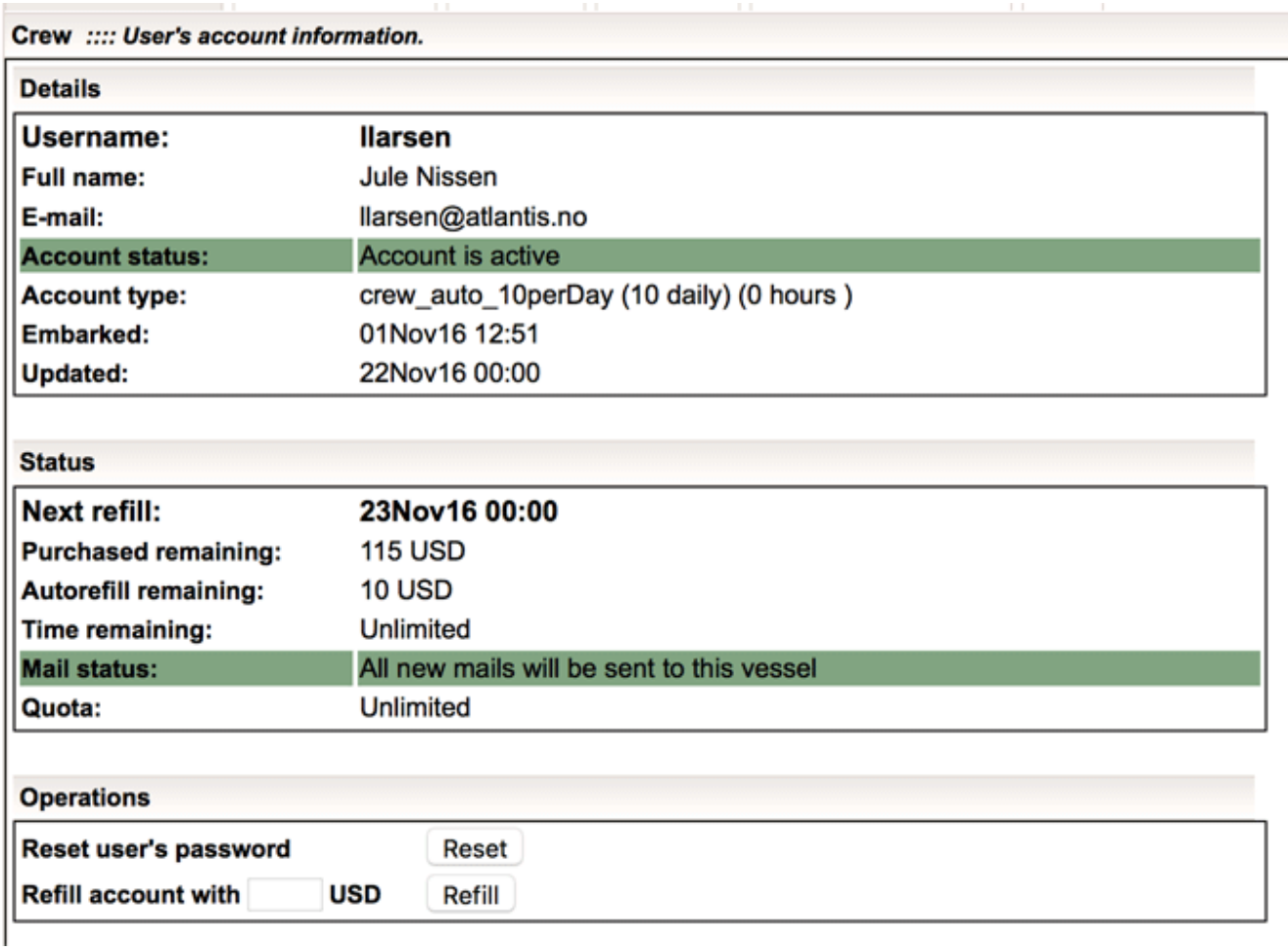
  Disembark
  : You can disembark a crew member; this will block their already given access.

Details

Displays account information, see below.

Details view

Account information

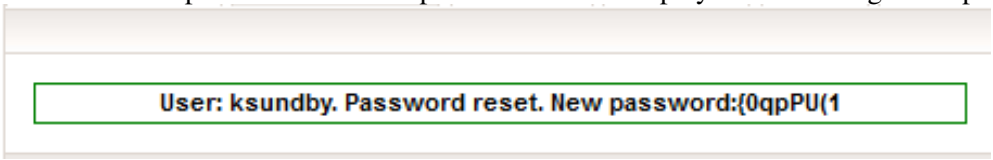


Actions

From the ***Crew::::User's account information*** you have access to two actions.

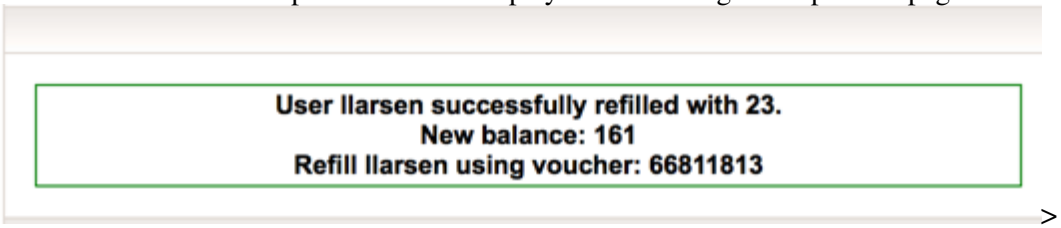
Reset password

Resets the user password. The new password will be displayed in a message on top of the page:



Refill

Refill crew member's account, credits are immediately added to the user's account using a voucher. Feedback from the refill process will be displayed in a message on top of the page:



>

Transaction log

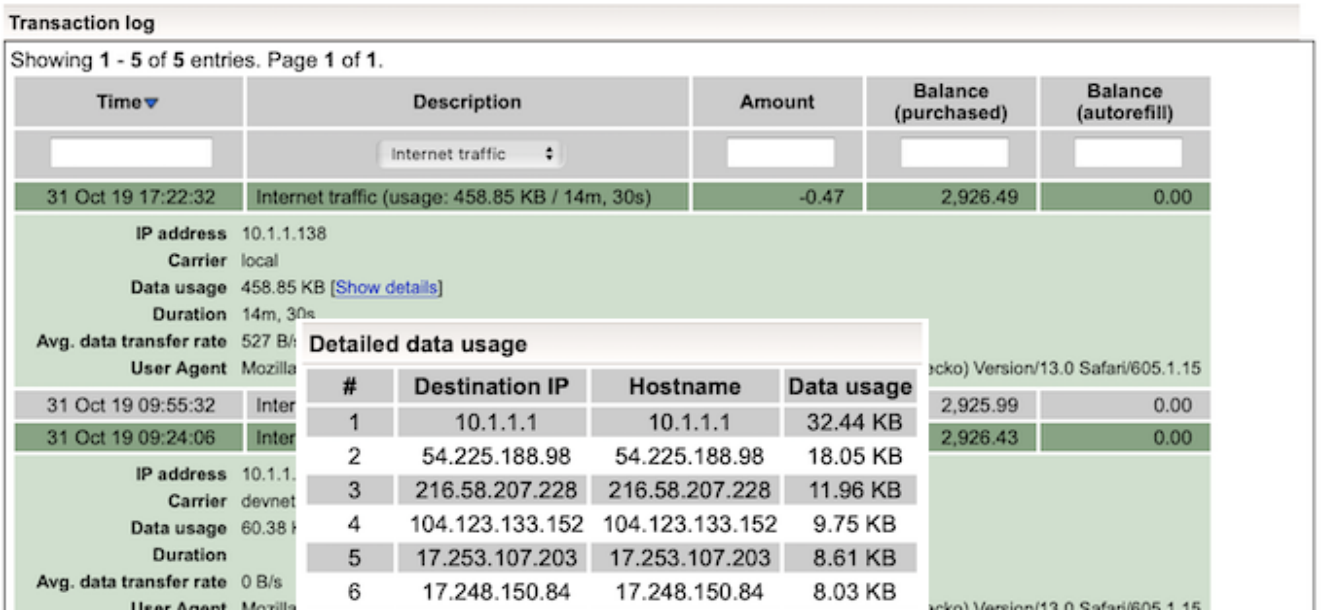
In the screenshot below, each row represents a transaction for a user with the amount deducted or added, as well as the purchased and autorefill balance after the transaction took place. Each row is expandable to show more details about the transaction. All columns are sortable and it is possible to filter out certain rows. For the time column, the start date is specified and the system will automatically show transaction for the next 24 hours from the start date. Please note that the list is sorted by transaction datetime in a descending order as default.

Transaction log

Showing **1**-**23** of **23** entries. Page 1 of 1.

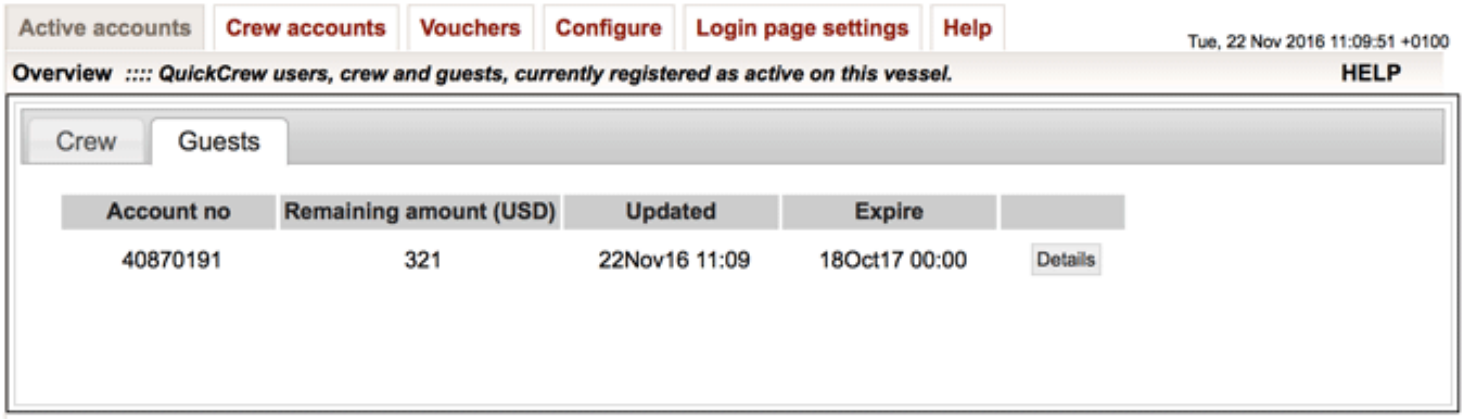
Time	Description	Amount	Balance (purchased)	Balance (autorefill)
15 Feb 18 00:00:02	Auto refill	50.00	686.00	6,065.16
14 Feb 18 00:00:02	Auto refill	50.00	686.00	6,015.16
13 Feb 18 12:55:17	Direct refill (voucher: 30376075)	123.00	686.00	5,965.16
13 Feb 18 00:00:02	Auto refill	50.00	563.00	5,965.16
12 Feb 18 16:38:02	Mail transfer (usage: 1.41 KiB)	-0.00	563.00	5,915.16
12 Feb 18 16:29:35	Mail transfer (usage: 0 B)	0.00	563.00	5,915.16
12 Feb 18 16:24:41	Mail transfer (usage: 1.41 KiB)	-0.00	563.00	5,915.16
12 Feb 18 16:07:26	Mail transfer (usage: 1.02 MiB)	-1.02	563.00	5,915.16
12 Feb 18 16:04:02	Internet traffic (usage: 1.30 MiB / 3m, 40s)	-1.30	563.00	5,916.18
IP address	10.1.1.117			
Carrier	devnet			
Data usage	1.30 MiB			
Duration	3m, 40s			
Avg. data transfer rate	6.04 KiB/s			
12 Feb 18 16:02:00	Mail transfer (usage: 1.02 MiB)	-1.02	563.00	5,917.48
12 Feb 18 15:51:12	Auto refill	50.00	563.00	5,917.48
12 Feb 18 15:50:39	Direct refill (voucher: 91984550)	500.00	563.00	5,867.48
12 Feb 18 15:37:48	Internet traffic (usage: 685.01 MiB / 2m, 52s)	-685.01	63.00	5,867.48
12 Feb 18 15:34:38	Internet traffic (usage: 20.17 MiB / 5m, 57s)	-20.17	63.00	6,552.49
12 Feb 18 00:00:02	Auto refill	50.00	63.00	6,572.66
11 Feb 18 00:00:02	Auto refill	50.00	63.00	6,522.66
10 Feb 18 00:00:01	Auto refill	50.00	63.00	6,472.66
09 Feb 18 22:17:48	Internet traffic (usage: 103.58 MiB / 4h)	-103.58	63.00	6,422.66
09 Feb 18 14:40:08	Direct refill (voucher: 39377166)	33.00	63.00	6,526.24
09 Feb 18 14:39:30	Auto refill	50.00	30.00	6,526.24
09 Feb 18 14:31:39	Auto refill			
09 Feb 18 12:44:22	Internet traffic (usage: 145.81 MiB / 2h, 8m, 50s)	-145.00	30.00	6,426.00
09 Feb 18 00:00:02	Auto refill			

"Show details" will show details about the current session; ip / host (if available) / amount of data transfered. The link is not always available.



17.13.2 Active accounts - Guest users

Overview::::QuickCrew users, crew and guests, currently registered as active on this vessel.



Actions

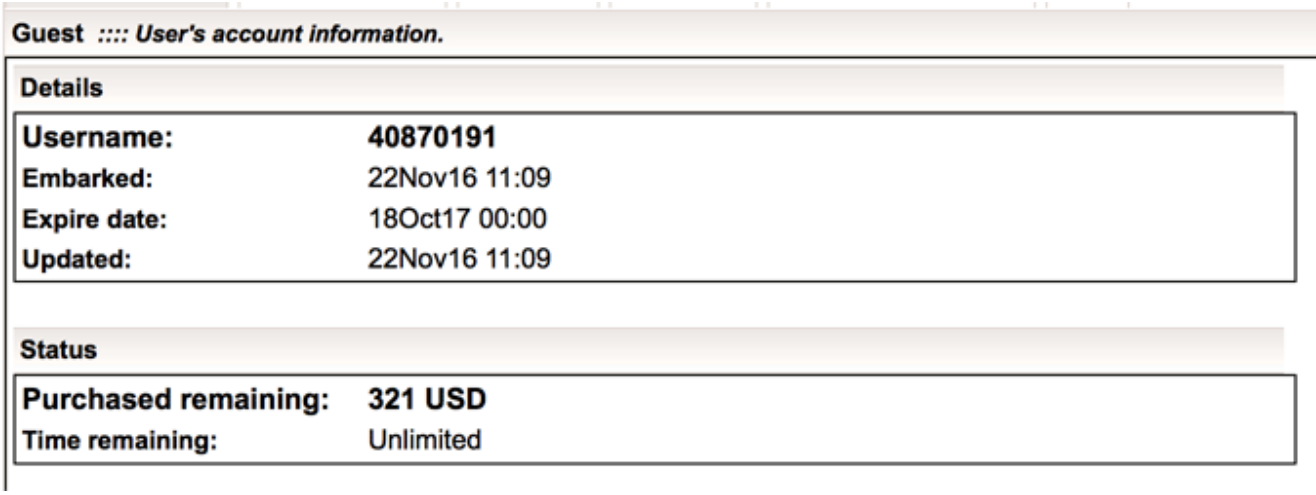
You can perform actions only on the accounts of guests on the vessel

Details

Displays account information, see below.

Details view

Account information



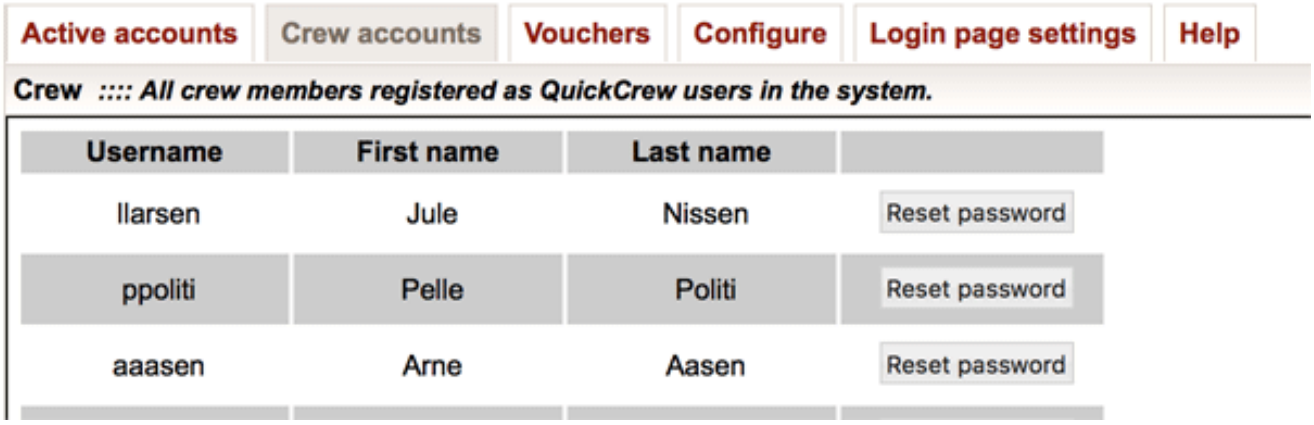
Transaction log

See *QuickCrew, crew user transaction log* for details.

17.14 QuickCrew - Crew accounts

Crew::::All crew members registered as QuickCrew users in the system.

The list contains all crew members of the fleet that have roaming access and can log on and become active crew users in vessels QuickCrew system.



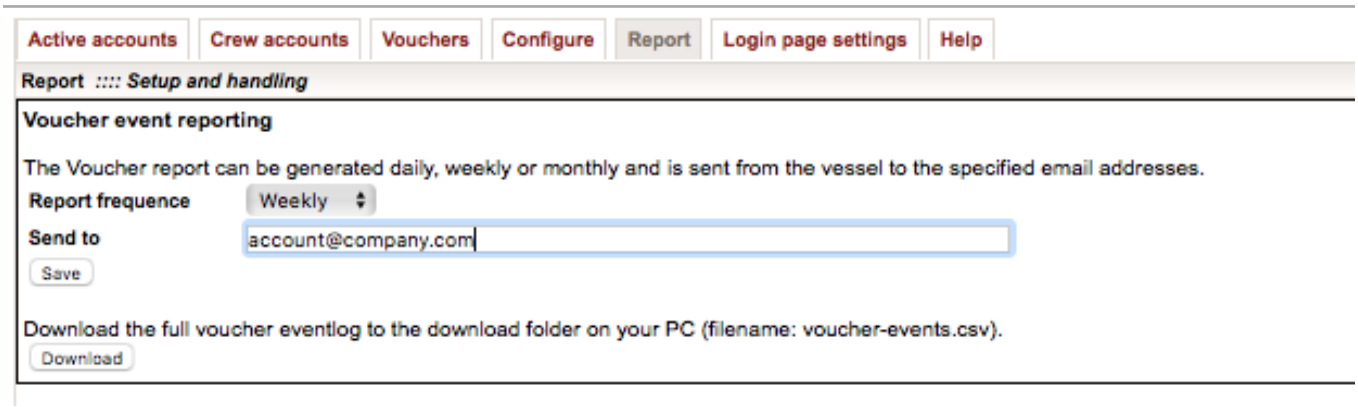
17.15 Voucher event reporting

All events related to vouchers are stored.

17.15.1 Configuration

It is possible to configure how often the report is sent to a recipient of choice. Available options are Daily (at midnight for previous day), Weekly (first day of week for previous week) and Monthly (first day of month for previous month).

From this page it is also possible to download directly the complete Voucher Event log as CSV formatted text ready to be imported into e.g. a spreadsheet for further analysis.



17.15.2 Email content

The following screenshots are form the report (HTML formatted) sent by email to the configured address (see screenshot above). The report contains "voucher events". For instance, under Voucher created, you will find all voucher that was created during the period. Since a several events can occur for a voucher in a period, a voucher may appear several times in the report.

These are the following events that are logged for a voucher:

- when the voucher is created

- when a voucher was credited, activated vouchers cannot be credited
- when administrator used a voucher to refill a crew users account directly
- when crew user used a printed voucher to refill his/her account
  or when a guest used the voucher to access the Internet for the first time
- when a voucher expired
- when a guest voucher was depleted

Voucher event log for vessel **osShip193**
Period: **01Jan70 01:00 - 15Feb18 13:56**
Generated: **15Feb18 13:56**

Voucher(s) created

Created	Voucher number	Voucher value	Voucher for	Created by	Expire
15Feb18 13:55	9400 2846	1.0	Crew	admin	15Feb19 00:00
15Feb18 13:55	7184 7955	3.0	Guest	admin	15Feb19 00:00
15Feb18 13:55	6192 9640	1.0	Guest	admin	15Feb19 00:00

Voucher(s) credited

Credited	Voucher number	Voucher value	Voucher for	Created by
15Feb18 13:55	6192 9640	1.0	Guest	admin

Voucher(s) direct refilled

Refilled	Voucher number	Voucher value	Activated by	Created by
15Feb18 13:56	8892 0670	12.0	DEMO	admin

Voucher(s) taken in use
- None in selected period

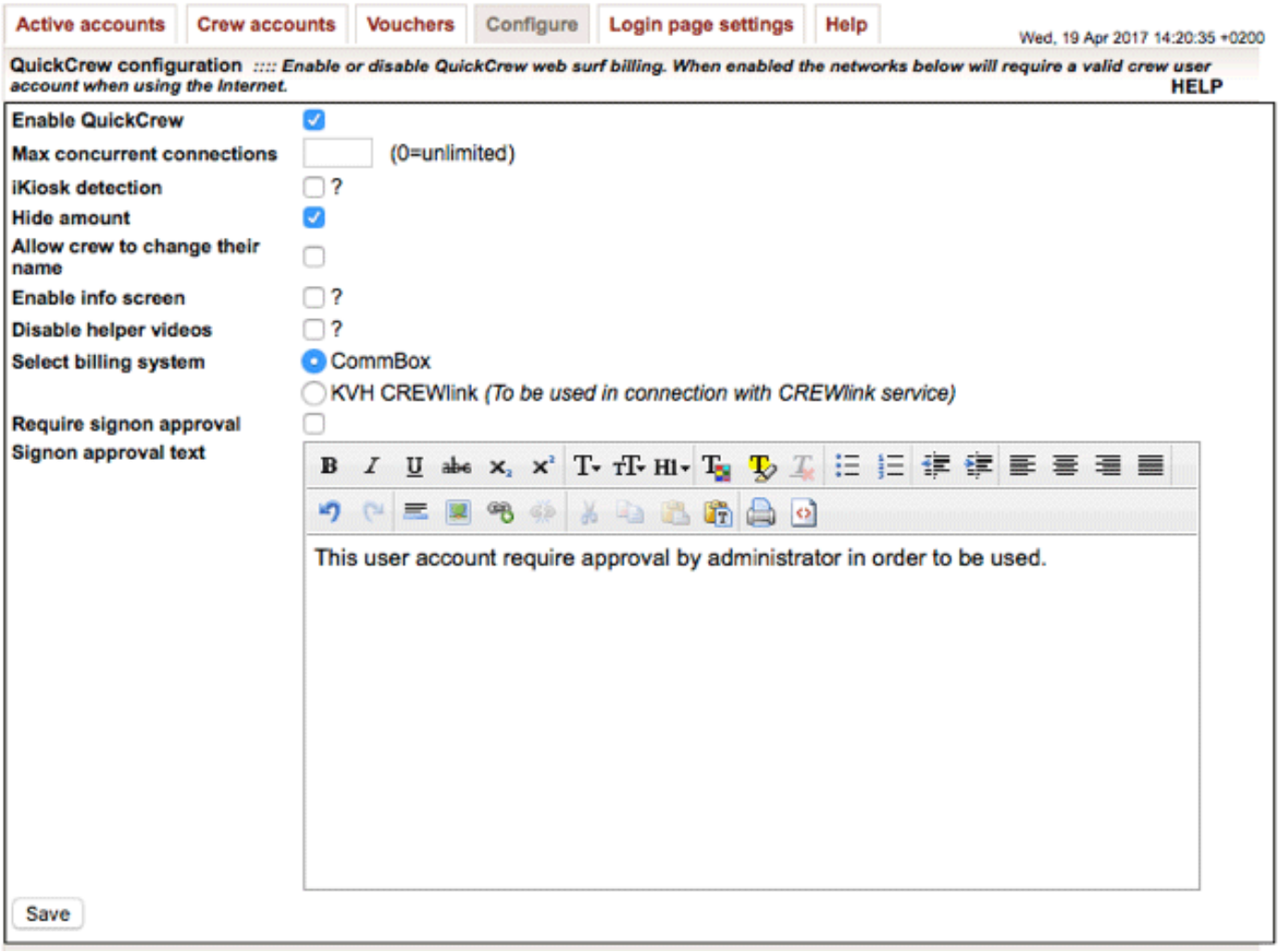
Voucher(s) expired
- None in selected period

Voucher(s) depleted guest
- None in selected period

17.16 Configuring QuickCrew access (vessel)

From "QuickCrew->Configuration" you can set some configuration parameters for the QuickCrew system.

17.16.1 QuickCrew configuration



Enable QuickCrew
: Tick this to enable the QuickCrew system.

Max concurrent connections
: Enter here the maximum number of users that will be allowed to have a web session at the same time.

iKiosk detection
: When enabling iKiosk detection, the CommBox will show ordinary QuickCrew pages for iKiosk enabled clients.
Note: Nokia phones and SymbianOS may not be recognized as mobile devices when iKiosk detection is enabled.

Hide amount
: Tick this to hide all references to credit from the crew users' "MyAccount" page. They will see their allowance in terms of remaining MB or remaining time depending on whether the connection is set up as 'Pay per byte' of 'Pay by time'.
Note that the amount shown as remaining MB/time can vary depending on the cost profile linked to the currently active connection.

Allow crew to change their name
: By default, the crew users are not allowed to change the first and last name on their QuickCrew account. Tick this to allow it. The setting is only valid locally, and must be ticked off on both vessel and hub for full effect.

Enable info screen
: Will redirect QuickCrew users to an information page after login.
See Appendix: Customizable web page for QuickCrew users

Disable helper videos
: When a KVH Media Server is available on the local network, it will serve helper videos on how to use QuickCrew and other KVH services. This content is available through links listed on the QuickCrew / CREWlink login page.
If you do not want Crew to see this helper videos, click on the "Disable helper videos" checkbox to hide these links.

Select billing system
: There are two ways of handling credits for QuickCrew users: in one everything is managed by the interaction of the hub and vessel CommBoxes. In the other, credits are managed by the KVH CREWlink system.
CommBox
: Only accounts fully managed by the vessel and hub CommBoxes are allowed.

KVH CREWlink

KVH CREWlink accounts are allowed **in addition** to the CommBox-managed accounts.

Require signon approval / Signon approval text

Tick this to present the crew user with the message defined as "Signon approval text". The message will be presented to the user on the login page and the user will not be able to use Connect to Internet before the administrator has Approved the QuickCrew user account.

[Save]

Remember saving your changes when done.

17.16.2 Deny crew net access to local users

You can choose to disable log-in access to the CommBox for local users (those defined in "Config->User/Group") when they are connecting from the billing network.

17.16.3 Billing networks

You can define ranges of IP addresses that are required to log in before being allowed to generate traffic.

Note that here you define ranges (e.g. all addresses from '172.18.1.0' to '172.18.1.255') and not address/mask ('172.18.1.0/24').

17.17 KVH CREWlink account holders (vessel)

KVH CREWlink can be used even without a main hub defined.

Credit handling for KVH CREWlink users is managed externally. The usual CommBox 'Refill account' functionality will not be available for this users

Please note that KVH CREWlink users will not have access to any web mail client.

17.18 Crew login page settings (vessel)

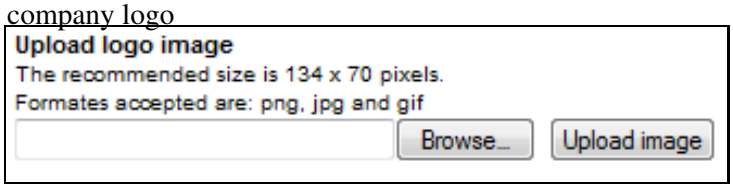
This customization of login page is only valid for systems (vessels) using Classic view. The Classic view was replaced by KVH Blue in version 1.13 of the CommBox software.

Some of the elements in the "QuickCrew login page" are customizable. It is possible to change the color of the header, the "welcome text" and the company logo. These changes are done from the "QuickCrew->Login page settings" page.
The lower part of the page shows a preview of the login form as it appears to crew members. From this you can perform the desired changes and have immediate feedback of what the users will see.

Page colors

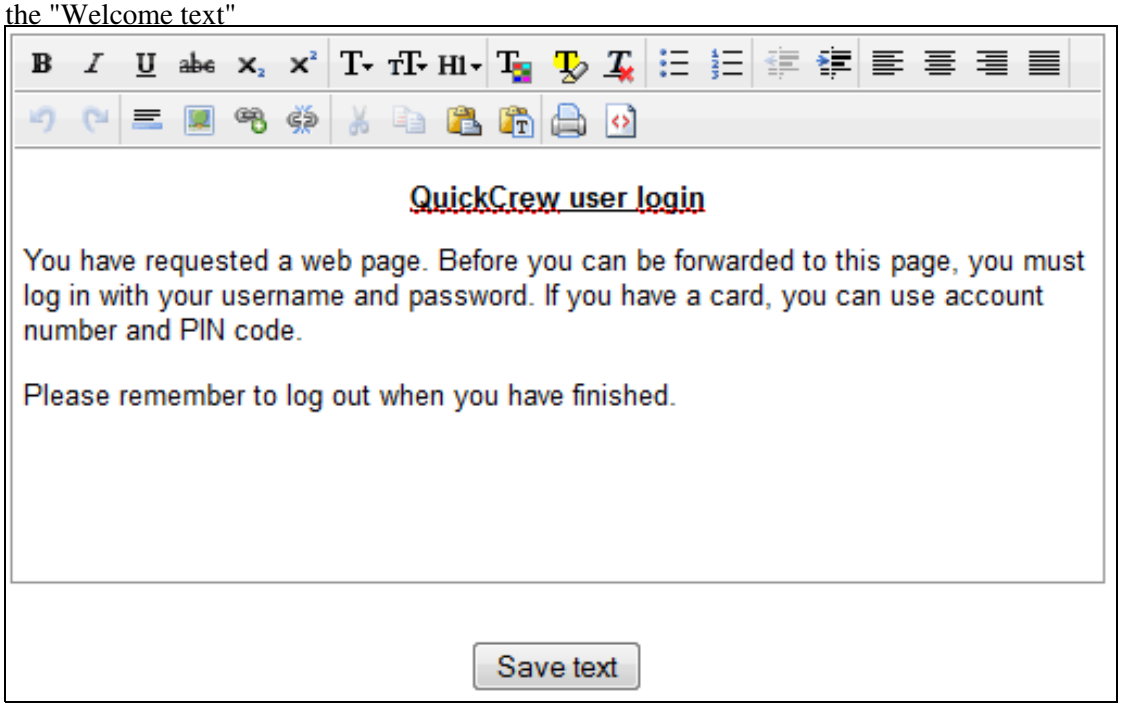
It is possible to change the color of the two stripes of the page header, and the color of the text in the lower stripe. To change colors, click on the color selector next to the element and use the mouse to select the new color (click *and drag* on the colored square). When you are finished, just click outside of the color selector to close it.

Custom company logo



To replace the standard KVH logo with one of your choosing, use the upload form under "Upload logo image" at the top of the page. Select the image you want to upload and use and click "Upload". If you use an image larger than 134 pixels wide and 70 pixels high, the system will resize the image.

Change the "Welcome text"



The "welcome" message can be edited in place from the preview. When you are finished, click [Save text].

Remember that, to make the change effective, you also need to click [Commit changes] (see later).

17.18.1 Commit and revert changes

When changes are done to any of the editable elements in the page, two buttons [Commit changes] and [Revert changes] will appear. To activate the changes and make them visible on the QuickCrew login page, click [Commit changes]. If you want to remove all the changes you have done to the page, click [Revert changes].

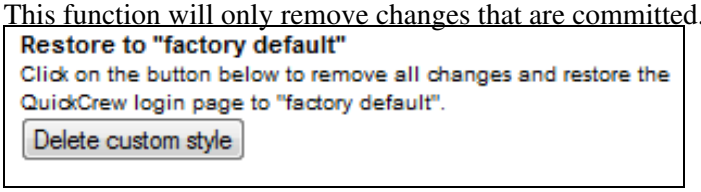
To see the changes in the crew login page, open another browser, or log out from the one you are working on.
Try the following URL:

"http://<ip to CommBox>/commbox.php?req_uri" (where '<ip to CommBox>' is the IP address of the CommBox) this will take you to the login page used for crew logins.

17.18.2 Delete custom style

[Remove custom style] is found next to the [Commit] / [Revert], and will remove the active customized style and reset the layout to factory default.

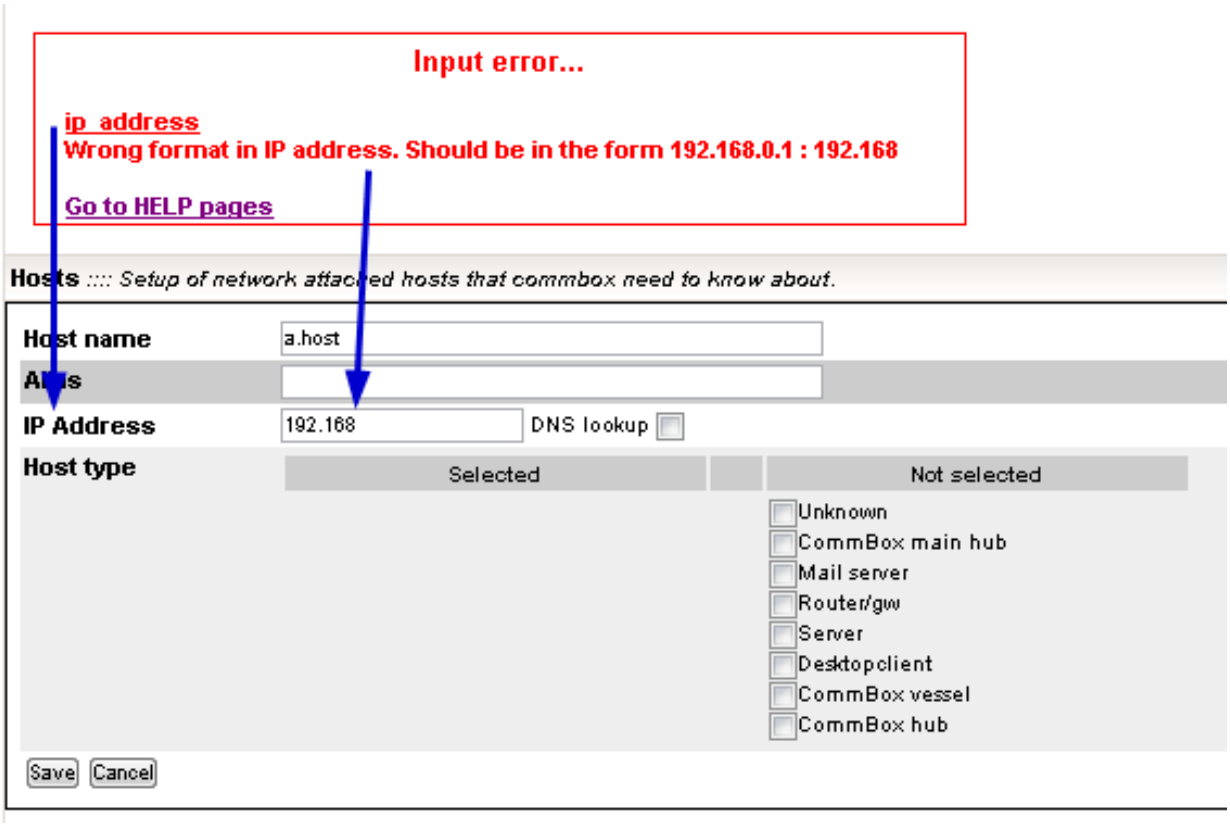
This function will only remove changes that are committed. To delete uncommitted changes, use [Revert] instead.



18 Error handling in the user interface

When you save some new or changed values for a configuration, these are checked for validity. If one of the values entered is of the wrong type, the CommBox will display an error message in the top area of the page. The message will contain the field name and an error message describing what is wrong.

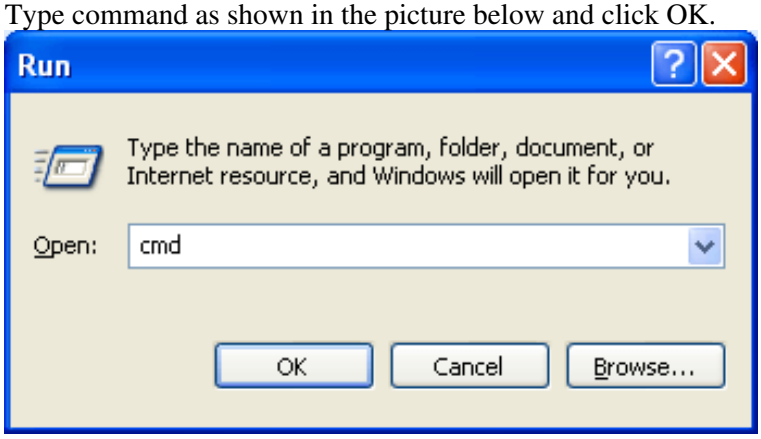
In the following example we see that we have added an IP address with a wrong format.



19 Troubleshooting

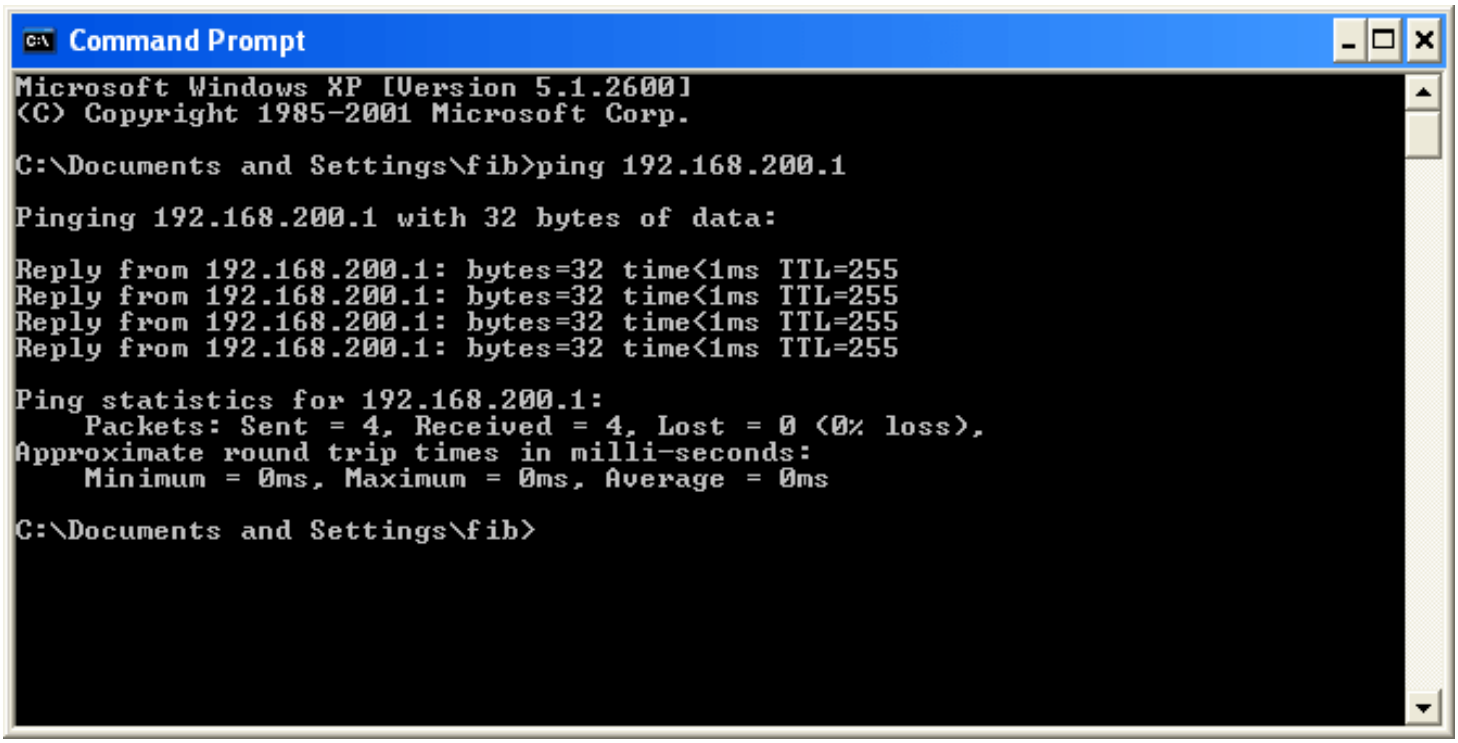
19.1 Check network connection

1. Open a command window; click Run… on the Start menu.
2. Type command as shown in the picture below and click OK.

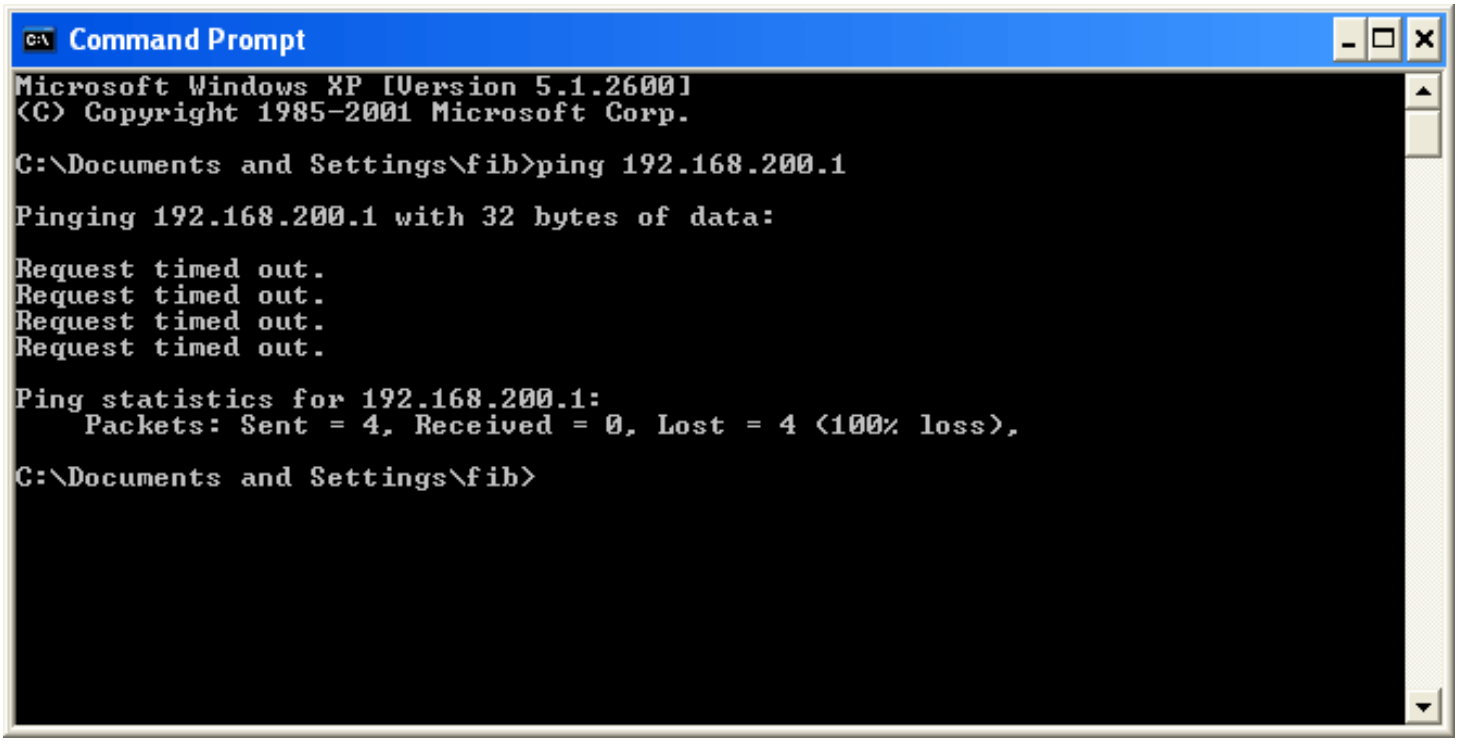


3. In the “Command Prompt” window type:
   ping <ipaddress>, where <ipaddress> is the IP address of the CommBox.

19.1.1 Connection successful:



19.1.1.1 Connection unsuccessful:



19.1.1.2 If the connection is unsuccessful:

- Try to ping an IP address that you know works. If that works, the problem is on the CommBox or on the network connection between the CommBox and your computer.
- Check the connection of the network cable to the CommBox, the light next to it should be lit.
- Check cables from the CommBox to the hub.

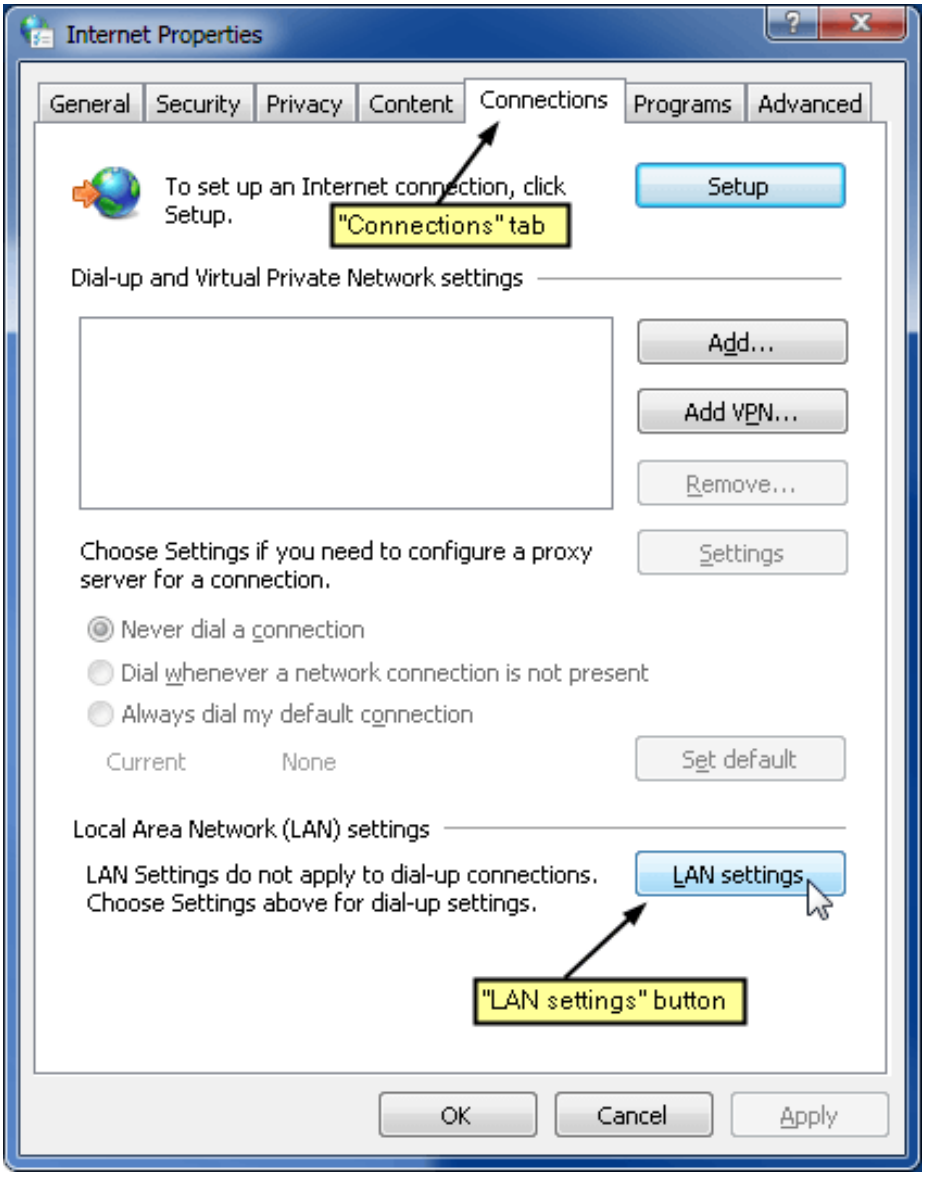
19.2 If you can’t connect to CommBox

If you cannot connect to the CommBox through your Web browser there may be several reasons.

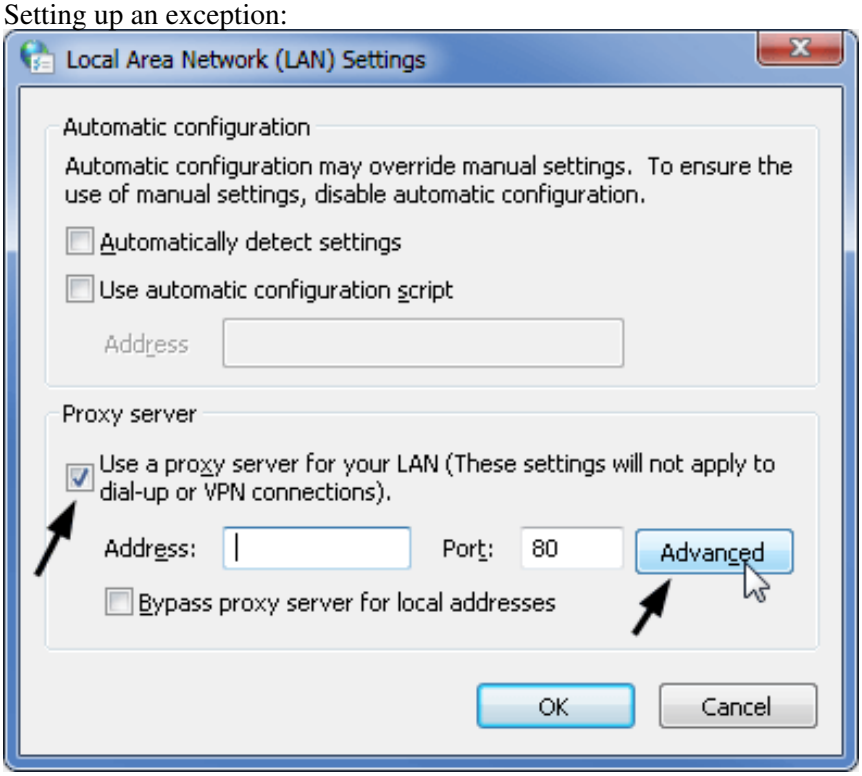
19.2.1 ERROR: The requested URL could not be retrieved

Solutions:

- Have you typed the address correctly? In the address field type the following http://<ipaddress>, where <ipaddress> is the IP address of the CommBox.
- Check if the network is working (See section above “Check network connection”).
- Check the proxy setting for the web browser:
    1. From Internet Explorer, open the menu item: Tools->Internet Options ("Internet Options" is also available from the control panel).
    2. In the “Internet Options” dialog box, click the Connections tab.
    3. From the Connections tab click [LAN Settings].

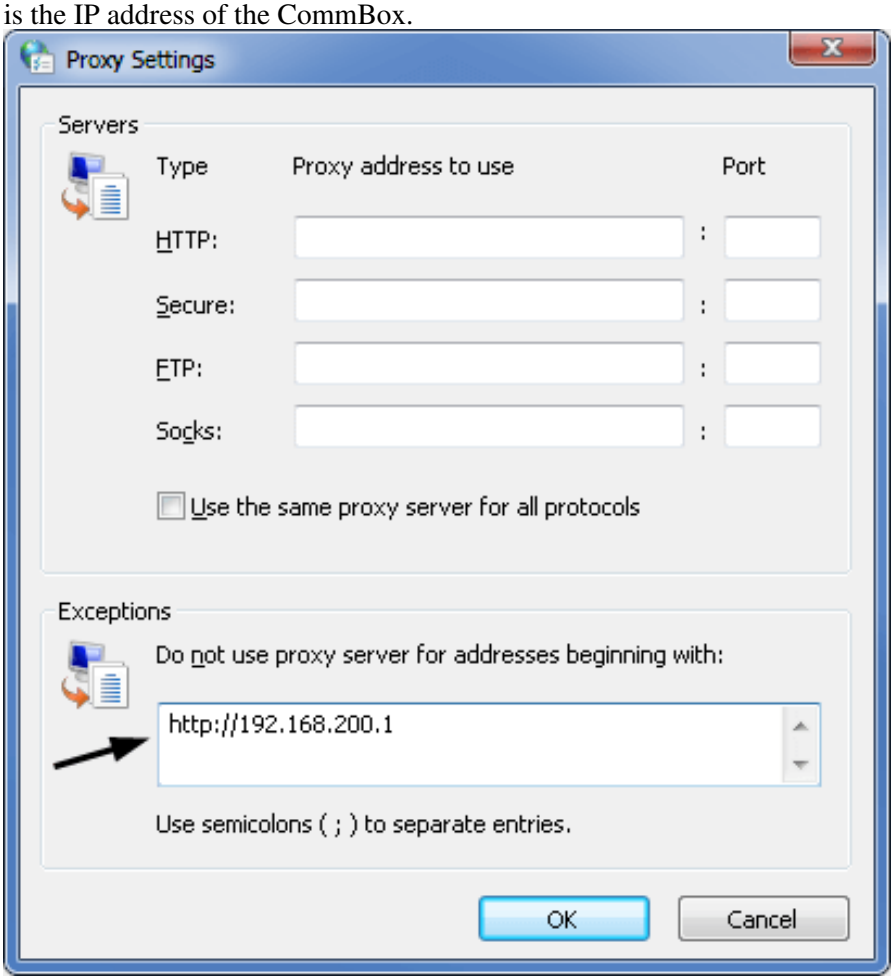


4. If “Use a proxy server” is checked (below), you should set up an exception for CommBox.
   Setting up an exception:



5. Click [Advanced].

6. In the new dialog box, add the following to the Exceptions text box. http://<ipaddress>, where <ipaddress> is the IP address of the CommBox.



7. Close the dialog boxes by clicking [OK] and try to connect to CommBox again.

19.3 CommBox can’t connect

Solutions:

- Check that the modem and terminals are connected properly and are switched on.
- If you use a fixed link solution (NORSAT or VSAT) try to reboot the multiplexer.
- Some ports or software may hang on CommBox, reboot CommBox from the "System->Reboot / Shutdown"
- For mobile phones, check that the SIM card is inserted and that the PIN code has been disabled.
- For satellite terminals, disable the PIN code for data communication.
- See also Carriers status, particularly the description for Red and Yellow.

19.4 CommBox establishes the link, and it often disconnects

This is a common problem often caused by bad signal-to-noise ratio. This may be caused by:

- Mobile phones far away from a transmitter, or with obstructions between the antenna and the transmitter.
- The vessel turns and the antenna is temporarily obstructed by for example a mast.
- Swell and vessel movements that make it difficult for the antenna to be correctly positioned.

These problems are not easily fixed.

Other causes:

- If the timeout on the satellite terminal for data is set to a too low value, the connection will close before CommBox has finished the transfer.

20 Support

If you need support, kindly first read the troubleshooting section above to try to solve the problem. If that doesn’t give any solution to the problem please contact KVH or others familiar with CommBox.

Please provide as much information as possible. Check the logs available from Dashboard, to see if they can provide any information about the problem.

Support contact:
Normal support hours 08:00 to 16:00 Norwegian time (CET): +47 33 03 05 34
Emergency support hours 16:00 to 08:00 Norwegian time (CET): +47 97 57 09 77
Support email: commboxsupport@kvh.com

Please have the following ready when calling!

- Vessel name and phone number
- Contact and phone number
- Situation (When, What, How, repeating problem?)

21 Definitions

HTML
: Hyper Text Markup Language, a formatting language used to create documents on the world wide web.

IP address
: Internet Protocol address, a unique number that identifies a computer within a network. The IP address has four numbers separated by dots. For example: 192.168.1.4

Mail queue
: All mails are grouped in a queue on the CommBox before they are sent. They are then sent all together to save connection costs.

MPDS
: Mobile Packet Data Service, when using this service the payment is for the data amount transferred and not the time used.

Signal noise ratio
: A number that says how much stronger the signal are in relation to the noise. Says much about the expected quality of the transmission.

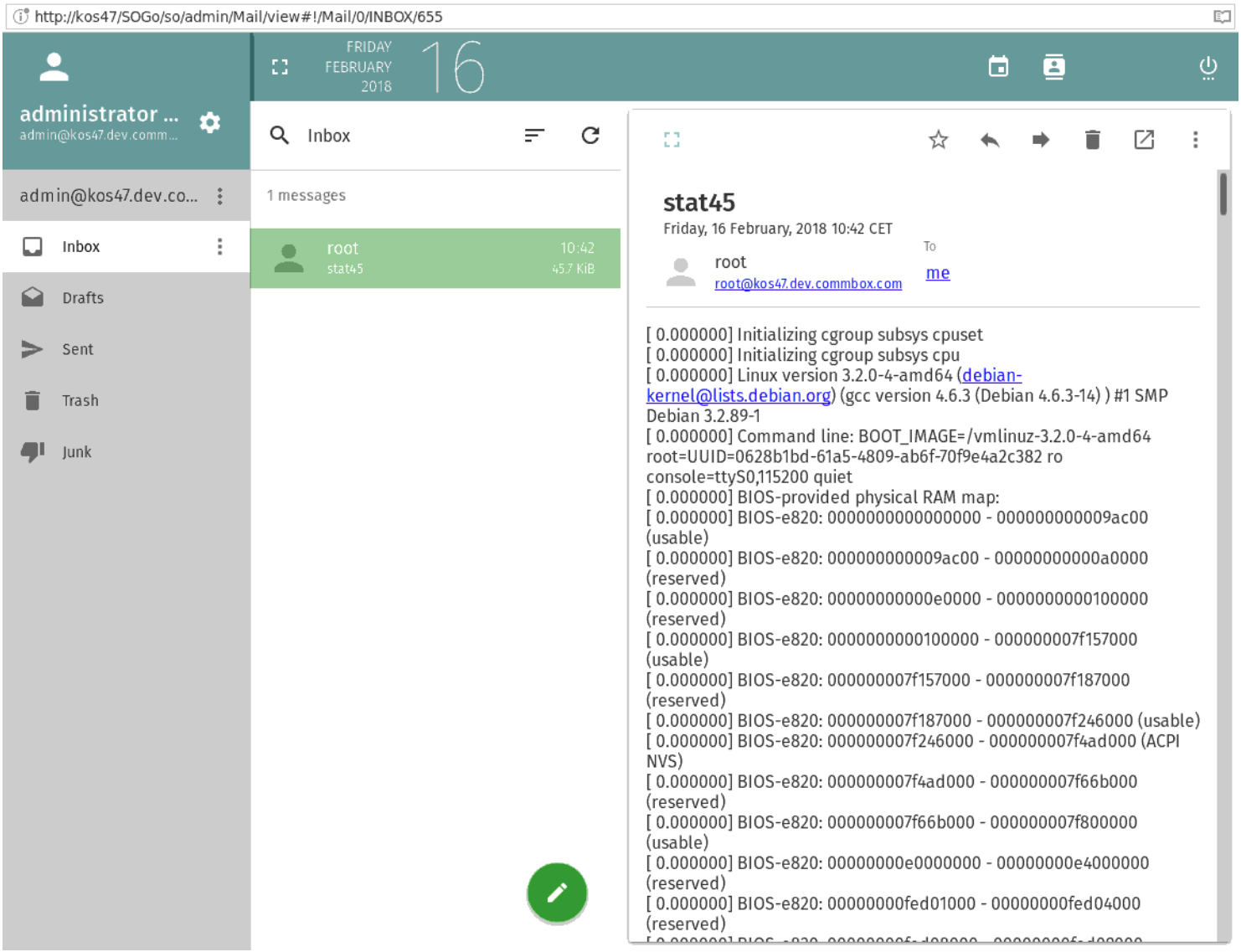
Software configuration
: CommBox stores all data specific for a customer in predefined files. All these files make up the software configuration.

TCP/IP
: Transmission Control Protocol/Internet Protocol, a protocol used to transfer data on a computer network.

VSAT
: Very small aperture terminal, in the maritime business VSAT are systems having a permanent IP connection from vessel to shore via satellites.

Web browser
: Web browsers (such as Microsoft Internet Explorer, Safari, Google Chrome, Opera or Firefox) are computer programs used to view web pages formatted with HTML.

22 Appendix: SOGo



SOGo is the most recent webmail client used on the CommBox. It contains features commonly expected in a modern webmail client. For more information see the SOGo web pages

23 Appendix: Zarafa

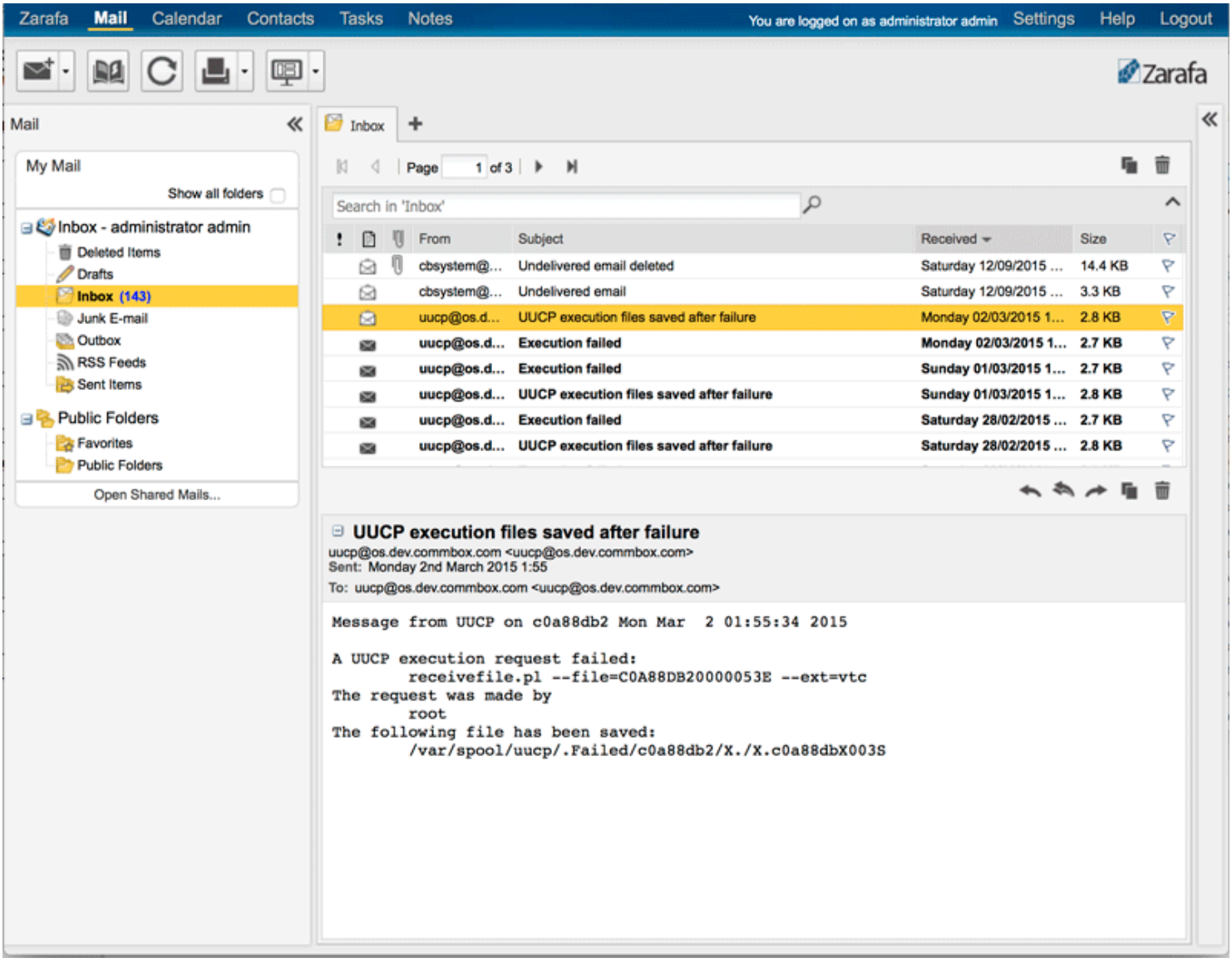
Older CommBoxes that have been upgraded may still use the old SquirrelMail email client. For information about it, please see Appendix: SquirrelMail.

CommBox embeds the 'WebApp' email client from Zarafa (see Zarafa (external link)). This is a feature-rich application and only the main points will be described here.

For more detailed information about the use of Zarafa WebApp, please refer to its user manual.

To access Zarafa WebApp, click on "Webmail" in the left menu, the webmail client will open in a new window.

23.1 The Zarafa WebApp main panel:



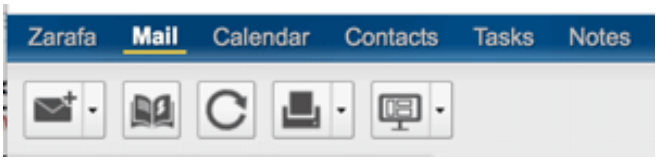
23.1.1 How to read mail

You can read incoming messages by clicking on 'Inbox' in the left menu.

It is possible to create new folders by right-clicking on the left menu. You will then be able to move messages by dragging them to the appropriate folder.

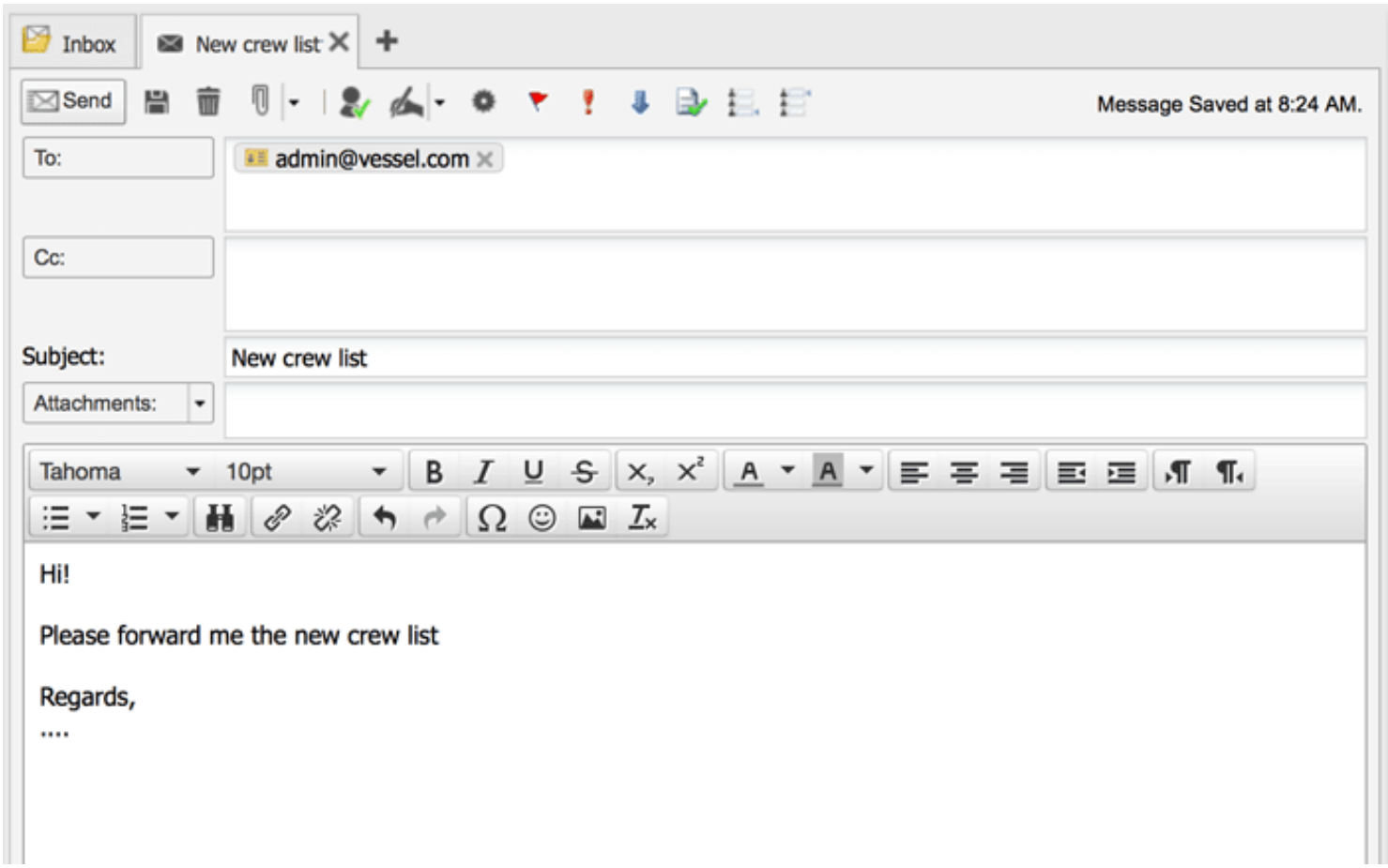
23.1.2 How to create and send email

23.1.2.1 The Zarafa WebApp tools:



Click on the down arrow next to the "Envelope" icon on the tool bar and select "Email message", if you are viewing one of the mail folders you can click directly on the "Envelope" icon. A new e-mail tab will appear, from this you will be able to compose your message and select the recipients.

23.1.2.2 Compose mail in Zarafa WebApp:



If you click on the "To...", "CC...", or "BCC..." buttons you will be able to choose an address from your address book. This includes all users on the ship, all of your contacts, the contacts in the global contact list.

The top menu gives you access to functionality for saving the message, add attachments and more. Hover the mouse pointer on each icon to see a short description of the different functions.

Once you are finished with composing your message click [Send] on the top-left.

23.1.3 Contact lists

You can create your own list of contacts by clicking on [Contacts] on the left menu and then [New] on the top-left.
This list will be automatically transferred to the next boat on which you log in.

From the "Public Folders" > "Global Contacts" in the left menu you have access to a global contact list which is maintained on-shore and distributed to all vessels in a fleet.

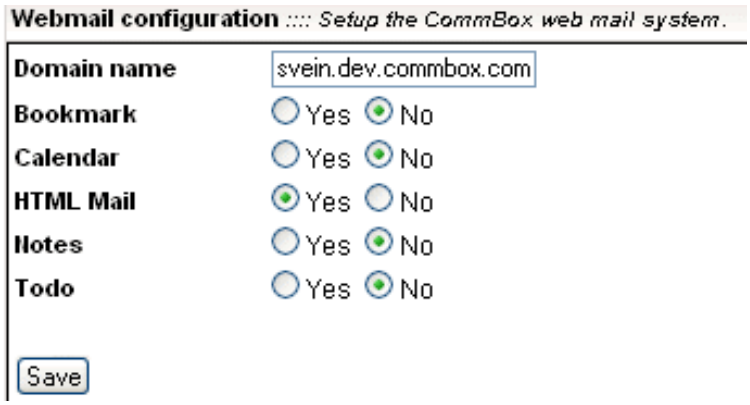
You cannot add, remove, or edit information in this list.

24 Appendix: SquirrelMail

Some CommBoxes that have been upgraded from older versions will have a simpler webmail application called SquirrelMail. Its configuration and use are described in this appendix.

24.1 QuickMail > Webmail

Web mail configuration lets you define parameters that affect the functionality of the embedded email client.



The QuickMail page has an extra "Webmail" tab which allows setting some configuration parameters.

Parameter description

Domain name

Add the domain name for the CommBox.

Bookmarks

Enable bookmarks. This lets users save their bookmarks in their Web mail user area. This is a nice feature if multiple users share the same PC.

Calendar

Enable calendar. This module give users a calendar where they can add tasks.

HTML Mail

Enable HTML mail. Lets users use a Word-like editor to write formatted HTML mail.

Notes

Enable notes. This module allows users to add personal reminder notes.

Todo

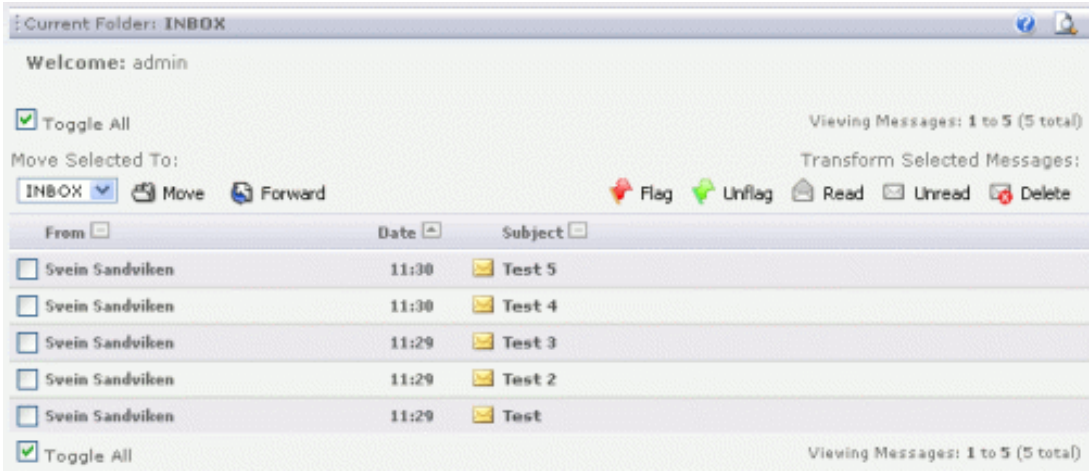
Enable todo. This module allows users to create to-do list.

24.2 Web mail client

CommBox has an integrated web mail client. Each CommBox user can use it to access their email account to send and receive email. To access web mail, click on “Webmail” in the left menu, the webmail client will open in a new window.

Please note that KVH CREWlink users will not have access to any web mail client.

For more detailed information about the Webmail client, click on the question mark icon that appears on the top-right.



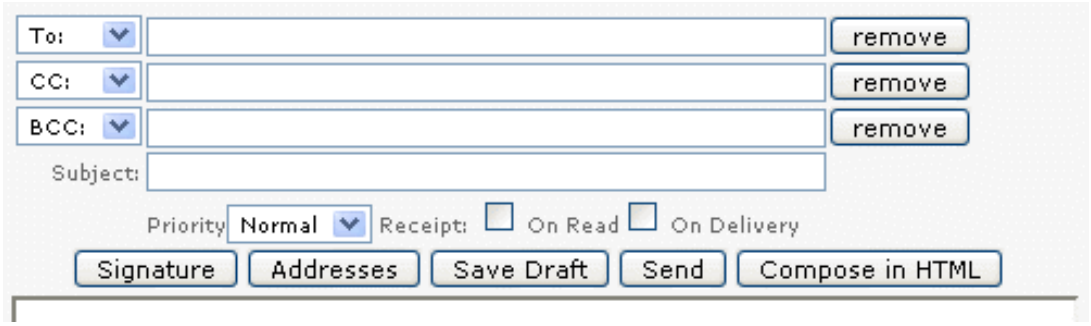
24.2.1 How to read email

The web mail client opens in the Inbox view where you get a list of all mails that are stored in your CommBox email system. To read a message, click on its subject.
You can organize your messages by creating folders (click on the 'folders' option on the top menu) and moving messages into these.

24.2.2 How to create and send email

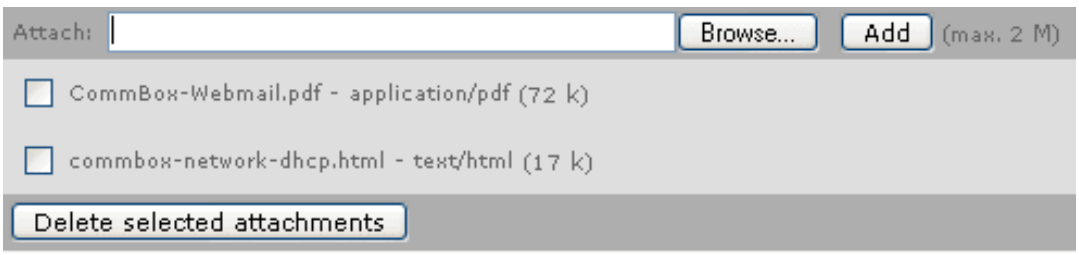
Open the web mail client and click [Compose]. You can choose to use HTML formatting for your email by clicking [Compose in HTML]. This option will add a set of icons to your composer window. From here you can choose to add tables, text colors, font size and more.

This functionality is only available if the CommBox administrator has enabled it in "QuickMail->Webmail" and if Javascript is enabled (see below).
Another function you get with Javascript is “Auto complete” of addresses as you type in the name in the address field.



24.2.3 Add attachment to your email

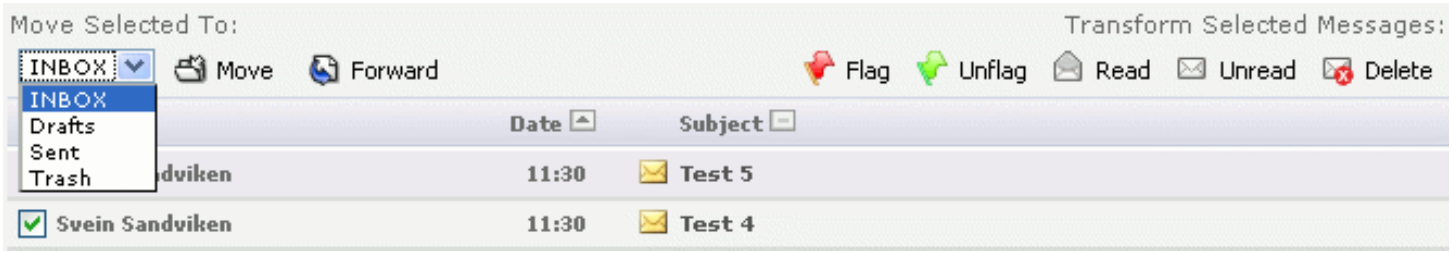
If you want to add attachments to the email you are composing, click [Browse] below the mail body area.



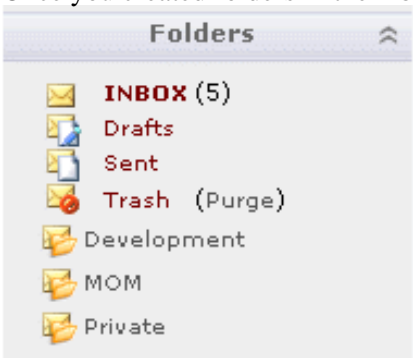
Browse to find the file on your local computer, then click [Add] to upload the file to the server, and attach it to the mail.

24.2.4 Delete, move, forward and more

You can delete, move, forward or change status for one or more emails by first ticking off the checkbox next to them. Next you choose the action you want to perform from the menu above the email list.



Move
: Once you created folders in the inbox structure, you can move the selected message in it.



Forward
: Forward selected message

Flag / Unflag
: Mark / unmark messages in red (important)

Read / Unread
: Mark messages as read / unread

24.2.5 Enable Javascript

To enable HTML composer and Auto complete you must set Javascript settings to
“Use Javascript: Always”

To do so, go to "Options->Display Preferences" in the mail client view.

25 Appendix: Fields in the import/backup/restore roaming (crew) users files

From the hub's crew management page it is possible to import, backup and restore crew users to / from a csv file (see Import or export users).

The format of the file accepted by the Commbox is:

- Semicolon (;) separated values.
- Values optionally quoted with double quotes (").
- Values containing a semicolon **must** be quoted.
- The first line contains the field names.

This is format can be used with most spreadsheet programs (Microsoft Excel, OpenOffice Calc, etc.).

The following list describes the fields in the file.

username
: The username used for login and for the email address.
It can contain only: latin letters without modifiers (accent, umlaut etc.), numbers, dot, underscore, dash. The first character must be a letter. Maximum length is 25 characters.
If missing, it will be generated automatically based on the firstname and lastname fields.
It is used to match the user to be updated and it must be unique.
It must be present when doing an update operation.

password
: The password used for login.
If absent, it will be auto-generated based on the rules defined in *QuickCrew->Configuration "Crew user password generation"*.

firstname
: The first name (given name), it must be present when doing an insert and the username is not supplied.

lastname
: The last name (family name), it must be present when doing an insert and the username is not supplied.

* vessel
: The IP address of the vessel on which the user is boarded. This field is only useful when using the import function to restore data after in a disaster-recovery scenario. Changing it does **not** transfer the user account on a new vessel.

email
: The email for the crew user.
If present, it must be based on the username and an existing roaming domain i.e. "<username>@<roaming domain>". The value of the roaming_domain filed will be ignored if the email is defined.
If absent, it will be auto-generated based on the username and the roaming domain.

roaming_domain
: The domain used to compose the email address (FQDN), if set it must match one of the domains specified under *QuickCrew->Configuration "Roaming mail domains"*.
The value of this field is ignored if the email is present.

phone
: The telephone number.

address
: The street address.

* embark
: Time when the user embarked (UNIX time)

active
: Mail forwarding to vessel: 1 = mail is forwarded, 0 = mail is **not** forwarded.

credit
: Credit (if the user has an KVH CREWlink account this is the KVH CREWlink credit).

freefield1

CommBox credit (in case the user has an KVH CREWlink account).

* mail_usage_amt
  Credits used for mail transfers.
* mail_usage_byte
  Bytes of mail transfer.
* mail_sent
  Number of mails sent.
* mail_recv
  Number of mails received.
* web_usage_amt
  Credits used for Web access.
* web_usage_byte
  Bytes transferred for Web access.

account_type
: Account type ID (as shown in *QuickCrew->Configuration*).

* last_refill
  Last refill time.

status
: One of 'changed' or 'deleted'. To 'revive' a deleted user, set its status to 'changed'.

idt_accountno
: The account number used for the KVH CREWlink system.

idt_pin
: The personal PIN used for the KVH CREWlink system.

* created
  The date the user was created.
  Ignored when importing.
* updated
  The date the user was updated.
  Ignored when importing.

25.1 Notes and suggestions

1. (*) The vessel, mail_usage_amt, mail_usage_byte, mail_sent, mail_recv, web_usage_amt, web_usage_byte, last_refill, created, updated, and embark fields are for information only. It does not make sense to update them unless you are restoring an accidentally deleted database.
2. The username must be unique in the file. When importing a large number of new users, it may be problematic to make sure that their usernames are unique. Unless you have a strict requirement to choose usernames it is suggested that you omit the username column: the CommBox will automatically generate unique usernames based on the first and last names, adding digits if the combination is already in use. For example a user called "Fred Olsen" will receive a username of "folsen", if another user is called "Frank Olsen", he will receive a username "folsen1".
3. The email must consist of the username and the roaming_domain. If not defined, it will be automatically generated using the default roaming domain. To simplify operations, you can avoid to include the email field in the import. If you need to assign a roaming domain, you can specify it in its own field.

26 Appendix: Fields in the contact list file

From the hub "QuickMail->Contact list" page it is possible to export or import a list of email contacts to distribute to the fleet (see Contact list (hub)).

- Semicolon (;) separated values.
- Values optionally quoted with double quotes (").
- Values containing a semicolon **must** be quoted.
- The first line contains the field names.
- Each contact must have a numeric 'id' field.

This is the default format used by OpenOffice Calc.
The order of the fields is not important, the first row in the file must contain the corresponding field name for each column. Note also that your file may contain only the columns related to the fields you use, for example a very simple file may look like this:

```
id;firstname;email1
1;John;john@commbox.com
2;Peter;peter@commbox.com
```

When distributing updates to the fleet, the CommBox will send only the fields that have changed since the last distribution. This causes a considerable reduction in the amount of data transferred. To take advantage of this feature you will need to take care of the "id" that is attached to each user: this allows the CommBox to recognise users across updates and determine which fields have changed.

The file is assumed to be always complete i.e. contacts that are not in the file will be deleted.

The following is a list of all the available fields, the names should be self-explanatory.
Installations using the old SquirrelMail webmail will use only those marked with '#'.

#	id
	birthday
	business_address
	business_address_city
	business_address_country
	business_address_postal_code
	business_address_state
	business_address_street
	business_title
	business_web_page
	company_name
	department
	display_name
#	email1

	email2
	fax
#	firstname
	home_address
	home_address_city
	home_address_country
	home_address_postal_code
	home_address_state
	home_address_street
	home_phone
	home_web_page
#	lastname
	mobile_phone
#	nickname
	pager
	work_phone

27 Appendix: Interface drivers

Many satellite terminals and GSM phones use similar equipment. The most common terminal types are listed in the "Interface drivers" dropdown. In many cases a driver can be used for different terminals. The table below lists which driver to use for equipment not listed in the dropdown.

Equipment	Driver
Thrane and Thrane Sat B Sailor Sat B Skanti Scansat Sat B	Sailor SP4400 ASD
Furuno Felcom 70 - Ramsat JRC JUE 410F - Ramsat Nera F55 - Ramsat Nera F77 - Ramsat Sailor Fleet55 - Ramsat Sailor Fleet77 - Ramsat	Fleet ISDN - Ramsat
Furuno Felcom 70 - Eicon JRC JUE 410F - Eicon Nera F55 - Eicon Nera F77 - Eicon Sailor Fleet55 - Eicon Sailor Fleet77 - Eicon	Fleet ISDN - Eicon

28 Appendix: Format of telephone numbers

Dialing from vessel with GSM phone, use the format:

```
<+> + <country code> + <office phone number>
```

Dialing from vessel with satellite terminal, use the format:

```
<00> + <country code> + <office phone number>
```

Some satellite terminals require a prefix and/or postfix for the phone number:

Satellite terminal	Formatted phone number
Furuno Felcom 70 ISDN	<902> + <phone number>
Furuno Felcom 82 ASD	<3 digit LES code> + <phone number> + <#>
Nera Saturn B ASD	<phone number> + <#>
Nera Worldphone	<phone number> + <#>
Nera Fleet ISDN	<902> + <phone number>
JRC JUE 310B	<3 digit LES code> + <#> + <phone number> + <#>
Sailor mini-M TT-3064A	<phone number> + <#>

29 Appendix: LED, LCD and Buttons

The hardware version is detected by looking at the hardware (cpu) installed:

- Celeron©-> QuickBlue
- Atom© -> C2
- Pentium® -> R8

If none of the above hardware is detected the function(s) described below will be disabled.

The "reset to factory default" is temporary not available! (CommBox sw version 1.8.0)

29.1 QuickBlue (and other unknown hardware versions)

No programmable LED; LCD or buttons, the daemon will exit at startup.

29.2 C2

2 LED (RUN, CONNECT) and 1 RESTORE button

At startup the RUN (green) LED will flash.
When CommBox software is up running the LED will be green, no flash.
At shutdown the RUN (green) LED will flash.

The RESTORE button is used to do reset to factory default:

Push the button for minimum 30 secs, the RUN (green) LED will flash rapidly for about 30 secs
After 30 secs the CONNECT (blue) LED will flash ones.
If the RESTORE button is released within the next 30 seconds, the "reset to factory default" will be activated
The reset process takes about 60 secs

When up running the LED will show -

- if CONNECT (blue) LED will be steady blue as long as the CommBox is connected or transferring data
- else it's off

29.3 R8

1 LED (STATUS) and 1 RESET button (left side)
1 LCD (2 lines, 16 characters) and 1 KEYPAD with 4 buttons

At startup the STATUS LED will flash green.
When CommBox software is up running the LED will be green, no flash.
At shutdown the STATUS LED will flash green.

The RESET button is used to do reset to factory default:

Push the button for minimum 30 secs, the STATUS LED will flash red
LCD shows "CommBox RESET!", "Reset in: x s" where x will count down
If the RESET button is released within the next 30 seconds, the "reset to factory default" will be activated
The LCD will than show "Factory Default!", "HW: QuickRack 20"
The reset process takes about 60 secs
The LCD will, at startup, show "CommBox", "Starting: x" where x is secs after restart.

When up running the LCD will show -

- if connected:

"Online: xxxx", where xxx is connection, will show in line one
"Uptime hh:mm:ss", hh:mm:ss is running time for the connection in line two

- if offline:
"CommBox by KVH Industries, Inc." will scroll in line one
"nnnnnnnn", where nnn is the software version will scroll in line two

- if connected and the button marked "ENTER" is pushed:
"CommBox by KVH Industries, Inc." will scroll in line one
"nnnnnnnn", where nnn is the software version will scroll in line two

The LCD will, at shutdown, show "CommBox", "Stopping: x" where x is secs into shutdown.

29.4 R6

In front

3 LEDs showing the following (from top)
Disk LED
Yellow when disk activity
Connection LED
Blue means connected
Power LED
Red when box has power, but not turned on
Green when power on
Each LAN port connector has 2 LEDs, the left one lights yellow when connected, the right one indicates traffic.

In back

Power button together with power connector that takes power from an external power supply.
Other button has no function.

30 Appendix: Customizable web page for QuickCrew users

30.1 User interaction and design

30.1.1 Administration

Admin user on HUB will have the possibility to upload (through Samba share or web form) a web page to the CommBox which will be displayed after the QuickCrew user have logged in.

30.1.2 User Scenarios *with* QuickCrew

Two user scenarios are valid; I) user request any www page, II) user request CommBox/QuickCrew login page. The only difference in the example below will be the jump page for scenario II.

1. Kermit the Frog opens his browser to surf the web (e.g. procycling.no)
2. When he requests a web page he is redirected to the QuickCrew/Prepaid login page
3. He enter his credentials and click Log in
4. Scenario I only: Popup window is opened
5. The new advertisement/information page is shown. Now Kermit may be:
    a. redirected automatically to the site he initially requested (e.g. procycling.no or MyAccount page, base on jump page parameter)
    b. presented with a link to go to the site he initially requested (base on jump page parameter)

30.1.3 User Scenarios *without* QuickCrew

This is a much more delicate issue in terms of how intrusive the showing of the advertisement page may be perceived by the user. Technically it may use the same pattern as for QuickCrew above (firewall redirect rule that is removed when user have viewed the page).

1. User request a web page
2. Firewall redirects request to crewredir program which responds with advertisement page, or show a page that ask the user to Connect (even though not necessary, but may be perceived as less intrusive)
3. Same as for bullet point 5 above

After the user have clicked Connect he will not have to do that again for defined number of days (when expired, the redirect rule is put back).

30.2 Implementation

30.2.1 Splash screen html page

The web page that is going to be used as a "splash" screen must either have a automatic JavaScript redirect or a link that takes the user to the "jump page". The "jump page" will be available in the URL that opened up the splash page as "**j**".

Ex: 192.168.141.180/c/index.html?j=cnn.com

If no jumppage parameter (j) is present in the URL the splash screen must send the user back to myAccount.
The web page must be wrapped in a archive file containing a index.html document and all underlying files (images, css, js).

30.2.2 Transfer to vessel

The splash screen archive file will be sent to the vessels from the hub or from CMS in a CPIO archive. To add the file to the file queue on the hub we will use a Samba share or a web upload form. On arrival on the vessel the archive will be unpacked to the folder "/var/www/custom"" (alias "c").

30.2.3 Enable "splash/info screen" on vessel

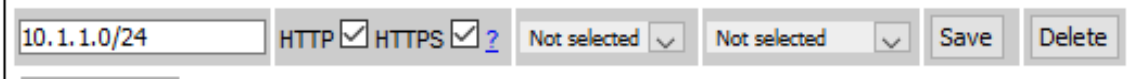
To enable use of "splash/info screen" on a vessel a switch, "Enable info screen", on the QuickCrew configuration page must be set to on. On "activate changes" this will trigger a reconfiguration of Apache2 that will add a new config file in "/etc/apache2/conf.d/customalias" and restart Apache2. This file will create the alias "c" that points to the "/var/www/custom" directory. Disabling of "splash screen" will remove the config file.

30.2.4 Redirect from MyAccount page

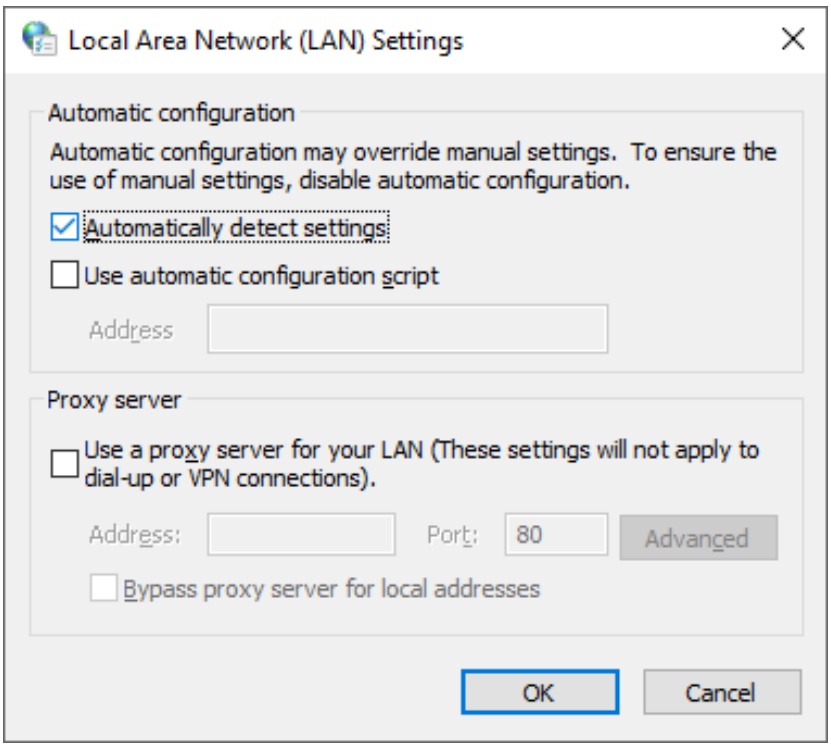
If "splash screen" is enabled in QuickCrew and "/var/www/" contains files, the user will be redirected to the "c" alias when the login sequence is finished.

31 Appendix: Web Proxy Auto-Discovery (WPAD)

When HTTPS is configured on a filter rule for QuickWeb (ref. image below), the client system must use the proxy directly (either setting it manually or use automatic detection), in order to visit HTTPS based web sites.



Using auto-config proxy setting sets the web client to automatically use the proxy and eliminates manual settings. When QuickWeb is enabled, a suitable wpad configuration is served by CommBox upon request. Clients supporting wpad will fetch it when they are configured to automatically detect settings (ref. screen shot below from Windows 10).

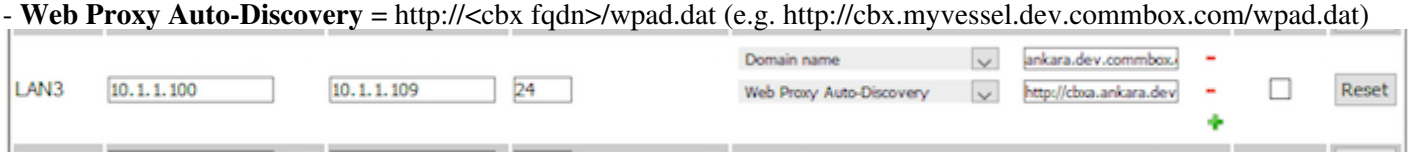


NOTE: *Some browsers also support automatically detecting the proxy settings on their own. Some mobile devices do not support the DNS variant of the WPAD Protocol and will require to get the reference as DHCP option.*

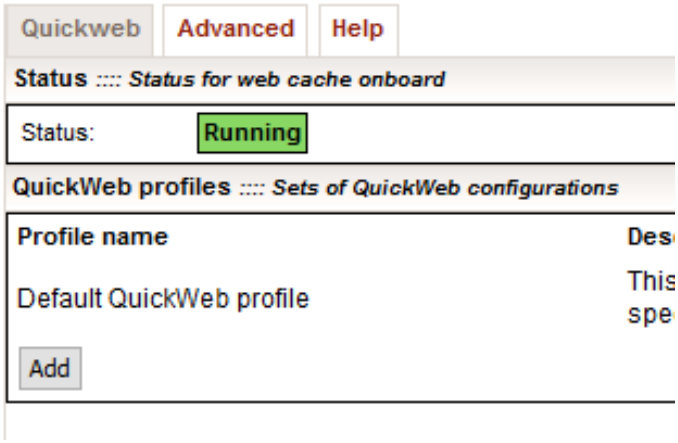
In order to make the file available for the clients, the following manual settings must be configured in CommBox:

1. Config >> Hosts:
   - define wpad CNAME for commbox hostname (e.g. cbx.vessel.net => wpad.vessel.net)

2. Config >> Network >> Configure DHCP server:
   Add (+) the following options for the subnet in question
   - **Domain name** = <cbx domain> (e.g. myvessel.dev.commbox.com)
   - **Web Proxy Auto-Discovery** = http://<cbx fqdn>/wpad.dat (e.g. http://cbx.myvessel.dev.commbox.com/wpad.dat)



3. QuickWeb:
   Enable QuickWeb and configure filter rule(s)


Quickweb
Advanced
Help
Status :::: Status for web cache onboard
Status:
Running
QuickWeb profiles :::: Sets of QuickWeb configurations
Profile name
Des
Default QuickWeb profile
This
spe
Add