



ELSIGHT HALO USER GUIDE

Standalone BondBox Version

SW VERSION 12.0.0

REVISION 1

FEBRUARY 17, 2025

ELS User Guide – Copyright and Disclaimer

Copyright

Copyright © 2024 Elsight Ltd.

All rights reserved. This manual is protected under international copyright laws.

No part of this manual may be copied, reproduced, distributed, translated, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or storing in any information storage and retrieval system without the written consent of Elsight Ltd.

In support of our policy of continuous product improvement we reserve the right to change materials and specifications and to make changes in the content of this manual without obligation to notify any person or organization of such changes or improvements. Go to www.elsight.com for current updates and supplemental information concerning the use of this product.

Drawings, where shown, may not be to scale. Dimensions are metric and size maybe approximate. Where possible, data sheets, specifications and user manuals are made available on our website: <http://www.elsight.com>. All products should be installed and used in accordance with manufacturer's instruction provided. Warning: products may be subject of registered designs and patents. Refer to our website for terms and conditions on warranty. Every effort has been made to ensure accuracy of content. However, no liability will be met by Elsight Ltd or its suppliers for any errors or omissions. All brands and logos are registered trademarks and are subject to copyright laws.

ELS User Manual – Part Numbers

This guide is relevant for the following device part numbers:

- HNF4W
- HNF2W
- HEU4W
- HEU2W
- HAP4W
- HAP2W
- HCN4W
- HCN2W
- HLA4W
- HLA2W
- HWW2W
- HWW4W

FCC Regulatory Notices

FCC ID Information

The Halo FCC ID is **2AWEB-HALOHNF4W**.

Mobile Device RF Exposure Statement

This device is only authorized for use in a mobile application. Users must maintain a distance of at least 20 cm from this device at all times.

FCC Modification Warning

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC Rules.

Class A Warnings

The FCC Wants You to Know:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Interference Statement

This device complies with Part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Wireless Notice

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and meets the FCC radio frequency (RF) Exposure Guidelines and RSS-102 of the radio frequency (RF) Exposure rules. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contents

FCC Regulatory Notices	2
Contents	3
Introduction	6
Elsight Halo Communication Platform	6
System Flow	7
Hardware Overview	8
The Halo BondBox Front Panel	8
The Halo BondBox Back Panel	9
GNSS Sources	9
The Elsight Halo Web GUI	11
IP Configuration for Windows	12
Static IP Configuration for Ubuntu	13
Connecting to the Halo Device	16
The Halo GUI Main Window	17
Using the Home Dashboard	18
Using the Header Bar	20
Using the Main Menu	21
NICs (Network Interface Controllers)	22
Using the NICs Management Page	22
WAN Prioritization	22
Throughput	25
Iptables Configuration	25
Adding an iptables Rule	26
Port Forwarding via the API	27
Using Specific NIC Pages	28
Status	29
Settings	29
Configuring the DHCP State	29
Configuring a WAN Link	30
Assigning an Alias	31
Operations	31
Cellular NICs	31
Status	32
Recording RF Signals	34

Dialing Rules and APN	35
Optional Settings	36
Network Limitations	36
Operator Selection	37
Ethernet NICs	38
Settings	39
Ethernet NIC Added to VLAN	40
WiFi NICs	40
Settings	40
Adding a Configuration	41
WiFi NIC Added to VLAN	42
VLAN NICs	43
Settings	43
SatCom	45
Data Path	46
Application Rules	47
VPN Profiles	47
Adding a Direct-VPN profile	48
Services	49
MAVLink	49
Remote-ID	51
Remote ID Status	51
Detecting Other Remote ID Devices	51
Configuring Remote ID	52
Users	54
User Permission Levels	54
Editing a User	55
Adding a User	55
Maintenance	56
Serial Number	56
Firmware	56
Firmware Upgrade	57
Realm	57
Environment	58
Logs	58
Factory Reset	58

Hardware	58
Advanced	59
Tunnel Settings.....	59
Working in P2P Mode	59
The Elsight Help Center	60
Accessing the Help Center	60
Submitting a Request	60
Appendix A: Connectors Description.....	62
CAN Bus	62
Power In Connector	62
Appendix B: User Access Level Permissions	63
Appendix C: Cellular NIC RF Recording Data	65
Cellular NIC Signal Quality.....	67
RSRP - RX Level	67
SNR – Signal to Noise	67
RSSI.....	68
SINR	68

Introduction

The Elsight cutting-edge technology provides secure, real-time, adaptive data transmission over multiple IP links. Ground-breaking hybrid data connectivity solutions allow for on-the-move and high-bandwidth communication, anytime and anywhere.

Elsight Halo Communication Platform

The world's most compact, next-generation bonding technology, Elsight Halo provides high-bandwidth, highly-secured communication for the transmission of live data, in real-time, from anywhere and to anywhere, while on-the-move or on-the-ground.

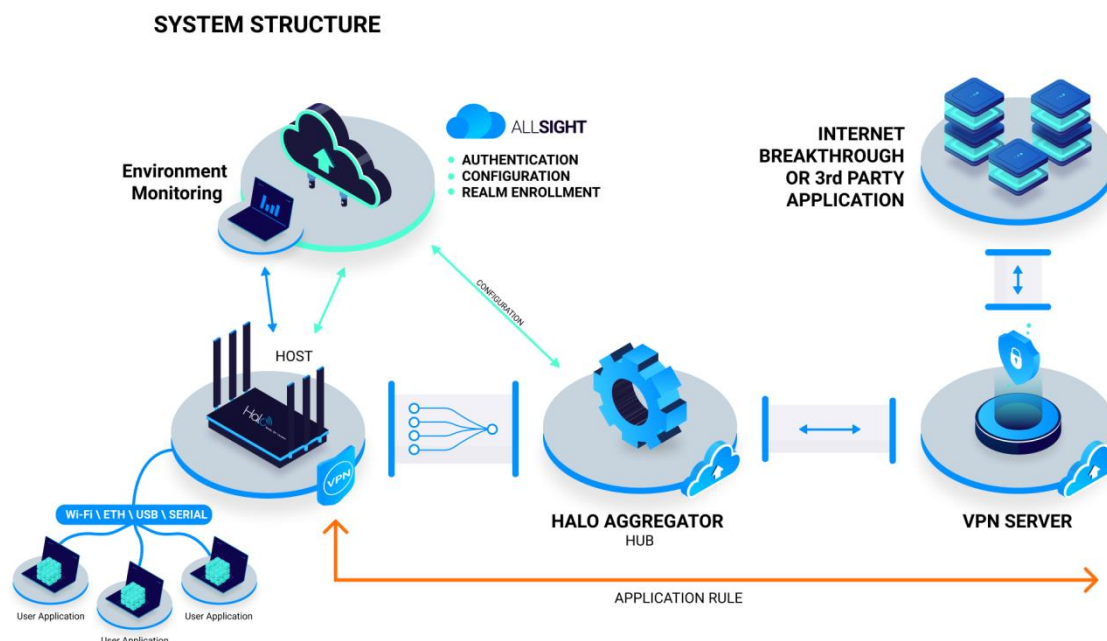


The Halo communication platform is available in 2 form factors:

- As a standalone device (described in this guide)
- As an OEM card (see the [Elsight Halo User Guide OEM Version](#))

System Flow

The Elsight system flow is illustrated in the diagram below.



The system falls into 3 basic zones:

- AllSight Cloud and Halo host devices:

The AllSight Cloud Platform provides authentication and configuration support for the Halo host devices.

The host is the Halo communication platform described in this guide, which breaks the data into separate data streams and transmits those streams over multiple IP links.

Note that in some cases, for example a P2P connection, the Halo hardware can be both the host and the hub.

- Hub:

The hub is the Halo aggregator, which reassembles the data for final transmission to the endpoint.

- Hub endpoint:

The hub endpoint is in 3rd party space, such as a VPN.

The application rules, which are configured via the Cloud Platform, define the functionality and relationships of all 3 zones. (See the [AllSight Cloud Platform User Guide](#) for more information.)

Hardware Overview

This section describes the Halo interfaces and LEDs.

The Halo BondBox Front Panel



On the Halo front panel are the status LEDs:

- LEDs 1-4: Cellular status LEDs

The cellular status LED states are described in the following table.

State	Description
Red	SIM card issue*, unable to dial
Blinking -Red	SIM identified, initializing
Blinking Blue Red	SIM identified, custom APN settings required (see Dialing Rules and APN.)
Blinking Blue	• Connected to the network (dialed and IP obtained) but not connected to the aggregator** OR • Link is not in use due to low priority
Blue	Connected to the aggregator

* - possibly due to data plan

** - possibly due to bad signal

- LED 'S': System status LED

The system status LED states are described in the following table.

State	Description
Off	Not connected to the to the VPN
Green	Connected to the VPN

The Halo BondBox Back Panel



The following figure shows the back panel connector labels (top view of the device). The connectors are described in the table below.



#	Description
1	RS/CAN BUS
2	ETH 2
3	ETH 1
4	USB 2.0
5	DC IN (9-30V)

GNSS Sources

The Halo supports 3 GNSS input options:

- MAVLink
- API
- Built-in GNSS

By default, the priority of the inputs is in the order listed above. If a higher source is not active for 3 seconds, the next lower source is automatically accessed.

If a higher priority source becomes available, it will immediately be used.

The data from the currently active source is always used throughout the system for all location-related applications, such as Halo location, Remote ID, etc.

NOTE: The priority of the inputs can be changed by our support team. Please contact the Elsight support team for assistance.

The Elsight Halo Web GUI

The Elsight Halo Web GUI provides access to the Halo device for configuration, monitoring, management, and maintenance.

The application consists of the following modules:

- **Home page**

Dashboard that displays basic information about the device:

- Connectivity, environmental and identifying information
- Announcements
- NIC status summary
- Real time graph of the total download and upload WAN data rate over the last minute.

- **NICs (Network Interface Controllers)**

This module provides access to all of the device Network Interface Controllers:

- NICs Management
- Cellular Modem NICs
- Ethernet NICs
- WiFi NICs
- VLAN NICs.

Network Interface Controllers Management:

- Configure WAN prioritization
- Configure port forwarding according to specified iptables rules.

For each NIC you can:

- See relevant information such as NIC ID and IP address
- Configure parameters such as dialing rules or IP/subnets
- Perform operations such as enable/disable.

- **Data Path**

- View a listing of application rules applicable to this device
- Define direct VPN profiles.

- **Services**

- Configure MAVLink forwarding and MAVLink service
- Enable remote ID transmission.

- **Users**

In the Users module you can:

- Add and edit users
- Change the admin username and password.

- **Maintenance**

In the Maintenance module you can:

- Verify device firmware packages versions
- Upgrade or downgrade device firmware
- Setup device to a realm and associate device to an environment
- Shutdown or reboot the device
- Download the OpenVPN log
- Reset the device to factory defaults
- Disable the hardware LEDs.

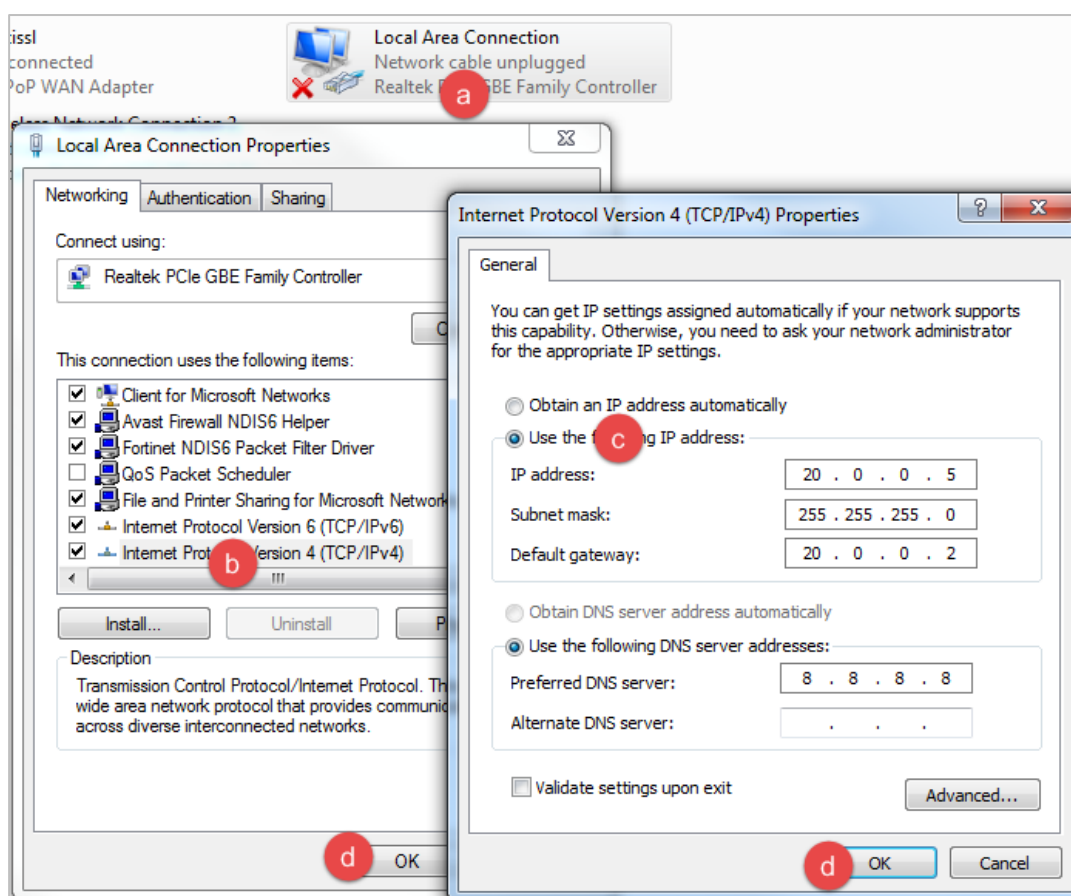
- **Advanced**

In the Advanced module you can:

- Work in P2P mode.

IP Configuration for Windows

1. In the **Network and Sharing Center**, go to **Change adapter settings** and find the relevant local area connection or Ethernet connection.
2. In the **Networking** tab, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
3. In the **General** tab> **Use the following IP Address**: enter the IP address and subnet mask
 - IP address: Similar to the default IP address of the Halo, just change the last number (for example 20.0.0.4 if the device IP is 20.0.0.2)
 - Subnet mask: Appropriate for the configured IP address (for example, if only the last digit was changed, use 255.255.255.0)
 - Default gateway
 - Preferred DNS server
4. Click **OK** and again **OK**.



Static IP Configuration for Ubuntu

The simplest way to configure the static IP address to talk to the Halo through Ubuntu, is to use the GNOME graphical user interface.

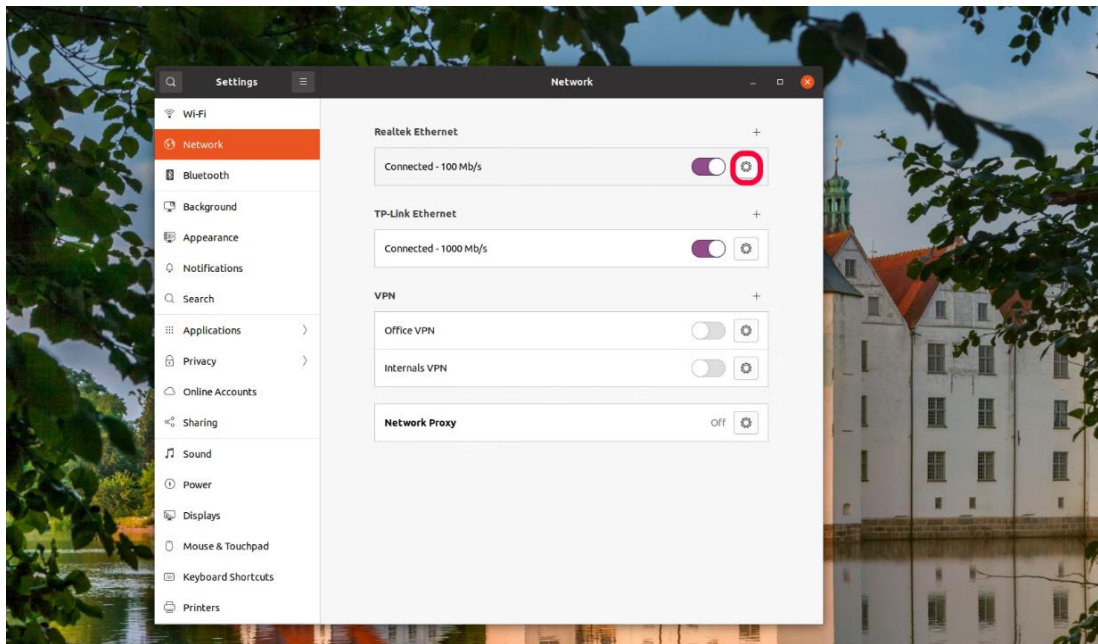
1. Click the network icon in the top right and navigate to the network port you wish to configure.



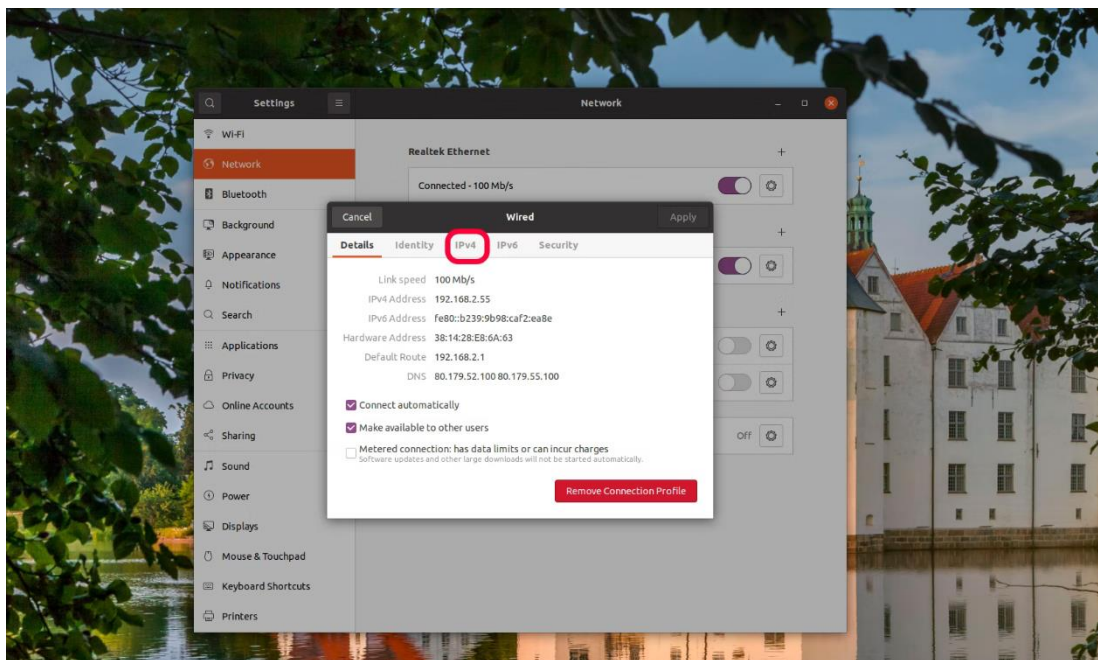
2. Click **Wired Settings**.



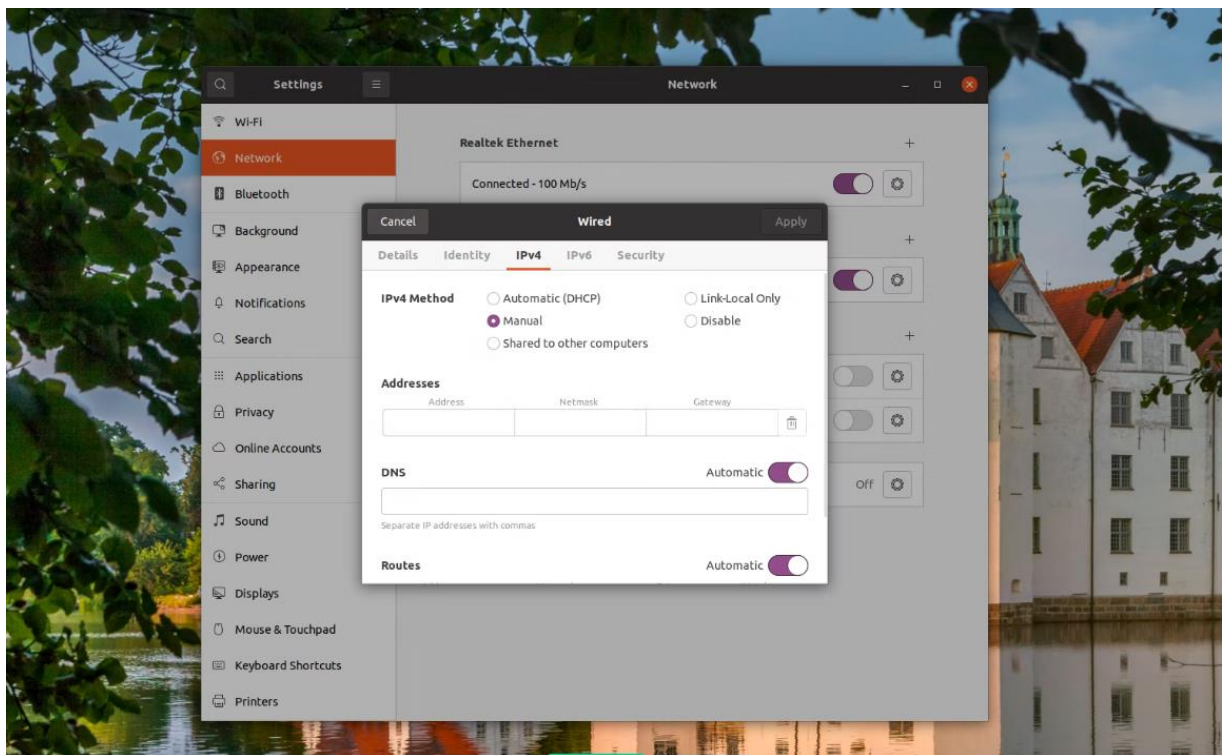
- Click the **Settings** icon.



- Select the **IPv4** tab.

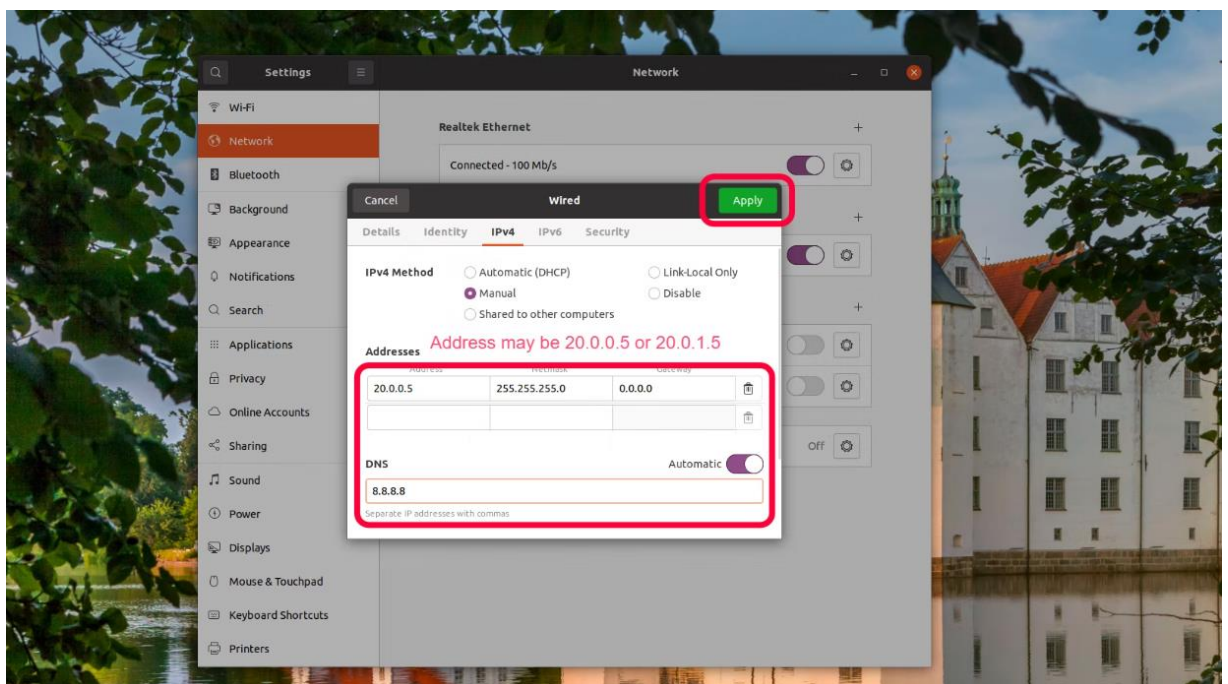


5. Select **Manual**.



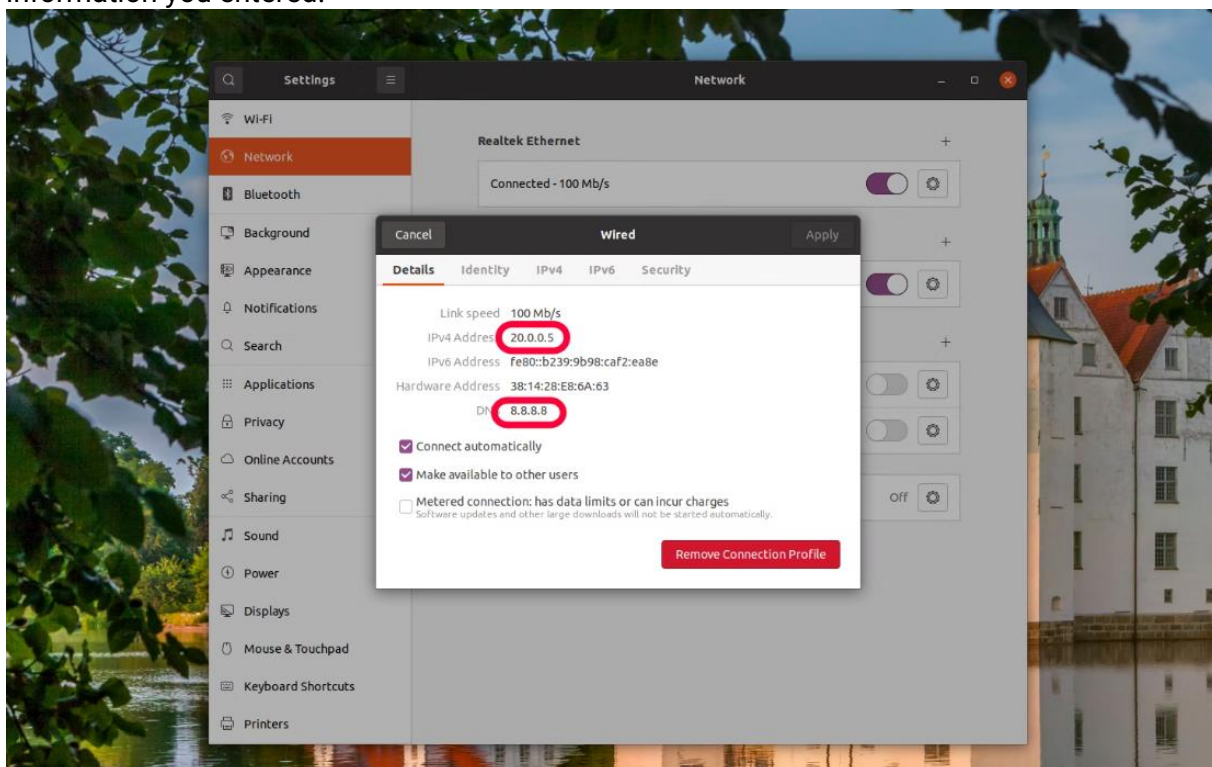
6. Enter the following information and click **Apply**.

- IP address:
 - ETH1: 20.0.0.5
 - ETH2: 20.0.1.5
- Netmask: 255.255.255.0
- Gateway: 0.0.0.0
- DNS address: 8.8.8.8



- Turn the network port off and on to apply the new settings.

Navigate to the network port **Settings** again, and check that the Details match the information you entered.



Connecting to the Halo Device

NOTE: It is recommended to use the latest version of Google Chrome web browser.

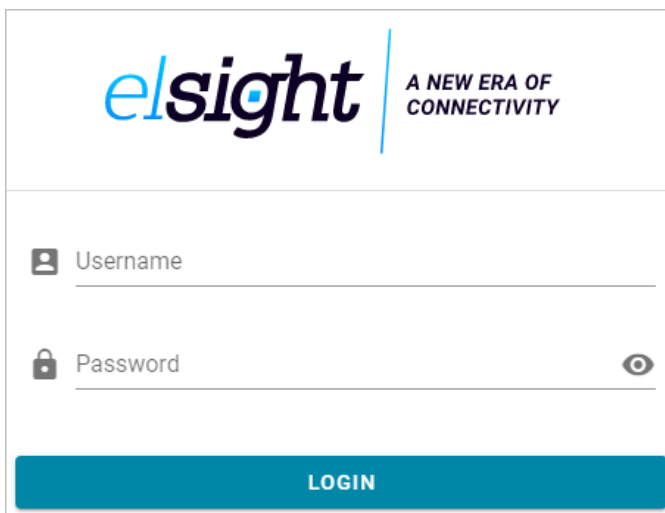
- Connect the unit to a computer via one of the Ethernet ports and plug it into a power source.
- Open a web browser and enter the IP address of the port in the address line:

By default the IP addresses are:

- ETH 1: 20.0.0.2
- ETH 2: 20.0.1.2

Note that these IPs can be changed in the NIC/Ethernet configuration (see Ethernet [Settings](#)).

- When the login page appears, enter your user name and password and click **Login**.



The login form features the Elsight logo and tagline at the top. Below is a 'Username' field with a person icon, followed by a 'Password' field with a lock icon and a toggle eye icon. A prominent blue 'LOGIN' button is at the bottom.

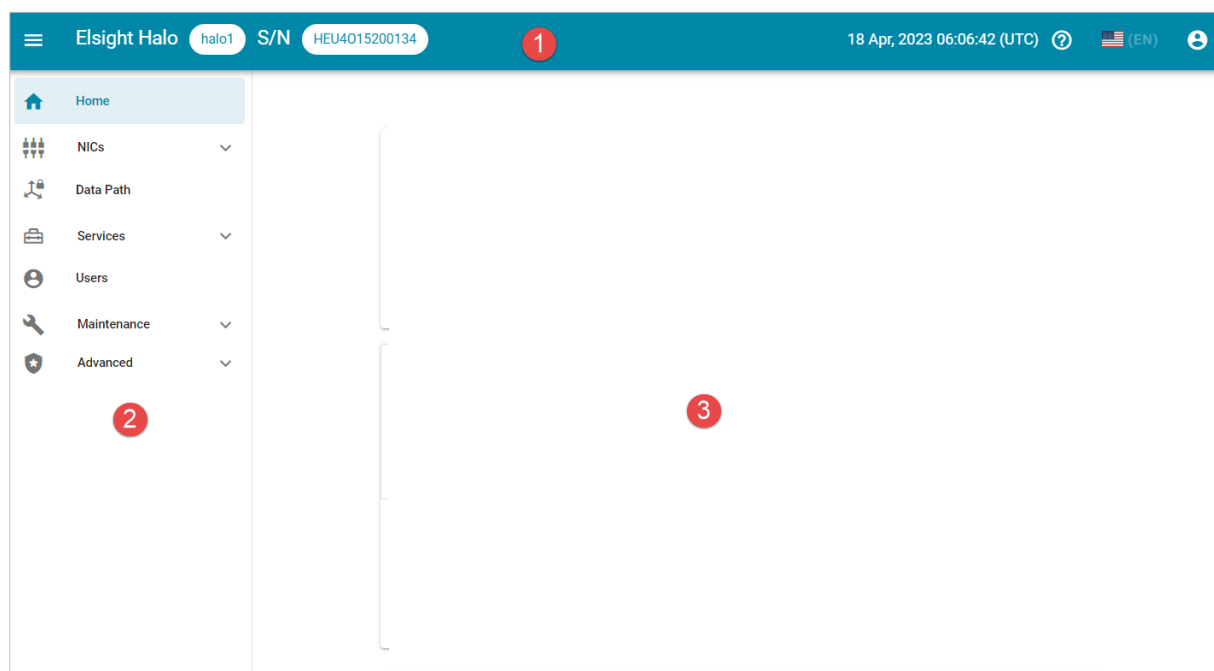
The default values are:

- Username: admin
- Password: admin

The Halo GUI opens to the Home page.

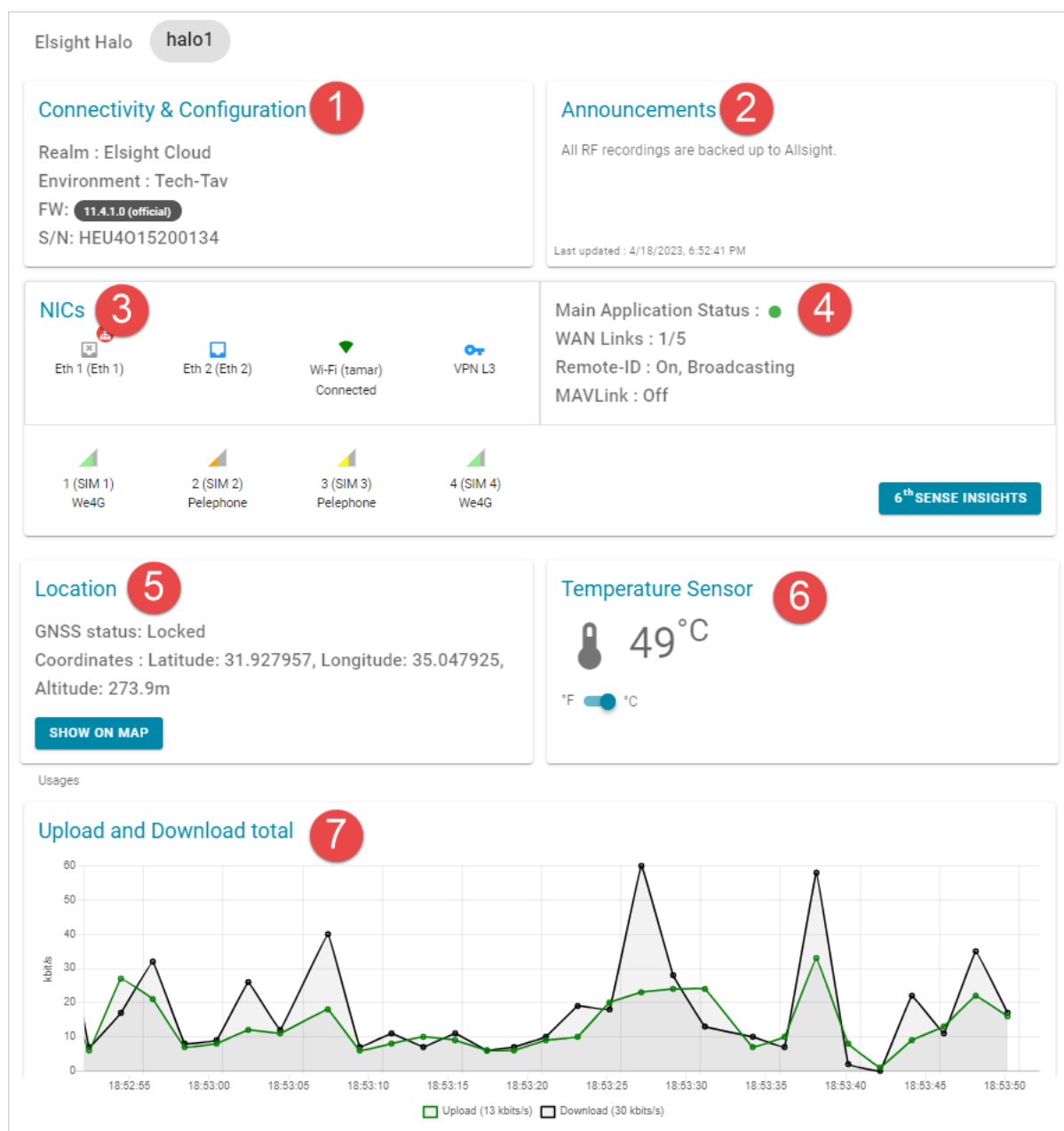
NOTE: The first time you log in you must change the admin password. See [Editing a User](#).

The Halo GUI Main Window



1. Header Bar
2. Main Menu
3. Workspace (Home or specific element configuration page)

Using the Home Dashboard



The Home dashboard displays the following information:

1. Connectivity and identifying information.
Click to edit the **Realm** and **Environment**.
2. Announcements.
3. NIC status summary. The icon indicates the link type and the color of the icon indicates the current status of the link
 - **Green**: link is up (WAN link only)
 - **Red**: link is down or other known issue
 - **Blue**: cable connected (non-WAN link only)
 - **Grey**: no data or not relevant (ETH or WiFi link NOT defined as a WAN link)
 - **▲**: cellular link

-  : Ethernet link
-  : WiFi link
-  : VPN
-  : VLAN
-  (X on icon): interface is disconnected
- 
 - Gray- Satcom is enabled and connected.
 - Red- Satcom is enabled but misconfigured.

Click on any icon to go to the relevant NIC page.

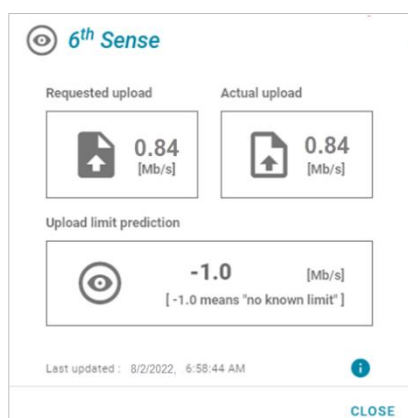
4. Additional NIC data:

- Main application status: application rule status
 - Green: the device is connected end-to-end for at least 1 application rule. (For most devices there will be only 1 relevant application rule. However, if there are more than 1, only 1 needs to be connected.)
 - Red: no application rule is connected end-to-end
 - Grey: no data or not relevant (server, for example)
- WAN links: {The number of links that are currently up}/{the total number of links}
- Remote-ID on or off and current Remote-ID broadcast status
- MAVLink on or off
- 6th Sense Insights: 6th Sense is the Halo network prediction algorithm.

Click **6th Sense Insights** to display the 6th Sense parameters.

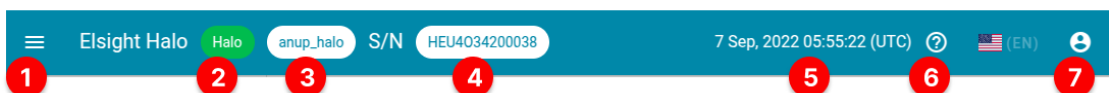
Click  to display an explanation of the parameters:

- **Requested upload** (Current throughput from application) – amount of throughput received from the user and transmitted by the device in Mb/s.
Note that the reported amount does not include redundancy.
- **Current upload** (Tunnel current upload throughput) – current actual throughput sent from the aggregation tunnel of the device (including redundancy) in Mb/s.
- **Upload limit prediction** (Tunnel detected upload limit) – predicted maximum throughput in Mb/s that can be transmitted by the device (value of -1.0 indicates no limit).



5. Location coordinates of the Halo device. If there is an internet connection to the device, you can click **Show on Map** to see it on a map and also update the control station location.
6. Temperature. Toggle to select Centigrade or Fahrenheit.
7. Real time graph of the total download and upload WAN data rate over the last minute.

Using the Header Bar



The header bar lets you do the following:

1. Minimize the main menu
2. Type of product with Color, on hover displays the tooltip



- a. Green: Connected
 - b. Orange: Alerts with icon and alerts message on the tooltip
 - c. Grey: Not-Connected
 3. Device name from the Allsight Cloud
 4. Copy the serial number
- The image shows a blue button with the serial number 'HEU4034200038' in white text. Below the button is a grey button with the text 'Click to copy'.
5. Device UTC clock
 6. Access the support portal (if the device is on-premises, it must have an active internet connection)
 7. Open User Menu: [same content, no changes]

Using the Main Menu

The following table explains the main menu icons:

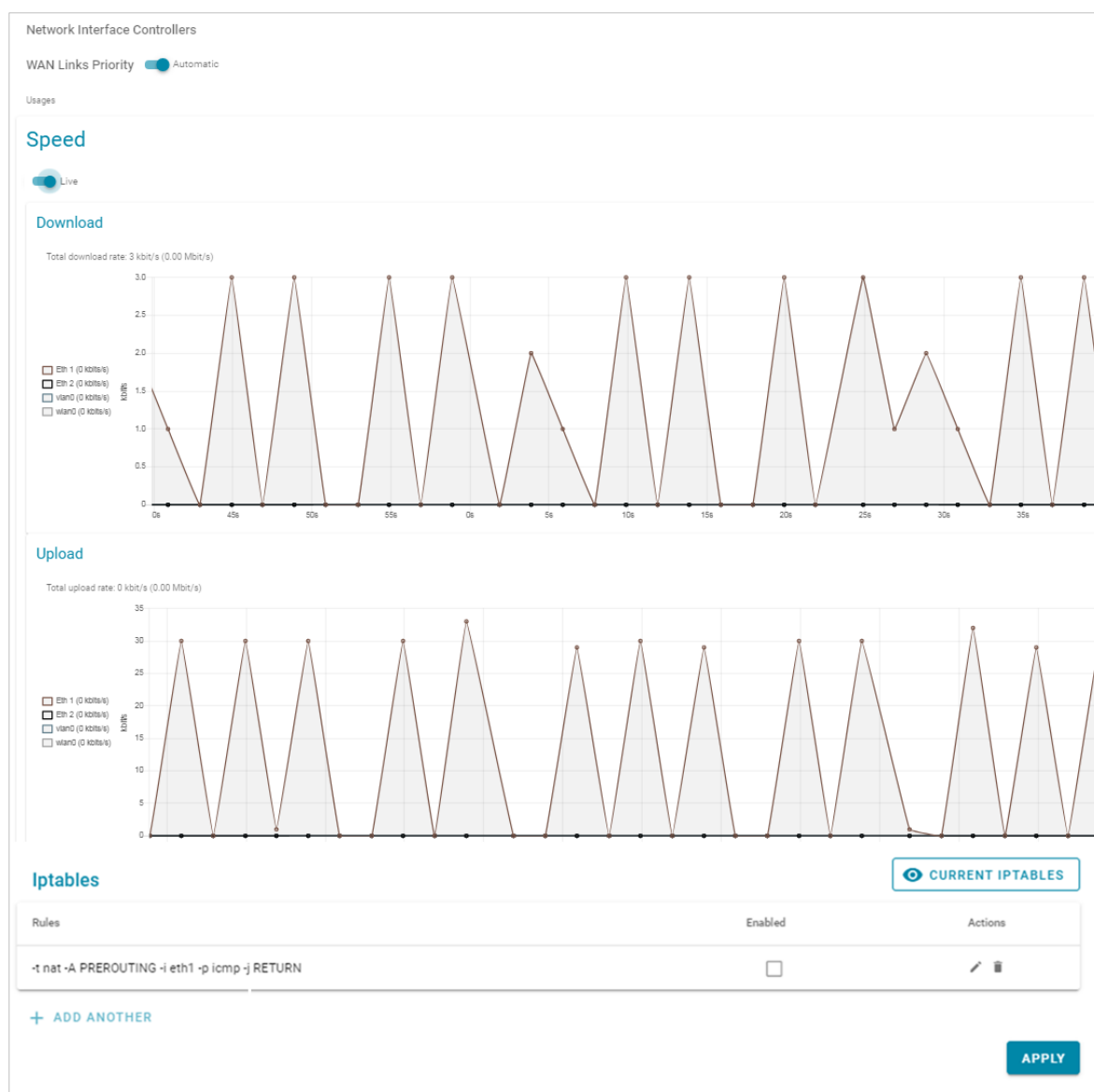
	Home
	NICs
	NICs Management
	Cellular NICs
	Ethernet NICs
	WiFi NICs
	VLAN NICs
	Data Path
	Services
	MAVLink
	Remote-ID
	Users
	Maintenance
	Hardware
	Advanced
	Tunnel Settings

NICs (Network Interface Controllers)

Use this module to configure and manage the device NICs. There are 2 main sections:

- The main NIC management page: global status and configuration
- Specific NIC pages: access to status and configuration for each specific NIC type

Using the NICs Management Page



The NIC Management page displays:

- WAN link prioritization configuration (see [WAN Prioritization](#))
- The throughput graphs (see [Throughput](#))
- Iptables configuration (see [Iptables Configuration](#))

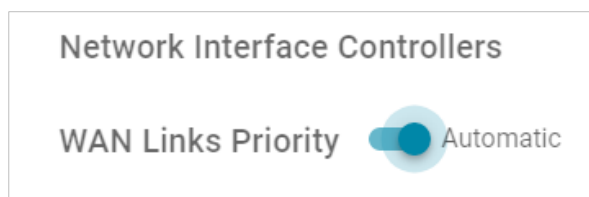
WAN Prioritization

In this section you can choose between letting the Halo prioritize the various WAN links automatically, which uses all the links according to link performance and need, and

specifically configuring the priorities manually according to your preference.

To select automatic WAN links prioritization:

Set the WAN Links Priority toggle to **Automatic**.



To manually specify WAN links priority:

1. Move the WAN Links Priority toggle to turn off **Automatic**.

The priority WAN Links Priority table opens. All configured WAN links will be listed under Priority 1.

WAN Links Priority ☐ Automatic			
Priority 1 - Preferred			
⋮	cell1 (We4G)	Cellular	Dialing
⋮	cell2 (Pelephone)	Cellular	Error
⋮	cell3 (Pelephone)	Cellular	Error
⋮	cell4 (We4G)	Cellular	Error
⋮	Eth1	Ethernet	Up
⋮	wlan0	Wi-Fi	Up
Priority 2 - Hot backup			
Priority 3 - If there is no choice			
Priority 4 - Cold backup			
Priority 5 - Never use			
Note: Remote-ID and FOTA will not follow the priority and may use any of the active links			

Drag and drop the WAN links to the desired priority.

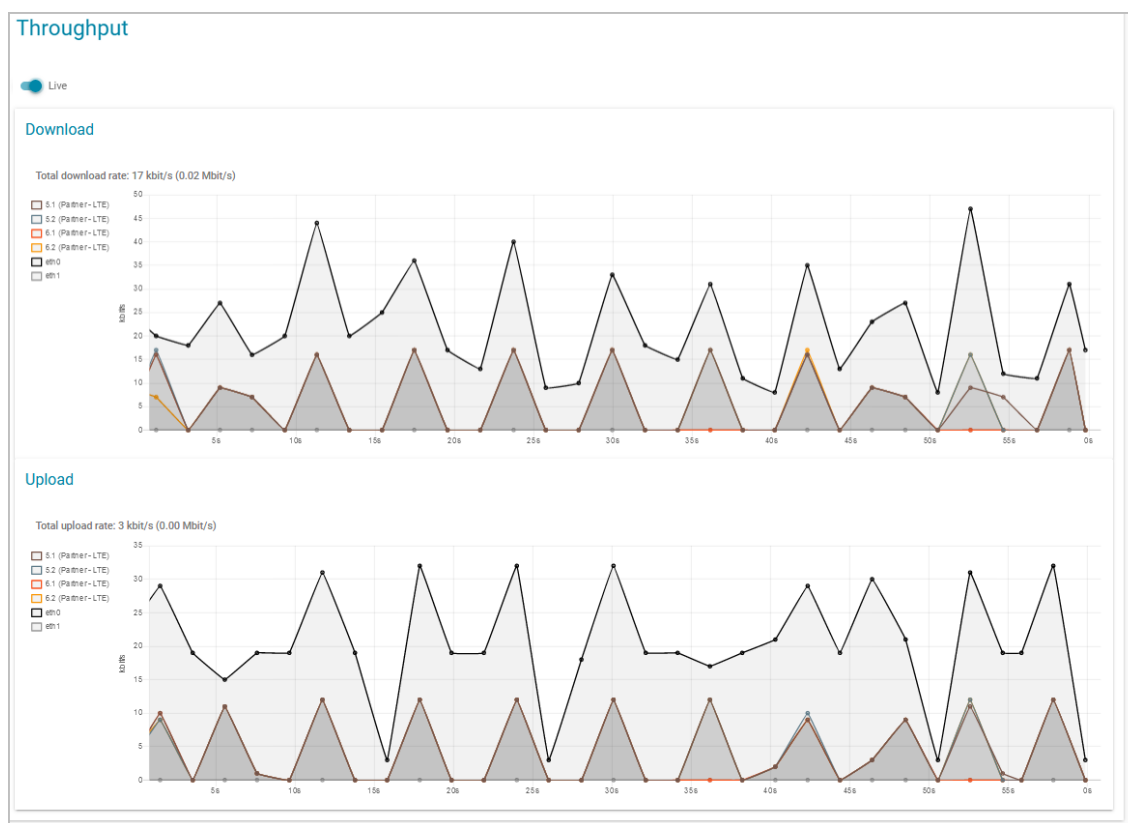
Priority 1 - Preferred			
⋮	cell1 (We4G)	Cellular	Error
⋮	cell2 (Pelephone)	Cellular	Error
⋮	cell3 (Pelephone)	Cellular	Error
⋮	cell4 (We4G)	Cellular	Dialing
Priority 2 - Hot backup			
⋮	wlan0	Wi-Fi	Up
Priority 3 - If there is no choice			
Priority 4 - Cold backup			
Priority 5 - Never use			
Note: Remote-ID and FOTA will not follow the priority and may use any of the active links			

NOTES:

- Links in priorities 1-4 are always available.
A link in priority 5 (Never use) will not be used unless moved to a higher priority, and then it might take some time to initialize the link.
 - A WAN link assigned to a low priority may not be used by the system. For cellular WAN links, this would be indicated by the corresponding LED on the front panel blinking blue.
 - Except for priority 5 links, even links that are not in use due to low priority consume a minimal amount of data in order to keep the VPN tunnel open.
 - As stated in the **Note**, priority is not applicable to Remote-ID and FOTA and therefore they may use any active link.
 - Although the same priority is applicable for upload and download, in actual use upload and download are independent, each direction according to its needs and capabilities.

For example; it is possible that at one point only priority 1 would be used for download and priorities 1, 2, and 3 for upload, but the use may vary within seconds in response to changes in the network.

Throughput



The NIC page displays the total download and upload rate **per second** for each NIC.

- You can view the graph live or freeze it ("**Live**" switch).
- The legend at the left explains the colors in the graph. You can hide any of the NICs as long as the display is live.
- You can hover on any point on the chart to display a tooltip showing rates for each NIC at this point in time.

Iptables Configuration

You can configure port forwarding on the Halo according to iptables rules that you specify.

The screenshot shows the 'Iptables' configuration interface. At the top right is a 'CURRENT IPTABLES' button with a red circle '1' next to it. Below is a table with columns 'Rules', 'Enabled', and 'Actions'. A single rule is listed: '-t nat -A PREROUTING -i eth1 -p icmp -j RETURN'. The 'Enabled' checkbox is unchecked, with a red circle '3' next to it. The 'Actions' column has edit and delete icons, with red circles '4' and '5' respectively. Below the table is a '+ ADD ANOTHER' button with a red circle '2' next to it. At the bottom right is an 'APPLY' button with a red circle '6' next to it.

1. Click to see the current Iptables configuration.

Current Iptables

```
# Generated by iptables-save v1.6.2 on Mon Jun 27 08:31:23 2022
*filter
:INPUT ACCEPT [308915:70660346]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [314337:88081868]
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i tun0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -j ACCEPT
COMMIT
# Completed on Mon Jun 27 08:31:23 2022
# Generated by iptables-save v1.6.2 on Mon Jun 27 08:31:23 2022
*nat
:PREROUTING ACCEPT [297:30798]
:INPUT ACCEPT [199:15051]
:OUTPUT ACCEPT [30989:1867571]
:POSTROUTING ACCEPT [31029:1869836]
-A POSTROUTING -o eth0 -j MASQUERADE
-A POSTROUTING -o tun0 -j MASQUERADE
COMMIT
# Completed on Mon Jun 27 08:31:23 2022
```

CLOSE

2. Click to add a new rule (see [Adding an iptables Rule.](#))
3. Check to enable the selected rule.
4. Click to edit the selected rule.
5. Click to delete the selected rule.
6. Click to apply changes. Changes will take effect after reboot.

Adding an iptables Rule

1. Click **Add Another**.

Add Rule

Rule Type

2

Enable

4

CANCEL
ADD

5

2. Select the rule type.

Add Rule

Rule Type

2

Enable

4

CANCEL

Rule Type

3

Description

NIC

Protocol

- Fill in the fields as they appear in the Rule Type dialog. Fields vary according to the selected rule type (see the table below).
- Toggle to enable the rule, if applicable.
- Click **ADD**.
- You can add multiple rules. When finished, click **Apply**.

Rule Type	Fields
Custom	Rule Text
Port Forward	- Description - NIC - Protocol - Destination IP - Forward IP
Masquerade	- Description - NIC
Return	- Description - NIC - Protocol

Port Forwarding via the API

You can also configure port forwarding via the API, using the 'PUT' command.

- Create a text file similar to the sample below, containing the iptables rules that you want to apply to port forwarding.

Sample iptables rules text file:

Rules to forward connections on port 91 of the gateway to the internal machine:

```
-A PREROUTING -t nat -i eth1 -p tcp --dport 91 -j DNAT --to 192.168.1.2:8080
-A FORWARD -p tcp -d 192.168.1.2 --dport 8080 -j ACCEPT
```

- Upload the file using the api.

```
PUT /api/v1/iptables_settings
```

- Restart the Halo device.

NOTE: The restart is required in order to load the rules from your rules file (uploaded in step 2) to iptables.

- Verify the rules:

```
GET /api/v1/iptables_settings
```

Returns all the active/existing rules in iptables as plain text .

sample response:

(Note that this is a random sample and is not correlated to the sample file in Step 1.)

```
iptables -t filter --append INPUT -j DROP
iptables -t filter -A INPUT -p udp -j DROP
iptables -t filter -A INPUT -s 192.168.1.230 -j ACCEPT
```


Using Specific NIC Pages

There are 4 types of NICs in the Halo device:

- Cellular NICs
- Ethernet NICs
- WiFi NICs
- VLAN NICs

Each of the specific NIC pages consists of the following sections the Ethernet NIC page is shown as a sample:

Ethernet Network Interface Controllers

Status

Device	Status	IP	Use as WAN	Built-in NIC	Enabled
 Eth 1	Up	20.0.0.2	☒	☒	
 Eth 2	Cable Unplugged	20.0.1.2	☐	☒	

Latest update at: 12/7/2021, 9:45:53 PM

Settings

Static Data

IP

20.0.0.2

Subnet

255.255.255.0

Gateway

0.0.0.0

DNS

☒ Use as WAN

+ ADD ADDRESS

DHCP State

None

CHOOSE WAN LINK

APPLY

Operations

Destination IP

Source IP

20.0.0.2

SEND PING

• Status

Displays a Status listing of all NICs of that type.

Click on one of the entries to display the settings and operations available for the specific NIC type.

• Settings

This section varies, depending on the NIC type:

- For Cellular Modem NICs you can configure [Network Limitations](#), [Operator Selection](#), and [Dialing Rules and APN](#).
- For Ethernet NICs you can configure IP [Settings](#), static IPs, dynamic IPs, DHCP.
- For WiFi NICs you can configure routing and security type [Settings](#).
- For VLAN NICs you can add interfaces to the VLAN and configure static data [Settings](#).

• Operations

This section allows you to perform operations such as pinging a selected destination IP.

Status

Status										
	Slot #	Alias	Model	Carrier	Signal	Net	Status	IP	Enabled	
☐	1	SIM 1	Telit LE910-EU V2	We4G		N/A	Dialing	N/A	☒	
☐	2	SIM 2	Telit LE910-EU V2	Pelephone		N/A	Searching	N/A	☒	
☐	3	SIM 3	Telit LE910-EU V2	Pelephone		N/A	Error	N/A	☒	
☐	4	SIM 4	Telit LE910-EU V2	We4G		N/A	Error	N/A	☒	

The **Status** listing appears at the top of the each specific NIC page and shows the status of all interfaces of that type.

- Click on any line to display the settings and **Operations** sections for the selected NIC.
- For the cellular modem and WiFi NICs, you can click to display **Further Information**.

Settings

Settings that apply to all or most NICs are explained below.

Configuring the DHCP State

You can configure the DHCP state for the following NIC types:

- Ethernet
- WiFi
- VLAN

Choose client or server role. Or if DHCP is not applicable, choose **None**.

Configuring a DHCP Client

(Optional) You can select a WAN link. (see [Configuring a WAN Link](#)).

DHCP State
Client

CHOOSE WAN LINK

APPLY

For a DHCP client, the WAN link options include the DHCP client dynamic link.

Define WAN link

Choose which link should act as WAN

☐ None

☐ 20.0.0.2

☒ DHCP client dynamic

CANCEL

UPDATE LINK

Configuring a DHCP Server

NOTE: Any change in server configuration requires a reboot of the device.

1. Fill in the identifying IP address pool information.

2. (Optional) You can select a WAN link (see [Configuring a WAN Link](#)).
3. (Optional) Depending on your network configuration, there may be specific additional DHCP options.

Click **+Add Option**. Select the option ID and enter the relevant IP addresses.
Hover over the **Options** field to see the option definition.

Configuring a WAN Link

You can configure one IP address per NIC to be used as the WAN link. The selected link will then be used as WAN for that NIC.

A WAN link can be configured for the following NIC types:

- Ethernet (One WAN link for each ETH NIC)
- WiFi
- VLAN

To configure the WAN link:

- Click **Choose WAN Link** to select the link

Select the link and click **Update Link**.

The **Use as WAN** checkbox in the listing will be checked and the link will appear in the **WAN Link Priority** table (see [WAN Prioritization](#)).

Assigning an Alias

The **Settings** section for all types of physical NICs allows you to assign a meaningful, descriptive name to the element to make it easier to identify.

You can also specify that the alias should appear only on the local Halo device and not be exposed to the AllSight Cloud Manager.

Alias (Optional)
NIC alias

☐ Use alias only on local device

Operations

Destination IP

Source IP
20.0.1.2

SEND PING

The available operations vary slightly depending on the NIC type. The following table summarizes available operations.

Restart	Restart the element	Cellular modem only
Send Ping	Ping specified destination IP	All NIC types, including VLAN

For all NICs, you can ping a specified IP address to test connectivity and verify that the card has internet access to the desired IP address.

To ping a specified IP:

- Enter the destination IP (the IP address of the NIC is displayed in the Source IP field) and click **Send Ping**.

If the test fails, check that the card is connected correctly. You may need to edit some of the parameters such as the dialing rules (cellular modem) or IP addresses (Ethernet).

Cellular NICs

The Halo platform may contain 2 to 4 embedded cellular modules.

This page lets you do the following:

- See the status of the cellular modules, including advanced RF data
- Configure the dialing rules
- Assign an alias
- Limit to a specific cellular technology and/or limit to a specific band, per technology
- Force a roaming SIM to a specific mobile network operator
- Enable, disable, or restart the NIC
- Ping a specified destination IP

Status

Cellular Network Interface Controllers

Status

	Slot #	Alias	Model	Carrier	Signal	Net	Status	IP	Enabled	
☐	1	SIM 1	Telit LE910-EU V2	We4G		N/A	Error	N/A	☒	
☒	2	SIM 2	Telit LE910-EU V2	Pelephone		N/A	Searching	N/A	☐	
☐	3	SIM 3	Telit LE910-EU V2	Pelephone		N/A	Error	N/A	☐	
☐	4	SIM 4	Telit LE910-EU V2	We4G		N/A	Error	N/A	☐	

Latest update at: 4/15/2024, 3:06:00 PM

SHOW ADVANCED RF DATA

SHOW

Further Information

IMEI:

Carrier FW version:

Modem FW version:

IMSI:

ICCID:

eID:

Cell ID:

LAC:

Network Reject Cause:

351622076676374

N/A

20.00.405

425030043222700

8997250400032227009

N/A

N/A

N/A

N/A

0

Dialing Rules

Optional Settings

Default

Username

pcl@3g

Password

Auth Mode

CHAP

APN

internet.pelephone.net.il

PDP Type

IP

APPLY

Alias (Optional)

SIM 2

☐ Use alias only on local device

APPLY

Limit to specific radio technologies

☐ Automatic

APPLY

Limit to specified radio technology

LTE

Limit to specific radio bands

☒ Automatic

APPLY

Operator Selection

☒ Automatic

APPLY

The **Signal** column tells you the signal-to-noise value, which is read from the relevant parameter below, depending on which specific technology is currently in use:

- 3G: RxQual
- LTE: RSRQ
- 5G: NR_RSRQ

The color of the Signal icon indicates the value. Refer to the following table.

Signal Icon Color	Signal to Noise Value
Green	≥ -10
Light Green	$-15 \leq \text{to} < -10$
Yellow	$-18 \leq \text{to} < -15$
Orange	< -18

- For the cellular NICs, you can click  to display **Further Information** including:

- IMEI
- Carrier firmware version
- Modem firmware version
- IMSI
- ICCID
- eID
- Cell ID
- LAC
- Network Reject Cause (Error code the network sends upon failure to connect. **Note** – there will be a code even if the modem connected successfully.)

- To display detailed live RF data for all cellular NICs, click **Show Advanced RF Data**.
- To hide the RF data, click **Close Advanced RF Data**.

Status										
	Slot #	Alias	Model	Carrier	Signal	Net	Status	IP	Enabled	
	1	SIM 1	Telit LE910-EU V2	We4G		N/A	Dialing	N/A		
	2	SIM 2	Telit LE910-EU V2	Pelephone		N/A	Error	N/A		
	3	SIM 3	Telit LE910-EU V2	Pelephone		N/A	Error	N/A		
	4	SIM 4	Telit LE910-EU V2	We4G		N/A	Error	N/A		
Latest update at: 1/25/2023, 2:20:05 PM										
 										
GNSS satellites detected: 0 Velocity: N/A Km/h Direction: N/A °										
	Slot #	Network Name	Rx level	Signal To Noise	Band	ARFCN Original	Cell Id	RSSI		
	1	We4G	-255	-255	-	65535	-	-		
	2	Pelephone	-100	-8	-	10738	-	-		
	3	Pelephone	-123	-16.5	-	1400	-	-		
	4	We4G	-115	-17	-	1825	-	-		

NOTE: In some hardware versions (geography dependent), if the technology is limited to 3G, the band is shown as "-1".

Recording RF Signals

The screenshot shows the 'Recording Settings' and 'Recordings' sections. In the 'Recording Settings' section, there are two toggle switches: 'Auto-record' (1) and 'Auto-backup' (2), both currently turned on. To their right, the 'GNSS status' is 'Not Locked' (3). Further right is a 'Time Period' field (4) set to 'minutes'. A 'START NEW RECORDING' button is on the far right. In the 'Recordings' section, there is a 'REFRESH' button (5). Below it is a table with three columns: '#', 'Start Time', 'End Time', and 'Backed up to Allsight'. The table contains three rows of recordings. Each row has a checkbox for 'Backed up to Allsight' (7), a trash icon (8), a 'DOWNLOAD CSV' button (6), and an 'ALLSIGHT BACKUP' button (7). At the bottom of the table, there are 'DELETE ALL' (8) and 'DOWNLOAD ALL' (6) buttons.

By default, the cellular reception indicators of the cellular links are recorded automatically, together with their timestamp and GNSS coordinates (if connected). Recording starts automatically once the GNSS lock is received. All existing recordings are then automatically uploaded to the AllSight cloud on device startup.

If there are recordings that have not been backed up to AllSight, there will be a message in the **Announcements** section of the **Home** dashboard.

Announcements

2 RF recordings not backed up to Allsight.

- The device can store up to 20 records of 1 hour each
- Records can also be downloaded manually from either the Halo or from the AllSight cloud (after backup) as a csv file
- The default automatic behavior can be disabled to allow you to manage RF recording manually
- AllSight's HeatSight functionality displays a map showing historical cellular reception data from these recordings, once they are backed up to AllSight. See the AllSight guide for details.

To manage recording sessions manually:

1. Click **Show Recording Settings**. (It toggles to **Close Recording Settings**.)
2. Toggle Auto-record and Auto-backup to 'Off'. (Automatic recording and automatic backup are independent, so you can disable only one or the other if desired.)
3. Click **Time Period** to set the number of minutes to record (1-60).
4. Click **Start New Recording**.

A **Stop Recording** button appears. You can click it to stop the recording before the configured time period is finished.

5. Click **Refresh** to see the recording in the listing if it does not appear.
6. You can download a selected recording (**Download CSV**) or all recordings (**Download All**).
7. You can back up a selected recording to AllSight.
 - A message appears confirming that the backup was successful
 - The **Backed up to AllSight** checkbox disappears.
 - In the **Announcements** section of the **Home** dashboard, the number of RF recordings that have not been backed up is decreased by 1.
8. You can delete a selected recording (🗑️) or all recordings (**Delete All**).
9. To hide the recording settings, click **Close Recording Settings**.

Dialing Rules and APN

Dialing Rules

Custom

Username

None

Password

Auth Mode

Auto

APN

apn_name

PDP Type

ip

APPLY

Dialing rules are provided by your carrier. The system has pre-defined dialing rules for many global carriers.

If your carrier is familiar, you will find its settings pre-defined. If there are no pre-defined rules for your carrier, manually configure them here.

- If the carrier is familiar, with pre-defined dialing rules, choose **Default** and click **Apply**. All other fields are unavailable.
- If the carrier is not familiar choose **Custom**. All other fields will then be available.

Configure the custom fields and click **Apply**.

- Username: can be a specific username or can be blank
- Password: required only if username is specified
- Authentication Mode (select from drop-down list)
- APN: enter the Access Point Name
- PDP Type: enter the protocol type

Optional Settings

Optional Settings

Alias (Optional)
SIM 1 ☐ Use alias only on local device **APPLY**

Limit to specific radio technologies
☒ Automatic **APPLY**

Limit to specific radio bands
☒ Automatic **APPLY**

Operator Selection
☒ Automatic **APPLY**

Network Limitations

These settings let you:

- Assign an alias
- Limit to a specific cellular technology
- Limit to a specific band
- Force a roaming SIM to a specific mobile network operator

Network Limitations

You can limit each modem NIC to a specific technology and/or a specific radio band.

NOTE: Band limitation is not currently supported for 5G modems.

- If you select a specific technology, the band must match the technology.
- If you specify only the bands or only the technology, then select '**Automatic**' for the parameter you are not limiting
- If you do not want to limit to one technology or one band, choose **Automatic** for both.

To specify a network technology or radio band:

1. Turn off the **Automatic** toggle.
2. Open the relevant drop-down list.
3. Select the desired option.
4. Click **Apply**.

Operator Selection

You can force a SIM to use a specific mobile network operator. Most often, this is set for a SIM with a roaming profile. We support three ways to define the operator manually. Access them by turning off the **Automatic** toggle.

- To specify the Mobile Country Code / Mobile Network Code, activate the **Custom MCC/MNC** toggle, enter the data, and click **Apply**. Multiple values can be entered.

- If only a single Custom MCC/MNC is defined, the definition will be applied very quickly, without any scan of available operators. Otherwise, a scan will take place, of all available operators to find a match between an available operator and a configured one. Priority is given to the operators defined as Custom MCC/MNC.
- To select a country and network, select the country and the operator, and click **Apply**.
Currently the following country options are available:
 - US
 - Israel
 - None (Operator selection not available)

- You may select predefined operators, that were previously added for the relevant locale. Click on the **Predefined Operator Name** tab, and then select the Area and Operator.

The screenshot shows the 'Operator Selection' interface. At the top, there is a checkbox labeled 'keep the settings persistent for this modem'. Below it is a toggle switch for 'Automatic'. A blue 'APPLY' button is in the top right corner. Under the heading 'Manually lock using', there are three tabs: 'MCC/MNC', 'PREDEFINED OPERATOR NAME' (which is selected and highlighted with a blue underline), and 'CUSTOM OPERATOR NAME'. Below the tabs, there are two dropdown menus: 'Area' and 'Operator'.

- You can also configure the operator manually, by selecting the **Custom Operator Name** tab. Activate the **Long Format Operator Name** toggle and then enter the name as published by the carrier, or deactivate the toggle and enter the operator's short format name.

This screenshot shows the 'Operator Selection' interface with the 'CUSTOM OPERATOR NAME' tab selected and highlighted with a blue underline. The 'Long Format Operator Name' toggle switch is turned on (blue). Below the toggle is a text input field labeled 'Manual Operator Name'. The 'APPLY' button remains in the top right corner.

- If you select the checkbox **Keep the settings persistent for this modem**, the settings will remain unchanged, even if you replace the SIM card.

Ethernet NICs

The Ethernet interfaces can be used either for management of the device or to carry data. You can select a WAN link to use the selected Ethernet interface as connectivity to the internet (or external network) (see [Settings](#) below).

This page lets you do the following:

- See the status of the Ethernet modules

The **Built-in** column indicates whether the NIC is built-in to the Halo device or external.

- Configure routing settings
- Enable or disable the card
- Ping a specified destination IP

Settings

Ethernet Network Interface Controllers

Status

	Device	Alias	Status	IP	WAN link	Speed	Built-in NIC	Enabled
☐	Eth 1	Eth 1	Cable Unplugged	20.0.0.2	☐	10 Mbps	☒	☐
☒	Eth 2	Eth 2	Up	20.0.1.2	☐	1000 Mbps	☒	☒

Latest update at: 4/15/2024, 3:16:15 PM

Settings

Alias (Optional)
Eth 2 ☐ Use alias only on local device

Connection mode and speed
Auto negotiation

Static Data

IP	Subnet	Gateway	DNS
20.0.1.2	255.255.255.0	0.0.0.0	

+ ADD ADDRESS

DHCP State
None

CHOOSE WAN LINK APPLY

This section is a listing of all currently configured IP addresses for the selected interface, as well as the DHCP configuration.

You can:

- Assign an alias.
- Select the connection mode and speed.
- Add a new IP address:

Click **Add Address** and enter the IP address, subnet, gateway and DNS.

- Delete an IP address:

Click the  icon at the end of the row.

- Configure **DHCP**:

See [Configuring the DHCP State](#).

- Configure a WAN link:

See [Configuring a WAN Link](#).

- After making any of these changes, click **Apply** for the change to take effect.

Ethernet NIC Added to VLAN

When an Ethernet NIC has been added to a VLAN, you cannot change the settings.

Ethernet Network Interface Controllers						
Status						
	Device	Status	IP	Use as WAN	Built-in NIC	Enabled
	Eth 1	Added to VLAN	vlan0	☒	☒	☒
	Eth 2	Up		☒	☒	☒

Remove Eth 1 from the VLAN in order to change the settings.

WiFi NICs

This page lets you do the following:

- See the status of the WiFi modules

The **Built-in** column indicates whether the NIC is built-in to the Halo device or external.

- Configure access such as routing information and security type
- Enable or disable the WiFi card
- Ping a specified destination IP
- Click  to display **Further Information**.

Settings

WiFi Network Interface Controllers

Status

	Device	Alias	SSID	Role	Status	IP	Signal	Built-in NIC	WAN link	Enabled	
	wlan0	tamar	tamar	Station	Up	10.100.102.48, 20.0...		☒	☒	☒	

Latest update at: 11/23/2022, 6:58:56 PM

Settings

Alias (Optional)

tamar

Configuration

* Any change requires a reboot of the device

State

Access Point

SSID

tamar

☐ Hide SSID

Security Type

WPA

Encryption Key

Frequency Band

2.4GHz

Frequency Channel

1 (2412 MHz)

+ ADD CONFIGURATION

Static Data

IP

20.0.2.2

Subnet

255.255.255.0

Gateway

0.0.0.0

DNS

+ ADD ADDRESS

DHCP State

Server

DHCP Server

* Any change requires a reboot of the device

IP

Subnet

Gateway

DNS

Starting IP

Ending IP

Options

+ ADD OPTION

CHOOSE WAN LINK

APPLY

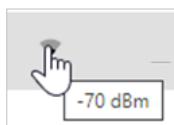
This section is a listing of all currently configured IP addresses for the selected interface, as well as the security and DHCP configurations.

You can:

- Assign an alias.
- If you set an Access Point:
 - You can select a **Frequency Band** of either 2.4GHz or 5GHz and also select a specific **Frequency Channel**.
 - You can also hide the SSID so that it will not appear on a scan for WiFi networks.

NOTE: Any change in access point configuration requires a reboot of the device.

- If the NIC role is Station, you can:
 - Select the network from a listing of available networks by clicking **Available Networks**. See [Adding a Configuration](#).
 - Hover over the signal icon in the listing to display the signal strength.



- Add a new IP address:

Click **Add Address** and enter the IP address, subnet, gateway and DNS.

- Delete an IP address:

Click the  icon at the end of the row.

- Add a new security configuration (Station mode only):

See [Adding a Configuration](#).

- Delete a configuration:

Click the  icon at the end of the row.

- Configure **DHCP**

See [Configuring the DHCP State](#).

- Configure a WAN link:

See [Configuring a WAN Link](#).

- After making any of these changes, click **Apply** for the change to take effect.

Adding a Configuration

When the Role is set to **Station**, you can have multiple configurations.

1. Click **Add Configuration**.

Configuration

Role: Station | SSID: [AVAILABLE NETWORKS]

Security Type: None

+ ADD CONFIGURATION

Static Data

IP: 20.0.2.2 | Subnet: 255.255.255.0 | Gateway: 0.0.0.0 | DNS: []

+ ADD ADDRESS

DHCP State: None

CHOOSE WAN LINK | APPLY

2. Fill in the fields, including selecting a network.
3. Click **Apply**.
4. Reboot the device to make the changes.

WiFi NIC Added to VLAN

When a WiFi NIC has been added to a VLAN, not all of the settings options are relevant and therefore, only the relevant options remain available.

WiFi Network Interface Controllers

Status

Device	Status	State	SSID	IP	Signal	Built-in NIC	Use as WAN	Enabled
wlan0	Added to VLAN	Access Point	Yoav_Halo	vlan0	[Signal Icon]	[X]	[X]	[Toggle On]

Latest update at: 2/28/2022, 3:12:29 PM

Settings

Configuration * Any change requires a reboot of the device

State: Access Point | SSID: Yoav_Halo | [] Hide SSID

Security Type: WPA | Encryption Key: []

Frequency Band: 2.4GHz | Frequency Channel: 6 (2437 MHz)

+ ADD CONFIGURATION

APPLY

- The WiFi NIC must be an access point. It cannot be a station.
- You cannot add additional configurations.
- Static Data configuration is not available.
- DHCP configuration is not available.

VLAN NICs

To bridge ports, you can define a VLAN and can add Ethernet and/or WiFi NICs to it. An interface that has been added to a VLAN displays the VLAN name in the relevant NIC listing in the IP address column. Click on the VLAN name in the listing to open the corresponding VLAN information in the VLAN NIC page.

WiFi Network Interface Controllers

Device	Status	State	SSID	IP	Signal	Built-in	Use as WAN
wlan0	Added to VLAN	N/A		vlan0		☒	☐

Latest update at: 10/22/2020, 1:20:52 PM

VLAN Network Interface Controllers

Device	Status	IP	Use as WAN
vlan0	Down	20.0.0.5	☐

Latest update at: 11/28/2021, 4:56:17 AM

This page lets you do the following:

- Configure a VLAN interface, defining the static data and the DHCP state. You can add Ethernet and or WiFi NICs to the VLAN.
- Ping a specified destination IP
- To delete a VLAN, click the  icon at the end of the row.

Settings

VLAN Network Interface Controllers

Device	Status	IP	Use as WAN	Add VPNs to VLAN	Actions
vlan0	Down	20.0.0.5	☐	☐	

Latest update at: 11/28/2021, 4:24:58 AM

Settings

Display Name: vlan0 VLAN NICs: ▼ ☐ Add VPNs to VLAN

Static Data

IP	Subnet	Gateway	DNS
20.0.0.5	255.255.255.0	0.0.0.0	

[+ ADD ADDRESS](#)

DHCP State: None ▼

[CHOOSE WAN LINK](#) [APPLY](#)

This section displays the VLAN ID and associated interfaces, as well as a listing of all currently configured IP addresses for the selected VLAN and the DHCP configuration.

You can:

- Edit the name of the VLAN.
- Add or remove NICs to/from the VLAN:

Open the VLAN NICs listing and select/deselect the desired NICs.



- Check the **Add VPNs to VLAN** option to add the VPNs to the VLAN.

The **Actions** checkbox in the listing will be checked.

- Add a new IP address:

Click **Add Address** and enter the IP address, subnet, gateway and DNS.

- Delete an IP address:

Click the  icon at the end of the row.

- Configure **DHCP**

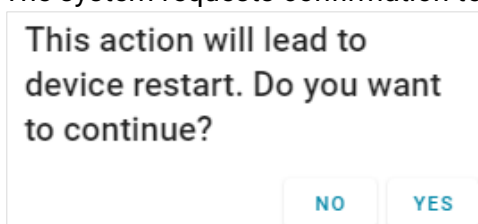
See [Configuring the DHCP State](#).

- Configure a WAN link:

See [Configuring a WAN Link](#).

- After making any of these changes, click **Apply** for the change to take effect.

The system requests confirmation to restart.



Click **Yes**.

SatCom

To support SatCom communication, a designated SatCom modem can be connected to the Halo.

Choose SatCom from the main menu, to define the communication settings.

First, use the toggle switch to enable SatCom communication.

Define the connection type (typically USB) and Baud Rate.

Define the number of seconds that pass without communication with AllSight, that will be considered a loss of connectivity. By default, this is set to 5 seconds. Setting a value of 0 disables this periodic message.

After clicking on Apply, if the modem is properly connected and identified, the following data will be displayed:

- Satcom State
- Satcom Network
- Satcom Model
- Satcom IMEI (International Mobile Equipment Identity)

Messages sent by this modem can be seen in the AllSight Messaging Log.

Send a Message

Use a POST /API/v1/satcom/message request to send a message via satellite. Sending can take up to 15 minutes due to satellite availability and network conditions. Only one message can be sent at a time.

Data Path

Application rules together with the VPN profiles define the data path.

Application rules define the connectivity configuration, specifying the overall network topology, hub, and related hosts. It can include a user-defined VPN profile as part of the connectivity definition. Application rules are created and managed in the AllSight Cloud platform (see the **AllSight Cloud Platform User Guide**).

A VPN profile contains the authentication information required for an OpenVPN connection. It contains the following:

- CA certificate file
- File containing the client key and the client certificate
- OVPN configuration file

All tunnel VPN profiles used by the application rules that are applicable to this Halo device are also inherited from the AllSight Cloud Manager and are identified in the application rules descriptions.

There are 2 VPN profile types:

- Tunnel VPN

Tunnel VPN profiles are created and managed in the AllSight Cloud platform (see the **AllSight Cloud Platform User Guide**). They can then be used in application rules.

There are 2 tunnel VPN profile modes:

- Automatic: The customer is using the ElSight VPN service
- Private Certificate Service: The customer is using a private VPN service
 - Direct VPN

Direct VPNs are for peer-to-peer mode between 2 devices that use both RF and dynamic IP. They are created and managed in the relevant Halo devices.

NOTE: When you use an OpenVPN profile with Layer 2 configuration selected, it is recommended to define a bridge between the ETH1 interface and the VPN NICs (see [VLAN NICs](#).)

The Data Path page has 2 sections:

- Application Rules: A listing of all application rules applicable to this Halo device, inherited from the AllSight Cloud Manager.
- VPN Profiles: Configure the Halo to use private VPN.

In addition, customers working in peer-to-peer mode can create tunnel VPN profiles.

Application Rules

Total: 1

Search

Application Rule Name	Aggregation Server Address	AR Data Ports Range	Control Port	Redundancy	Reorder Buffer	Related Devices	Device Role	VPN Profile Name	VPN Enabled	VPN Server Port	VPN Server Address	Config
L3 Secure Network with Internet Access	555.100.222.444		10001	0	20	Device 100	Client	L3_VPN	☒	1311	100.66.0.1	Config

VPN Profiles

Use Private VPN

Show Peer-to-peer Mode

Application Rules

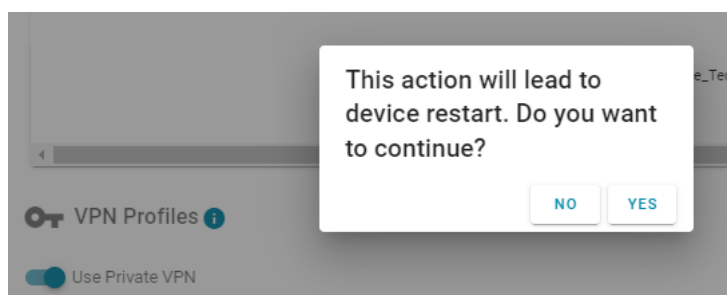
Any application rules applicable to a specific Halo device are inherited by that device from the AllSight Cloud Manager and listed here.

Relevant VPN profiles are identified in the 'VPN Profile Name' column of the application rules listing.

VPN Profiles

By default, automatic VPN is assumed.

- To use a private VPN, toggle **Use Private VPN** to select private VPNs and confirm device restart.



Adding a Direct-VPN profile

You must configure a direct VPN separately for each side of each link.

The screenshot shows the 'Add Direct-VPN' form within the 'Direct-VPN Profiles' section. The form is titled 'Add Direct-VPN' and has a 'Total:0' indicator. It includes a 'Module Name' dropdown, a 'Profile Name' text field, an 'Automatic Activate' checkbox, a 'Server Port' text field, a 'VPN IP' text field, and three file upload fields for 'CA Certificate', 'Client Certificate', and 'Client Key'. Below these is a 'Configuration Source' dropdown set to 'Standard'. Further down are dropdowns for 'Encryption Type' (Blowfish), 'Compression Type' (LZO), and 'Layer Type' (Layer 3). At the bottom are 'CANCEL' and 'ADD' buttons. Red numbered callouts (1-9) point to specific elements: 1. 'Hide Peer-to-peer Mode' toggle, 2. 'Profile Name' field, 3. 'Automatic Activate' checkbox, 4. 'Module Name' dropdown, 5. 'Server Port' field, 6. 'VPN IP' field, 7. The file upload fields for certificates and keys, 8. 'Configuration Source' dropdown, and 9. 'ADD' button.

1. Toggle **Show Peer-to-peer Mode** to show the Direct VPN profiles.
2. Enter a valid name for the profile. (Alphanumeric characters only, no spaces.)
3. **Automatic Activate**: Check if this OpenVPN should be activated
4. Select the cellular modem NIC.
5. Enter the server port
6. Enter the VPN IP
7. Browse to import the required client or server certificate and key files.
8. Define the configuration source:
 - For a **Custom** configuration source:
 - Browse to import the OVPN configuration file.
 - NOTE**: The OVPN configuration file **MUST** be syntactically valid in conformation with the guidelines in the [OpenVPN Reference Manual](#).
 - For a **Standard** configuration source:
 - Define the following:
 - Encryption type
 - Compression type
 - Layer type
9. Click **Add**

Services

Use this module to configure the following:

- MAVLink: The Halo supports 2 uses of the MAVLink protocol:
 - MAVLink Forward: for communicating between selected sources and destinations
 - MAVLink Service: lets the Halo access selected data
- Remote ID: Customers who purchased the Remote ID can enable and configure it here.

MAVLink

MAVLink is a protocol for communicating with and controlling UAVs. It is generally used to link the drone flight computer to the control center and transmit commands between the HQ and the drone. It can be used to transmit the orientation of the vehicle, its GNSS coordinates, and speed.

The Halo supports 2 MAVLink options. You can use either one independently or use both options.

MAVLink Forward

MAVLink forward allows the Halo to transmit MAVLink commands between selected source(s) and selected destination(s). The Halo passively transmits and does not actually read any data.

You must specify at least one source and one destination. Multiple sources and destinations are supported, depending on the physical connections.

You can connect your control center to your drone via any of the following:

- UART cable
- USB cable
- UDP listening

MAVLink Service

MAVLink service lets the Halo read data transmitted by the protocol. To use the MAVLink service with your Halo device, you must define at least one source; destinations are not required. You must also specify exactly which parameters to read.

To configure MAVLink:

The screenshot shows the MAVLink configuration page. At the top left, the 'MAVLink' toggle switch is turned on (1). Below it, the 'Sources (Mandatory)' section (2) has 'Source type' with 'UART via Halo UART' selected. Under 'UART via Halo UART configurations', the 'Baud Rate' dropdown menu is open (3), showing options: 9600, 19200, 38400, 57600, and 115200. To the right, the 'Destinations for MAVLink Forward (Optional)' section (2) has 'Destination type' with three options: 'UART via Halo UART', 'UART via Halo USB', and 'UDP Targets'. At the bottom left, the 'MAVLink Service' section has 'Read from MAVLink' with checkboxes for 'GNSS coordinates and timestamp', 'Heading and Velocity', 'Roll, Pitch, Yaw' (5), 'Aircraft ID and status', and 'Battery Status'. At the bottom right, there are two 'APPLY' buttons (4 and 6) for the sources and destinations sections respectively.

1. In **Services>MAVLink**, toggle **MAVLink** to ON.

2. Select the sources and destinations as follows:

- If using MAVLink forward, select both source(s) and destination(s)
- If using MAVLink service *only*, select only source(s)

You can configure multiple sources and destinations.

When you select a source(s) only permitted destinations will be available to select.

3. Configure the data fields that appear:

- UART via UART or via USB: Baud rate. It must be the same as for the device that the Halo is communicating with.
- UDP Listeners/Targets: IP address and port that the Halo is communicating with.

You can configure multiple listeners or targets.

The screenshot shows the 'UDP Listener configurations' section. It contains two input fields: 'Listening IP' and 'Listening Port'. Below these fields is a blue link that says '+ Add another UDP Listener'.

4. Click **Apply**.

5. If using MAVLink service: In the MAVLink Service section '**Read from MAVLink**', select the data to read from MAVLink.

6. Click **Apply**.

Remote-ID

The Halo supports remote ID transmission, including velocity and aircraft status, if available, according to the regulations requirement via broadcasting (in accordance with FAA part 89 requirements, sub-part D) and/or over the network. The data contained in the form is transmitted once a second.

- Aircraft status is sourced from MAVLink or via the API and transmitted.

For details on how to set up MAVLink (see [MAVLink](#)).

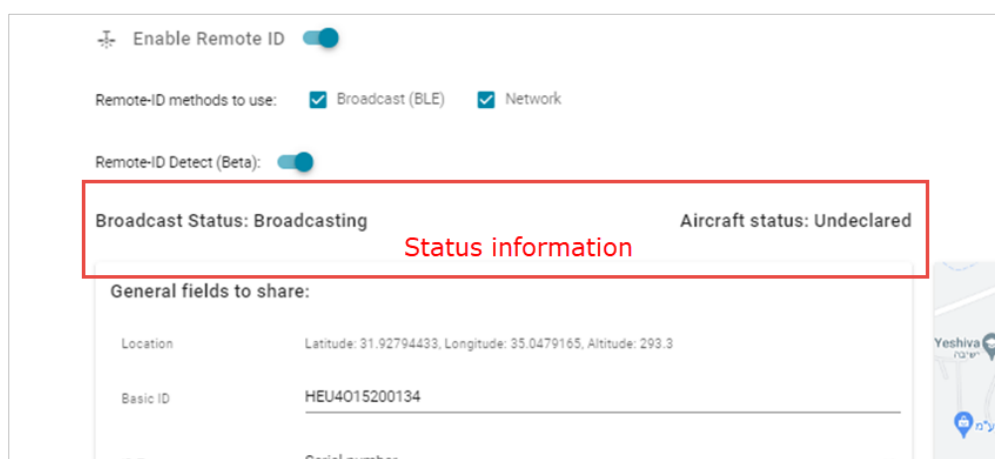
- Velocity is reported in meters per second.

Remote ID Status

- The current status of Remote-ID broadcast, as well as the aircraft status, is displayed in the Remote-ID status information.
- Remote-ID status is also always displayed in the Home dashboard.

The Remote ID states are:

- Broadcasting
- Malfunction: Malfunction may be due to
 - No GPS lock
 - BLE cannot transmit for any reason
- Off, Disabled



Detecting Other Remote ID Devices

The Remote ID feature can detect other Remote ID devices nearby. Any detected Remote ID devices are displayed in a listing at the bottom of the Remote ID page (9 in the graphic below). Note that information may be updated in chunks, resulting at times in partially filled rows that will be completed as more information arrives.

You can enable this feature as part of the overall Remote ID feature, working in conjunction with the Halo Remote ID broadcasting capabilities, or by itself as a standalone feature.

To use the Remote ID device detection as a standalone capability, simply enable Remote ID and then enable **Remote-ID Detect** (see Step 3 [below](#)).

Configuring Remote ID

The screenshot shows the 'Remote ID' configuration page. It includes a 'FREE TRIAL' badge in the top right. The interface is divided into several sections:

- Enable Remote ID:** A toggle switch (1) is set to 'ON'.
- Remote-ID methods to use:** Two options are shown: 'Broadcast (BLE)' (2) and 'Network' (checked).
- Remote-ID Detect (Beta):** A toggle switch (3) is set to 'ON'.
- Broadcast Status:** Shows 'Broadcasting'.
- Aircraft status:** Shows 'Undeclared'.
- General fields to share:** (4) A section with input fields for Location (Latitude: 31.92794433, Longitude: 35.0479165, Altitude: 293.3), Basic ID (HEU4015200134), ID Type (Serial number), UA Type (Other), Self-ID (toggle), and Operator ID (toggle).
- Network Settings:**
 - UTM settings:** (5) Includes a dropdown for UTM (Custom Elsight) and a text field for UTM url (https://example.com/rid).
 - GNSS status:** Locked.
 - UAS Location:** Latitude: 31.927944, Longitude: 35.047916, Altitude: 293.3.
 - Control station location method:** Take off coordinates (6).
 - Control station location:** Latitude: 31.927927, Longitude: 35.047845, Altitude: 277.5.
 - RESET LOCATION & APPLY:** A button (7).
 - Last updated:** 4/18/2023, 3:41:22 PM.
- Other Remote-ID Devices:** (9) A table with columns: MAC Address, Basic ID, Coordinate, and Altitude. It currently shows 'No data available'.

Numbered callouts 1 through 9 are placed over the interface elements described above.

To configure remote ID:

1. In **Services>Remote-ID**, toggle **Enable Remote ID** to ON.
2. Select the method(s) to use.
3. To identify and display a listing of other remote ID devices, toggle **Remote-ID Detect** to ON.

The Other Remote-ID Devices listing is displayed at the bottom of the page (9).

4. Identify the fields to share.
Fields with toggle buttons are optional.
5. (For Network) Select the desired USSP/UTM from the list.
If UTM type 'Custom Elsight' is selected, the **UTM url** field becomes active so you can enter the custom URL.
6. Select the control station location method:
 - **Take off coordinates:** Coordinates will update automatically once GNSS is locked.
If this option has already been selected at startup, the device will automatically use the coordinates captured once GNSS is locked without any action on the part of the user.
 - **Fixed coordinates:** Manually enter latitude, longitude, and altitude, or click **Use Current Location** to fill in the current device coordinates automatically.

7. Click **Reset Location & Apply** (Take off coordinates) or **Apply** (Fixed coordinates) to update the control station location:
 - Control station location coordinates are updated
 - Device is located in the map
 - Broadcast begins and Broadcast Status is changed to '**Broadcasting**'
8. Click **Apply**.

Users

Use this module to add and edit users.

User Permission Levels

Each user is assigned a permission level. There are 4 user permission levels:

- Basic: mostly read-only and no access to user configuration
- Technician: device configuration and access to their own user information
- Manager: can do everything except:
 - Edit or delete other users
 - Factory reset
- Device Admin (only 1 per device): can do everything including managing other users and factory reset. Since Managers and Device Admin can edit their own user configuration, the Device Admin can also change the admin username and password.

See [Appendix B: User Access Level Permissions](#) for the specific permissions for each level.

Users		
ADD USER 1		
Total: 2		Search
Username	Permission Level	Actions
admin	Device Admin	
user1	Basic	2 3

This page lets you do the following:

1. Add a new user
2. Edit the selected user
3. Delete the selected user. (You cannot delete the device administrator.)

Editing a User

Edit User

Username
admin

Password

Permission Level

Basic
Technician
Manager

CANCEL

SAVE

1. Click the Edit icon .
2. Make desired changes in the username and password dialog.
3. Set the permission level.
4. Click **Save**.

NOTE: Changes to an existing user only take effect the next time the user logs in. Changes will not affect a user who is currently logged in to the device.

Adding a User

1. Click **Add User**.
2. In the **Add User** dialog, enter the username and a strong password.
3. Select the permission level.
4. Click **Add**.

Add User

Username

Password

Permission Level

Basic
Technician
Manager

CANCEL

ADD

Maintenance

Use this module to the following:

- Upgrade the device firmware.
- Configure the realm and associate the device to an environment.
- Shut down the device.
- Reboot the device.
- Download the OpenVPN log
- Reset the device to factory defaults.
- Disable the device LEDs.

Serial

HEU4015200134

Firmware

Running Version

Version: 11.5.0.1

Base Package: 0.14.0-11.1-search64

Core Package: 2.20.0.1-11.5.0

Web Package: 1.23.0.0-11.5.0

Installed Version

Version: 11.5.0.1

Base Package: 0.14.0-11.1-search64

Core Package: 2.20.0.1-11.5.0

Web Package: 1.23.0.0-11.5.0

SHUTDOWN REBOOT

Choose File No file chosen

UPDATE

Realm

☒ Elsight Cloud ☐ On-Premises

SETUP

Environment

Associated environment: Tech-Tav

Environment name

ASSOCIATE

Logs

OpenVPN Log

DOWNLOAD

Factory Reset

RESET

Serial Number

The serial number is assigned as part of the manufacturing process. Each Halo device is given a serial number in the factory, which is associated with the unique hardware details of the unit.

Firmware

You can see both the running firmware version and the installed version. The difference between running and installed version is related to the automated upgrade process.

- Installed version: When you install a new firmware version, that version appears as the installed version. However, it is not yet running.
- Running version: Upon the next successful restart, the system firmware updates to the latest installed version, which is now also the running version.

You can also shut down or reboot the device.

Firmware Upgrade

Elsight will notify you when a firmware upgrade is available. Halo firmware as well as the modem firmware can be upgraded using the process detailed below. Halo firmware is comprised of multiple components, including base, web and core. If any component is not upgraded successfully, a warning message will be displayed. In that case, retry the upgrade or contact Elsieht Support.

To upgrade your firmware:

1. Use the link provided by Elsieht and download the firmware upgrade file to a location on your local system.
2. In the Halo Web GUI, in the Firmware section of the Maintenance tab, click **Choose File** to locate and select the firmware version file.
3. Click **Update**.



A progress bar will keep you informed on the current state of the upgrade. After the upgrade is completed successfully, the new firmware version will appear as the *installed* firmware version and a **REBOOT TO UPGRADE** reminder will appear at the top of the page.

4. Reboot the device.

The new firmware version will be displayed as the *running* firmware version.

5. The progress bar will display information on errors or failures, so that you can retry the upgrade as needed.



Realm

A realm is the location where the total AllSight cloud is installed, including all services under the cloud.

To assign the device to a realm:

1. Select the realm according to your cloud configuration.

For an on-premises realm:

- (a) Enter at least one enrollment service IP address or URL. Press **Enter** after each entry.
- (b) Click in the **Realm CA** field to browse to and attach the certificate.

2. Click **Setup**.

Environment

An environment is a defined group of users who have access to the environment as well as all devices associated with the environment.

The environment **MUST** be defined via the AllSight Cloud Platform (unless the device is on-premises) and the device **MUST** be associated to that environment using the proper device serial number as displayed above (see the [AllSight Cloud Platform User Guide](#)). In addition, you **MUST** associate the device with the relevant environment here from the Maintenance page.

To associate the device with an environment:

1. Define both the environment and the device in the AllSight Cloud Platform or on-premises (see the [AllSight Cloud Platform User Guide](#)).
2. Make sure to enter the environment name exactly as it is defined in the Cloud Platform; the name is case-sensitive.
3. Click **Associate**.

Logs

Click **Download** to download the OpenVPN log to a selected location.

Not relevant for the server side.

Factory Reset

Click **Reset** to reset the Halo device to factory defaults. All configured settings, including IP addresses will be lost.

Hardware

This setting lets you turn the device LEDs off or on.

Hardware Settings

LED State

DISABLE

ENABLE

Advanced

Use this module to do the following:

- Configure tunnel settings. You can manually configure specific IP addresses for any interface.

Tunnel Settings

This module lets you work in Point-2-Point mode, in a non-star topology.

- Enabled: P2P mode - You can assign a specific IP address (modem) to each interface.
- Disabled: Work with a server

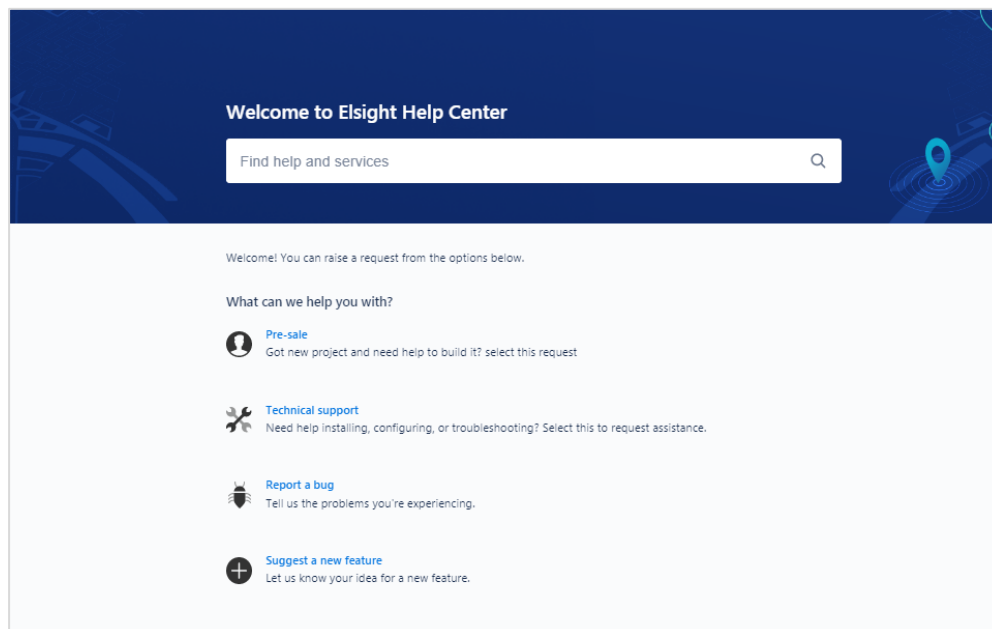
Working in P2P Mode

1. In **Advanced>Tunnel Settings** click **Add**.
2. Select the module number or interface name and enter the IP address.

3. Click **Apply**.
4. Click **Enable**.

The Elsight Help Center

The Elsight Help Center is a 24/7 support portal for submitting questions and issues to the Elsight support team.



Requests are divided into 4 categories, from the planning stage to suggestions for improvements you would like to see implemented:

- **Pre-sale:** For help in designing and building a new project.
- **Technical support:** For help in installing, configuring, or troubleshooting an existing project.
- **Report a Bug:** To report a problem that we need to fix.
- **Suggest a new feature:** To tell us when you have an idea that would improve your user experience.

Accessing the Help Center

There are 2 ways to access to the Help Center:

- Via the Elsight website:

Click **Support**.

- Via the following direct link:
<https://elsight.atlassian.net/servicedesk/customer/portals>.

Submitting a Request

1. Gather all relevant supporting material such as log files, messages, or screenshots. Anything you think will help us to understand the issue.
2. Log in to the center.
3. Choose the relevant category.

Elsight Support

Welcome! You can raise a request from the options below.

What can we help you with?



Pre-sale

Got new project and need help to build it? select this request

Priority

Medium

Summary *

Description

Attachment

Drag and drop files, paste screenshots, or browse

Browse

Share with *

Share with Test

Send Cancel

4. Fill out the form:

- Indicate what the priority level is
- (Required) Summarize the main points
- Explain the issue in more detail.
- (Required) Can we share this information?

5. Attach supporting material.

6. Hit **SEND**.

Response time will depend on the priority level you indicated as well as your specific SLA package.

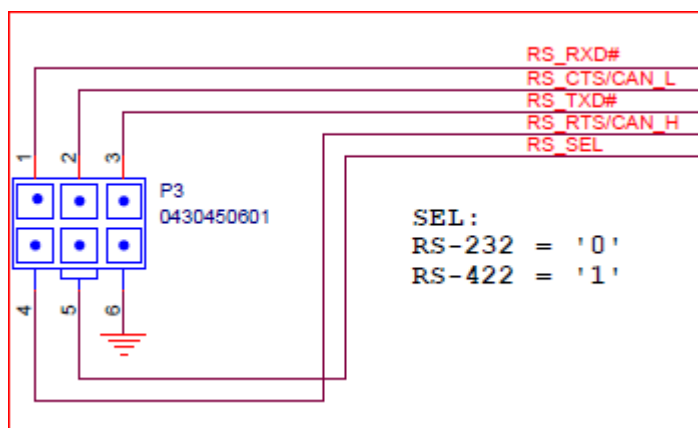
Appendix A: Connectors Description

This appendix describes pinouts for the following connectors located on *The Halo BondBox Back Panel*.

- CAN bus
- Power

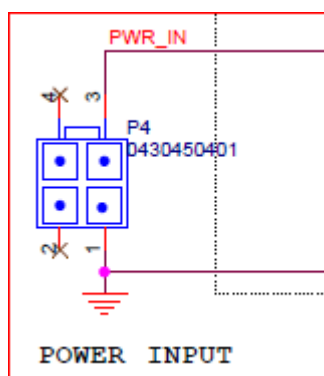


CAN Bus



PIN Number	Description
1	RS_RXD#1
2	RS_CTS/CAN_L
3	RS_TXD#1
4	RS_RTS/CAN_H
5	RS_SEL
6	Ground

Power In Connector



PIN Number	Description
1	Ground
3	DC in (12 v)

Appendix B: User Access Level Permissions

As described above in [User Permission Levels](#), there are 4 user permission levels. The specific permissions for each level are listed in the following table.

Module	Operation	Basic	Technician	Manager	Device Admin
NICs Management					
	Status	TRUE	TRUE	TRUE	TRUE
	View real-time NICs usages update (graph)	TRUE	TRUE	TRUE	TRUE
	WAN links priority view	TRUE	TRUE	TRUE	TRUE
	WAN links priority	FALSE	FALSE	TRUE	TRUE
	IPTables view	TRUE	TRUE	TRUE	TRUE
	IPTables edit	FALSE	FALSE	TRUE	TRUE
Cellular NIC					
	Disable/enable	FALSE	TRUE	TRUE	TRUE
	Dialing rules	FALSE	TRUE	TRUE	TRUE
	Network limitations view	TRUE	TRUE	TRUE	TRUE
	Network limitations edit	FALSE	TRUE	TRUE	TRUE
	Operator selection view	TRUE	TRUE	TRUE	TRUE
	Operator selection edit	TRUE	TRUE	TRUE	TRUE
	Operations restart	FALSE	TRUE	TRUE	TRUE
	Operations ping	TRUE	TRUE	TRUE	TRUE
	Show advanced RF data	TRUE	TRUE	TRUE	TRUE
	Backup recordings	TRUE	TRUE	TRUE	TRUE
	Show recording settings view	TRUE	TRUE	TRUE	TRUE
	Show recording settings edit	FALSE	TRUE	TRUE	TRUE
Ethernet NIC					
	Settings	FALSE	TRUE	TRUE	TRUE
	Disable/enable	FALSE	TRUE	TRUE	TRUE
	Ping	TRUE	TRUE	TRUE	TRUE
WiFi NIC					
	Settings	FALSE	TRUE	TRUE	TRUE
	Disable/enable	FALSE	TRUE	TRUE	TRUE
	Ping	TRUE	TRUE	TRUE	TRUE
VLAN NIC					
	Settings	FALSE	TRUE	TRUE	TRUE
	Delete VLAN	FALSE	TRUE	TRUE	TRUE
	Add new VLAN	FALSE	TRUE	TRUE	TRUE
	Ping	TRUE	TRUE	TRUE	TRUE

Module	Operation	Basic	Technician	Manager	Device Admin
Data Path					
	View	TRUE	TRUE	TRUE	TRUE
	Delete	FALSE	TRUE	TRUE	TRUE
	Update	FALSE	TRUE	TRUE	TRUE
	Private VPN and Edit/delete	FALSE	FALSE	TRUE	TRUE
Services MAVLink					
	Enable/configure	FALSE	FALSE	TRUE	TRUE
	View	TRUE	TRUE	TRUE	TRUE
Services Remote-ID					
	Enable/configure	FALSE	FALSE	TRUE	TRUE
	View	TRUE	TRUE	TRUE	TRUE
Users					
	Edit/delete other users	FALSE	FALSE	FALSE	TRUE
	Edit self password and username	FALSE	FALSE	TRUE	TRUE
	Edit self password	FALSE	TRUE	TRUE	TRUE
	View all	FALSE	FALSE	TRUE	TRUE
	View self	TRUE	TRUE	TRUE	TRUE
	Add new users	FALSE	FALSE	TRUE	TRUE
Maintenance					
	Factory reset	FALSE	FALSE	FALSE	TRUE
	Realm setup	FALSE	FALSE	TRUE	TRUE
	Environment associate	FALSE	FALSE	TRUE	TRUE
	Shutdown	FALSE	TRUE	TRUE	TRUE
	Reboot	TRUE	TRUE	TRUE	TRUE
	Firmware Upgrade	FALSE	FALSE	TRUE	TRUE
	View versions	TRUE	TRUE	TRUE	TRUE
	Serial	TRUE	TRUE	TRUE	TRUE
	View realm	TRUE	TRUE	TRUE	TRUE
	View environment	TRUE	TRUE	TRUE	TRUE
Maintenance Hardware					
	LED state update	TRUE	TRUE	TRUE	TRUE
	LED state view	TRUE	TRUE	TRUE	TRUE
Advanced Tunnel					
	Update	FALSE	TRUE	TRUE	TRUE
	View	TRUE	TRUE	TRUE	TRUE
Logout					
	Logout	TRUE	TRUE	TRUE	TRUE
API Only					
	External GNSS	FALSE	FALSE	TRUE	TRUE
Diagnostics					
	Test LEDs	TRUE	TRUE	TRUE	TRUE

Appendix C: Cellular NIC RF Recording Data

The following tables provide information regarding the Cellular NIC RF recording data.

Note that for certain parameters, the various technologies have fields that are similar, but not exactly the same and with different field names. The Halo API wraps these fields under one field name. For example, **rx_level** is RSCP (on 3G) / RSRP (on LTE) / NR_RSRP (on 5G). Refer to the 'Comments' column.

Cellular NIC RF Recording Fields

Field Name	Source	Value / API	Units	Comments
Date	GNSS/MAVLINK		Days	
Time (UTC)	GNSS/MAVLINK		Seconds	Invalid, No Value, or Unknown: 0xFFFF
Longitude	GNSS/MAVLINK	GPS_RAW_INT::lat/lon	degree, WGS84, EGM96 ellipsoid	No Value, or Unknown: 0 deg
Latitude	GNSS/MAVLINK	GPS_RAW_INT::lat/lon	degree, WGS84, EGM96 ellipsoid	No Value, or Unknown: 0 deg
Altitude	GNSS/MAVLINK	RAW_INT::alt	MSL, meters (converted from mm)	Invalid, No Value, or Unknown: -1000m
Satellites	GNSS/MAVLINK	GPS_RAW_INT::satellites_visible	Integer	
GNSS Source	Halo device		Integer	7. Built-in GNSS 8. Other 9. MAVLink 10. Flask API 11. High Precision API 12. External Serial
Velocity	GNSS/MAVLINK	Sqrt (GLOBAL_POSITION_INT::vx **2 + GLOBAL_POSITION_INT::vy **2)	m/s (converted from cm/s)	- From halo-v11.4. x: m/s - Versions older than Halo-v11.4.0: km/h - Positive only. - Invalid, No Value, or Unknown: 255m/s.
Direction	GNSS/MAVLINK	GLOBAL_POSITION_INT::hdg	cdeg, Vehicle heading	Invalid, No Value, or Unknown: 361deg

Field Name	Source	Value / API	Units	Comments
			(yaw angle), 0.0..359.99 degrees (x100)	
Roll	MAVLINK	ATTITUDE::roll/pitch/yaw	Rad	
Pitch	MAVLINK	ATTITUDE::roll/pitch/yaw	Rad	
Yaw	MAVLINK	ATTITUDE::roll/pitch/yaw	Rad	
Battery Status	MAVLINK		%	Maximum of 100%
Network name	Modems	Carrier	Text	All the rest of the fields are repeated for each SIM card.
Alias	User input (optional)	User input (optional)	Text	Alternative SIM name
Cellular generation	Modems	2G/3G/LTE/5G-SA/ 5G-NSA	Text	
Tx kbps	Modems		Kb/s	
Rx kbps	Modems		Kb/s	
LAC/TAC	Modems		Text	
Rx level	Modems * see Comments	Value depends on technology in use: • 3G: RSCP • LTE: RSRP • 5G: NR_RSRP	dBm	See RSRP - RX Level for signal quality ratings
Signal-to-noise	Modems * see Comments	Value depends on technology in use: • 3G: RxQual • LTE: RSRQ • 5G: NR_RSRQ	dB	See SNR – Signal to Noise for signal quality ratings
Band number	Modems		Integer	
Band frequency	Modems		MHz	
ARFCN original	Modems		MHz	Absolute radio-frequency channel number is the channel number: • ARFCN • EARFCN • UARFCN • NR_CH
Cell ID	Modems		Alpha numeric ID	Cell tower ID

Field Name	Source	Value / API	Units	Comments
RSSI	Modems		dBm	See RSSI for signal quality ratings.
Raw data	Modems		text	

Cellular NIC Signal Quality

The following tables explain the Cellular NIC signal quality ratings for the various specific parameters (depending on the technology).

Note that the value of the RSRQ parameter determines the color of the 'Signal' icon, as shown in the **SNR** table.

RSRP - RX Level

Average power received from a single reference signal. Typical range: -44dbm (good) to -140dbm (poor)

RSRP	Signal strength	Description
>= -80 dBm	Excellent	Strong signal from the base station with maximum data speeds
-80 dBm to -90 dBm	Good	Strong signal with good data speeds
-90 dBm to -100 dBm	Fair to poor	Reliable data speeds may be attained, but marginal data with drop-outs is possible. When this value gets close to -100, performance will drop drastically
<= -100 dBm	No signal	Disconnection

SNR – Signal to Noise

RSRQ: quality of the received signal. Typical range: -19.5dB (poor) to -3dB (good).

RSRQ	Quality	Description
≥ -10 dB	Excellent	Strong signal relative to interfering neighboring base stations, enabling maximum data capacity
-10 dB to -15dB	Good	Good signal and speeds with no dropouts expected
-15 dB to -20 dB	Fair to poor	Fair/usable signal with possibility of dropouts and slowdowns
≤ -20 dB	Unusable	No usable signal - expect frequent disconnections and sluggish performance

RSSI

Total received power including:

- power received from the serving cell
- all cochannel power
- other sources of noise

It's relationship to above parameters is expressed in the following formula:

$$RSRQ=N*(RSRP/RSSI)$$

Where N is the number of resource blocks of the E-UTRA carrier RSSI measurement bandwidth.

RSSI	Signal strength	Description
>= -65 dBm	Excellent	Strong signal with maximum data speeds
-65 dBm to -75 dBm	Good	Strong signal with good data speeds
-75 dBm to -85 dBm	Fair	Fair but useful. Fast and reliable data speeds may be attained, but marginal data with drop-outs is possible
-85 dBm to -95 dBm	Poor	Performance will drop drastically
<= -95 dBm	No signal	Disconnection

SINR

Signal to interference and noise ratio

SINR	Signal strength	Description
>= 20 dB	Excellent	Strong signal with maximum data speeds
13 dB to 20 dB	Good	Strong signal with good data speeds
0 dB to 13 dB	Fair to poor	Reliable data speeds may be attained, but marginal data with drop-outs is possible. When this value gets close to -0, performance will drop drastically
<= 0 dB	No signal	Disconnection