MARLINK

XCHANGE

MARLINK

On board Installation Guide

November 2024

Ref: Version 5.6

Table of Contents

1. INTRODUCTION

This document is designed to guide installers through the XChange installation and configuration process.

1.1 Preparation

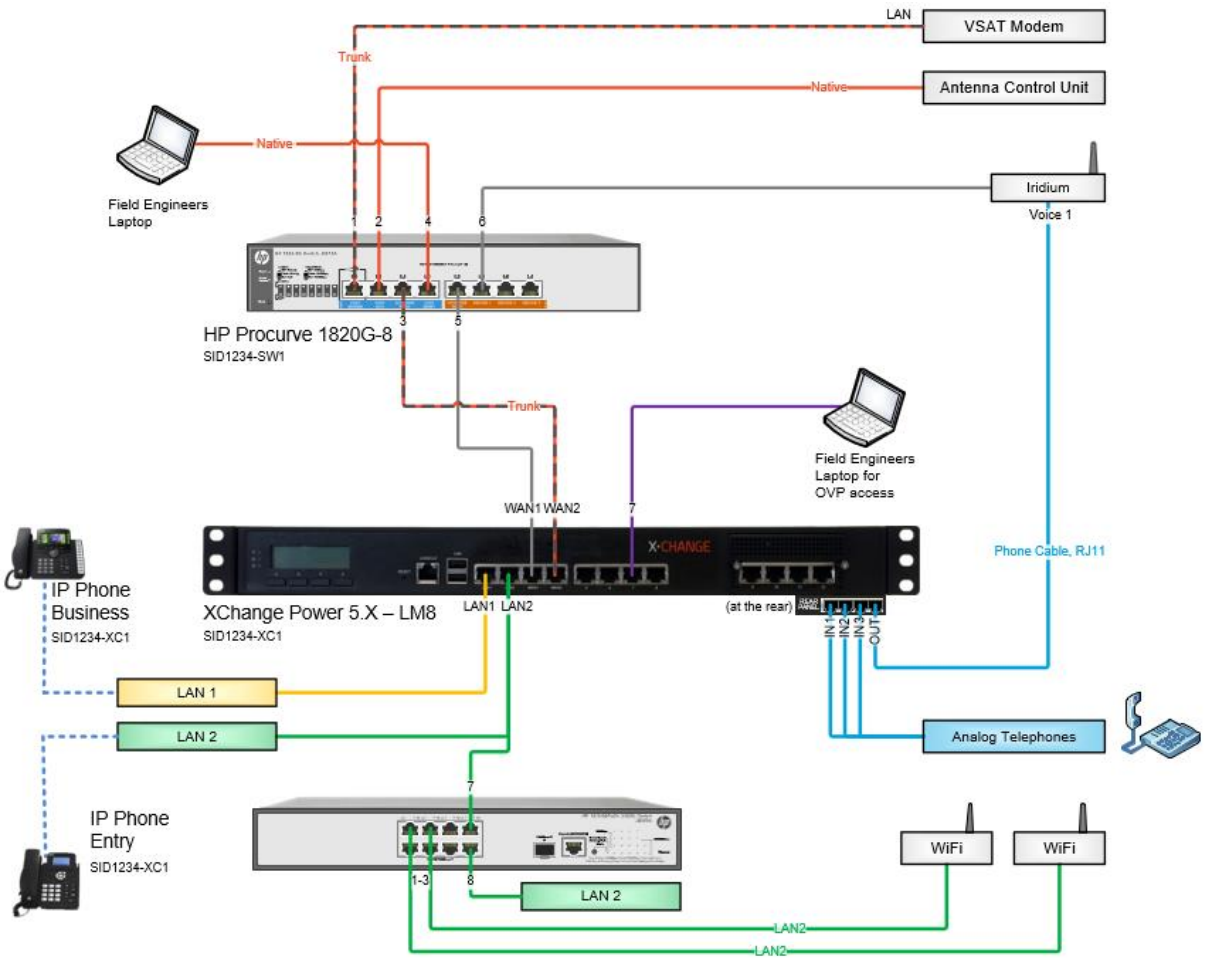
Before going on board, ensure the following listed prerequisites are fulfilled and you have all required information available:

- All required information in the IOF/COF are duly filled by previous departments.
- An XChange Solution Design Blueprint document is available
- You received the network drawing with all IP addresses and phone numbers.

2. Installation

Before starting the XChange Box, all physical connections between the XChange Box and any equipment to be connected communication device must be done.

Use the network drawing for orientation.



2.1 Terminal Connections for Data into VSAT Switch

To streamline Marlink´s VSAT installations, please note that all connected communication devices must be connected to the VSAT switch. A direct connection of e.g. the MSS backup to an XChange WAN port must be avoided.

The table below illustrates the possible devices connecting to the LAN of the VSAT switch port:

VSAT Port No	VSAT Port Name	Communication Equipment
1	VSAT Modem	VSAT Newtec Modem
2	VSAT ACU	VSAT Antenna Control Unit
3	XChange WAN 2	XChange WAN 2 Port
4	VSAT MGMT	Empty
5	XChange WAN 1	XChange WAN 1 Port
6	Device 1	1st Backup Terminal
7	Device 2	2nd Backup Terminal
8	Device 3	3rd Backup Terminal

IMPORTANT

Any Sealink or FleetXPress device must be connected to the WAN2 port of the XChange without exception.

Please follow the XChangeFX configuration guide when XChangeFX will be installed on board.

Any Starlink device must be connected to network port 7 or 8 directly of XChange Power. The cabling instructions provided must be strictly followed.

2.1.1 VSAT

The Marlink VSAT equipment must be connected as listed in the table above. Neither connect any equipment to a different port on the VSAT switch nor connect any component directly to the XChange unless stated otherwise.

The WAN port 2 of the XChange must always be connected to port 3 of the Switch.

Port 4 of the switch must be kept empty. Only Marlink support equipment (Field Engineers Laptop) can use that port connection.

2.1.2 FleetXpress / XChangeFX

The XChangeFX equipment must be connected as described in the separate installation manual. After XFX setup, follow this manual to finish the configuration of XChange to manage the XChangeFX.

2.1.3 Fleet Broadband

A Fleet Broadband terminal can be connected to any port between 6-8 of the VSAT Switch.

Please Note

In a “MSS only” setup, the VSAT switch is not delivered. Here the controlled Fleet Broadband can be connected to a WAN port of the XChange directly.

2.1.4 Iridium

An Iridium Open Port (Pilot) or Certus terminal can be connected to any port between 6-8 of the VSAT switch.

Please Note
In a “MSS only” setup, the VSAT switch is not delivered. Here the Iridium can be connected to a WAN port of the XChange directly.

2.1.5 Other Broadband Services

A 3rd party broadband service like Marlink 4G, ICE… can be connected to any port between 6-8 of the VSAT switch.

Please Note
In a “MSS only” setup, the VSAT switch is not delivered. Here the other broadband service can be connected to a WAN port of the XChange directly.

2.1.6 Multiple Broadband Services without VSAT on XChange Base

For setups without a Marlink VSAT, no VSAT switch is delivered. Up to 2 Broadband terminals can be connected directly to WAN ports 1 or 2 of the XChange Base unit.

If more than 2 broadband terminals must be connected, a switch must be connected between WAN2 and the broadband terminals.

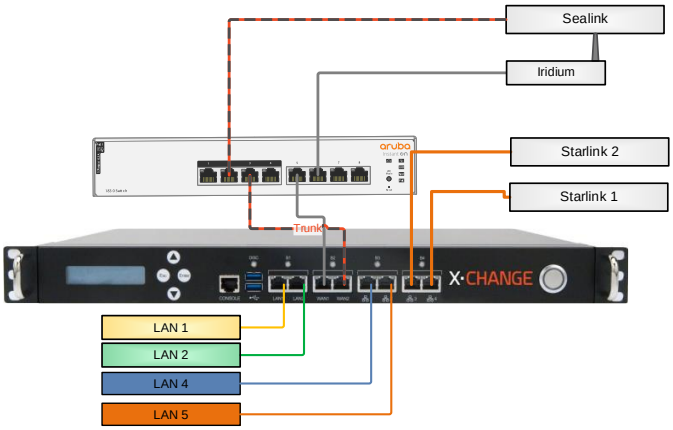
2.1.7 Multiple Broadband Services without VSAT on XChange Power

For setups without a Marlink VSAT, no VSAT switch is delivered. Up to 6 Broadband terminals can be connected directly to WAN ports of the XChange Power unit.

2.1.8 Starlink

Starlink is supported by XChange. Always follow the installation documentation and IT Policy and follow strictly the cabling instructions.

2.1.8.1 Starlink on XChange Power

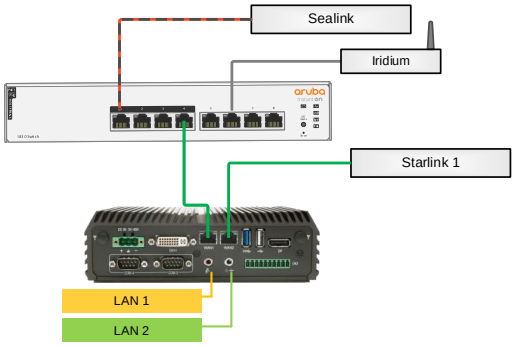


Starlink must be connected to the last 2 ports of an XChange Power.

- 1st Starlink to be connected to port 8
- 2nd Starlink (optionally) to be connected to port 7

2.1.8.2 Starlink on XChange Base

XChange Base supports up to 1 Starlink antenna. In total 2 connectivity services can be supported.



- Starlink must be connected to WAN1

Other connectivities can remain connected to the WAN switch as drawn above but cannot be used. This temporary limitation will be removed during 2024.

2.1.8.3 Starlink by Marlink

During the installation wizard, if the Starlink is provided by Marlink and/or activated through Marlink the device driver “Starlink” must be selected.

2.1.8.4 Starlink not by Marlink

During installation wizard, if the Starlink is not provided by Marlink and not activated through Marlink an “Autonomous Device” driver must be selected. Do not use the Starlink driver in such a case.

2.2 Terminal connections for voice

Important
The Analog voice card is declared End of Sale. Marlink maintains for no long time the analog card as a component. It´s recommended to not use the analog voice card anymore.

3. Pre-boarding Preparations

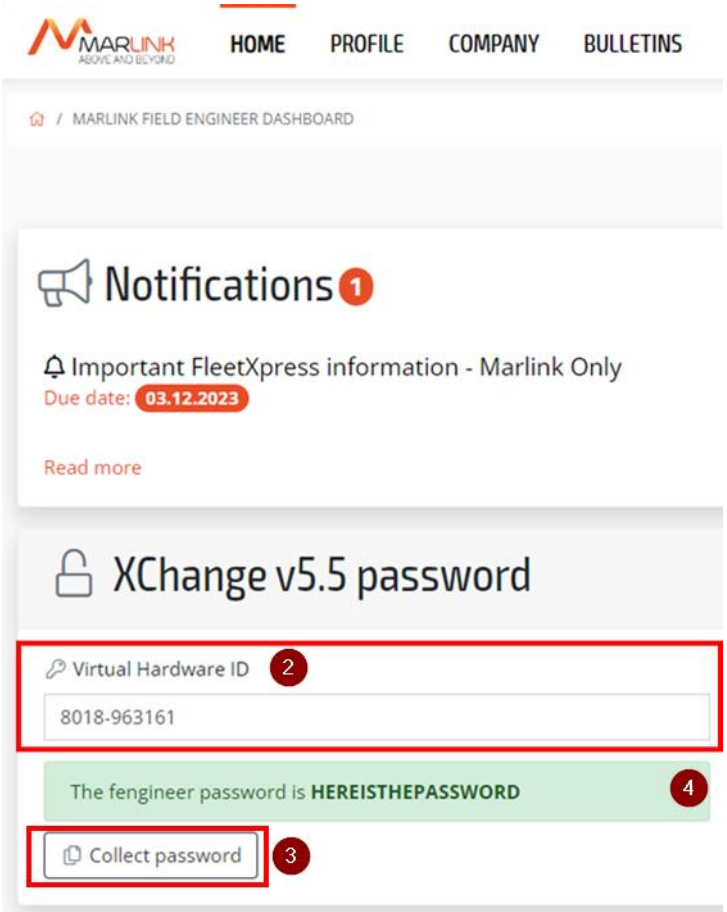
With XChange core version 5.5, the 'superadmin' account and fixed passwords were removed. As from XChange version 5.5, a dedicated "fengineer" account must be used.

A unique password will be generated using the XChange Hardware ID on each attempt and can be retrieved from your Field Service Portal login.

The XChange Hardware ID should be mentioned in the scope of work or Ticket the.

To retrieve the password, follow the below steps:

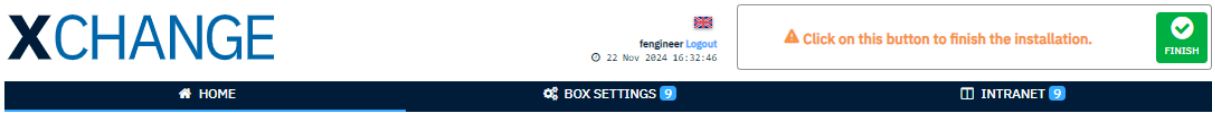
1. Login to the https://fieldservice.sealink.net/ (Only Marlink-certified engineers have or will receive access). You can find an XChange password tool on the Home page.
2. Fill the XChange box Virtual Hardware ID with the "-" into the Field Service Portal. The Virtual Hardware ID can be found in the lower-right corner of the XChange log-in page. For XChange Power the Hardware ID printed on the box and the Virtual Hardware ID are different.
3. Click on the 'Collect Password' button and the password is automatically copied for your convenience.
4. The password will be displayed.
5. Save the password for this installation safely before logging in to the XChange with the "fengineer" user account.



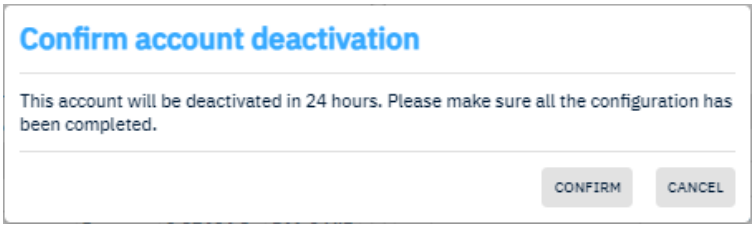
NOTE: If no hardware ID is known or there was no chance to retrieve the password before onboarding the installation site, contact Marlink Service Desk to request the password.

3.1 Finalisation of an Installation

Field engineers who have completed the XChange's installation, configuration and final testing using the 'fengineer' account should click on the "FINISH" button before leaving the vessel.



Once the action above is triggered, the 'fengineer' account **WILL BE DISABLED** 24 hours later after clicking on the "CONFIRM" button as indicated in the message below.



➔ <u>This step is mandatory to officially finalise the installation and officially hand over the system to the customer.</u>

3.2 Field Engineer Account automatic deactivation

If the step above is forgotten, the 'fengineer' account is deactivated automatically 96 hours after the first login. Ensure you start setting up the XChange once all preparations are completed. It is not possible to reopen a deactivated account locally. If the 'fengineer' account needs to be opened, please call the Service Desk.

IMPORTANT
When attending a vessel where XChange 5.5 is already installed, the 'fengineer' account will be disabled. The only way to enable the account is to call the Service Desk and kindly ask them to enable the account. The Service desk can also provide the 'fengineer' password for that box. Or you can get the password from the field service portal as described above.

4. Special Instructions for SNG Installations

Marlink SNG is a single subscription service integrating:

- Marlink Starlink
- Sealink and
- XChange SmartEdge platform

Into one service with one contract, one subscription and one invoice.

The described guidelines and rules are strictly to be followed.

4.1 SNG Fair use policy on XChange

For SNG installations specific rules apply. Below described XChange parameters are fixed to ensure Marlink´s fair use policy and cannot be altered on customer´s demand:

- An "SNG IT Policy" per SNG installation must be prepared
- The network design is fixed
- XChange Switching option must be "SD-WAN Lite"
- Automatic device switching is reinforced (Setup from shore)
- Other connectivity services remain
- Data traffic routing is split between:
  - Business critical communication via Sealink
  - Crew and personal communication via Starlink

4.2 SNG with Other Connectivity Services

Other connectivity services can remain connected and used through XChange.

On XChange Base additional connectivity services can be re-integrated with additional Field Service attendance after Firmware update version 5.6 is launched.

On XChange Power any additional connectivity service can be used.

MSS Backups can be kept in deactivated mode or removed from vessel, as per customer´s choice.

- Network design rules must be strictly followed
- Data routing rules apply (see below)

4.3 Device Ranking

The device ranking and data routing per type of user group must be strictly followed.

- Device ranking
  - Within SNG, Sealink is always higher ranked that Starlink.
    - Rank 1: Sealink
    - Rank 2: Starlink

Regardless of the device ranking within SNG connectivity following applies:

- Business Critical communication must be routed via Sealink first, Starlink second
- Crew and private communication shall not be routed via Sealink, only Starlink
- XChange System traffic shall be routed via Sealink
- XChange File Cloud traffic shall be routed via Starlink.

Device Ranking SNG only

In SNG-only installation following global device ranking applies*:

- Rank 1: Sealink
- Rank 2: Starlink

*on XChange Base this is the only valid device ranking for the time being

Device Ranking SNG plus additional Connectivity

Ranking of additional connectivity can be chosen by the customer.

Example with 4G and MSS Backup:

- Rank 1: 4G
- Rank 2: Sealink
- Rank 3: Starlink
- Rank 4: MSS Backup

➢ It is not allowed to rank the 4G between Sealink and Starlink. The SNG connectivity must be grouped next to each other in the ranking.

4.9 Data Routing Template

Data communication must be routed differently:

➢ Business Critical communication must be routed via Sealink
➢ Crew and personal communication must be routed via Starlink

4.9.1 Business Critical Communication

Business relevant user groups, networks, machines accounts must be routed via Sealink as 1st device and Starlink as 2nd.

If more connectivity services are available, customer can choose to use the additional connectivity services as main device before Sealink or as a backup after Starlink.

Typical business critical user groups are:

- Machine accounts, Captain (opt)
- OpenLAN for corporate networks
- XChange system traffic for data synchronization, remote access…

Business Critical Communication Examples:

- Corporate Emails
- Engine control, IOT networks
- Navigation charts updates
- VPN communication
- URA or other remote access services.

4.9.2 Crew Communication

Crew or private communication user groups, networks, machine accounts must be routed via Starlink only. Sealink has not to be assigned to these types of users.

Typical crew communication user groups are:

- Captain
- Officer, Crew
- Clients, Visitors
- Crew LAN OpenLAN
- XChange Cloud

Crew Communication Examples:

- Netflix, Youtube
- Web surfing, Social Media

4.9.3 Payment Modes

The XChange payment modes, Local allowance & Corporate, do not influence the routing. Customer is free to chose if user groups should be in local allowance or corporate usage.

Please Note: In case a SNG contract includes Marlink´s prepaid service, separate rules do apply. These will be available in a separate document after the service has been launched.

4.9.4 Default User Group routing Overview

User Group	Type	1st Device	2nd Device
Captain	Private/Crew	Starlink	Sealink
Cloud	Private/Crew	Starlink	Sealink
Crew	Private/Crew	Starlink	
EcoHost/System	Business Critical	Sealink	Starlink
Machine	Business Critical	Sealink	Starlink
NewEntry	Private/Crew	Starlink	
Officer	Private/Crew	Starlink	
OpenLAN	Private/Crew	Starlink	
OpenLAN	Business Critical	Sealink	Starlink

Any additional user group must be setup following above principles.

If additional connectivity services are available, customer can choose to route for example:

User Group	Type	1st Device	2nd Device	3rd Device	4th Device
Captain	Private/Crew	4G	Starlink	Sealink	MSS Backup
Cloud	Private/Crew		Starlink	Sealink	
Crew	Private/Crew		Starlink		
EcoHost	Business Critical	4G	Sealink	Starlink	
Machine	Business Critical	4G	Sealink	Starlink	MSS Backup
NewEntry	Private/Crew	Starlink	4G		
Officer	Private/Crew	Starlink	4G		
OpenLAN	Private/Crew	Starlink	4G		
OpenLAN	Business Critical		Sealink	Starlink	

5. XChange Installation

Before starting the XChange Box, ensure all communication devices are connected properly and at least one device is ready to go online.

Connect your Computer to a LAN controlled by XChange and access the XChange interface using your web browser via the URL https://xchange-box.com.

XChange Base

When starting the XChange Base for the first time, you ´re directed to the Installation Wizard immediately after login.

XChange Power

When starting the XChange Power for the first time, through XChange Login page you can directly arrive at the XChange dashboard.

IMPORTANT

The wizard can be started by an authorized installer at any time to reconfigure the XChange Box. To restart the wizard, login as 'fengineer' and go to *Box Settings > System > Start Wizard.*

The 'fengineer' access is restricted to Marlink personnel and qualified installers only! The fengineer access details shall never be left on board or given to any end customer representative.

5.1 Starting the configuration

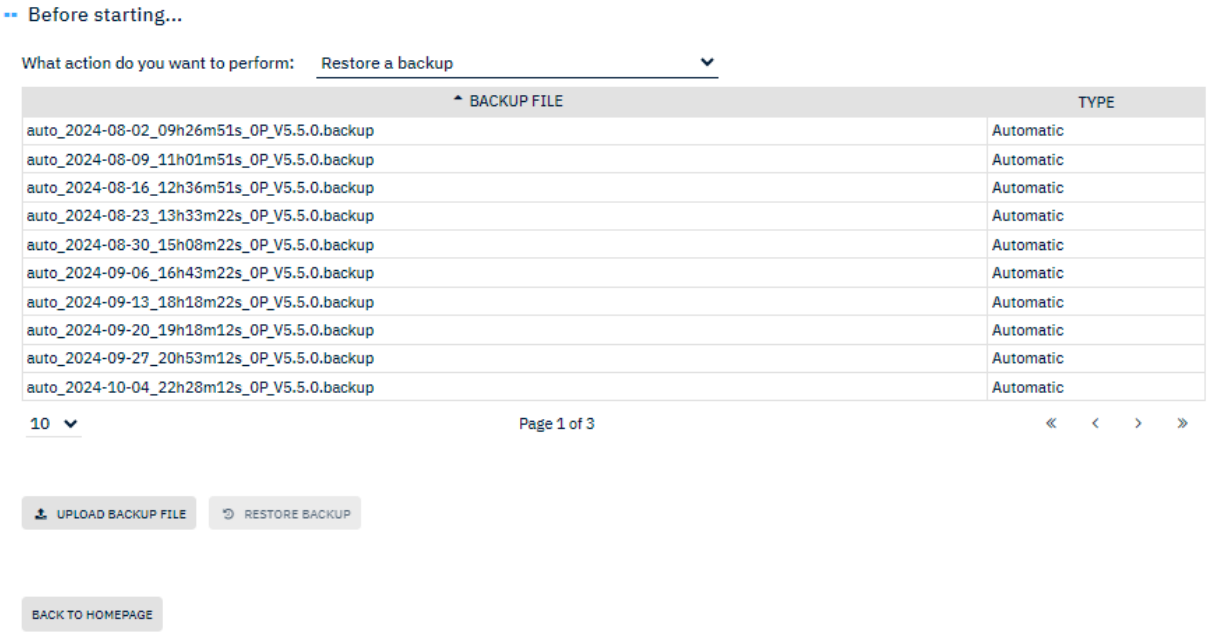
To access the XChange Installation wizard go to: *Box Settings > System > Start Wizard*

Select the action which should be performed:

1. Restore from a backup file
2. Proceed with wizard

In case of a box-swap or fleet-wide deployment of the XChange with a similar configuration, the 'Restore a backup' option should be selected.

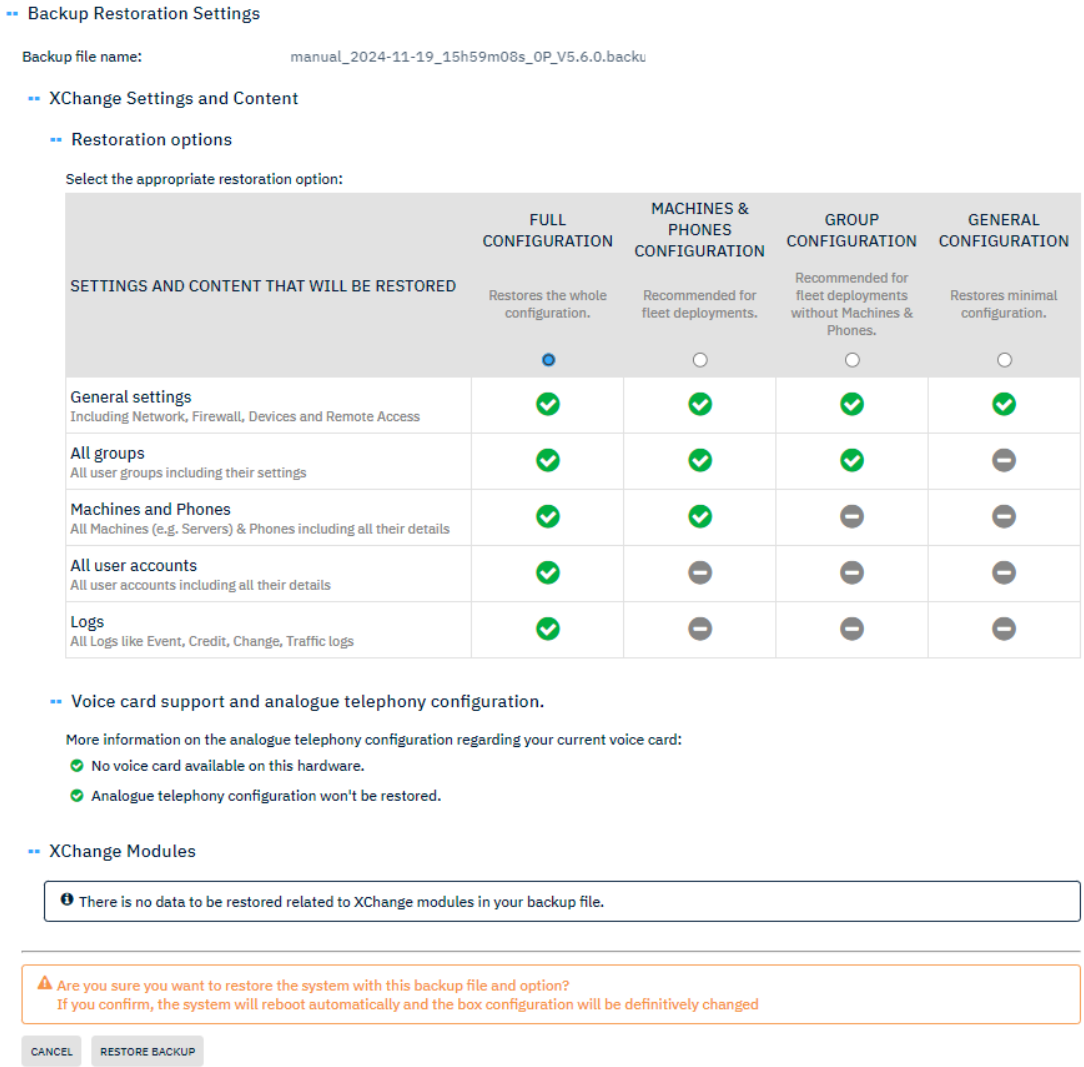
When backup files are already stored locally, a table provides all available files. In addition, a backup file can be uploaded from the Installer's computer.



For a new installation, select option 2 'Start Installation Wizard' and follow the next steps.

5.1.1 Import 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.

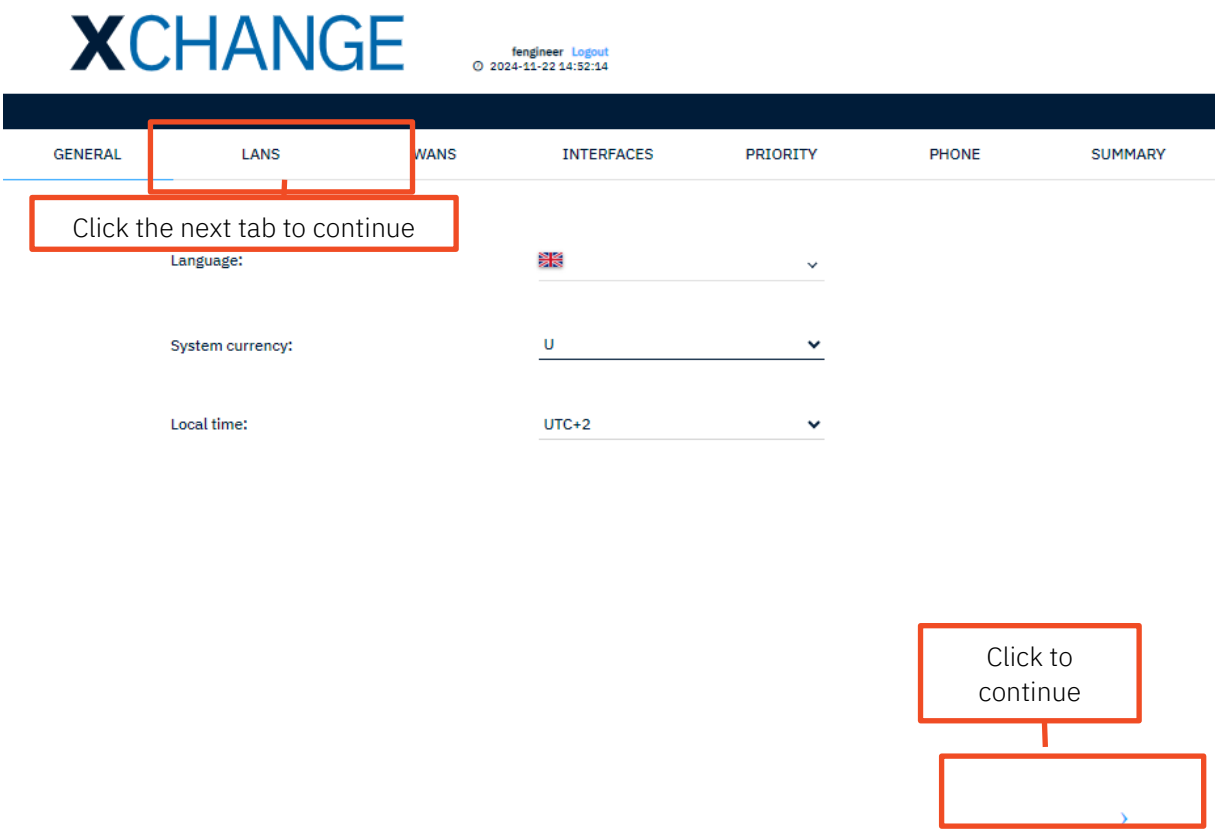
5.2 General Configuration

For a new installation, select the 'Start Installation Wizard' option and follow the next steps:

The first tab is called 'General Configuration' and contains settings such as:

- Default Language
- System currency ($-dollar, €-Euro or U-Units)
- Local system time (UTC offset)

Once completed, either click the small orange arrow on the bottom-right or click the tab on top.



5.3 LAN Configuration

On any XChange two local access networks are prepared in default.

Please follow the detailed LAN-IP settings according to the Network Drawing. Depending on the specific installation requirements the existing networks can be kept and adjusted or new ones can be added.

5.3.1 Network Management Modes

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

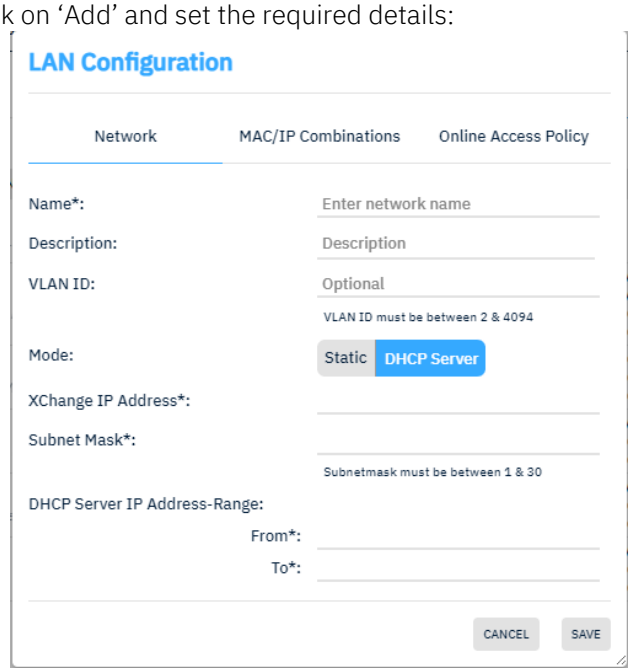
Access Mode: This mode is used for end devices such as computers, printers, and IP phones. Each port in Access mode can be assigned to only one network with or without VLAN-ID and typically connects to a single device or a LAN. It ensures that traffic from the device/LAN is carried only within its designated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

5.3.2 Creating new Networks

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

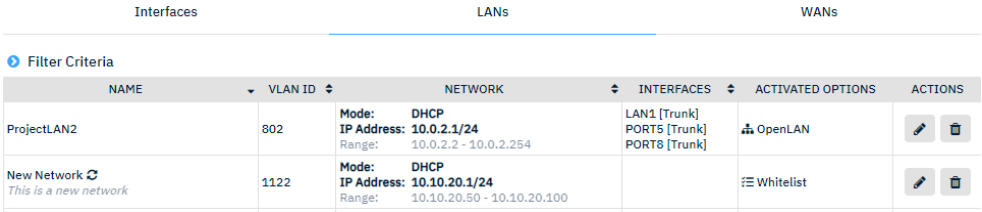
If DHCP is enabled, the embedded DHCP service requires a valid IP Address-range within the same IP Address-range like the XChange IP Address.

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.

Strickly follow the instructions provided

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



5.3.2.1 Excluded IP ranges

Some IP ranges are excluded and shall not be used for a LAN on board, independent of whether DHCP or static IP-addressing is selected.

The following IP ranges cannot be used to avoid conflicts with the system itself:

10.10.102.0/24	172.31.3.0/24
10.10.103.0/24	172.31.8.0/21
10.11.0.0/16	172.31.16.0/21
10.12.0.0/16	172.31.24.0/21
10.13.0.0/16	172.31.32.0/21
10.0.9.0/24	172.31.40.0/21
10.242.16.0/24	

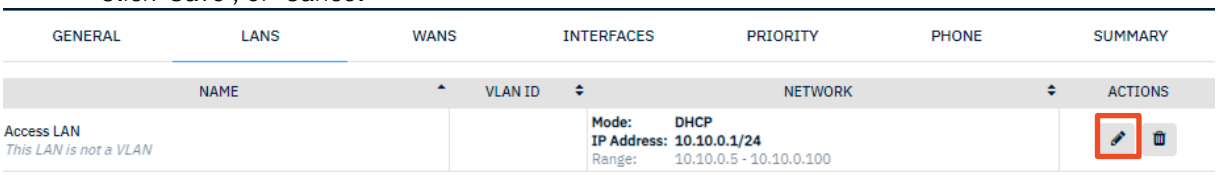
PLEASE NOTE

To avoid conflicts, the system prevents the use of the same IP range for communication devices on the WAN side and on local networks (LAN). Marlink recommends the use of the factory default IP address ranges starting with 10.0.x.x.

5.3.3 Edit LAN Settings

Any LAN in the list can be changed at any time.

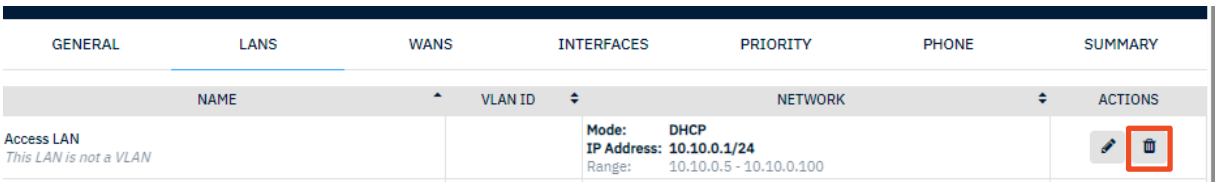
- Click on the 'Edit' icon of the LAN
- Change the LAN or DHCP server details
- Change the IP addressing if required
- Add or remove a VLAN-ID if required
- Assign new MAC to IP addresses or remove any existing
- Click 'Save', or 'Cancel'



5.3.4 Delete LANs

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

- Click on the 'Delete' icon of the LAN
- Click 'Delete' to confirm or 'Cancel'

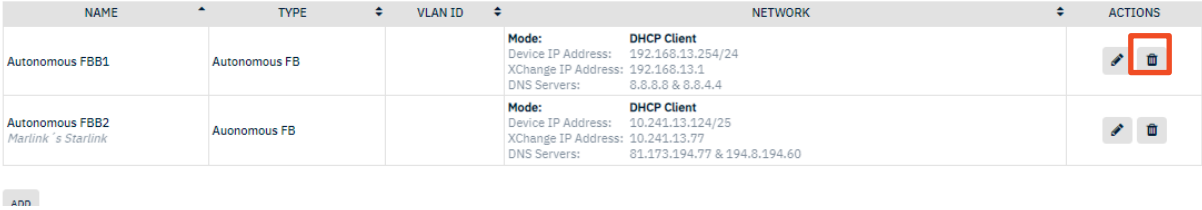


5.4 WAN Device Setup

5.4.1 XChange Power preparation

XChange Power units are preinstalled with 2 “Autonomous FleetBroadband” devices per default. Before configuring the communication devices, those 2 default devices must be deleted.

XChange Base does not have any devices preset. Therefore this step can be ignored for XChange Base installations.



IMPORTANT

Both default devices must always be deleted, independent of whether an autonomous FleetBroadband is used on board.

The detailed procedure is:

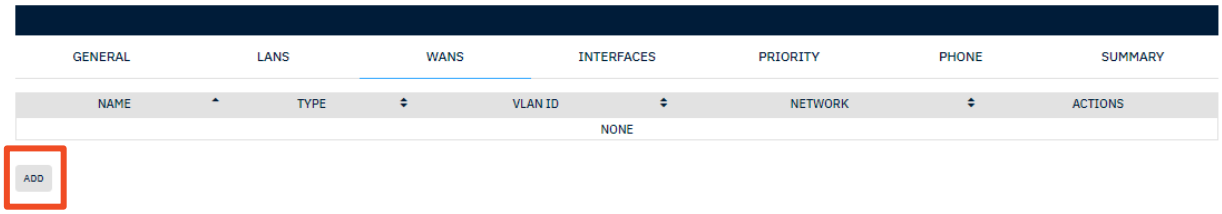
- Click on the ‘Trash’ icon of the 1st device
- Click on DELETE (light grey button)

- Click on YES
- Repeat the same for the 2nd device

5.4.2 New Device Setup

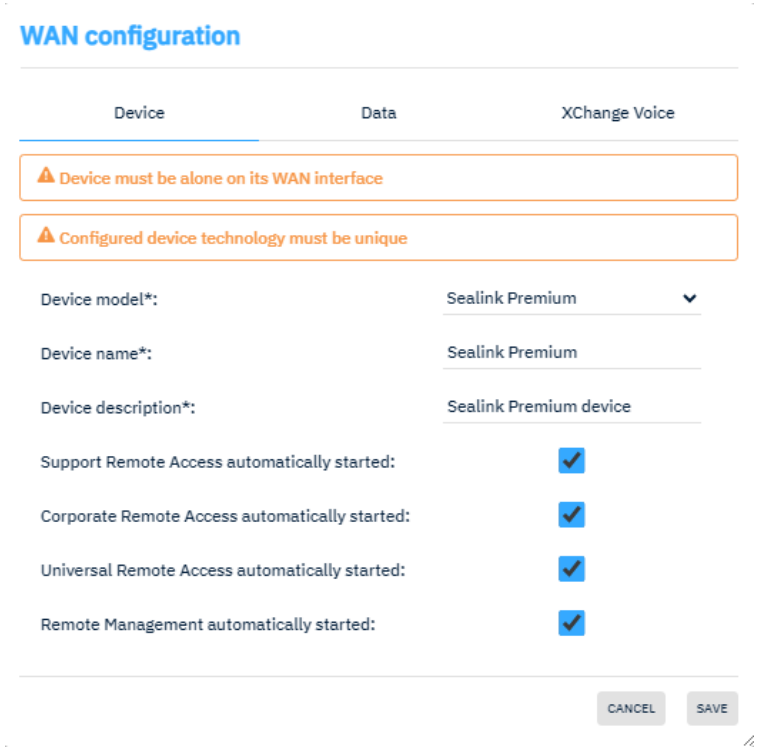
The steps described in this chapter need to be redone for each communication device separately.

To create a new communication device, click the 'Add' button to start.



IMPORTANT
Remember, VSAT must be configured on the WAN2 device

A new window appears guiding through the device-specific configuration steps.



5.4.3 Adding Marlink VSAT

To add a Marlink VSAT select 'Sealink Premium' and follow the steps below.

- Change the device name and description to the Sealink type, like "Sealink Allowance", "Sealink Business" or "Sealink Premium".
- 'Support Remote Access' is preselected [Mandatory for Marlink VSAT]
- Select 'Corporate Remote Access' if required
- Select 'Universal Remote Access automatically started' [Mandatory for Marlink VSAT]
- Select 'Remote Management automatically started' [Mandatory for Marlink VSAT]

IMPORTANT

The installation process does NOT differ for iDirect X7 or Newtec modems!

After reboot, the XChange from version 5.2 will automatically recognise the connected modem type. **Do not use "Sealink Allowance" driver**

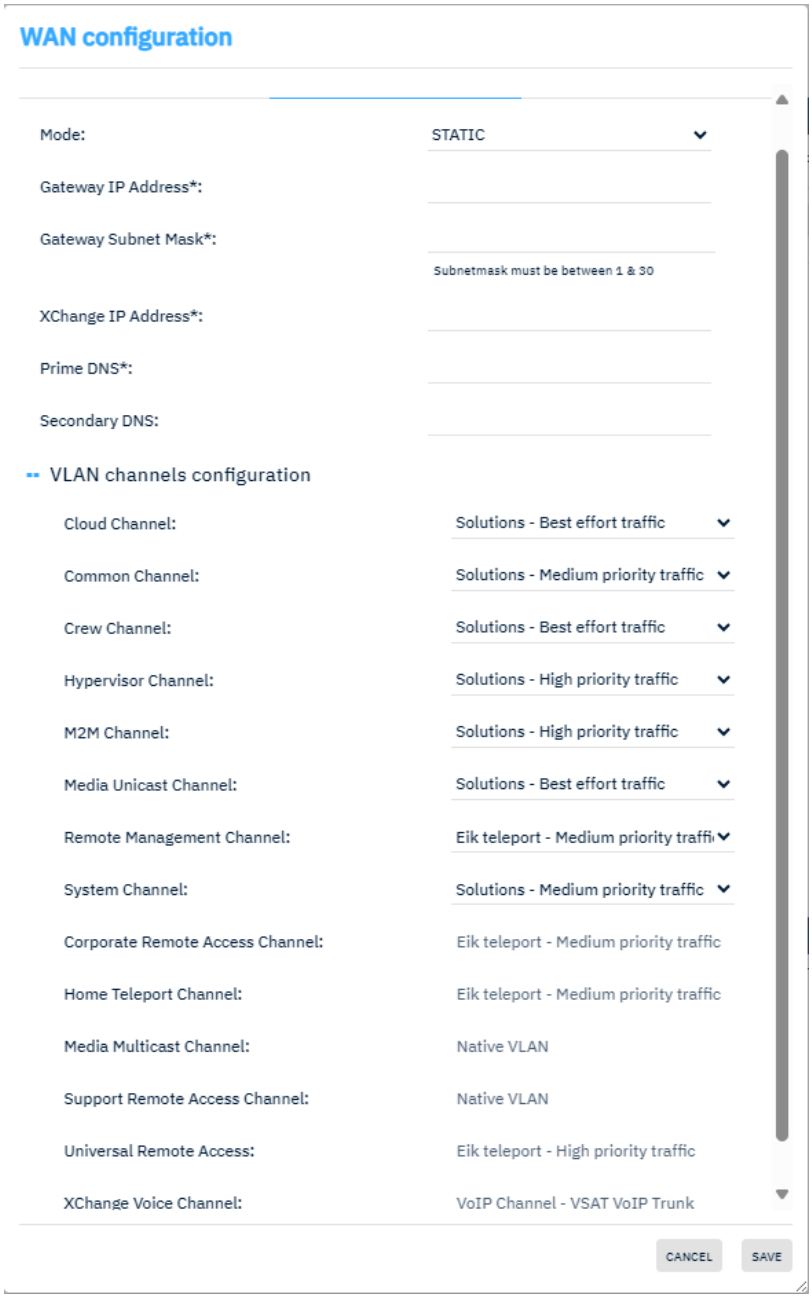
☝ Please enable "Universal Remote Access-" and "Remote Management automatically started" for all VSAT devices.

When all these required details have been correctly set, click on 'Data' to continue.

5.4.3.1 Data Configuration

In this step the data connectivity details need to be setup:

- Set the WAN configuration according to the Network drawing provided by Marlink.
  - Set the Mode to STATIC
  - Gateway address/subnet: IP address and subnet of the Modem
  - XChange IP address: IP address of the XChange Box, usually modem IP +3.
  - Primary DNS, Secondary DNS



Scroll down to see the VLAN channel configuration:

- VLAN Channel configuration
  - Change the default VLAN configuration of the XChange only if requested in IOF
  - To change the default VLAN configuration, select from the drop-down menu the desired VLAN ID for the Common-, M2M- and Crew Channel according to the IP Map
  - The default VLAN per communication channel are:
    - Common Channel → VID 465 Solutions – Medium priority traffic
    - Crew Channel → VID 466 Solutions – Best effort traffic
    - M2M Channel → VID 463 Solutions – High Priority traffic

IMPORTANT

It is not possible to edit the IP configuration of the VLAN interface from the Installation Wizard assuming that it is automatically retrieved via DHCP. Nevertheless, it is possible to enforce the IP configuration afterwards through the management interface.

IMPORTANT

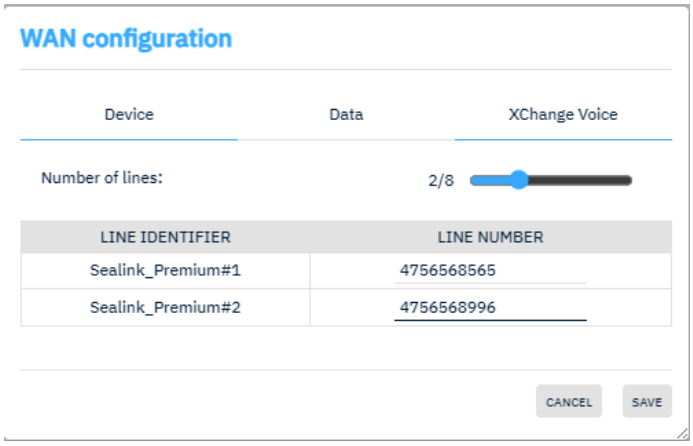
Do not change the VLAN association for Remote Management.

When all these required details have been correctly set, click on 'XChange Voice' to continue.

5.4.3.2 Voice Line Configuration

Set the number of available VSAT voice lines according to the VSAT documentation.

Set the relative phone number for each voice line without any prefix like '00' or '+'.



IMPORTANT

Each voice line must be provisioned with a unique phone number. It is not possible to keep a voice line without a phone number.

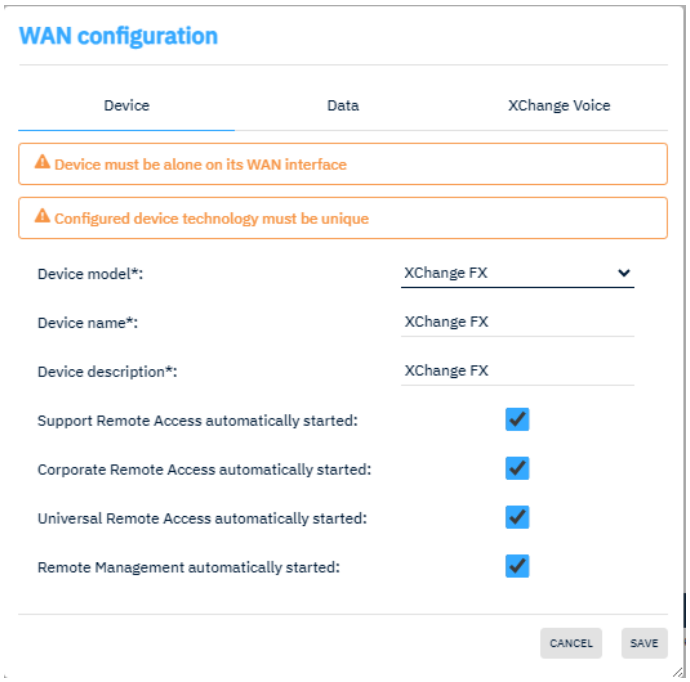
If the phone numbers are not properly set, incoming calls will not work

5.4.4 Adding Marlink XChange FX as a controlled Device

Please follow the separate XChange FX installation guide for detailed information about XChange FX installations. Herewith only the Xchange-specific steps are described.

5.4.4.1 Device Details

To add an XChange FX device select “XChange FX” and follow the steps below.



- Change the device name and description if you wish.
- ‘Support Remote Access’ is preselected [Mandatory for XChange FX]
- Select ‘Corporate Remote Access’ if required
- Select ‘Universal Remote Access automatically started’
- Select ‘Remote Management automatically started’

Please Note
Please enable “Universal Remote Access-” and “Remote Management automatically started” for all XFX devices.

When all these required details have been correctly set, click on ‘Data’ to continue.

5.4.4.2 Data Configuration

In this step the data connectivity details need to be setup:

- Set the WAN configuration according to the Network drawing provided by Marlink. Only change the default parameter when you are requested to. Otherwise do not change the IP addressing
  - Gateway IP address: IP address of XChange FX
  - Gateway Subnet mask: Subnet of XChange FX
  - XChange IP address: IP address of the XChange Box.
  - Primary & Secondary DNS

- VLAN Channel configuration
  - Change the default VLAN configuration of the XChange only if requested
  - To change the default VLAN configuration, choose the desired VLAN ID for the common, M2M and Crew Channel according to the IP Map from the drop-down menu.
  - The default VLAN per communication channel are:
    - Common Channel → High Priority traffic (2330/3)
    - Crew Channel → Medium Priority traffic (2331/2)
    - M2M Channel → High Priority traffic (2330/3)
    - Marlink Voice Channel → Marlink Voice (2332/1)

IMPORTANT

It is not possible to edit the IP configuration of the VLAN interface from the Installation Wizard assuming that it is automatically retrieved via DHCP. Nevertheless, it is possible to enforce the IP configuration afterwards through the management interface.

IMPORTANT

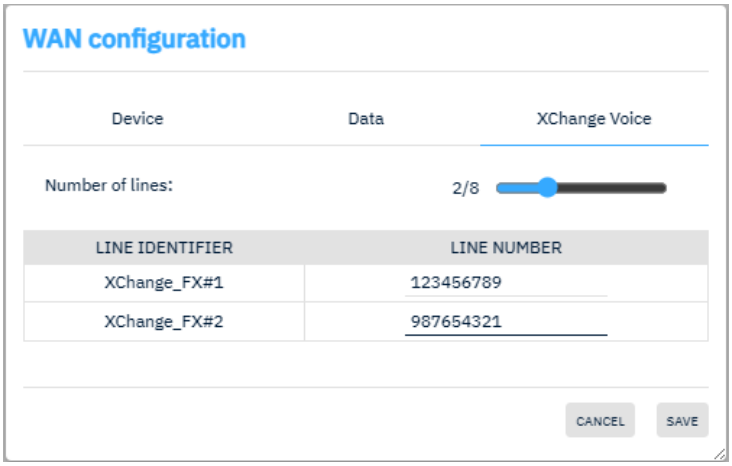
Do not change the VLAN association for Voice, URA and Remote Management.

When all these required details have been correctly set, click on 'XChange Voice' to continue.

5.4.4.3 Voice Line Configuration

Set the number of available FX voice lines according to the documentation.

Set the relative phone number for each voice line without any prefix like '00' or '+'.



IMPORTANT

Each voice line must be provisioned with a unique phone number. It is not possible to keep a voice line without a phone number.

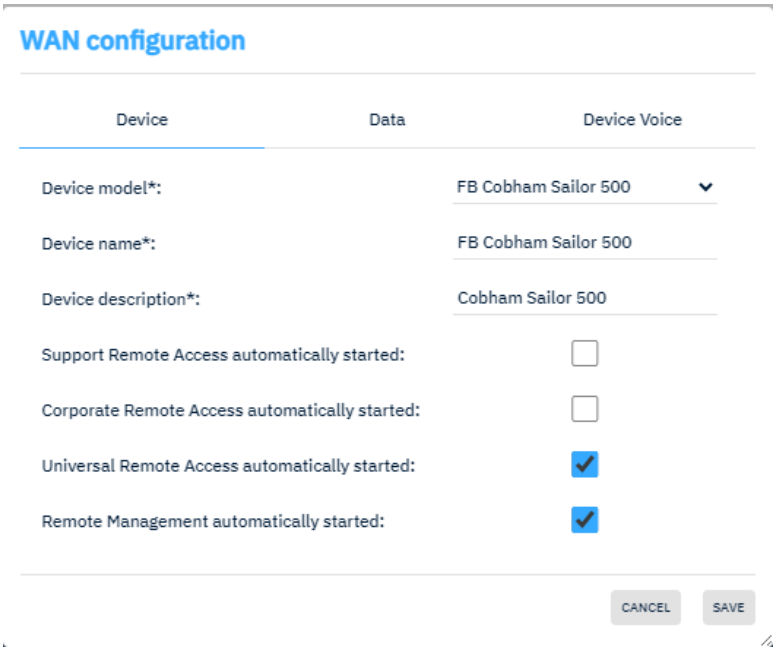
If the phone numbers are not properly set, incoming calls will not work

5.4.5 Adding Marlink MSS Terminals as Controlled Device

Only valid for supported Fleet Broadband and Iridium terminals with Marlink airtime.

5.4.5.1 Device Details

To add a Marlink MSS select the related Fleet Broadband (or Iridium) device model and follow the below steps.



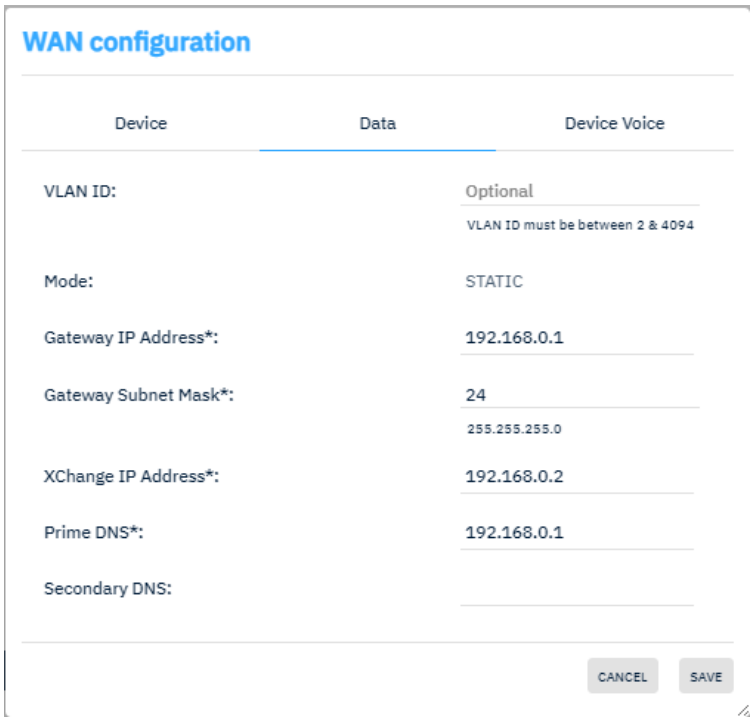
- Change the device name and description if you wish.
- Select 'Support Remote Access' to enable remote access for Marlink support teams
- Select 'Corporate Remote Access' if wished
- Select 'Universal Remote Access'
- Select 'Remote Management'

When all these required details have been correctly set, click on 'Data' to continue.

5.4.5.2 Data Configuration

In this step the data connectivity details need to be setup:

Select the WAN interface the Marlink MSS terminal is connected to:



For a Fleet Broadband terminal connected to the XChange Box, change the IP parameters only if necessary like for instance, the Fleet Broadband terminal has set a non-default IP address range.

It is recommended that for most usage scenarios you keep the predefined IP parameters.

For multiple Fleet Broadband setups, it is mandatory to change the IP address range of the second terminal and, the XChange Box IP parameters accordingly to avoid IP address conflicts between the two terminals.

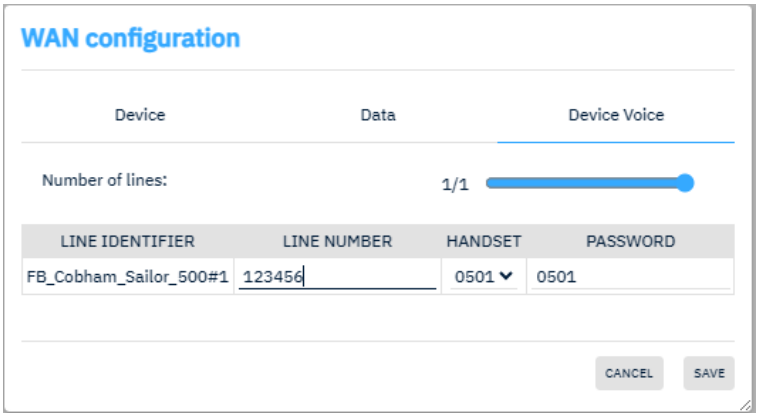
For an Iridium Open Port (or Pilot) connected to the XChange Box, set the IP parameters according to the IP details used on the Iridium terminal.

Please Note
Only IT specialists familiar with IP addressing should change the predefined IP parameters where necessary.
Please Note
Set a VLAN-ID only when mentioned in the installation documentation

When all these required details have been correctly set, click on ‘Device Voice’ to continue.

5.4.5.3 Device Voice Line Configuration

Set the number of available analogue voice lines accordingly.



IMPORTANT

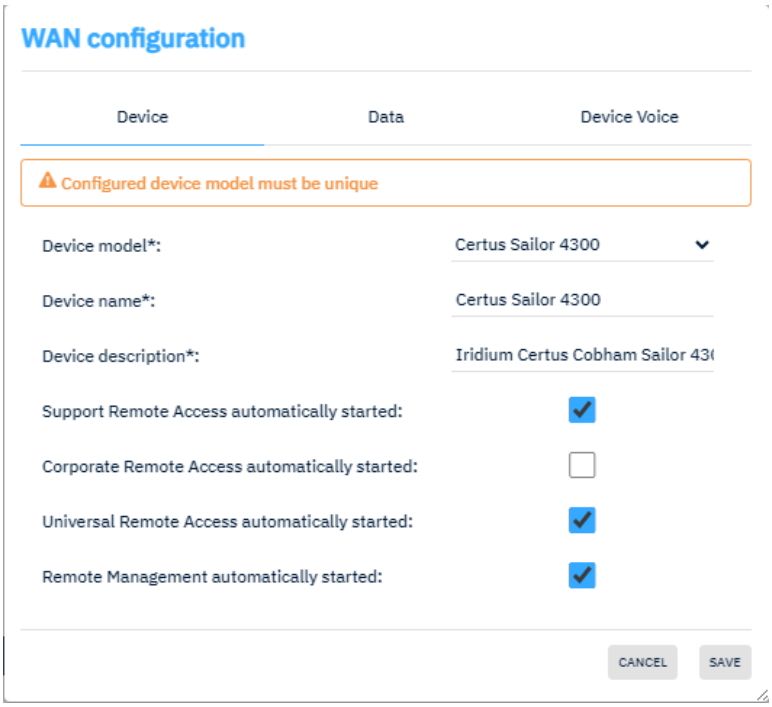
No analogue connection to MSS devices are supported. In that case, please select 1 'SIP' Account which is preconfigured in the Sailor devices. If a MSS device does not support VoIP, skip that step.

Set the relative phone number for the voice line without any prefixes like '00' or '+'.

When all these required details have been correctly set, click on 'Save'.

5.4.6 Adding Iridium Certus Devices

To add an Iridium Certus device, select the related device model and follow the below steps. Select either "Certus Sailor 4300", "Certus Thales VesseLINK" or "Certus Intellian C700".



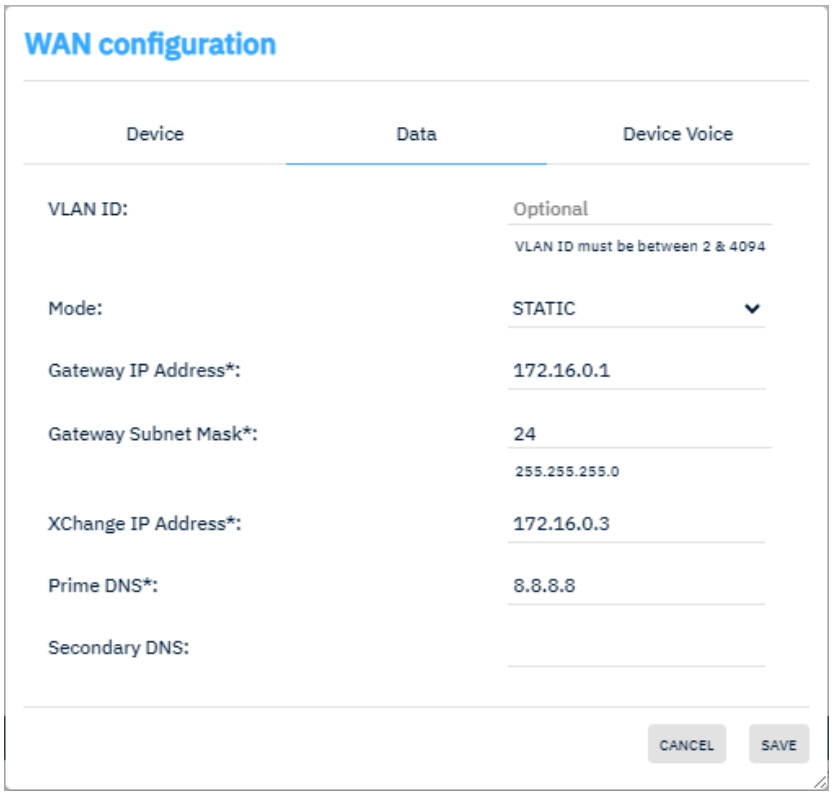
- Change the device name and description if you wish.
- Select 'Support Remote Access' to enable remote access for Marlink support teams

- Select ‘Corporate Remote Access’ if wished
- Select ‘Universal Remote Access’
- Select ‘Remote Management’

When all these required details have been correctly set, click on ‘Data’ to continue.

5.4.6.1 Data Configuration

In this step the data connectivity details need to be setup:



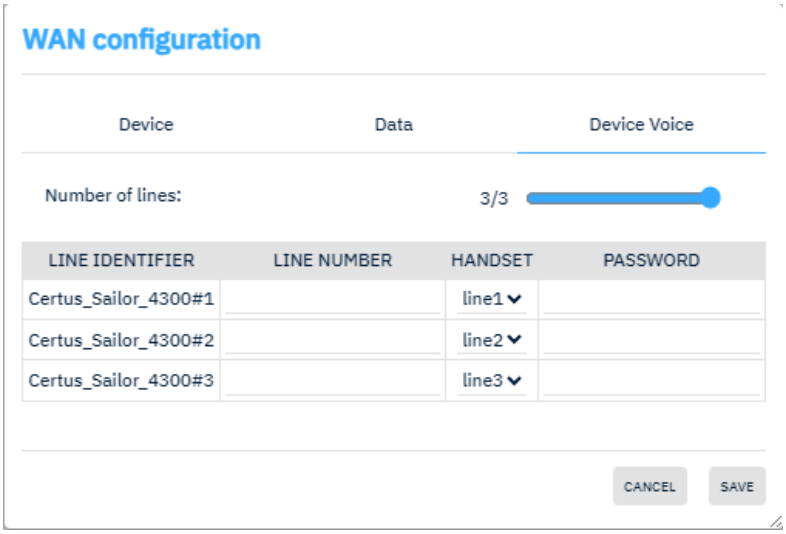
For any Certus device, the default IP addresses are preconfigured. Change the IP parameters only if necessary. It is recommended that for most usage scenarios you keep the predefined IP parameters.

Please Note
Set a VLAN-ID only when mentioned in the installation documentation

When all these required details have been correctly set, click on ‘Device Voice’ to continue.

5.4.6.2 Voice Line Configuration Certus Sailor

Set the number of available voice lines accordingly.



Set the relative phone number for the voice line without any prefixes like '00' or '+'.

Select the handset-line, of the assigned voice number and set the corresponding password.

When all these required details have been correctly set, click on 'Next' to continue.

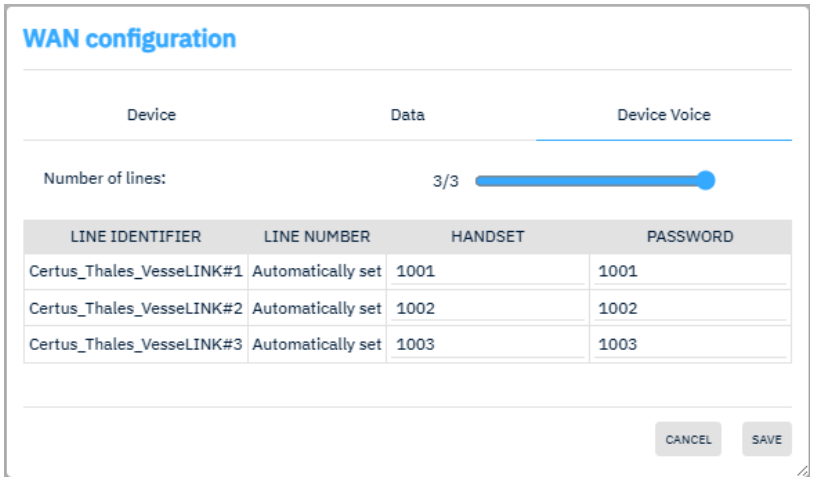
IMPORTANT Bug

When not all voice lines of a Certus device should be created in XChange, the XChange prevents you from finalising. When e.g. Line 1 should not be in XChange, but Line 2 & 3 the system considers this as a double-assigned line.

To avoid this temporary bug, set the lines in XChange starting from 1 instead.

5.4.6.3 Voice Line Configuration Thales VesseLINK & Certus Intellian C700

Set the number of available voice lines accordingly.



Please Note

Installations with a VesseLINK or Intellian C700 device do not allow setting the voice-line numbers in the XChange interface. The according voice numbers are retrieved from the device automatically.

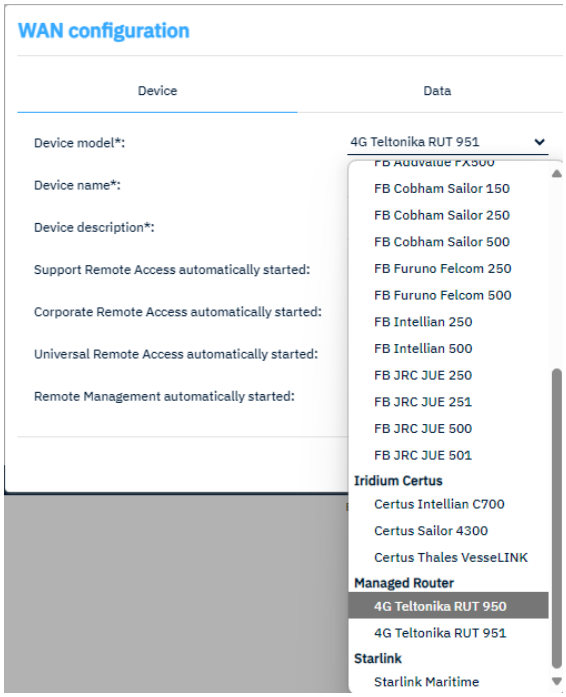
If other than the default handset lines should be managed by XChange, change the handset number and password accordingly.

When all these required details have been correctly set, click on ‘Save’.

5.4.7 Adding Marlink 4G

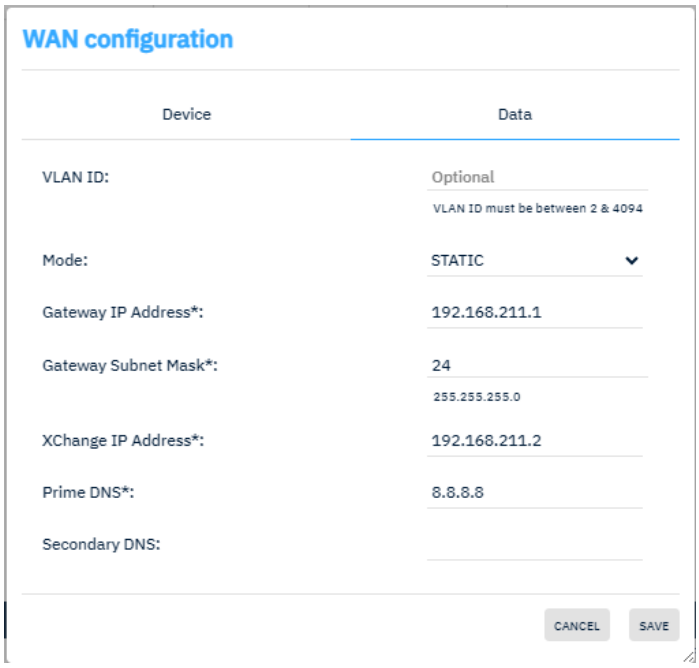
Follow the steps below:

- Select the '4G Teltonika RUT 950 or 951' device driver depending on the hardware on board



- Change the device name and description if you wish
- Select 'Support Remote Access' to enable remote access for Marlink support teams
- Select 'Corporate Remote Access' if wished
- Select 'Universal Remote Access'
- Select 'Remote Management'

When all these required details have been correctly set, click on 'Data' to continue.



For any Marlink 4G device, the default IP addresses are preconfigured. Change the IP parameters only if necessary. It is recommended that for most usage scenarios you keep the predefined IP parameters.

Please Note
Set a VLAN-ID only when mentioned in the installation documentation

When all these required details have been correctly set, click on ‘Save’ to continue.

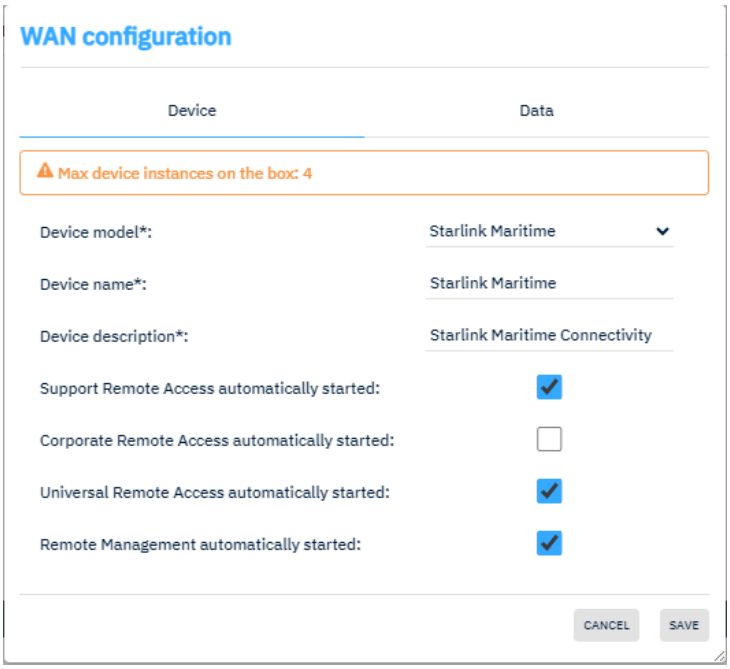
5.4.8 Adding Starlink

As per installation documentation, the Starlink terminal must be connected to either network port 7 or 8 directly on the XChange Power, or WAN1 on the XChange Base.

5.4.8.1 Starlink by Marlink

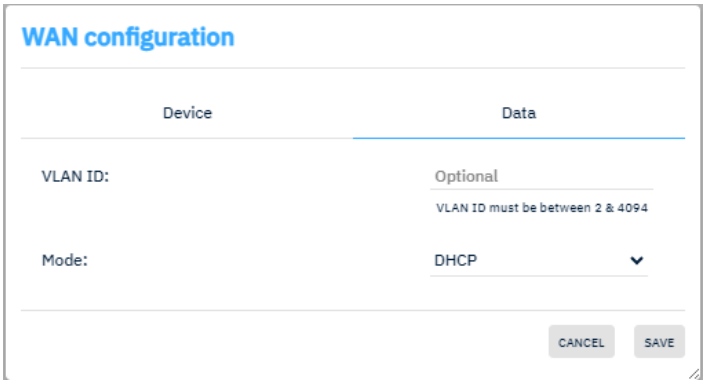
Follow the steps below:

- Select the 'Starlink Maritime' device driver



- Change the device name and description if you wish
- Select 'Support Remote Access' to enable remote access for Marlink support teams
- Select 'Corporate Remote Access' if wished
- Select 'Universal Remote Access'
- Select 'Remote Management'

When all these required details have been correctly set, click on 'Data' to continue.



For any Starlink device, the default IP addressing mode should be kept on DHCP. Change the IP parameters only if necessary.

Please Note
Set a VLAN-ID only when mentioned in the installation documentation

When all these requisite details have been correctly set, click on 'Save'.

☝During the installation wizard, if the Starlink is provided by Marlink and/or activated through Marlink the device driver "Starlink" must be selected.

5.4.8.2 Starlink not by Marlink

During installation wizard, if the Starlink is not provided by Marlink and not activated through Marlink an "Autonomous Device" driver must be selected. Do not use the Starlink driver in such cases.

Follow the steps below:

- Select each autonomous broadband terminal
- Change the device name and description to "Starlink" not "Marlink".
- Select the WAN port and set the IP addressing details
  - The WAN IP addressing mode can only be 'DHCP'
- Set the price for Data ($/MB)

When all these requisite details have been correctly set, click on 'Save' and click on 'Device Priority'.

5.4.9 Adding Autonomous Devices

If more than one terminal is connected to an XChange WAN port, connect all terminals to a WAN port of the XChange Box, using an Ethernet switch (DHCP disabled).

☝Please set any non-Marlink communication device similar.

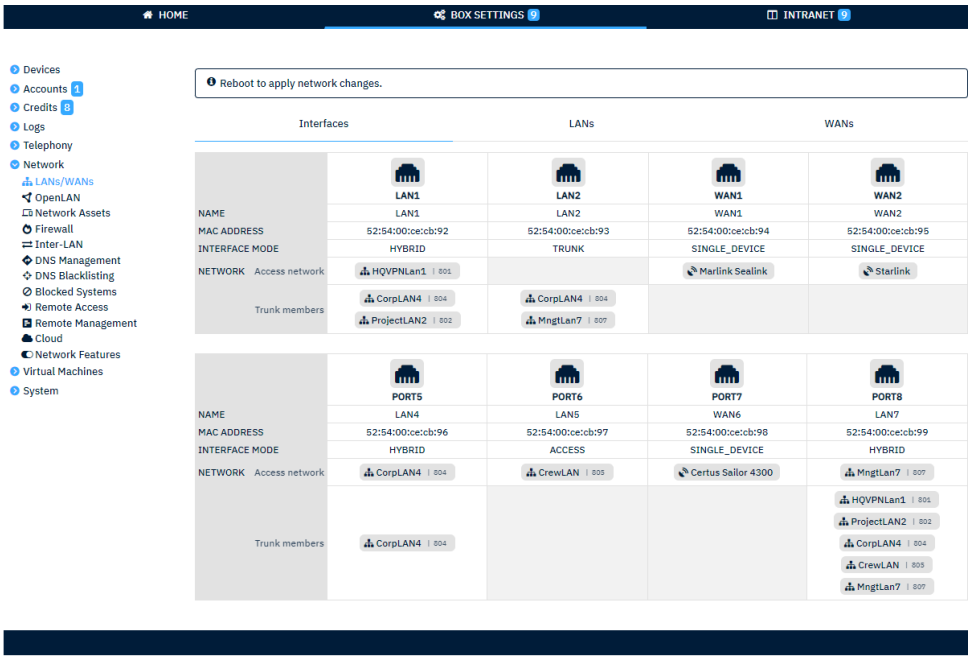
Follow the steps below:

- Select each autonomous broadband terminal
- Change the device name and description if you wish
  - Enable Remote management, URA and Support Remote Remote Access
- Set in 'Data' the IP addressing details
  - The WAN IP addressing mode can only be 'Static'
  - Set the IP address of the XChange Box for each terminal
  - Set the gateway IP addresses
  - Set primary and secondary DNS server addresses
- Each terminal must be in a separate IP address range.

When all these requisite details have been correctly set, click on 'Save'.

5.5 Assigning WAN devices and Networks to Interfaces

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



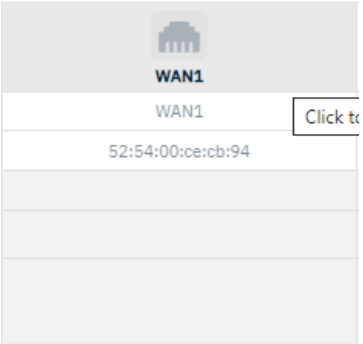
The 'Interfaces menu provides an easy overview of interfaces, assigned networks or WAN devices per interface. While interfaces can be defined and changed at any time for local networks, all interfaces connected to WAN devices can only be changed in the Installation Wizard.

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

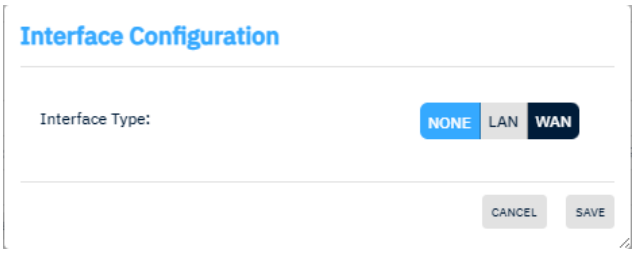
- The name of the physical port as printed on the hardware
- The MAC address of each physical port
- The networking interface mode
- Assigned access network (if any) or WAN device (if any)
- Assigned trunk members (if any) or WAN devices (if any

5.5.1 Interface Configuration for WAN devices

Any previously created WAN device can be assigned to any interface as per installation documentation. To assign WAN devices to an interface, click on the interface:



Unused interfaces are disabled by default. Select 'WAN' to enable the interface



Follow the installation instructions for each WAN port separately.

5.5.1.1 Interface modes

XChange supports for WAN devices 3 interface modes:

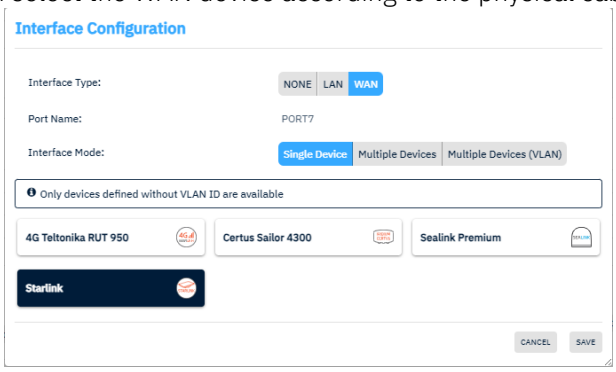
<u>Single Device:</u>
Select “Single Device” if a WAN device shall be connected directly to the selected XChange port (e.g. Port 7 or 8 for Starlink), or if Sealink, XChange FX or SDWAN are connected (WAN2).

<u>Multiple Devices:</u>
Select “Multiple Devices” for ports being connected to the VSAT Switch and multiple devices such as MSS, 4G, Autonomous devices with static IP addressing are connected to the switch.

<u>Multiple Devices (VLAN)</u>
Only select that mode if stated in the installation instructions. The ‘Multiple Devices VLAN’ mode is only applicable if previously WAN devices were created with a VLAN-ID and the WAN Switch is setup accordingly to support multiple VLANs.

5.5.1.2 Assigning WAN devices to interfaces

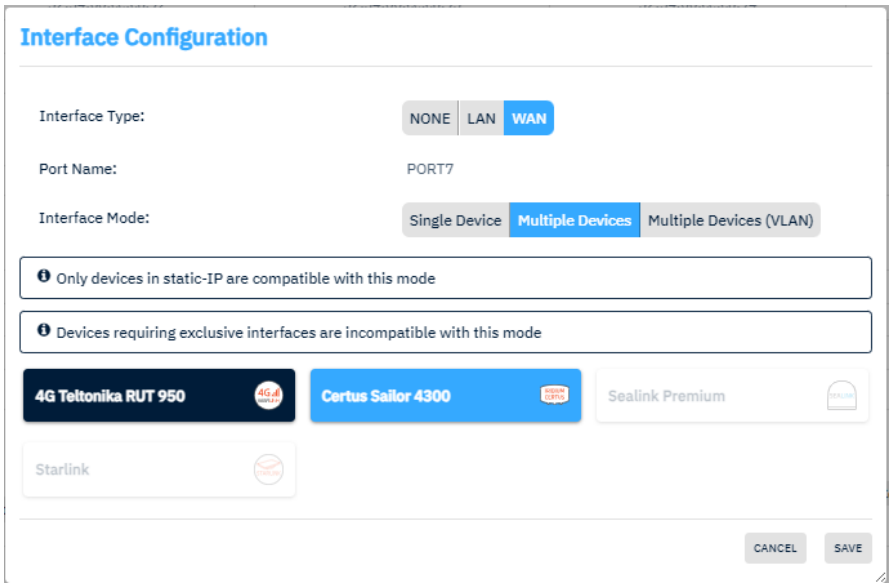
<u>Single Device:</u>
Select ‘Single Device’ and select the WAN device according to the physical cabling:



☝Use this mode for Sealink or XFX installation on port WAN2 or Starlink on ports WAN7 or WAN8.

<u>Multiple Devices:</u>

Select ‘Multiple Devices’ and select the WAN devices being set in static IP addressing and according to the physical cabling:



☝Only WAN devices with static IP addressing are selectable.

☝Just select each WAN device by clicking which is connected using the VSAT switch to that port.

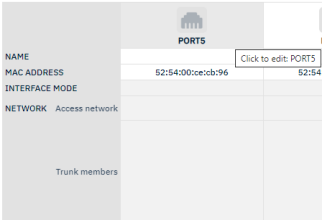
<u>Multiple Devices (VLAN):</u>

Select 'Multiple Devices (VLAN)' and select the WAN devices being set with a VLAN-ID and according to the physical cabling only if described in the installation instructions.

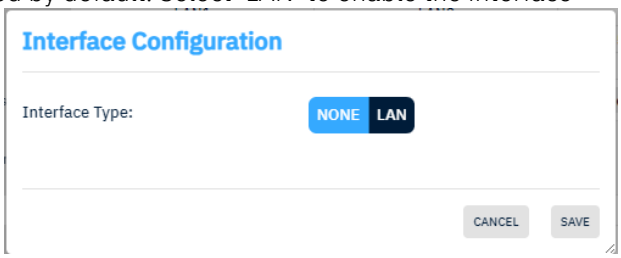
☝Only WAN devices with VLAN-IDs are selectable.

5.5.2 Interface Configuration for LANs

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:



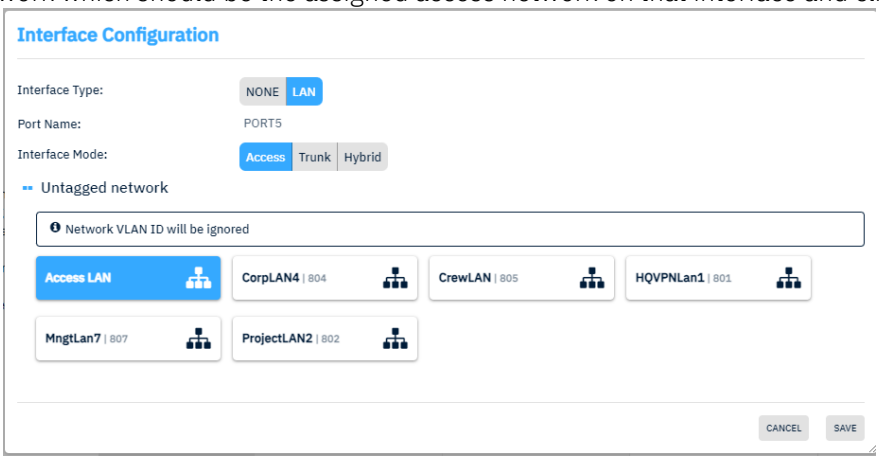
Unused interfaces are disabled by default. Select 'LAN' to enable the interface



5.5.2.1 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'.



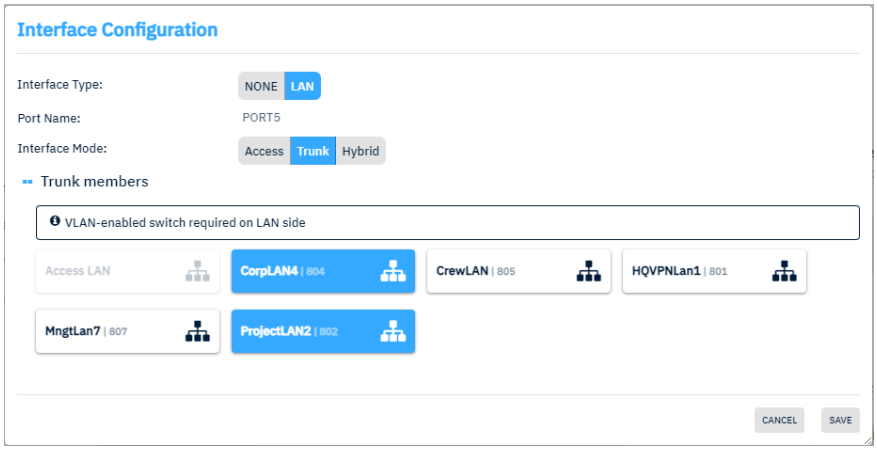
☝ Only 1 network can be assigned as access network to an interface.

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

5.5.2.2 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'.



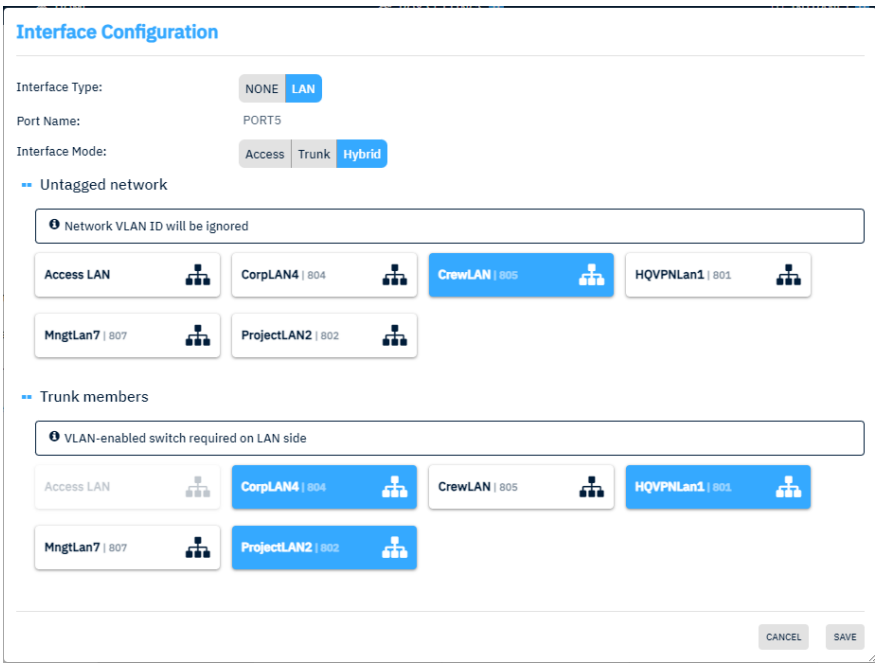
☝ Only networks with valid VLAN-IDs can be assigned as trunk members to an interface. Networks without a VLAN-ID (Access) cannot be selected.

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

5.5.2.3 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.



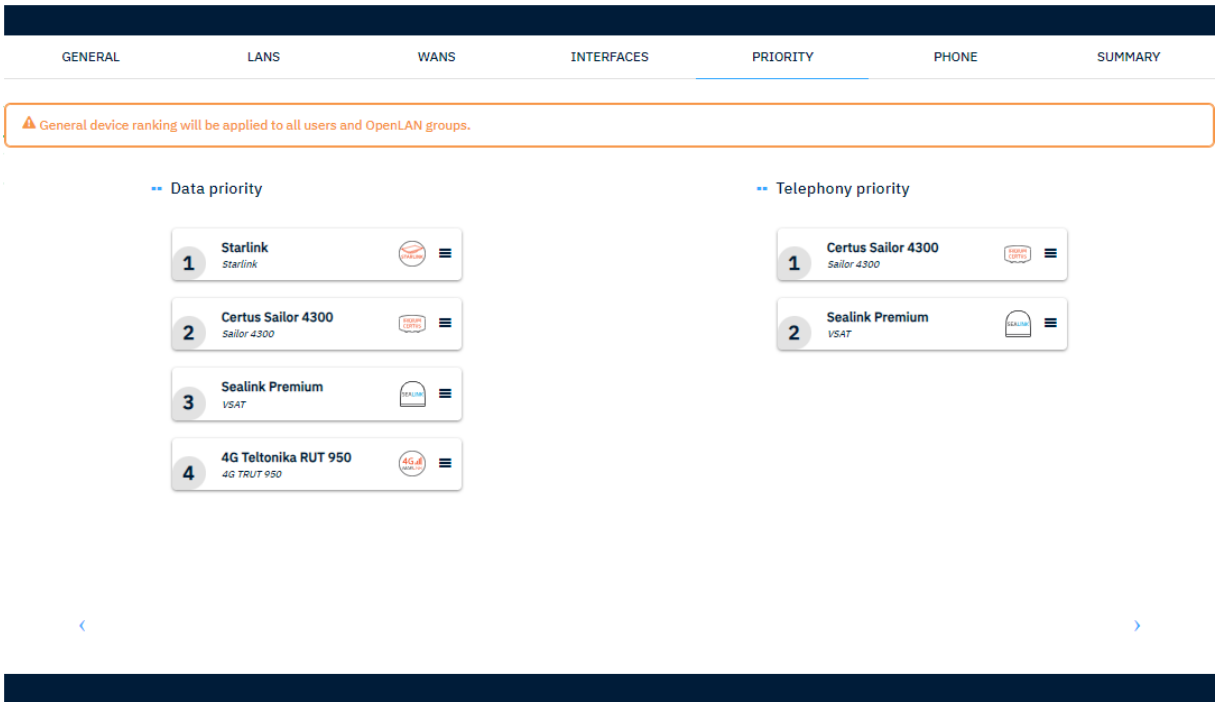
☝ Any network, with or without VLAN-ID can be assigned as access network. Trunk member must have a valid VLAN-ID.

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

Once all WAN devices and all networks are assigned to interfaces, go to the Device Priority.

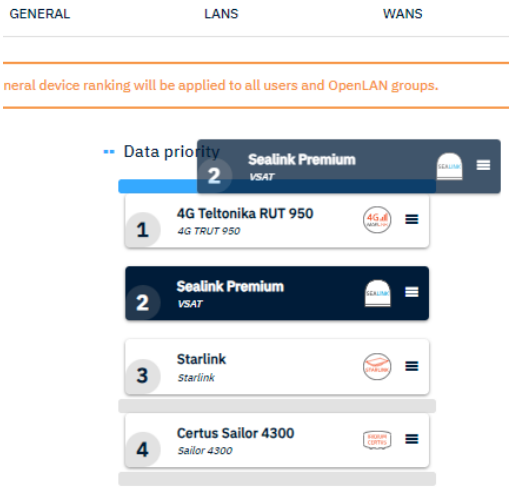
5.6 Device priority

The system allows the prioritization of the terminals for data and telephony service.



To change the Rank of a device, click on the 'Burger-icon' behind the device icon and drop the dragged device at the right position.

You need to 'hit' the priority line correctly. Only when the separator line turns blue, the device will be put to the right position.



☝ The ranking affects the system behaviour for all voice services used with XChange as well as data communication for XChange with the "SDWAN-Lite" applied switching option.

IMPORTANT

Follow precisely the instructions given for any installation especially when Starlink is involved. Only if you don't have any instructions, define the ranking as follows:

1. 4G/5G (if available)
2. Sealink
3. Starlink
4. MSS backup

Prioritize user groups to rank 'Sealink' above 'Starlink' for corporate users.

Prioritize user groups to rank 'Starlink' for crew users.

5.7 Phone Configuration

In the phone configuration step, the available outgoing and incoming voice lines per phone will be assigned. Furthermore, you can configure to hide the last four digits of the destination numbers in the call log.

DETAILS	TYPE	OUTGOING LINES	INCOMING LINES	EDIT
bridge [sipphone1] (2001) OPEN_ACCESS	DIGITAL	Certus_Sailor4300_eth6_#1 Sealink_Premium#1 Sealink_Premium#2	Certus_Sailor4300_eth6_#1	
Personal SIP Phone OPEN_ACCESS	DIGITAL	Certus_Sailor4300_eth6_#2 Sealink_Premium#1 Sealink_Premium#2	no incoming lines	
sipphone#2 [sipphone2] (2002) PIN_RESTRICTED	DIGITAL	Certus_Sailor4300_eth6_#1 Certus_Sailor4300_eth6_#2 Sealink_Premium#1 Sealink_Premium#2	Certus_Sailor4300_eth6_#1 Certus_Sailor4300_eth6_#2	
sipphone#3 [sipphone3] (2003) PIN_RESTRICTED	DIGITAL	Certus_Sailor4300_eth6_#2 Sealink_Premium#1 Sealink_Premium#2	Certus_Sailor4300_eth6_#2	

The XChange selects automatically an outgoing line based on the settings following a set prioritization and availability of assigned voice lines.

Below listed phone devices are preconfigured in the XChange Box:

- Personal SIP phone (1x) [Used on all private smartphones using the 'XChange Voice' App]
- SIP Phone (3x) [Used for IP phones]
- Analog Phone 3x for 4-port voice card on XChange Power only

☝The described assignment can be redone for any phone.

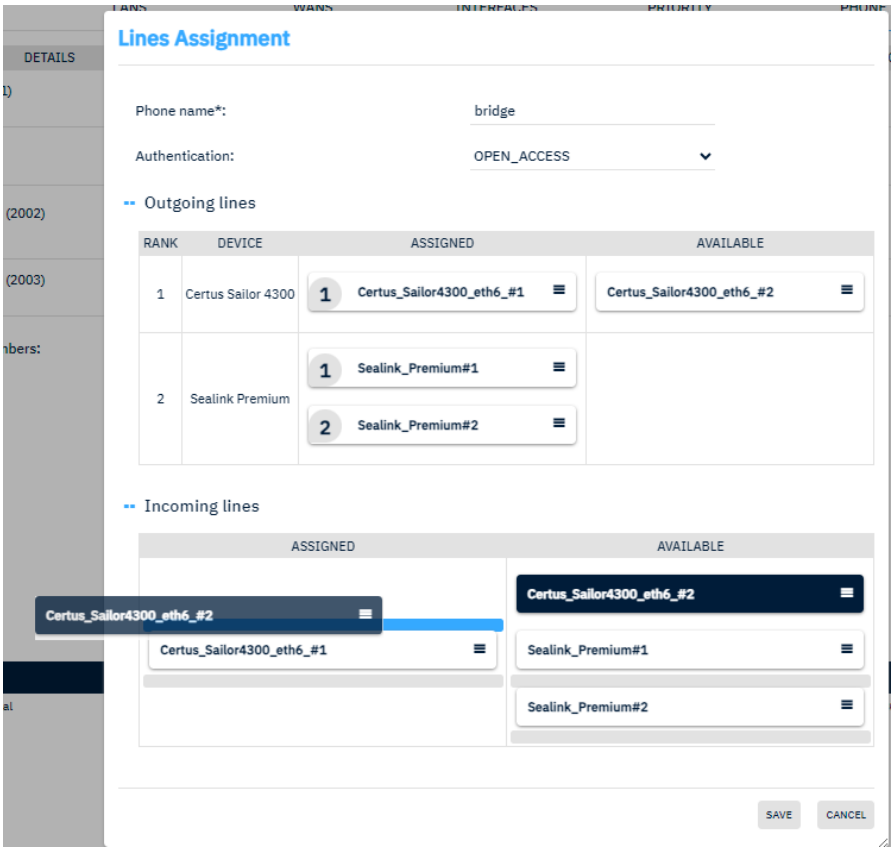
5.7.1 Hide Destination Numbers

To hide the last four digits of the called destination numbers in the call log, set the respective control to ON.

5.7.2 Line Assignment

To set the voice line assignment for a phone, click the 'Edit' icon of the desired phone in the table.

- Change the phone name if wished
- 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 prioritization for outgoing calls
- Set the incoming phone lines



☝Assigned phone lines appear on the left side, not assigned phone lines on the right. To change the assignment of a phone line, select the desired phone line and use ‘drag and drop’ to shift from the right to the left (and vice versa).

☝The phone configuration can be changed later on by the administrator.

When all these requisite details have been correctly set, click on ‘Save’ and click ‘Summary’ to continue.

5.8 Configuration Summary

Check the configuration summary. Make sure all devices and additional equipment are connected to the XChange Box and that they are all switched on.

Phone devices

DETAILS	TYPE	OUTGOING LINES	INCOMING LINES
bridge [sipphone1] (2001) OPEN_ACCESS	DIGITAL	Certus_Sailor4300_eth6_#1 Sealink_Premium#1 Sealink_Premium#2	Certus_Sailor4300_eth6_#1
Personal SIP Phone OPEN_ACCESS	DIGITAL	Certus_Sailor4300_eth6_#2 Sealink_Premium#1 Sealink_Premium#2	no incoming lines
sipphone#2 [sipphone2] (2002) PIN_RESTRICTED	DIGITAL	Certus_Sailor4300_eth6_#1 Certus_Sailor4300_eth6_#2 Sealink_Premium#1 Sealink_Premium#2	Certus_Sailor4300_eth6_#1 Certus_Sailor4300_eth6_#2
sipphone#3 [sipphone3] (2003) PIN_RESTRICTED	DIGITAL	Certus_Sailor4300_eth6_#2 Sealink_Premium#1 Sealink_Premium#2	Certus_Sailor4300_eth6_#2

Hide destination numbers: ENABLED

SAVE PRINT

If any setting is incorrect, click on ‘Back’ to return to the specific configuration page and change the settings accordingly.

If the configuration setup is correct, press ‘Save’ to continue with initialising the box.

Please Note

You can use the “Print” function to print out the configuration summary for your documentation.

The XChange Box will restart after the initialization wizard has been completed. After rebooting, you must synchronise the box before the XChange will be ready for use.

5.9 Synchronisation

5.9.1 XChange Base Synchronisation

After successful Initialisation, login as fengineer. On the dashboard in the top-right corner, a "Synchronise Now" button is present.

Ensure that at least one of the installed devices is online and ready to be used. The XChange box will send several pings to the server to verify connection, after a few minutes online devices will turn green.

To go further with the installation, press the "synchronize" button. The system will connect for the first time to the XChange server and exchange some information. The first synchronisation may take several minutes. After successful synchronisation, the box should be usable.

Please Note
If you get a message in the top-right corner, that the system is barred please contact Marlink support desk and request the unbarring. In case the synchronisation fails, check for certificate updates and try again.

5.9.2 XChange Power Synchronisation

After successful Initialisation, login as fengineer and go to:

Box Settings > System > Synchronisation

Ensure that at least one of the installed devices is online and ready to be used.

To go further with the installation, press the "Synchronise" button. The system will connect the first time to the XChange server and exchange some information. The first synchronisation may take several minutes. After successful synchronisation, the box should be usable.

Please Note
On XChange Power, you don´t see a message on the dashboard. Please do not forget to synchronise the XChange.

5.10 Upgrade to latest firmware

If the XChange you installed is not in the latest firmware version, update it to the latest version, preferably perform an online update.

Please review the 'XChange update quick guides' for further instructions on how to upgrade.

Updating to the latest firmware version is mandatory.

6. Exclusive Write Access

IMPORTANT

Forcing the Exclusive Write Access to Ship is only allowed for Marlink Technical Support teams and Field Engineers. Do not share the “fengineer“ credentials with customers.

The Exclusive Write Access (EWA) is a control command administered from Portal360. To avoid misconfiguration and potential issues, it is only allowed to configure and administer the XChange configuration and Users either on “Ship” or on “Shore”. The EWA setting defines if the control is available on board “Ship” or moved to Portal360 “Shore”. If the EWA is set to “Shore” the User administration and/or the system configuration is in Read-Only mode.
The factory default setting is set to “Ship” to ensure that the installation can be performed.

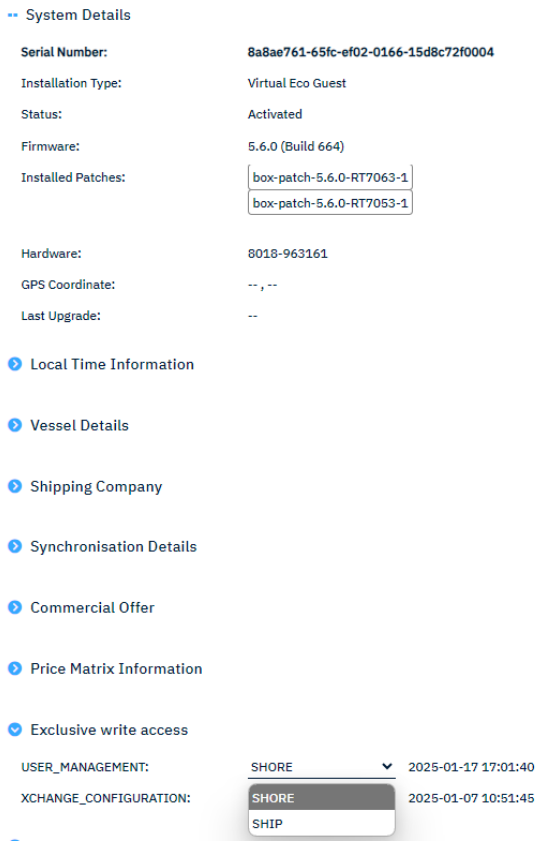
Please note

When importing a Backup file the EWA is may set to “Shore” to prevent any change in the system configuration.

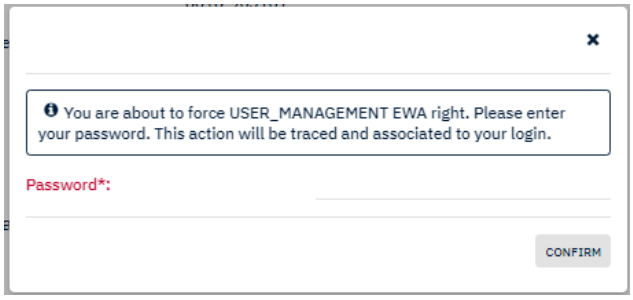
If the EWA setting is on “Shore”, it is possible for the fengineer only to force the EWA setting to “Ship” again without the need to synchronise the system.

6.1 Forcing EWA settings to Ship

Only if the EWA setting is set to “Shore”, the below procedure can be followed. In normal situations, this process can be skipped.
To force the EWA setting back to “Ship”, login as superadmin and go to: Box Settings > System > Overview and expand the panel “Exclusive Write Access”.



To force either the configuration or user management EWA to “Ship” simply click on the button in column “Side”:



Enter the fengineer password in the popup window. The window refreshes and changes the EWA setting to “Ship” again.

IMPORTANT

If you manually force the EWA setting back to “Ship” you must report this to Marlink Service desk.

The manual forcing sets a “Dirty Flag” on the XChange Shore Servers which prevents the move of the EWA setting to “Shore”.

7. Remote Access Setup

7.1 Support Remote Access Setup

To access the XChange Box, a terminal or the local network remotely, the terminal used must be connected to the internet using a public IP address. To enable remote access for Marlink support teams, the Support Remote Access rules must be set.

To be able to access a terminal connected on the WAN side, the support remote access rules must be set correctly according to instructions specified in the IOF or IT Policy document. To change the configurations go to Box Settings->Network -> Remote Access -> Support Remote Access.
Redo the below steps for each equipment. Please use the “Remote Access Defaults” document.

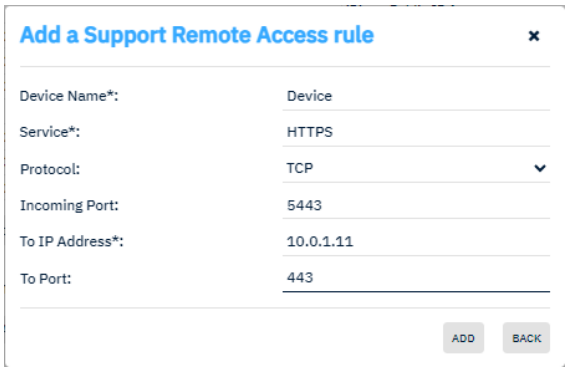
Support Remote Access Rules

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, follow the instructions below:

- 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’

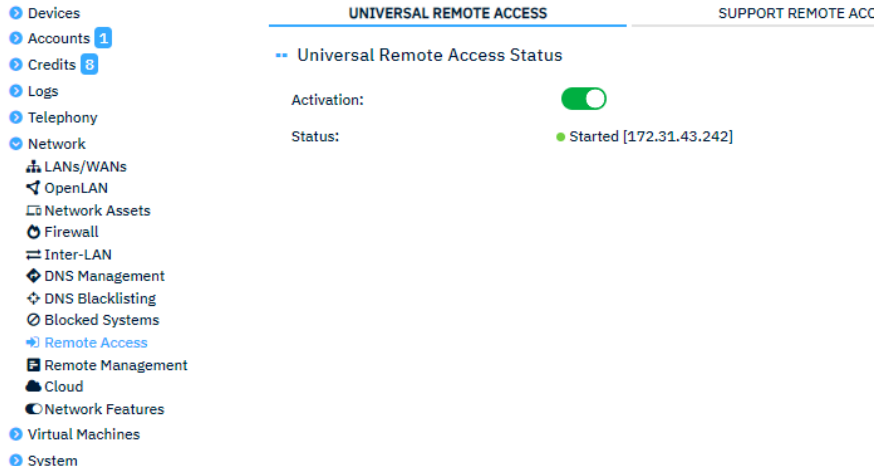


Verify that Support Remote Access and Universal Remote Access have started.

Please check the port forwarding default rules document to setup the correct parameter.

7.2 Universal Remote Access Setup

If the Universal Remote Access is enabled to start automatically (see device settings), then the Universal Remote Access will start automatically once a device is online.
To manually activate the Universal Remote Access, go to Box Settings-> Network->Remote Access and perform the following steps.



- Click the 'Off' button to enable the URA service
- The button will slide to 'On' and the URA service will be enabled.
- To restart the Universal Remote Access, click on the 'Refresh' button
- To stop or restart the Universal Remote Access, either click on 'Stop' or 'Restart' respectively.

8. Machine accounts

On board many vessels, a server or computer must be online all the time. Create a machine account for Machine to Machine devices. i.e. Server or ChartCo PC. If the documentation states to create machine accounts, please follow those steps accordingly.

9. XChange WiFi Installation

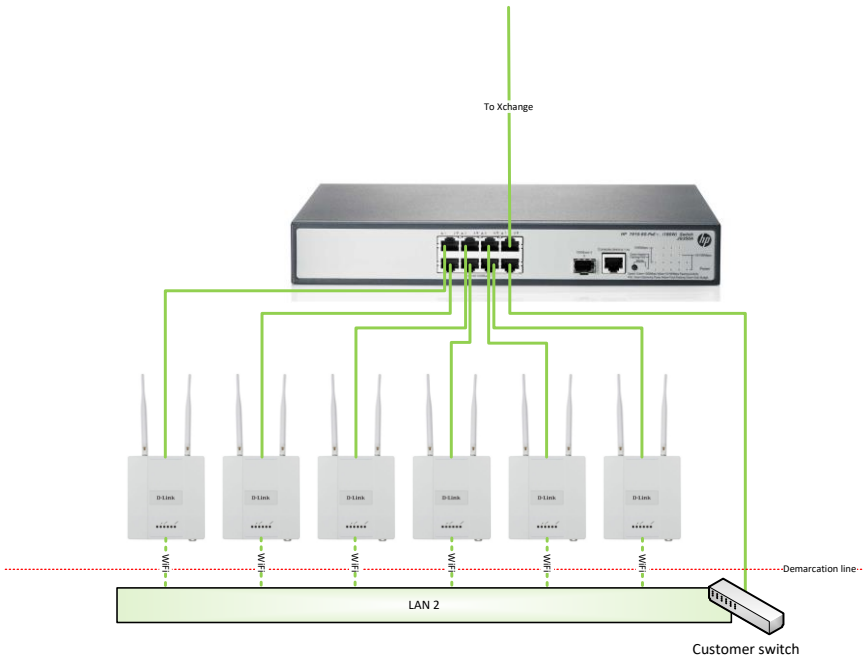
The XChange-WiFi solution adds a wireless component to one of the XChange Box local networks. XChange-WiFi is delivered with a PoE switch and multiple Access Points.

9.1 Cabling

To support PoE recommended cabling is at least CAT5, to a length up to 100M.

The switch can be connected to any local network of the XChange Box.

The following diagram describes the cabling:



To streamline XChange-WiFi installations, please note that all access points must be connected to the switch. A direct connection (e.g. an access point) to an XChange LAN port has to be avoided.

The table below lists which port are the equipment supposed to be connected on the switch:

Switch Port Number (1-8)	Equipment
Port 1	WiFi Access Point
Port 2	WiFi Access Point
Port 3	WiFi Access Point
Port 4	WiFi Access Point
Port 5	WiFi Access Point
Port 6	WiFi Access Point
Port 7	XChange Box LAN
Port 8	Local Vessel Network Switch

10. Trouble Shooting

Please Note

The instructions given in this chapter only apply, if the described issue appears. Otherwise, those can be skipped.

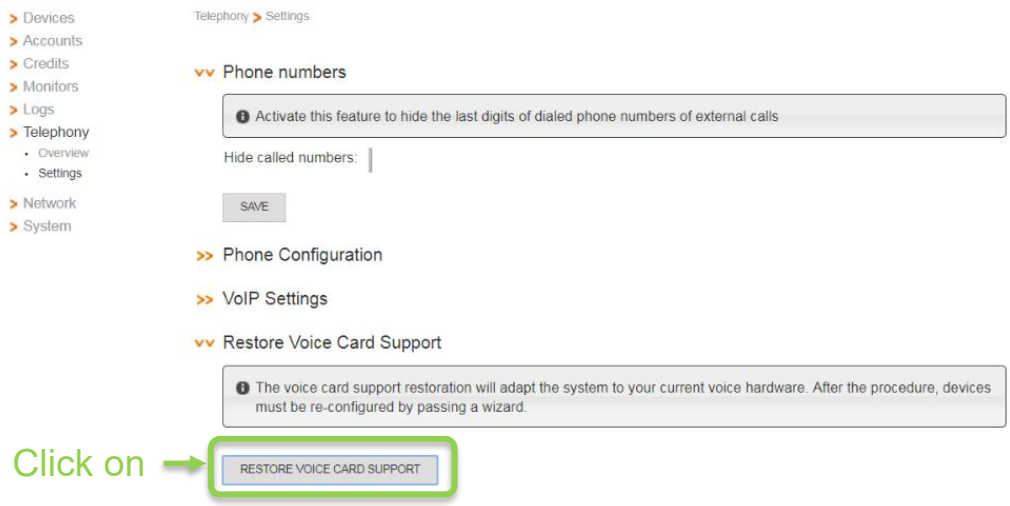
10.1 Missing analogue telephony settings

In case the analogue telephony settings are not shown in the installation wizard, you may follow the below steps:

10.1.1 Voice Card Activation

If an analogue voice card is installed, the Voice configuration on XChange may need to be amended.

Go to Box Settings > Telephony > Settings > **Restore Voice Card Support**



IMPORTANT

This operation must be executed BEFORE running the XChange Wizard.

The XChange will restart and the installation wizard can be performed after the successful restart.

10.2 Factory Reset

If the XChange Box was reset to factory defaults, please follow the instructions above on how to run and configure the XChange System using the installation wizard. After that, the XChange must be registered on the XChange servers on shore. After reboot, a “Register Now” button should be shown on the top-right of the dashboard after login. Please check if the XChange can connect to the internet by pressing that button. After successful registration, the XChange unit must be synchronised with the servers.

IMPORTANT

DO NOT! Factory reset the XChange.

Only after advice from the Marlink CCTS Team, resets are allowed.

11. XChange Finalisation

11.1 Testing

Data connection:

Login as captain using the default captain's account ‘dcaptain’. If not already done, activate the VSAT (or any other primary device) and click the green ‘Connect’ button in the top-right corner of the captain´s dashboard.

After successful online access, try to surf the web or send and receive emails with the vessel's email system.

Voice connection:

To validate if the phones work, use each of them for a short call to Marlink service desk. If you can reach the service desk’s automated voice prompts, the voice line is ready.

11.2 Close Installation

As described earlier, do not forget to click the finalisation button.

11.3 Handover

After the successful installation and test of the XChange and all connected communication devices, make a clear but short handover training to the captain and at least with another officer. Explain the main topics to them like how to switch between devices, how to go online, and how to use the phones. You should also give a copy of relevant user manuals and quick guides to the captain.

Explain in detail how to reboot the system. Explain crystal clear, that a ‘hard shutdown’ (disconnecting the XChange from power or the whole rack) must be avoided at any time. If the reboot option in the user interface cannot be accessed, a short press on the power button is a sufficient workaround.

Provide additional training to the staff on board on how to manage users and credits and explain the types of data communication restrictions imposed by the company’s specific firewall rules.

11.4 Handover Documents

The XChange File Cloud should automatically download the latest XChange Crew Apps for Android and manuals for Captain and Crew. It may take a while before the content is downloaded. Make the staff aware to check the local Intranet for the latest manuals.

11.5 Certificate update

To finalise the installation, go to Box Settings – System – Certificates.

Select each certificate and click on 'Check Updates'. After a new installation, its is may required to try another time in case you see an error message.

Before updating the XChange Firmware to the latest version, the check of certificate updates must be done to ensure a proper installation.

Please Note
If a certificate is outdated, several issues may appear on board. E.g. firmware updates, initial synchronisation can fail, URA not establish connections and more. Up-to-date certificates are mandatory.
IMPORTANT
Therefore it is a mandatory step to check for certificate updates. Before finalising the tests or contacting support. Do NOT factory reset or contact support without having each certificate updated.

12. Installation Checklist

Please document the installation according to Marlink standards. It is important that Marlink support be able to access documentation from the installation for future troubleshooting.

12.1XChange System

No.	Description	OK	N/A	Comments
1	Wizard completed according to documentation	☐	☐	
2	Synchronise the XChange	☐	☐	
3	Check certificate updates	☐	☐	
4	Upgrade firmware to latest revision	☐	☐	Firmware version:
5	Added Support Remote Access rules	☐	☐	
6	Verified that Support Remote Access has started	☐	☐	
7	Verified that Universal Remote Access has started	☐	☐	
8	Configured fixed IP to WiFi switch	☐	☐	IP address:
9	If needed, create machine accounts and test it	☐	☐	
10	Logged in as *dcaptain* and tested data connections	☐	☐	
11	Tested XC Voice App	☐	☐	
12	Tested XC Data Ap	☐	☐	
13	XChange is configured and tested according to documenation	☐	☐	
14	Save backup file	☐	☐	
15	Installation is finalised	☐	☐	

12.2XChange WiFi Access Points

Device information	AP1	AP2	AP3	AP4	AP5
Location					
Sufficient coverage	☐	☐	☐		

13. Annex 1: XChange Box Remote Access Default Rules

13.1 Introduction

To streamline the XChange installations, this document described default remote access rules settings that need to be followed to reduce complexity and ease support procedures. The described defaults are set up in the 'Support Remote Access' section during onboard installation of the XChange Box.

13.2 Default Remote Access Rules for XChange Power

Set all those Port Forwarding rules only when installing an XChange Power.

Device Name	Service	Protocol	From Port	To IP Address	To Port
OVP GUI	HTTPS	TCP	23131	[OVP IP ADDRESS]	3131
OVP Console	SSH	SSH	23122	[OVP IP ADDRESS]	22
OVP remote access portal	HTTP	TCP	6901	[OVP IP ADDRESS]	6901
OVP graphical console	HTTP	TCP	23180/23181	[OVP IP ADDRESS]	80
OVP monitoring SNMP 1	SNMP	UDP	23161	[OVP IP ADDRESS]	161
OVP netconf	NETCONF	TCP	23830	[OVP IP ADDRESS]	830

13.3 Default Remote Access Rules for VSAT

Below listed are the mandatory default remote access rules to be set for VSAT.

Note:

- Only the installed ACU model / Modem model needs to be set up.

13.3.1 iDirect X7 Modem

Device Name	Service	Protocol	From Port	To IP Address	To Port
VSAT iDirect X7 Modem	HTTPS	TCP	10443	[X7 IP ADDRESS]	443
VSAT iDirect X7 Modem	SSH	TCP	10022	[X7 IP ADDRESS]	22
VSAT iDirect X7 Modem	Telnet	TCP	10023	[X7 IP ADDRESS]	23

13.3.2 STI iDirect Dialog MDM 3100 / 2510 / 5010

Device Name	Service	Protocol	From Port	To IP Address	To Port
VSAT Newtec Modem	HTTP	TCP	12080	[MODEM IP ADDRESS]	80

13.4 HPE Aruba 1830 8G

Device Name	Service	Protocol	From Port	To IP Address	To Port
HPE Aruba 1830 8G	HTTP	TCP	10080	[SWITCH IP ADDRESS]	80

13.5 T&T Sailor 900 ACU

Device Name	Service	Protocol	From Port	To IP Address	To Port
VSAT TT Sailor 900 ACU	HTTP	TCP	11080	[ACU IP ADDRESS]	80

13.6 Seatel ACU

Device Name	Service	Protocol	From Port	To IP Address	To Port
VSAT Seatel ACU	HTTP	TCP	11080	[ACU IP ADDRESS]	80

13.7 Intellian ACU

Device Name	Service	Protocol	From Port	To IP Address	To Port
VSAT Intellian ACU	HTTP	TCP	11080	[ACU IP ADDRESS]	80

13.8 Default Remote Access rules for MSS

Below listed are the mandatory default remote access rules to be set for Fleet Broadband.

Notes:

- Only the installed ACU model needs to be set up.
- For old JRC 250/500 FB terminal access the incoming 'From' port must be identical with the 'To' destination port 1829 or 1840.

If a 2nd Fleet Broadband terminal exists on board, the incoming port for it must begin with 3.

13.9 Cobham Sailor 150/250/500 BDU

Device Name	Service	Protocol	From Port	To IP Address	To Port
FB TT Sailor 500	HTTP	TCP	20080	[FB IP ADDRESS]	80

13.10 JRC JUE 250/500 BDU

Device Name	Service	Protocol	From Port	To IP Address	To Port
FB JRC 500	JRC Launcher	TCP	1829	[FB IP ADDRESS]	1829
FB JRC 500	JRC Launcher	TCP	1840	[FB IP ADDRESS]	1840

13.11 JRC JUE 251/501 BDU

Device Name	Service	Protocol	From Port	To IP Address	To Port
FB JRC 501	HTTP	TCP	20080	[FB IP ADDRESS]	80

13.12 Furuno Felcom 250/500 BDU

Device Name	Service	Protocol	From Port	To IP Address	To Port
FB Furuno 500	HTTP	TCP	20080	[FB IP ADDRESS]	80

13.13 Default Remote Access rules for Iridium

Device Name	Service	Protocol	From Port	To IP Address	To Port
Iridium Certus / IOP	HTTP	TCP	40080	[IOP IP ADDRESS]	443

13.14 Default Remote Access rules for Leo/Meo/Shore connectivity

Below listed are the mandatory default remote access rules to be set up for Marlinks 4G Teltonika router and Starlink.

13.14.1 M arlink 4G Teltonika

Device Name	Service	Protocol	From Port	To IP Address	To Port
4G Teltonika RUT	HTTP	TCP	20080	[FB IP ADDRESS]	80

13.14.2 S tarlink

The below list is already set by default so doesn't need to be added.

Device Name	Service	Protocol	From Port	To IP Address	To Port
Starlink Maritime	HTTP	TCP	2398X	[XC IP ADDRESS]	80

Where X = 1, 2, 3 or 4 depending on the number of the Starlink to reach

13.15 Optional XChange WiFi remote access rules

Device Name	Service	Protocol	From Port	To IP Address	To Port
WiFi Switch	HTTP	TCP	8080	[Switch IP ADDRESS]	80
AP1	HTTP	TCP	8081	[AP1 IP ADDRESS]	80
AP2	HTTP	TCP	8082	[AP2 IP ADDRESS]	80
AP3	HTTP	TCP	8083	[AP3 IP ADDRESS]	80
AP4	HTTP	TCP	8084	[AP4 IP ADDRESS]	80
AP5	HTTP	TCP	8085	[AP5 IP ADDRESS]	80
AP6	HTTP	TCP	8086	[AP6 IP ADDRESS]	80

13.16 Optional remote access rules

The below table shows, how to set up port forwarding rules to equipment if Telnet commands must be used. The accessing supporter can adapt the port forwarding rules in *Box Settings > Network > Support Remote Access*. It´s not needed to restart the service or the XChange Box. All changes take effect immediately.

13.17 VSAT:

Device Name	Service	Protocol	From Port	To IP Address	To Port
VSAT Sailor ACU	Telnet	TCP	11023	[ACU IP ADDRESS]	23
VSAT Seatel ACU	Console	TCP	12001	[ACU IP ADDRESS]	2001
VSAT Intellian ACU	PCController	TCP	14002	[ACU IP ADDRESS]	4002

13.18 FleetBroadband:

Device Name	Service	Protocol	From Port	To IP Address	To Port
FB Sailor 500	TelnetAT	TCP	25454	[FB IP ADDRESS]	5454
FB Sailor 500	Telnet	TCP	20023	[FB IP ADDRESS]	23
FB JRC 500	Telnet	TCP	20023	[FB IP ADDRESS]	23
FB JRC 501	Telnet	TCP	20023	[FB IP ADDRESS]	23
FB Furuno 500	Telnet	TCP	22533	[FB IP ADDRESS]	2533

13.19 Addtional Remarks

If more than 2 connectivity systems are connected to the XChange Box and Marlink´s support teams need to have remote access available, the incoming 'From' ports must begin with:

- 3 for the 3rd terminal
- 4 for the 4th terminal
- 5 for the 5th terminal

14. Annex 2: XChange Interconnect

14.11.INTRODUCTION

XChange Interconnect is an optional VPN service offered for XChange customers. This annex describes the procedure to configure the XChange to make it possible for the communication between dedicated groups/LANs and the customer's Headquarter.

14.2Prerequisites

- The XChange runs version 5.0 or higher. (Firmware version 4.1 is the absolute minimum)
- Previously, the customer must have ordered the XChange Interconnect before, which has been validated by TSS.
- A fully filled "XChange Interconnect Service Order Form" must be made available for you, and vessel-dedicated VPN certificates must be provided.
- The XChange and all communication devices must be well prepared.
- The dedicated LANs (Admin, IT, Nav.) must be configured based on the Service Order Form.

If you don´t have a vessel-dedicated VPN certificate available, contact the support team immediately!

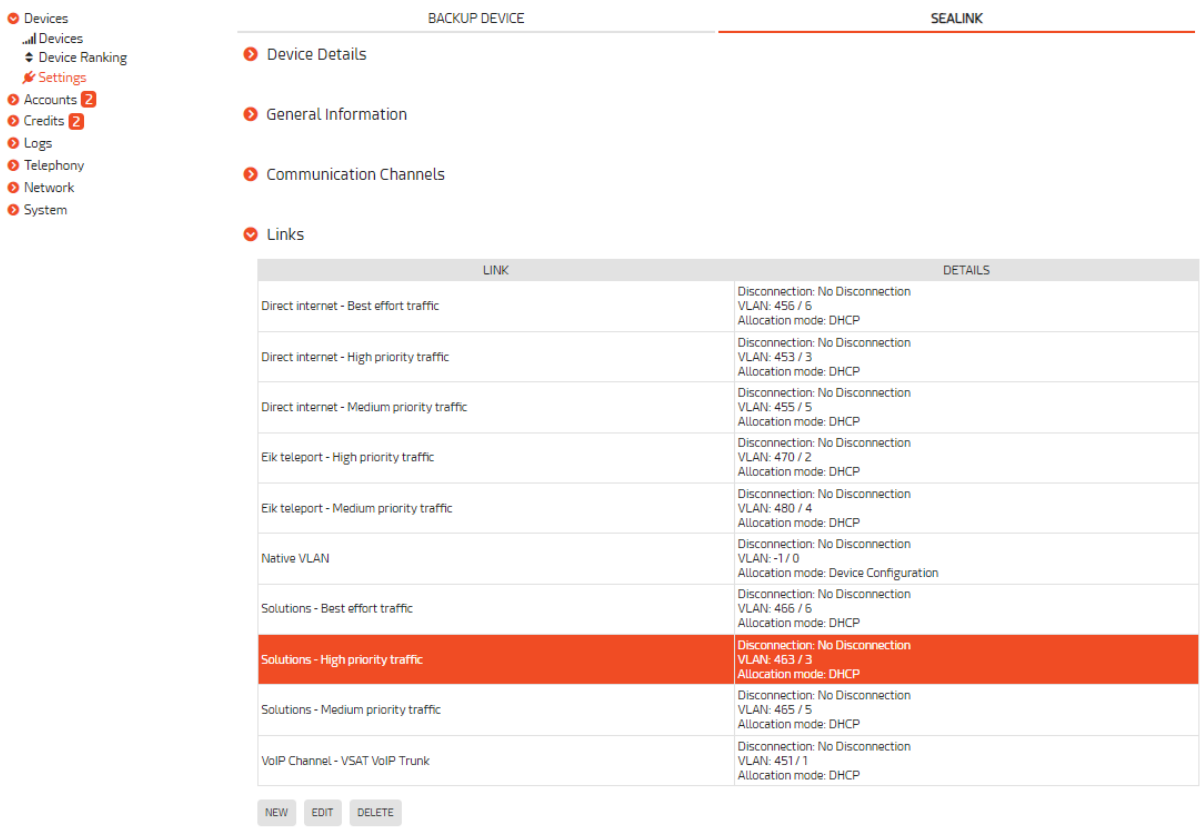
14.3Setup Interconnect channels

14.3.1 Setup links

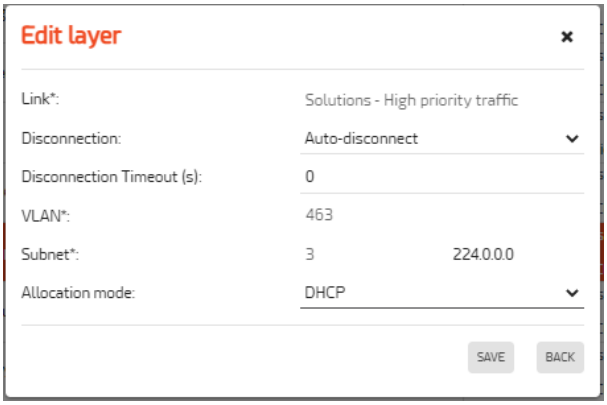
Note: This part is only for the XChange configured with the Full Auto switching commercial offer.

The following configuration is actually a workaround for making the VPN channel switch between the devices. The VPN channel will be automatically mounted with the higher-prioritised device.

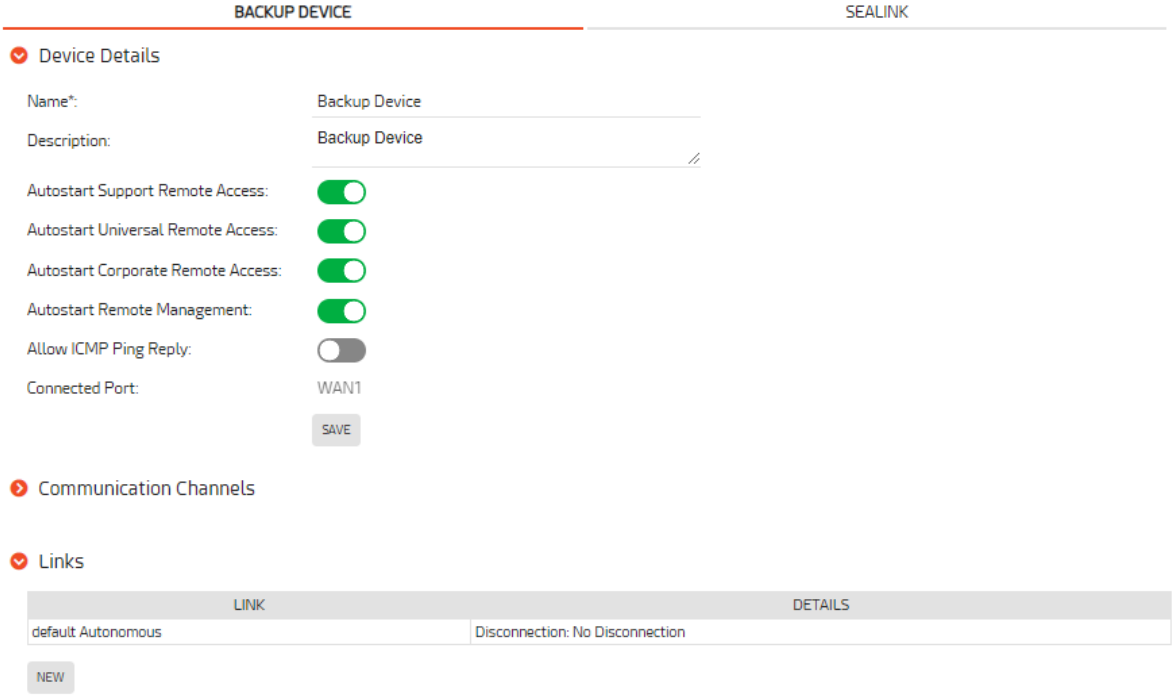
Go to *Box Settings > Devices > Settings* and select the "Solutions – High priority traffic" channel and click on Edit



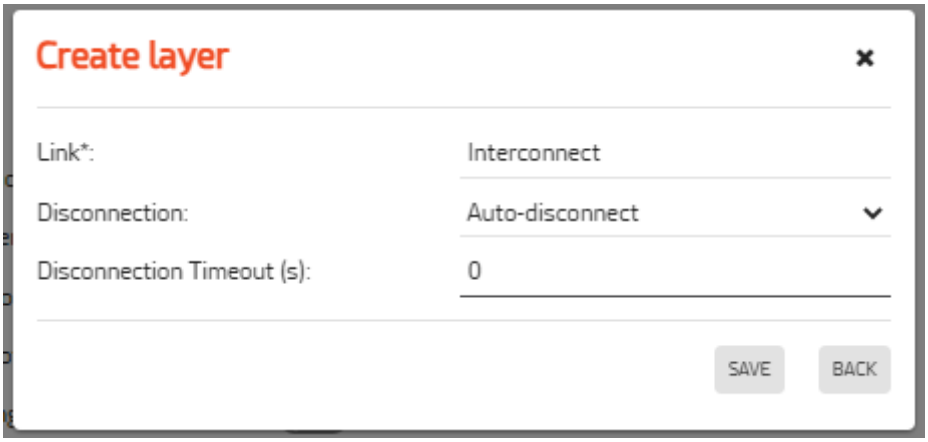
1. Set the following options then click on “Save”:
    a. Disconnection = “Auto-Disconnect”
    b. Disconnection Timeout (S) = “0”



2. For any other communication device other than Sealink, go to the second device section and click on “New”.



3. Set the following options and click on “Save”:
    a. Link = “HQ interconnect ”
    b. Disconnection = “Auto-Disconnect”
    c. Disconnection Timeout (S) = “0”

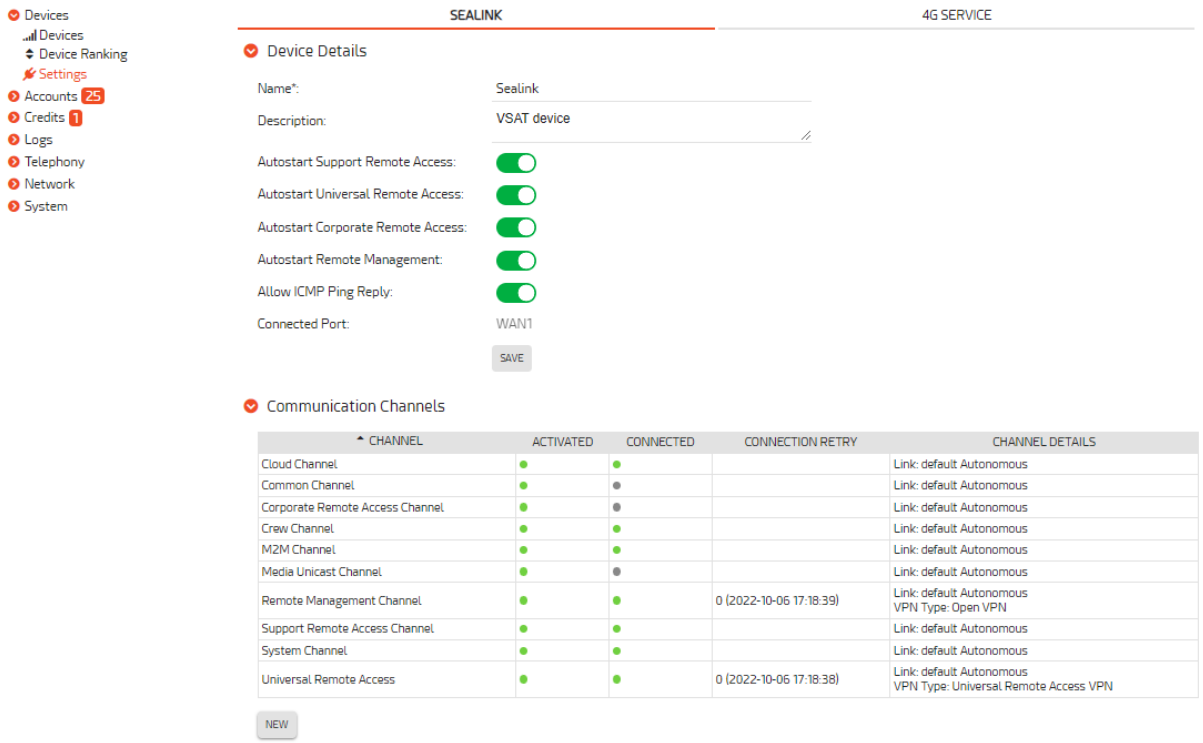


14.3.2 Setup channels

*Note: The following operations have to be performed for each device. In addition, only the **"fengineer"** has the required rights to perform these actions.*

Go to Box Settings > Devices and select Sealink. Expand the "Communication Channels" panel

1. Click on "New"



2. Fill the fields of the following form:

Status:	Enabled
Channel Name:	XChange Interconnect
Description:	XChange Interconnect VPN connection
Communication type:	Data
Link:	Interconnect
VPN Type:	Open VPN
Direction:	Both-Way
Endpoint address:	<SERVER_IP>
Data compression:	Enabled
Keepalive period:	10
Protocol:	UDP
Endpoint port:	
Authorize unsecured connection:	
Cryptographic cipher:	AES (256 bits)
Certificate State:	Not uploaded yet BROWSE
Incremental retry interval timer:	
Start incrementing counter:	3
Stop incrementing counter:	13
Maximum retry interval timer:	300
	SAVE BACK

3.
   a. Where <Link> is the previous edited/created links according to the device with High priority traffic
   b. Where <server_ip> and <server_port> are the **public IP Address** and the **port** of the OpenVPN server (refer to **Interconnect Service Order Form**)
   c. For the certificate, click on browse and select the previously created certificate (**vessel.p12** file)
4. Click on SAVE
5. Renew these actions for each device

***Important**: The following configuration is a part of the workaround of the channel switching and must be performed to ensure to avoid wrong behaviour.*

Go to *Box Settings* > *Devices* > *Settings* and select Sealink, then expand the “Communication Channels” part

1. Make sure that no channel uses the previously edited link. In our case, M2M Channel uses this link by default so select it and edit it:

Communication Channels

CHANNEL	ACTIVATED	CONNECTED	CONNECTION RETRY	CHANNEL DETAILS
Cloud Channel	●	●		Link: Solutions - Best effort traffic VLAN: 466 / 6
Common Channel	●	●		Link: Solutions - Medium priority traffic VLAN: 465 / 5
Corporate Remote Access Channel	●	●		Link: Eik teleport - Medium priority traffic VLAN: 480 / 4
Crew Channel	●	●		Link: Solutions - Best effort traffic VLAN: 466 / 6
M2M Channel	●	●		Link: Solutions - High priority traffic VLAN: 463 / 3
Media Multicast Channel	●	●		Link: Native VLAN VLAN: -1 / 0
Media Unicast Channel	●	●		Link: Solutions - Best effort traffic VLAN: 466 / 6
Remote Management Channel	●	●		Link: Eik teleport - Medium priority traffic VLAN: 480 / 4 VPN Type: Open VPN
Support Remote Access Channel	●	●		Link: Native VLAN VLAN: -1 / 0
System Channel	●	●		Link: Solutions - Medium priority traffic VLAN: 465 / 5
Universal Remote Access	●	●		Link: Eik teleport - High priority traffic VLAN: 470 / 2 VPN Type: Universal Remote Access VPN
XChange Voice Channel	●	●		Link: VoIP Channel - VSAT VoIP Trunk VLAN: 451 / 1

NEW EDIT DIAGNOSE

2. Set the option Link = “<solution> - Medium priority traffic” then click on Save

Status: Enabled
Channel Name: m2m_channel
Description: M2M Channel
Communication type: Data
Link: Solutions - Medium priority traffic
Incremental retry interval timer:
SAVE BACK

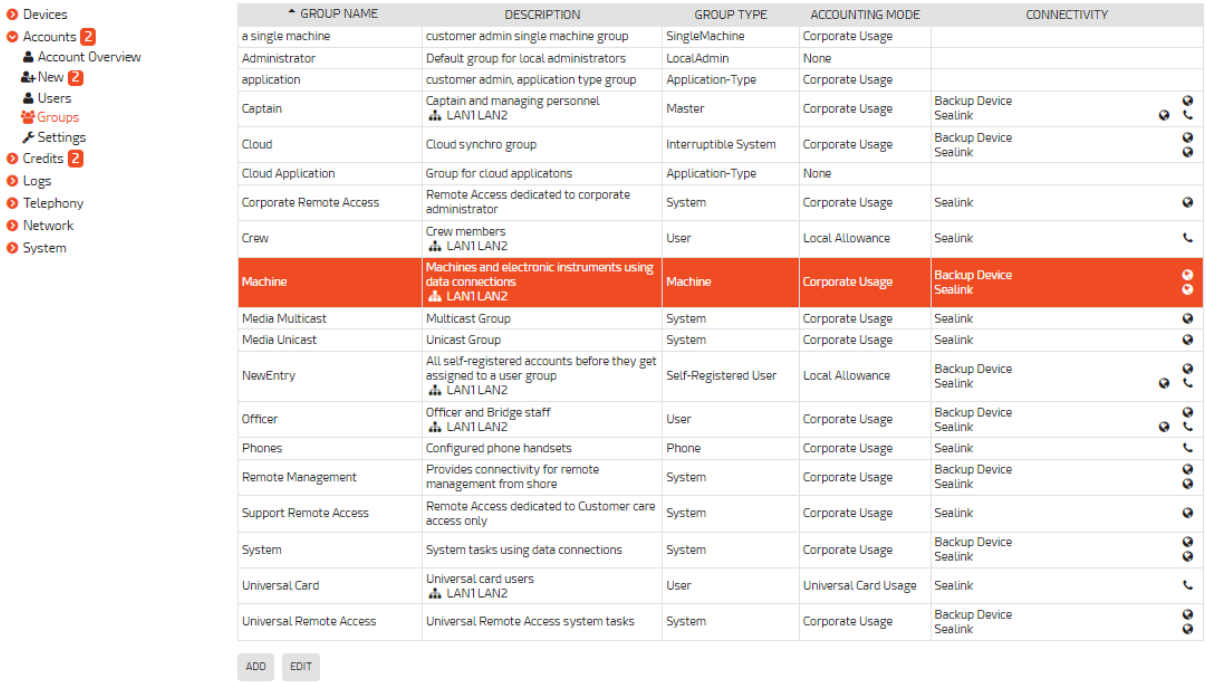
The groups can now be configured with the VPN channels

14.4 Setup accounts

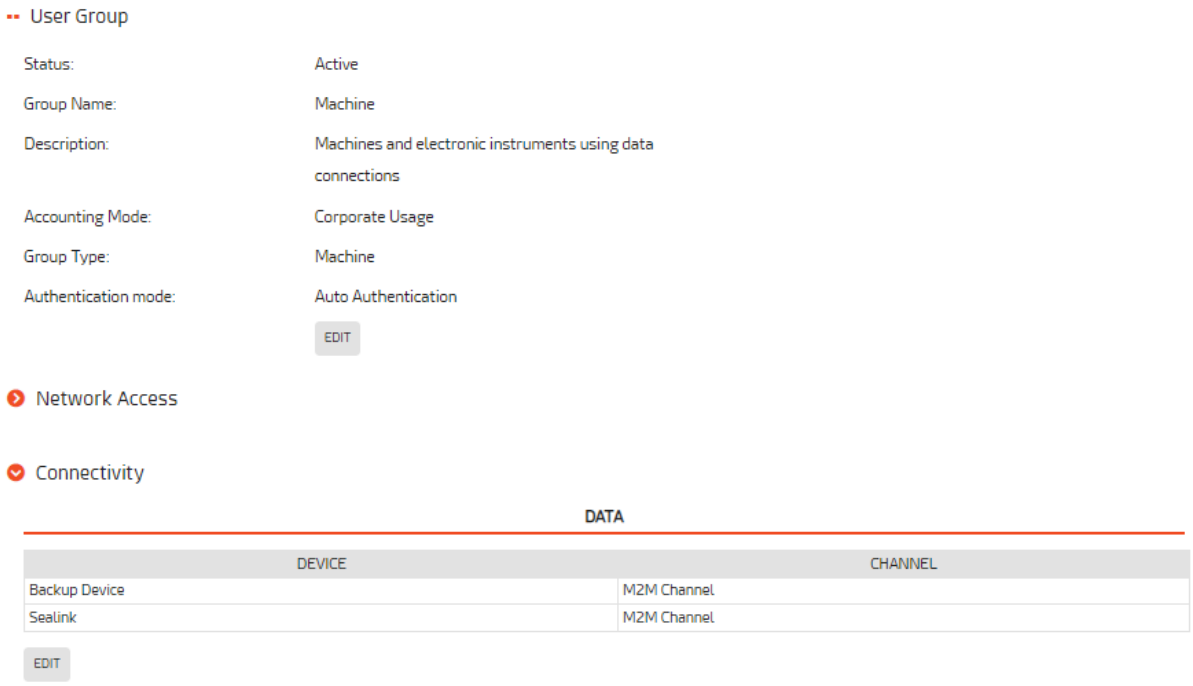
14.4.1 Setup groups

Note: In this example, we modify the "Machine" group. The following operations can be performed for other group types than the Machine groups. It depends on the customer's needs.

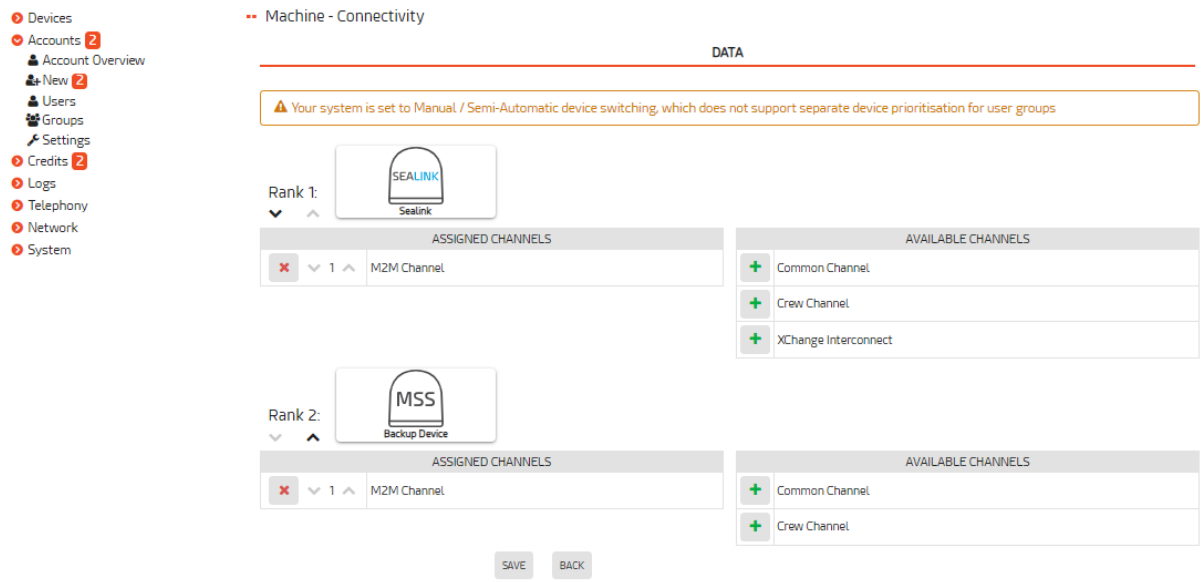
The channels have to be declared for all the groups which will use the VPN connection (here, the Machine group).



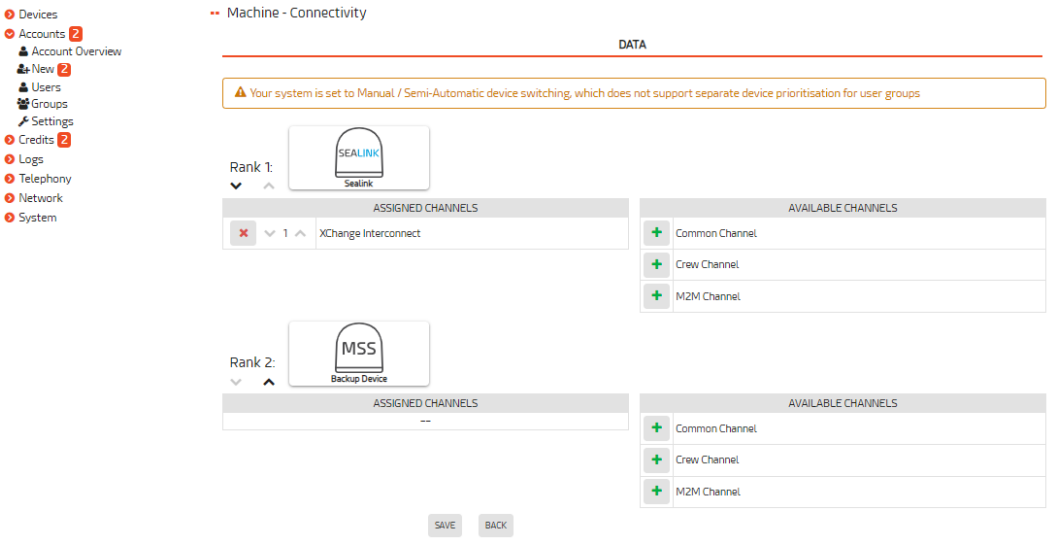
1. Expand the "Connectivity" part then click on "Edit":



2. Select "XChange Interconnect" and click on the green Plus:



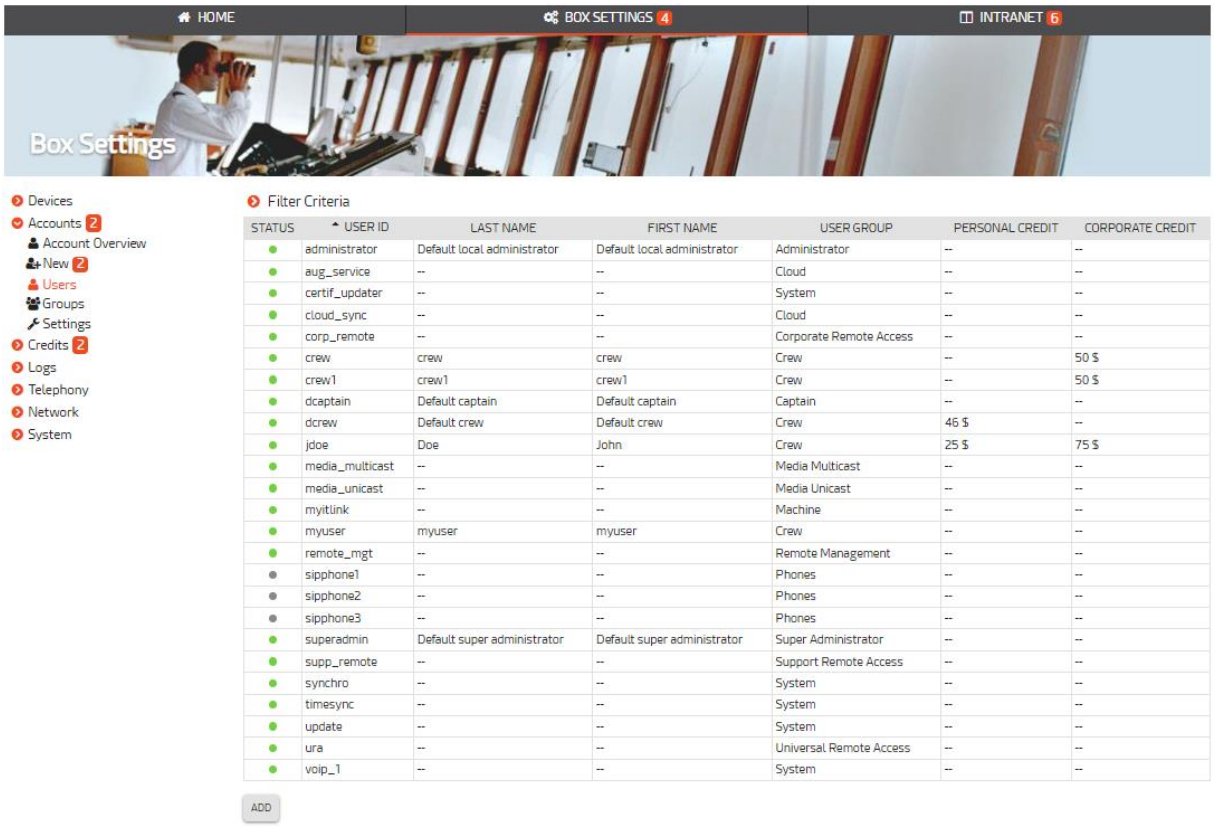
3. Make sure that the “XChange Interconnect” are in the first position (remove the other channels if needed). Then click on “Save”:



The “Machine” group is now configured to use the Interconnect channel, which means when a Machine account is connected, a VPN tunnel will automatically be established by the XChange autonomously.

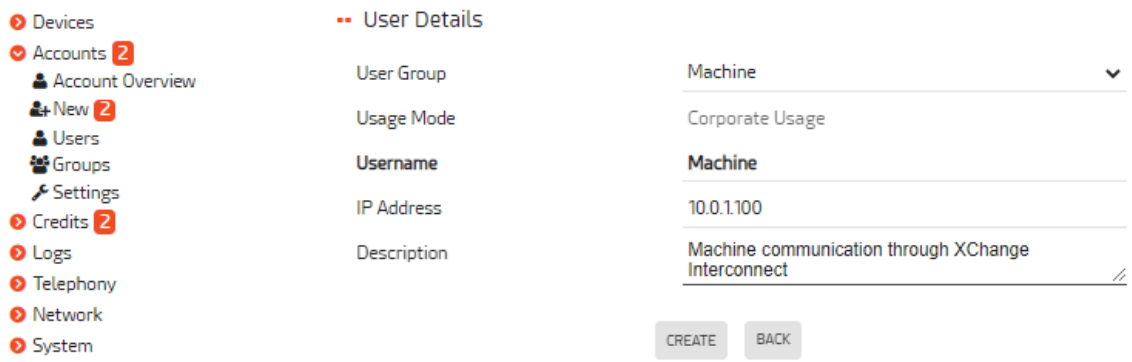
14.4.2 Create a Machine account

1. Go to “BOX SETTINGS”
2. Go to tab Accounts / Users
3. Click on “Add”



STATUS	USER ID	LAST NAME	FIRST NAME	USER GROUP	PERSONAL CREDIT	CORPORATE CREDIT
●	administrator	Default local administrator	Default local administrator	Administrator	--	--
●	aug_service	--	--	Cloud	--	--
●	certif_updater	--	--	System	--	--
●	cloud_sync	--	--	Cloud	--	--
●	corp_remote	--	--	Corporate Remote Access	--	--
●	crew	crew	crew	Crew	--	50 $
●	crew1	crew1	crew1	Crew	--	50 $
●	dcaptain	Default captain	Default captain	Captain	--	--
●	dcrew	Default crew	Default crew	Crew	46 $	--
●	jdoe	Doe	John	Crew	25 $	75 $
●	media_multicast	--	--	Media Multicast	--	--
●	media_unicast	--	--	Media Unicast	--	--
●	myitlink	--	--	Machine	--	--
●	myuser	myuser	myuser	Crew	--	--
●	remote_mgt	--	--	Remote Management	--	--
●	sipphone1	--	--	Phones	--	--
●	sipphone2	--	--	Phones	--	--
●	sipphone3	--	--	Phones	--	--
●	superadmin	Default super administrator	Default super administrator	Super Administrator	--	--
●	supp_remote	--	--	Support Remote Access	--	--
●	synchro	--	--	System	--	--
●	timesync	--	--	System	--	--
●	update	--	--	System	--	--
●	ura	--	--	Universal Remote Access	--	--
●	voip_1	--	--	System	--	--

4. Fill in the mandatory fields:



   a. Username can be customized
   b. Select “Machine” as the User Group
   c. Enter the IP Address of the machine. This IP will be fixed. When a machine with this IP will be connected, it will be directly connected to the OpenVPN server with a VPN tunnel

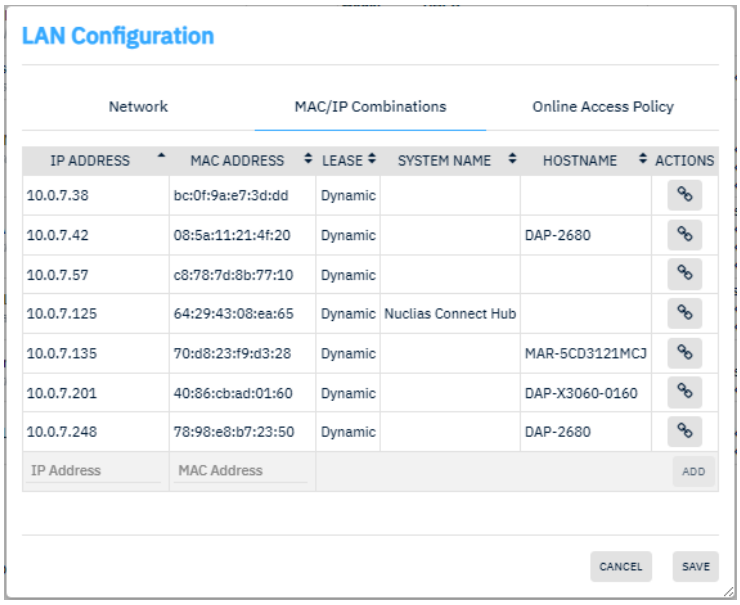
5. Click on “SAVE”

14.5 Others

14.5.1 (Optional) Fix the IP Address for a machine with the MAC Address

In the XChange, it is possible to allocate an IP Address for a specific MAC Address:

1. Go to “BOX SETTINGS”
2. Go to Network / “LANs/WANs”
3. Select the LANs on which the machine(s) will be connected
4. Click the “Edit” icon of that network and jump to MAC/IP combinations



5. Enter the MAC Address and the IP Address then click on “ADD”:
6. A new line has been added with the MAC Address and IP Address combination.
7. Repeat if there are several assignments to do.
8. Click on “SAVE” to finalise the task.

15. Need Support?

If you have any questions, please contact Marlink Service Desk:

Marlink Service Desk

Email: servicedesk@marlink.com
EMEA: +33 (0)1 70 48 98 98
Americas: +1 (310) 616-5594 +1 855 769 39 59 (toll free)
Asia Pacific: +65 64 29 83 11