MARLINK

XCHANGE

MARLINK

Administrator Handbook

Reference Version: 5.6

Table of Contents

1. INTRODUCTION

This handbook is a complete guide that explains the features and functions of the XChange system. This handbook describes how the XChange system works and how it can be set up to meet specific requirements.

This handbook is designed to be used by IT Administrators and trained Technicians.

1.1 What is XChange?

XChange is a sophisticated network management platform specifically designed for maritime environments. It seamlessly integrates vessel IT systems with corporate networks, optimizing bandwidth usage and ensuring secure data transmission.

XChange excels in network integration, allowing onboard IT infrastructure to connect seamlessly with shore-based corporate networks. This facilitates secure data exchange and remote management, making it a robust solution for maritime digitalization. The platform optimizes available bandwidth, ensuring efficient use of satellite connections and maintaining reliable network performance.

It delivers voice, Voice over Internet Protocol (VoIP), data and Internet access in one solution, independent of the communication technology used: Sealink VSAT, Marlink FX, Mobile Satellite Services (MSS) such as Inmarsat, Iridium, Low- and Medium Earth Orbit (LEO/MEO) service such as Starlink, Terrestrial Communication Services like Marlink´s Global 4G and others.

Security is a key focus of XChange, which incorporates advanced measures to protect against cyber threats and safeguard data integrity. It also offers remote monitoring and management tools, enabling proactive maintenance and troubleshooting of network devices and systems.

XChange supports a multi-user environment, providing granular control over access permissions and user roles. This ensures that each user has the appropriate level of access based on their role and responsibilities, enhancing overall network security and efficiency.

XChange significantly improves crew welfare by providing reliable internet connectivity. This connectivity allows crew members to stay in touch with family and friends, access entertainment, and manage personal affairs, thus maintaining morale and well-being during long voyages.

The platform also includes various operational modes, such as VPN management, network VLAN segregation, and secure data channels. Its centralized dashboard offers a user-friendly interface for managing network settings, viewing system status, and configuring devices.

In practical terms, XChange ensures secure and efficient data transfer between vessels and corporate networks, allows continuous monitoring of network performance, and provides robust security management to protect sensitive information. It also enhances the quality of life for crew members by providing stable internet access, supporting their mental and emotional well-being.

XChange is an essential tool for managing the complex IT and network demands of modern vessels, ensuring they remain connected, secure, and supportive of crew welfare.

1.2 Legal Notice

This documentation and the related XChange solutions are protected by copyright.

Marlink reserves all rights that are not expressly granted to the customer. Without previous approval in writing, and except for in cases permitted by law, it is particularly prohibited to:

- copy, propagate or in any other manner make this documentation publicly accessible, or

- process, disassemble, reverse engineer, translate, decompile or in any other manner open the system and subsequently copy, propagate or make the system publicly accessible in any other manner.

This documentation and the systems have been produced with all due care and checked for correctness in accordance with the best available technology. Marlink disclaims all liability, and responsibility for, whether express or implied, Marlink's solutions quality, performance or suitability for any given purpose which deviates from the performance specifications contained in the product description. The customer bears all risks regarding hazards and impairments of quality which may arise about the use of this system.

Marlink will not be liable for damages arising directly or indirectly from the use of the manual or the system, nor for incidental or consequential damages, except in case of intent or gross negligence. Marlink expressly disclaims all liability for the loss of or damage to hardware or software or data because of direct or indirect error or destruction and for any costs (including connection charges) related to the documentation and the system and due to incorrect installations not performed by Marlink itself.

Marlink reserves the right to update or modify the information in this documentation and the systems at any time without notice for technical improvement.

1.3 Copyright

 Marlink has provided every effort to ensure the correctness and completeness of the information in this document. However, Marlink shall not be liable or responsible with regards to errors contained herein. The information in this document is subject to change at any time without notice. Marlink gives no warranty of any kind regarding the information contained in this document including but not limited to the implied warranties of merchantability and fitness for a purpose.

1.4 Security, Safety and Handling

Before installing and using the XChange, please read the following security and handling instructions. The following general safety precautions and warnings must be observed when operating and servicing the XChange. Failure to comply with these precautions or with specific warnings given elsewhere in this manual violates the safety standards governing the design, manufacture and intended use of the equipment. Marlink assumes no liability for the end-user's failure to comply with the present terms.

1.4.1 Safety Instructions

Before handling any equipment, be fully aware of the hazards of working on electrical circuitry. Ensure that Users are familiar with standard practices for preventing accidents. Please observe the following safety guidelines when installing or handling the XChange:

- Overloaded outlets, extension cords and power strips can lead to fires or electric shocks
- Avoid using socket strips and extension cords if at all possible
- Do not connect multiple extension cords or socket strips to each other
- Before mounting the XChange on the wall, make sure that there are no electrical lines, gas or water pipes located where you need to drill the holes. If necessary, check the site with a pipe detector or consult with qualified experts
- Heat accumulation can lead to overheating of the XChange and subsequent damage to the XChange
- Ensure there is adequate air circulation and avoid any risk of tipping over by NOT stacking or balancing the box on top of other devices. Ensure the installation is firmly and securely in place
- Make sure that the ventilation slits on the XChange housing are always free from obstruction
- Do not cover the XChange
- The base of the XChange can heat up during normal operation. This heat can cause damage to heat-sensitive surfaces
- During electrical storms, lightning and electrical surges present a danger to connected electrical devices
- Do not install the XChange during an electrical storm
- Moisture and liquids that find their way into the XChange can cause electric shocks or short circuits
- Only use the XChange indoors
- Never allow liquids to get inside the XChange
- The device contains hazardous components and should only be opened by authorised Marlink repair Technicians
- Do not open the XChange housing
- Always disconnect all power supply connections before working on XChange hardware
- Check for possible work-area hazards such as damp floors, ungrounded power extension cables and missing safety grounds
- Do not carry out any action that creates a potential hazard to people or renders the equipment unsafe
- Do not work alone if there is any risk of a potentially hazardous condition

WARNING

The chassis of the equipment is tamper proof and should never be opened under any circumstances. Doing so will void the warranty.

WARNING

Do not work on the device during periods of lightning activity. It is especially important *not* to connect or disconnect cables at this time, as the equipment could act as a conductor.

1.4.2 Handling and Mounting

- Do not stack or balance the equipment on top of other devices. This prevents problems due to tripping over cords and cables and allows air to circulate. Check that the installation is fixed securely in place
- Install the box in an open rack whenever possible. If you install it in an enclosed rack, you should make sure that it has adequate ventilation. Do not add too many devices as each unit generates heat. An enclosed rack should have louvered sides and a fan to cool the air
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, you should check the position of the chassis when sliding it all the way into the rack
- Ensure you have a properly working UPS system available and connect the XChange to this UPS. Do not install the system, if no UPS is available or defective
- In an enclosed rack that has a ventilation fan on the top, the excess heat generated by equipment near the bottom of the rack may be drawn upwards into the intake ports of the equipment above. Make sure you provide adequate ventilation for the equipment at the bottom of the rack
- You can place the XChange on a horizontal surface or mount it on to a wall
- Place or hang the XChange in a dry location that is free of dust and protected from direct sunlight
- When connecting the XChange to your on-board network using a network cable, keep in mind that the cable can be no longer than 100m
- If you would like to establish wireless connections between the XChange and a specific area on board, you should position the XChange WiFi access points at a central location in the target area
- Never pull the power supply if the XChange still runs

WARNING

Failure to comply with the listed safety and operating instructions is a violation of the general terms and conditions. In such cases, Marlink accepts no liability or warranty and reserves the right to charge the contractual penalty fee.

1.5 Turn off and Reboot

The XChange is designed to operate without a reboot for long time. In rare cases, it can be useful to reboot the XChange.

When should an XChange be rebooted:

1. After installation of important security patches, the box notifies the Captain to reboot
2. In the 'Event Logs' section of the Dashboard a message asks for a reboot
3. Marlink support asks to reboot the unit
4. During a firmware update
5. In the rare case, the XChange is frozen or a service of XChange does not work

When is no reboot required:

1. The internet speed appears very slow
2. Phone calls cannot be established
3. Access to the internet is not possible
4. A communication device is shown as 'offline' in the XChange Dashboard
5. The local network (wired or WiFi) seems inaccessible or slow
6. Access to the XChange interface is slow or seems inaccessible
7. As regular habit

1.5.1 Preferred Reboot / Shut Down

The 'Power Control' allows the Administrator and Captain to either reboot or shut down the XChange without touching the XChange hardware.

To restart or shut down the XChange, go to *BOX SETTINGS > System > Power Control* and click the 'Shutdown' or 'Restart' button.

The XChange will stop all running services and reboot appropriate. A reboot can last a few minutes. Do NOT interfere with the system or disconnect from power supply during that time. Wait until the XChange user interface is accessible again.

1.5.2 Alternative Reboot / Shut Down

Reboot the XChange hardware directly only, if the XChange user interface is absolutely not accessible or an error message is displayed in the web browser.

➔ To reboot the hardware, press the power-button just short, just for 1 second, and release

The XChange will stop all running services and reboot appropriate. A reboot can last a few minutes. Do NOT interfere with the system or disconnect from power supply during that time. Wait until the XChange user interface is accessible again.

IMPORTANT

If you press the power button for more than 10 seconds, the XChange is shutdown completely.
Shut down the XChange via the power button only when being advised by Marlink Support!

WARNING

Never disconnect the power cable while the XChange is in operation. Pulling the power cable can harm the system and lead to a loss of the system.

2. Access and Login

To access the XChange web interface, you need to connect a computer or smart device to the local network and have a valid User account ready.

To log in and use the XChange web interface your browser must accept cookies.

2.1 URL and Login

The login page can be accessed using any web browser that supports JavaScript by entering the URL: https://xchange-box.com.

The mobile-optimised web interface can be accessed directly by entering the URL: https://m.xchange-box.com.

A 'Captive Portal' function can be enabled, which forwards a User to the XChange login page automatically if the User tries to access a web page directly and is not already logged in. Depending on the device used, the User is automatically redirected to the desktop or mobile web interface.

If the system forwards the User to the wrong XChange web page type, then a link is provided to click through to the other type.

2.1.1 Security Warnings in Webbrowsers

The secured 'https' access to the XChange user interface requires up to date certificates, which are updated by the system automatically. In the rare case, a certificate is not updated in time, the web browser may shows a warning message about potential security risks:

This is not a real security risk and it´s recommended to add an exception to avoid getting these warnings again. Please review the browser´s documentation, how to add such an exception.

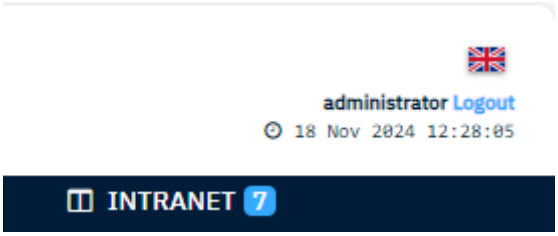
2.1.2 Login

To log in to the XChange, use the username and password provided by the Master on board or another responsible person.

Users without a valid User account can use the 'Create an Account' option on the login page to create their own User accounts. For more details, please check the 'User Account Management' chapter later in this document.

2.1.3 Logout

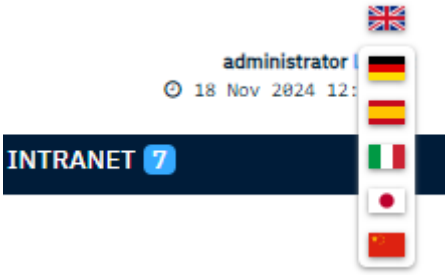
To log out from the XChange, click the 'Logout' link at the top centre of any page.



2.1.4 Multilingual Interface

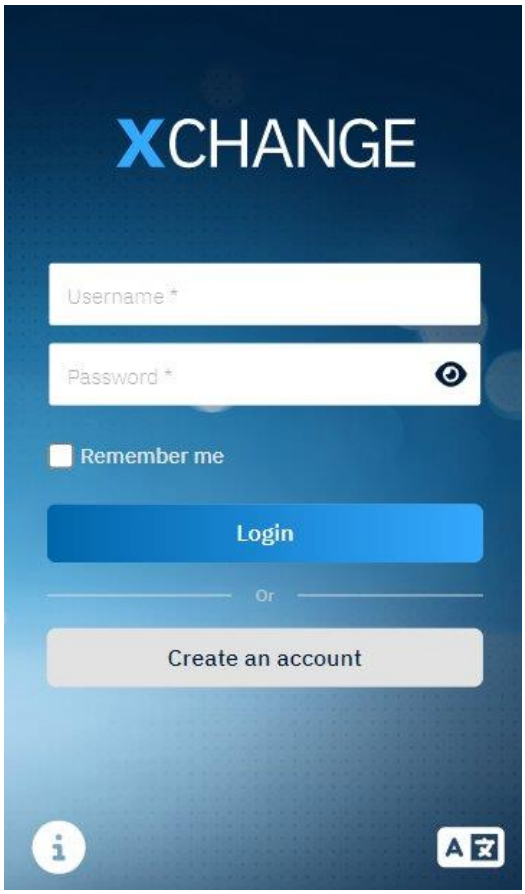
For an easier use on board, each onboard XChange user can choose his preferred language for the XChange user interface. Available languages are English, Italian, German, Spanish, simplified Chinese and Japanese. During installation, the default system language can be selected, while each user can select and change the display-language at any time. The desktop-version and mobile version support the language selection.

To change the interface language just click on the flag next to the 'Logout' option and select the preferred language. The page will be refreshed and displayed with the last selected language.



2.1.5 Access Mobile-Optimised Web Interface

The mobile-optimised version of the XChange web interface can be accessed using any web browser by entering the URL: https://m.xchange-box.com.



Please note

It is highly recommended to access the internet through the mobile interface while using a smartphone or tablet. Smart devices accessing the internet through the desktop version are disconnected if another App is started. When accessing the internet through the mobile version, the data connection will be disconnected automatically (default 2 hours).

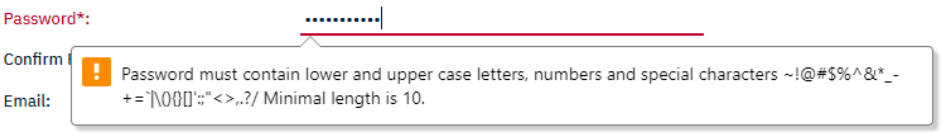
2.2 Create Your Own User Accounts

If it is enabled by the Administrator, then Users may create their own User accounts without the need to request the account to be created by an Administrator on board.

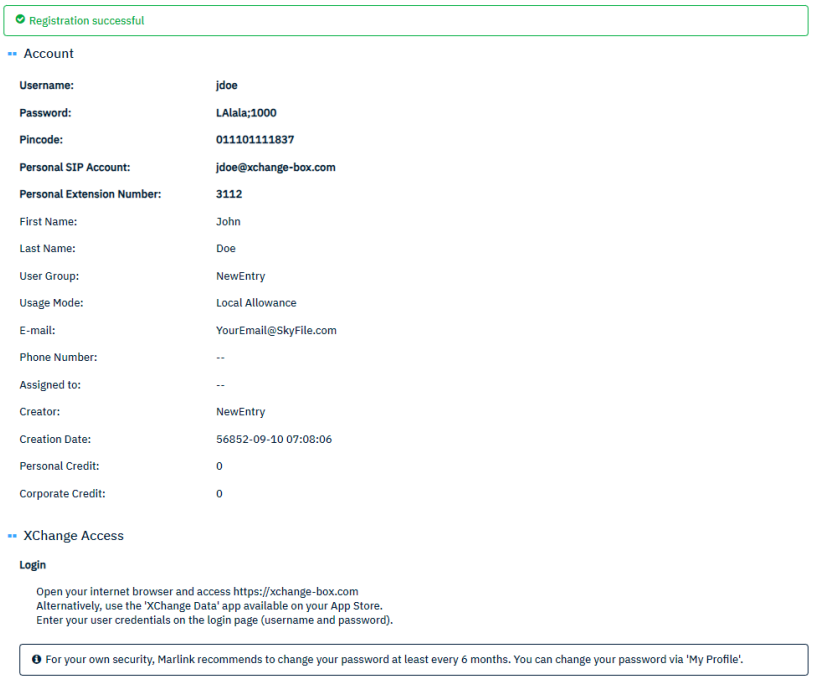
To create your own User account, access the XChange login page and click on ‘Create an Account’.

Set all your personal details as requested and click ‘Register’.

You password must be at least 10 digits long and contain upper, lower case letters, numbers and special characters.



The page will refresh and show the ‘User Account Voucher’ with account details such as username and password, PIN code, Internet access and voice call description. If you want to, you can note down the User credentials or click ‘Print’ to print them.



2.3 User Profiles

There are 3 predefined access level profiles that provide different access rights for usage, management and configuration. There is one account preconfigured for each access level. Details of access rights for each preconfigured account are described in the following pages.

2.3.1 Superadmin & Field Engineer

Only the Field Engineer can install and set up the XChange. Only the Superadmin and Field Engineer have full access to all XChange detailed configurations.

The Field Engineer is not allowed to launch a data session or voice call, so there is no 'MY PROFILE' page for this account.

WARNING

The Superadmin login details shall only be known by a certified Installer and never be given to any on-board staff to avoid misconfiguration of important components and the loss of connectivity. The Superadmin password is only provided to trained and certified Technicians or Installers.

WARNING

The Field Engineer account will be automatically disabled 3 days after first login.

2.3.2 Administrator

Only the local Administrator can change the configuration of the XChange. The Administrator is the highest access level that is given to customers.

The Administrator is not allowed to launch a data session or voice call, so there is no 'MY PROFILE' page for this account.

2.3.3 Captain and Master

The Captain can manage the XChange.

Generally, the Captain has read-only access to the XChange configuration, can manage local Users and User groups and can launch data sessions and voice calls.

2.3.4 Crew

Crew members are only allowed to use the XChange and have no access to the configuration. They are only permitted to launch data sessions, make voice calls (depending on their local prepaid allowance) and access the XChange Intranet.

2.3.4.1 Default User Accounts

The table below shows the factory default User accounts that are available for all new installed XChange. The same usernames and passwords are available on all XChange:

ACCOUNT	ACCESS GROUP	USERNAME	PASSWORD
Administrator	Administrator	administrator	Request from Marlink Service Desk
Captain	Master	dcaptain	10041234
Crew Member	Crew	dcrew	10051234

Please note

The password of the Administrator account will change with each XChange Firmware upgrade. Please contact Marlink Service Desk for the latest Administrator password if you are qualified to manage the XChange system.

The customer is obliged to change the default administrator password via Portal360 soon after installation.

Recommendation

For security reasons it is strongly recommended to deactivate the default user accounts after initial installation. To ensure a high level of access security, please create new user accounts with a stronger password.

2.3.5 Access Rights

The following table displays access rights for all User profiles.

Meaning of the code words:

- Admin = Full read and write access
- Access = Read and execute access
- √ = Read-only access
- Blank = No access

	Installer	Administrator	Captain	Crew
Box Initialisation (Using the Wizard)	Admin			
Personal Homepage	√	√	√	√
Box Settings	Admin	Admin	√	
Devices				
Overview and Device Switch	Access	Access	Access	
Device Ranking	Admin	√	√	
Device Settings	Admin	Admin (partly)	√	
Accounts				
Overview	√	√	√	
User Management	Admin	Admin	Admin	
Groups	Admin	Admin	Admin	
Accounts Settings	Admin	Admin	√	
Price Matrix	The Price Matrix is managed from shore only.			
Credits				
Credits Overview	Admin	Admin	Admin	
Prepaid Vouchers	Admin	Admin	Access	
Credit Settings	Admin	Admin	√	

	Installer	Administrator	Captain	Crew
Logs	√	√	√	
Telephony				
Telephony Overview	Admin	Admin	√	
Settings	Admin	Admin	√	
Network				
Overview	Access	Access	Access	
LANs	Admin	Admin	Access	
WANs	Access	Access	√	
OpenLAN	Admin	Admin	Admin	
Network Assets	Access	Access	Access	
Firewall	Admin	Admin	Access	
Inter-LAN & Local DNS	Admin	Admin	√	
DNS Management	Admin	Admin	√	
DNS Blacklisting	The DNS Blacklisting is managed from shore only.			
Blocked Systems	√	√	√	
Remote Access	Admin	Admin	Access	
Remote Management	Admin	Admin	Access	
Cloud	Access	Admin	Access	
Virtual Machines (opt)				
Guests	√	√	√	
Host	√	√	√	
Disk Image Store	Access	Access	√	
System				
Overview	√	√	√	
System Monitoring	√	√	√	

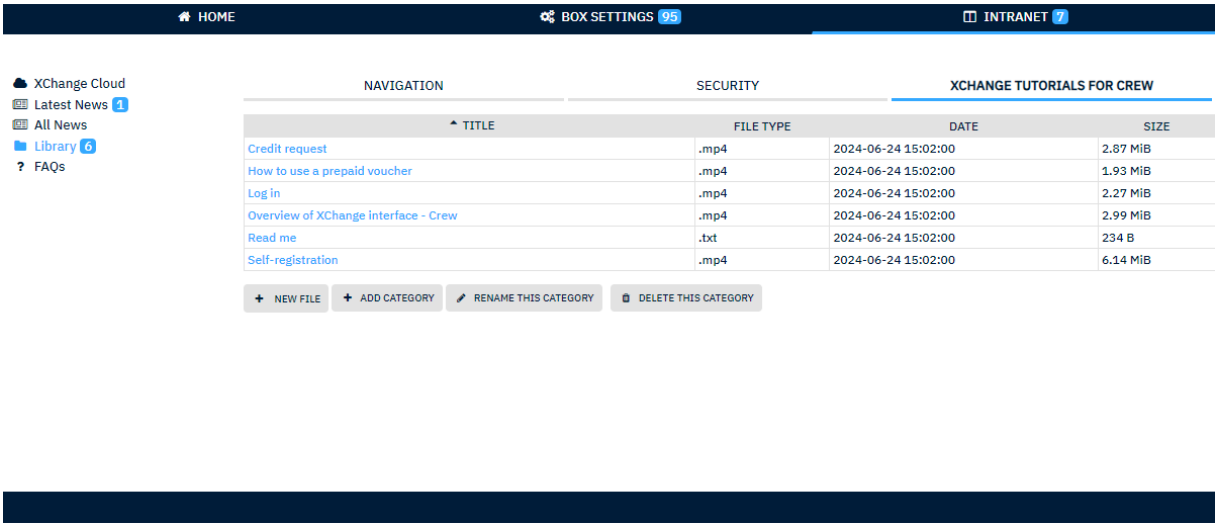
	Installer	Administrator	Captain	Crew
Time Management	Admin	Admin	Admin	
Backup and Restore	Admin	Access	Access	
System Update	Admin	Admin	√	
Synchronisation	Admin	Admin	Access	
Power Control	Admin	Admin	Admin	
Certificates	√	√	√	
Start Wizard	Admin	√	√	
My Profile				
Account			Admin	Admin
Usage Log			√	√
Permissions			√	√
Telephony Cost			√	√
Intranet				
Local Library	Admin	Admin	Admin	Access
FAQs	√	√	√	√
XChange Cloud	Access	Access	Access	Access
All News	√	√	√	√

3. User Portal and Web Interface

3.1 Navigation Design

The XChange uses 'L-shaped navigation' design – the most frequently used navigation design for 'classic' web navigation. This involves a combination of horizontal and vertical navigation.

Horizontal navigation is used for main pages such as 'MY PROFILE' or the local Intranet. Vertical navigation is used to navigate down into specific functions inside the main pages or sections.

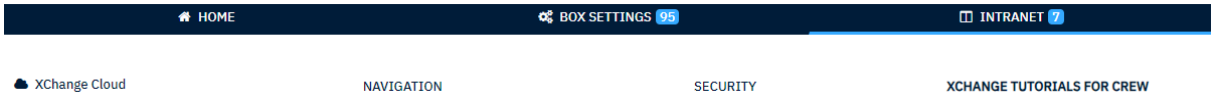


3.1.1 Top Navigation Bar

The top navigation bar includes the main sections of the XChange. The table below shows which sections are displayed to each of the 3 User profiles:

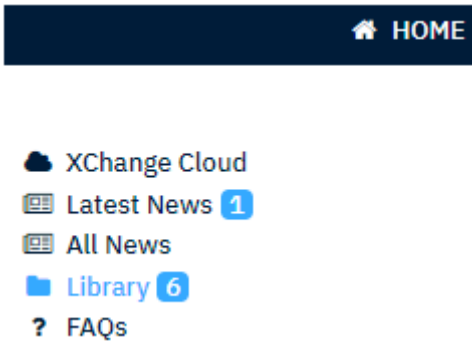
	ADMINISTRATOR	CAPTAIN	CREW
'HOME'	√	√	√
'BOX SETTINGS'	√	√	
'MY PROFILE'		√	√
'INTRANET'	√	√	√

The top navigation bar is grey with each section named in white text. When the mouse pointer rolls over a section, the tab turns orange. When you click on a section or on one of its pages, the section tab stays orange.



3.1.2 Left Navigation Bar

The left navigation bar lists the subsections (2nd level of navigation) and the pages inside the subsections (3rd level).



3.1.3 Weblets

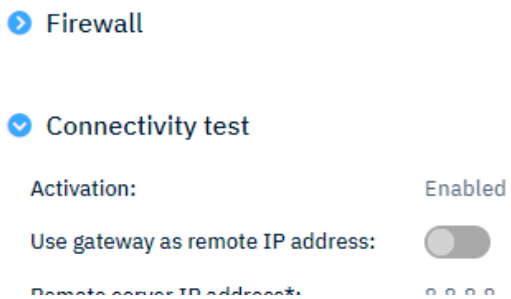
A 4th level of navigation is possible using horizontal ‘weblets’:

- Before they are selected, a weblet is coloured white
- When you select a weblet, the text changes to bold and an orange line appears

3.1.4 Collapsible Panels

To avoid displaying a very large amount of information on a single page, the system uses collapsible panels to describe a long table or a process.

These panels can be opened or closed independently of each other as shown below:



You can click on each panel and toggle between the expanded and collapsed view. An arrow indicates the status: pointing to the right (collapsed state) or pointing downwards (expanded state).

3.1.5 Tables

To avoid displaying a very large amount of lines on one page, the system uses flexible tables to display a large table.

The User can choose what information is displayed.

DATE	USER	GROUP	TYPE	DEVICE NAME	MODE	DURATION	CONSUMED UNITS	BILLED UNITS	TOTAL COST	DESTINATION
2024-11-18 11:41:02	synchro	System	DATA	Starlink Maritime 2	Corporate Usage	7s	23 KiB	23 KiB	0.00022 U	--
2024-11-18 11:01:19	timesync	System	DATA	Starlink Maritime 2	Corporate Usage	1min 7s	6 KiB	6 KiB	0.00006 U	--
2024-11-18 11:01:10	timesync	System	DATA	Starlink Maritime 2	Corporate Usage	8s	3 KiB	3 KiB	0.00003 U	--
2024-11-18 10:39:33	timesync	System	DATA	Starlink Maritime 2	Corporate Usage	3s	2 KiB	2 KiB	0.00002 U	--
2024-11-18 09:41:01	synchro	System	DATA	Starlink Maritime 2	Corporate Usage	7s	23 KiB	23 KiB	0.00022 U	--
2024-11-18 08:41:02	synchro	System	DATA	Starlink Maritime 2	Corporate Usage	7s	23 KiB	23 KiB	0.00022 U	--
2024-11-18 08:39:27	timesync	System	DATA	Starlink Maritime 2	Corporate Usage	4s	2 KiB	2 KiB	0.00002 U	--
2024-11-18 06:41:01	synchro	System	DATA	Starlink Maritime 2	Corporate Usage	7s	24 KiB	24 KiB	0.00023 U	--
2024-11-18 06:39:24	timesync	System	DATA	Starlink Maritime 2	Corporate Usage	2min 16s	4 KiB	4 KiB	0.00004 U	--
2024-11-18 05:41:01	synchro	System	DATA	Starlink Maritime 2	Corporate Usage	7s	23 KiB	23 KiB	0.00022 U	--

3.1.5.1 Sort the Displayed Information

Click once on the title of a column to sort the list in ascending order and click twice to sort into descending order.

3.1.5.2 Change the Number of Lines Displayed

The number of lines to be displayed can be changed by clicking on the number on the bottom line of each table.

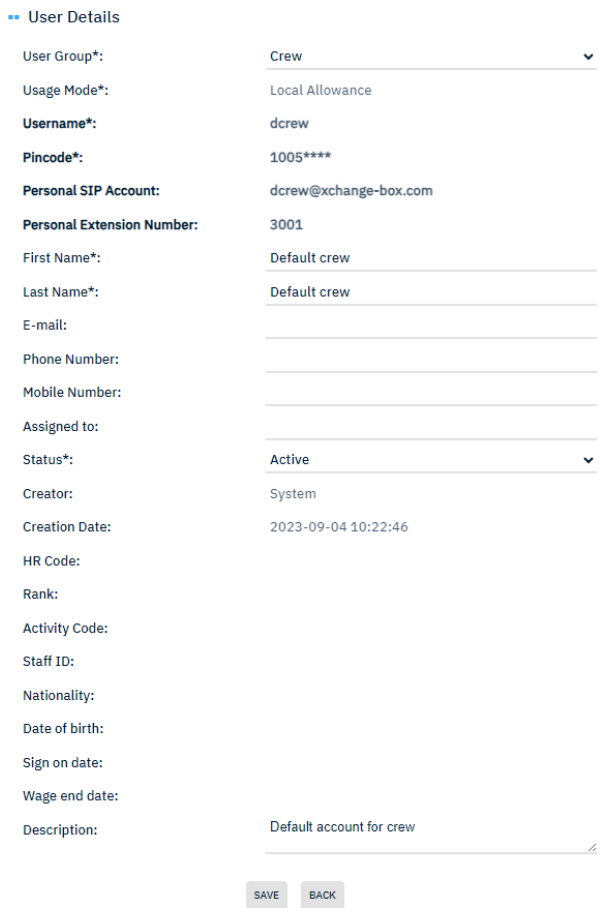
Click '10' to display 10 lines per page or '100' to display 100 lines per page. If more lines are available, then they will be displayed on additional pages.

3.2 General Editing of Data

An example of how to edit the data using the XChange web interface is given below: the example involves changing the User details for a Crew member. The general method for editing and configuring values is the same for much of the XChange data.

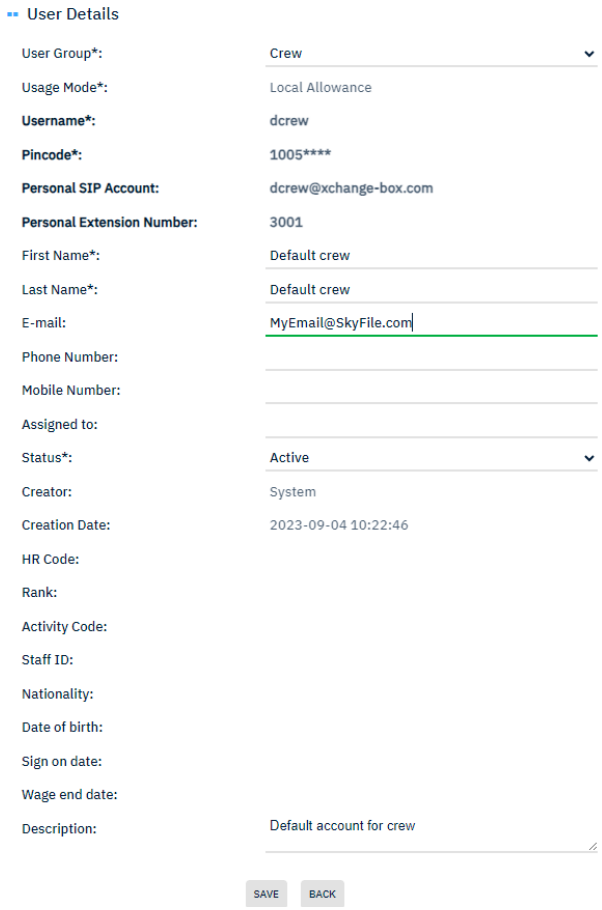
3.2.1 Information Overview

First, the system provides an overview of the existing data:



3.2.2 Edit Data Values

The data fields being displayed are converted into editable fields.

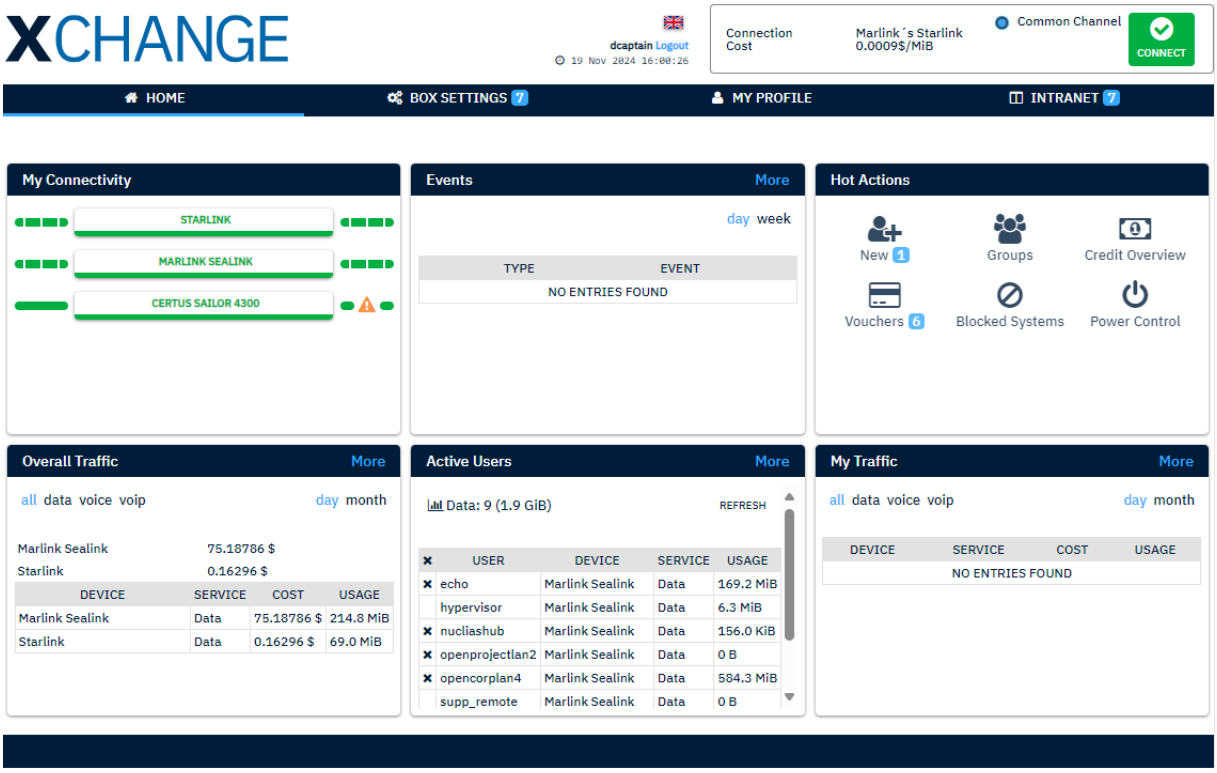


By clicking on ‘Save’, the data that has been changed is stored in the XChange system and the page is refreshed.

☝ You cannot edit fields missing an underline.

3.3 Dashboard

When the User successfully logged in, the system automatically redirects them to the ‘HOME’ screen.



The table below shows which information blocks are displayed on the ‘HOME’ page for each User’s profile.

	ADMINISTRATOR	CAPTAIN	CREW
‘Connectivity’	√	√	√
‘Overall Traffic’	√	√	
‘Hot Actions’	√	√	√
‘Events’	√	√	√
‘Active Users’	√	√	
‘Latest News’			√
‘Latest Files’			√
‘My Traffic’		√	√

3.3.1 Connectivity

The connectivity block shows the actual status of each installed communication device.

A red cross indicates an error, either on board (left side) or on the connectivity side (right side). Moving the mouse pointer above the red cross will display the error message.

All available communication devices that can be used for communication have a green bar below their name, while any devices that are not available have a red bar below their name. For a better judgement of connectivity's quality, a signal strength bar indicates the signal quality for most SatCom connections.

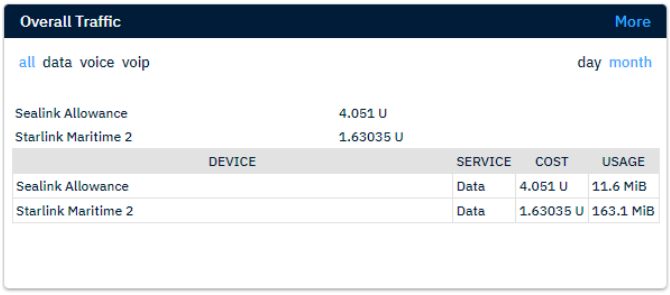
The communication device that is currently in use has an animated light and dark green bar to represent the communication that is happening.

Clicking the 'More' link redirects the Administrator or Captain to the 'Device Management' page, giving access to the device switching overview and the user group – device priority (if Hybrid Switching is ordered).

3.3.2 Overall Traffic

The 'Overall Traffic' block shows the overall traffic consumption for the current day and the current month. The information is displayed separately for each connected broadband terminal:

- Name of broadband terminal
- Data traffic consumption in volume (MB or Min) and amount (€ or $)
- Voice traffic consumption in minutes and amount
- VoIP traffic consumption in minutes and amount



Clicking the 'More' link redirects the Administrator or Captain to the 'Traffic Log' page, providing a detailed account of changes in traffic over time.

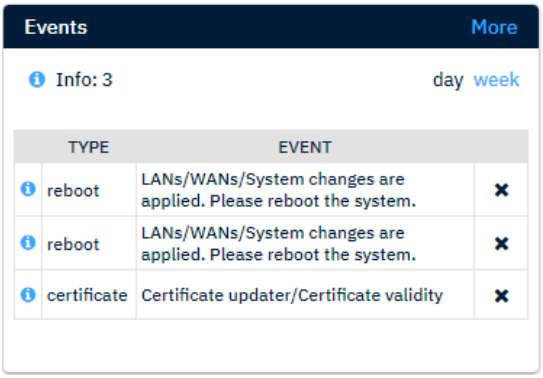
☝ The 'Overall Traffic' block is only displayed for the Administrator and Captain.

👍 Tip!! Clicking to change the communication type from 'all' to either 'data', 'voice' or 'voip' will filter the display to show only the selected type.

3.3.3 Events

The ‘Events’ block displays all event messages if, for example, a device is no longer ready for connection.

If an alert is issued, then the ‘Type’ (‘Certificate, ‘Connection’, etc.) and the ‘Event’ description will be displayed inside the box corresponding to the alert category:



Clicking on the ‘More’ link redirects the Administrator or Captain to the ‘Event Log’ page, providing more details about the events.

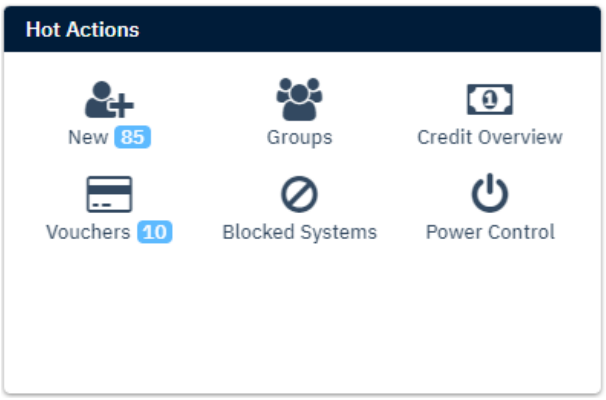
To acknowledge and to hide an event message from the dashboard, simply click the ‘X’ next to the message.

3.3.4 Hot Actions

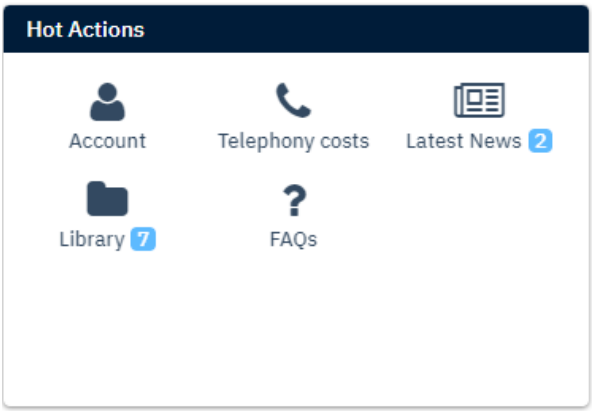
The ‘Hot Actions’ block provides direct access to the most important and commonly used management functions. With a simple click on one of the ‘Hot Actions’, the User is redirected to the corresponding subsection within the XChange interface.

If there is an update to the data in one of the ‘Hot Actions’ sections, then the number of new updates is displayed in an orange cube.

☝ The ‘Hot Actions’ block contains different actions depending of the User profile.

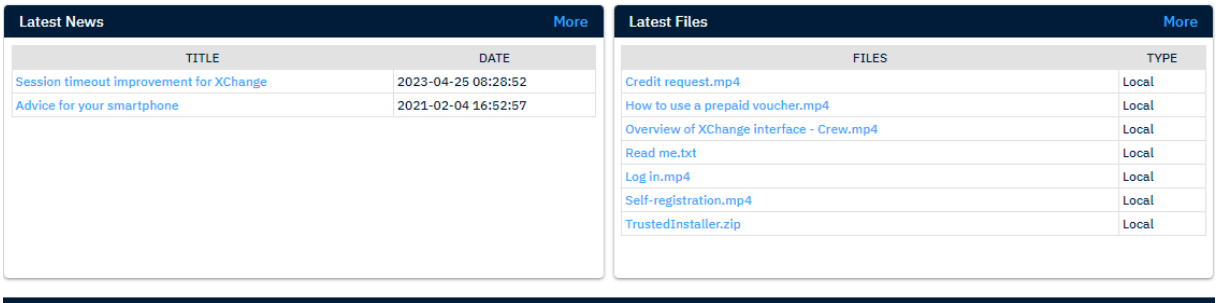


Captains and Administrators typically have access to the main administration functions within User and credit management, while the Crew have direct access to the local Intranet and other selected functions.



3.3.5 Latest News and Latest Files

The ‘Latest News’ and ‘Latest Files’ blocks are only displayed on the Crew dashboard. Each time the local Intranet is updated from shore, the latest and newest updates are shown within these blocks.

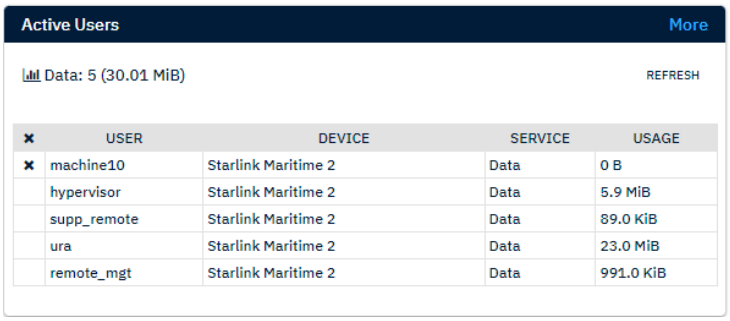


The hyperlinked news ‘Title’ forwards the Crew member to the specific news content.

☝ The updated news or files are only displayed until the User views/reads them. After the first view, this information is removed from the User’s dashboard to make space for new updates.

3.3.6 Active Users

Only Captains and Administrators have a block on their dashboard called ‘Active Users’ that provides real-time information about any active User, machine or system account. The ‘Active Users’ section displays the Users’ name, device used, type of communication and the total usage of the active communication session.



The small X next to the ‘User’ and the username represents a session cut function for all active sessions.

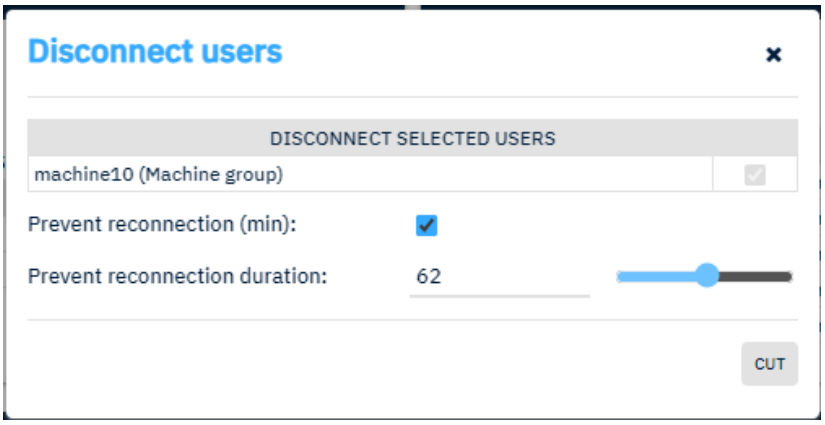
Please note

Some system-user may are displayed in the ‘Active User’ section. Because those Users are mandatory to guarantee a full operational service, their sessions cannot be interrupted.

3.3.6.1 Cut an Active Session (Disconnect single Users)

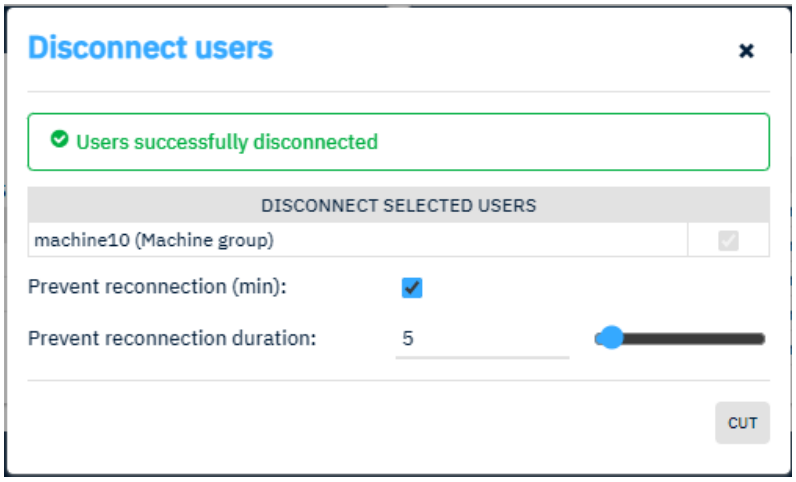
In case the Administrator or Captain wants to make a phone line available or to open the data bandwidth, it is possible to disconnect single users.

There is an option to prevent reconnection for a defined period to keep the bandwidth available.

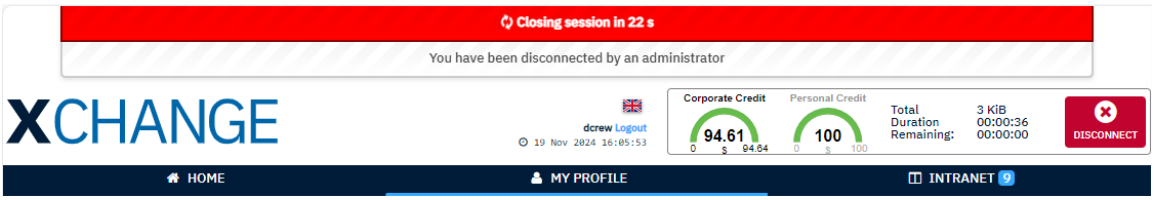


The reconnect prevention time is controlled by a slider. The minimum time is 5 minutes and the maximum reconnect prevention time is 120 minutes. Within this time, disconnected User(s) cannot log in or make a call.

The disconnect function takes a few seconds to initiate and then the Captain receives the following message to confirm the disconnection:



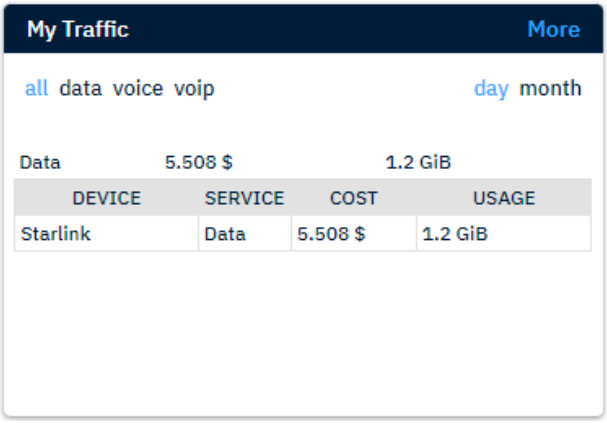
The disconnected User either hears a voice prompt on the phone or a notification on the top of his XChange view informing him that he has been disconnected.



3.3.7 My Traffic

The 'My Traffic' block shows a User's personal traffic consumption for the current day and current month. The information is displayed separately for each connected broadband terminal and type of service:

- Name of broadband terminal
- Data traffic consumption in amount ($/€) and volume (MB/Min)
- Voice traffic consumption in amount ($/€) and volume (MB/Min)
- VoIP traffic consumption in amount ($/€) and volume (MB/Min)



☝ This block is not displayed for an Administrator, as they are not allowed to launch a data session or voice call,.

👍 Tip!! Clicking to change the communication type from 'all' to either 'data', 'voice' or 'voip' will filter the display to show only the selected type.

3.3.8 Connection

The 'Connection' block enables the Captain and Crew member to launch/disconnect a data session.

3.3.8.1 Displayed Information

Before launching a new data session, the 'Connection' block displays:

- 'Connection' (available data device)
- 'Personal Credit' (local prepaid User)
- 'Corporate Credit' (local prepaid User)
- 'Cost' (cost per MB/min)
- Available channel
    - The number of available channels depends on the available device and the User profile.

3.3.8.2 Launch a Session

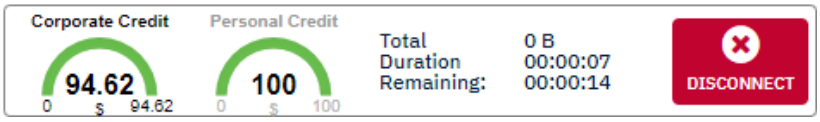
To launch a data session, select the communication channel and press the green 'Connect' button. Depending on the individual setup, you may only be able to select one communication channel.

A status bar will inform you about the connection status:

When the data session is established, the User's personalised favourites are displayed automatically.

☝ **During a data session, you can still access the local Intranet, but do not close the XChange portal. If you close the XChange portal, your session will be disconnected automatically.**

During an active data session, the 'Connection' block gives Users information about traffic consumption and credit levels:



3.3.8.3 Disconnect

To disconnect and close the data session, just press the red ‘DISCONNECT’ button.

3.3.8.4 Connect using other Device

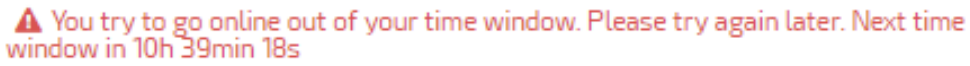
Users can change their device to internet access at any time. If the user forgot to disconnect his previous online-session properly, the XChange offers a forcement to disconnect the previous session.

Please note

On purpose it is not possible to go online with multiple devices in parallel while using 1 user account. To avoid potential side effects, the system forces the user to disconnect before a new connection can be started.

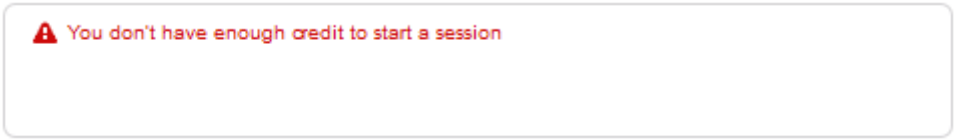
3.3.8.5 Daily Access Limits

When the User exceeds their allowed time window, or when they have already reached the set maximum communication duration for that day, the ‘Connection’ block displays a warning message and the User can no longer connect to the Internet.



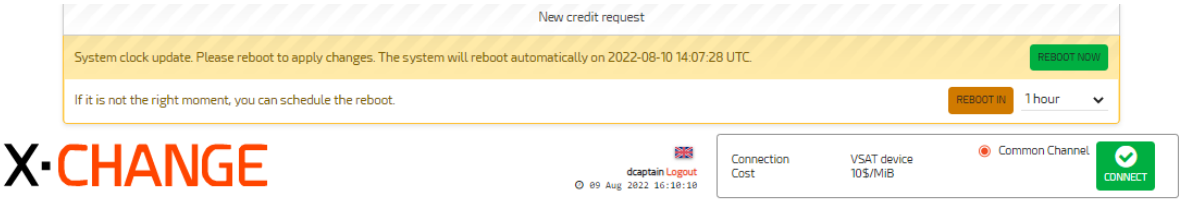
3.3.8.6 No Credit

When the User logs into the XChange web interface but does not have enough prepaid credit left, the system displays the following message instead of the connection controller:



3.4 Notifications

The XChange will occasionally notify the User of important notifications. These notifications are event-driven and are mainly to inform the Captain.



The notifications will be displayed each time the User logs in until the notifications are all resolved.

Some notifications are only to provide information, such as 'The Price Matrix has been updated', while others can forward the Captain directly to the correct subsection of the XChange interface, for example to the 'Credit Management' page. Appendix E lists all available notifications.

3.4.1.1 Important Notifications with Actions

For very important events, such like for instance system clock update, security patch deployment or others, the system plans a specific reboot time afront. If the Captain does not react, the system will reboot automatically at the planned & displayed time UTC.

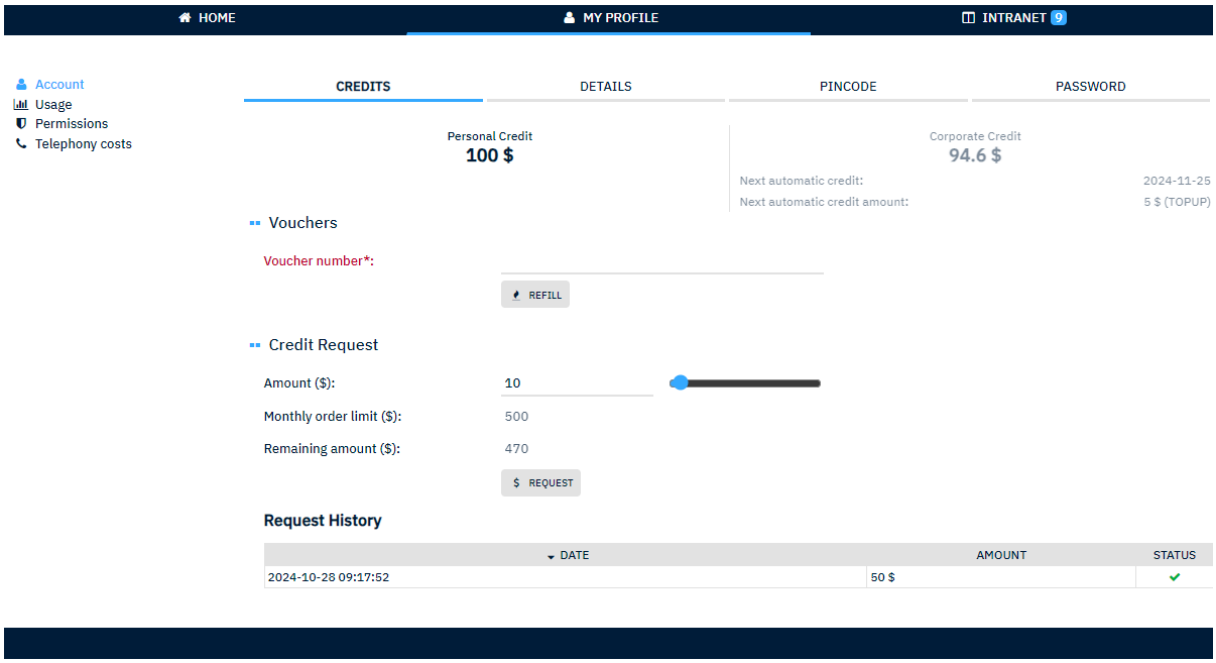
The system plans automatically with a waiting period of 48 hours, since the event happened. E.g. the Captain influence the reboot time by either clicking on "Reboot Now" or reboot in the given options.

3.5 My Profile

The ‘MY PROFILE’ section is displayed for both the Captain and Users.

‘MY PROFILE’ provides individual account management and personalisation capabilities to access:

- User account details
  - Password / PIN code management
  - Credit management
  - Personal account management
- Usage log
- Permissions
- Check telephony costs



3.5.1 Account

The ‘Account’ section gives an overview of the User’s account details.

3.5.1.1 Corporate vs. Personal Credit

The XChange works with 2 separate credit accounts, called ‘Credit Baskets’.

The corporate credit basket is typically refilled manually by the responsible personnel or filled automatically via the ‘Automatic Credit Renewal’ function. The corporate credit can only be spent by the User for online data sessions, while voice communication is prohibited.

The personal credit basket can be filled manually by the responsible personnel, reloaded via XChange embedded prepaid vouchers or by a User’s individual credit requests. Personal credit can be used for any kind of communication, including voice communication. For data connections, the system will, by default, first try to spend the corporate credit and will only use the personal credit if there is no corporate credit remaining.

3.5.1.2 Manage Own Credits

The ‘Credits’ tab is where you can manage XChange local prepaid functions. This tab provides the latest information on remaining corporate and personal credit and when the next automatic credit top up of the corporate credit is planned. You can top up your credit by either using a previously purchased prepaid voucher or by requesting new credit directly.

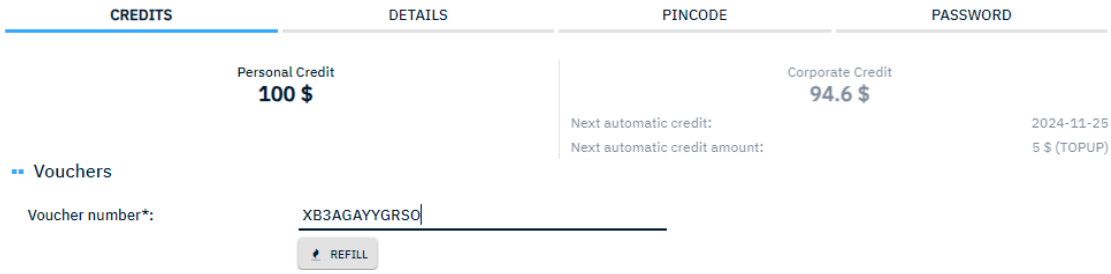
3.5.1.2.1 Credit Top-Up via Prepaid Voucher

To top up your personal credit with prepaid vouchers, a valid prepaid voucher must be purchased by the responsible personnel on board, such as the Captain.

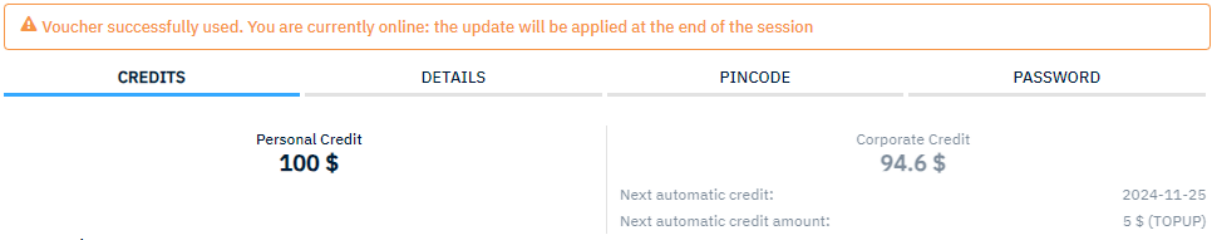
Prepaid voucher codes always consist of 12 characters.

After purchasing a voucher, access the XChange interface and log in with your personal account details.

Go to “MY PROFILE” and type the voucher code in the ‘Voucher number’ field:



Once the credit refill is successful, a notification is shown in green and the ‘Personal credit’ value is topped up with the amount of credit that was linked to that voucher:



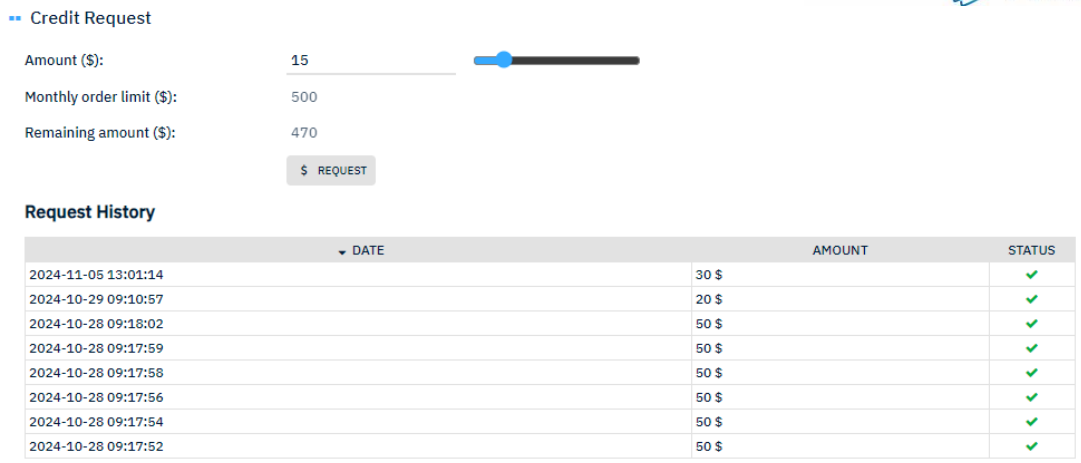
If there is an error during refill, for example, if the voucher code has already been used, is blocked, or not does not exist, then the corresponding error message is displayed above the refill function.

3.5.1.2.2 Credit Top-Up via Credit Request

In case the ‘Credit Request’ function is activated, it is possible to request credit top-up directly through the “MY PROFILE” page, without the need to ask the Administrator on board.

Top-up requests of between 10 and 50 $/€ can be made by using the slider.

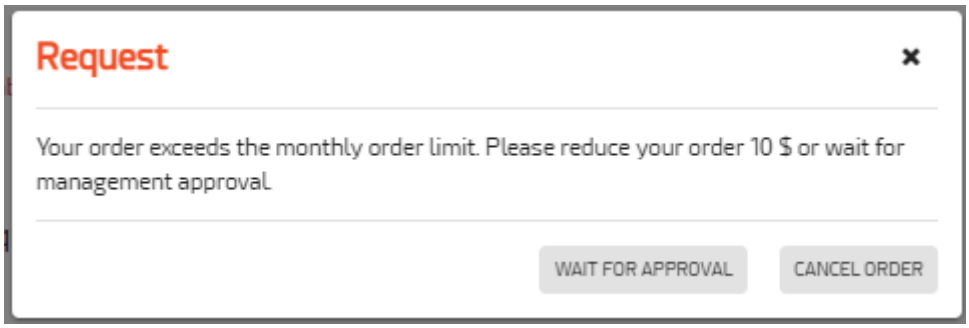
A monthly order limit can also be set and displayed on the interface, as well as the remaining amount that can be ordered before the monthly limit is reached.



To request new credit, simply drag the slider to the correct amount to be requested.

If the new request is still within the monthly order limit, the credit top-up will be processed immediately.

If the new request exceeds the monthly order limit, a warning message is shown:



If the button 'WAIT FOR APPROVAL' is pressed, the credit request is stored and transmitted to the responsible personnel to decide.

For example, the Captain will receive this credit request and can accept or decline the request.

The 'Request History' table, shown below the credit request, provides tracking information for each credit request. The 'Status' column indicates if a pending credit request was accepted or declined.

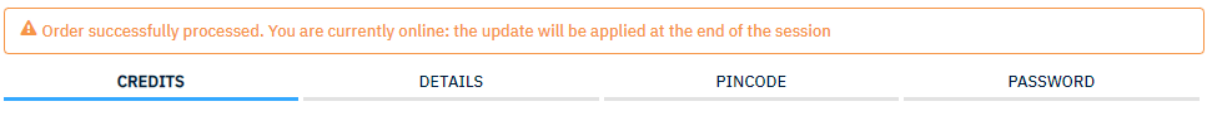
PLEASE NOTE

The credit request function may not be available. The decision for this is taken by the responsible Administrator or Fleet Management on shore.

3.5.1.2.3 Credit Top-Up while online

When credit top-ups are requested, or prepaid voucher loaded, during an active voice call or data session, the system will not issue that credit top-up immediately.

Once the voice call or data session ends, the credit top-up will be executed immediately.



3.5.1.3 Change Password

A password is required to log in to the XChange User interface (desktop and mobile version), as well as to make use of the XChange Voice smartphone app.

To change your password, go to the 'Password' tab and first enter your current password, and then your new password twice to confirm your change.

Once you click on the 'SAVE' button, the new password will be stored in the system and is usable immediately.

3.5.1.4 Change PIN Code

The PIN code is an 8-digit code which is required by a phone before being able to call out.

To change the PIN code, click the 'Pincode' weblet and proceed as follows:

- Type in the last 4 digits of the current PIN code
- Type in a new set of 4 digits (only the last 4 digits can be changed)
- Confirm the new set of digits
- Click 'SAVE'

3.5.1.5 Account Details

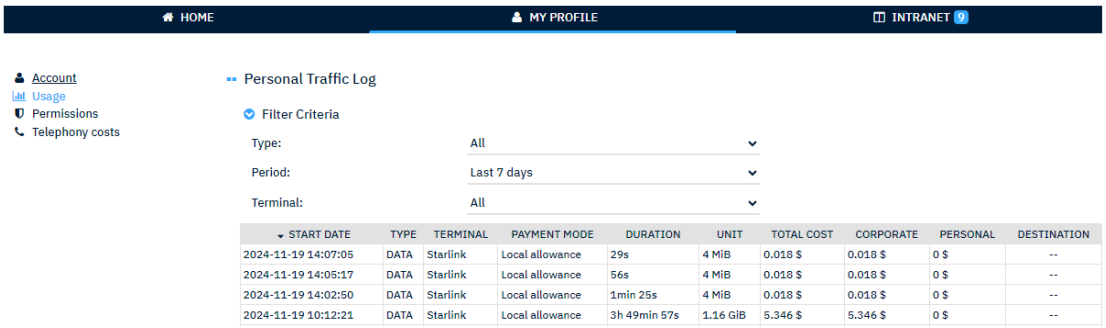
Within the ‘Details’ tab, you can edit the name, email address and mobile number fields. Just type the new values into the white text fields and save the changes. An overview of all the information is shown in the table below:

	EDITABLE	READ-ONLY
Status		√
Account Type		√
First Name	√	
Last Name	√	
Email Address	√	
Fixed Number	√	
Mobile Number	√	
User Group		√
PIN Code		√
Personal SIP Account		√
Personal Extension		√
Rank		√
Additional Details		√

The non-editable fields (except for the PIN password) can only be changed by the Administrator or Captain in the ‘Accounts’ section of the XChange.

3.5.2 Usage

The ‘Usage’ page provides each User with their personal usage and credit consumption log for all broadband terminals and types of communication for up to 30 days.



	DESCRIPTION
‘START DATE’	Start date and time of the session
‘TYPE’	Data, voice or VoIP
‘TERMINAL’	Terminal used
‘PAYMENT MODE’	Corporate usage, local prepaid, or Universal Card
‘DURATION’	Duration of the session
‘UNIT’	Units consumed e.g. KB, min
‘TOTAL COST’	Credit consumption of the session
‘CORPORATE’	Corporate credit consumed by a session (data only)
‘PERSONAL’	Personal credit consumed by a session (data and voice possible)
‘DESTINATION’	Displays the number dialled (For voice calls only)

By default, all available usage data can be displayed by entering the usage log.

You can display specific usage details using the selection criteria given at the top. The selection criteria include:

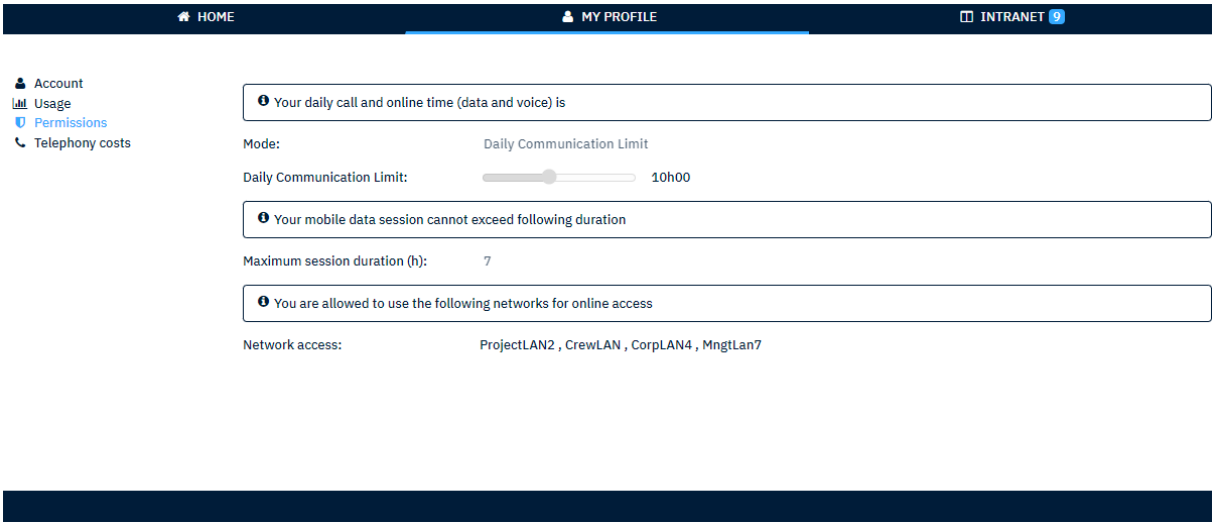
- Type
  - All
  - Voice
  - Data
  - VoIP
- Period
  - Current month
  - Last 7 days
  - Last 14 days
  - Last 30 days
- Terminal (if more than one is available on board)
  - All terminals
  - A specific terminal

To filter specific usage details, select the criteria you want the log filtered. The page refreshes, and only the selected usage details will display.

Tip!! Click once on the name of any column to sort the list in an ascending order and twice for a descending order.

3.5.3 Permissions

The ‘Authorizations’ section provides each User with information about their allowed online usage and access authorisations.



The level of detail on online usage authorisations provided to the User varies according to the User’s group settings.

The ‘Maximum Daily Duration’ shows the allowed online time per day, per User. This setting is defined by the Administrator. If the maximum daily duration is exceeded, the User is prevented from going online or making a call on that day.

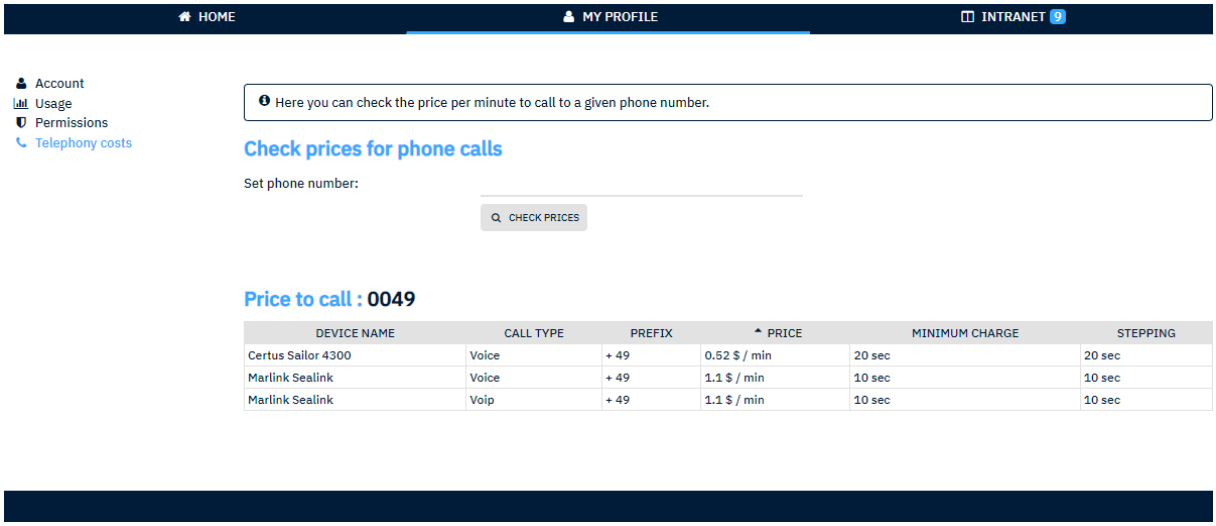
The ‘Daily Time Windows’ show up to 3 different time windows during the day when a User is allowed to go online or to place a voice call.

The ‘Maximum session duration’ is an automatic set threshold displaying the time after which a User is disconnected automatically.

The ‘Network access’ shows which of XChange’s local networks are accessible for a User. If a network is not shown in the ‘Authorizations’ page, then the User will be not able to get online from a computer on that network.

3.5.4 Telephony Costs

All XChange Users can see the price per minute that has been defined by the Administrator for calling a specific country.



The system provides a list of all available call types and installed communication devices separately. To check the call price for a specific country, simply enter the phone number and click ‘CHECK PRICES’.

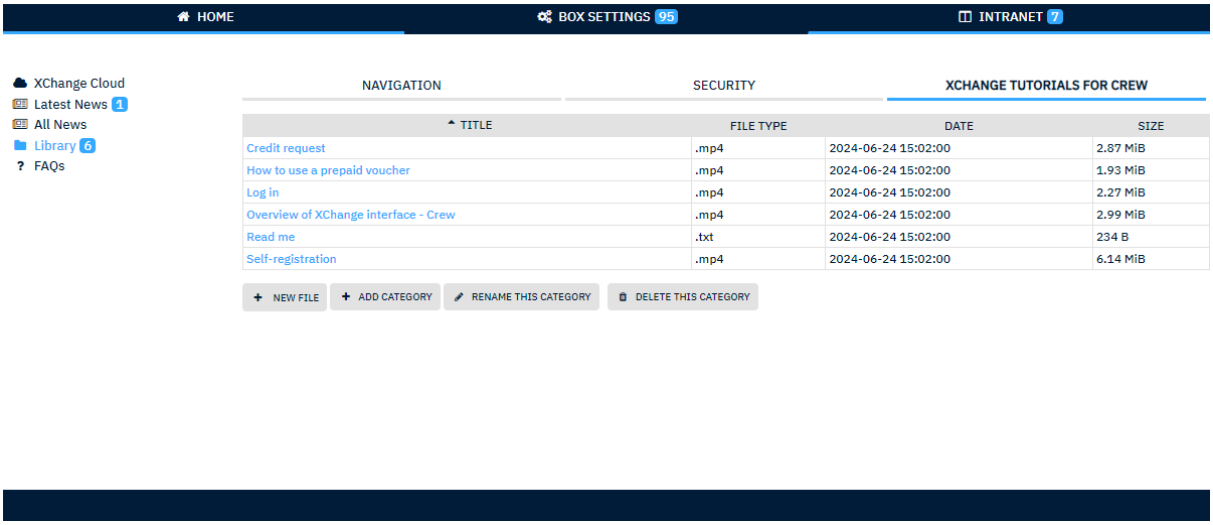
PLEASE NOTE

Marlink recommends that you always search for the full phone number. Depending on the defined price matrix, calls to fixed lines and cellular networks can differ – even within the same destination country.

3.6 Intranet

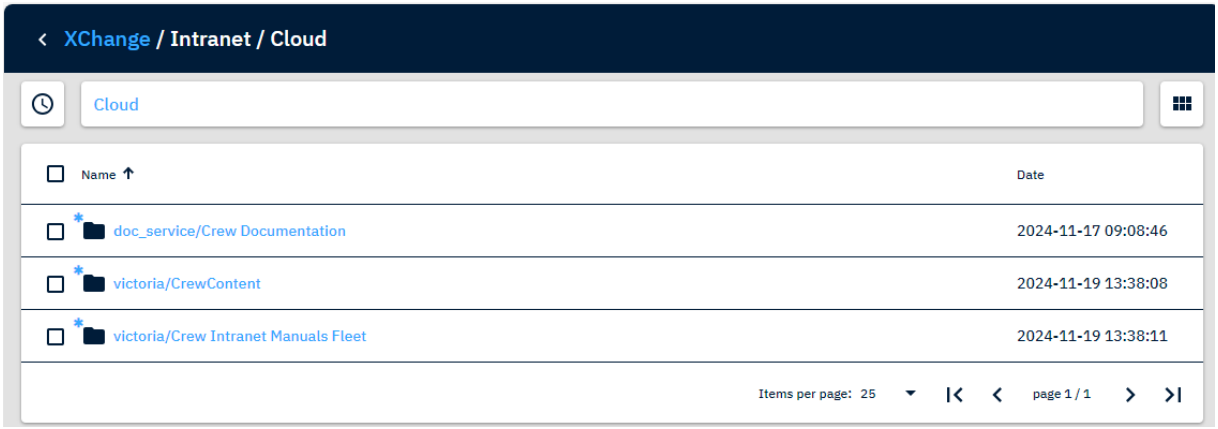
The ‘Intranet’ section is displayed for all Users on board and gives access to:

- XChange Cloud
- Newsroom
- Local Library
- Frequently Asked Questions (FAQs)

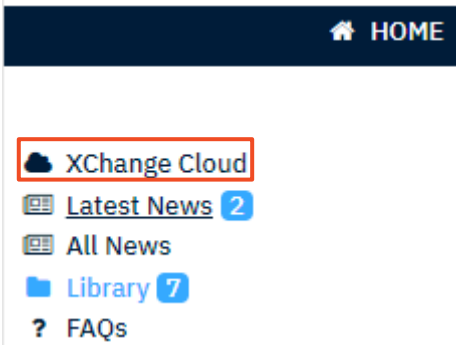


3.6.1 XChange File Cloud

The XChange Cloud provides access to content being made accessible via the XChange user interface. As a default service, Marlink´s documentation service is made available on all XChange platforms. It provides latest user manuals, applications for onboard use and other additional content as free service. There are documents available for all XChange user and in addition separate documents only available for Captains.
XChange File Cloud may presents additional folders if the File Cloud service was ordered as additional XChange service.

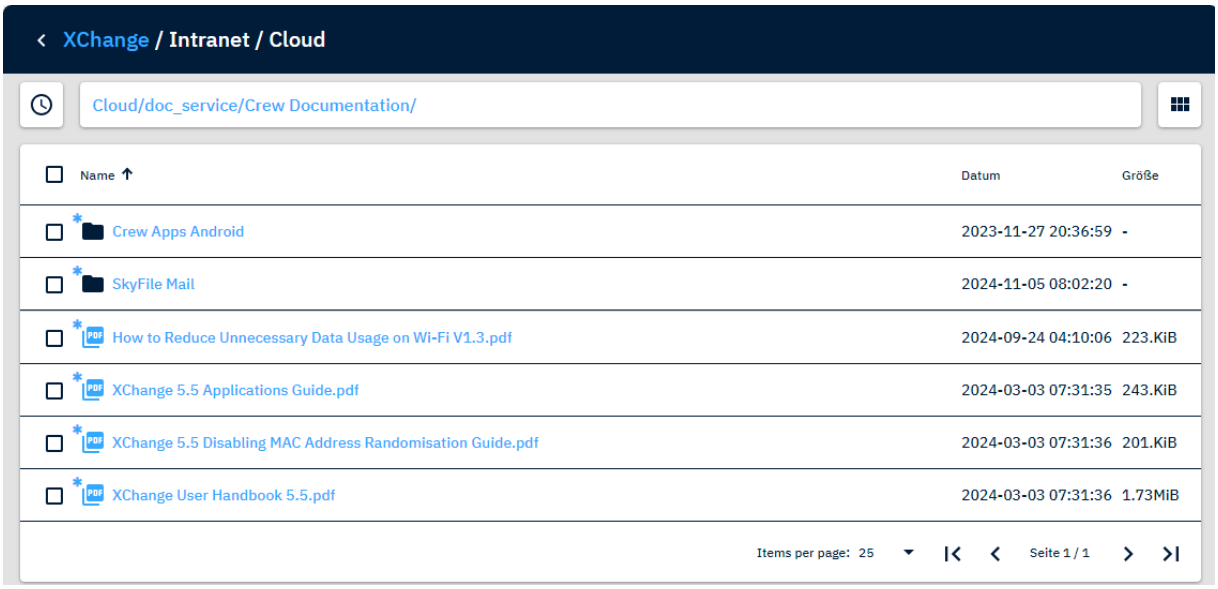


To enter the XChange Cloud section, click on 'XChange Cloud' within the Intranet section.



Depending on the setup, defined by the responsible personnel on shore, the number of top-level folders may vary.

By clicking on a folder, the page will refresh and show all files and subfolders.
Dependent on the available content the device used, some files like documents, images can be opened directly with a simple click on the file-name.
Some file formats, not supported by the web browser, can be downloaded first. To download a file, select the file and click the 'download' button:



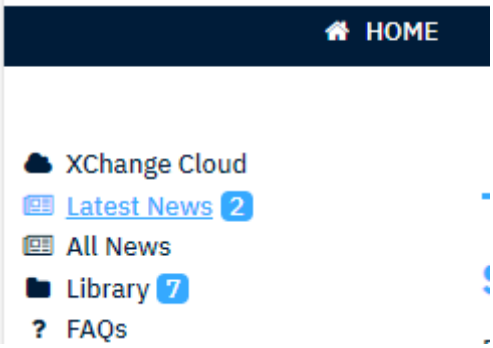
Please note: The 'delete' option is only available for administrative staff.

INFORMATION

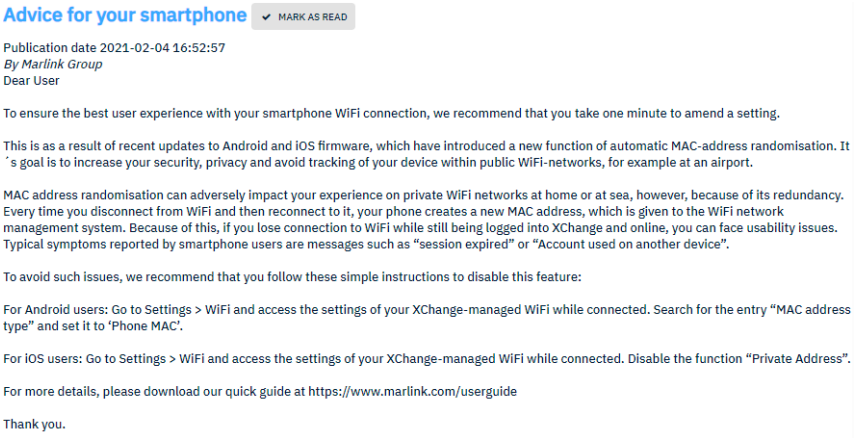
The documentation service is based on XChange Cloud and made freely available to all XChange users. XChange Cloud can be ordered as an optional service to benefit from its features optimising file transfers shore to ship in the best possible way.

3.6.2 Newsroom

The newsroom provides news sent from the shore to the XChange.



☝News cannot be edited or deleted by local Users.



Advice for your smartphone MARK AS READ

Publication date 2021-02-04 16:52:57
By Marlink Group
Dear User

To ensure the best user experience with your smartphone WiFi connection, we recommend that you take one minute to amend a setting.

This is as a result of recent updates to Android and iOS firmware, which have introduced a new function of automatic MAC-address randomisation. It ´s goal is to increase your security, privacy and avoid tracking of your device within public WiFi-networks, for example at an airport.

MAC address randomisation can adversely impact your experience on private WiFi networks at home or at sea, however, because of its redundancy. Every time you disconnect from WiFi and then reconnect to it, your phone creates a new MAC address, which is given to the WiFi network management system. Because of this, if you lose connection to WiFi while still being logged into XChange and online, you can face usability issues. Typical symptoms reported by smartphone users are messages such as “session expired” or “Account used on another device”.

To avoid such issues, we recommend that you follow these simple instructions to disable this feature:

For Android users: Go to Settings > WiFi and access the settings of your XChange-managed WiFi while connected. Search for the entry “MAC address type” and set it to ‘Phone MAC’.

For iOS users: Go to Settings > WiFi and access the settings of your XChange-managed WiFi while connected. Disable the function “Private Address”.

For more details, please download our quick guide at https://www.marlink.com/userguide

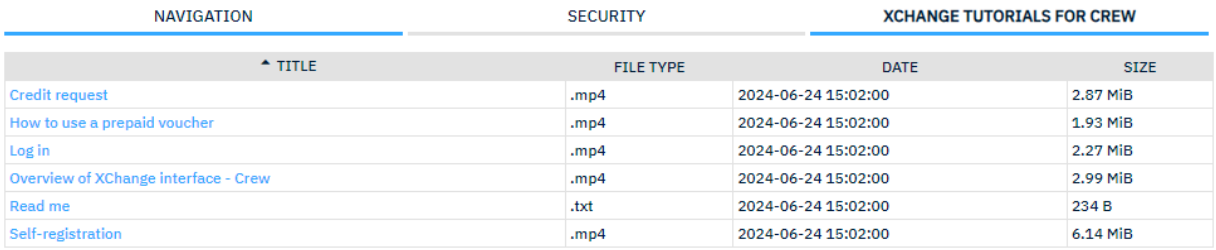
Thank you.

To access to complete news database, click on ‘All News’. The page is refreshed and displays an overview of all news stored on the XChange.

3.6.3 Local Library

The libraries can be accessed by all Users and offer a local store-and-share feature.

The Administrator or Captain can manage categories and upload or delete documents and files to be shared with the entire vessel.



TITLE	FILE TYPE	DATE	SIZE
Credit request	.mp4	2024-06-24 15:02:00	2.87 MiB
How to use a prepaid voucher	.mp4	2024-06-24 15:02:00	1.93 MiB
Log in	.mp4	2024-06-24 15:02:00	2.27 MiB
Overview of XChange interface - Crew	.mp4	2024-06-24 15:02:00	2.99 MiB
Read me	.txt	2024-06-24 15:02:00	234 B
Self-registration	.mp4	2024-06-24 15:02:00	6.14 MiB

Please note

Only the Administrator and Captain have write access!

3.6.3.1 Open Shared Files

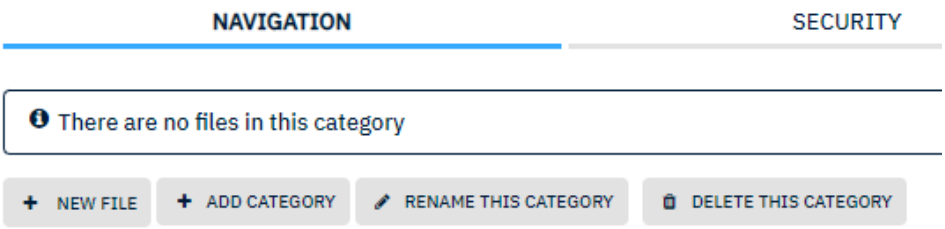
Shared files can easily be opened by clicking on the title.

Depending on the file format and the computer's default settings, either the web browser will open a new window to display the content of the file, or the default application will either open the file or ask if the file should be downloaded.

3.6.3.2 Manage Categories

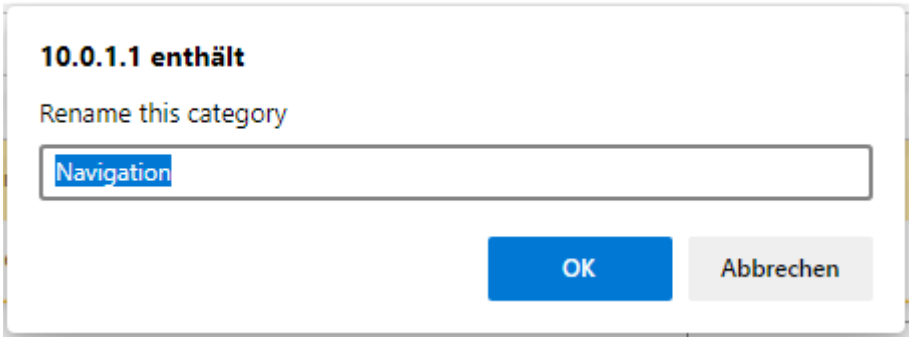
The Administrator or Captain can create new categories and edit or delete existing categories displayed in the local library.

To manage categories, click on the appropriate button at the bottom.



To rename a category:

- Click the pen icon
- Rename the category in the pop-up
- Click ‘Save’ or ‘Cancel’



Please note

Files stored in a category will be deleted.

To add a new category:

- Click the ‘+’ icon
- Type a name for this category in the pop-up
- Click ‘Save’, or ‘Cancel’

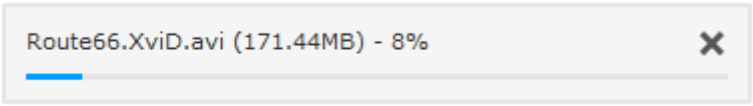
3.6.3.3 Manage Shared Files

The Administrator and Captain can upload new files and edit or delete shared files in the local library.

To upload new files:

- Click ‘New File’
- Select the category under which the new file is to be saved
- Click ‘Browse’ and navigate to the folder where the new file is stored on your computer
- Click ‘Open’ to start the upload

During the upload, the XChange displays a status bar showing the file name and size.



After the file is successfully uploaded, click ‘Back’ to return to the category display.

Please note

The maximum file size is 750 MB.

For security reasons, zipped “.tar” files are not supported and cannot be upload to the Library.

3.6.3.4 Edit and Delete Shared Files

To edit or delete a shared file, click on the line of the file and then:

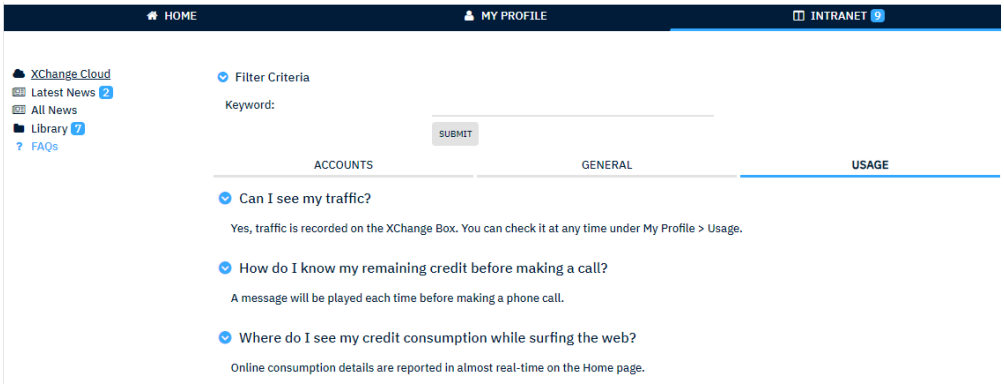
- Click ‘Edit’ to change the name
- Click ‘Delete’ to delete the file

Click ‘Back’ to return to the category display.

3.6.4 FAQs

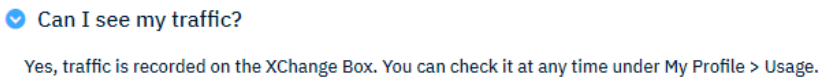
The FAQs (Frequently Asked Questions) enable self-support by providing answers to the most common questions from Users. The FAQ section can be managed remotely and is not only linked to XChange, but also to any other area of interest.

Through Portal360, shore Administrators can manage by adding categories, questions and answers for the FAQ.



The FAQ section is divided into categories, with a set of questions and answers for each category.

By clicking on a question, the panel opens and the corresponding answer is displayed below.



Please note

Only shore Managers accessing Portal360 can change shared content in the FAQs or Newsroom. Local Users can only view the FAQ section and cannot edit its content.

4. Devices (Connectivity)

4.1 Terminals (WAN)

Please only connect broadband terminals to the WAN (Wide Area Network) RJ-45 sockets of the XChange.

Please review Appendix B for a detailed list of controlled and supported connectivity services.

WARNING

Do not connect devices such as computers or network routers between the broadband terminals and the XChange. Any device which is connected to the terminal directly cannot be controlled and managed by XChange.
Marlink will not accept any claims for high traffic consumption if, for example, a device bypasses the XChange.

Please note

You will find a dedicated setup procedure for Furuno Felcom and JRC JUE FleetBroadband terminals in the Appendix section at the end of this document.

4.1.1 Broadband Device Prerequisites

Ensure that the broadband devices listed below are configured as indicated:

Controlled broadband devices (MSS)

FleetBroadband:

- The LAN port connected to the XChange is enabled
- Router mode is enabled
- Profile 'automatic activation' is disabled
- *PPPoE* is enabled
- The analogue voice port is set to 5.4 Hz only
- The IP handset is set to static IP mode using, for example, 192.168.0.20
  (IP range 192.168.0.1 to 192.168.0.19 are reserved for XChange)

Iridium Certus:

- The LAN port connected to the XChange is enabled
- The SIM card is on 'postpaid' mode and not 'prepaid'
- SIP accounts are created and set to proper lines
- Wifi is disabled

Autonomous broadband devices

- The LAN port connected to the XChange is enabled
- The DHCP service is either enabled or disabled depending on the WAN port settings during the XChange wizard initialisation process
- The autonomous terminal has the profile 'automatic activation' enabled to connect to the Internet automatically once within coverage

4.1.2 Controlled vs Autonomous Devices

Only broadband terminals with Marlink airtime are deemed to be ‘controlled’ devices.

XChange can ‘control’ the online status of controllable devices and to make use of the voice service (if available). The XChange turns the controllable device ‘online’ only when this is required to establish a data connection and it returns the device ‘offline’ again if there is no online connection required. This automatic action ensures cost-optimal usage while avoiding unnecessary traffic consumption, especially on typical MSS devices with smaller allowance plans.

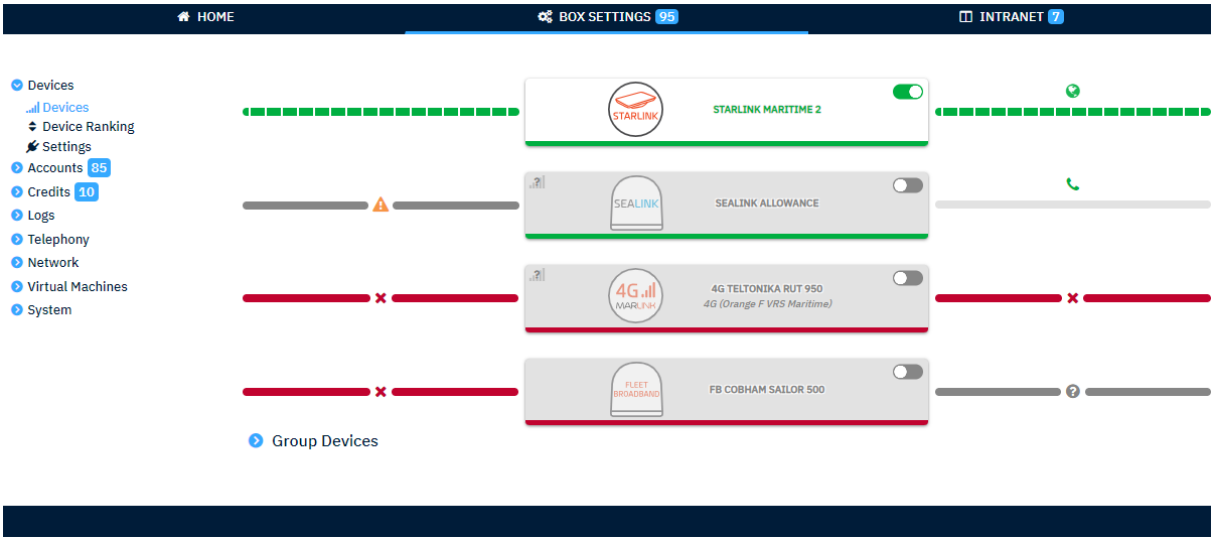
The same applies for voice calls. The XChange only supports the voice service which comes with the satellite device if that device is deemed to be a controlled device using Marlink airtime.

Autonomous devices are deemed to be ‘supported’ by XChange. XChange does not handle those terminals the same way as controlled devices. If an autonomous device offers voice service, then sometimes, due to non-Marlink airtime being used, or if the autonomous device uses another technology that prevents XChange from taking control, then it cannot be used through the XChange but can only be used with phone equipment directly connected to the device.

4.2 Devices Overview & Switching

To access the connections overview, go to: *BOX SETTINGS > Devices > Devices.*

The overview page provides information about all broadband terminal connections set up during the initialisation wizard process.



The ‘Overview’ provides information about the status of each broadband terminal.

A red cross indicates an error either on board (left side) or on the connectivity side (right side). Moving the mouse pointer above the red cross will display the error message.

All available communication devices that can be used for communication have a green bar below their names. Devices that are not available have a red bar below their name.

The communication device currently in use has a moving bar with light and dark green to show that communication is possible. Above the moving bar on the right side, icons show which type of communication is happening, for example ‘Data’ and/or ‘Voice traffic’.

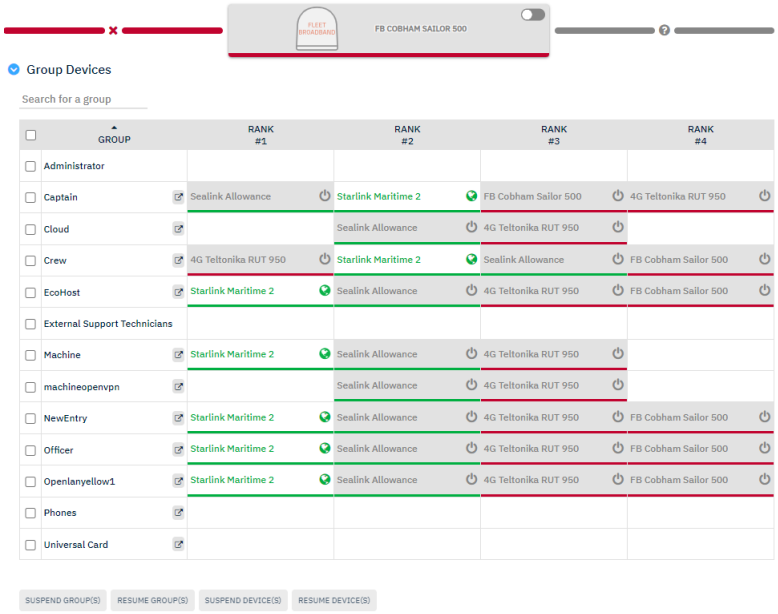
On the device overview all available user groups are shown. If many user groups are created, the list is extended. Above the user group overview, a search option simplifies finding the group in question.

Devices being ready to use, are shown in green followed by a green Globe-icon. This Globe-icon flashes if at least 1 user of a group is online via that device.

4.3 Multiple Device Routing

If your XChange is setup with Auto-Switch / SD-WAN Lite (aka Hybrid connectivity), the overview page provides the status which user group has which unique terminal ranking defined.

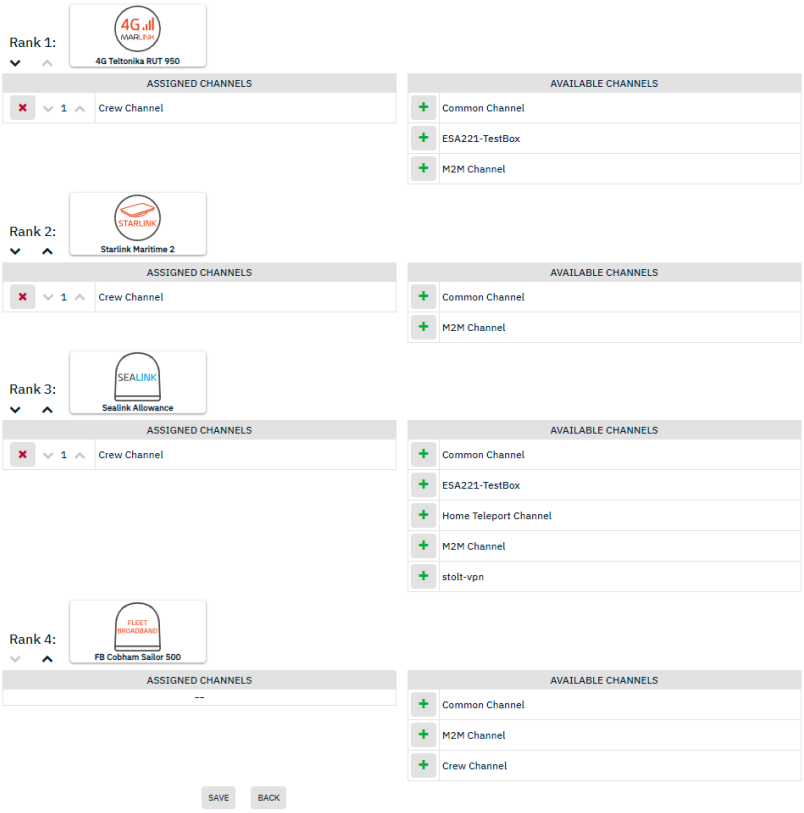
Only in this switching mode, the use of all online devices at the same time is possible.



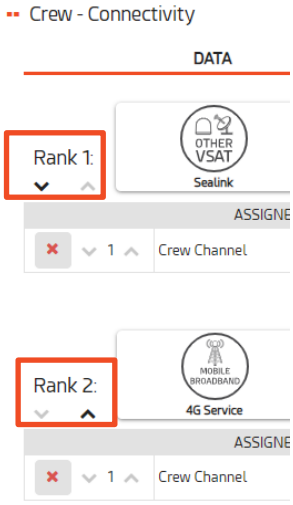
Based on the global device ranking, which is defined during installation, per default all user groups follow this general device ranking.

Only with SD-WAN Lite connectivity the device ranking can be re-defined at any time for each user group individually.

To change the default device ranking for a user group, click the  icon. The page refreshes and shows the communication channel assignment page for that user group.



To redefine the device priority, click on the arrows below the “Rank”.



With a single click the priority can be changed, or a device removed. The changes can be saved with clicking the ‘Save’ button.

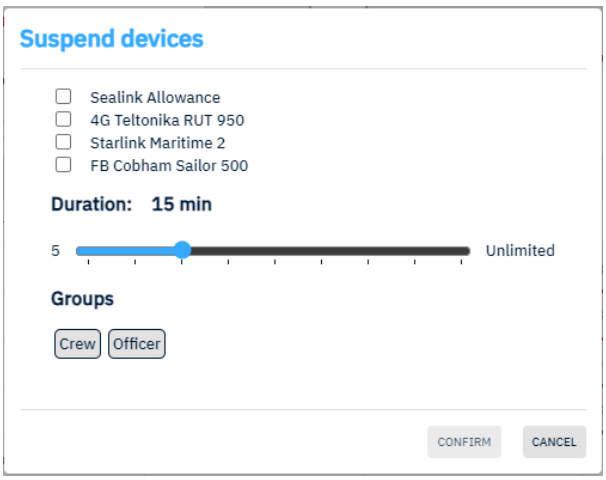
Further it is possible to change the available communication channels for that group. For more details please read the “User Administration” chapter.

Please note

After the device-priority is changed for a user group, users of that group will be rerouted to the new prioritised device as from next connection.

4.3.1 Device Suspension

To free up the bandwidth of a specific device, or to temporarily block specific user groups from using a specific device select the user group(s) and click ‘Suspend Device(s)’:



Either one, or all available device of the selected user groups can be suspended. The duration slider offers multiple time options from 5 minutes to ‘Unlimited’.

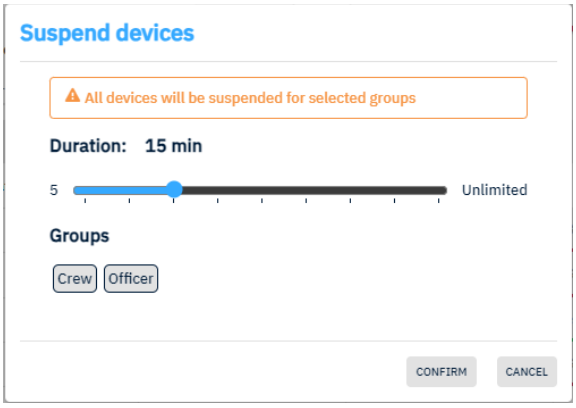
To confirm the device suspension, select the devices, set the suspension time and click ‘Confirm’.

After confirmation, the suspension-timer shows the remaining time before this device will be released automatically.

The set suspension can be removed at any time, by selecting the user groups and clicking the “Resume Device(s)” button.

4.3.2 User group Suspension

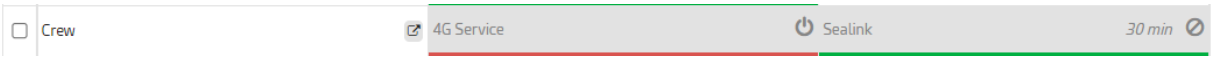
Instead of suspending single communication devices for user group(s), entire user group(s) can be suspended from any online access for a given period of time.
To suspend whole user groups from all devices, select these groups and click on ‘Suspend Group(s)’.



The duration slider offers multiple time options from 5 minutes to ‘Unlimited’.

To confirm the group suspension, set the suspension time and click ‘Confirm’.

After confirmation, the suspension-timer shows the remaining time before this device will be released automatically.

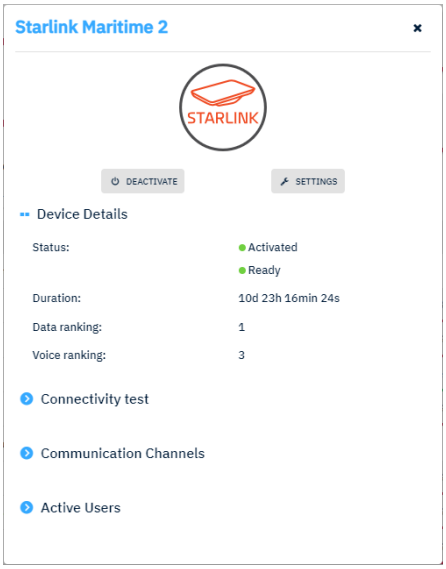


The set suspension can be removed at any time, by selecting the user groups and clicking the “Resume Group(s)” button.

4.4 Device Details

Clicking on one of the device icons brings up a small pop-up window giving more detailed information about the device, connection status, available communication channel and currently active User.

In the details window, the Administrator or Captain can activate/deactivate a device or access the detailed settings page.



If there is an error, then an error message is shown in red below the device icon.

Within ‘Connectivity Test’ (click to expand), you can view the activation status of the connectivity test, its detailed settings and the current status.

The ‘Current Status’ shows the amount of consecutively sent pings since the last status change. Once a terminal changes from ‘online’ to ‘offline’, the counter is reset to 0 (zero).

While the connectivity test is happening, the ping counter counts each successful ping until the defined threshold is met. Once the threshold is met, the device is indicated as online again.

Within ‘Communication Channels’ (click to expand), you can view status information about each channel that has been set up. Activation and connection status are displayed separately for each communication channel.

Within ‘Active Users’ (click to expand), you can see all users communicating through that device at the moment you´re watching.

☝ The number of communication channels displayed varies according to the broadband terminal and the individual setup.

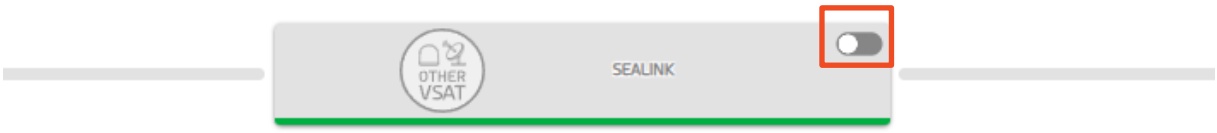
4.5 Manual Device Switching

The XChange makes it possible to switch manually from one terminal to another. The Captain or Administrator can activate or deactivate one of the configured broadband devices. All data, voice and VoIP communications are carried out for the activated device.

While switching off the device, all traffic to the device will be blocked and, for controlled devices, all online connections will be terminated at the same time.

4.5.1 Activate a Terminal

To activate a terminal, go to *BOX SETTINGS > Devices* and click once on the 'On/Off' button next to the name of the device as shown below.



Confirm in the pop-up window that this terminal should be activated. The previously grey bars on the left and right side turn dark green and once a User or automatic system starts to communicate with the Internet, the bars start to move in light and dark green again.

If the XChange is set to "Manual Switch" as the only switching method, the previously activated terminal, will be automatically deactivated after confirmation and the active data and voice session will be disconnected without sending a warning message to the User who is connected.

4.5.2 Deactivate a Terminal

To deactivate a terminal, follow the same process described above.

All active data and VoIP sessions will be disconnected immediately, and, for controlled devices, all active IP sessions will be terminated.

4.6 Semi-Automatic Device Switching (VSAT Fall-Back)

The XChange allows semi-automatic device switching from the backup to the default device. The semi-automatic device switch is preconfigured by Marlink and needs no additional manual action.

The manual device switch for Captain and Administrator remains available with a limited time of use.

In case the default device goes offline, the Captain has to switch on the backup device to continue communications.

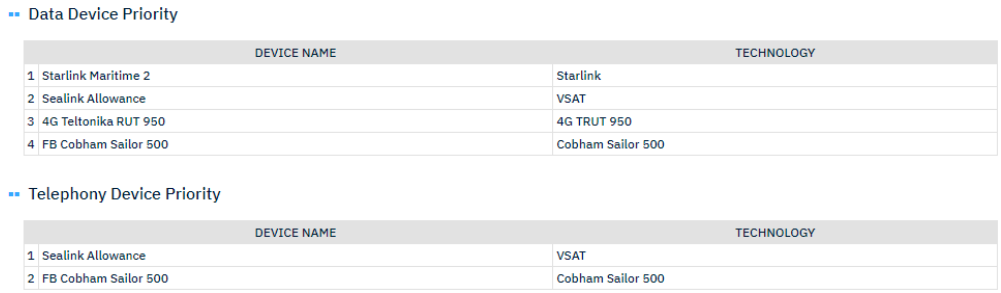
The XChange periodically checks the availability and stability of the default device in the background. When the default connection is ready and stabilised again, the connection will be switched automatically back to the default device.

Please note

If a backup device is manually enabled, then although the main device is considered as 'online', the maximum use time should be limited avoiding unnecessary use of the backup.

4.6.1 Determine a Default Device

To check the default device, go to: *BOX SETTINGS > Devices > Device Ranking.*



Data Device Priority

	DEVICE NAME	TECHNOLOGY
1	Starlink Maritime 2	Starlink
2	Sealink Allowance	VSAT
3	4G Teltonika RUT 950	4G TRUT 950
4	FB Cobham Sailor 500	Cobham Sailor 500

Telephony Device Priority

	DEVICE NAME	TECHNOLOGY
1	Sealink Allowance	VSAT
2	FB Cobham Sailor 500	Cobham Sailor 500

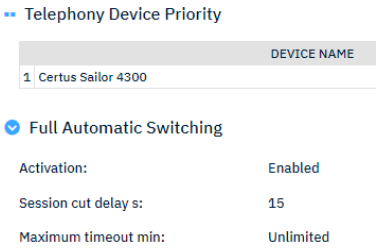
The overview shows which communication device is the default device for data and voice separately. The priority may differ for data and voice communication.

Please note

Only Marlink can determine the default device. Marlink's Sealink VSAT is the default main device in most cases.

4.6.2 Backup Device Timeout

For the semi-automatic and fully automatic device switching options, an automatic backup device timeout is predefined by Marlink.

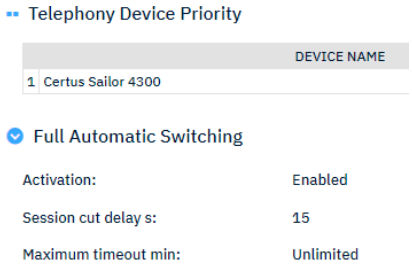


To check the maximum timeout, in minutes, please check the ‘Full Automatic Switching’ or ‘Semi-Automatic Switching’ panel below the device priority.

The default maximum timeout is set to 30 minutes. This setting can only be changed by Marlink super Administrators if an exception is part of the contract.

4.6.3 Automatic Device Switching / SD-WAN Lite

To see the automatic device switching settings, go to *BOX SETTINGS > Devices > Device Ranking*.



The general device switching settings can be checked here. The switching can be either enabled or disabled. If this feature is set on disabled, then automatic device switching will not be available.

The session cut delay (in seconds) is preset to 15 seconds. When the default device is online and stabilised again, the system will wait 15 seconds before cutting active sessions during device switching.

Please note

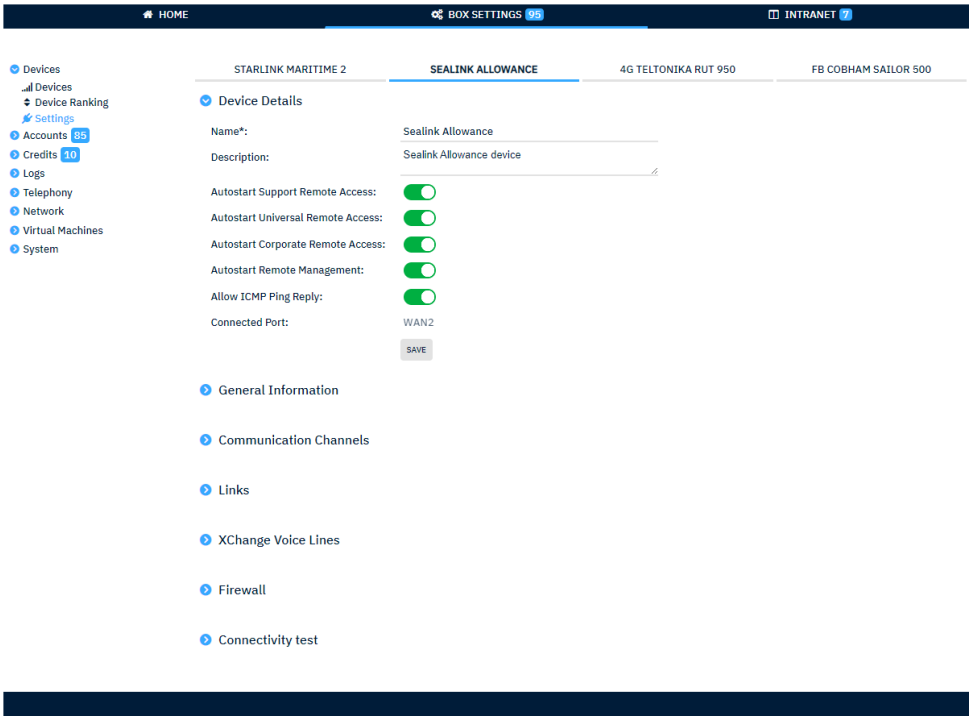
Only Marlink can change the activation status for the device switching.

Please note

Automatic device switching is performed only on change of default device status. If device switching is performed manually while the default device is online, the system will not switch back to the default device after the timeout function counts to 0 (zero).

4.7 Device Management

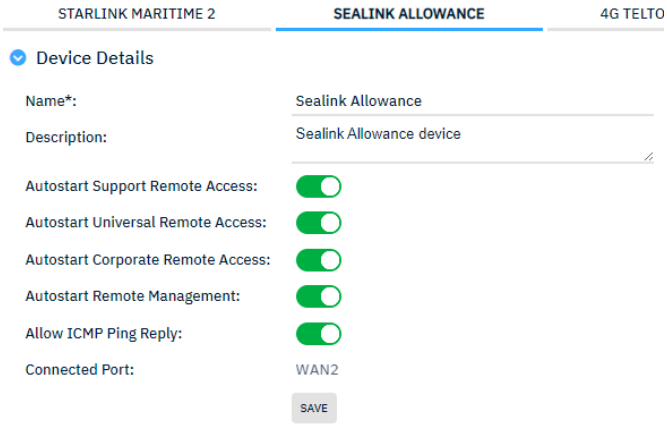
To change the details on connected devices and manage communication channels and firewall filters go to: *BOX SETTINGS > Devices.*



Each connected device is separated by a weblet. To switch views from one device to another, click on the appropriate weblet.

4.7.1 Device Details

You can change the details of the connected device directly and click ‘Save’ to store the changes.



The name and description are free-text fields and can be edited via the web interface. The ‘Port’ and ‘Tunnelling Ability’ cannot be edited. To change the port connection and tunnelling settings, use the initialisation wizard again.

The ‘Serial Number’ and ‘DID’ of the controlled device are retrieved by the XChange for display here.

4.7.1.1 Services Auto-start

When you wish to access the XChange, a terminal or the local network remotely, without contacting staff on board, you should enable automatic start of remote access for each terminal separately.

Simply tick a check box to enable ‘Support Remote Access’, ‘Corporate Remote Access’ or ‘Universal Remote Access’ to be automatically available when a terminal is enabled.

Please note

When an auto-start option is selected on a controlled MSS device, the XChange opens a separate Public IP session automatically. When using a FleetBroadband 150 terminal, each User group that is allowed to make data communication needs to have the same ‘Remote Access’ communication channel available.

WARNING

The ‘Support Remote Access’, ‘Remote Management’ and ‘Universal Remote Access’ option are enabled by default for connected Marlink devices and shall be kept enabled at any time to guarantee a seamless support access for Marlink support teams.

4.7.2 Communication Channels

Through 'Communication Channels', the XChange manages the multiple 'PDP Contexts' available over Inmarsat FleetBroadband and multiple 'VLANs' available on Sealink VSATs. Specific settings can be defined for each communication channel including: prioritisation on VSAT, public vs dynamic IP addressing on FleetBroadband and embedded VPN settings.

To manage the communication channels for a connected device, click the 'Communication Channels' collapsed panel. The following list of communication channels are predefined and activated by default (they are terminal-dependent):

	DESCRIPTION	SEALINK	CONTROLLED DEVICES	SUPPORTED DEVICES
Cloud Channel	Used for XChange Cloud content transmissions	√	√	√
Common Channel	Opens a background IP connection. Mainly used for corporate traffic	√	√	√
Crew Channel	Opens a background IP connection. Mainly used for Crew traffic	√	√	
Remote Access	Opens a Public IP connection		√	
Home Teleport	VSAT connection to Marlink home Teleport	√		
M2M Channel	Opens a background IP connection. Mainly used for machine traffic	√	√	
Media Multicast	Not used	√		
Media Unicast	Not used	√	√	
Native VLAN	Used for VSAT administration	√		
Remote Management Channel	Opens a connection to Portal360 to enable shore-based administration access	√	√	√
Universal Remote Access	Opens a connection to XChange URA Server	√	√	√
System Channel	Used for synchronisation with XChange server		√	
XChange Voice Channel	Used for VSAT Voice calling	√	√	

Using the communication channel management, Users can raise or lower the number of available communication channels for each terminal and set separate IP addresses.

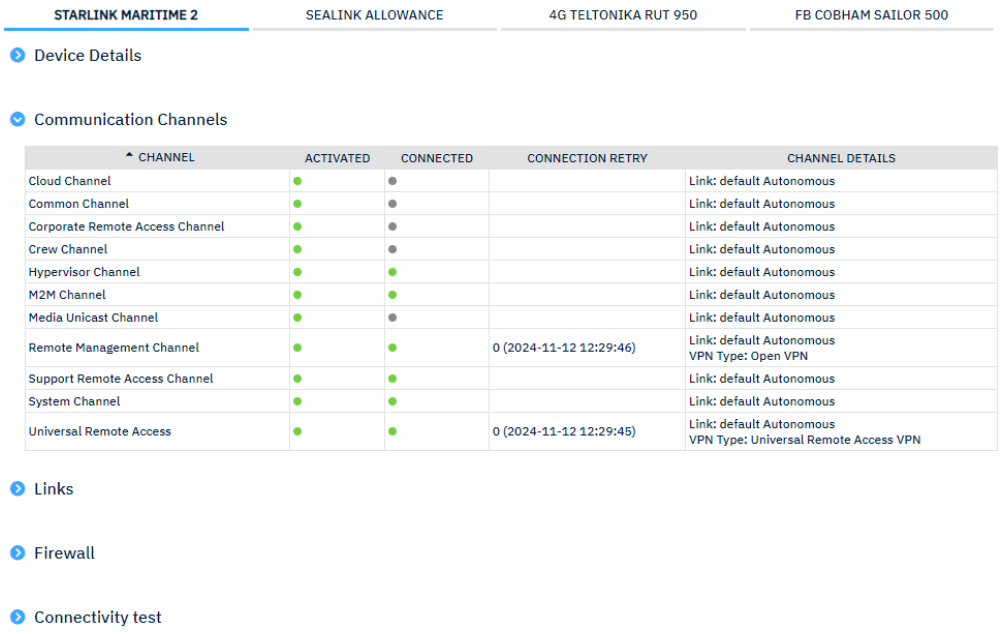
Communication channels are linked to User groups. User groups are only allowed to launch data sessions using one of the linked communication channels and the stored options for the channel. One communication channel can be linked to several User groups at the same time.

Please note

The XChange File Cloud channel is not activated on other communication devices than Sealink. If XChange File Cloud transmissions should be allowed through a MSS- or alternative device, the Cloud Channel must be activated by the administrator.

4.7.3 Communication Channel Overview

To view the communication channels for each device, go to *BOX SETTINGS > Devices > Settings*.



CHANNEL	ACTIVATED	CONNECTED	CONNECTION RETRY	CHANNEL DETAILS
Cloud Channel	●	●		Link: default Autonomous
Common Channel	●	●		Link: default Autonomous
Corporate Remote Access Channel	●	●		Link: default Autonomous
Crew Channel	●	●		Link: default Autonomous
Hypervisor Channel	●	●		Link: default Autonomous
M2M Channel	●	●		Link: default Autonomous
Media Unicast Channel	●	●		Link: default Autonomous
Remote Management Channel	●	●	0 (2024-11-12 12:29:46)	Link: default Autonomous VPN Type: Open VPN
Support Remote Access Channel	●	●		Link: default Autonomous
System Channel	●	●		Link: default Autonomous
Universal Remote Access	●	●	0 (2024-11-12 12:29:45)	Link: default Autonomous VPN Type: Universal Remote Access VPN

If the configuration details need to be adjusted for one or more communication channels, the Marlink superadmin can either create a new or adapt an existing communication channel.

4.7.4 Create a New Link

To create a new communication link, click on 'New' under the list of available links of the desired device and follow the steps:


Communication Channels

CHANNEL	ACTIVATED	CONNECTED	CONNECTION RETRY	CHANNEL DETAILS
Cloud Channel				Link: Low priority VLAN: 56 / 6
Common Channel				Link: Medium priority VLAN: 55 / 5
Corporate Remote Access Channel				Link: Home Teleport VLAN: 54 / 4
Crew Channel				Link: Low priority VLAN: 56 / 6
Home Teleport Channel				Link: Home Teleport VLAN: 54 / 4
Hypervisor Channel				Link: High priority VLAN: 53 / 3
M2M Channel				Link: High priority VLAN: 53 / 3
Media Unicast Channel				Link: Low priority VLAN: 56 / 6
Remote Management Channel			0 (2024-10-23 12:30:02)	Link: Very High priority VLAN: 52 / 2 VPN Type: Open VPN
Support Remote Access Channel				Link: Native VLAN VLAN: -1 / 0
System Channel				Link: Medium priority VLAN: 55 / 5
Universal Remote Access			0 (2024-10-23 12:30:02)	Link: Very High priority VLAN: 52 / 2 VPN Type: Universal Remote Access VPN
vpn				Link: High priority VLAN: 53 / 3 VPN Type: Open VPN
XChange Voice Channel				Link: Marlink Voice VLAN: 51 / 1

NEW

- Define a link name
- Select the disconnection mode
  - Auto-disconnect: disconnects after defined timeout
  - No disconnection: remains always online
- MSS devices:
  - Select one of the predefined Marlink (Marlink) APNs (MSS only)
  - Set a service name. Otherwise, the SIM card default service will be used
    - Set 'public.dynamic' as the service name to receive a Public IP address for the data session
- VSAT:
  - Name the VLAN which should be used with that link
  - Set the subnet in CIDR
  - Set the allocation mode (DHCP/Static)
    - If static, please put all required IP details for the XChange device

Click 'Save' to store your changes.

WARNING

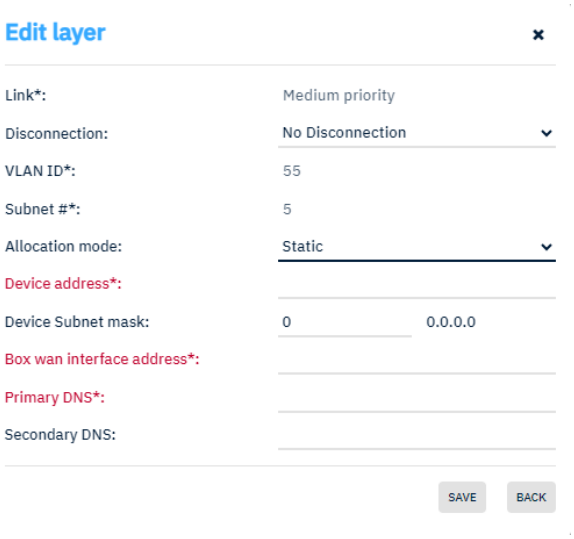
Only Marlink Technicians are allowed to define new device links. The defaults stored on the XChange system cover all communications needs. A new link is only required for heavily customised communication setups and contracts.

Please note

New links only need to be created if the Sealink VSAT has additional communication VLANs which are not part of Marlink's default set of VLANs.

4.7.5 Edit a Link

To edit a communication link, mark the link in question and click on ‘Edit’. A new pop-up window appears:



The disconnection method and IP allocation mode can be changed.

Disconnection methods

By default, the disconnection is disabled. This means that this communication channel is always available for that device whether it is used or not.

‘Disconnection’ can be set to ‘Auto-Disconnect’ which will create a new line asking how many seconds this link should be kept open for before it is disconnected. Once the last User or system stops using a link with enabled auto-disconnection, the counter starts to count up to the set number of seconds. If no User or system requires this channel for data communication within this time, then it will be disconnected automatically.

Allocation mode

The IP allocation mode is normally defined by the Installer through the installation wizard, but the IP allocation mode and IP details can be changed here if they need to be adjusted.

Once the settings have been changed, click ‘Save’ to store the changes.

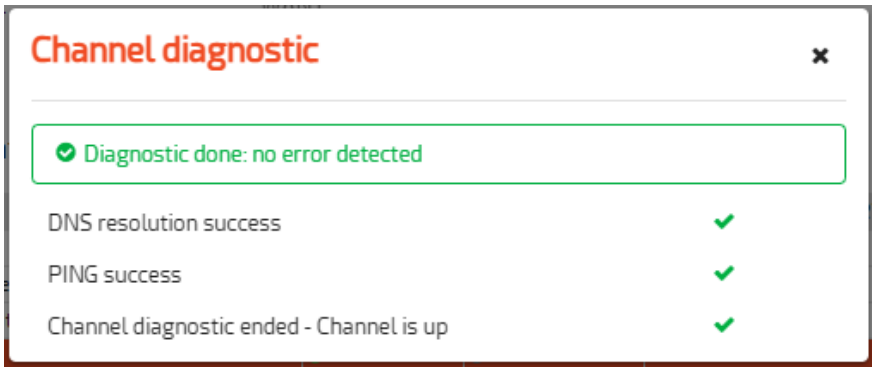
4.7.5.1 Communication Channel Diagnostics

In case one or more communication channels on Sealink VSAT do not work correctly, for example, if the Crew cannot access the Internet through the 'Crew Channel', then supporting personnel can diagnose each communication channel separately.

The diagnosis shows whether communication through this specific channel is possible or not. The test itself uses standard pings and DNS resolution to validate the channel availability.

To start the diagnosis, simply select a channel and click 'DIAGNOSE' below the list:

A new pop-up window appears, giving real-time information about the connectivity status of the tested communication channel:



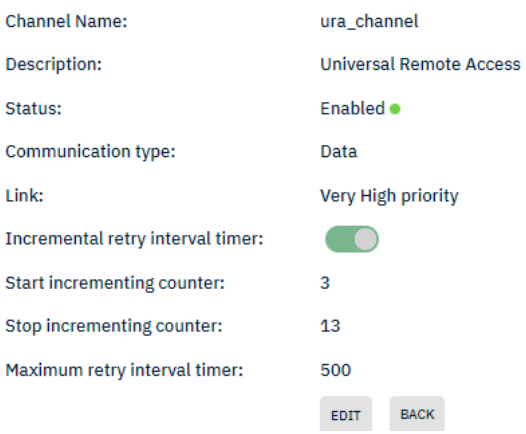
Please note

This channel diagnostic is not counted by XChange traffic logs, but still uses a small amount of data and bandwidth. Therefore, Marlink recommends that the diagnostics are only used for troubleshooting on request. This diagnostic cannot be proceeded remotely.

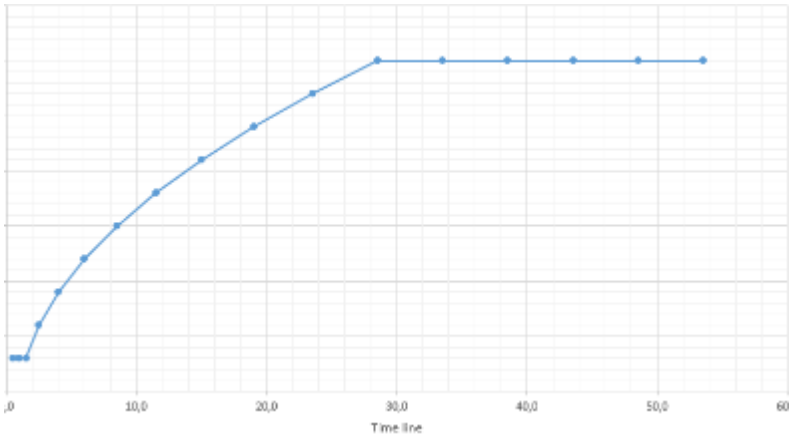
4.7.5.2 XChange URA Retry Mechanism

The XChange ‘Universal Remote Access’ (URA) channel tries automatically to connect to the shore servers. In some cases, the ‘URA channel’ may not be able to connect to the servers. To prevent the automatic retry mechanism from consuming a large amount of data traffic while retrying every few seconds, an incremental retry timer is enabled.

The default retry period for the XChange URA service is 30 seconds. If, after 3 attempts, the connection cannot be established, then the timer adds another 13 seconds to the delay for the next attempt. The increment timer adds another 13 seconds to the waiting period for each new attempt, until the preset maximum of 500 seconds between 2 connection attempts is reached.



This diagram visualises the subsequent retry delays over time:

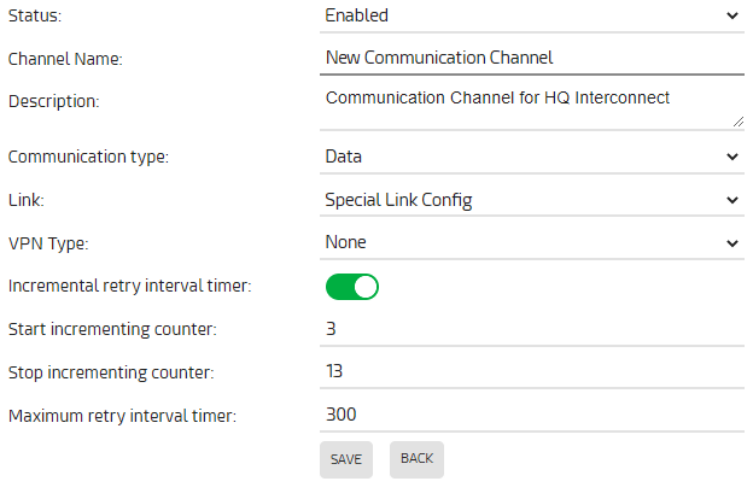


This incremental retry mechanism can be enabled for other communication channels if desired. To enable the incremental retry mechanism, ‘Edit’ the communication channel.

4.7.5.3 Create a New Communication Channel

In random cases and a more specialised setups, it is may required to create additional communication channel. Typically only required, if extra Links were created before, or if the XChange Interconnect service is ordered. To create a new communication channel:

- Go to the device
- Expand the 'Communication Channels' panel
- Click 'New'
- Define a channel name (no spaces or special characters)
- Define a description (this will appear on User home pages)
- Select the communication type
- Select a link (default or previously self created)
- Select a VPN type
- Optional: Set up the incremental retry mechanism (VSAT only)



Please note

The newly created communication channel is not associated to any User group. An association must be made at the User group level. Only Marlink technical staff has administrative access rights to edit or create communication channels.

4.7.5.4 Edit/Delete a Communication Channel

To edit a communication channel, click on the name of the channel. Click 'Edit' to change the channel parameters or to deactivate the channel. Click 'Delete' to delete a channel that you have created.

☝ You can only delete communication channels that you have created yourself. The predefined channels continue to exist but can be disabled if they are not linked to a User group.

4.7.6 VPN

The embedded VPN client supports connection to shore-based 'Open VPN' and 'GRE VPN' servers. The VPN client can be enabled and set up for any communication channel and broadband terminal individually.

This provides fully flexible configuration capabilities. It is possible to link the whole vessel data communication to the onshore VPN server, or just one User group such as machines or corporate traffic.

The VPN channel can be defined as one-way (XChange > shore) or two-way (XChange <> shore) communication.

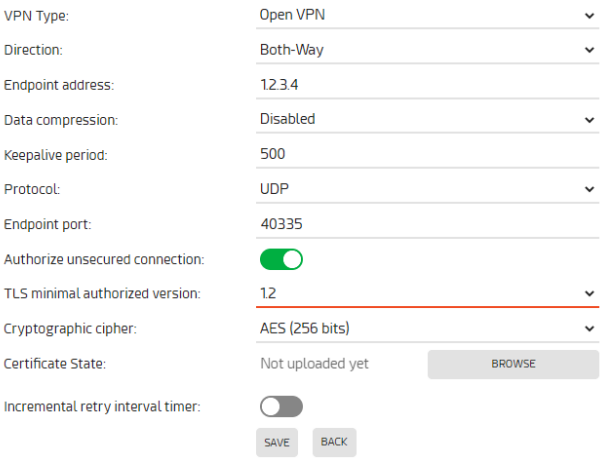
The two-way option provides remote access to on-board network clients linked to the VPN channel.

4.7.6.1 Create a VPN Connection

To create a VPN channel, follow the same process as for communication channel creation described above, and select the VPN type of your choice.

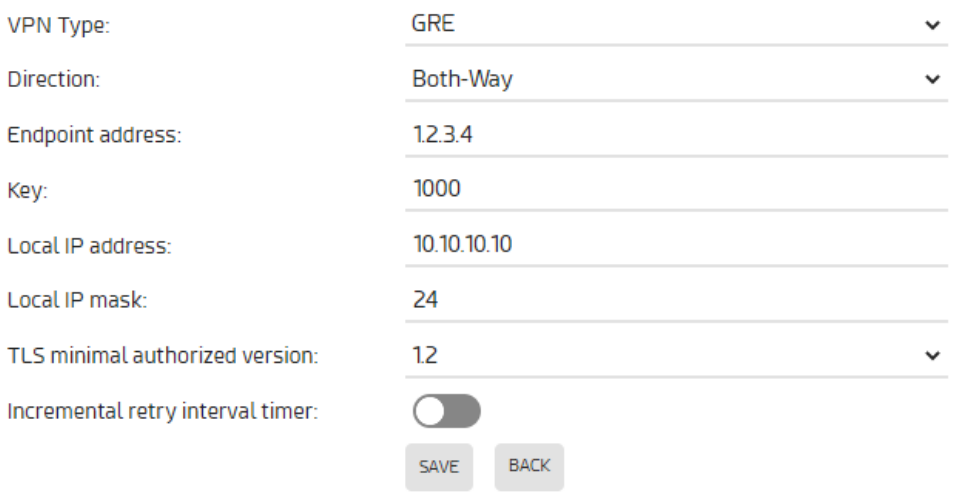
4.7.6.2 Set Up Open VPN Connection

- Set the VPN type to 'Open VPN'
- Set the direction 'One-Way' or 'Both-Way'
- Set the endpoint IP address of the shore-based VPN server
    - The server on shore should always have a public static IP address to be accessible
- Select a data compression mode
- Set the keep-alive period in seconds (how long should the VPN remain on if no traffic passes)
- Set the Protocol (TCP vs UDP)
- Set the endpoint port
- Optionally allow authorisation of unsecured connections (Not recommended)
    - Select the minimal authorised TLS version
- Select one cryptographic cipher
    - Blowfish 128 bit
    - AES 128 bit / AES 256 bit
    - Triple DES 192 bit
    - None (Not recommended)
- Upload the certificate file
    - The certificate file must be created by the VPN server in advance
- Click 'SAVE'



4.7.6.3 Set Up GRE VPN Connection

- Set the VPN type to ‘GRE’
- Set the direction ‘One-Way’ or ‘Both-Way’
- Set the endpoint IP address of the shore-based VPN server
- Enter the shared secret key
- Enter the local IP address
- Enter the local IP mask in CIDR
- Select the minimal authorised TLS version
- Click ‘SAVE’



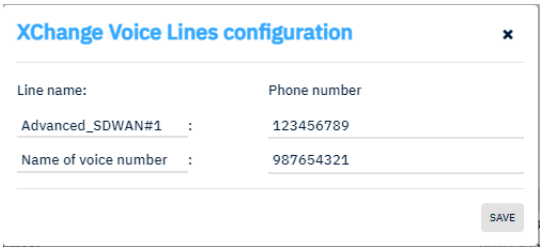
Please note

Once your VPN channel is created, you need to assign it to one of the User groups to be able to use it.

4.7.7 Adapt Voice Line Numbers

If there is an incorrect number entered during the installation wizard, only the superadmin can change the phone numbers for each voice line without the need to restart the installation wizard.

To change the voice line numbers, expand the panel ‘XChange Voice Lines’ and click ‘Edit’:



The line name and line number can be changed. Once the changes are entered, click ‘SAVE’ to store the changes. Please note that no additional voice line can be added here: to add or remove voice lines you need to restart the installation wizard.

Please note

The voice line adjustment works for all devices that provide voice services. This function is very useful during fleet-wide roll-out projects. If an XChange is configured with a backup file created on another XChange, then the individual device details can be changed without the need to restart the wizard.

4.7.8 Firewall

For each terminal connected, the Administrator can apply a different set of firewall filtering rules.

Firewall

POSITION	NAME	DESCRIPTION
1	Web	Allows web surfing (HTTP&HTTPS)
2	SkyFile Mail	Allows SkyFile Mail traffic

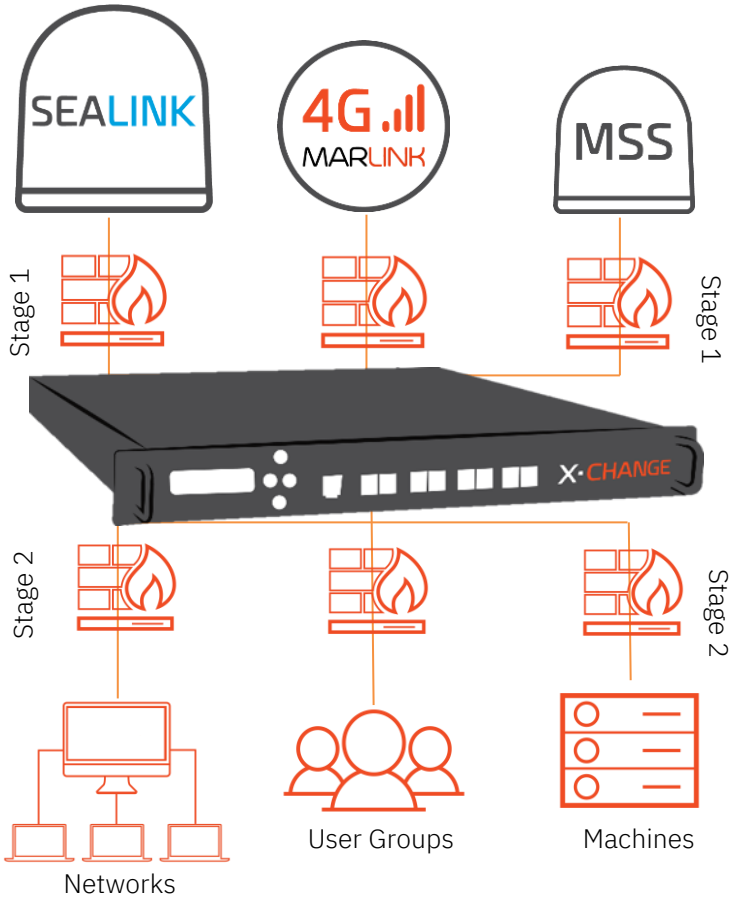
EDIT

Firewall filtering settings at the terminal level are the 1st stage of the XChange's integrated Firewall.

At this stage, you can set a first level of pre-filtering to allow traffic that should usually go through the terminal. This will block any type of traffic and ports not covered by a special firewall filter.

By default, there is no special firewall filtering and any kind of traffic is allowed through. It is recommended that you change the default setup and define the specific types of traffic to be allowed.

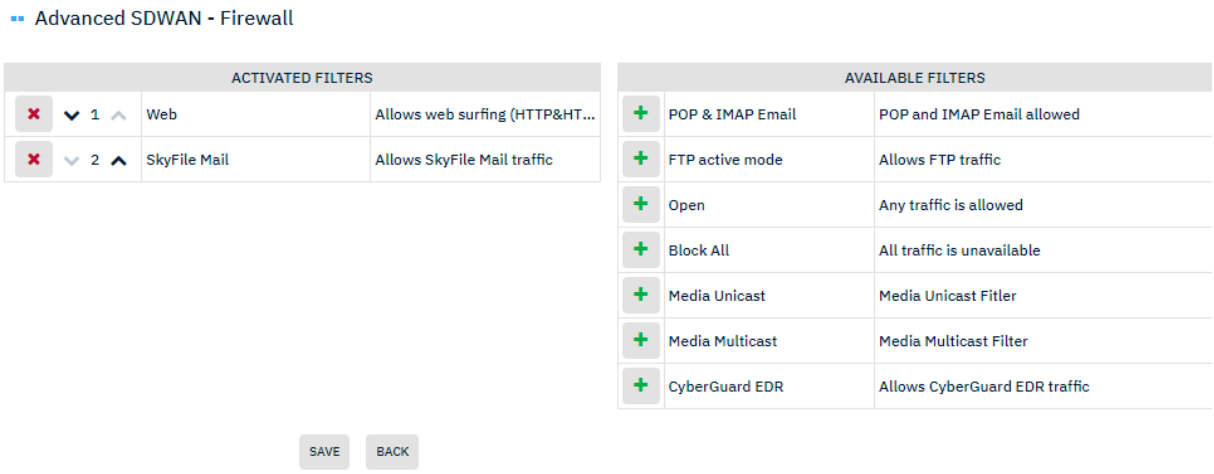
The drawing below indicates the 2-stage architecture of the XChange firewall:



4.7.8.1 Set Up Firewall Rules

To define the setting of a firewall filter for a given terminal:

- Go to the terminal
- Expand the 'Firewall' panel
- Click 'Edit'
- To activate a filter, click the green '+' from the list of available filters
- To remove an unwanted filter, click the red '-'
- To change firewall check sequence, click the arrows of an activated filter to define another check priority
- Click 'Save'



WARNING

Marlink does not recommend the use of the 'Block All' firewall filter at the device level. Please bear in mind that XChange may use the backup device for mandatory synchronisation and to support remote access, which consumes data volume.

4.7.9 Device Access

The broadband 'Device Access' dashboard enables device access to be opened or closed individually for each device. Opening device access allows the Administrator to access e.g. the terminal modem dashboard via any local network computer connected to the XChange local network.

To enable the device access simply expand the 'Device Access' collapsible panel and click 'Open device access'.

☝ Only the Administrator can access the device dashboard.

4.7.9.1 Access Device Dashboard

Controlled device

The FleetBroadband device dashboard can be accessed by clicking on 'Access device administration page'. A new browser tab opens displaying the device dashboard.

Autonomous device

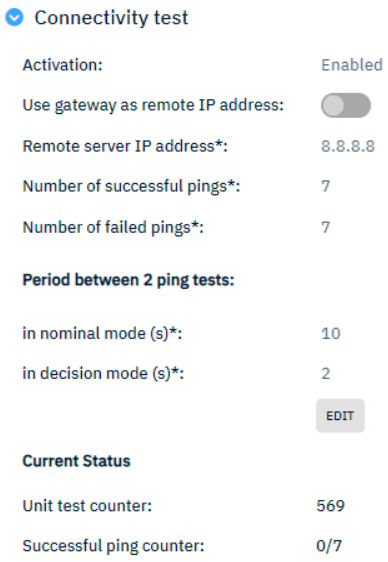
To access an autonomous device dashboard, open a new browser tab and type the device's IP address manually in the address bar or used dedicated software.

4.7.10 Connectivity Test

For all communication devices, a 'Connectivity Tester' automatically tests the online status.

The XChange tests the online connectivity periodically by pinging a defined onshore server. If the device is online, then this test will be performed every 10 seconds. If the set threshold of failed pings is reached, then the XChange defines the connection as offline and raises an alert on the Captain's dashboard.

For a device with status offline, the connectivity test will be performed every 10 seconds. When the set threshold of successful pings is reached, then the XChange recognises the connection as online and stabilises again.



The test settings can be changed by the Administrator by clicking on 'Edit'.

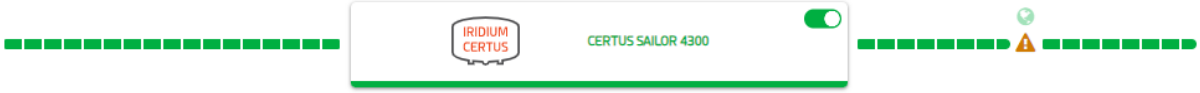
The remote IP address which should be pinged can be changed or the function itself can be switched off. The 'Status' counts all previous connectivity test pings and the number of unsuccessful pings.

WARNING

Marlink does not recommend the use of the 'Block All' firewall filter at the device level. As mandatory firewalling, in case no other communication should be available on the backup device please allow XChange required data traffic on shore-based firewalls as well to avoid that the connectivity tester is blocked.
If it is blocked, a huge number of pings can cause a high data traffic consumption.

4.7.10.1 Connectivity Test on Iridium

On Iridium devices, the connectivity test is setup differently. For Iridium devices, the tester checks if a valid connection between the XChange and the device is established. It does not test the data connection status.



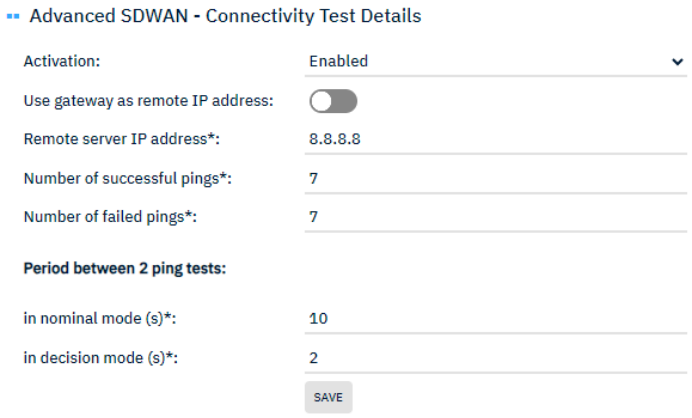
A warning message displayed with the yellow icon says: "Ready to use, if Iridium network is available"

4.7.10.2 Edit the connectivity tester

By clicking on ‘Edit’, it´s possible to change the connectivity tester parameter or to disable it completely.

If a faster online-status change is preferred, the number of pings can be reduced to 1.

If a more reliable online-status change is preferred, the number of can be increased to 20.



WARNING

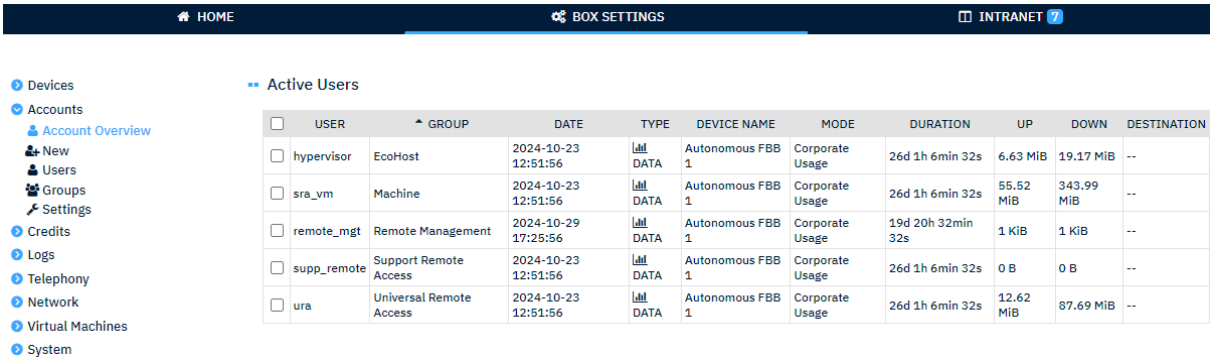
Marlink does not recommend the use very low numbers of pings. If the amount of pings is to small, the online status of a device may changes very often which can turn into an inconvenient situation.
Each time the XChange changes the connection, all communication going through the ‘offline’ device will be cut to reinitialise the communication on the next terminal.

5. User Account Management

The integrated User Account Management provides management capabilities for a single User or a User group. It enables the Captain and Administrator to manage User credits (local prepaid), User group firewalling, and general access restrictions for specific User groups. A real-time cost control and monitoring are other important management capabilities that are provided.

5.1 Overview

The ‘Accounts’ ‘Overview’ page provides a summary overview of active user connections.



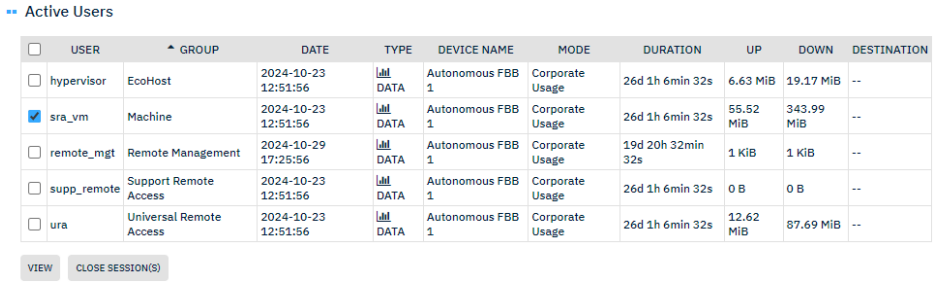
USER	GROUP	DATE	TYPE	DEVICE NAME	MODE	DURATION	UP	DOWN	DESTINATION
hypervisor	EcoHost	2024-10-23 12:51:56	DATA	Autonomous FBB 1	Corporate Usage	26d 1h 6min 32s	6.63 MiB	19.17 MiB	--
sra_vm	Machine	2024-10-23 12:51:56	DATA	Autonomous FBB 1	Corporate Usage	26d 1h 6min 32s	55.52 MiB	343.99 MiB	--
remote_mgt	Remote Management	2024-10-29 17:25:56	DATA	Autonomous FBB 1	Corporate Usage	19d 20h 32min 32s	1 KiB	1 KiB	--
supp_remote	Support Remote Access	2024-10-23 12:51:56	DATA	Autonomous FBB 1	Corporate Usage	26d 1h 6min 32s	0 B	0 B	--
ura	Universal Remote Access	2024-10-23 12:51:56	DATA	Autonomous FBB 1	Corporate Usage	26d 1h 6min 32s	12.62 MiB	87.69 MiB	--

The table displays all active user accounts and gives additional information about each connection:

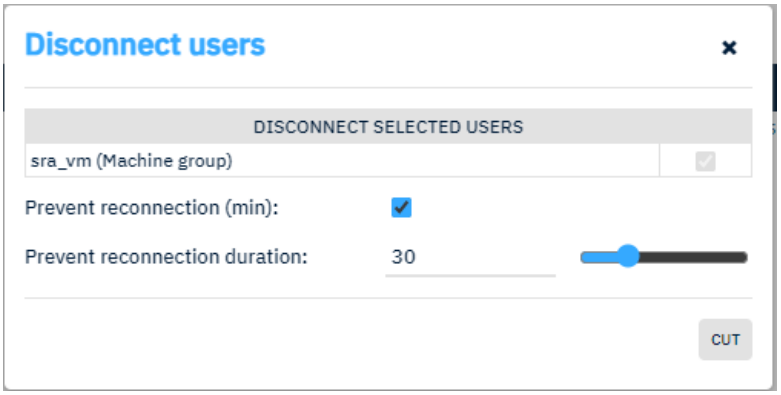
- Username
- Group
- Session initialisation date and time
- Traffic type
- Device used
- Payment mode
- Duration of the active connections
- Up/Down traffic consumption
- Destination (for voice and VoIP calls)

5.1.1 Disconnect Active Connections

By selecting one or multiple users additional action buttons appear offering to view this user specific details or to disconnect this active connection:



To close an active connection, click the ‘Close Session(s)’ button. A new window appears offering additional parameter to chose from.



Same as disconnection active users from the Captain´s dashboard, it is optionally possible to prevent a reconnection for a limited period of time. A timer can be set either by moving the slider, or by typing the time in minutes directly.
The minimum duration is 5 minutes and the maximum duration is 120 minutes.
With a click on the ‘Cut’ button, the selected connections will be disconnected.

5.2 Manage User Groups

To access the User group management feature, go to: *BOX SETTINGS > Accounts > Groups*.

With group management, you can create, manage and delete User groups. It is mandatory to work with User groups in XChange. Every single User must be linked to a specific User group, as User management is based on managing groups. By reducing the management effort to a minimum, the system becomes more user-friendly and at the same time ensures there are no 'uncontrolled' Users.

GROUP NAME	DESCRIPTION	GROUP TYPE	ACCOUNTING MODE	CONNECTIVITY
Administrator	Default group for local administrators	LocalAdmin	None	
Captain	Captain and managing personnel lan1 lan2	Master	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Cloud	Cloud synchro group	Interruptible System	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Cloud Application	Group for cloud applicatons	Application-Type	None	
Corporate Remote Access	Remote Access dedicated to corporate administrator	System	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Crew	Crew members lan1 lan2	User	Local Allowance	Advanced SDWAN Autonomous FBB 1
EcoHost	Group machine for hypervisor's connectivity	SingleMachine	Corporate Usage	Advanced SDWAN Autonomous FBB 1
External Support Technicians	Group for external support technicians	Ext Support Tech	None	
Machine	Machines and electronic instruments using data connections lan1 lan2	Machine	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Marlink service experts	Default group for Marlink service experts	Service Experts	None	
Media Multicast	Multicast Group	System	Corporate Usage	
Media Unicast	Unicast Group	System	Corporate Usage	
NewEntry	All self-registered accounts before they get assigned to a user group lan1 lan2	Self-Registered User	Local Allowance	Advanced SDWAN Autonomous FBB 1
Officer	Officer and Bridge staff lan1 lan2	User	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Phones	Configured phone handsets	Phone	Corporate Usage	Advanced SDWAN
Remote Management	Provides connectivity for remote management from shore	System	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Service Technicians	Default group for service technicians	Service Technicians	None	
Support Remote Access	Remote Access dedicated to Customer care access only	System	Corporate Usage	Advanced SDWAN Autonomous FBB 1
System	System tasks using data connections	System	Corporate Usage	Advanced SDWAN Autonomous FBB 1
Universal Card	Universal card users lan1 lan2	User	Universal Card Usage	Advanced SDWAN
Universal Remote Access	Universal Remote Access system tasks	System	Corporate Usage	Advanced SDWAN Autonomous FBB 1

ADD

The overview of groups provides general information about all User groups that have been defined, including:

- Group name
- Group description
- Group type
- Accounting mode
- Assigned type of connectivity per group

5.2.1 Group Types

The group type defines the kind of access, communication rights and authentication modes that will be provided for single Users linked to a group. In the XChange, predefined group types are as follows:

Master

The master type provides read and partial write access to the XChange system. Users linked to a master group can view XChange settings, manage Users and User groups, and carry out manual terminal switching.

User

The User type provides read-only access to the XChange portal. The XChange settings and support page is hidden and cannot be accessed. The User type is the default setting for Crew member groups. Users linked to a User group can see the XChange portal and can launch data or voice sessions (depending on the associated terminal connectivity).

Machine

The machine type is preset for a group of on-board network components and systems that communicate through the satellite link with host systems on shore. As these on-board systems cannot authenticate themselves, all the systems linked to the machine group do not need to authenticate before communicating through the associated connectivity.

Admin

The Admin type provides full read and write access to the XChange system. The Administrator can make changes to XChange settings but is not allowed to launch data or voice sessions.

Please contact Marlink Service Desk if additional administrative accounts should be created.

5.2.2 Payment Modes

Three payment modes are provided with the XChange:

- Corporate usage
- Local allowance

Corporate usage

The corporate usage mode is predefined for corporate postpaid communication. Typically, machines and the Captain can make corporate postpaid communications.

Local allowance

Linking a user group with the local allowance mode enables on-board User credit management without the need to use prepaid cards such as the Universal Card service.

Users linked to a local prepaid group need to have positive credit to be able to launch data or voice sessions.

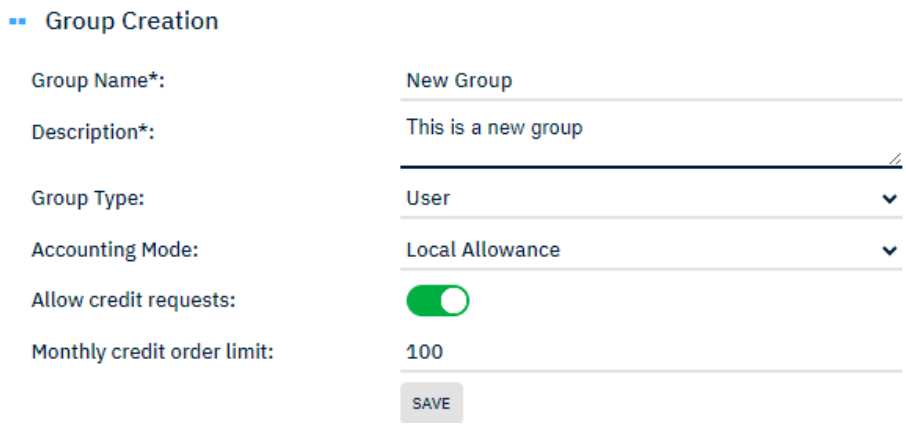
5.2.3 Create a User Group

To create new User groups, go to: *BOX SETTINGS > Accounts > Groups,* click 'Add' and proceed as follows:

- Set a group name
- Set a group description
- Select a group type
- Select a payment mode
- De- Activate the credit request (if applicable)
    - If activated, set a monthly credit order limit
- Click 'Save' to add the new group

The page is refreshed and the group details are displayed. This page enables you to review or change the group name or description. However, it is no longer possible to change the group type and payment mode.

When all general group settings are correct click 'Back' to reach the group-specific details and additional configuration parameter.



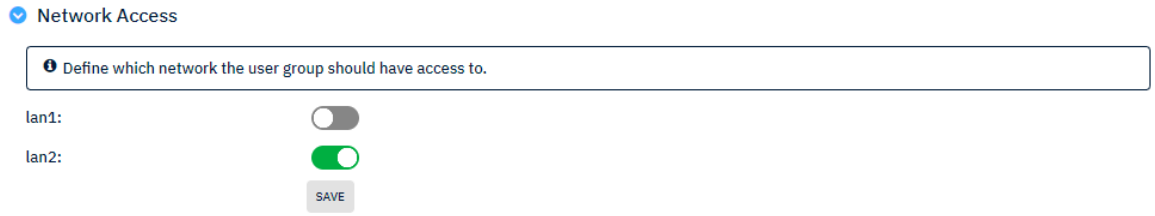
5.2.3.1 Credit Requests

For each local allowance User group, credit requests can be enabled or disabled with a simple click on the activation button. The monthly request limit is set by default to 100, and can be changed to any amount.

The monthly order limit only takes effect if the setting 'Validate every order' is not enabled. The validation of every order (credit request) can be enabled in the 'Credit Settings'.

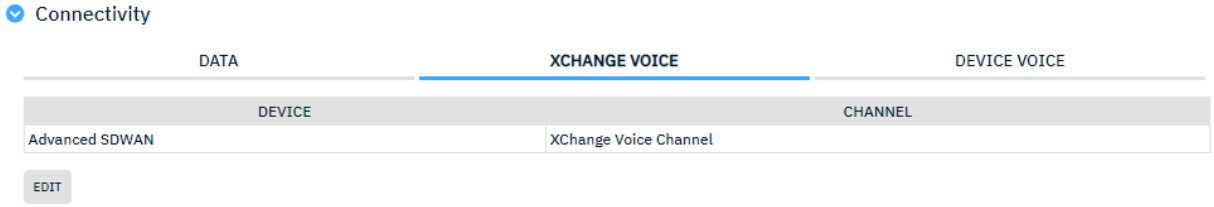
5.2.3.2 Enable Network Access

If you wish to restrict a user group from accessing the Internet through a specific network, click on 'Network Access' and disable the network to disable the access. Users with a disabled network access will not be able to use a computer on that network for online access, independent of any other configuration.

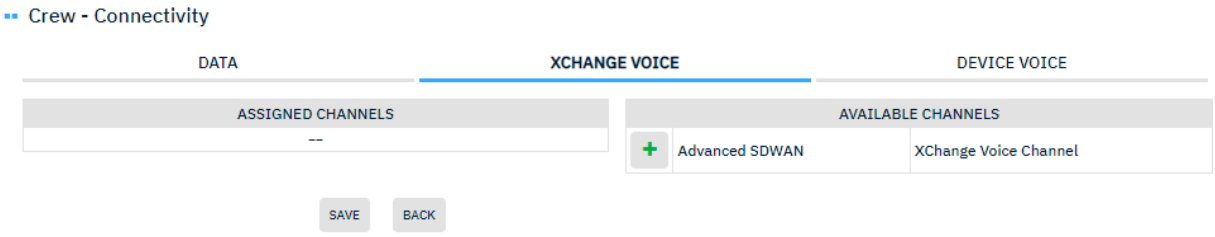


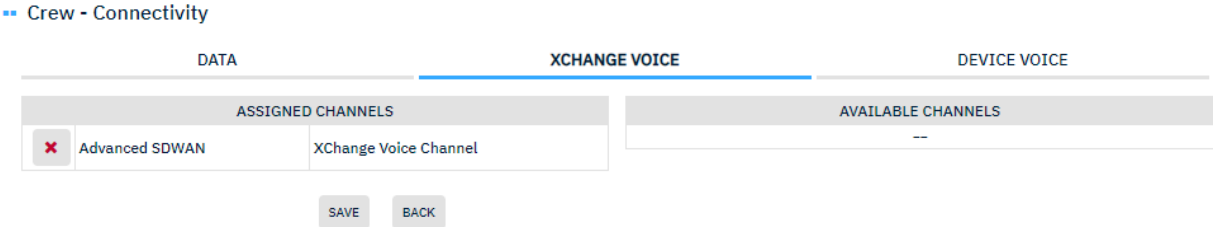
5.2.3.3 Enable XChange Voice Connectivity

If you wish to enable a User group to make calls via Marlink Voice services (Sealink or XChange FX), click on the 'Connectivity' panel to expand it, then click on the 'XChange Voice' weblet and associate the voice channel for the device to the group. By default, there is no voice channel linked to a newly created User group. If XChange Voice is not allowed or is not available, do not change anything in this panel.



To associate an XChange Voice channel to a group, click 'Edit'. The page refreshes and the available voice channels will be displayed. Click the green '+' on the right-hand table to move the preferred voice line to the left-hand table to allow access.





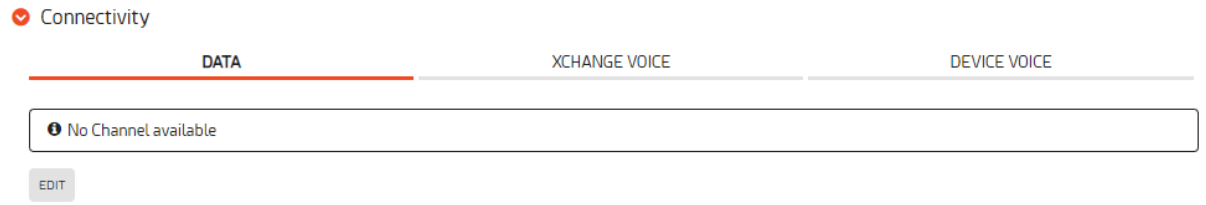
Click 'SAVE' to keep the settings.

To remove an already associated XChange Voice channel of a group, click the red 'x' and save.

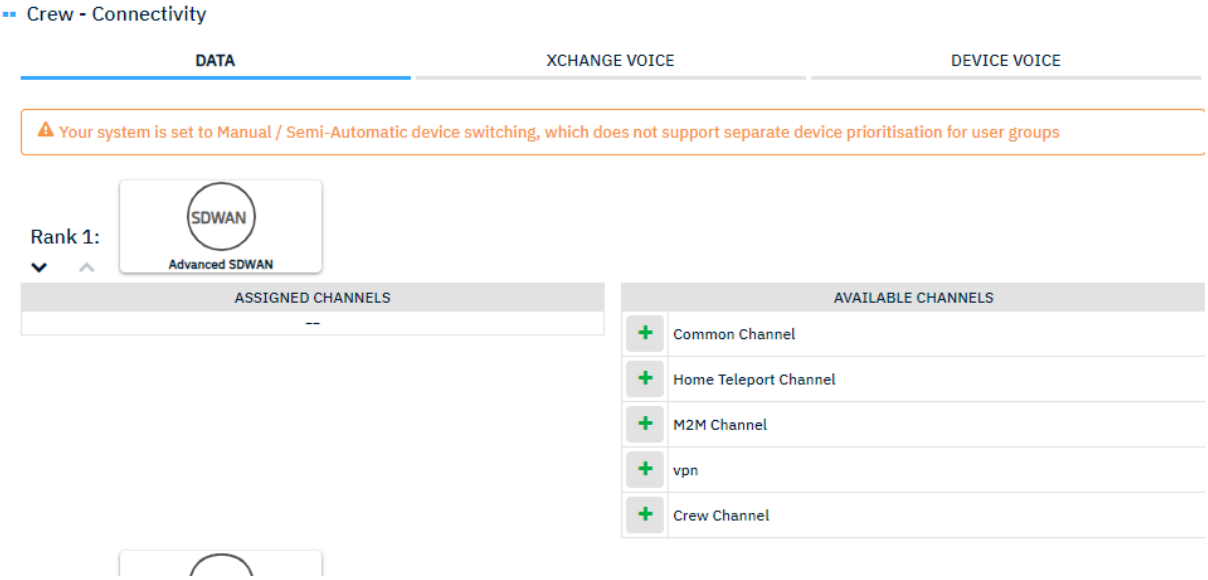
5.2.3.4 Enable Data Connectivity

To allow a User group to launch data sessions, click on the 'Connectivity' panel to expand it and associate each communication channel for each device to the group. By default, no data channel is linked to a newly created User group. If data communication is not allowed or is not available, do not change anything in this panel.

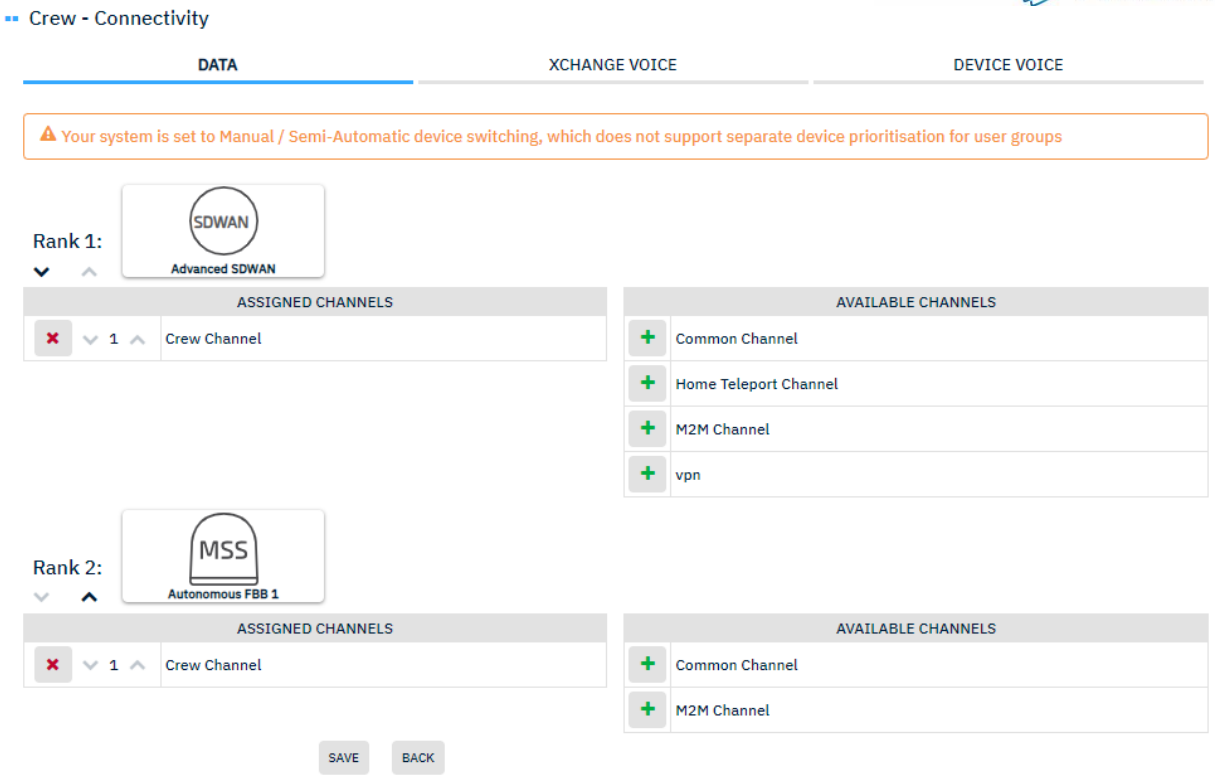
Click on 'Data' and then the 'Edit' button.



To associate a data channel to the group, click the green '+' in front of the channel on the right-hand table.



The channel moves to the left-handed table and is assigned and available now.

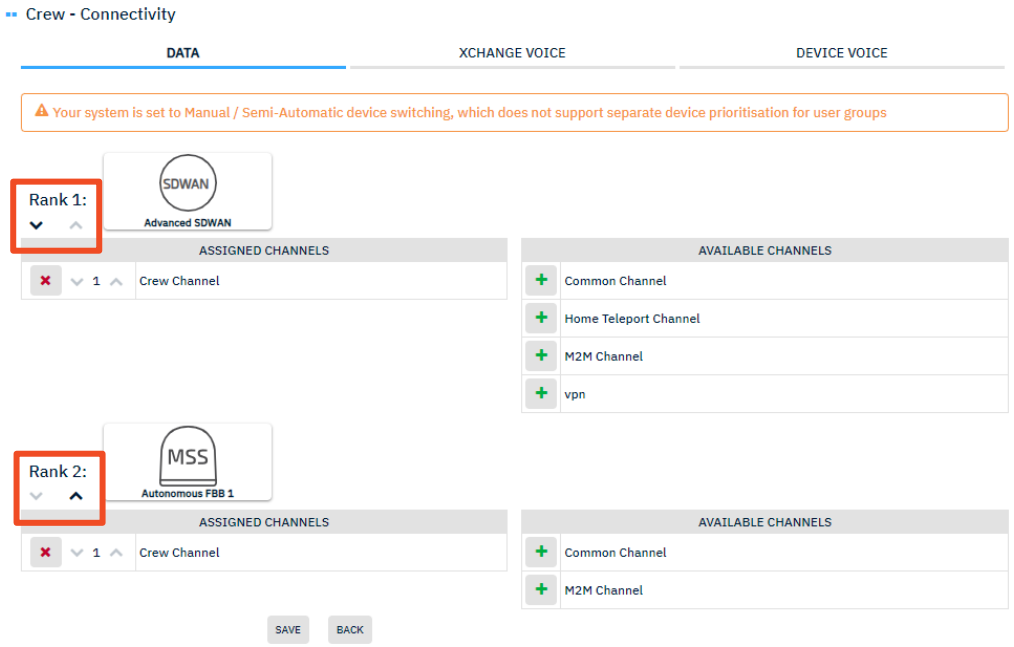


Repeat the same to assign more communication channels of 1 device or channel from multiple devices.

5.2.3.5 User group device Ranking

After all communication channel are assigned to a user group, it is optionally possible to redefine a user group-unique device priority ranking.

To change the priority ranking of the assigned devices, click the arrows below the ‘Rank’.



Please note

The number of available channels varies according to the connectivity device connected to your XChange.

Please note

The device priority ranking is only available for XChange setup on SD-WAN Lite.

Please note

On Marlink Sealink, data prioritisation is linked to the communication channel. In default settings, the ‘Crew Channel’ is the lowest priority. If you wish to give a group a different priority, please check the ‘Links’ section first and assign accordingly.

Click ‘Save’ to keep the settings.

5.2.3.6 Enable Device Voice (MSS)

To allow a User group to make standard voice calls, click on the ‘Connectivity’ panel to expand it and associate each communication channel for each device to the group. By default, no device voice channel is linked to a newly created User group. If standard voice communication is not allowed or is not available, do not change anything in this panel.

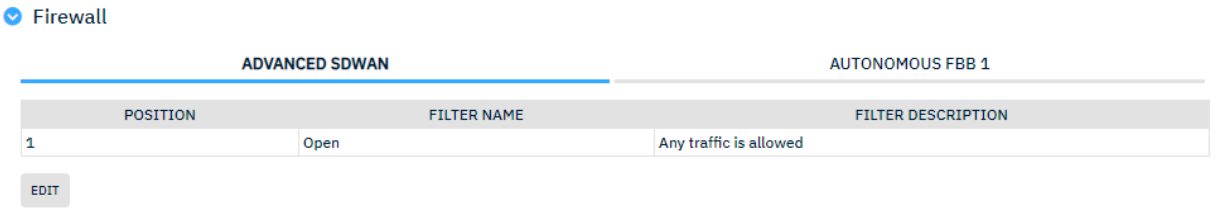
Please follow the same procedure as for XChange Voice described above.

Please note

The number of available voice channels varies according to the connectivity device connected to your XChange. Only MSS devices offer ‘Standard’ voice lines.

5.2.3.7 Firewall

For each User group, you can apply a set of firewall filtering rules.



Firewall filtering settings at the group level are the 2nd stage of the integrated firewall in the XChange.

In stage 2, a detailed filter can be set to enable the type of traffic allowed for group members. Traffic types and ports not covered by a given firewall filter will be blocked.

In the default setup, there is no firewall filtering and the group can use any kind of traffic. It is highly recommended that you change the default settings and define only those specific traffic types that are allowed for this User group.

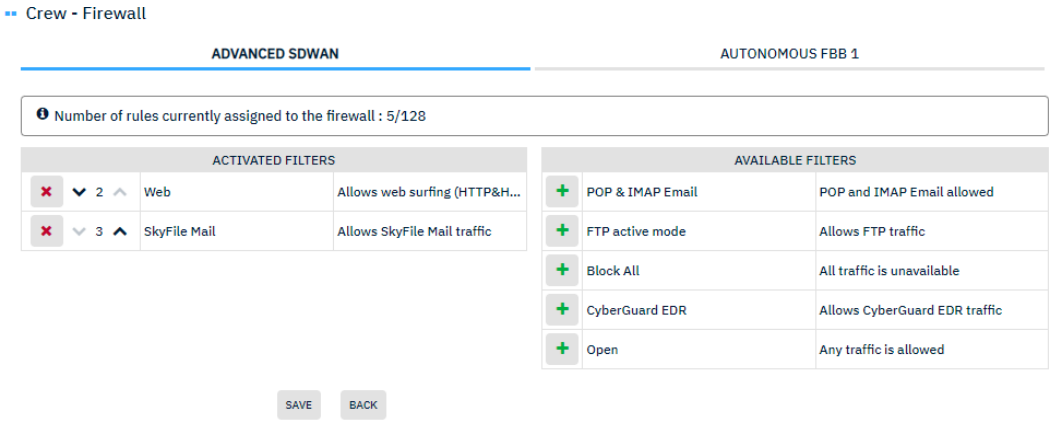
Please note

If User group firewall settings are different from terminal firewall settings, the terminal firewall will always prevail.

5.2.3.7.1 Set Up Firewall Rules

To define a firewall filtering for a group:

- Click on the group name
- Expand the 'Firewall' panel
- Select the terminal you want to apply a firewall
- Click 'Edit'
- To activate a filter, click the green '+' from the list of available filters
- To remove an unwanted filter, click the red '-'
- To change firewall check sequence, click the arrows of an activated filter to define another check priority
- Click 'Save', or 'Back' to cancel



5.2.3.8 Set up DNS Whitelisting

A DNS Whitelisting can be defined per user group, per device. Only whitelisted domains can be accessed by a user group if the whitelisting is activated. If the DNS whitelisting is activated for an user group, that user group will be able to access those whitelisted applications & websites only. Any not whitelisted DNS request will be denied.

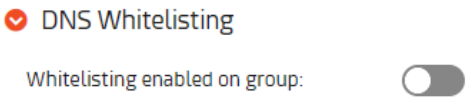
WARNING

If the DNS Whitelisting is activated, but no entry is stored it will not be possible to use any application using DNS.

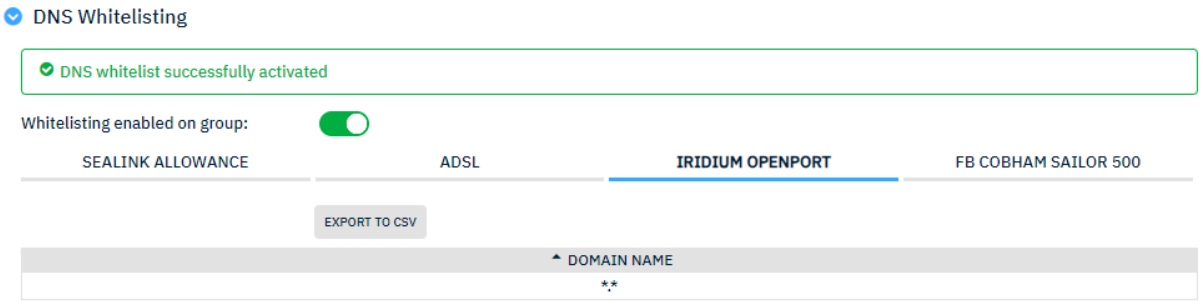
5.2.3.8.2 Managing DNS Whitelisting

Onboard it is only possible to enable and disable the DNS whitelisting for user groups. The whitelisting of desired web sites and applications can only be managed on shore using Portal 360.

To enable the DNS Whitelisting click the “ON/OFF” button.



Once the service is activated, the whitelisted DNS entries are displayed in table format.



The feature can be enabled / disabled at any time without the loss of previous entries.

Pressing the “Export” button will create a .csv file listing all DNS entries.

5.2.3.9 Set Up Daily Access Limits

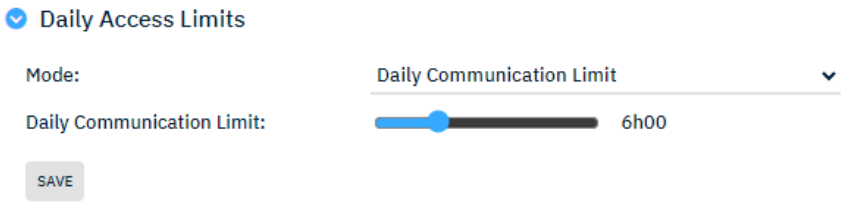
You can apply daily access limits to data and voice communications individually for each User group. The system will allow communication only either within the set time windows (based on the on-board set time) and/or until the set maximum duration has been reached. If a User tries to communicate outside of the set time windows or the maximum duration is already reached, then the system will decline the request and inform the User accordingly. For all members of a User group, the same settings will take effect regardless of when the User account was created.

The 'Daily Access Limits' offer 3 different modes:

1. 'Disabled'
    a. No access limitations
2. 'Maximum Daily Duration'
    a. A maximum number of hours per day for communication
3. 'Daily Time Windows'
    a. Communication is allowed within the time windows specified (up to 3 windows)

To set a daily access limit for a group, click the 'Daily Access Limits' collapsible panel to expand it, and then select the mode.

Daily Communication Limit



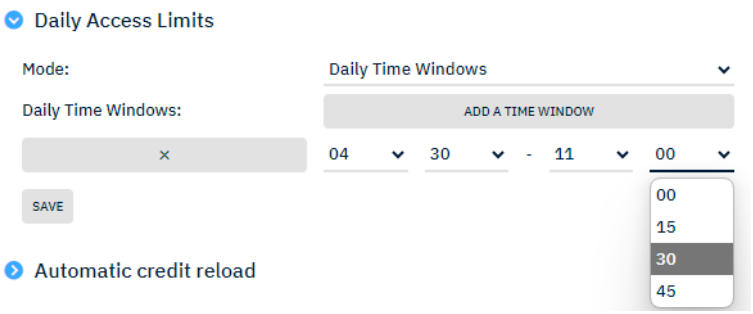
The daily communicaiton can be selected in steps of 15 minutes using the slider. The duration range goes from 15 minutes to 24 hours.

Click 'SAVE' to store and apply the setting to the entire User group.

☝ If the bar shows 24 hours, then the User will have no restriction on daily usage.

Daily Time Windows

Up to 3 different time windows can be set up. To add a new time window, click on ‘Add a time window’ and set the start- and end-time indicators to the desired times.



To set the time window, select hours and minutes from the appearing selection box.

To add a 2nd or 3rd time window, proceed in the same way.

To remove a time window, click the small ‘x’ sign.

Click ‘SAVE’ to store and apply the setting to the entire User group.

5.2.3.10 Set Up Automatic Credit Reloads

To ease the management of local prepaid credit, automatic credit reloads can be applied to any 'Local Allowance' User group. When set up, the XChange will reload the credits of all Users belonging to that User group automatically, as defined during the configuration of this function.

Please note

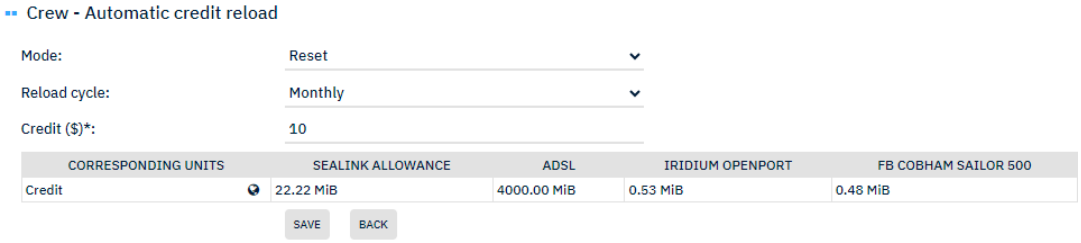
Credits provided automatically by the XChange can only be used for data communication. This special credit is named 'Corporate Credit'. Because telephony always carries a real-cost component, local allowance Users need to purchase 'Personal Credits' before telephony will be possible.

The automatic credit reload offers 2 different modes. Either a regular credit top-up can be defined, which adds the set top-up amount to any remaining corporate credit up to a defined maximum, or regular reset can be defined, which will reset the corporate credit to a set amount. Any remaining credit extra credit will be lost for the User.

The regular reload cycles can be set to:

- Daily
- Weekly
- Monthly

Automatic Credit Reset

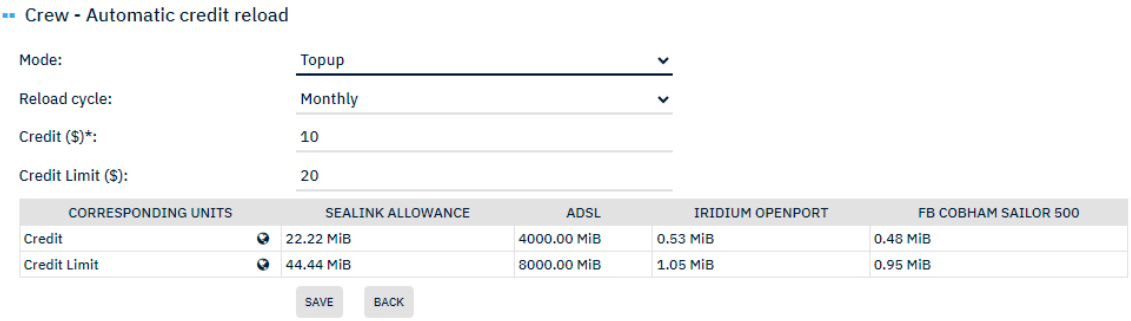


To set a regular credit reset, click on 'RESET' and select the reload cycle, such as daily, weekly or monthly.

The table below automatically shows the amount of online time or MiB per communication device, dependent on the set amount of credit and applied Price Matrix.

☝ The amount of time or value depends on the defined price matrix, which can be changed at any time through Marlink's Portal360.

Automatic Credit Top-up



To set a regular credit reload, click on 'TOPUP' and select the automatic reload cycle, such as daily, weekly or monthly.

The credit limit ensures that Users do not exceed a certain level of collected credits to avoid a potential overconsumption within a month.

The table below automatically shows the amount of online time or MiB per communication device, dependent on the set amount of credit.

☝ The amount of time or value depends on the defined price matrix, which can be changed at any time through Marlink's Portal360.

5.2.4 Edit a User Group

To edit a User group, go to: *BOX SETTINGS > Accounts > Groups*.

Click on the group name and then 'Edit' to access the page of User group details. From there you can change all parameters and additional features and edit the group details.

Click 'Edit' to change the details such as the group name or description. The group type and payment mode cannot be changed.

You can also change the XChange Voice and data connectivity settings. See the previous chapter for more details about setting voice and data connectivity.

☝ Changes to User groups will take effect immediately and changes to the name or description will switch all log entries to the new entry.

5.2.5 Delete a User Group

To delete a User group, go to: *BOX SETTINGS > Accounts > Groups*.

Click on the group name to mark it, then click the 'Delete' button below the group list.

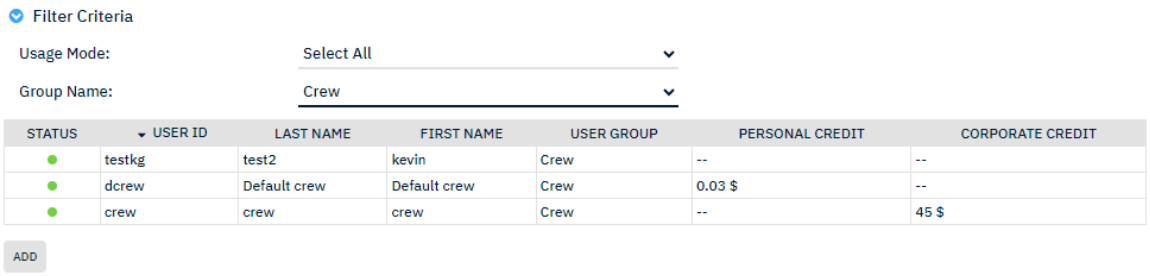
Please note

The Users linked to the group will automatically be deleted. To avoid deleting Users, empty the group before deleting it.

5.3 User Management

To enter the User management feature, go to: *BOX SETTINGS > Accounts > Users*.

User management enables you to create, manage and delete Users. Working with User accounts is mandatory in XChange. You cannot launch data or voice sessions or benefit from the XChange features without a User account.



The User overview provides general information about all defined Users such as:

- Account status
- User identifier
- Last name
- First name
- Linked User group
- Current available personal credit
- Current available corporate credit

As the User overview may have to display a very large number of Users, you can preselect which Users are displayed.

To preselect which Users will be displayed, open the 'Filter Criteria' panel and select the usage mode or group name from the list that you want to be displayed. The page is refreshed and only the selected User accounts will be displayed.

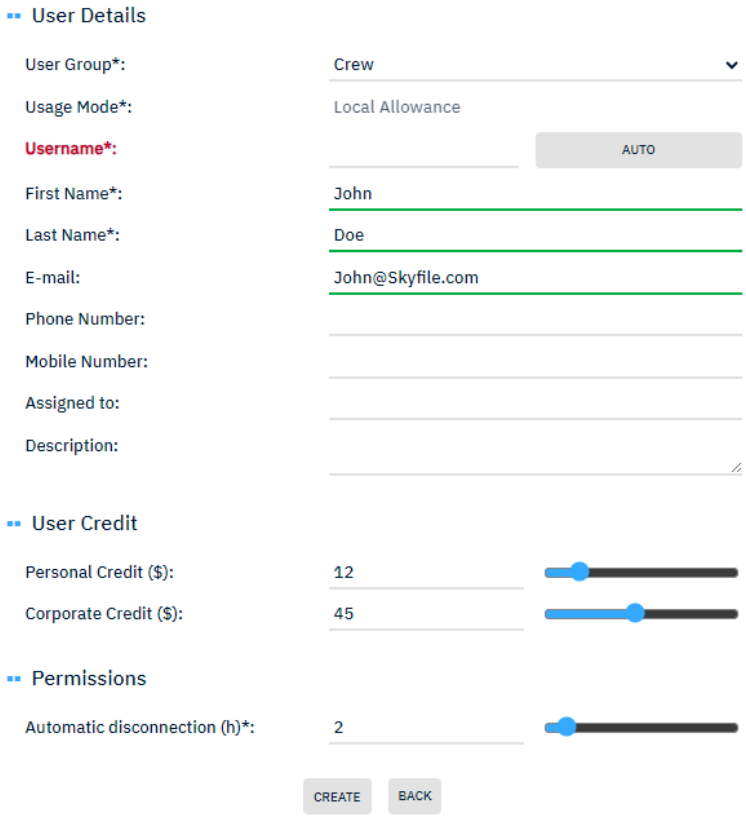
In the bottom line of the list the number of rows shown on each page can be set from 10 to 100. If more rows are available, then they will be listed on additional pages.

Click once on the title of a column to sort the overview list in ascending order and click twice to sort into descending order.

Create a User

To create new Users, go to: *BOX SETTINGS > Accounts > Users,* click 'Add' and proceed as follows:

- Select the user group
- Type in the first and last names
- Set a username or click 'Auto' (first letter of the first name concatenated with last name)
- Select a description
- Type in the email address and phone number
- Set the initial credit allowance (appears only for local allowance groups)
- Set the automatic mobile disconnection (default 2 hours)
- Click 'Create' to save the new User



5.3.1.1 Automatic Mobile Disconnection

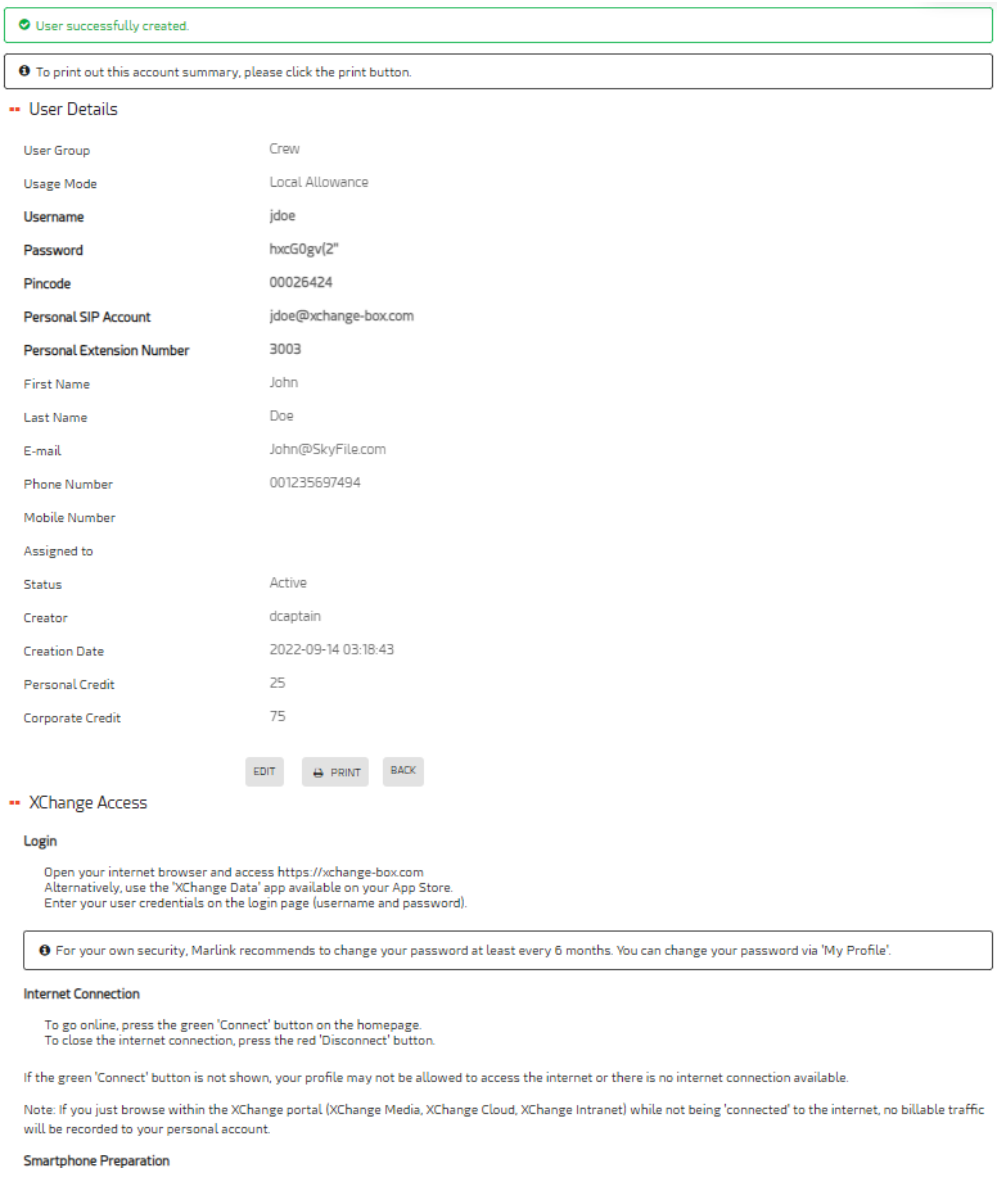
The 'automatic mobile disconnection' indicates the automatic disconnection time for users of a smartphone or tablet via the mobile web interface or XChange Apps.

When a smartphone user's online data session reaches the set threshold, 2 hours by default, the XChange disconnects the data session to avoid unwanted traffic consumption.

To change the default value, simply click and hold the mouse button on the slider and move it from left to right to the desired position or type the wished time directly.

5.3.2 User Account Voucher

After clicking on ‘Create’, the page is automatically refreshed and a User account voucher appears providing all account details, such as username and password, login, Internet access and voice call description. Make a note of the User credentials or click ‘PRINT’. Click ‘EDIT’ to change the User details or to change the password.



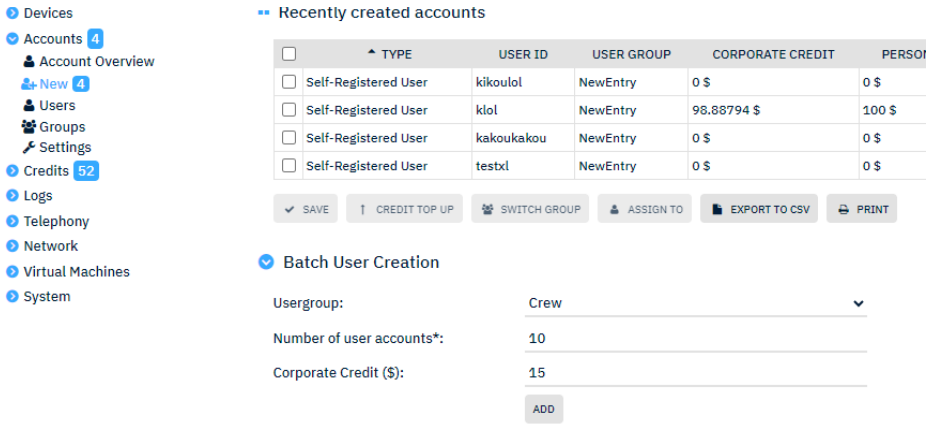
Please note

Username and password can be used to connect the XChange VoiceApp to use private smartphones as phones. The personal extension number is unique for each User and can be used for direct calls on board (free of charge).

The password is required to log in into the XChange User interface via a web browser before being able to go online. The PIN code is used to authenticate the User on a shared phone.

5.3.3 Create a Batch of Users

The 'Batch User Creation' tool provides the ability to create up to 100 User accounts in one click. Go to: *BOX SETTINGS > Accounts > New:*

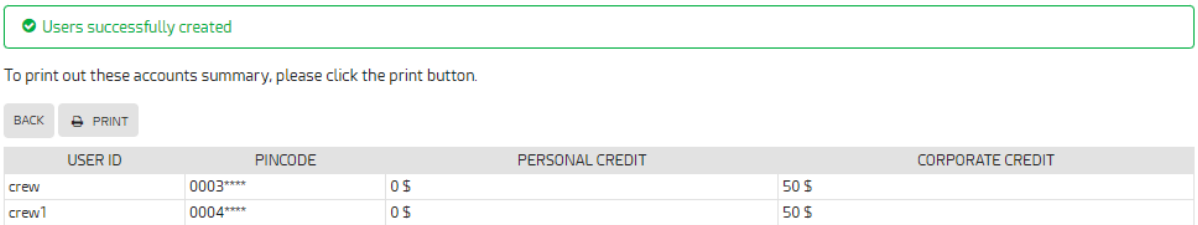


To create User accounts in a batch, follow the instructions below:

- Expand the 'Batch User Creation' panel
- Select the User group
- Set the number of User accounts to create
- Set the credit amount
    - Only available for local prepaid User groups
- Click 'Add'

The page refreshes and displays all newly created User accounts in a table.

Pressing 'PRINT' will print the overview table and each User account voucher on a separate page.



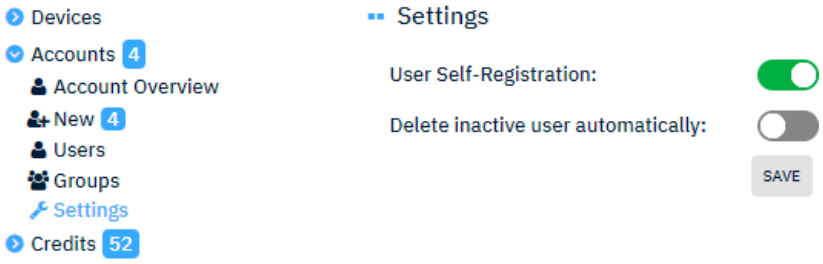
Please note

The batch-created User accounts are 'anonymous' User accounts. The username derives from the selected User group plus a consecutive number. It is not possible to alter these usernames.

5.3.4 User Self-Creation

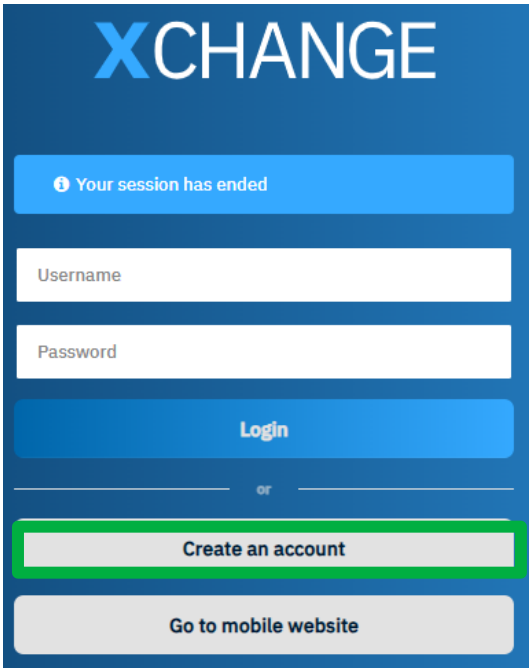
To reduce administrative tasks, it is possible to allow Crew to create their own User account without losing control.

To enable User self-creation, go to: *BOX SETTINGS > Accounts > Settings* to enable/disable the function.



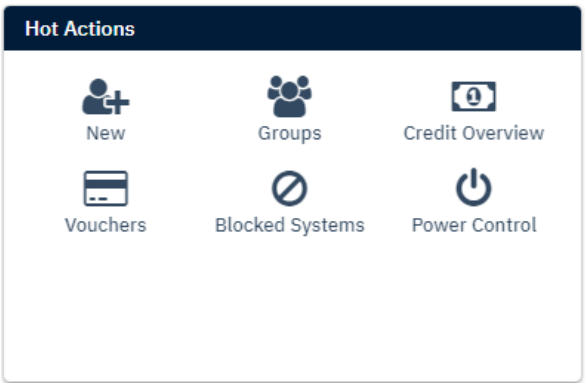
Click on 'SAVE' to store the changes.

Once User self-registration is enabled, the XChange login page shows the option to create an account:

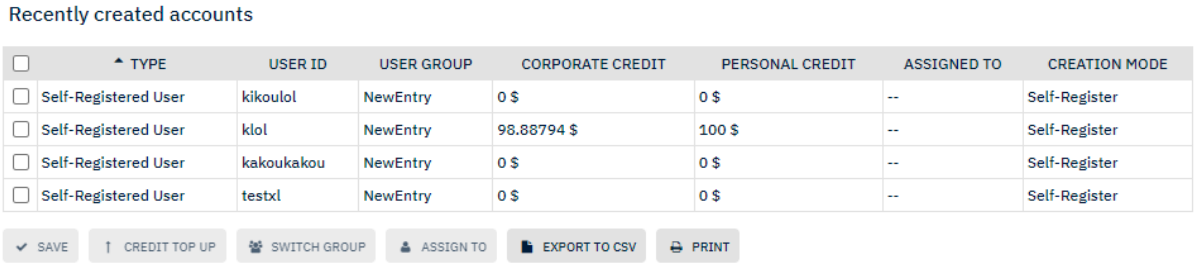


5.3.4.1 Manage Self-Created Users

Once a new self-created User account is available, the Captain will be notified on his dashboard immediately after login.



Either by clicking on the 'Hot Actions' field or by accessing: *BOX SETTINGS > Accounts > New,* a focused overview page provides details about all self-registered User accounts.

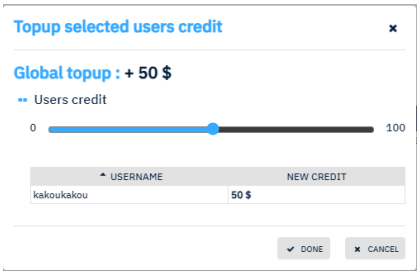


Options in this view are:

- Credit top-up for the corporate credit
- Change the User account from the 'NewEntry' User group to the desired User group
- Export this table to Excel or print

<u>Adding credit</u>

To update credit for self-created Users, if there is no need to move them to another User group, then just select the specific User and click the first grey button 'CREDIT TOP UP'. A new pop-up will appear offering a slider option to select the amount that the User credit should be topped up by:

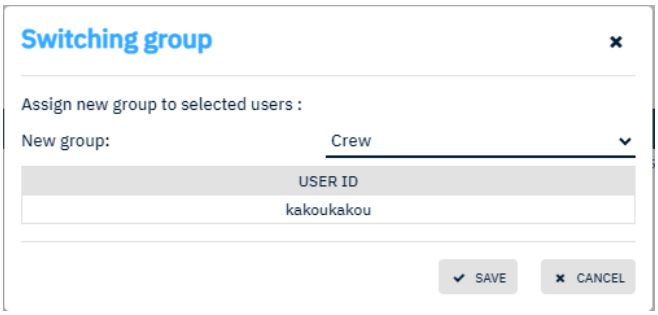


Click the slider and hold the mouse button down to slide to the position desired. The top-up amount will change accordingly between the defined limits of 0 and 100.

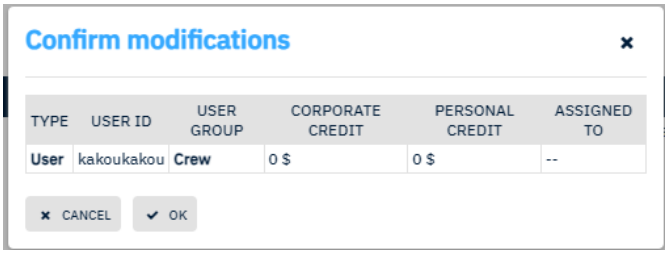
Click 'CANCEL' to discard changes or 'DONE' to store the credit update.

Changing User group

To change the User group, select the User in question and click the grey button ‘SWITCH GROUP’. In the pop-up window that appears, select the new User group and click ‘SAVE’.



Before this User group change occurs, reselect the User and click the grey ‘SAVE’ button below the table.



An ‘Updates Summary’ pop-up appears with an overview of changed User accounts. Click ‘OK’ to finally confirm the change.

Please note

After the change is saved, a new User account voucher is presented with the new PIN code , which is changed AUTOMATICALLY by the system. The changed User accounts disappear from the ‘NewEntry’ User group.

5.3.4.1.1 Keep Self-Created User Groups

To simplify User administration in general, it is possible to keep all self-created User accounts within the default ‘NewEntry’ User group and manage this User group the same way as any other local allowance User group.

The available User group functions are:

- Restrict network access
- Manage granted connectivity
- User group firewall
- Daily access limits

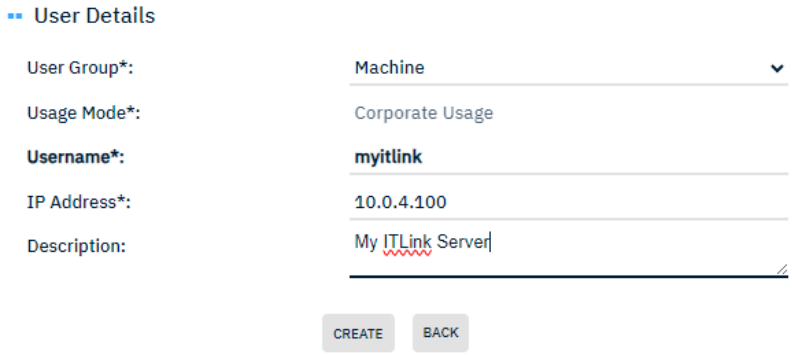
Please note

The automatic credit reloads and credit self-order functions are not available to this User group to avoid misuse of a potentially ‘free’ allowance by Crew. A standard User group is required to use these functions.

5.3.5 Create a Machine Account

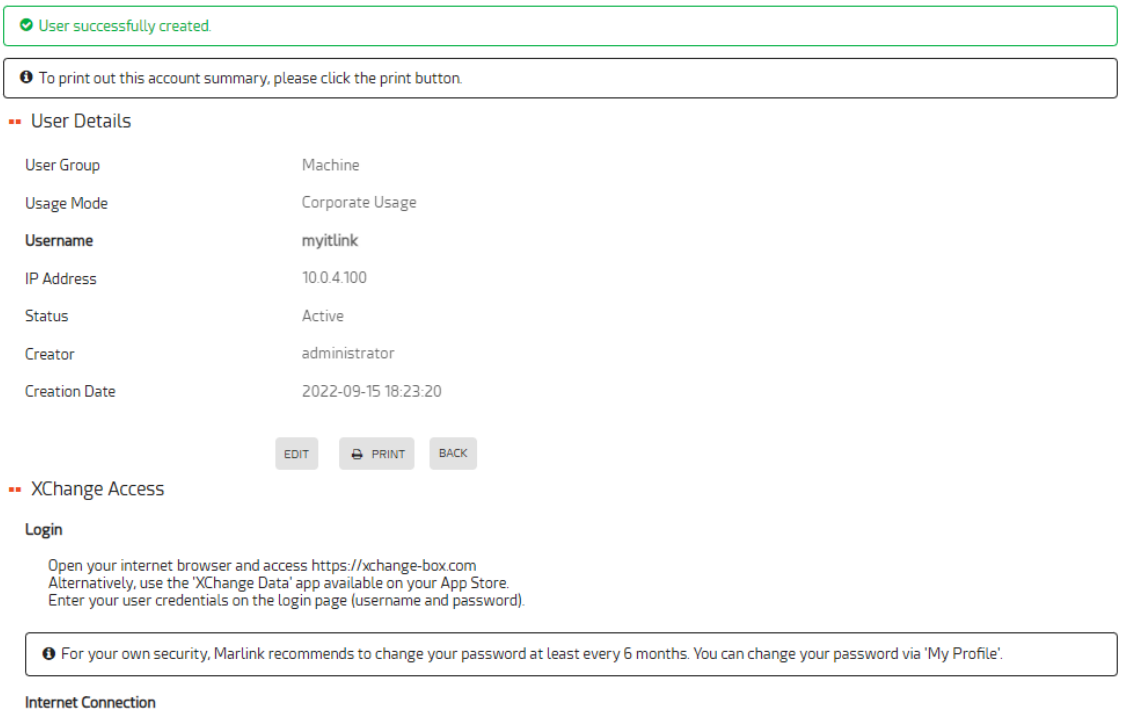
To create a new machine account, go to: *BOX SETTINGS > Accounts > Users,* click 'Add' and proceed as follows:

- Select a machine user group
- Set a username
- Set a description
- Set the local IP address of the machine (only appears for a machine group)
- Click 'Create' to save the new machine



☝ Use only lower case for usernames.

After clicking on 'Save', the page is automatically refreshed and an account voucher appears providing all account details such as username, login, Internet access and voice call description. Note down the User credentials or click 'Print'. Click 'Edit' to change the User details or to change the password.

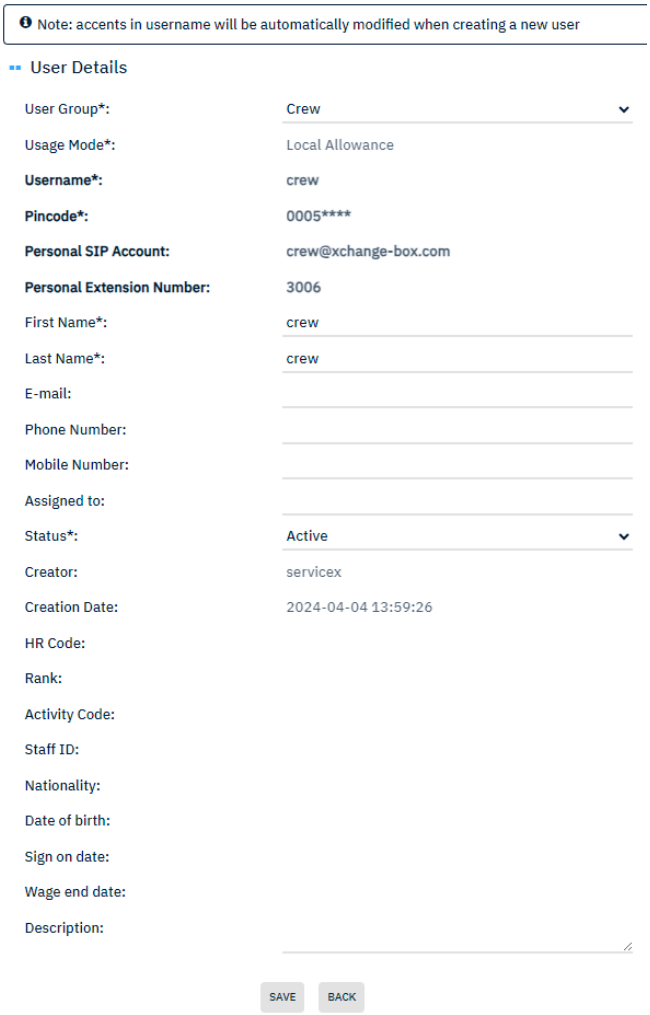


5.3.6 Edit a User Account

To edit a User account, go to *BOX SETTINGS > Accounts > Users* and click the desired username.

Click 'Edit' to enter the User details page, where you can:

- Change the User status
  - Active (ready to use)
  - Deactivated (user suspended)
- Change the name
- Change the user group
- Edit the description and contact details
- Click 'Save', or 'Back' to cancel



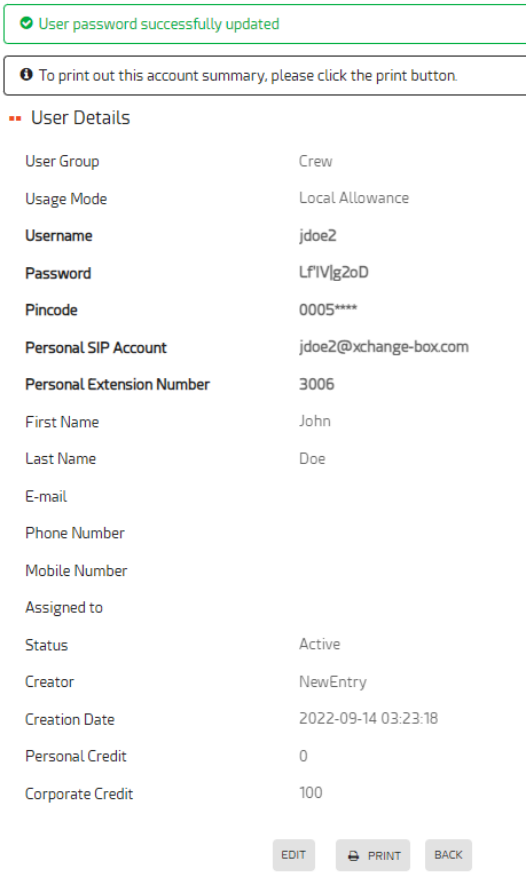
The User status can be changed from 'Active' to 'Deactivated'. This feature is useful for vessels with many changes in Crew members. There is no need to delete and recreate User accounts each time a Crew member leaves the vessel.

If a Crew member leaves the vessel, then their User account can be temporarily deactivated and easily reactivated when they return to the vessel.

5.3.7 Reset User Password

To reset a User password, go to *BOX SETTINGS* > *Accounts* > *Users* and select the specific user and proceed as follows:

- Click 'Reset Password'
- Note the new password delivered by the User credential summary

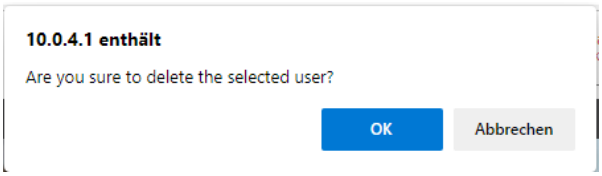


5.3.8 Delete User Account

5.3.8.1 Manual Deletion

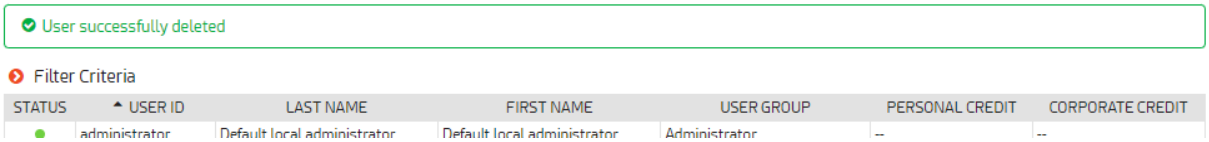
To delete a User account, go to *BOX SETTINGS > Accounts > Users* and click the specific username and then click 'Delete' and confirm the deletion in the pop-up window.

Reset the remaining credit to zero.



☝ Reset the remaining credit to zero before deleting a User account. The deleted User account remains in all local logs.

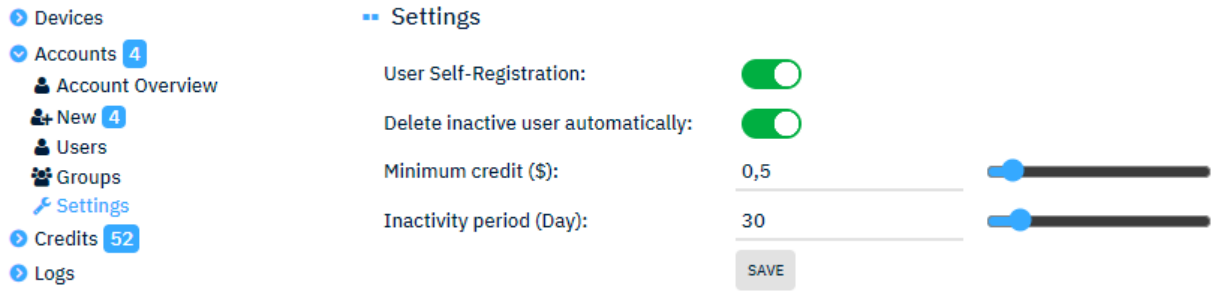
When the User account is successfully deleted, the following status message will be displayed:



5.3.8.2 Automatic User Deletion

Unused User accounts can be deleted automatically. By default, automatic deletion is disabled and can be easily enabled.

To enable automatic deletion, go to *BOX SETTINGS > Accounts > Settings*:



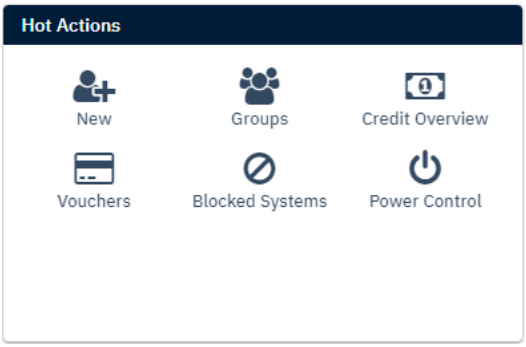
If enabled, the XChange will only delete User accounts that reach the set thresholds of 'Minimum credit' and 'Inactivity period'.

If a User has less credit and is inactive for longer than the settings, then XChange will delete this account automatically. XChange will keep a User account if either one of those thresholds are met.

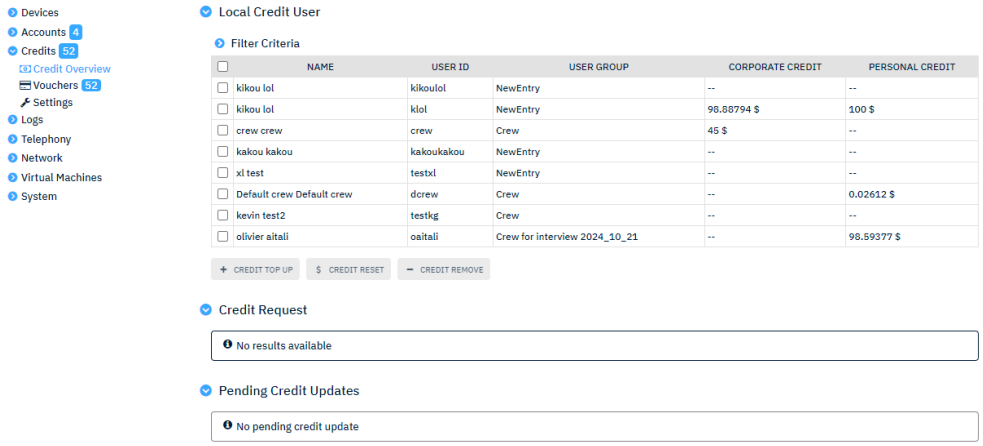
6. Credit Management

All local allowance (aka local prepaid) administration tasks are centralised in a focused menu.

There are several ways to access credit management. One of the 'Hot Actions' on the dashboard can be clicked, redirecting to the specific sub-page of the credit management functions:



Or, simply go to *BOX SETTINGS > Credits* to access the credit management overview:



The credits overview contains the most common credit administration tasks such as providing an overview of actual credit for each local allowance User, individual credit management, pending credit requests and pending credit updates.

Currencies:

XChange supports 3 different currencies. €=Euro, $= Dollar, U=Units. Depending on the preferred currency selected during installation, one of the currencies will be used across the installation.

6.1 Corporate vs Personal credit

The XChange works with 2 separate credit accounts, called 'Credit Baskets'.

The corporate credit basket is typically refilled manually by the responsible personnel or filled automatically via the 'Automatic Credit Renewal' function. The corporate credit can only be spent by the User for online data sessions, while voice communication is prohibited.

The personal credit basket can be filled manually by the responsible personnel, reloaded via XChange embedded prepaid vouchers or by a User's individual credit requests. Personal credit can be used for any kind of communication, including voice communication. For data connections, the system will, by default, first try to spend the corporate credit and will only use the personal credit if there is no corporate credit remaining.

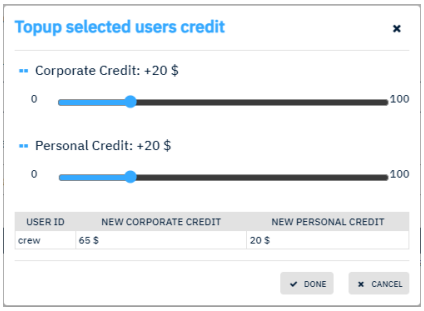
6.2 Individual Credit Management

To manage a User's local credit, select the specific username(s) in question. There are 3 ways of changing a User's credit:

- Top-up
- Reset
- Remove

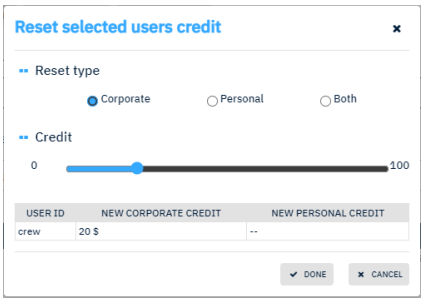
Top-up

To top up the credit, click the 'Credit Topup' button and use the slider to add credit to one or both credit baskets. Click on 'DONE' to refresh the page and display the updated current credit.



Reset

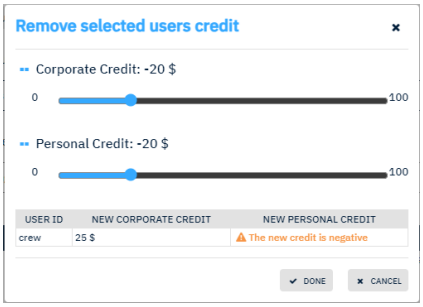
To reset the credit, click the 'Credit Reset' button, select the credit basket to be reset and set the credit amount to which the credit should be reset to. Click on 'DONE' to refresh the page and display the updated current credit.



☝ Reset the User's credits will set the credit basket to the set amount. Any credits remaining before the reset will be lost/overwritten, i.e. the reset does not add to the existing amount of credit, it replaces it with a new amount.

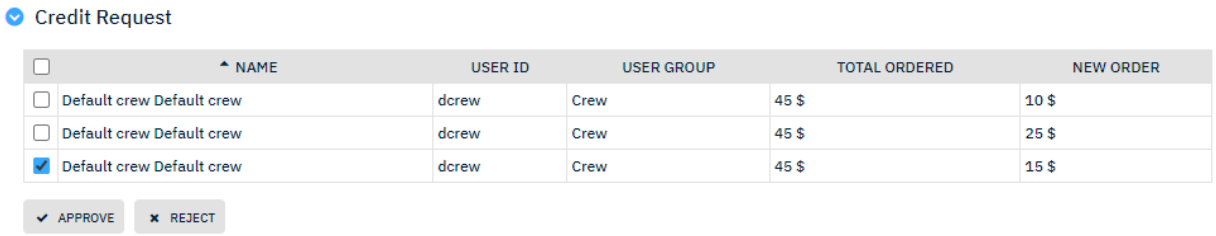
Remove

To subtract an amount from the User's credit, click the 'Credit Remove' button, select the credit basket to be reset and set the credit amount to be removed. Click on 'DONE' to refresh the page and display the updated current credit.



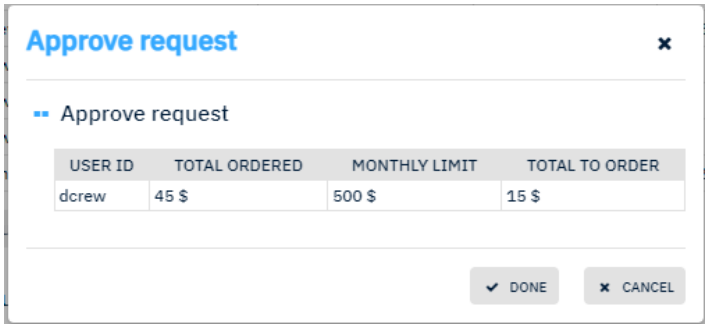
6.3 Manage Credit Requests

If the credit self-ordering function is enabled, then a local allowance User will be able to request credit top-ups without the need to request any action from the Administrator. If the credit order limit is reached, or the option to 'validate each order' is enabled, then each request will be displayed in the 'Credit Request' table.



The table shows the real name of the User, User ID, User group, the total ordered amount within the actual month and the amount of the latest order. If the User has exceeded the monthly order limit, then a warning icon will indicate this.

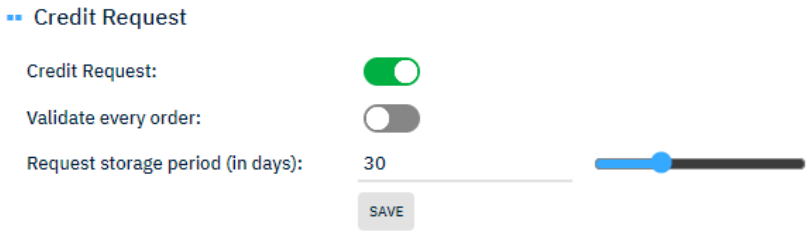
Any credit request can be either approved or rejected. To do so, select the specific request and click either the 'Approve' or the 'Reject' button.



Once any credit request is approved, the respective credit log entry is created by XChange automatically and the User's credit is updated.

6.3.1 Credit Request Configuration

To configure or disable the credit request function, go to *BOX SETTINGS > Credits > Settings*:



Activation

By default, the credit request function is enabled and can be simply disabled with a click on the green 'On' button.

Configuration

The default configuration is set to NOT await an approval for each credit request. Approval will only be requested if the monthly order limit for a local allowance User group is reached.

Enabling 'Validate every order' will ignore any monthly order limit set for a User group. To enable the validation, click the tick-box and click 'Save' to store the settings.

Request storage

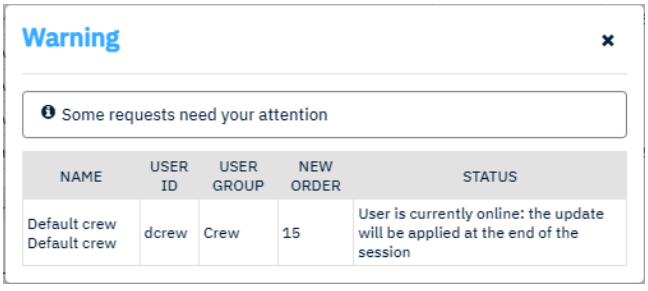
The request storage period (in days) is set to 30 days. The period can be changed between 0 and 90 days for how long requests are stored in the database.

6.4 Credit Updates while user online

Whatever credit update option is used, all credits are changed immediately.

If the user is online, during credit change the system will store the credit update and execute it as soon as the user goes offline. Once the user went offline, the system will automatically apply any credit change.

After a credit update is stored, the system informs immediately about the online user:



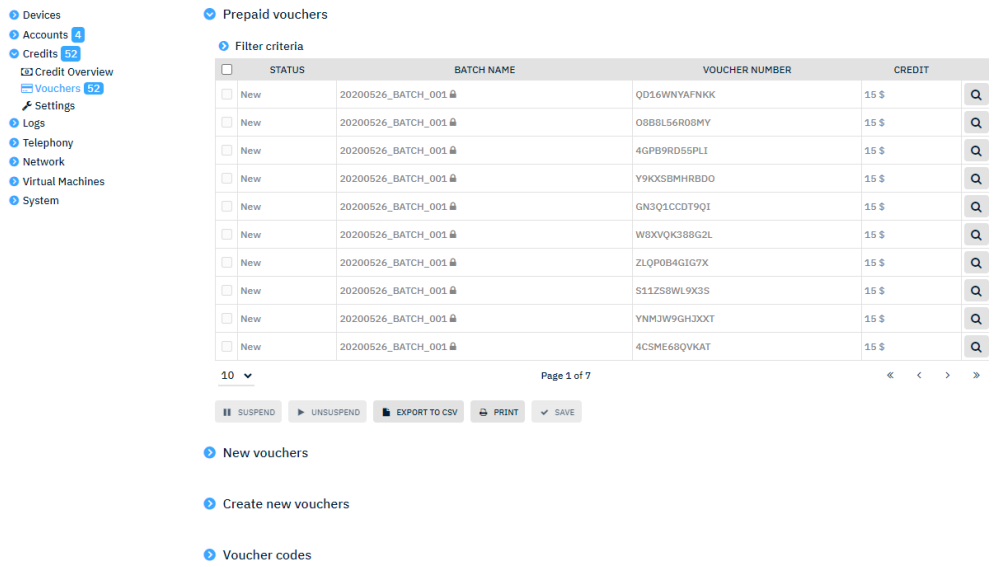
6.5 Prepaid Voucher Management

The embedded prepaid voucher mechanism enables the sale of prepaid PIN vouchers to any local allowance User. The Administrator can freely decide the amount of credit to be available per voucher. A combination of vouchers with different credit amounts can be used at the same time.

Prepaid voucher can be bought by a local allowance User. The User can use that voucher code to top up their personal credit basket by accessing the 'My Profile'. Once the User has topped up their personal credit, the used voucher code status will be set to 'used' and it cannot be reused.

Please note

Prepaid vouchers cannot be used for online or voice access. A valid User account is strictly mandatory.

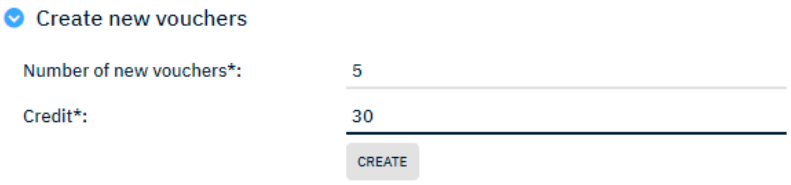


The overview page shows a table with all created vouchers, containing the status, batch name, unique voucher number and the assigned credit amount.

6.5.1 Create New Vouchers

To create a new batch of vouchers, go to *BOX SETTINGS > Credits > Prepaid Vouchers*:

Expand the 'Create new vouchers' panel and set the number of new vouchers to be created and the amount of credit per voucher:



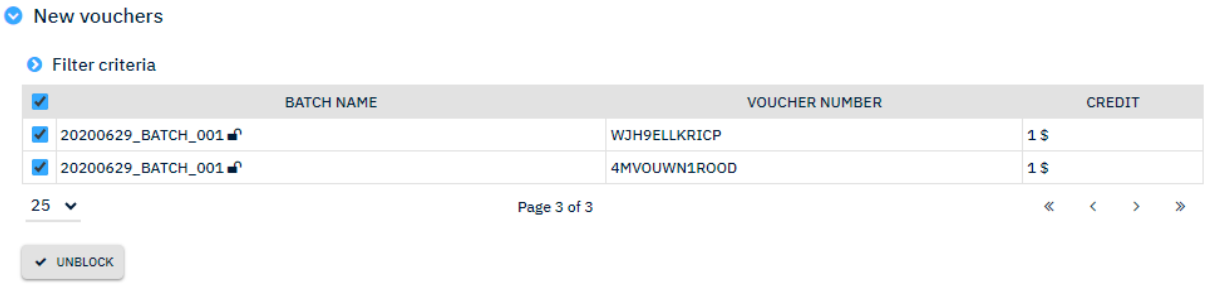
Clicking the 'CREATE' button will refresh the page and the newly created voucher codes with status 'New' are shown in the overview table.

Please note

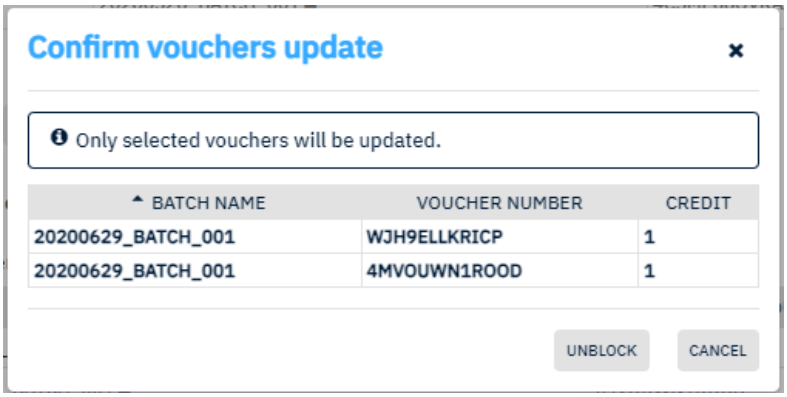
Before newly created prepaid vouchers can be used for credit top-ups, it is mandatory that these vouchers are unblocked by the Administrator.

6.5.2 Unblock New Vouchers

To unblock new vouchers, expand the panel ‘New vouchers’.



Select the new voucher(s) to be unblocked and click the ‘UNBLOCK’ button above the table. A confirmation pop-up appears summarising the selected vouchers. Click on ‘UNBLOCK’ to process the action.



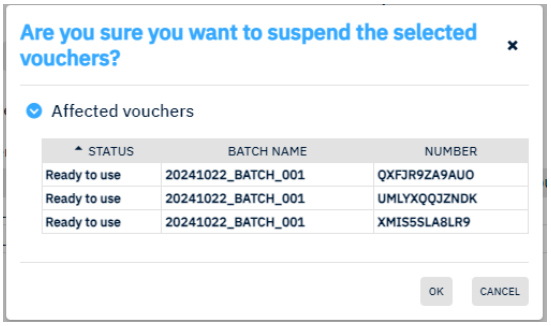
6.5.3 Manage Prepaid Vouchers

The system offers multiple management functions. Newly created vouchers can be unblocked, suspended, unsuspended, deactivated, reactivated or deleted.

6.5.3.1 Suspend Vouchers

If a prepaid voucher becomes lost, then it is possible to suspend these vouchers, and then to unsuspend them once they are found again.

To suspend a voucher, select the specific voucher in the overview table and click the ‘Suspend’ button above the overview.



A pop-up appears summarising the vouchers to be suspended. Click on ‘OK’ to activate the suspension.

Please note

Only previously unblocked vouchers can be suspended or unsuspended.

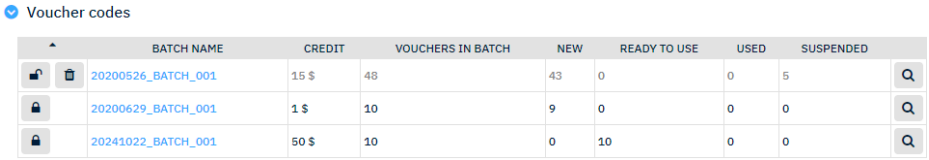
To unsuspend a previously suspended voucher, repeat the above procedure.

6.5.3.2 Deactivation and Deletion

Voucher batches can be deactivated and deleted at any time. When all voucher codes are used, the batch can be deleted to free up space on the voucher overview.

Before a voucher batch can be deleted, it needs to be deactivated.

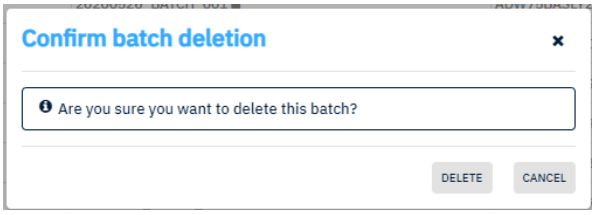
Expand the ‘Voucher codes’ panel and click the closed-lock icon to the left of a specific voucher batch to deactivate it.



The page refreshes and displays the deactivated voucher batch written in light grey.

To reactivate a voucher batch, click the ‘Open Lock’ icon in to the left of the voucher batch.

To delete a voucher batch, click the ‘Bin’ icon. A confirmation pop-up will appear asking for confirmation.



Click on ‘DELETE’ to delete the voucher batch – all voucher codes that formed part of that batch will be deleted immediately and will disappear from the voucher overview.

7. Logs

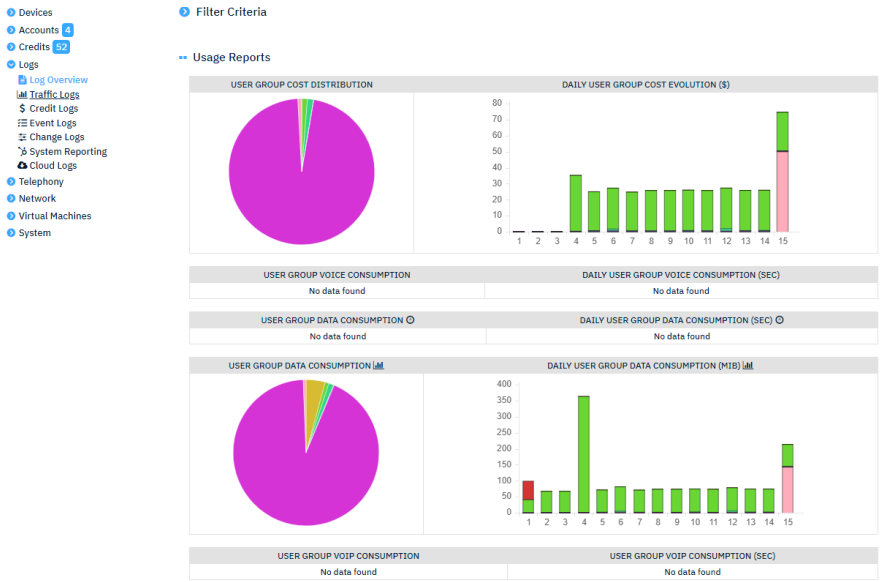
The XChange has an embedded log feature. This provides the Captain and Administrator with near real-time information about traffic, local credit consumption, changes, system and event logs.

The log function is divided into the following log types:

- Overall development of traffic
- Traffic Logs
- Cloud Logs
- Credit Logs
- Event Logs
- Change Logs
- System Reporting

7.1 Traffic Development

To view the overall development of traffic, go to: *BOX SETTINGS > Logs > Overview*.

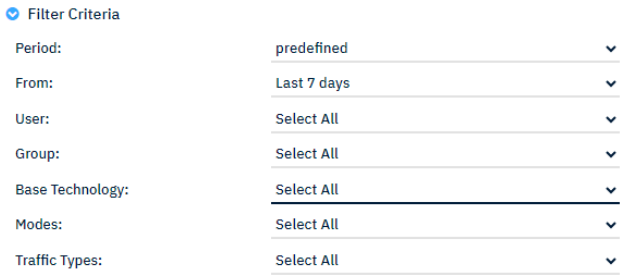


Graphical usage reports are displayed showing the traffic patterns for the current month for each User group and communication type (e.g. data and voice).
On every chart, if you hover the mouse pointer over the image, then a mouse-over function provides additional information.

7.2 General Filter Criteria

Filter criteria are provided separately for each log type. By default, the last 7 days are displayed when entering a log section. You can display a specific period, usage mode or device by selecting from the boxes at the top of the page. These cover:

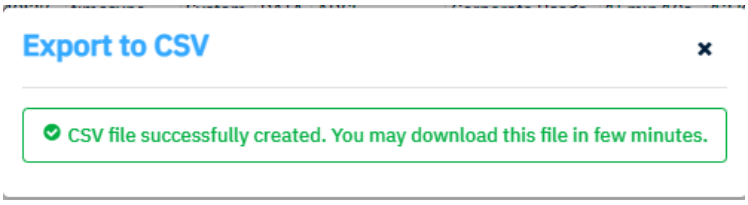
- Period
  - Current month
  - Last 7, 14, 30 days
  - Custom
    - From–To specific date range
- User
  - All or a specific User
- Group
  - All or a specific group
- Modes
  - Corporate usage
  - Local prepaid
- Traffic Types
  - Data
  - Voice
  - VoIP
- Base Technology
  - All or a specific terminal



To filter the chosen log details, select the options from the various selection criteria. The page will refresh and the selected log details will be displayed.

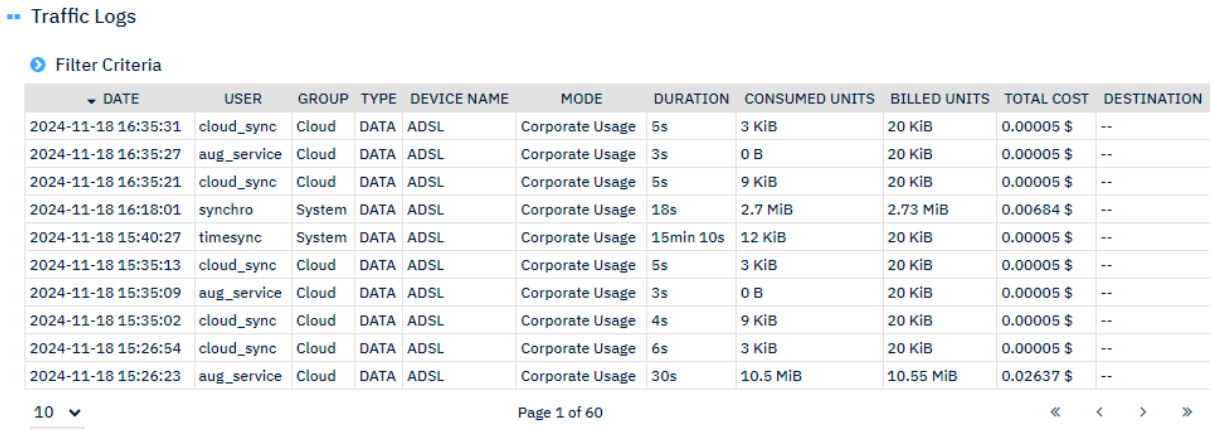
7.2.1 Export to CSV

All logs can be exported to a .csv file simply by clicking on ‘Export to CSV’. To export a log, filter the log display to show the options you want and click ‘Export to CSV’.



7.3 Traffic Logs

To view the detailed traffic log, go to: *BOX SETTINGS > Logs > Traffic Log.*



	DESCRIPTION
'DATE'	Start date and time of the session
'USER'	Username launched this session
'GROUP'	User group for this User
'TYPE'	Data, voice or VoIP
'DEVICE NAME'	Terminal used
'MODE'	Corporate usage, local allowance, Universal Card
'DURATION'	Duration of the session
'CONSUMED UNIT'	Consumption units e.g. KiB, or min
'BILLED UNIT'	Charged units including minimum charge and charge increments
'TOTAL COST'	Cost of the session
'DESTINATION'	Displays the number dialled (For voice calls only)

Tip!! Click once on the name of any column to sort the list in an ascending order and twice for a descending order.

7.4 Cloud Logs

The cloud logs are only available if the optional Premium Service “XChange Cloud” is activated. The cloud logs show all cloud synchronisations for all XChange Cloud accounts which are assigned to a specific XChange.

Cloud Synchronisation Logs

Filter Criteria

STATUS	DATE	FOLDER	ACTION	FILE SIZE	DEVICE NAME	TRANSFER MODE	ADDITIONAL INFORMATION
✔	2024-11-05 08:02:19	doc_service/Crew Documentation/SkyFile Mail/SkyFile Mail_User Guide_Full Version 2024_v24.pdf	Download	1.7 MiB	Starlink	ONE_WAY	-
✔	2024-11-05 08:02:19	doc_service/Crew Documentation/SkyFile Mail	Download	0 B	Starlink	ONE_WAY	-
✔	2024-11-05 08:02:15	doc_service/Captain Documentation/SkyFile Mail/SkyFile Mail_User Guide_Full Version 2024_v24.pdf	Download	1.7 MiB	Starlink	ONE_WAY	-
✔	2024-11-05 08:02:15	doc_service/Captain Documentation/SkyFile Mail	Download	0 B	Starlink	ONE_WAY	-

The Cloud Log shows all details related to a single file being transmitted through XChange Cloud. For simplicity, the full storage path of each individual file is shown as well as additional information like the synchronisation-action (Upload, Download, Delete) and the original file-size.

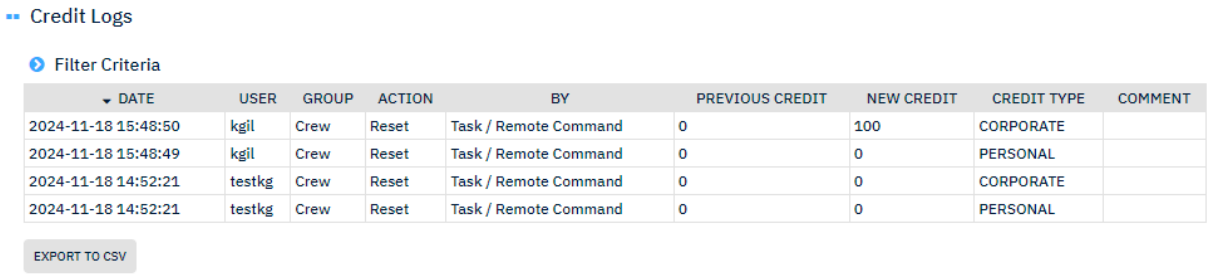
Please note

The file-size shown in this log do not include the compressed value or the really consumed synchronisation traffic. For traffic consumption details please check the traffic log.

	DESCRIPTION
‘STATUS’	File synchronisation status
‘DATE’	Start date and time of the synchronisation
‘FOLDER’	Detailed path of a file
‘ACTION’	Logged action: Download, Upload, Delete
‘FILE SIZE’	Original file size without compression and consumed traffic
‘DEVICE NAME’	Terminal used
‘TRANSFER MODE’	Direction of the file synchronisation
‘ADDITIONAL INFO’	If error apply, a description is shown here

7.5 Credit Logs

To view the detailed credit log, go to: *BOX SETTINGS > Logs > Credit Log.*

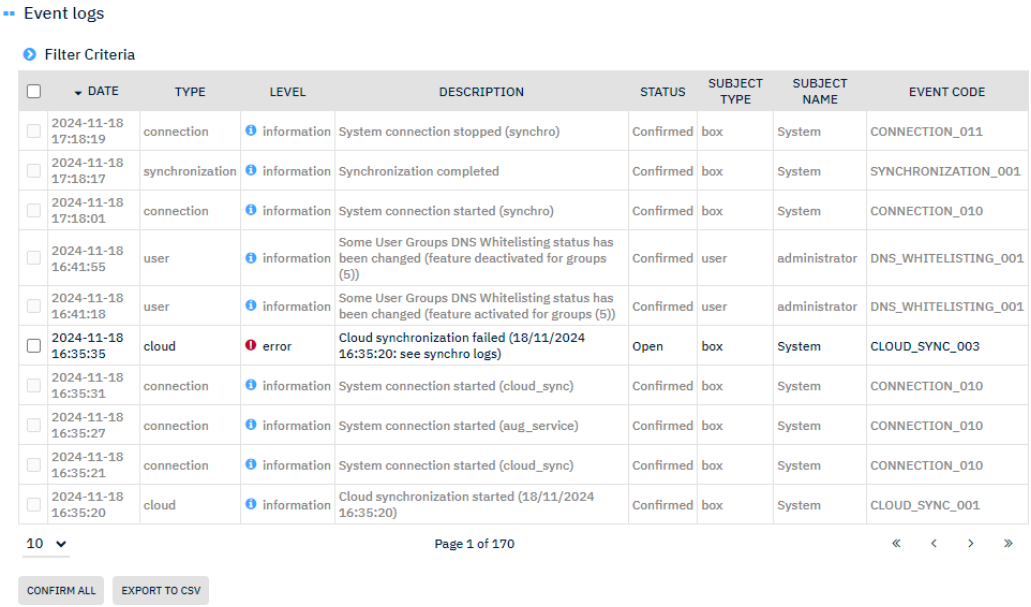


	DESCRIPTION
'DATE'	Date and time of a credit operation
'USER'	Username affected by credit operation
'GROUP'	User group this User belongs to
'ACTION'	Reset, Up, Down
'BY'	Username for changed credit amount
'PREVIOUS CREDIT'	Amount of credit before change
'NEW CREDIT'	New credit amount available for this User
'CREDIT TYPE'	Displays the name of the credit basket that has been updated
'COMMENT'	Displays the used prepaid voucher

Tip!! Click once on the name of any column to sort the list in an ascending order and twice for a descending order.

7.6 Event Log

To view the detailed event log, go to: *BOX SETTINGS > Logs > Event Log.*


Event logs

Filter Criteria

DATE	TYPE	LEVEL	DESCRIPTION	STATUS	SUBJECT TYPE	SUBJECT NAME	EVENT CODE
2024-11-18 17:18:19	connection	information	System connection stopped (synchro)	Confirmed	box	System	CONNECTION_011
2024-11-18 17:18:17	synchronization	information	Synchronization completed	Confirmed	box	System	SYNCHRONIZATION_001
2024-11-18 17:18:01	connection	information	System connection started (synchro)	Confirmed	box	System	CONNECTION_010
2024-11-18 16:41:55	user	information	Some User Groups DNS Whitelisting status has been changed (feature deactivated for groups (5))	Confirmed	user	administrator	DNS_WHITELISTING_001
2024-11-18 16:41:18	user	information	Some User Groups DNS Whitelisting status has been changed (feature activated for groups (5))	Confirmed	user	administrator	DNS_WHITELISTING_001
2024-11-18 16:35:35	cloud	error	Cloud synchronization failed (18/11/2024 16:35:20: see synchro logs)	Open	box	System	CLOUD_SYNC_003
2024-11-18 16:35:31	connection	information	System connection started (cloud_sync)	Confirmed	box	System	CONNECTION_010
2024-11-18 16:35:27	connection	information	System connection started (aug_service)	Confirmed	box	System	CONNECTION_010
2024-11-18 16:35:21	connection	information	System connection started (cloud_sync)	Confirmed	box	System	CONNECTION_010
2024-11-18 16:35:20	cloud	information	Cloud synchronization started (18/11/2024 16:35:20)	Confirmed	box	System	CLOUD_SYNC_001

10 Page 1 of 170

CONFIRM ALL EXPORT TO CSV

The event log refreshes automatically every 10 seconds. You can also update the log manually by clicking the 'Refresh' button on your browser or by pressing F5.

All events are displayed in this log. Event messages that are black with status 'Open' are not acknowledged by the Administrator or Captain and are displayed on their dashboards in the 'Events and Alerts' block.

	DESCRIPTION
'DATE'	Date and time of the event
'EVENT ON'	Event location/affected process
'EVENT TYPE'	Type of event
'DESCRIPTION'	Detailed explanation of what happened
'STATUS'	Acknowledgement status
'SUBJECT TYPE'	Event triggered equipment type
'SUBJECT NAME'	Device name
'EVENT CODE'	Detailed event code

☝ Messages in the event log can be used for troubleshooting and for status information. A detailed list of available event log messages is provided in Appendix A at the end of this document.

7.6.1 Acknowledge an Event

Events remain on the dashboard ‘Events and Alerts’ block until they are acknowledged.

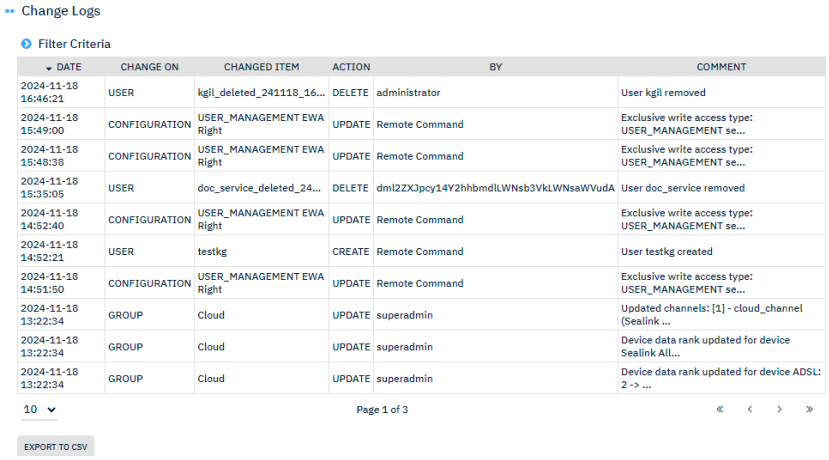
To acknowledge all open events, click the ‘Confirm All’ button.

To acknowledge a specific event, click on the event and press the ‘Confirm’ button that appears.

Acknowledged events change to grey and will no longer be displayed on the dashboard.

7.7 Change Log

To view the detailed change log, go to: *BOX SETTINGS > Logs > Change Log.*


Change Logs

Filter Criteria

DATE	CHANGE ON	CHANGED ITEM	ACTION	BY	COMMENT
2024-11-18 16:46:21	USER	kgil_deleted_241118_16...	DELETE	administrator	User kgil removed
2024-11-18 15:49:00	CONFIGURATION	USER_MANAGEMENT EWA Right	UPDATE	Remote Command	Exclusive write access type: USER_MANAGEMENT se...
2024-11-18 15:48:38	CONFIGURATION	USER_MANAGEMENT EWA Right	UPDATE	Remote Command	Exclusive write access type: USER_MANAGEMENT se...
2024-11-18 15:35:05	USER	doc_service_deleted_24...	DELETE	dml2ZXJpcy14Y2hhbmdlLWNsb3VkLWNsaWVudA	User doc_service removed
2024-11-18 14:52:40	CONFIGURATION	USER_MANAGEMENT EWA Right	UPDATE	Remote Command	Exclusive write access type: USER_MANAGEMENT se...
2024-11-18 14:52:21	USER	testkg	CREATE	Remote Command	User testkg created
2024-11-18 14:51:50	CONFIGURATION	USER_MANAGEMENT EWA Right	UPDATE	Remote Command	Exclusive write access type: USER_MANAGEMENT se...
2024-11-18 13:22:34	GROUP	Cloud	UPDATE	superadmin	Updated channels: [1] - cloud_channel (Sealink ...
2024-11-18 13:22:34	GROUP	Cloud	UPDATE	superadmin	Device data rank updated for device Sealink All...
2024-11-18 13:22:34	GROUP	Cloud	UPDATE	superadmin	Device data rank updated for device ADSL: 2 -> ...

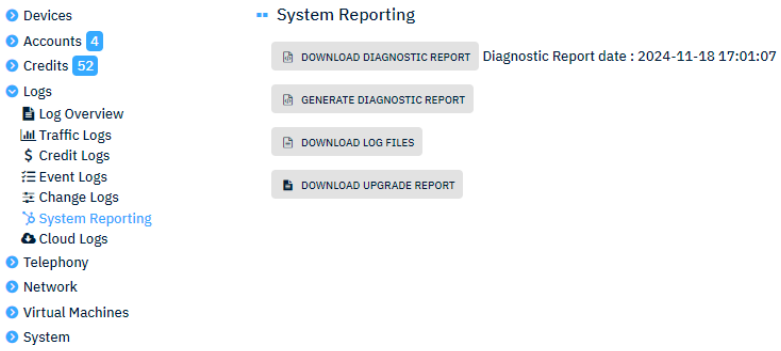
10 Page 1 of 3

EXPORT TO CSV

	DESCRIPTION
‘DATE’	Date and time of the change
‘CHANGE ON’	Name of object changed
‘CHANGE ITEM’	Name of item changed
‘ACTION’	Delete, Create, Update
‘BY’	Username that changed a setting
‘COMMENT’	Detailed explanation of what was changed

7.8 System Reporting

To access the system reporting, go to: *BOX SETTINGS > Logs > System Reporting.*



In support cases, the system reporting offers the option to either download a diagnostic report or all system log files.

Please note

The system reports can only be analysed by Marlink technical departments and should only be downloaded and forwarded to Marlink technical support on request.

8. Telephony

In the XChange is a fully functional telephony server (PBX) that can support analogue phones and a nearly unlimited number of IP phones. In addition, Users who own a smartphone can use the XChange Voice App to connect their private smartphone to the XChange PBX.

This telephone service provides up to 5 different types of voice communication:

- Standard voice telephony for FleetBroadband and Iridium (vessel <> shore bidirectional)
- Voice telephony for Marlink VSAT (vessel <> shore bidirectional)
- Voice telephony for XChange FX (vessel <> shore bidirectional)
- Universal Card calling service (vessel > shore only)
- Local on-board telephony

Please note

Analogue connectivity is achieved through an optional voice connection card which is End of Life and cannot be purchased anymore.

Only the XChange Power supports this optional analogue connectivity, if a voice is present already.

8.1 Satellite Voice Services

To use the XChange telephone service, connect the box to any FleetBroadband or Iridium Pilot terminal (via its 'OUT' ports) using RJ-11 cables.

Marlink VSAT, Marlink FX, Cobham Sailor FB and Iridium Certus Voice services are available without the need to connect a separate voice cable.

If no analogue voice card is available, the XChange supports IP-based telephony with Marlink XChange Voice, Marlink FX Voice , Iridium Certus Voice and Cobham Sailor FB terminals.

8.2 Phones

8.2.1 Analogue Phones

Any analogue phone with an RJ-11 connection port is supported by the XChange. To connect an analogue phone, make sure you use the correct RJ-11 cable. Up to 3 analogue phones can be connected.

☝ ISDN phones are not supported.

8.2.2 IP Phones, Softphones and Smartphones

IP phones, softphones and smartphones are supported by the XChange.

For each IP phone or softphone, a dedicated SIP account needs to be created in the XChange.

IP phones can be connected using an RJ-45 cable either to a LAN port on the XChange directly or to a LAN port of a network switch.

Softphones use a computer-installed IP calling application.

To use a softphone application, the computer must be connected to the XChange network either via WiFi or cable.

8.2.2.1 Smartphones

Smartphones can only be used if the following are in place:

- There is a WiFi connection to the XChange
- A SIP client application is installed on the smartphone
- The XChange VoiceApp is installed on the smartphone

To connect the SIP client app to the XChange PBX, the username and PIN code are required.

To connect the XChange Voice App, the username and password are required.

Please note

The system automatically creates a SIP account for any created User.

Each User has their own unique local extension number provided during account creation.

8.2.3 Connect an IP Phone

To set up an IP phone:

- Connect the IP phone to the XChange network
- Create a new SIP phone account in the XChange
  - Create a new User in the 'Phones' User group
- Go to the setup menu on the IP phone
- Check that the IP phone is set to receive automatic IP addresses
  - Check that the IP phone received an IP address
- Set up the account details
  - SIP server: xchange-box.com
  - SIP port: 5060
  - SIP account: SIP account name, for example, sipphone1
  - Password: Password provided during account creation

The local extension number is unique to each SIP account and is provided automatically by the system during account creation.

8.2.4 Connect a Smartphone or Softphone

To set up a smartphone or softphone:

- Connect the phone or computer to the XChange network
- Check that the phone or computer is set to receive automatic IP addresses
  - Check that the device received an IP address
- Install a SIP client app or software on your device
- Set up the account details
  - SIP Server: xchange-box.com
  - SIP Port: 5060
  - SIP account: username
  - Password: Password

The local extension number is unique for each User account and is provided automatically by the system during account creation.

8.2.5 Connect via XChange Voice App

To set up a smartphone or tablet with XChange VoiceApp:

- Connect the phone or tablet to the XChange network
- Check that the phone or tablet is set to receive automatic IP addresses
  - Check that the device received an IP address
- Install the XChange VoiceApp on your device
- Set up the account details
  - SIP account: username
  - Password: Password

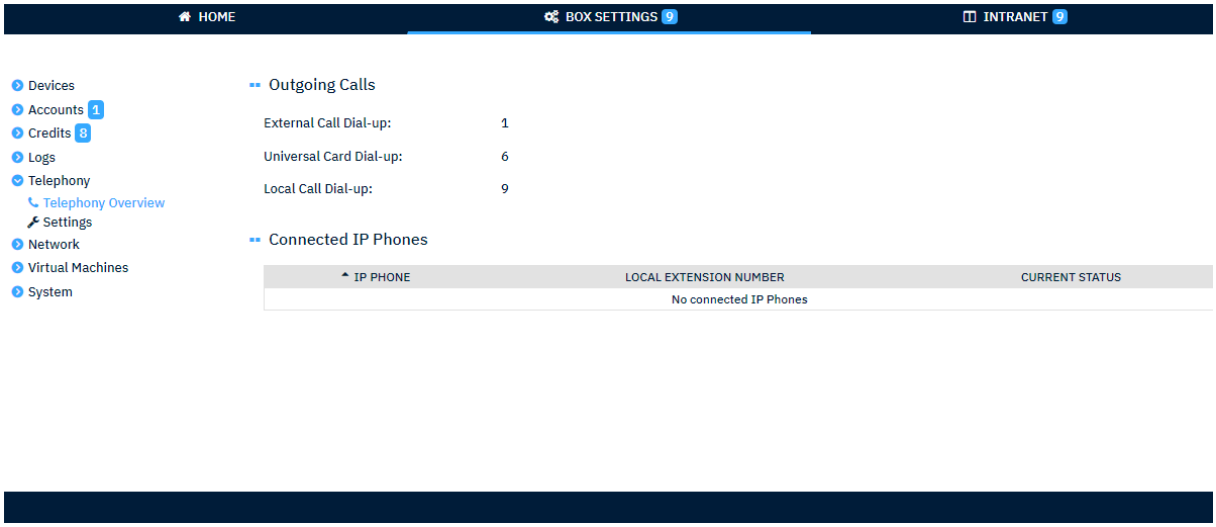
The local extension number is unique for each User account and is provided automatically by the system during account creation.

8.3 Telephony Overview

To view the XChange telephone setup go to: *BOX SETTINGS > Telephony > Overview*.

The overview provides information on which type of telephony service is accessible through which access number. It also provides an overview of connected and currently used SIP accounts.

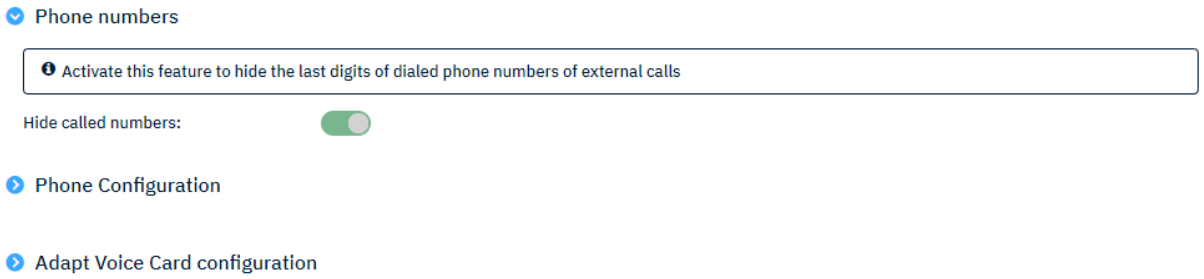
☝ This page only gives information. You cannot edit or change the telephone settings here.



8.4 Telephony Configuration

The telephony configuration can be accessed through: *BOX SETTINGS > Telephony > Settings*.

In the settings menu, it is possible to activate voice destination number anonymisation and to configure connected phones.



8.4.1 Hide Dialled Phone Numbers

The dialled phone numbers, which are shown in the traffic log, can be anonymised. To enable the anonymisation, expand the ‘Phone numbers’ panel and click the ‘ON/OFF’ button.

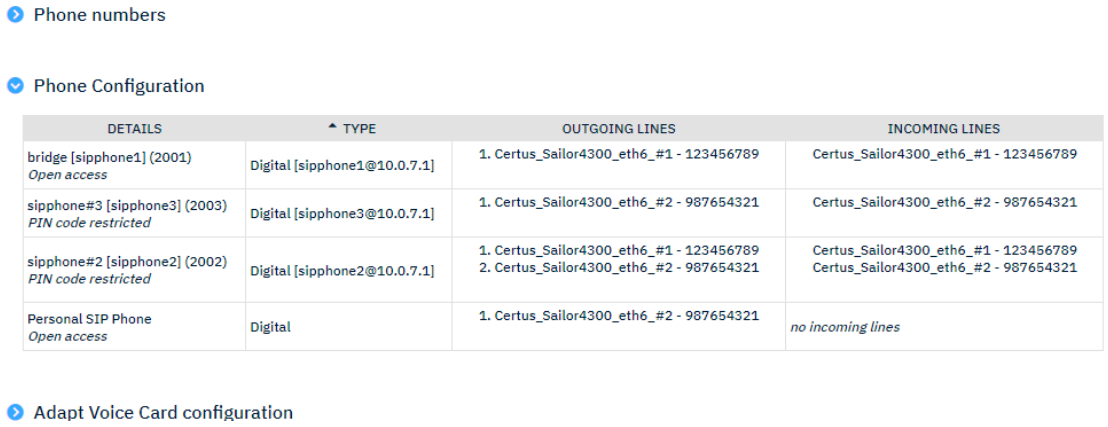
If this feature is enabled, then the last 4 digits of any called phone number are replaced by ‘XXXX’.

8.4.2 Phone Configuration

To configure a connected phone, expand the ‘Phone Configuration’ panel.

The following phone devices are preconfigured in the XChange:

- Personal SIP phone (1x) (used for all private smartphones)
- SIP phone (3x) (used for IP phones)
- Analogue phone (3x if 4-port voice card installed)



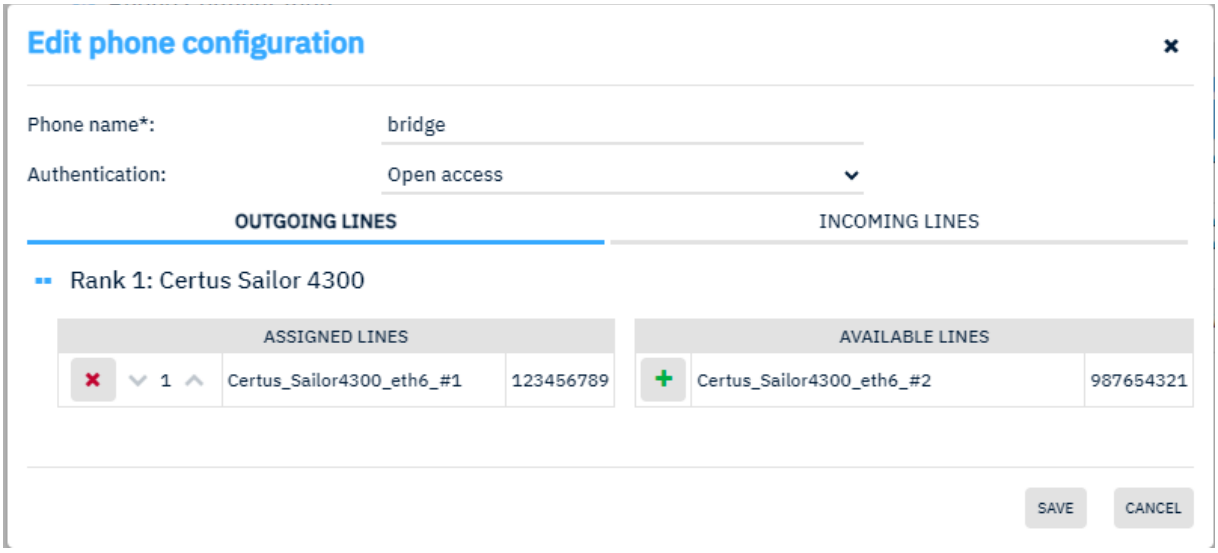
The assignment of available outgoing and incoming voice lines can be changed for each phone.

The XChange automatically selects an outgoing line based on the settings, following a set prioritisation that considers the availability of assigned voice lines.

8.4.3 Voice line Assignment

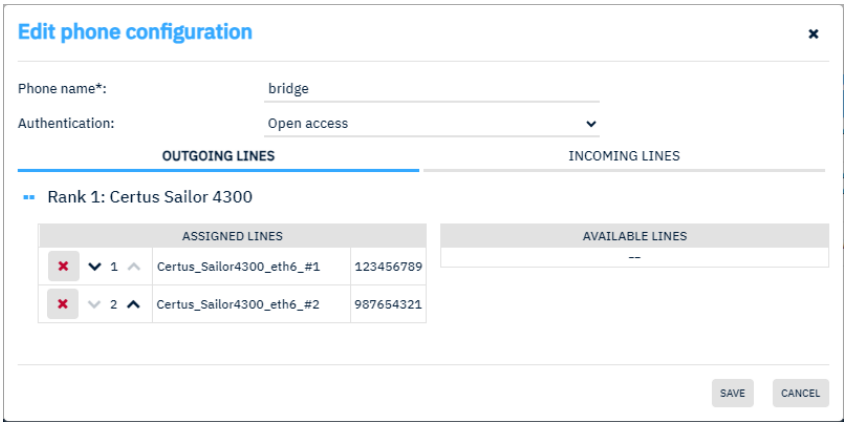
To set the voice line assignment for a phone, select the desired phone in the table and click 'EDIT'.

- If you want, you can change the phone name
- Declare the authentication mode for each phone:
  - 'Open access' = no User authentication required
  - 'PIN code restricted' = User authentication required
- Set the available outgoing phone lines
- Set the prioritisation for outgoing calls
- Set the incoming phone lines



☝Assigned phone lines appear on the left side, non-assigned (available) phone lines appear on the right. To change the assignment of a phone line, click the green '+' to add or the red '-' to remove a line.

To change the prioritisation of a phone line, click the arrows next to the 'x' icon to change the priority.



9. Network

The XChange acts as a network router that manages all connected broadband terminals and the on-board local networks. One of its key features is an embedded multi-network management optionally splitting into several physical networks or trunking multiple networks into 1 physical port. Sophisticated features such as Firewall filter management, remote access and many more can be accessed & managed in the Network section.

9.1 Network Connection

First, connect all network devices such as computers and switches to the LAN ports of the XChange using RJ-45 cables.

- LAN port 1 is pre-set for connecting to the bridge/operation network
- LAN port 2 is pre-set for connecting to the Crew network
- 'ETH' ports 5–8 are optional network ports available on XChange Power only

WARNING

Never connect devices such as computers or network routers, directly to the broadband terminal. Such computers would not form part of the managed network of the XChange and so cannot use its features!

9.1.1 Local Network Extensions

All local networks can be extended to connect multiple network devices together into a single shared network. To extend the corporate or crew network, you can use Ethernet switches and/or a WiFi access point.

As only 1 IP range and only 1 DHCP server can act in one network, ensure that you disable the DHCP service on all connected switches and routers to avoid any IP addressing conflicts.

9.1.2 Network Management Modes

The XChange support all three network management modes in interface assignments.

Access Mode: This mode is used for end devices such as computers, printers, and IP phones. Each port in Access mode can be assigned to only one network with or without VLAN-ID and typically connects to a single device or a LAN. It ensures that traffic from the device/LAN is carried only within its designated network.

Trunk Mode: Trunk mode is used to carry traffic for multiple VLANs between switches or network devices. It allows a single port to handle traffic from multiple VLANs by tagging with the appropriate VLAN-ID. This mode is essential for inter-switch links and maintaining VLAN continuity across the network.

Hybrid Mode: Hybrid mode combines the characteristics of both Access and Trunk modes. It allows a port to manage traffic for multiple VLANs in Trunk mode, but also supports untagged traffic for a native network, similar to Access mode. This flexibility makes Hybrid mode suitable for complex network setups requiring versatile VLAN handling.

9.2 Local Area Networks (vLANs/LANs)

XChange efficiently manages physical networks and VLANs, ensuring seamless connectivity and optimal performance. It provides robust tools for configuring, monitoring, and securing network infrastructures. To manage the network parameters, go to: *BOX SETTINGS > Network > LANs/WANs*.

WARNING

Only IT specialists familiar with virtual networks and network management should change the networking section of XChange.

WARNING when using VLANs

Make sure connected networking peripherals such as Switches and WiFi Access Points are configured accordingly to the XChange networks and interfaces to ensure accessible networks. Any missing or wrong configuration in connected network peripherals may cause an inaccessibility of the XChange.

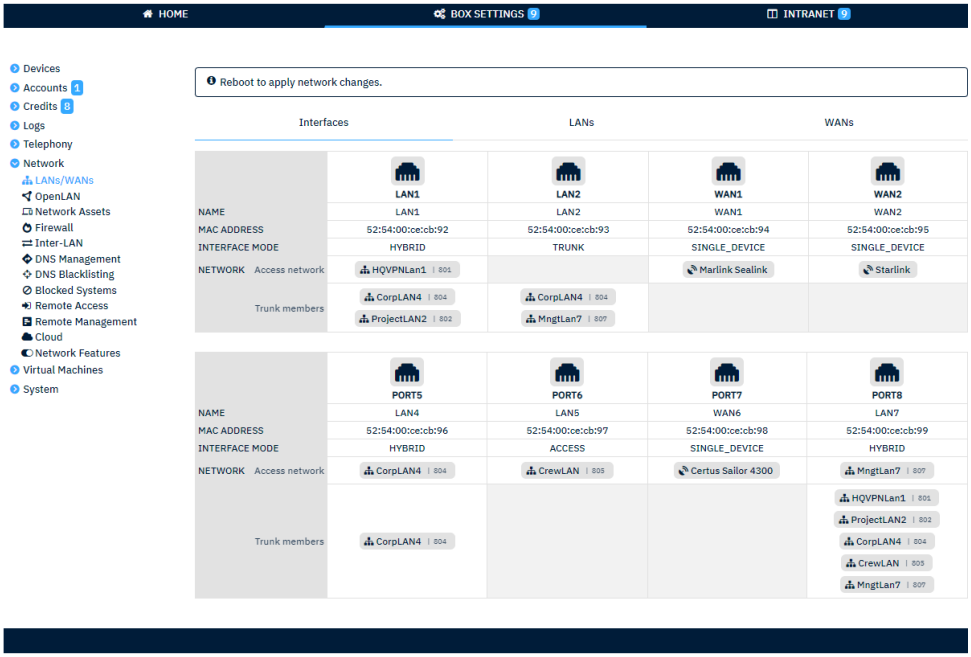
Never delete all networks at once. Before rebooting to apply network changes and interface assignments, ensure at least 1 interface has at least 1 valid network assigned.

Please note

Changes in network settings or interface assignments take effect only after a reboot.

9.2.1 Interfaces

The Interfaces page is different between an XChange Base and XChange Power hardware due to the different amount of network interfaces.



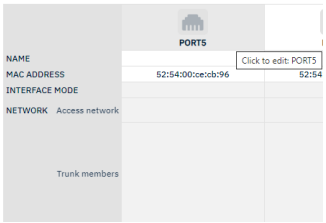
The ‘LANs/WANs’ menu provides an easy overview of interfaces, assigned networks or WAN devices per interface. While interfaces can be defined and changed at any time for local networks, all interfaces connected to WAN devices provide an informative read-only.

The ‘Interfaces’ overview provides the following details for each physical port:

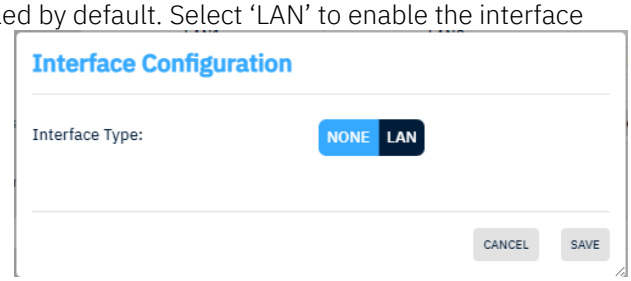
- The name of the physical port as printed on the hardware
- The MAC address of each physical port
- The networking interface mode
- Assigned access network (if any) or communication device (if any)
- Assigned trunk members (if any) or communication devices (if any

9.2.2 Interface Configuration

Any previously created network can be assigned to any interface. Assignments can also be changed at any time.
To assign networks to an interface, click on the interface:

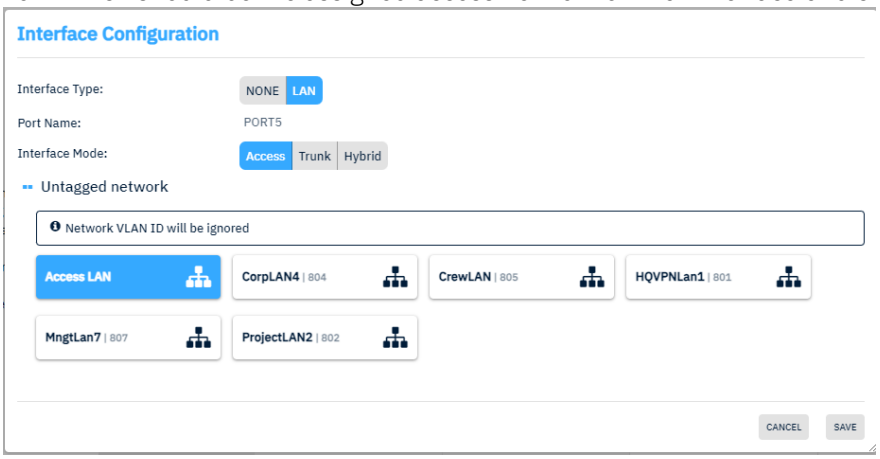


Unused interfaces are disabled by default. Select ‘LAN’ to enable the interface



9.2.2.1 Configuration in Access Mode

Any network can be configured as Access Network. Optionally stored VLAN-IDs are ignored.
Select the network which should be the assigned access network on that interface and click ‘Save’.



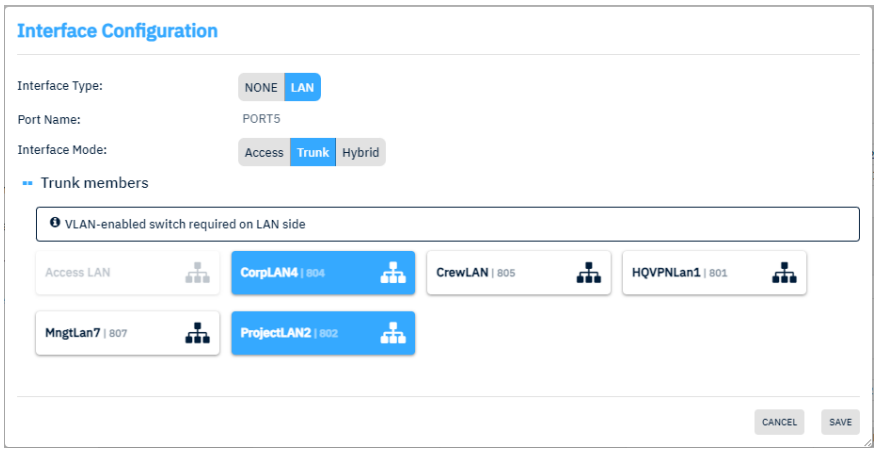
☝ Only 1 network can be assigned as access network to an interface.

☝ Tip!! XChange supports to have the same network assigned on multiple interfaces in access mode.

9.2.2.2 Configuration in Trunk Mode

Any network with a valid VLAN-ID can be configured as Trunk Member. Any number of networks can be assigned as a trunk member.

Set the interface mode to ‘Trunk’ and select the networks which should be members of the network trunk on that interface and click ‘Save’.



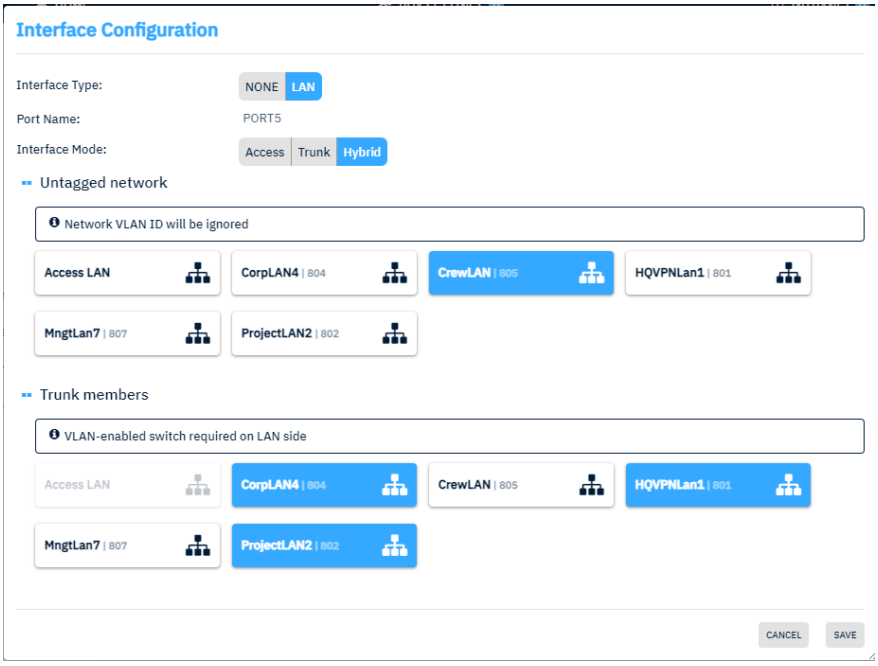
☝ Only networks with valid VLAN-IDs can be assigned as trunk members to an interface. Networks without a VLAN-ID (Access) cannot be selected.

☝ Tip!! XChange supports to have the same network assigned on multiple interfaces in trunk mode.

9.2.2.3 Configuration in Hybrid Mode

In Hybrid Mode its is possible to assign mixed networks to one interface. 1 network can be assigned as Access Network plus any number of networks can be assigned as trunk member.

Set the interface mode to 'Hybrid' and select the network which should be the access network and the networks which should be the members of the network trunk on that interface.

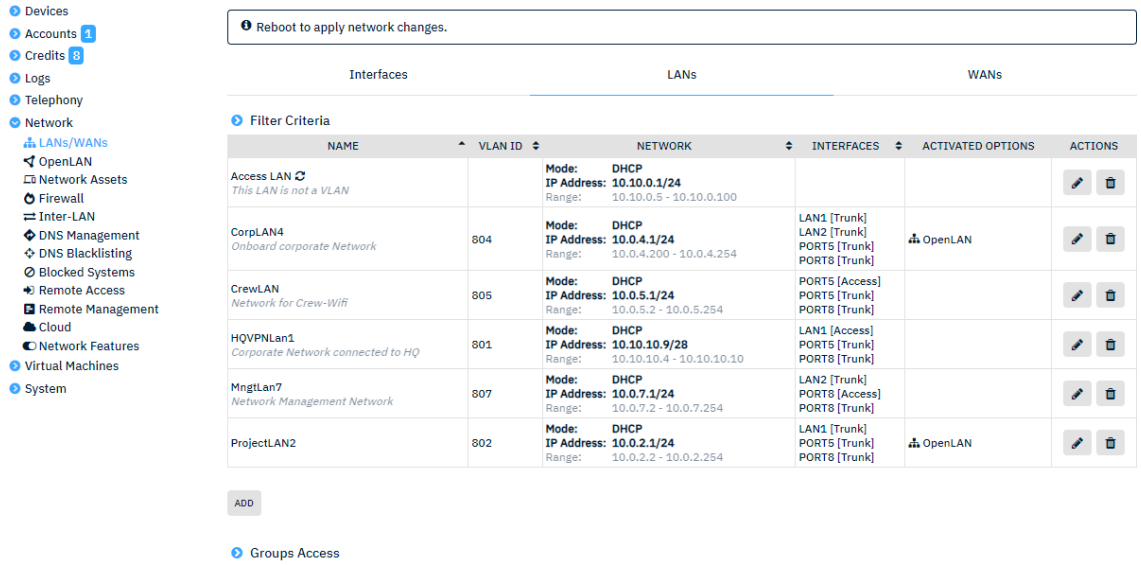


☝ Any network, with or without VLAN-ID can be assigned as access network. Trunk member must have a valid VLAN-ID.

☝ Tip!! XChange supports to have the same network assigned as Access and Trunk member at the same time.

9.2.3 Network Management

To overview existing LANs and to manage networks go to Box Settings > Network > LANs/WANs > LANs:

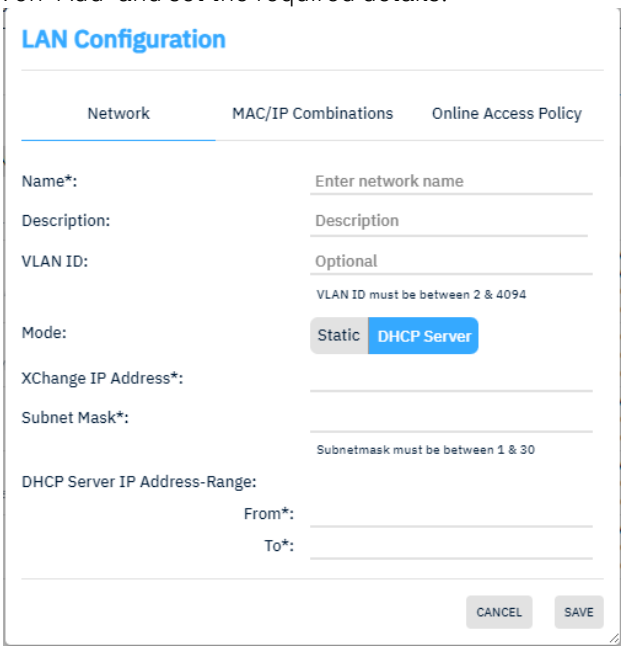


The overview shows all LAN details of existing networks:

	DESCRIPTION
‘NAME	Given name and description.
‘VLAN ID	Given VLAN-ID if any
‘INTERFACES	List of assigned interfaces and used mode
‘ACTIVATED OPTIONS’	Activated OpenLAN, Asset white- or blacklisting
‘ACTIONS’	‘Edit’ and ‘Delete’

9.2.3.1 Create a new LAN

To create a new LAN click on ‘Add’ and set the required details:



Fields marked with * are mandatory fields which must be filled.

Name:

Define a name for each network. The name must have 1-11 alphanumeric characters. Only ‘-‘ or ‘_’ are allowed. No other special characters are possible.

VLAN ID:

A VLAN-ID is optional and only required if the network should be used as trunk member. If no VLANs are used on board, it is possible to create LANs without VLAN-ID.

LAN details

It is possible to change the IP address mode from ‘Static’ to ‘DHCP Server’ and to set the XChange’s local IP address according to the IP address range within that network.

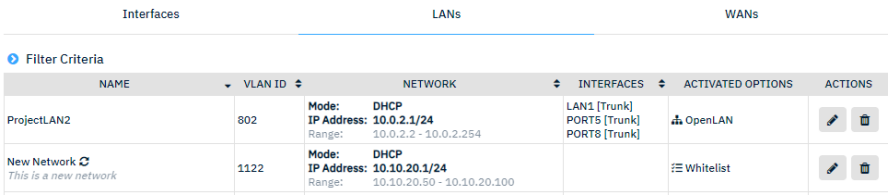
DHCP server IP Address-Range

If DHCP is enabled, the embedded DHCP service requires a valid IP Address-range within the same IP Address-range like the XChange IP Address.

Please note

VLAN-IDs and IP Address ranges must be unique per network. It is not possible to create multiple LANs with the same VLAN-ID or same IP Address range.

After creation the new network will be listed in the LANs overview.



The icon behind the name shows that this network is ready to be created during reboot of XChange.

9.2.3.1.1 Not allowed IP addresses

To avoid conflicts between different networks and the devices on the communication side, several IP address ranges are forbidden from being used.

IP RANGE	CIDR	SUBNET
10.10.102.0	/24	255.255.255.0
10.10.103.0	/24	255.255.255.0
10.11.0.0	/16	255.255.0.0
10.12.0.0	/16	255.255.0.0
10.13.0.0	/16	255.255.0.0
10.0.9.0	/24	255.255.255.0
10.242.16.0	/24	255.255.255.0
172.31.3.0	/24	255.255.255.0
172.31.8.0	/21	255.255.248.0
172.31.16.0	/21	255.255.248.0
172.31.24.0	/21	255.255.248.0
172.31.32.0	/21	255.255.248.0
172.31.40.0	/21	255.255.248.0

Please note

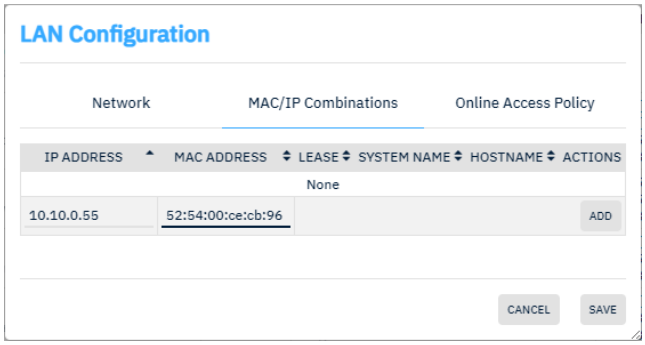
Additionally, don´t use any IP address range on your local networks which is already used by a communication device. The XChange will prevent using communication-device IP address range on your local network to avoid conflicts.

9.2.3.2 MAC–IP Address Combinations

If the DHCP service is enabled in one network, then the XChange provides a MAC–IP address association.

The MAC–IP addressing combination is used in dynamically managed networks to lock an IP address to a specific MAC address of a network client. This means that this network client receives the same local IP address every time it connects to the network.

While creating a new LAN, any planned MAC/IP combination can be set immediately.



Combining a MAC to an IP address after network creation

To make a combination on a:

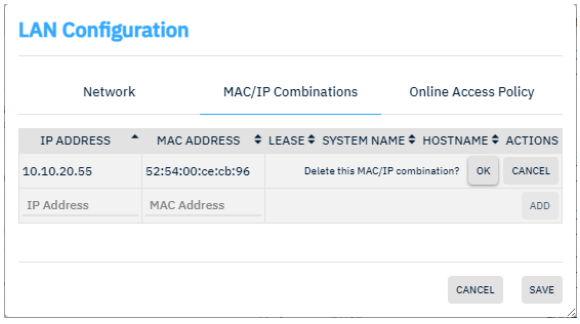
- Go to *BOX SETTINGS > Network > LANs/WANs > LANs*
- Click the 'Edit' icon of the network
- Go to MAC/IP combinations
- Set an IP address
- Set the MAC address
- Click 'Add'

☝ Tip!! To ease the IP–MAC address association, return to the network settings after the network is established. In MAC/IP combinations all known network assets will be listed automatically. Click on an active network asset the icon'Add static lease'. This avoids the need to manually type in the IP and MAC addresses of all the network clients.

Deleting a MAC/IP combination

To delete a combination:

- Go to *BOX SETTINGS > Network > LANs/WANs > LANs*
- Click the 'Edit' icon of the network
- Go to MAC/IP combinations
- Click the 'Delete Static Lease' icon
- Click 'OK' to confirm or 'Cancel'
-

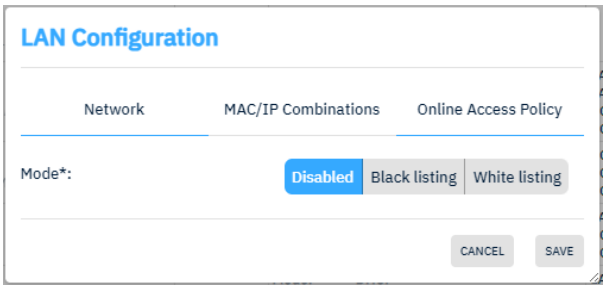


9.2.3.3 Online Access Policies

The online access policy can be used to restrict online data access for network clients on each local network separately. When a client is restricted from online access, nobody can use that client (for example, that PC) to access the Internet.

Available modes are:

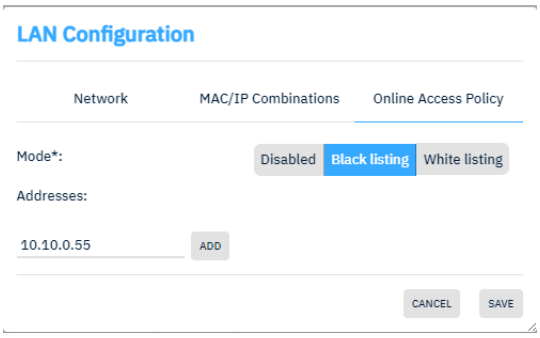
- Disabled
  - No online access restrictions
- Blacklisting
- Whitelisting



To set up an online access policy, select the preferred mode:

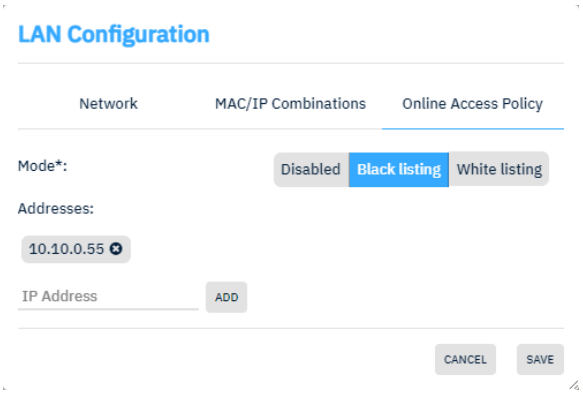
Blacklisting

In ‘Black listing’ mode, it is possible to restrict (blacklist) specific network clients from online data access.



To set up the blacklisting:

- Select ‘Black listing’
- Enter the IP address of the network client
- Click ‘Add’
- Repeat IP for every IP address
- Click ‘Save’ to store the settings

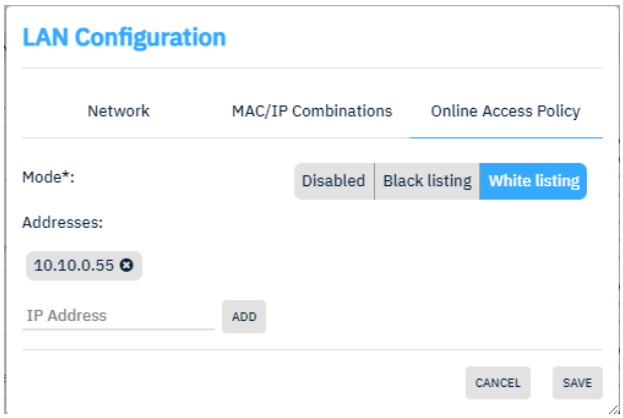


☝ Tip!!: Do the IP–MAC address assignment before you blacklist the network client.

☝ Tip!!: Click the ‘X’ icon behind an IP address to remove it again.

Whitelisting

In ‘White listing’ mode it is possible to generally restrict online data access for all network clients and then to allow (whitelist) online data access for specific network clients only.



To set up the whitelisting:

- Select ‘White listing’
- Enter the IP address of the network client
- Click ‘Add’
- Repeat IP for every IP address
- Click ‘Save’ to store the settings

☝ Tip!! Do the IP–MAC address assignment before you whitelist the network client.

9.2.4 Edit LAN Settings

Any LAN setting can be changed at any time.

- Go to *BOX SETTINGS > Network > LANs/WANs > LANs*
- Click on the ‘Edit’ icon of the LAN
- Change the LAN or DHCP server details
- Change the IP addressing if required
- Add or remove a VLAN-ID if required
- Assign new MAC to IP addresses or remove any existing
- Define or deactivate an online access policy
- Click ‘Save’, or ‘Cancel’
- Reboot the system to apply the changes

9.2.5 Delete LANs

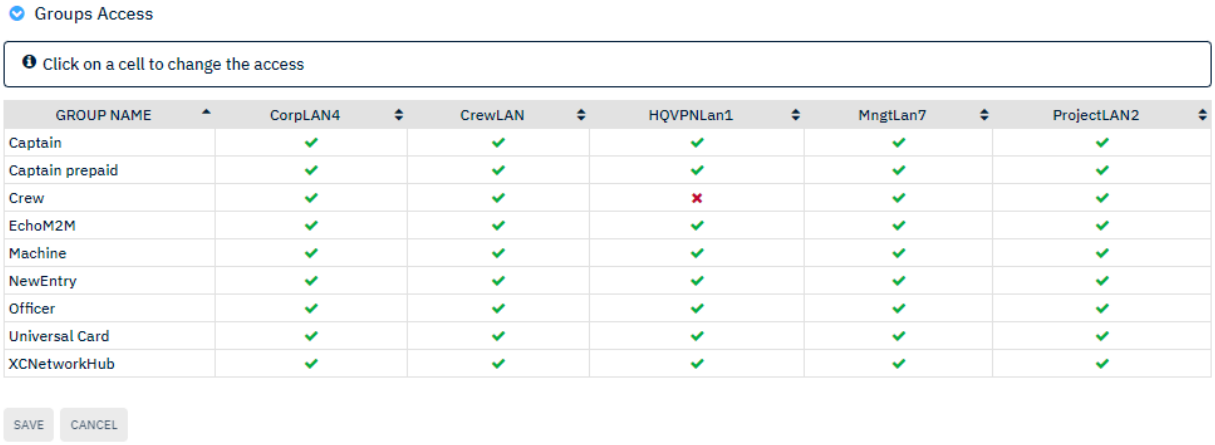
Any LAN can be delete at any time if it is not required anymore.

- Go to *BOX SETTINGS > Network > LANs/WANs > LANs*
- Click on the ‘Delete’ icon of the LAN
- Click ‘Delete’ to confirm or ‘Cancel’
- Reboot the system to apply the changes

WARNING
Never delete all LANs at once. Ensure that at least 1 LAN remains active after reboot

9.2.6 Groups Access

The 'Groups Access' panel gives an overview of all User groups available on an XChange system. This overview shows, for each LAN *assigned to an interface*, which User group is allowed to access the Internet through this network.

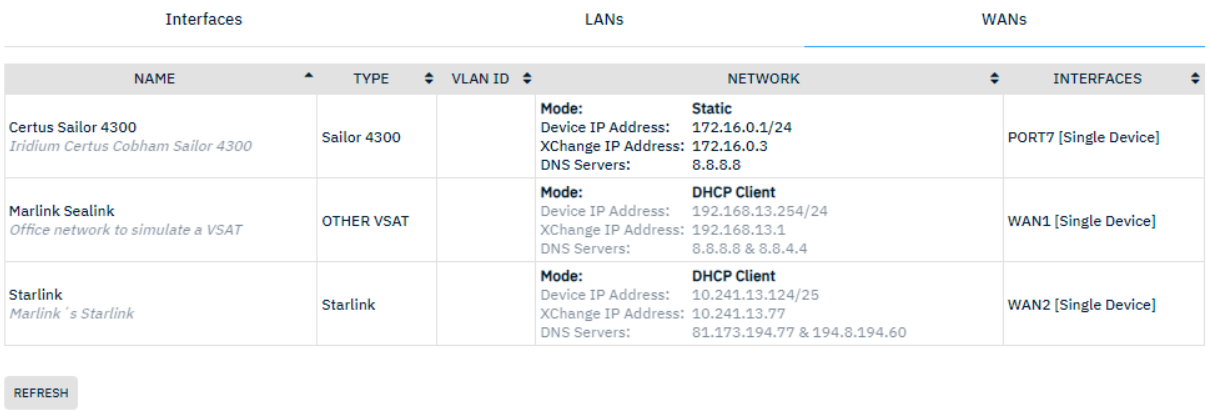


The opened-lock icon shows that a group can access the Internet. The closed-lock icon shows that a group is not allowed to access the Internet.

To change the internet access for a user group within a network, click the corresponding field in the matrix.
Click 'Save' to confirm or 'Cancel'

9.3 Wide Area Networks (WANs)

To view the XChange WAN setup, go to: *BOX SETTINGS* > *Network* > *LANs/WANs* > WANs



The 'WAN Details' provides the following detailed information for each physical WAN:

- The WAN device name and type
- The IP retrieving mode used
- Gateway IP addresses from connected terminals
- XChange IP addresses communicating to the terminals
- The assigned interface and networking mode

You cannot change the WAN settings in the web interface. If you need to make changes, contact Marlink support.

9.4 Open LAN

A whole LAN can be defined as ‘Open LAN’, which disables the per default required user authentication. Any computer/user connected to an Open LAN has immediate internet access. To ensure highest security and access control, all control mechanisms normally available within user-group management are available for Open LANs including assignment of communication devices, Sealink data priorities, Firewall, DNS whitelisting and daily access restrictions.

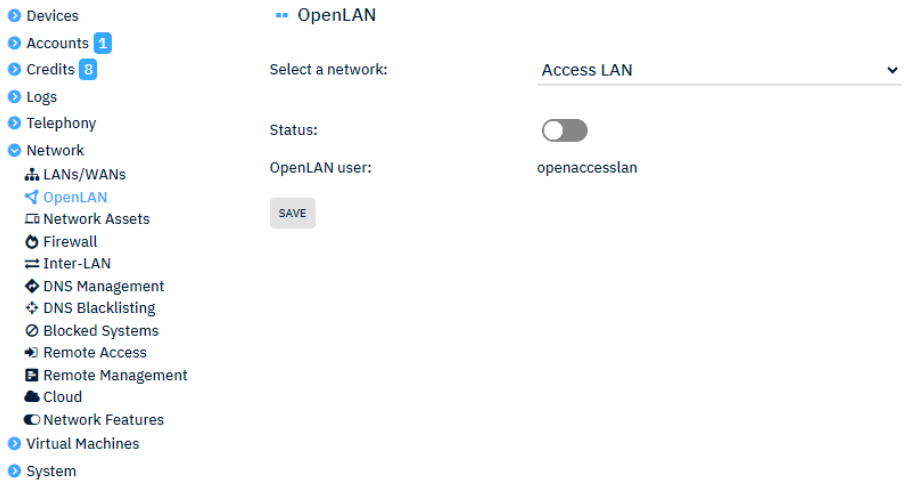
Please note

Activating a Local Network as ‘OpenLAN’ will bypass the user authentication and the embedded local prepaid system.

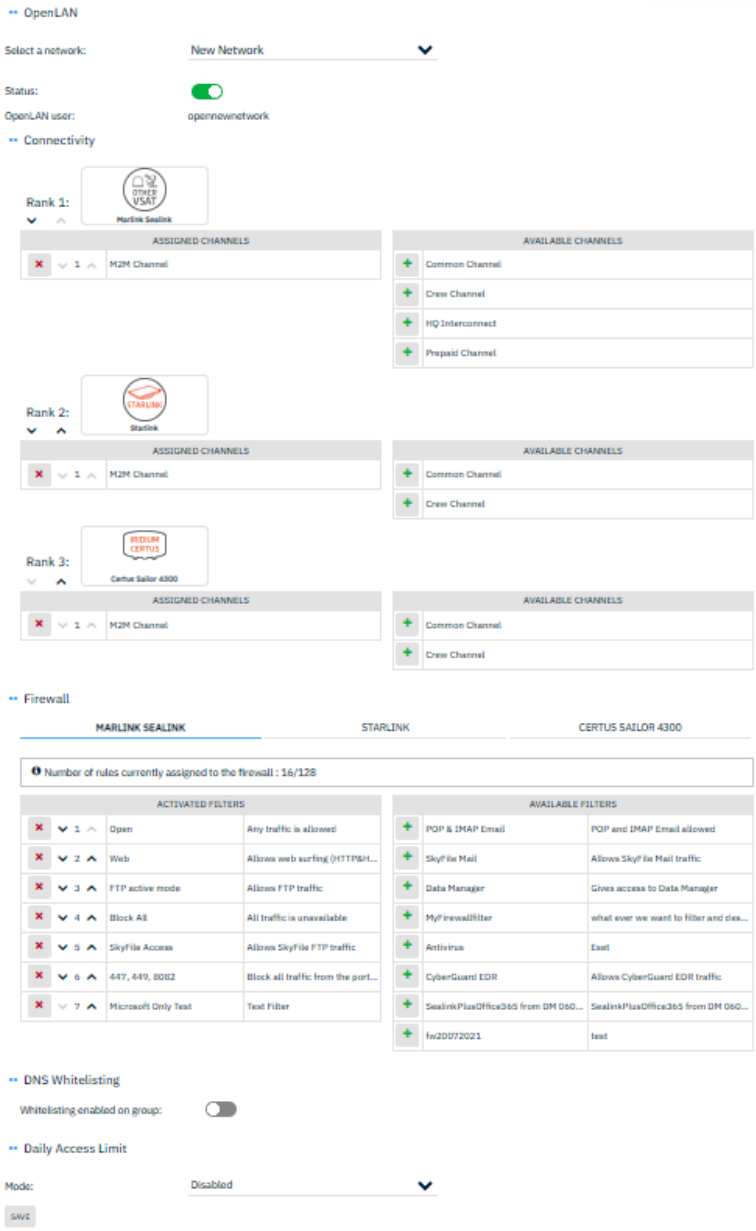
Users connected to an Open LAN can still access the XChange interface but not connect to the internet with their personal account.

To define a local network as ‘Open LAN’ click the ‘Edit’ button. You are redirected to a new page where the status can be changed to ‘On’.

To define a LAN as ‘Open LAN’ go to Box Settings > Network > Open LAN.



Select a network from the drop-down menu and activate the status.



After feature activation it is possible to define the online access policy for this network. The Connectivity assignment, Firewall, DNS Whitelisting and Daily Access Limits can be defined.

The way how to setup the online access features does not further differ compared to the user-group based setup process. Please read the detailed instructions in the user group management paragraph carefully.

To store the defined feature settings, click the ‘Save’ button.

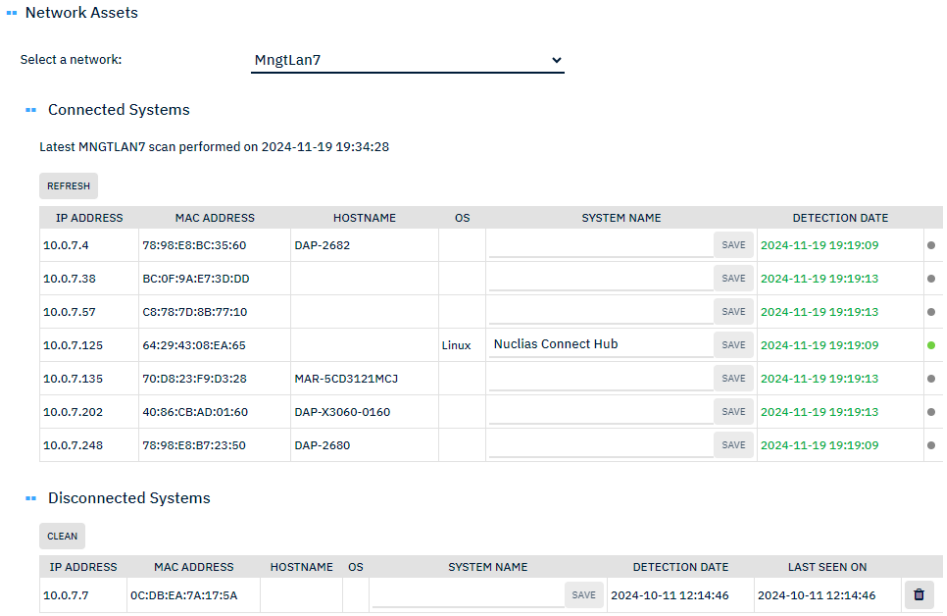
Each local network can be set as ‘Open LAN’ with the above mentioned security parameter individually.

Please note

After Open LAN activation, the XChange will automatically create a dedicated user containing the LAN name with a prefix ‘Open’. All special characters will be removed.

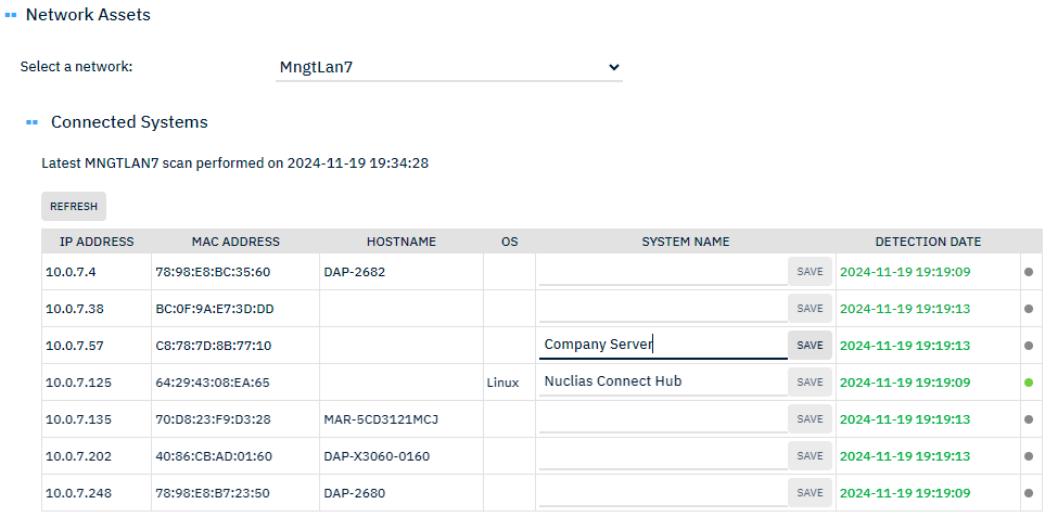
9.5 Network Assets

The ‘Network Assets’ provide an overview of all network clients for each local network. The ‘Network Assets’ shows detailed information of all network clients identified as connected and an overview of disconnected systems:



The green ‘user’-icon shows the logged in XChange username on that particular network client.

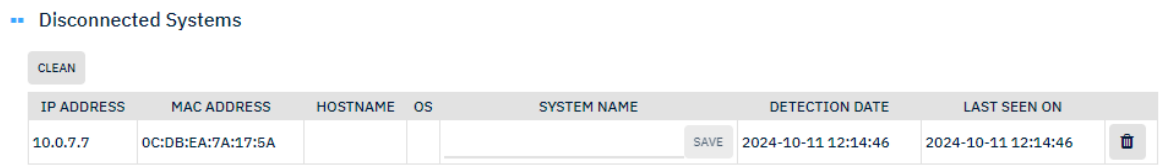
You can give each known network client a System Name as you prefer. Just click in the line and ‘Save’ after the name is defined.



To refresh displayed data, by clicking the ‘Refresh’ button the system will scan the network again.

After a few seconds the screen refreshes and displays the updated overview again.

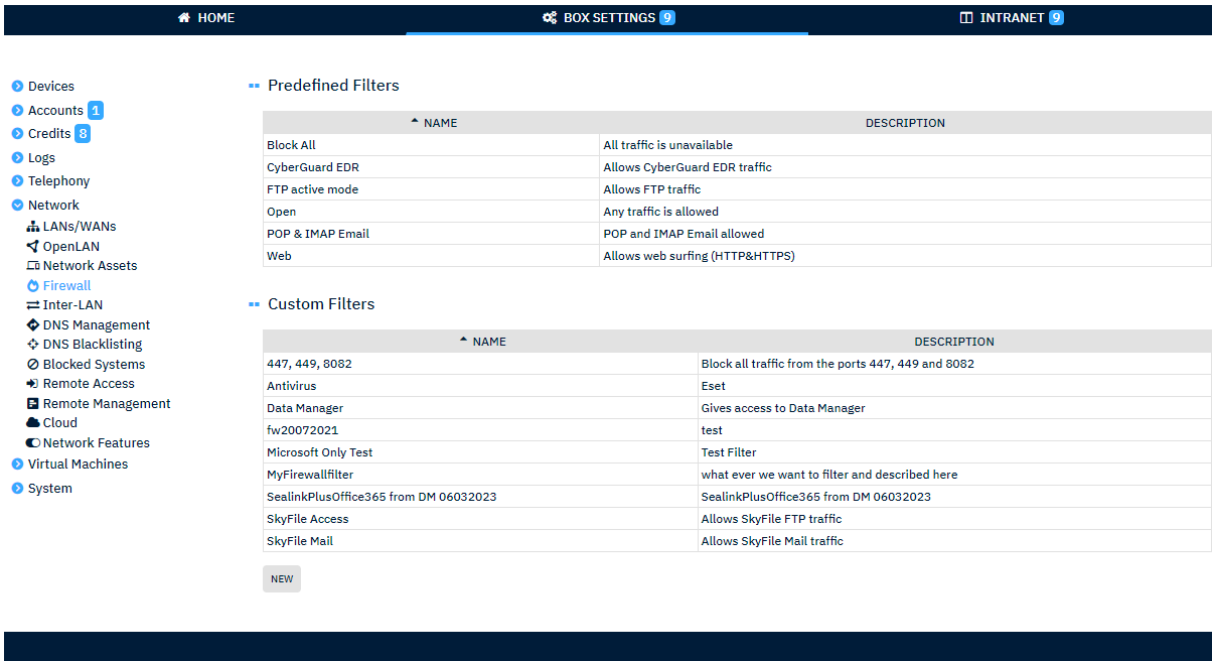
To clear the table of disconnected systems, click the ‘Clean’ button.



9.6 Firewall Filter Management

To manage firewall filters, go to: *BOX SETTINGS > Network > Firewall*.

The firewall page inside the 'Network' subsection represents the core of the embedded firewall feature of the XChange. On this page, the Administrator can create, edit or delete firewall filters.



The embedded firewall is created to support the Administrator with optimal filter management resources.

The firewall filters that are managed here are allocated to User groups and to broadband terminals connected to the system.

9.6.1 Predefined Firewall Filter

The XChange provides a full set of predefined firewall filters covering the most popular types of traffic and requirements.

Predefined filters are a preconfigured set of rules that contain combinations of the most common IP protocols and services used for satellite communications. They ensure that only specific applications or protocols are allowed to pass through the XChange (also known as whitelisting).

The predefined filters are:

	DESCRIPTION
'BLOCK ALL'	Blocks any type of data traffic
CYBERGUARD EDR	Allows EDR update communication
'FTP ACTIVE MODE'	Allows FTP traffic. ☝ Software must be set to 'active mode'
'OPEN'	Any traffic is allowed. ☝ This filter is preselected for all new terminals and User groups!
'POP AND IMAP EMAIL'	Allows POP and IMAP email communication
'SKYFILE MAIL'	Allows SkyFile Mail traffic
'WEB'	Allows web (Internet) access (HTTP and HTTPS)

Please note

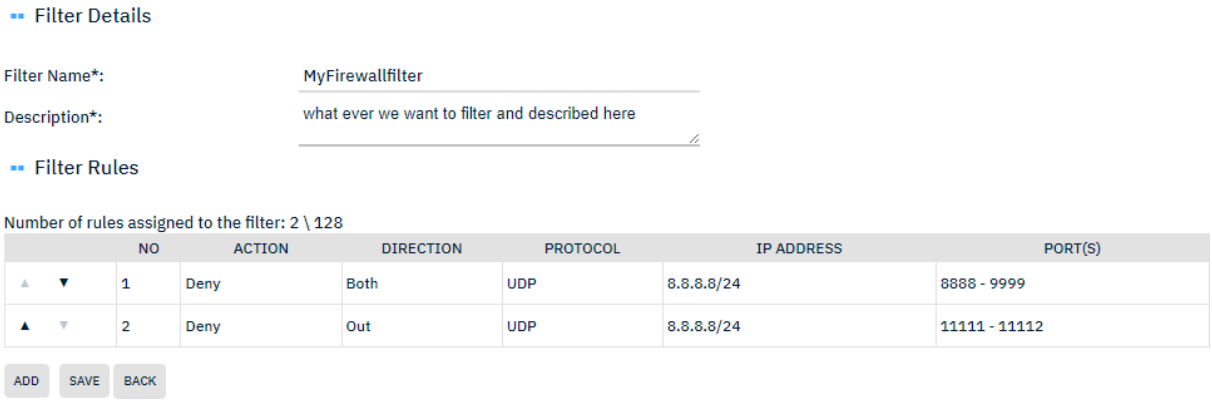
The device firewall offers more predefined filters which are NOT shown in the firewall management page. Marlink prohibits access to these filters to avoid accidently changing system-critical filters such as XChange System traffic.

9.6.2 Create a Firewall Filter

In addition to the predefined firewall filter, the Administrator can create a personal firewall filter to meet specific firewalling requirements.

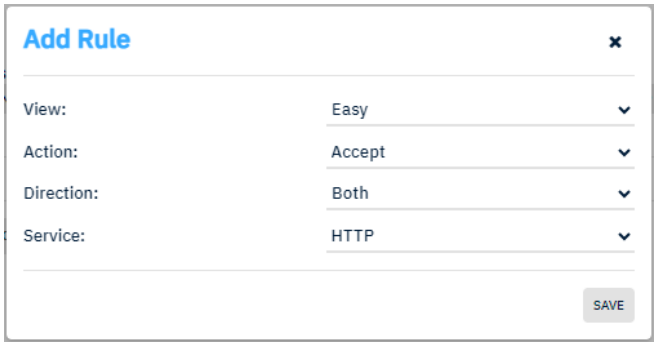
To create a personal firewall filter:

- Go to *BOX SETTINGS > Network > Firewall*
- Click ‘New’
- Type in a filter name and description
- Click ‘Add’
- Select ‘Easy’ or ‘Expert’
- Click ‘Save’
- Repeat steps 3–5 to add more rules
- Set the rule sequence (if more than 1 rule is applied)
- Click ‘Save’ to save the settings



Easy mode

The easy mode enables a filter rule to be created based on predefined services.

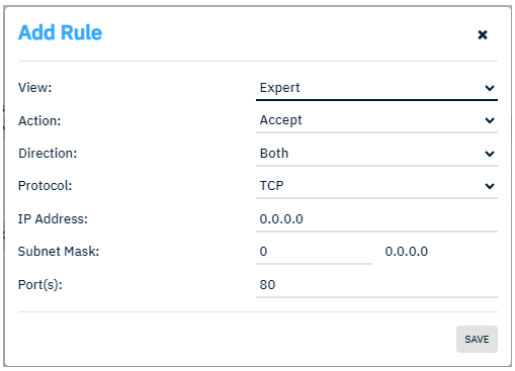


To create a rule in easy mode:

- Select the action
- Select the direction
- Select a service
- Click ‘Save’ to save the rule

Expert mode

The expert mode enables a detailed filter rule to be created based on protocols, IP addresses and ports.



To create a rule in expert mode:

- Select the action
- Select the direction
- Select a protocol
- Set the designated IP address and subnet mask
- Set the ports
- Click 'Save' to save the rule

Available parameters

Action:

There are 2 possible actions in the 'Action' drop-down list: 'Accept' or 'Deny'. These specify whether the rule will whitelist ('accept') or blacklist ('deny') the service that has been selected in the XChange.

Direction:

There are 3 directions available in the 'Direction' drop-down list: 'In', 'Out' and 'Both'. These specify whether the rule will accept the service for incoming 'In' or outgoing 'Out' communication only.

To enable a service to have bidirectional communication, use the preset 'Both' option.

IP Protocol/Services:
'Protocol' and 'Service' define which protocol (TCP, UDP, etc.) or services (FTP, DNS, etc.) will be affected by the rule.
'Protocol' enables the creation of traffic profiles based on network layer 3 protocols (ICMP) or layer 4 protocols (UDP, TCP). Go to the following link for more details:
http://en.wikipedia.org/wiki/OSI_model.

List of preconfigured protocols

- ICMP: Network control protocol. Mostly used by ping and trace-route to check network paths and connectivity
- TCP:Connection-oriented reliable transport protocol. Concerns most Internet-based applications (web browsing, email, file transfer, etc.)
- UDP: Connectionless 'best effort' transport protocol. Mostly used for streaming applications and server name resolution

The preconfigured protocols are displayed in the 'Expert Mode' and in 'Filter Rules' overviews.

List of preconfigured services

- DNS: Domain name resolution messages
- FTP (control): FTP control traffic
- FTP (data): FTP data traffic
- HTTP: Web traffic on port 80
- HTTPS: Secure web traffic on port 443
- ICMP: ICMP traffic (trace-route, ping, etc.)
- IMAP: Email traffic on IMAP protocol
- IMAP SSL: Secure email traffic on IMAP protocol
- POP3: Email traffic on POP protocol
- SMTP: Email traffic on SMTP protocol
- SkyFile Mail: Marlink SkyFile Mail traffic
- NTP: Network Time Protocol
- Feedback (TCP): Special feedback service for XChange Media (Not used anymore)

The preconfigured services are only displayed in 'Easy Mode'.

Rules Sequence

When more than one rule is configured, it is important to make sure that the sequence of rules is in the correct order. The XChange firewall will treat incoming and outgoing traffic sequentially, based on the order in which the rules are displayed from top to bottom.
The 1st rule in the list is treated first (followed by the 2nd rule, and so on). Rules in the wrong order are likely to produce unexpected behaviour.

In order to change the sequence, use the up/down arrows on the left to move the rules.


Number of rules assigned to the filter: 2 \ 128

	NO	ACTION	DIRECTION	PROTOCOL	IP ADDRESS	PORT(S)
▲ ▼	1	Accept	Both	UDP	0.0.0.0/0	53
▲ ▼	2	Accept	Both	TCP	0.0.0.0/0	443

9.6.3 Edit a Firewall Filter

To edit a firewall filter, go to *BOX SETTINGS > Network > Firewall* and select the specific filter.

Click 'Edit' to enter the page on firewall filter details. On this page, you can:

- Change filter information, such as name and description
- Add new rules
- Edit/delete existing rules
- Change the order of rules
- Click 'Save' to save the changes

9.6.4 Delete a Firewall Filter

To delete a firewall filter, go to *BOX SETTINGS > Network > Firewall*.

Click on the filter name to select the filter. Click 'Delete' below the list

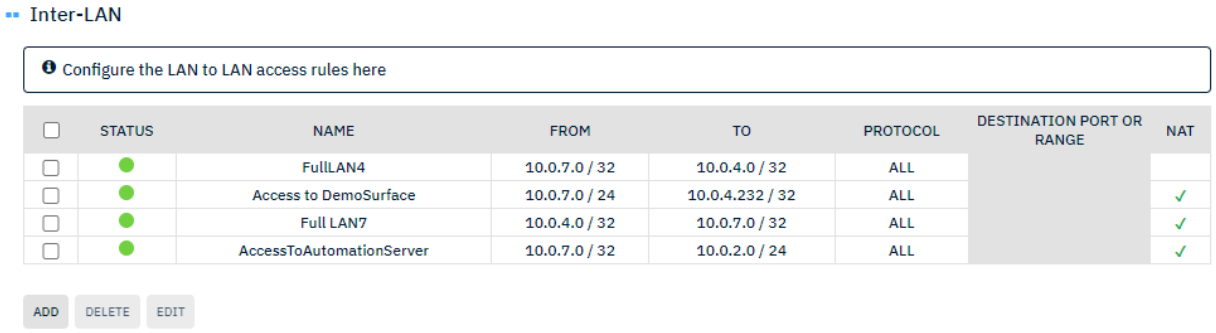
Please note

To avoid unwanted firewall behaviour, you can only delete a firewall filter when there is no User group or terminal associated with this filter.

9.7 Inter-LAN Access Management

The "Inter-LAN" management allows setting up access rules between different LANs managed by XChange. It allows specific network clients connected on different networks, with different IP address schemes, to communicate directly.

The overview page shows a list of existing inter-LAN access rules, their status and offers to add, delete or edit rules.



The option is very simple and can be configured on a flexible way. From full access between networks, up to very restricted, secured, access just between 2 network clients through a specific Protocol and Port.

Optionally, an internal 'NATing' can be activated per rule. If activated, the destination system will receive requests from the XChange-IP within the same network. If not activated, the destination system will receive requests from the original IP address of the accessing computer.

The Inter-LAN rules are based on internal networking and IPs. All rules work bi-directional. This means, just one rule must be defined to allow a inter-LAN communication between 2 systems. There is no need to create unique rules for requests and answers. No user-based access management is offered herewith.

The overview page shows a list of existing inter-LAN access rules, their status and offers to add, delete or edit rules.

Please note

The system does not check for conflicts between those rules. It´s not recommended to create more than 50 access rules.

9.7.1 Examples for Inter-LAN rules:

Access to a Web Server on LAN 1 from the whole LAN2:

	STATUS	NAME	FROM	TO	PROTOCOL	DESTINATION PORT OR RANGE	NAT
☐	●	LAN2 access WebServer	10.0.2.0 / 24	10.0.1.10 / 32	TCP	443	

Full access between all LAN1 and LAN2 network clients: (Not Recommended!)

	STATUS	NAME	FROM	TO	PROTOCOL	DESTINATION PORT OR RANGE	NAT
☐	●	Full access between LANs	10.0.2.0 / 24	10.0.1.0 / 24	ALL		

Access to a Web Server on LAN1 from some computer on LAN2:

In this example, 14 clients of LAN2 can access the Web Server. If specific PCs should access a system on another LAN, one rule per accessing computer should be setup.

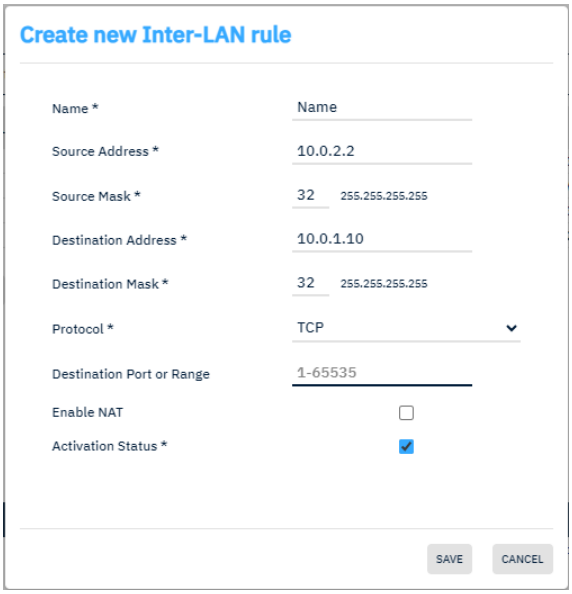
	STATUS	NAME	FROM	TO	PROTOCOL	DESTINATION PORT OR RANGE	NAT
☐	●	Some Clients access to WebServer	10.0.2.0 / 28	10.0.1.10 / 32	TCP	443	

Access to a Web Server on LAN1 from one specific computer on LAN2:

	STATUS	NAME	FROM	TO	PROTOCOL	DESTINATION PORT OR RANGE	NAT
☐	●	Unique access for 1 Computer	10.0.2.100 / 32	10.0.1.10 / 32	TCP	443	

9.7.2 Creation of Inter-LAN rules

To add a new inter-LAN rule, click the ‘Add’ button and fill all required information according the needs.



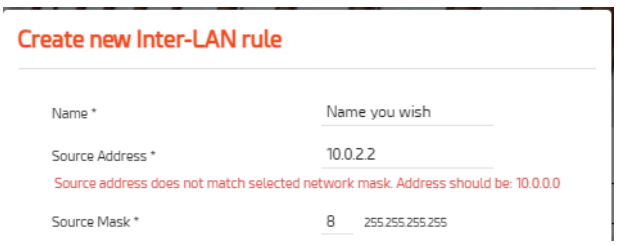
Fields to be added and their meaning:

- “Name”: Set a unique name
- “Source Address”: IP address(es) of clients which should access another client
- “Source Mask”: Subnet mask to restrict granted IP addresses to access
- “Destination Address”: IP address(es) of the system to be accessible
- “Destination Mask”: Subnet mask to restrict the number of accessible IP addresses
- “Protocol”: Option to limit communication to a specific protocol:
    - ICMP
    - IGMP
    - TCP
    - UDP
    - ALL
- “Destination Port or Range”: Option to limit communication to a specific or to a range of ports
- “Enable NAT”: If checked, the accessing IP address will be masquerated with XChange´s own IP
- “Activation Status”: To enable or disable any rule

Once all details are checked, press the ‘Save’ button to store the new rule.

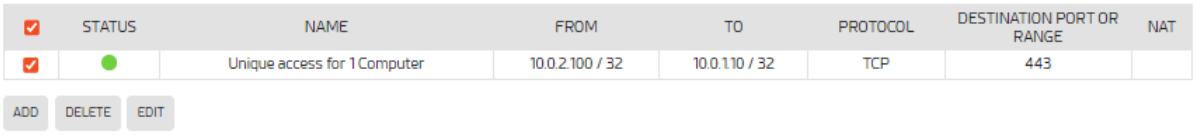
Automatic check of entered rules:

The system does not check for conflicts between different rules. The system checks if the combination of IP address and subnet mask is valid. If wrong information is used, the system will decline to save a faulty rule:



9.7.3 Edit of Inter-LAN rules

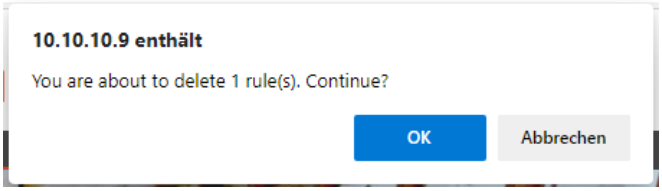
To edit an existing inter-LAN rule, or to change the activation status, mark the rule and click the ‘Edit’ button.



9.7.4 Deletion of Inter-LAN rules

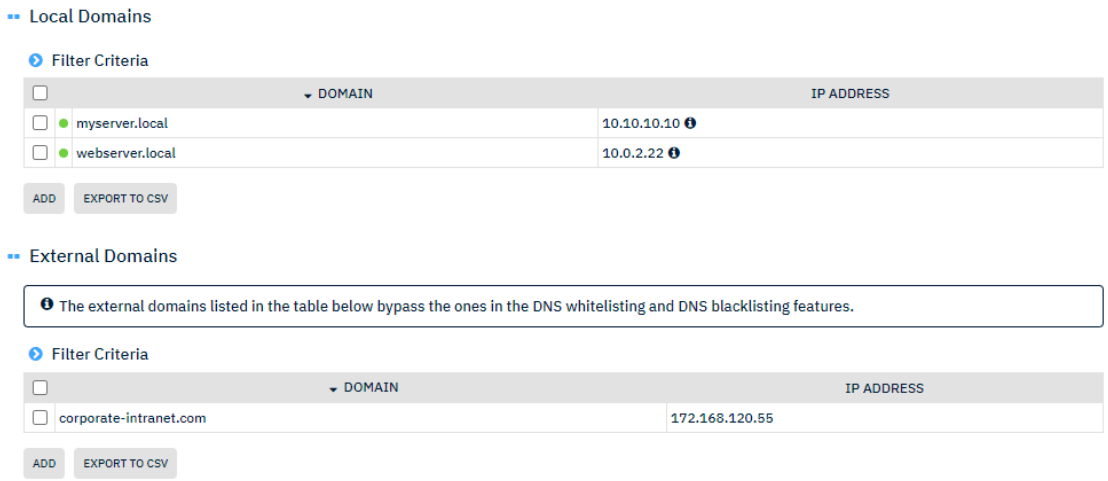
To delte an inter-LAN rule, mark the rule and click the ‘Delete’ button.

A popup window will request a confirmation. If the rule should be deleted, press the ‘OK’ button in the popup window.



9.8 DNS Management

The DNS management option is an embedded DNS Server in the onboard XChange system. It allows the Domain Name Resolution execution locally on board, by XChange. The local DNS server is fully combinable with the inter-LAN access, offering a very user friendly way to manage access to for instance Web Servers. Thanks to the DNS server, users do not need to remember the IP address of the system to access, but a simple local domain can be remembered instead. Further the DNS server can be used to simplify access to shore-based systems if a VPN Network between the XChange and the Headquarter network is established.



The DNS management offers local and a remote domains to be created.

Local Domains:

Local domains are used to simplify the access to systems/servers locally on board.

External Domains:

External domains can be used to add simple domain names for any server / IP address outside the XChange network, such as for example servers in the Headquarter network.

Please note

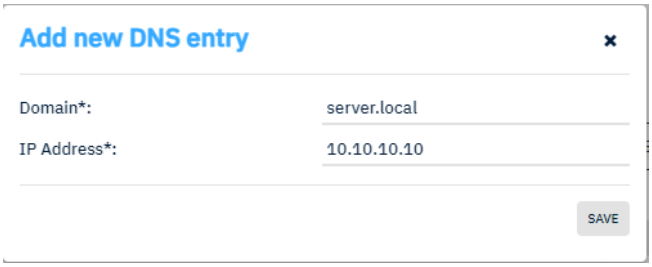
The external Domain option can bypass any DNS Blacklist- or Whitelist options defined. Please validate, that any external domain setup is valid.

It´s not recommended to setup any domain name of existing internet sites such as for example “google.com” to avoid conflicts.

9.8.1 Adding new DNS entries

The instructions, how to add a new DNS entry is identical for ‘Local Domains’ and ‘External Domains’.

To add a new DNS entry, click the ‘Add’ button and fill the fields accordingly.



Click ‘Save’ to store the new DNS entry.

☝ The domain name must be written in small letters only. Capital letters are not possible. Depending on the used systems on board, the domain ‘.local’ should be avoided to avoid future complications if a Linux-based system is used.

9.8.2 Edit DNS entries

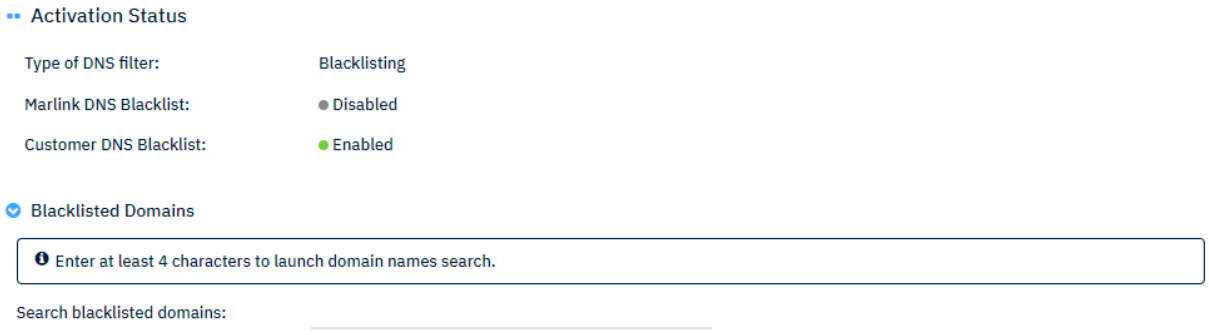
To edit an existing DNS entry, or to change the activation status, mark the rule and click the ‘Edit-option’ button required.

☝ The ℹ -icon next to the IP address informs, if no network client uses this IP address.

9.9 DNS Blacklisting

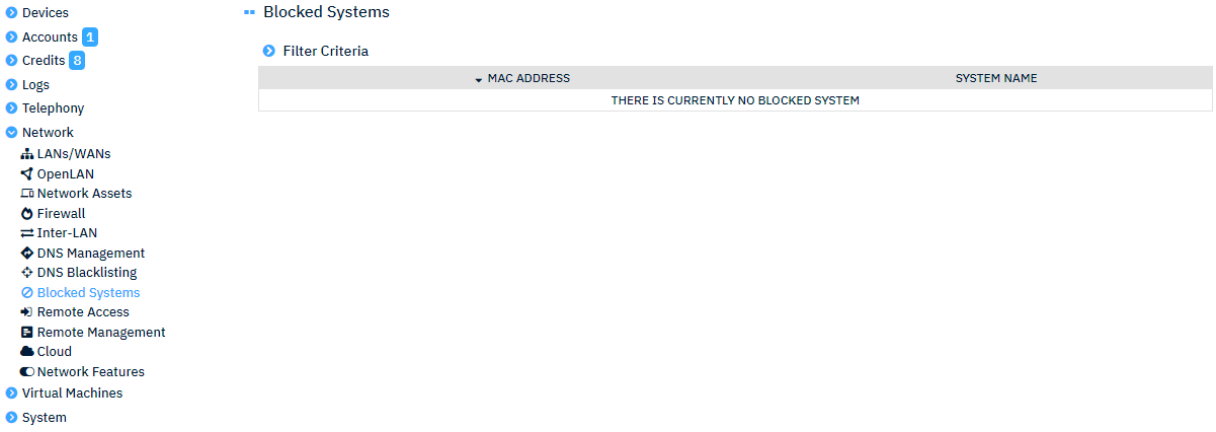
A DNS blacklisting is setup centrally and acts on the whole vessel. Blacklisted domains cannot be access by any person or system on board, independent of the user group or communication device in use. Onboard it is not possible to edit the DNS Blacklisting feature. Exclusively through Portal 360 it is possible to activate and define blacklisted DNS entries.

Blacklisted DNS can be searched by simply typing at least 4 digits.



9.10 Blocked Suspicious Systems

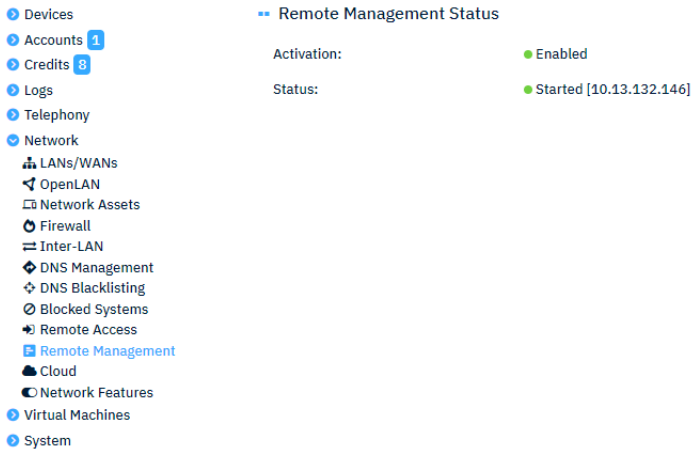
The new MAC address Blacklisting empowers Marlink´s Cyber Detection service.
The MAC Blacklisting feature manages a blacklist of MAC Addresses which are blocked from external communication. Following the detection of a threat using Cyber Detection, a typical short-term corrective action is to quarantine the infected machine(s) so that it/they can no longer communicate externally. After having resolved the threat on the infected machine(s), these can be removed from the MAC blacklist and they will be able to communicate externally again



9.11 Remote Management

The remote management functionality is required to allow User, credit administration or IT configuration management from shore via Portal360 without the need to remotely access an XChange.

By default, the remote management function is enabled. This page provides additional information, such as assigned IP address for trouble shoot purposes.



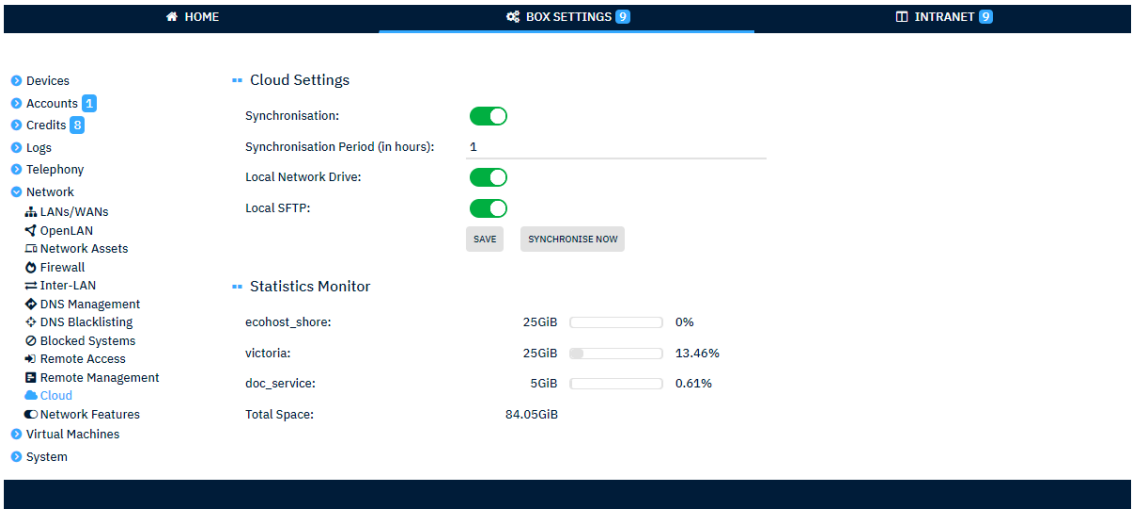
WARNING

Remote management is a core functionality for XChange shore-based management. Marlink recommends not disabling this function, even if it is not in daily use. Even unused remote management enables shore-based support teams to provide on-board support without the need for remote access.

9.12 XChange File Cloud

The Cloud-section allows the captain to keep the available cloud storage-quota in mind to identify early enough if the Cloud storage-quota is already reached and needs to be cleaned up.

The Administrator can check the used storage-quota per Cloud account and manage the Cloud configuration details:

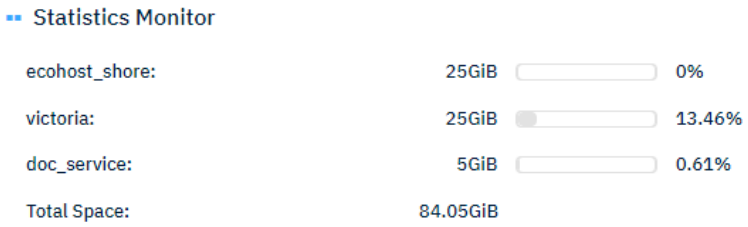


By clicking the ‘Synchronise Now’ button, the cloud synchronisation will start immediately to check if new files must be uploaded from ship to shore or vice versa.

Please note

The file synchronisation frequency is the main setting. Manual synchronisation attempts may not result in an immediate file synchronisation if the last synchronisation happed earlier than the defined frequency.

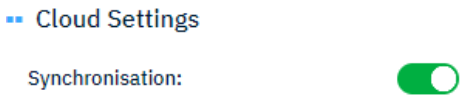
The ‘Statistics Monitor’ show for each assigned XChange Cloud Account the used vs free vs. total storage quota.



9.12.1 File Synchronisation

Within the 'Cloud Settings' the file synchronisation mechanism can be de-/activated and the period between two synchronisation attempts can be defined.

To start/stop the Cloud file synchronisation mechanism, click the button next to 'Synchronisation' and click 'Save'.



During the time the synchronisation is disabled, the XChange Cloud folders and the content will not be accessible on board. To reactivate the local network access, enable the file synchronisation again.

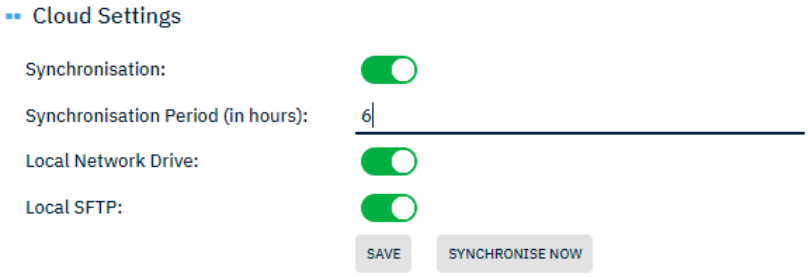
WARNING

It is not recommended to disable the Cloud synchronisation mechanism for more than 1 day, because this setting can influence the actuality of the content stored within XChange Cloud. If the synchronisation is reactivated after a longer period, it may occur that a huge number of files are being synchronised which can lead into a occupied bandwidth for a longer time.

9.12.2 Synchronisation Period

The 'Synchronisation Period' shows the number of hours between two file synchronisation attempts. Per default, the period is set to once per hour. Independent of the contracted synchronisation frequency, the system will check automatically if new content is available. Once the contracted frequency is reached, the file transmission will start automatically.

To change the synchronisation period, type the preferred amount of hours.



Click 'Save' to store the new setting.

9.12.3 Manage Local Cloud Access

Onboard, the XChange Cloud can be access from any local network by any user or system being allowed to access.

The access technologies on the local network are:

- Local Network Drive (Samba) SMBv2 / SMB v. 3.0
- Local SFTP

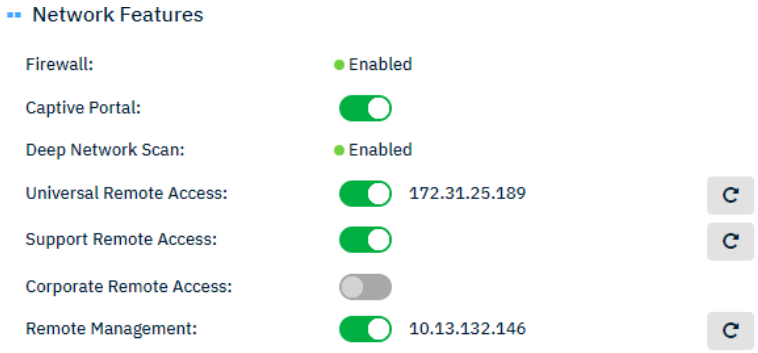
For security reasons it is recommended to only allow the technology used and to disable the other. To disable one technology, click the radio button and click the 'Save' button.

9.13 Network features

The ‘Network Features’ section provides information about the status of each network feature. Each available remote access or remote management feature can be manually activated. To activate or deactivate a network feature, click the ‘ON/OFF’ button.

Please note

If, for any remote access feature, the automatic start option is enabled within the device settings, then the service will immediately reactivate itself if it is deactivated here.



Captive Portal

The captive portal is an option which can be deactivated by the administrator. For a positive user experience, its not recommended to deactivate the captive portal. The captive portal automatically appears on the user ´s device when trying to access the internet. Only user with valid user accounts are allowed to login and proceed to the internet.

Deep Network Scan

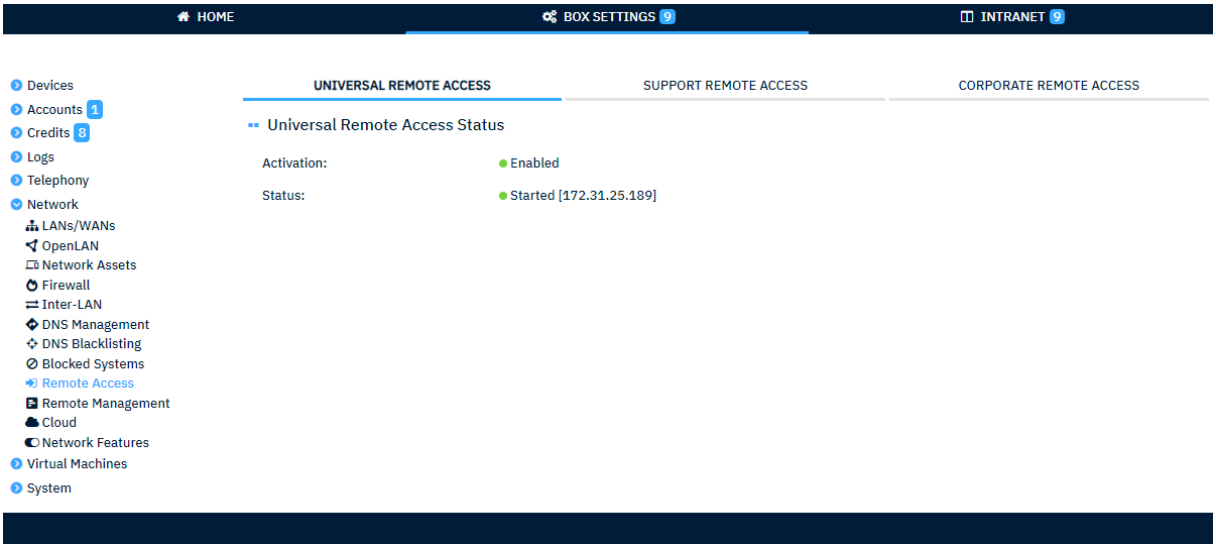
The deep network scan is an option which can be enabled on request by Marlink Service Desk. The deep network scan provides more details network overview and insights.

Please note

The deep network scan is disabled by default to avoid that some Antivirus applications on board produce wrong positive alarms.

10. Remote Access Settings

The XChange embeds multiple remote access features. To access the remote access area, go to *BOX SETTINGS > Network > Remote Access.*



The 'Remote Access' overview displays multiple weblets, each representing one remote access feature.

10.1 XChange Universal Remote Access (URA)

XChange 'Universal Remote Access' (URA) is a separate premium feature within XChange. Any XChange customer can order the XChange URA service at any time. There is no need for on-board attendance to activate this service.

Using the XChange URA service makes remote access simpler and more flexible. The XChange URA service is completely embedded within the XChange system minimising the need for configuration. URA is based on 'Open-VPN' and using encrypted communication as a standard.

There is NO need to configure trusted clients or port-forwarding rules to make use of the XChange URA service.

XChange Universal Remote Access should stay activated even without an active XChange URA subscription.

Please note

Any remote access service that is set to start automatically at device activation ('Device Settings') will automatically reconnect if you deactivate it in the 'Remote Access Area'.

Please note

The XChange Universal Remote Access service is enabled so that Marlink support can be available in case of an issue. Marlink support will request that the XChange URA service be activated manually by the Master if automatic start is not enabled.

10.1.1 XChange URA Prerequisites

A valid URA user account and the latest available URA client software are required to connect to an XChange with activated URA service.

To ensure a working XChange URA service, the XChange Firewalls shall allow XChange URA communication always, through any communication device.

XChange Universal Remote Access requires access to the Internet that allows outbound connections on TCP port 443 (https) and UDP/TCP port 1194 (VPN).

WARNING

If the XChange Firewall does not have the required XChange URA ports whitelisted, then it will be blocked. Marlink does not take any responsibility for issues with the XChange URA service if the firewall is not set up correctly.

10.2 Support Remote Access

The XChange provides a fully functional remote access feature to allow remote access to any connected system. The 'Support Remote Access' features are to be used by Marlink support teams only.

Support Remote Access Status

Activation: Enabled

Status: Started

Trusted clients

CLIENT IP	CLIENT NAME	
92.103.42.176/28	Customer Care	
193.252.234.0/24	Customer Care	
65.242.103.0/24	Customer Care	
58.185.96.40/29	Customer Care	
192.168.106.0/24	iDirect ssl-vpn Access	
192.168.128.0/20	iDirect Public IP Access	
10.102.33.1/32	iDirect Public IP Access	
10.103.33.1/32	iDirect Public IP Access	
10.107.33.1/32	iDirect Public IP Access	
10.114.33.1/32	iDirect Public IP Access	
10.115.33.1/32	iDirect Public IP Access	
10.116.33.1/32	iDirect Public IP Access	
192.168.107.0/24	iDirect ssl-vpn Access	
192.168.108.0/24	iDirect ssl-vpn Access	
192.168.109.0/24	iDirect ssl-vpn Access	
77.70.254.0/23	Customer Care	
10.10.109.14/32	XFX Access	
10.107.26.200/32	XFX Access 2	
192.168.50.1/32	XFX Server	

TRUST ALL ADD TRUSTED CLIENT

Support Remote Access Rules

DEVICE NAME	SERVICE	PROTOCOL	INCOMING PORT	TO IP ADDRESS	TO PORT	
BOX	HTTPS	TCP	444	127.0.0.1	35443	
BOX	SSH	TCP	22	127.0.0.1	30022	
HYPERVISOR	HTTPS_HYPERVISOR	TCP	24131	10.0.9.2	3131	
HYPERVISOR	SSH_HYPERVISOR	TCP	24122	10.0.9.2	22	
HYPERVISOR	Netconf	TCP	24830	10.0.9.2	830	
HYPERVISOR	SNMP	UDP	24161	10.0.9.2	161	
HYPERVISOR	Remote console 6901	TCP	6901	10.0.9.2	6901	
HYPERVISOR	Remote console 80	TCP	24180	10.0.9.2	80	
STARLINK	HTTP_STARLINK_1	TCP	24981	127.0.0.1	24981	
BOX	Local console	TCP	8069	127.0.0.1	8069	

ADD SUPPORT REMOTE ACCESS RULE

SAVE

To access the XChange, a terminal or the local network remotely, the terminal must be connected to the Internet using a Public IP address.

10.2.1 Support Remote Access Setup

The 'Support Remote Access' service must be configured to allow remote access to the XChange web interface and to any connected terminal on the WAN side.

To configure the 'Support Remote Access' feature:

- Go to *BOX SETTINGS > Network > Support Remote Access*
- Click 'Edit'
- Entrust the IP address to have access
- Click the 'Add' icon to submit a trusted IP address
- Set the remote control rules to terminals on WAN side
- Click 'SAVE'

10.2.1.1 Trusted Clients

To trust clients to access a terminal on the WAN side or the XChange web interface, follow these steps:

- Click 'ADD TRUSTED CLIENT'
- Set the public static client IP and range
- Set a client name
- Click 'Add' to confirm
- Click 'SAVE' to store changes

☝ Tip!! If more than one IP is to be entrusted, then click on 'Add' again to add more.
By default, Marlink Customer Care IP addresses are trusted and cannot be removed.

☝ Tip 2!! It is possible to enable remote control access for any IP address by clicking on the 'TRUST ALL' button. Marlink does not recommends this setting.

10.2.1.2 Remove Trusted Clients

To remove a trusted client, select the line of the client that you want to remove in the 'Trusted clients' table and click the 'Delete Trusted Client' button.

Trusted clients

CLIENT IP	CLIENT NAME	
92.103.42.176/28	Customer Care	
193.252.234.0/24	Customer Care	
65.242.103.0/24	Customer Care	
58.185.96.40/29	Customer Care	
192.168.106.0/24	iDirect ssl-vpn Access	
192.168.128.0/20	iDirect Public IP Access	
10.102.33.1/32	iDirect Public IP Access	
10.103.33.1/32	iDirect Public IP Access	
10.107.33.1/32	iDirect Public IP Access	
10.114.33.1/32	iDirect Public IP Access	
10.115.33.1/32	iDirect Public IP Access	
10.116.33.1/32	iDirect Public IP Access	
192.168.107.0/24	iDirect ssl-vpn Access	
192.168.108.0/24	iDirect ssl-vpn Access	
192.168.109.0/24	iDirect ssl-vpn Access	
77.70.254.0/23	Customer Care	
10.10.109.14/32	XFX Access	
10.107.26.200/32	XFX Access 2	
192.168.50.1/32	XFX Server	
1.2.3.4/32	Shore IT Department	

TRUST ALL | ADD TRUSTED CLIENT | DELETE TRUSTED CLIENT

10.2.1.3 Add Support Remote Access Rules

To be able to access a terminal connected on the WAN side, the support remote access rules must be set correctly.

Support Remote Access Rules

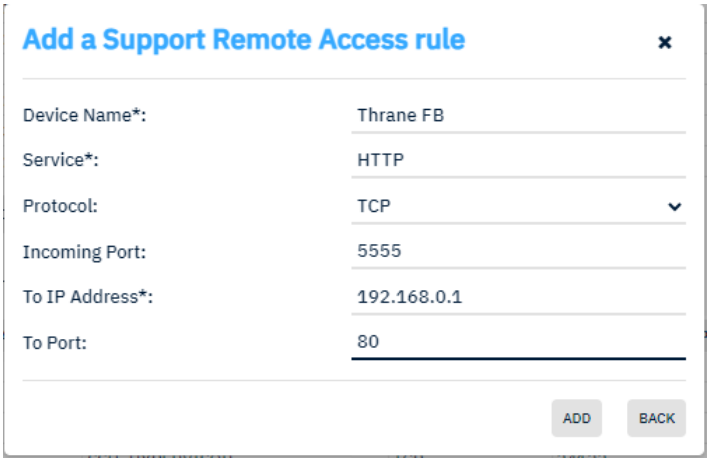
DEVICE NAME	SERVICE	PROTOCOL	INCOMING PORT	TO IP ADDRESS	TO PORT	
BOX	HTTPS	TCP	444	127.0.0.1	35443	
BOX	SSH	TCP	22	127.0.0.1	30022	
HYPERVISOR	HTTPS_HYPERVISOR	TCP	24131	10.0.9.2	3131	
HYPERVISOR	SSH_HYPERVISOR	TCP	24122	10.0.9.2	22	
HYPERVISOR	Netconf	TCP	24830	10.0.9.2	830	
HYPERVISOR	SNMP	UDP	24161	10.0.9.2	161	
HYPERVISOR	Remote console 6901	TCP	6901	10.0.9.2	6901	
HYPERVISOR	Remote console 80	TCP	24180	10.0.9.2	80	
STARLINK	HTTP_STARLINK_1	TCP	24981	127.0.0.1	24981	
BOX	Local console	TCP	8069	127.0.0.1	8069	

ADD SUPPORT REMOTE ACCESS RULE

To add a new rule:

- Click 'ADD SUPPORT REMOTE ACCESS RULE'
- Set a device name
- Set a service
- Select a protocol
- Set an incoming port
- Set the terminal IP address
- Set the 'To Port'

- Click ‘Add’
- Click ‘SAVE’ to store changes



10.2.1.4 Remove Support Remote Access Rules

To remove a rule, click on the respective line in the table to select it and click the ‘Delete Remote Control Rule’ button.

Support Remote Access Rules

DEVICE NAME	SERVICE	PROTOCOL	INCOMING PORT	TO IP ADDRESS	TO PORT	
BOX	HTTPS	TCP	444	127.0.0.1	35443	
BOX	SSH	TCP	22	127.0.0.1	30022	
HYPERVISOR	HTTPS_HYPERVISOR	TCP	24131	10.0.9.2	3131	
HYPERVISOR	SSH_HYPERVISOR	TCP	24122	10.0.9.2	22	
HYPERVISOR	Netconf	TCP	24830	10.0.9.2	830	
HYPERVISOR	SNMP	UDP	24161	10.0.9.2	161	
HYPERVISOR	Remote console 6901	TCP	6901	10.0.9.2	6901	
HYPERVISOR	Remote console 80	TCP	24180	10.0.9.2	80	
STARLINK	HTTP_STARLINK_1	TCP	24981	127.0.0.1	24981	
BOX	Local console	TCP	8069	127.0.0.1	8069	
Thrane FB	HTTP	TCP	5555	192.168.0.1	80	

ADD SUPPORT REMOTE ACCESS RULE DELETE SUPPORT REMOTE ACCESS RULE

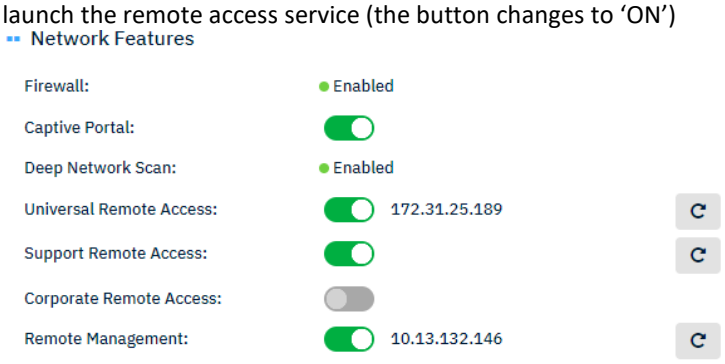
☝ Tip!! The system marks remote control rules that become irrelevant when local network settings or device settings change in red.

10.2.2 Manual Support Remote Access Initialisation

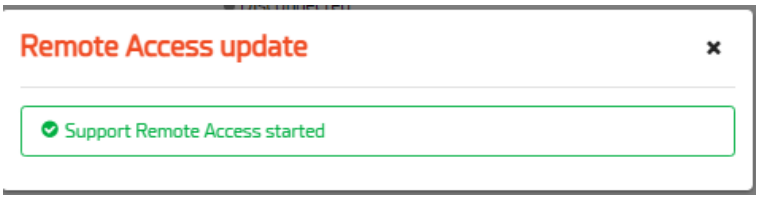
When automatic start of the support remote access is disabled, it can be initialised manually. It is then possible to remotely access the XChange or terminals on the WAN side.

To initialise the service:

- Go to *BOX SETTINGS > Network > Overview*
- Click 'OFF' to launch the remote access service (the button changes to 'ON')

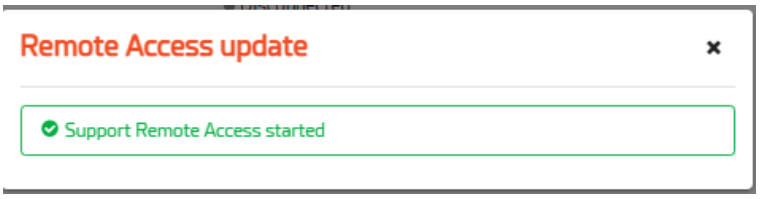


When the service is initialised, a data connection using a Public IP will be launched (FleetBroadband).



To access a terminal on the WAN side, the Administrator needs to use the incoming port pointing to the desired terminal, for example, https://<public_ip_address>:PORT

☝ Tip!! While using a different device than FleetBroadband, the Public IP address cannot be retrieved by the XChange.



To find out your current Public IP address, start a data session and browse to http://www.myipaddress.com. If the Public IP address is properly forwarded to the device interface (depending on the network's shore configuration), then the shore Administrator will be able to access the XChange.

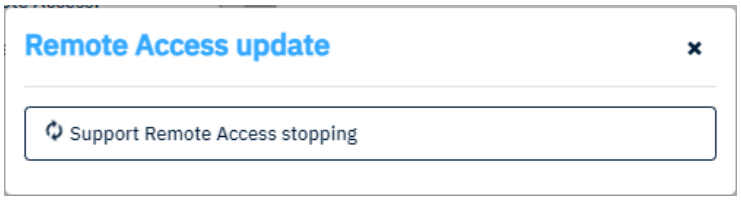
Before the XChange can be accessed remotely via an autonomous device, ensure that 'Port Forwarding' is set up correctly on this device, pointing to ports 444 and 22.

10.2.3 Terminate Support Remote Access

To end the remote access service:

- Go to *BOX SETTINGS > Network > Overview*
- Click 'ON' to terminate the remote access service (The button changes to 'OFF')

When the service stops, the Public IP data connection will also be terminated.



10.3 Corporate Remote Access

The XChange provides a fully functional remote access feature to allow remote access to any connected system. The 'Corporate Remote Access' is designed for use by customers and third-parties. Technically is no difference between the corporate and support remote access.

Please note

To configure your Corporate Remote Access, please follow the same instructions as described in the previous chapter.

WARNING

For Support- and Corporate Remote Access trusted clients must be setup. The option 'Trust All' shall only be used in exceptional cases for a very limited time.

If the vessel is setup with Public or Public Static IP, the 'Trust All' option shall not be used.

In case the 'Trust All' option is setup by the customer although Public IP addressing is used, Marlink takes no responsibility in case of a cyber security breach.

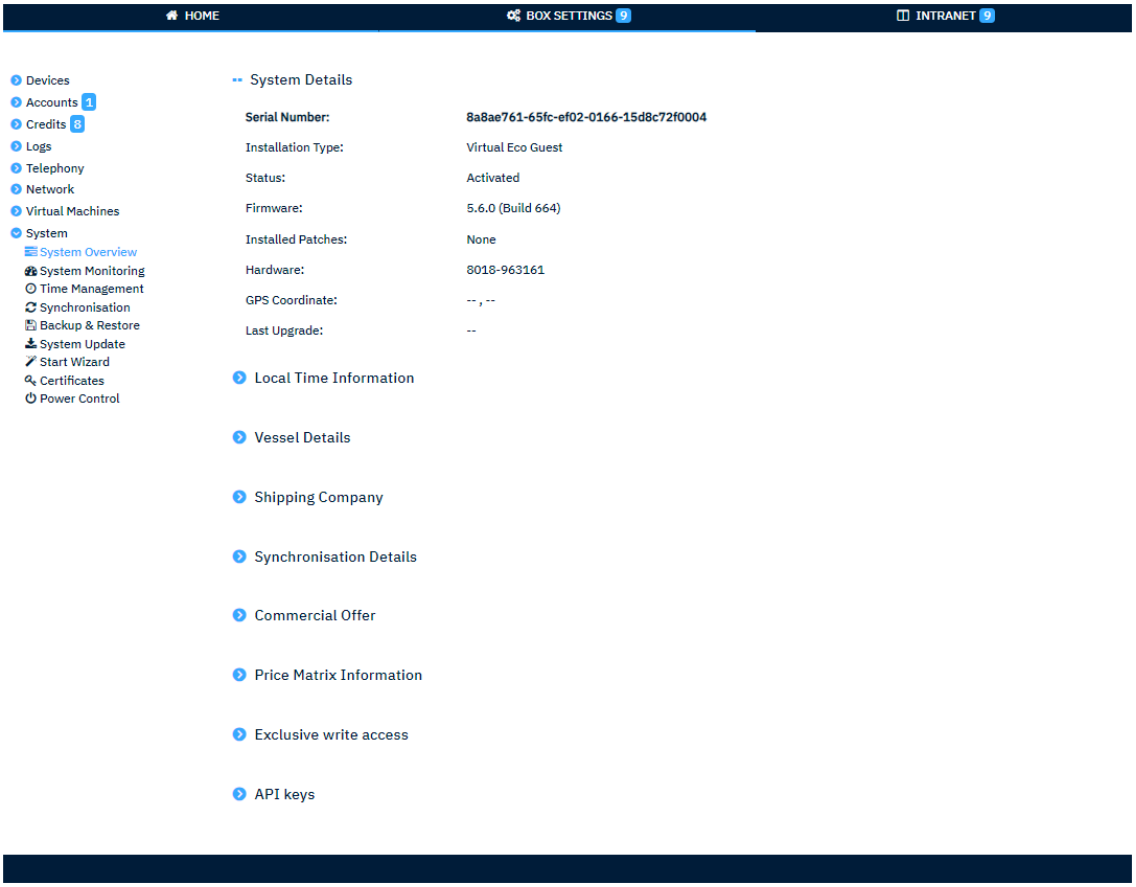
11.System

The ‘System’ section of the XChange provides general system management capabilities such as backup and restore for the box settings, firmware update, setting up synchronisation and power control.

11.1 Overview

To display the system overview, go to *BOX SETTINGS > System > Overview*.

The system overview gives general information about the system, the vessel, synchronisation details and the commercial package.

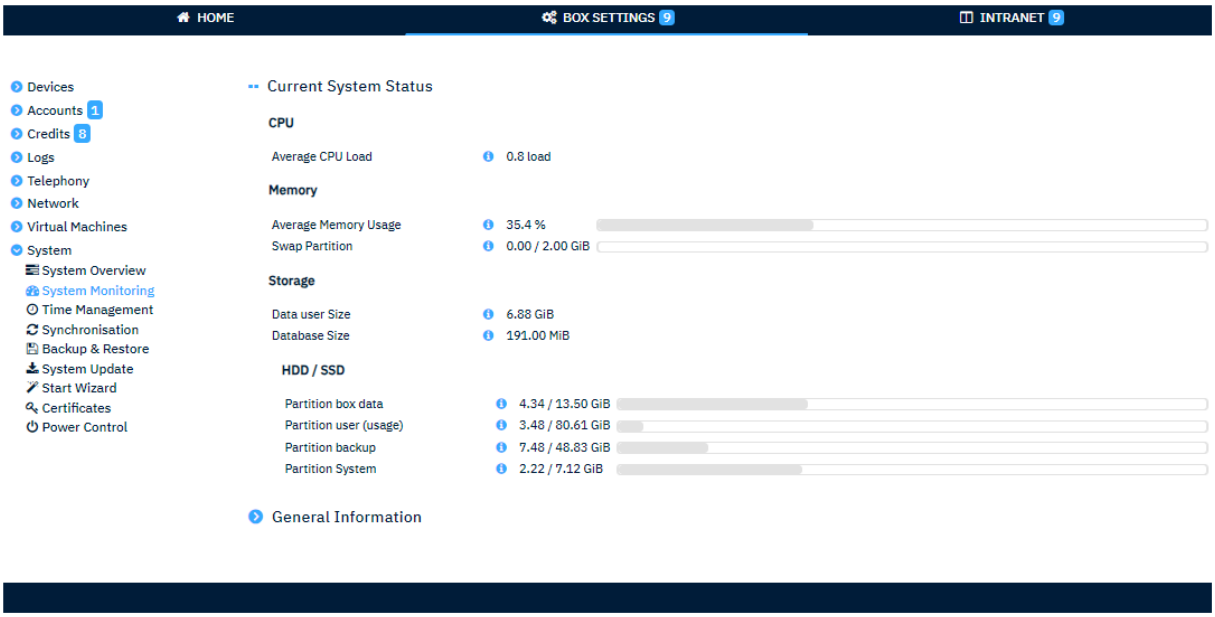


Detailed information is provided for cover:

	DESCRIPTION
'System Details' (box-related)	XChange Serial number
	Installation Type
	Status
	Firmware version
	Installed patches
	Hardware identifier
	GPS Coordinates
	Last Update
'Local Time Information'	Local time
	Set time zone
'Vessel Details'	Vessel name
	Call sign
	IMO
	Vessel type
	Vessel Contact Details
'Shipping Company	Name
	Contact Details
'Synchronization Details'	Status
	Date and time of last synchronisation attempt
	Date and time of last successful synchronisation
'Commercial Offer'	Commercial package type
	List of available features
'Price Matrix Informations'	Date of the last price matrix update and price per MiB
'Exclusive write access' (EWA)	Status of EWA setting and last change date

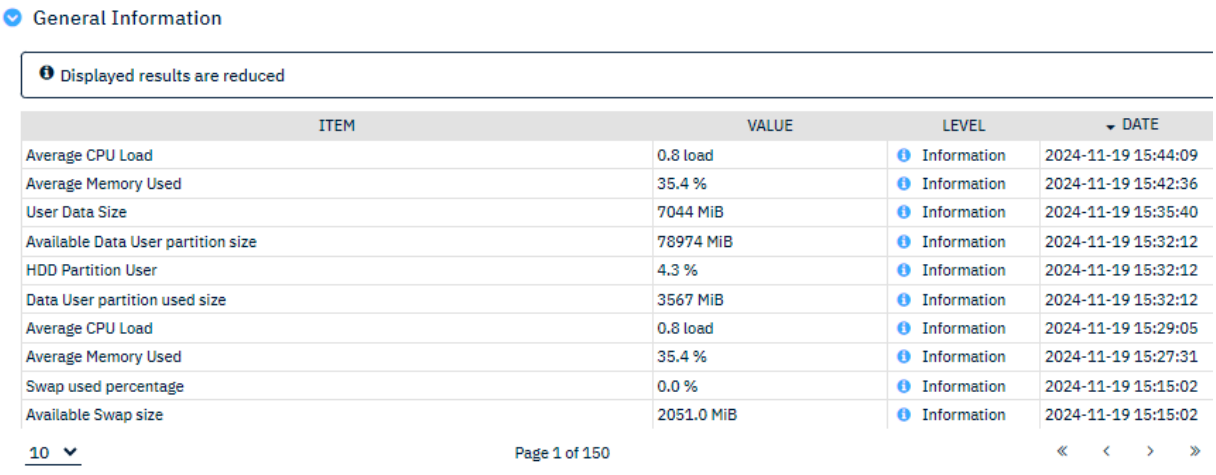
11.2 System Monitoring

The ‘System Monitoring’ feature provides the Captain and Administrator with current and historical system status information, updated every 3 hours.



11.2.1 System Monitoring Log

To access the system monitoring log, go to *BOX SETTINGS > System > System Monitoring* and expand the ‘General Information’ collapsible panel.



The system monitoring log is a historical log providing system status information from the last 3 months.

11.2.2 Current System Status

The current system status provides an overview of the latest information about CPU load, memory used and GPS coordinates, both with text and graphics.

If a defined threshold is reached, then the system raises a warning to the on-board administrative staff and those can also be access and reviewed any time via Portal 360.

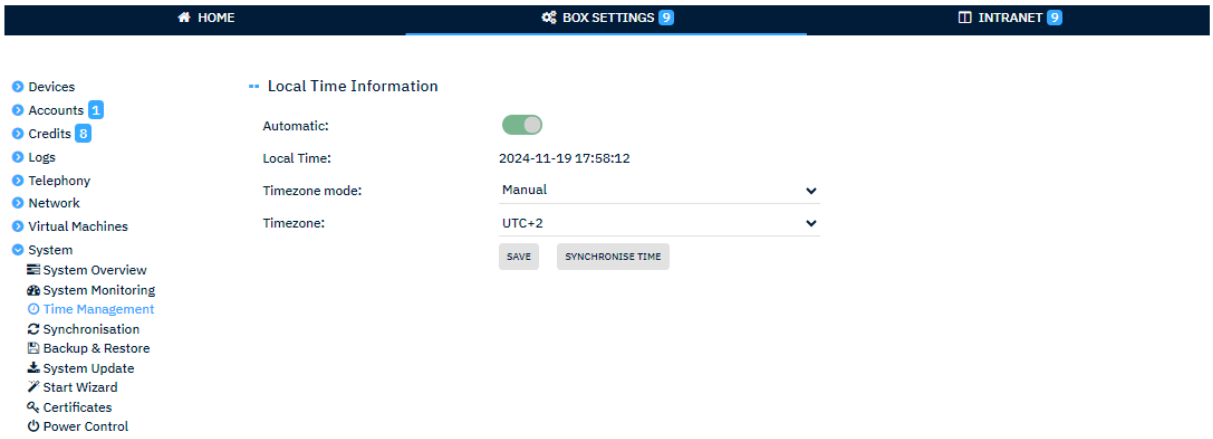
Depending on installed equipment, not all information is always available.

Displayed status details are:

#	TYPE	DESCRIPTION	WARNING THRESHOLDS
1	CPU Load	Processor load	1.5 CPU load
2	GPS Location	Last known GPS position	N/A
3	Memory Used	% of used system RAM	less than 400MB available
4	SSD Health	% of SSD lifetime reached	
5	Box Data	% of used data storage allowance	less than 800MB left
6	User Data	% of used User storage allowance	less than 500MB left
7	Backups	% of used backup file storage allowance	less than 1MB left
8	System	% of used system storage allowance	less than 500MB left
9	Database Size	Current size of entire database	
10	Data User Size	Current size of the user storage	
11	CPU Temperature	Temperature of the CPU	75°
12	Disk Temperature	Temperature of the disk if available	75-100°
13	Cloud Partner	Current size of the used Cloud storage	
14	Remaining Apache Workers	# of remaining users to go online via XC User Interface	
15	Volumetry Counters		
16	Active Users Sessions	#of concurrent active users online at the same time	

11.3 Time Management

The ‘Time Management’ feature enables the Administrator to change the local time settings at any time or to push for a time synchronisation.

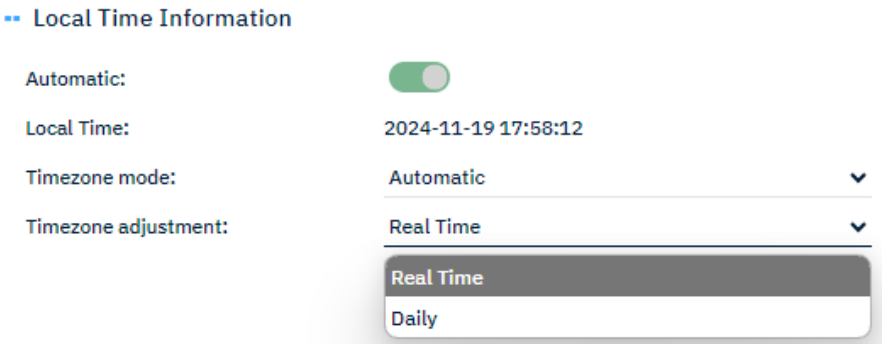


11.3.1 Change Time Zone Manually

To change the local time zone, select the preferred time zone in the ‘Timezone’ drop-down list and click ‘SAVE’.

11.3.2 Change Time Zone Automatically

To enable automatic time zone adaption, change the ‘Timezone Mode’ to ‘Automatic’ and select the time zone adjustment mode.



Automatic time zone adjustment is based on the actual XChange GPS coordinates. If a time zone changes due, for example, to transit, then the system can adapt the time zone either immediately or once per day.

11.3.3 Time Synchronisation

The system synchronises with a shore-based time server automatically. Additionally, it is possible to synchronise local system time settings at any time by clicking the ‘SYNCHRONIZE TIME’ button.

The XChange acts as a local NTP time server enabling local network devices to synchronise their time settings via XChange.

11.4 Synchronisation

The ‘Synchronization’ feature enables the synchronisation of vessel-to-shore and shore-to-vessel bidirectional data and files.

The following items are synchronised:

- News
- FAQs
- Logs
- Administrative settings

NAME	SYNCHRONISATION PERIOD
Backoffice Administrative Settings	0s
Backup files	1d
Beams	0s
Box Administrative Settings	0s
Change Logs	1h
Cloud Synchronisation Logs	1h
Commercial settings	0s
Credit Logs	1d
Cyber Logs	1d
DNS Blacklisting	0s
Error Logs	1d
Event Logs	1h
FAQs	0s
Media Bo	0s
Media Transmission Logs	1d
Media View Logs	1d
Network Settings	1d
News and Alerts	0s
OVP information	1d
Patches Download	0s
Patches Results	0s
Price Matrix	0s
synchronization_BackupUpdate	0s
System Monitoring	1d
Traffic Logs	0s
Update Diagnostic File	0s

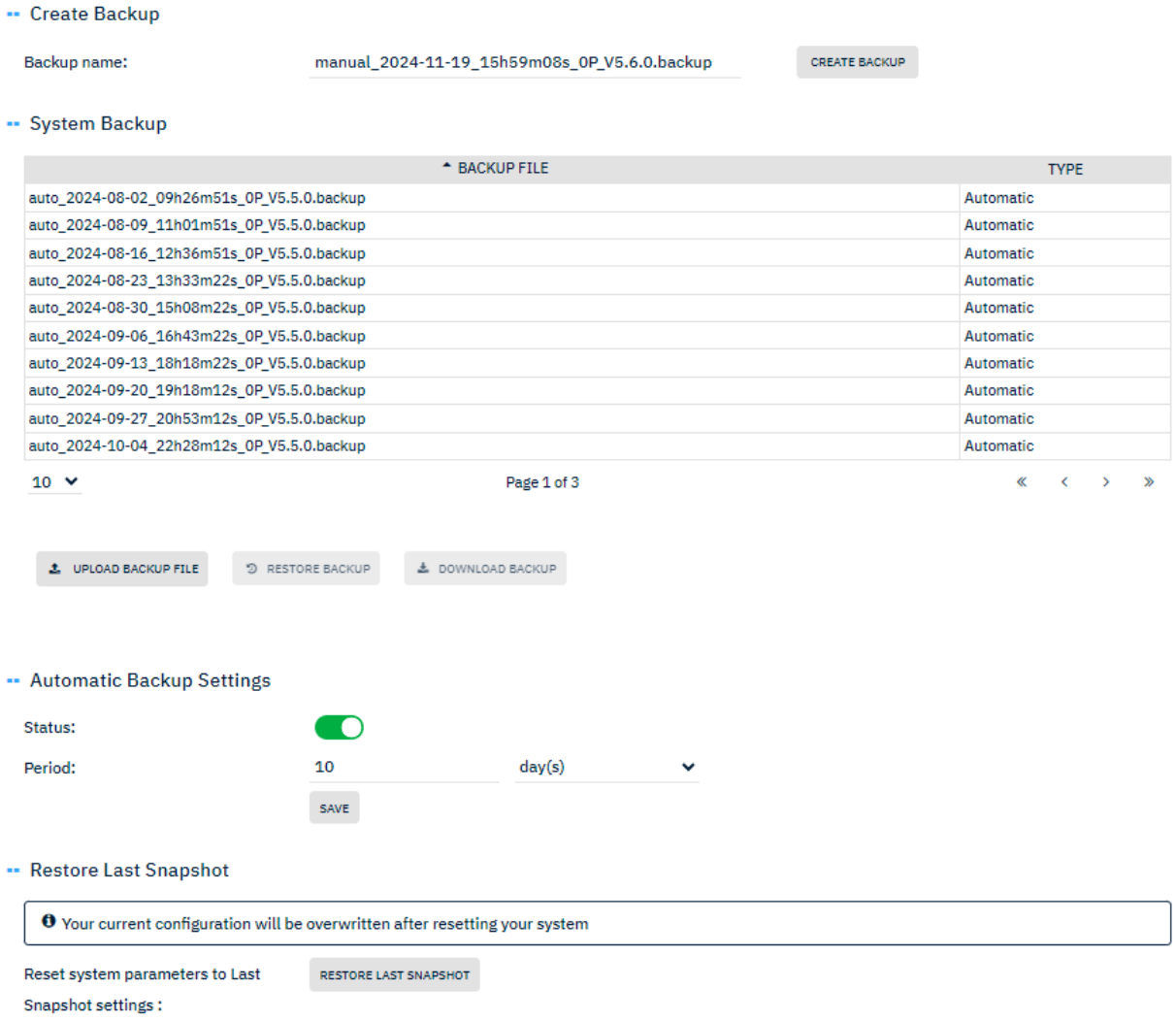
If needed, a manual synchronisation can be started at any time by clicking the ‘Synchronise Now’ button.

The XChange will then establish a connection to the XChange Servers and start a synchronisation.

11.5 Backup and Restore

The ‘Backup & Restore’ feature enables the Administrator to create backup files of the box’s configuration and logs.

For critical cases, it is possible to reset the box to factory default settings.



11.5.1 System Backup

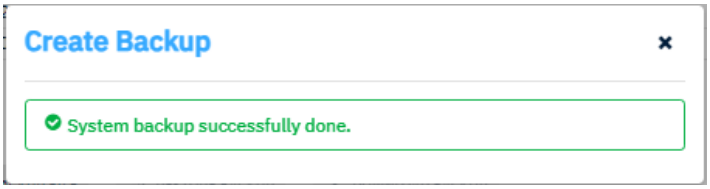
It is recommended that you back up the system regularly, for example, once a week. Depending on XChange usage, it is recommended to do it at regular intervals. There is no limitation in term of number of backups that can be made.

To create a backup file for the XChange:

- Go to *BOX SETTINGS > System > Backup & Restore*
- Click 'Create BACKUP'

The system starts creating the backup file, it will take just a few seconds.

The system notifies you once the backup procedure has completed.



The latest backup file will be displayed at the end of the backup file list. Each backup file is automatically named with the backup date and time. The 'Type' column indicates if the backup file was generated manually or automatically.

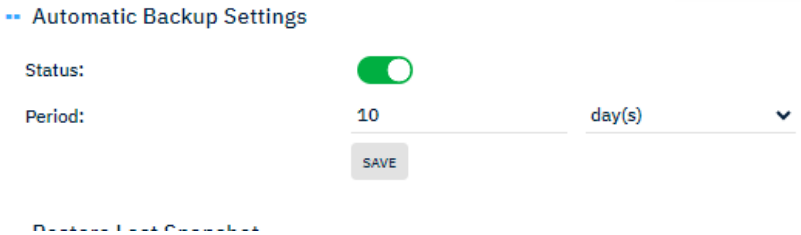
11.5.1.1 Automatic System Backup

An automatic system backup can be set up for regular backup file creation at periods based on:

- Days
- Weeks
- Months

To set up the automatic system backup, go to *BOX SETTINGS > System > Backup & Restore* and proceed as follows:

1. Set the status to 'ON'
2. Set the period
    a. For example, 'Every 1 Day'
3. Click 'SAVE'



WARNING

It is absolutely necessary to keep the automatic backup function enabled. If the automatism is disabled, Marlink cannot take responsibility for future replacements. If no backup files are available, the entire configuration must be redone manually and all users, credits and logs are lost.

11.5.1.2 Store Backup Files

All backup files are stored by default on the XChange hard disk drive. It is recommended that you also store backup files on an external storage device or computer.

To store backup files on an external storage device, click the backup file and choose the storage location.

11.5.2 System Restore

It is possible to restore the XChange system using previously created backup files. This is very helpful if there are problems. You can either restore the files using a locally stored file or by using a backup file stored in the XChange.

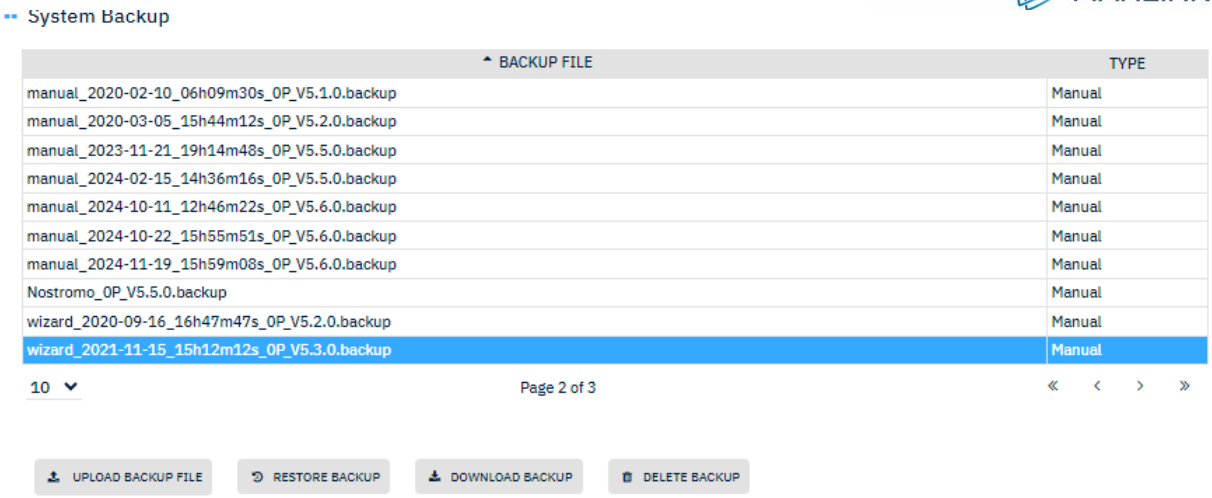
To restore using a locally stored file, click ‘Browse’ and select the latest backup file from the storage folder.

S

Please note

The name of the imported file must be different from those already stored in the XChange.

To restore the system using a backup file stored on the XChange, click the latest backup file in the list to select it and then click the ‘RESTORE’ button when it appears.

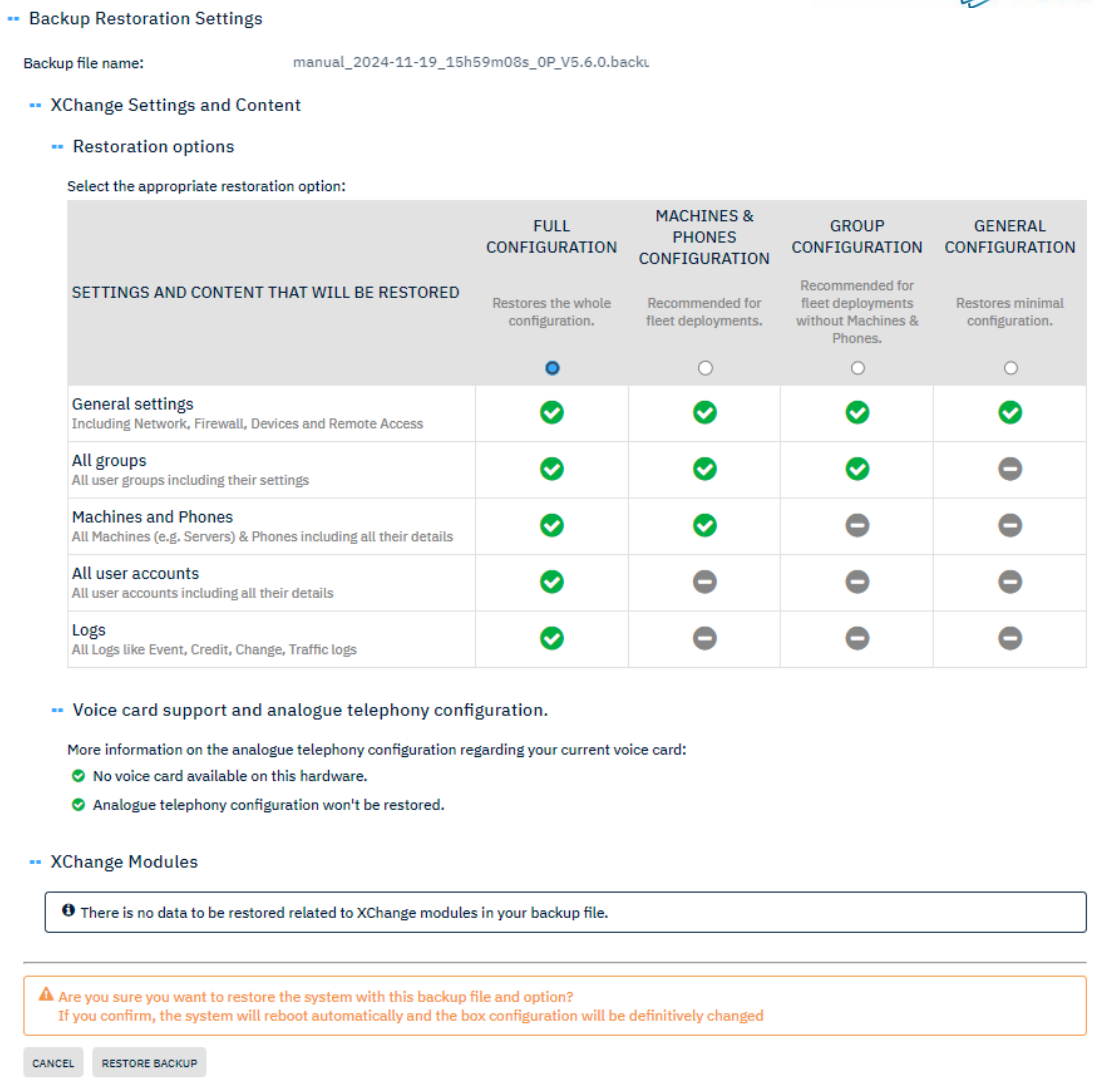


Please note

All changes carried out on the system configuration or data (e.g. logs) since the last backup and restore will be lost.

11.5.2.1 Restore Options

For backup restores, it is either possible to import a whole system configuration including all settings, logs and User account details, or just some parts of these.



The options are:

- Full Configuration
- Machines & Phones
- User group configuration
- General Configuration

To restore a configuration from a backup, select one of the presented options and press the 'Restore Backup' button at the end of the page.

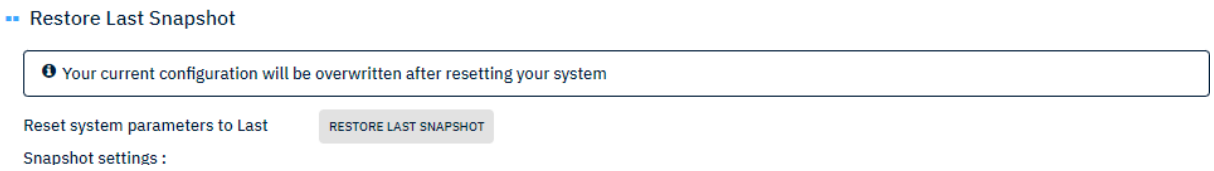
WARNING

Backup files carry all system details including the voice card settings. If the backup file was created with an XChange with a different voice card setup than the XChange that you import the backup file into, then this import option should be kept 'OFF' to avoid the risk of a failed system restoration.

11.5.3 Restore Last Snapshot

As a last resort, you can roll back the XChange to the last stored snapshot. This will reload the last system version before the last firmware update and all configurations you have made will be rolled back to the previous setup!

To reset the system, go to *BOX SETTINGS > System > Backup & Restore* and click 'Restore Last Snapshot'.



The system will reload the snapshot and restart. This procedure may take several minutes.

WARNING

While resetting, the system will revert to the last firmware version. You may then need to perform the firmware updates again.

WARNING

Please proceed with the snapshot restore of the XChange on Marlink's request only!!!

11.5.4 Manual Certificate update after Reset

As part of the reset, all previously installed security certificates are deleted and replaced by the original certificates. Depending on the age of the system, those original certificates are maybe outdated.

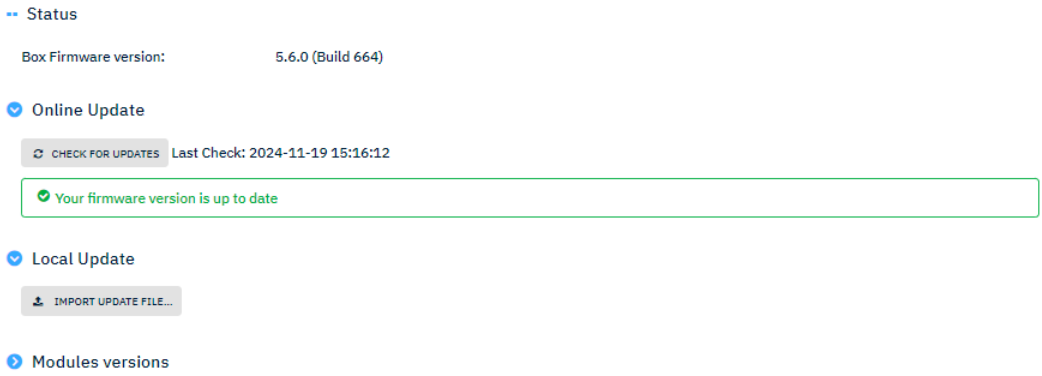
Once a System is re-initialised, it is mandatory to manually update XChange´s embedded security certificates.

Please note

Once a System is re-initialised, it is mandatory to manually update XChange´s embedded security certificates.

11.6 Firmware Updates

The ‘Firmware Update’ feature enables the Administrator to update the XChange firmware either using a local update file or online.



By clicking ‘CHECK FOR UPDATES’ the XChange will connect to the XChange server to check for new updates.

If there is a new update, then the status table displays the new version and the ‘Status’ column displays an ‘Update’ button.

To update the firmware online, click on the ‘Download’ button. The box will connect to the XChange server and download the update file. Once the download has completed, click the ‘Update’ button to start the procedure.

To update the firmware using a local update file, click ‘Browse’ and select the update file from the storage location.

WARNING

DO NOT REBOOT THE XCHANGE DURING THIS OPERATION!

11.6.1 Module Updates

The XChange system manages specific software modules next to the XChange core system. For instance, each communication device driver is a unique module.

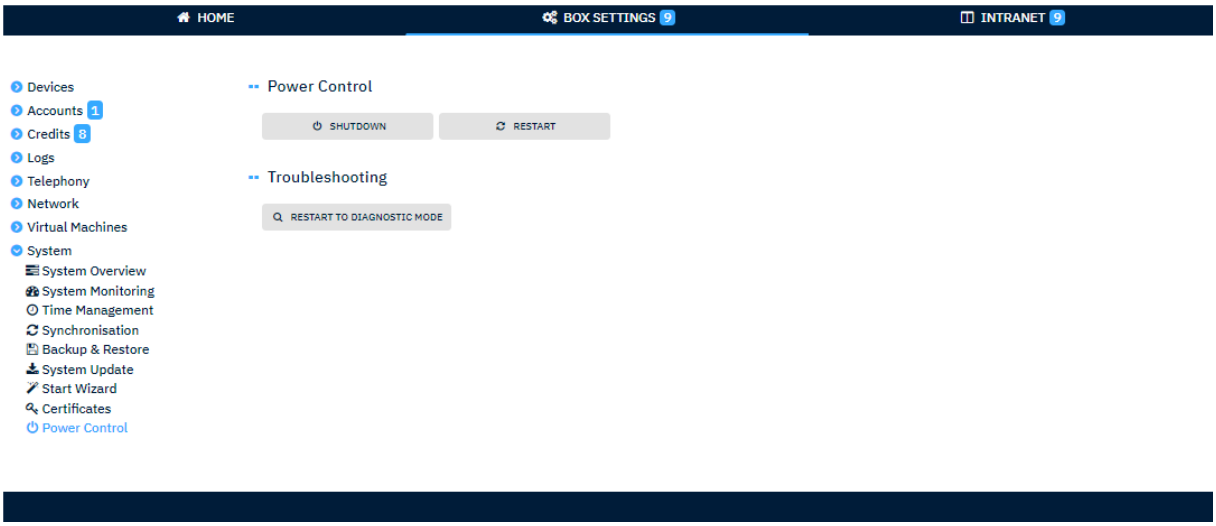
The modules may be update more frequently than the major core system. The “Modules Versions” panel lists all installed modules and provides a status for each of them.

NAME	VERSION	STATUS
Additional Firewall Rules	3.0.0-2	Up to Date
Drivers Thuraya	3.0.0-3	Up to Date
Drivers VSAT	3.0.2-2	Up to Date
Support Tools	1.1.0-1	Up to Date
Ecoguest module	4.22.4-1	Up to Date
Drivers 4G Teltonika RUT 950	3.3.1-1	Up to Date
Drivers Basic	3.0.1-1	Up to Date
Drivers Starlink	3.0.3-1	Up to Date
Drivers Iridium OpenPort	3.0.1-1	Up to Date
News	1.0.2-2	Up to Date
Drivers Certus	3.0.1-2	Up to Date
Drivers SDWAN	3.3.8-1	Up to Date
Cloud Intranet	1.1.2-2	Up to Date
Drivers XFX	3.0.2-2	Up to Date
Troubleshooting tools	3.1.0-2	Up to Date
Skins and languages	1.6.6-1	Up to Date
Channels Templates	3.1.2-1	Up to Date
Drivers FleetBroadband	3.0.1-1	Up to Date
Universal Remote Access	1.2.0-1	Up to Date

While the system automatically installs module updates, by clicking on ‘Force Module Update’ the check for updates can be executed manually at any time.

11.7 Power Control

The power control functionality enables the Administrator and Captain to either restart, shut down or reboot the XChange in maintenance mode, without the need for any physical action.



To restart or shut down the XChange, go to *BOX SETTINGS > System > Power Control* and click the appropriate button.

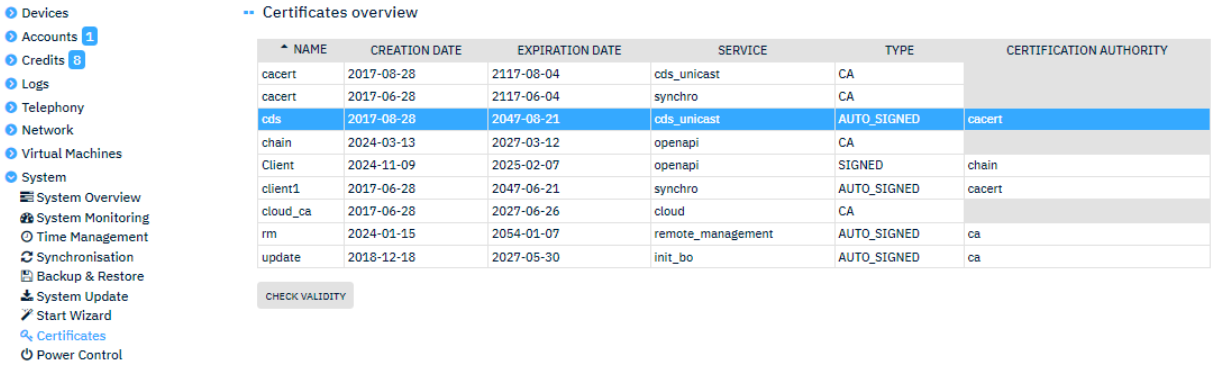
WARNING

If the XChange is shut down or restarted, then the embedded features will not be available. All data and voice sessions will be closed, without warning any Users, and network clients still connected will lose their network access.

11.8 XChange Security Certificates

The XChange synchronises in the background with Marlink´s XChange servers hosted within Marlink´s premises at shore, at regular intervals.
During this synchronisation for example freshly created log-entries are transmitted to the shore or XChange optional premium services are activated if ordered.
This synchronisation is based on secured and encrypted 'HTTPS' connection.
For security reasons, the XChange uses HTTPS certificates which are regularly updated automatically to ensure highest possible security.

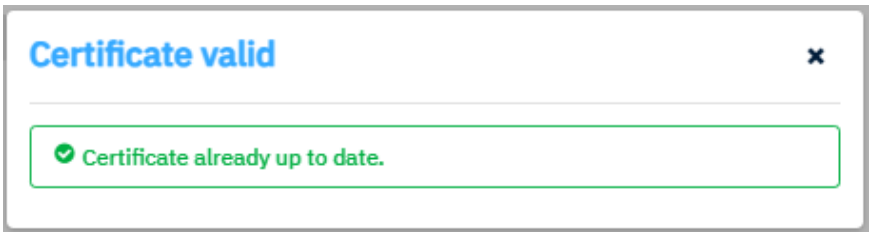
After a factory reset, or in cases an XChange service seems not to work properly, a check for updates of those security certificates is required.
To check and potentially update a security certificate, go to Box Settings > System > Certificates:



To check for updates, select one certificate after the next.
Once a certificate is selected, press the button "Check Availability":

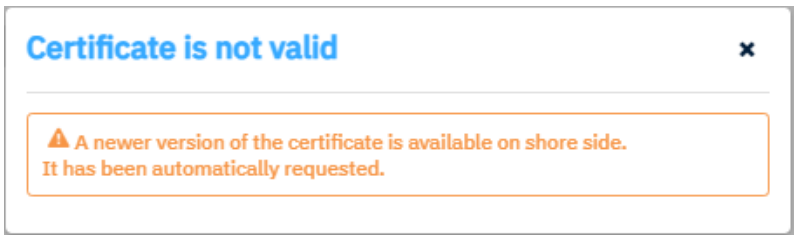
The system will check with the XChange server if that security certificate is still UpToDate and if not, the latest one will be downloaded in the background.

If the installed certificate is already the latest one, this popup message confirms the validity:



You can close the popup message and check the next certificate.

If a newer certificate version is found on the server, below message is displayed:



The system will automatically download and install the newer certificate in the background. You can close the popup message and check the next certificate.

11.9 Maintenance Mode

For support cases and troubleshooting, it can be useful to reboot the system in maintenance mode.

To reboot the XChange in maintenance mode go to *BOX SETTINGS > System > Power Control* and click the 'Restart to Maintenance Mode' button.

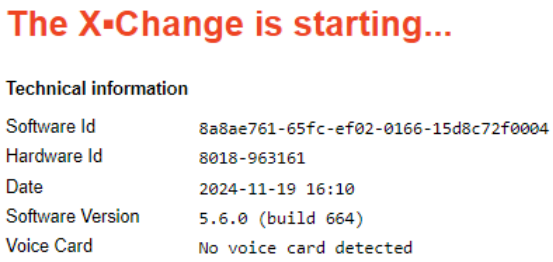
The system will reboot in maintenance mode.

Please note
Maintenance mode should be entered on Marlink's advice only!

Please note
The system automatically starts in maintenance mode if the normal boot sequence cannot be performed successfully.

Please note
The reboot sequence may take several minutes. Delete your browser cache while waiting.

When the reboot finishes, the information below will be displayed in the browser window:



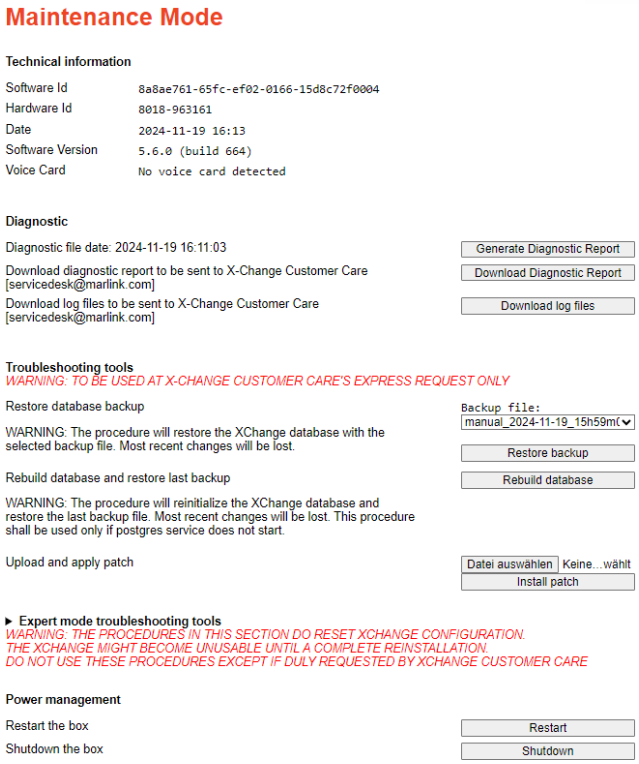
To enter maintenance mode, click on the 'here' hyperlink. A special dedicated login is needed to successfully log in.

11.9.1 Login Details for Maintenance Mode

Only the Administrator is allowed to log in to maintenance mode with a daily changing password.

Please note
Please contact your Service Provider or Marlink Service Desk for login details.

After a successful login, the maintenance page is displayed:



Technical information

The technical information provides all the required box-related details, including:

- Software ID
- Hardware ID
- Current date and time
- Actual installed firmware version

Diagnostic

In 'Diagnostic' you can download a diagnostic report and log files.

Troubleshooting tools

☝ The troubleshooting tools should be used on Marlink's advice only!

Provided tools are:

- Log file deletion
  - Clears the log file section to empty the used storage
- Database reset
  - Clears the database to empty the used storage
- Factory reset
  - Resets the XChange system to factory defaults
- Patch upload
  - In case of a system issue, Marlink may provide a patch to fix an issue

Power management

Within power management it is possible to shut down or restart the XChange.

12. Appendix A – List of Events

Please see the list of currently available events:

Event ID	Description	Type
ANALOG_001	Voice Card Support Restored	SYSTEM
APACHE_WORKERS_LOW	Almost all apache workers are used	MONITOR
AUTO_REBOOT_001	Reboot planned	REBOOT
AUTO_REBOOT_002	Reboot now from banner	REBOOT
BACKUP_001	Backup failed	BACKUP_RESTORE
BACKUP_002	Restore failed	BACKUP_RESTORE
BACKUP_003	Backup completed	BACKUP_RESTORE
BACKUP_004	Restoring of factory settings in progress	BACKUP_RESTORE
BACKUP_005	Restoring in progress	BACKUP_RESTORE
BACKUP_006	Restore failed	BACKUP_RESTORE
BACKUP_007	Restore completed	BACKUP_RESTORE
BACKUP_008	Analog phone ports and related telephony configuration were reset. Please perform a wizard to adapt the telephony configuration to this appliance.	BACKUP_RESTORE
BACKUP_009	Import of GPG keys has failed. It is needed to backup and update. Please contact support.	BACKUP_RESTORE
BACKUP_010	Import of GPG keys succeeded	BACKUP_RESTORE
BEAM_001	Beam change detected	UPDATE
BEARER_001	Bearer State changed	USER
CERTIFICATE_001	Certificate expiration	CERTIFICATE
CERTIFICATE_002	Certificate validity	CERTIFICATE
CHANNEL_001	Channel initialization succeeded.	SYSTEM
CHANNEL_002	Channel initialization failed.	SYSTEM
CHANNEL_003	Incompatible channel template version.	TEMPLATE
CLOUD_BACKUP_001	Partner login is already in use. The partner has not been created.	CLOUD
CLOUD_BACKUP_002	Partner creation during cloud backup	CLOUD
CLOUD_QUOTA_001	Putting a file has been rejected due to per-box quota reached	CLOUD
CLOUD_QUOTA_002	"Per-box" quota has been modified during synchronization but it is reached. Please delete files.	CLOUD
CLOUD_SYNC_001	Cloud synchronization started	CLOUD
CLOUD_SYNC_002	Cloud synchronization succeeded	CLOUD
CLOUD_SYNC_003	Cloud synchronization failed	CLOUD
CLOUD_SYNC_004	Cloud synchronization interrupted	CLOUD
CLOUD_SYNC_005	Cloud synchronization discarded	CLOUD
CLOUD_SYNC_006	The ongoing Cloud synchronization has been stopped intentionally	CLOUD
CLOUD_SYNC_007	Partner login is already in use. The partner has not been created.	CLOUD
CLOUD_SYNC_008	Partner creation during cloud synchronization	CLOUD
CLOUD_SYNC_009	Cloud synchronization succeeded but box quota has been reached for some partners	CLOUD
CLOUD_SYNC_010	Cloud synchronization succeeded but shore quota has been reached for some partners	CLOUD
CLOUD_TOO_LARGE_001	File max size reached	CLOUD
CONNECTION_001	Device not ready	CONNECTION

CONNECTION_002	Device ready	CONNECTION
CONNECTION_003	Device switching	CONNECTION
CONNECTION_004	Connection failed	CONNECTION
CONNECTION_005	Connection aborted, insufficient credit	CONNECTION
CONNECTION_006	Connection timeout	CONNECTION
CONNECTION_007	Connection dropped, auto-switching devices	CONNECTION
CONNECTION_008	Automatic device switching	CONNECTION
CONNECTION_009	Connection dropped, IP assignment may have changed	CONNECTION
CONNECTION_010	System connection started	CONNECTION
CONNECTION_011	System connection stopped	CONNECTION
CONNECTION_012	Connection failed, connection retry counter initiated	CONNECTION
CONNECTION_013	Successful connection, connection retry counter reset	CONNECTION
CONNECTION_014	Forced connection retry triggered, connection retry counter reset	CONNECTION
CONNECTION_015	Connection refusal	CONNECTION
CONNECTION_016	The device API is not responding. Check device status and configuration.	CONNECTION
CONNECTION_017	The device API is responding and back to normal mode	CONNECTION
CONNECTION_018	Connection dropped to be compliant with devices priority configuration	CONNECTION
CONNECTION_019	Sessions cut to be compliant with devices priority configuration	CONNECTION
CONNECTION_020	User has been disconnected	CONNECTION
CONNECTION_021	User has been disconnected and blocked	CONNECTION
CONNECTION_022	Group has been disconnected	CONNECTION
CONNECTION_023	Group has been disconnected and blocked	CONNECTION
CONNECTION_024	Device is suspended	CONNECTION
CONNECTION_025	Device is resumed	CONNECTION
CONNECTION_026	Device suspension is expired	CONNECTION
CONTENT_001	New multicast stream detected	CONNECTION
CONTENT_002	Unknown current beam replaced by a default one	CONNECTION
CONTENT_003	Unknown current beam ignored	CONNECTION
CYBERSECURITY_001	The device with the following MAC Address has been blocked following the detection of a malicious traffic	CYBERSECURITY
CYBERSECURITY_002	The device with the following MAC address has been unblocked by the remote administrator	CYBERSECURITY
DEVICE_001	Incompatible device template version.	TEMPLATE
DEVICE_002	Missing device in system configuration.	TEMPLATE
DNS_WHITELISTING_001	Some User Groups DNS Whitelisting statuses have changed	USER
FEATURE_001	Feature enabled	FEATURE
FEATURE_002	Feature disabled	FEATURE
FEATURE_003	Feature enabled	FEATURE
FEATURE_004	Feature disabled	FEATURE
INSTALLATION_001	Installation finalised by Field Engineer	SYSTEM
INSTALLATION_002	Field Engineer account deactivated automatically	USER
INSTALLATION_003	Installation complete, Field Engineer account deactivated	USER
INSTALLATION_004	Account activated	USER
INSTALLATION_005	Account deactivated	USER
INTERLAN_001	Some Inter-LAN rules have been invalidated following LAN configuration changes	USER

MODULE_001	Module download failed.	MODULE
MODULE_002	Module installation failed.	MODULE
MODULE_003	Module update succeeded.	MODULE
MODULE_004	Module uninstallation failed.	MODULE
MODULE_005	Module uninstallation succeeded.	MODULE
MODULE_CONTENT_001	Module content installation succeeded.	MODULE
MODULE_CONTENT_002	Module content installation failed.	MODULE
MODULE_CONTENT_003	Module content uninstallation succeeded.	MODULE
MODULE_CONTENT_004	Module content uninstallation failed.	MODULE
MODULE_CONTENT_005	Group has been renamed as its name is a reserved name for Marlink	MODULE
MODULE_CONTENT_006	User has been renamed as its username is a reserved name for Marlink	MODULE
MODULE_CONTENT_007	The short number has been modified for a phone user as it was using a reserved shortnumber for Marlink	MODULE
SYSTEM_MIGRATION_ERROR	The migration of module database has failed	MODULE
MONITOR_001	Allowance alert	MONITOR
MONITOR_002	Large session	MONITOR
MONITOR_003	The XChange Box has been started in a degraded state because the data_user partition is full. Please contact support.	SYSTEM
MONITOR_004	Data box partition is almost full	MONITOR
MONITOR_005	Data User partition is almost full	MONITOR
MONITOR_006	System partition is almost full	MONITOR
MONITOR_007	Backup partition is almost full	MONITOR
NETWORK_001	Configured interfaces are in conflict with reserved Marlink networks	SYSTEM
NETWORK_002	Blacklisted IP addresses belong to reserved Marlink networks	SYSTEM
NETWORK_003	New LAN added	SYSTEM
NETWORK_004	LAN deleted	SYSTEM
OPEN_LAN_001	Open LAN connected	USER
OPEN_LAN_002	Open LAN disconnected	USER
OPENAPI_001	Concurrent requests exceeded	SYSTEM
OPENAPI_002	Too many connections	SYSTEM
PHONELINE_001	Configured handset on box phoneline does not match device handset	CONNECTION
REBOOT_001	Boot completed after UI shutdown	REBOOT
REBOOT_002	Boot completed after UI restart	REBOOT
REBOOT_003	Boot completed after System restart	REBOOT
REBOOT_004	Boot completed after hard shutdown	REBOOT
REBOOT_005	System changes are applied. Please reboot the system.	REBOOT
REBOOT_006	Boot completed after SSH shutdown.	REBOOT
REBOOT_007	Boot completed after SSH restart.	REBOOT
REBOOT_008	Boot completed after hard electrical shutdown.	REBOOT
REBOOT_009	Boot completed after soft shutdown.	REBOOT
REBOOT_FACTORY	Boot completed after reset factory.	REBOOT
REBOOT_LAST	Boot completed after restoring last snapshot.	REBOOT
REGISTER_001	Registration completed	REGISTER
REGISTER_002	Registration failed	REGISTER

RESTORE_MODULE_FAILED	The XChange module data restoration has failed	BACKUP_RESTORE
RESTORE_MODULE_SUCCESS	The XChange module data has been restored	BACKUP_RESTORE
RESTORE_MODULES_COMPLETE	Restoration of XChange modules data is complete	BACKUP_RESTORE
SWITCHING_001	Device Activated	SWITCHING
SWITCHING_002	Device Deactivated	SWITCHING
SWITCHING_003	Group connectivity changed	SWITCHING
SWITCHING_004	WAN cable PLUG	SWITCHING
SWITCHING_005	WAN cable UNPLUG	SWITCHING
SYNCHRONIZATION_001	Synchronization completed	SYNCHRONIZATION
SYNCHRONIZATION_002	Commercial offer updated. Please reboot your box to apply changes	SYNCHRONIZATION
SYNCHRONIZATION_003	New firmware available	SYNCHRONIZATION
SYNCHRONIZATION_004	Synchronization failed	SYNCHRONIZATION
SYNCHRONIZATION_005	Box is active	SYNCHRONIZATION
SYNCHRONIZATION_006	Box is unauthorized	SYNCHRONIZATION
SYNCHRONIZATION_007	Prepaid mode has changed	SYNCHRONIZATION
SYNCHRONIZATION_008	OTA update request received	SYNCHRONIZATION
SYNCHRONIZATION_009	A new feature was activated	SYNCHRONIZATION
SYNCHRONIZATION_010	A feature was deactivated	SYNCHRONIZATION
SYSTEM_001	HDD partition almost full	MONITOR
SYSTEM_002	High CPU load detected	MONITOR
SYSTEM_003	High memory usage detected	MONITOR
SYSTEM_004	Large database size	MONITOR
SYSTEM_005	MMI skin updated. Please reboot to apply	SYSTEM
SYSTEM_006	Event log report mechanism has been stopped because the maximum number of logs has been reached	SYSTEM
SYSTEM_007	Exclusive Write Access updated	SYSTEM
SYSTEM_008	SSD health is low	MONITOR
SYSTEM_009	High CPU temperature detected	MONITOR
SYSTEM_010	High disk (HDD) temperature detected	MONITOR
SYSTEM_011	High disk (SSD) temperature detected	MONITOR
SYSTEM_012	High system temperature detected	MONITOR
SYSTEM_013	EWA right forced	SYSTEM
SYSTEM_014	Web cache clear launched	SYSTEM
SYSTEM_015	Successful web cache clearing	SYSTEM
SYSTEM_016	Web cache clearing failed	SYSTEM
SYSTEM_017	EWA dirty flag	SYSTEM
SYSTEM_018	Resized /mnt/data_user successfully	SYSTEM
SYSTEM_019	Too many processes already active	SYSTEM
SYSTEM_MIGRATION_ERROR	The migration of module database has failed	MODULE
TELTONIKA_001	Invalid password for API access. No more tries will be done until password reset.	SYSTEM
TELTONIKA_002	API fingerprint has changed	CYBERSECURITY
TELTONIKA_003	API credentials were updated	SYSTEM
TELTONIKA_004	Device reboot triggered	SYSTEM
TELTONIKA_005	SIM switching	SYSTEM
TELTONIKA_006	Networks scan triggered	CONNECTION

TELTONIKA_007	Modem connection triggered	CONNECTION
TELTONIKA_008	Modem disconnection triggered	CONNECTION
TIME_SYNCHRO_001	System time synchronization error	TIME_SYNCHRO
TIME_SYNCHRO_002	System requires reboot for time synchronization	TIME_SYNCHRO
TIME_SYNCHRO_003	System time synchronized	TIME_SYNCHRO
TIME_SYNCHRO_004	Time zone changed	TIME_SYNCHRO
TIME_SYNCHRO_005	Irrelevant time detected. Time synchronization triggered.	TIME_SYNCHRO
TIME_SYNCHRO_006	Time synchronization successfully triggered. Box may restart soon.	TIME_SYNCHRO
TIME_SYNCHRO_007	Time synchronization task could not be started	TIME_SYNCHRO
UPDATE_001	Firmware download in progress	UPDATE
UPDATE_002	Firmware download completed	UPDATE
UPDATE_003	Firmware update failed	UPDATE
UPDATE_004	Firmware installation in progress	UPDATE
UPDATE_005	Firmware installation completed	UPDATE
UPDATE_006	Security update installed	UPDATE
UPDATE_007	Security update available. Please reboot to apply	UPDATE
UPDATE_008	Critical security update installed, which enforces reboot	UPDATE
UPDATE_009	Update failed	UPDATE
UPDATE_010	Data connection available	UPDATE
UPDATE_011	Data connection is missing	UPDATE
UPDATE_012	Additional patches need to be downloaded	UPDATE
UPDATE_013	Update patch step successfully done	UPDATE
UPDATE_014	An error occurred during update patch step	UPDATE
UPDATE_015	Local update zip integrity check succeeded	UPDATE
UPDATE_016	Local update zip integrity check failed	UPDATE
UPDATE_017	Update backup successfully created	UPDATE
UPDATE_018	Update backup creation failed	UPDATE
UPDATE_019	Diagnostic file successfully created	UPDATE
UPDATE_020	Failed to create diagnostic file	UPDATE
UPDATE_021	System snapshot successfully created	UPDATE
UPDATE_022	Failed to create system snapshot	UPDATE
UPDATE_023	Patch synchronization successfully done	UPDATE
UPDATE_024	Import of GPG keys has failed. It is needed to backup and update. Please contact support.	UPDATE
UPDATE_025	Import of GPG keys succeeded	UPDATE
UPDATE_026	The scan of update packages revealed an issue.	UPDATE
UPDATE_027	New firmware update is available.	UPDATE
UPDATE_028	New firmware update installation started.	UPDATE
UPDATE_029	Mandatory module is missing	UPDATE
USER_001	User account automatically deleted	USER
USER_002	Large number of users detected	USER
VSAT_001	New VSAT modem detected	CONNECTION

13.Appendix B – List of Supported Controlled Devices

Please see the list of currently supported and controlled devices:

#	MANUFACTURER	DEVICE MODEL	CONTROLLED	SUPPORTED
1	Cobham	BGAN Explorer 700	√	√
2	Cobham	FleetBroadband Sailor 150	√	√
3	Cobham	FleetBroadband Sailor 250	√	√
4	Cobham	FleetBroadband Sailor 500	√	√
5	JRC	FleetBroadband JUE – 250 EoL	√	√
6	JRC	FleetBroadband JUE – 500 EoL	√	√
7	JRC	FleetBroadband JUE – 251	√	√
8	JRC	FleetBroadband JUE – 501	√	√
9	Furuno	FleetBroadband Felcom 250	√	√
10	Furuno	FleetBroadband Felcom 500	√	√
11	Intellian	FleetBroadband 250	√	√
12	Intellian	FleetBroadband 500	√	√
13	AddValue	FleetBroadband 250	√	√
14	AddValue	FleetBroadband 500	√	√
15	Marlink	Sealink VSAT on iDirect X7	√	√
16	Marlink	Sealink VSAT on Newtec Dialog	√	√
17	Marlink	Marlink 4G Teltonika RUT 950/ WiFi Option	√	√
18	Inmarsat FX	XChangeFX	√	√
19	Iridium	Iridium Open Port / Pilot	√	√
20	Iridium	Certus Thales VesseLink	√	√
21	Iridium	Certus Sailor 4300	√	√
22	Thuraya	Thuraya IP		√
23	UMTS/3G/4G/5G	Any mobile broadband router		√

24	Others	WiMax, other VSAT, other FleetBroadband		√
#	MANUFACTURER	DEVICE MODEL	CONTROLLED	SUPPORTED
25	SpaceX	Starlink Maritime	√	√
26	OneWeb	OneWeb		√
27	Iridium	Intellian Certus C700	√	√

14. Appendix C – List of Notifications

Please see the list of currently used messages in the notifications:

#	MESSAGE	SHORT DESCRIPTION
1	“Analog configuration has changed. The voice card support have been restored. Please check if devices must be re-configured by passing a wizard."	The system warns that analog configuration has been changed and that devices shall be adapted to this new configuration.
2	“Analog configuration has changed, some analog ports are now missing. Please check if you need to adapt the voice card configuration."	The system detected that some analog ports are missing on voice card configuration.
3	“Analog configuration has changed. You should restore voice card support. “	The system detected that a newly applied analogue voice card configuration differs from the current configuration.
4	"You have been disconnected by an administrator"	The captain manually disconnected the call or data session
5	"Security software update has to be installed. The box is about to be restarted. We apologize for the inconvenience"	If an important system patch is installed and a reboot is forced automatically
6	"Your network access settings have been changed: you are not allowed to open data sessions on this LAN."	When the users group is not allowed on a LAN
7	"Security update available. Please reboot to apply"	If a system patch is installed and a reboot is needed
8	"New credit request"	Displayed for the Captain when new credit requests are available
9	"New Price matrix(es) have been applied"	Shown when the prices for a communication device is changed through P360
10	"An important update is available. Please click "START UPDATE" to proceed now. If not a suitable timing, you can ignore the update for now. Note that the update will be triggered automatically by ${time} UTC at the latest" START UPDATE / ASK ME LATER	If the shore Administrator pushed a firmware update to be performed semi-automatically. The system will wait for Captains input. Install triggered at the latest 72h after firmware is downloaded if captain does not click on START UPDATE.
11	"A system update is planned. Your XChange is updating to version ${version}. Service will be unavailable for several minutes. PLEASE DO NOT REBOOT THE XCHANGE."	If the shore Administrator pushed a firmware update to be performed semi-automatically or automatically. This notification is displayed as soon as the XChange box gets the OTA order from shore.

12	"System clock update. Please reboot to apply changes. The system will reboot automatically on ${when} UTC." ‘Reebot Now” “Reboot In” (1h/6h/12h/18h/ As planned)	Displayed for Captain when a reboot is needed to apply the time synchro. Reboot will be automatically done 24h after the notification is triggered or it can be planned to (1h/6h/12h/18h/ As planned)
13	"New security update available. Please reboot to apply changes. The system will reboot automatically on ${when} UTC." ‘Reebot Now” “Reboot In” (1h/6h/12h/18h/ As planned)	Displayed for Captain when a reboot is needed to apply a system patch. Reboot will be automatically done 48h after the notification is triggered or it can be planned to (1h/6h/12h/18h/ As planned)
14	"Some XChange functionalities have been updated. Please reboot to apply changes. The system will reboot automatically on ${when} UTC." ‘Reebot Now” “Reboot In” (1h/6h/12h/18h/ As planned)	Displayed for Captain when a reboot is needed to apply a module firmware update. Reboot will be automatically done 72h after the notification is triggered or it can be planned to (1h/6h/12h/18h/ As planned)
15	“A new XChange hypervisor update is ready for installation. All Virtual Machines will be restarted at <date:time>. Click here to change the scheduled date.”	Displayed for Captain when the hypervisor OVP is ready to apply a firmware update. Reboot will be automatically done 72h after the notification is triggered or it can be planned to (1h/6h/12h/18h/ As planned) Clicking on “here” opens the OVP page to change the schedule.

15. Appendix D - Hardware and Operating System

The XChange is provided with different hardware options. The available services do not differ between the models available. The XChange Base is the smallest unit available offering a slightly limited number of supported networks and IP-telephony only.

The XChange Power is delivered on 1 of 2 19" rack-mountable units. There is no difference in performance or service availability between any of the 2 XChange Power units.

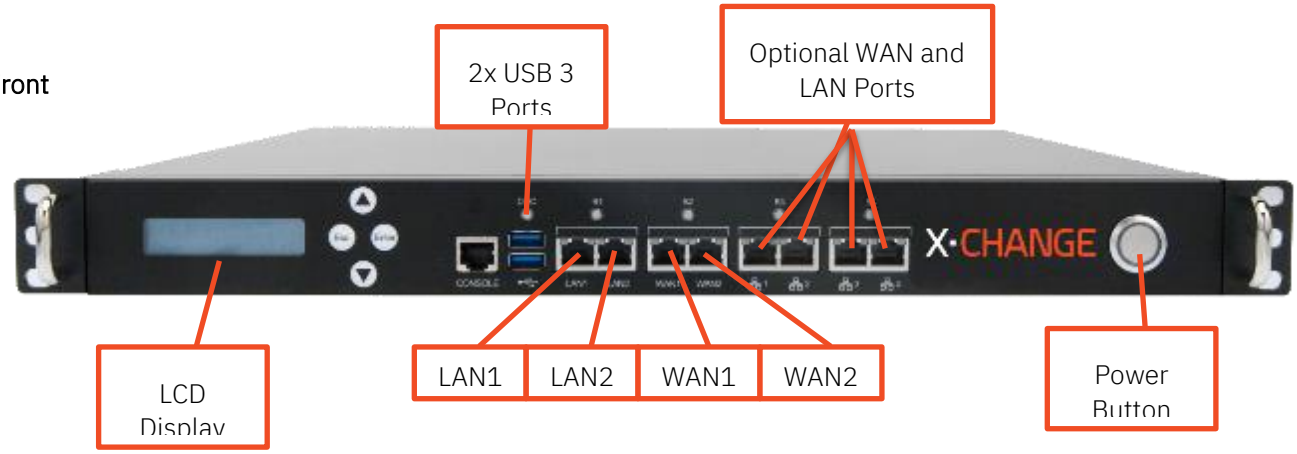
15.1 XChange Power NSA5150 Rack Mount 19" Unit

15.1.1 Specifications

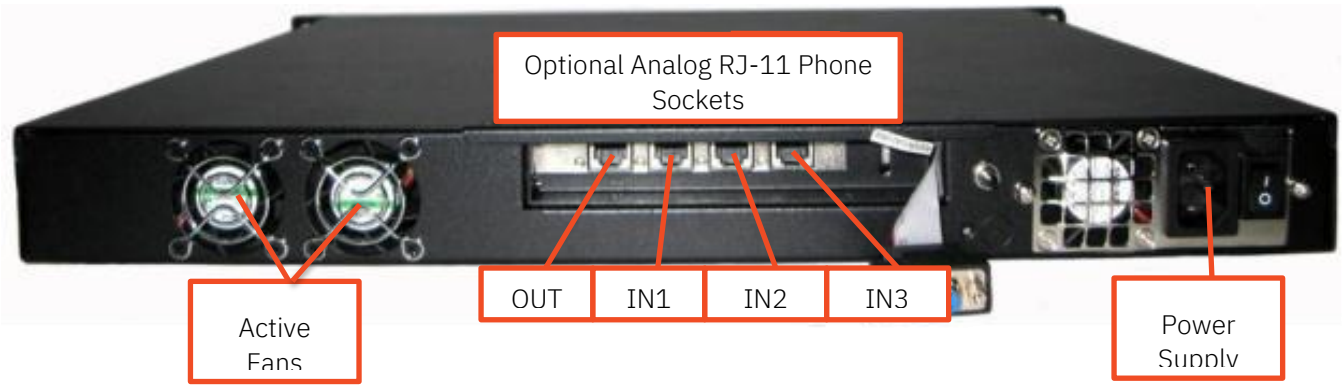
description	
Type	Rack Units (ATX AC or DC)
Dimensions	426mm x 450mm x 44mm
Weight	8 kg (16 lb)
Mounting	1U Rack Mount
System	
Operating System	Linux
Processor	Intel i7TM 4770TE 2.3 GHz
RAM	DDR3 16 GB
Storage	
System SSD (Main)	Industrial 2.5" SSD 256 GB
Content HDD (Secondary)	Industrial 2.5" HDD 1 TB
Power	
Supply	DC 20–28 V or AC 100–240 V
Consumption	200 W
Ports	
Ethernet (RJ-45) (10/100/1000 Mbits)	2 WAN and 2 LAN Fixed Up to 4 WAN/LAN Optionally Selectable
Voice (RJ-11)	Optional 1x FXO/3FXS
USB	4x
Serial (RS232)	N/A
Robustness (Incl. HDD)	
Vibration	1 g rms (5–500 Hz, 3 axis)
Shock	20 g (11 ms, 3 axis)
Humidity	0%–95%
Operating Temperature	-5 °C (+23 °F) to +45 °C (+113 °F)
Miscellaneous	
	Power On/Off, LCD Display, Activity LED

15.1.2 Port Overview XChange Power

Front



Back

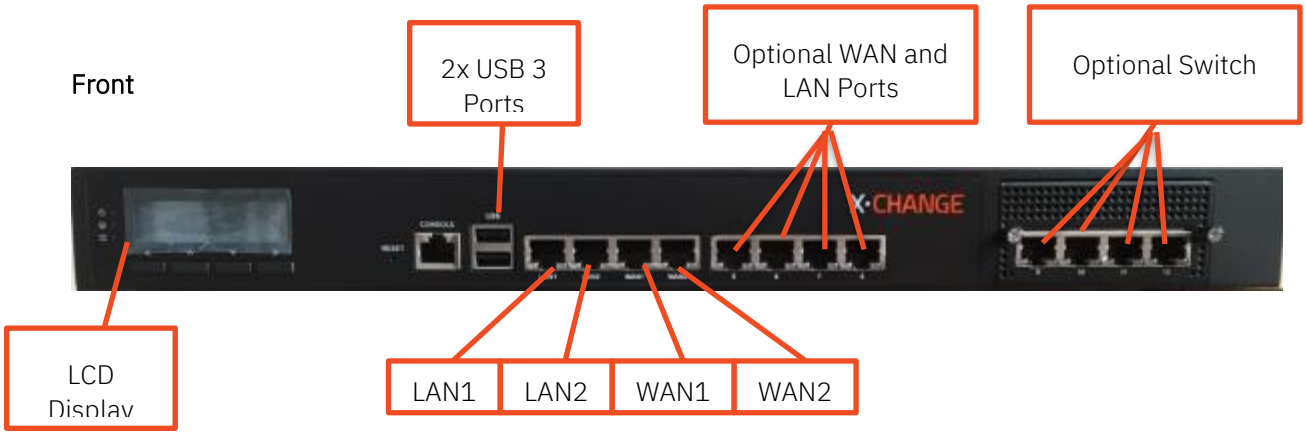


15.2 XChange Power OVP800 Rack Mount 19” Unit

15.2.1 Specifications

description	
Type	Rack Units (ATX AC or DC)
Dimensions	438mm x 321mm x 44mm
Weight	6 kg (12 lb)
Mounting	1U Rack Mount
System	
Operating System	Linux
Processor	Intel Xeon D-1518 2,2 GHz
RAM	DDR4 16 GB
Storage	
System & Content SSD	Industrial 2.5” SSD 1 TB
Power	
Supply	DC 20–28 V or AC 100–240 V
Consumption	220 W
Ports	
Ethernet (RJ-45) (10/100/1000 Mbits)	2 WAN and 2 LAN Fixed Plus 4 WAN/LAN Optionally Selectable Plus 4-port switch
Voice (RJ-11)	Optional 1x FXO/3FXS
USB	2x
Console (RJ45)	1x
Robustness (Incl. HDD)	
Vibration	1 g rms (5–500 Hz, 3 axis)
Shock	20 g (11 ms, 3 axis)
Humidity	0%–95%
Operating Temperature	-5 °C (+23 °F) to +45 °C (+113 °F)
Miscellaneous	
	Power On/Off, LCD Display, Activity LED

15.2.2 Port Overview XChange Power OVP800



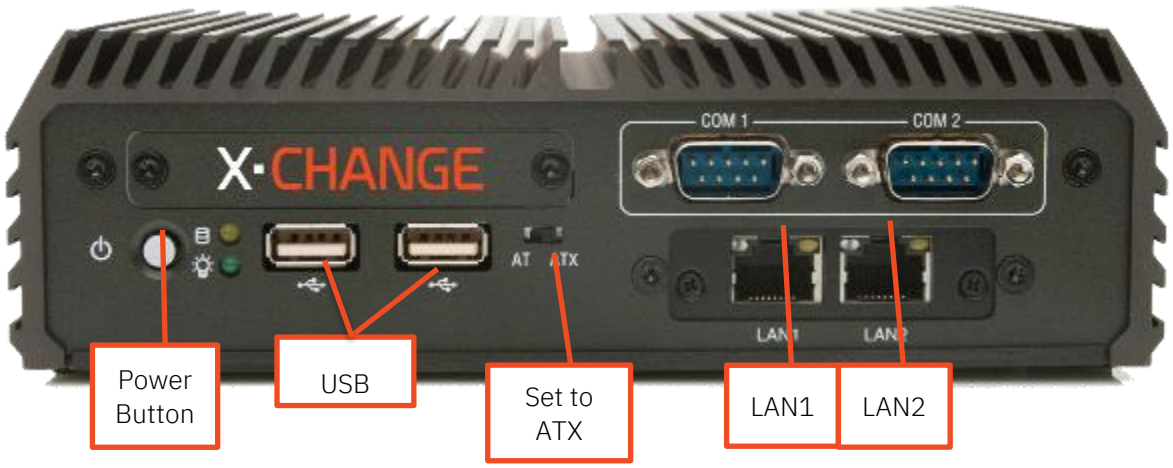
15.3 XChange Base

15.3.1 Specifications

description	
Type	Compact Unit (ATX DC) - Silent
Dimensions	185mm x 131mm x 54mm
Weight	2 kg (4 lb)
Mounting	Desk, Wall Mount or 2U Rack Mount
System	
Operating System	Linux
Processor	Intel Atom™ E3845 1.91 GHz
RAM	DDR3 8 GB
Storage	
System SSD (Main)	Industrial 2.5” SSD 128 GB
Content HDD (Secondary)	N/A
Power	
Supply	DC 9–28 V (optional: AC/DC adapter 90–240 V)
Consumption	60 W
Ports	
Ethernet (RJ-45) (10/100/1000 Mbps)	2 WAN and 2 LAN fixed
Voice (RJ-11)	N/A
USB	4x
Serial (RS232)	4x (not used)
Robustness (Incl. HDD)	
Vibration	5 g rms (5–500 Hz, 3 axis)
Shock	50 g (11 ms, 3 axis)
Humidity	0%–95%
Operating Temperature	-5 °C (+23 °F) to +45 °C (+113 °F)
Miscellaneous	
	Power On/Off, Activity LED

15.3.2 Port Overview XChange Base

Front



Back