

ELSIGHT HALO USER GUIDE

Standalone Version

REVISION 1.1

JUNE 22, 2020

SW VERSION 1.3.6-1.5

ELS User Manual – Copyright and Disclaimer

Copyright

Copyright © 2020 Elsite 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 Elsite 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: www.elsight.com. All products should be installed and used in accordance to 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 Elsite Ltd or its suppliers for any errors or omissions. All brands and logos are registered trademarks and are subject to copyright laws.

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 B Warnings

The FCC Wants You to Know:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- a) Reorient or relocate the receiving antenna.
- b) Increase the separation between the equipment and receiver.
- c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- d) Consult the dealer or an experienced radio/TV technician.

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

Introduction.....	4
Elsight Halo Communication Platform	4
System Flow	5
Hardware Overview.....	6
The Halo Front Panel	6
The Halo Back Panel	7
The Elsight Halo Web GUI	8
Logging in to the Halo Web GUI	9
NICs (Network Interface Controllers).....	10
Status.....	10
Operations.....	11
Speed.....	12
Cellular Modem NICs.....	12
Status.....	13
Network Limitations	13
Dialing Rules	13
Ethernet NICs	14
Settings.....	14
WiFi NICs	15
Settings.....	15
Applications.....	17
OpenVPN Application.....	17
Maintenance	19
Serial Number.....	19
Firmware	19
Realm.....	20
Environment.....	20
Appendix: Connectors Description.....	21
CAN Bus	21
Power In Connector.....	22

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.

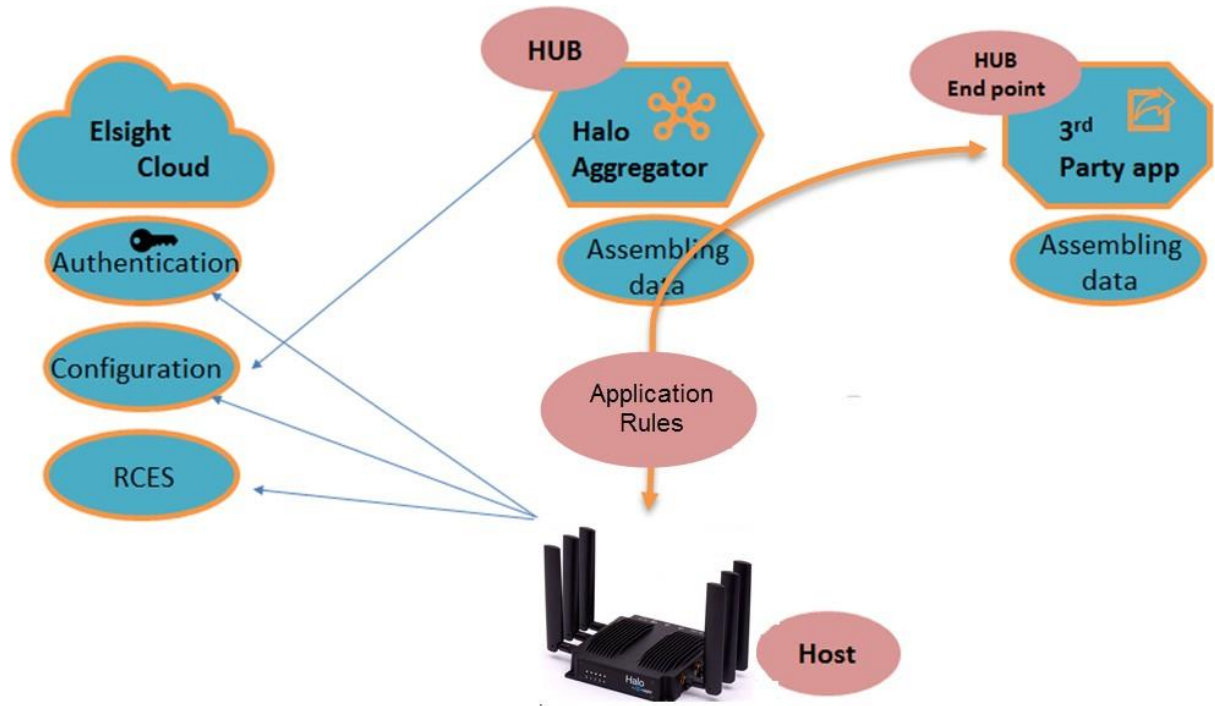


The Halo communication platform is available in 2 form factors:

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

System Flow

The Elsieht system flow is illustrated in the diagram below.



The system falls into 3 basic zones:

- Elsieht Cloud and Halo host devices:

The Elsieht 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. (See [OpenVPN Application](#).)

The application rules, which are configured via the Cloud Platform, define the functionality and relationships of all 3 zones. (See the [eiiGsr UoPr fllEP diolC t gisIE](#) for more information.)

Hardware Overview

This section describes the Halo interfaces and LEDs.

The Halo 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	Cannot recognize SIM card
Green	Connected to the cellular network
Blue	Connected to the aggregator
Blinking Green-Red	Requires custom dialing rules

- LED **'S'**: System status LED

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

State	Description
Red	Boot
Green	Connected to the VPN
Blue	Connected to the aggregator
Blinking Blue-Red	Dialing

The Halo 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 1
3	ETH 2
4	USB 2.0
5	DC IN (9-30V)

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 3 modules:

- **NICs (Network Interface Controllers)**

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

- Cellular Modem NICs
- Ethernet NICs
- WiFi NICs

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.

- **Application**

This module centralizes all the device applications:







- OpenVPN application
 - Define VPN profiles.




- **Maintenance**

Through 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.

The following table explains the main menu icons:

	Home
	NICs
	Cellular Modem NICs
	Ethernet NICs
	WiFi NICs
	Applications

	OpenVPN
	Maintenance
	Logout

Logging in to the Halo Web GUI

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

1. Connect the unit to a computer via one of the Ethernet ports and turn the unit on.
2. Open a web browser and enter the relevant IP address 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](#)).

3. Enter your user name and password and click Login

The default values are:

- Username: admin
- Password: admin

NICs (Network Interface Controllers)

Use this module to configure and manage the device NICs.

There are 3 types of NICs in the Halo device:

- Cellular Modem NICs
- Ethernet NICs
- WiFi NICs

The main NIC page displays monitoring and statistics graphs regarding each NIC network usage, such as the [Speed](#) graph.

Each of the specific NIC pages consists of the following sections:

- **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](#) and [Dialing Rules](#).
- For Ethernet NICs you can configure IP [Settings](#).
- For WiFi NICs you can configure routing and security type [Settings](#).

- **Operations**


This section allows you to perform operations such as enabling or disabling the NIC and pinging a selected destination IP.

Status

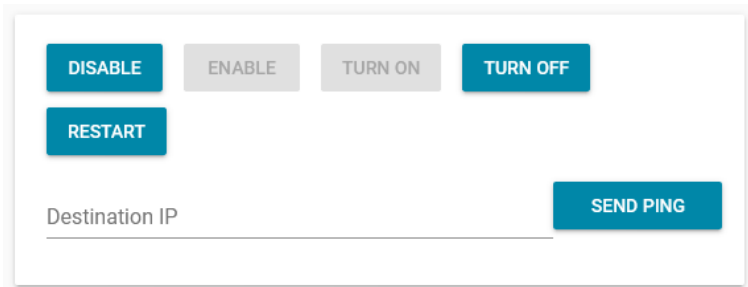
Status							
	#	Model	Carrier	Signal	Net	Status / IP	
<input type="radio"/>	5.1	Telit LE910C4-EU	Partner	▲	LTE	192.168.225.7	i
<input type="radio"/>	5.2	Telit LE910C4-EU	Partner	▲	LTE	192.168.225.8	i
<input checked="" type="radio"/>	6.1	Telit LE910C4-EU	Partner	▲	LTE	192.168.225.5	i
<input type="radio"/>	6.2	Telit LE910C4-EU	Partner	▲	LTE	192.168.225.6	i
Latest update at: 12/5/2019, 3:52:42 AM							

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

Operations



The screenshot shows a control panel with the following elements:

- A row of four buttons: **DISABLE** (blue), **ENABLE** (grey), **TURN ON** (grey), and **TURN OFF** (blue).
- A **RESTART** button (blue) below the first row.
- A text input field labeled "Destination IP" with a blue **SEND PING** button to its right.

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

Enable	Enable the element.	All NIC types
Disable	Disable the element.	All NIC types
Turn On	Turn on the element (must be enabled).	Cellular modem only
Turn Off	Turn off the element.	Cellular modem only
Restart	Restart the element (must be enabled).	Cellular modem only
Send Ping	Ping specified destination IP	All NIC types

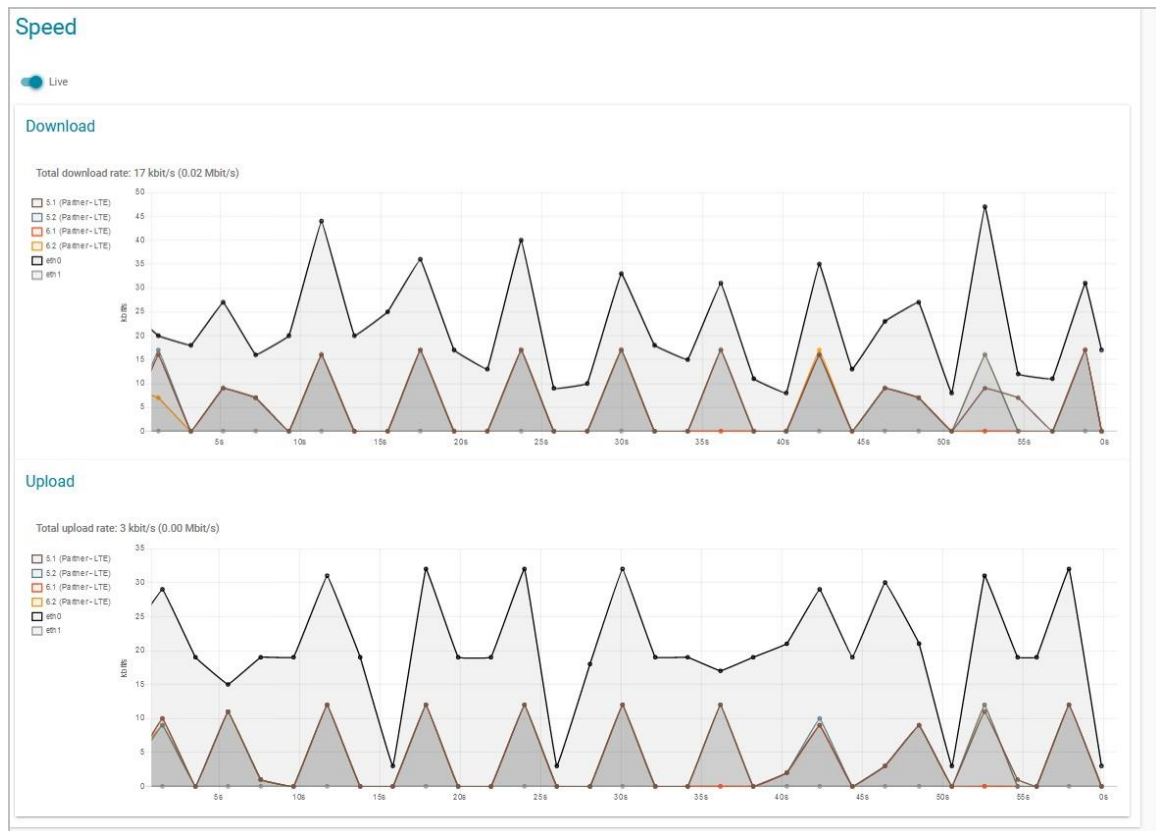
For all NICs, you can ping a specified IP address to test connectivity and verify that the card has internet access to the desired IP address.

To ping a specified IP:

- Enter the destination IP 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).

Speed



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.












Cellular Modem NICs

The Halo platform may contain either 2 or 4 embedded cellular modules.

This page lets you do the following:

- See the status of the cellular modules
- Configure the dialing rules
- Turn on and off or enable/disable
- Ping a specified destination IP

Status

Status							
	#	Model	Carrier	Signal	Net	Status / IP	
	5.1	Telit LE910C4-EU	Partner		LTE	192.168.225.7	
	5.2	Telit LE910C4-EU	Partner		LTE	192.168.225.8	
	6.1	Telit LE910C4-EU	Partner		LTE	192.168.225.5	
	6.2	Telit LE910C4-EU	Partner		LTE	192.168.225.6	

Latest update at: 12/5/2019, 3:56:52 AM


Further Information

Cell ID: 259E03

LAC: 5660

IMSI: 425010900326080

Raw Network Information
N/A RAW INFO

- For the cellular modem NICs, you can click  to display **Further Information**.

Network Limitations

You can limit each modem e C to a specific technology.

If you do not want to limit to one technology, choose **elbasID**.

Dialing Rules

Custom ▼

Username
None

Password
••••

Auth Mode
Auto ▼

APN
uinternet

Dial Number
*99#

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 rules and click **Apply**.

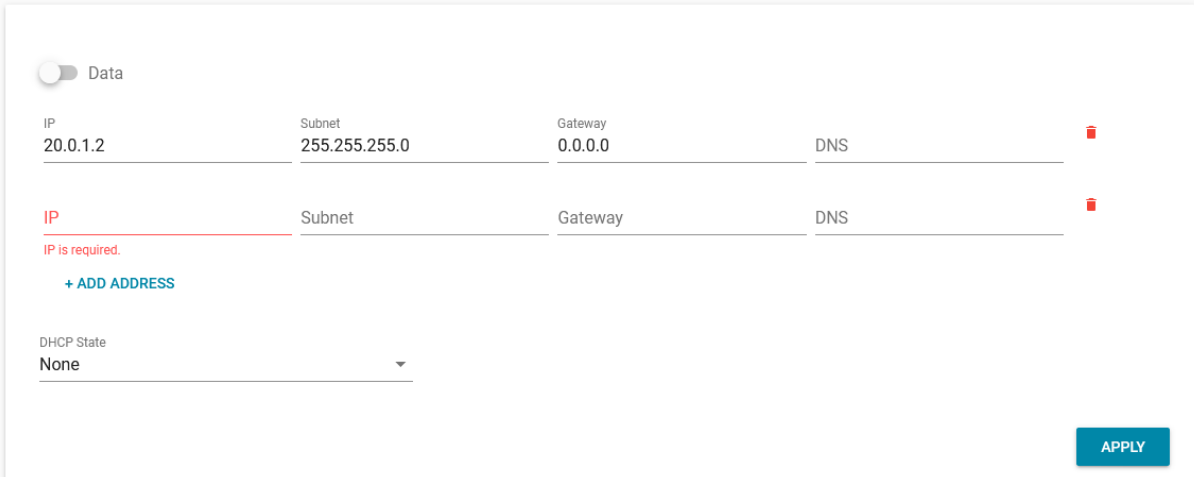
Ethernet NICs

In most cases, Ethernet interfaces are used for management of the device. However, you can use the **eaaa** switch to use the selected Ethernet interface to carry data (see [Settings](#) below).

This page lets you do the following:

- See the status of the Ethernet modules
- Configure routing settings
- Enable or disable the card
- Ping a specified destination IP


Settings



This section is a listing of all currently configured IP addresses.

You can:

- Switch the **Data** option to use this interface to carry data (rather than as a management interface).
- 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**:
Choose client or server role. Or if DHCP is not applicable, choose **None**.
- After making any of these changes, click **Apply** for the change to take effect.




WiFi NICs

This page lets you do the following:

- See the status of the WiFi modules
- Configure access such as routing information and security type.
- Enable or disable the WiFi card
- Ping a specified destination IP

Settings

Status

	Device	Status	State	SSID	IP	Signal	Built-in	Data	
	wlan0	Down	N/A				<input checked="" type="checkbox"/>	<input type="checkbox"/>	


Latest update at: 12/18/2019, 12:17:12 PM

Settings

☐ Data

☒ Built-in

Static Data

IP	Subnet	Gateway	DNS	
20.0.2.2	255.255.255.0	0.0.0.0		

+ ADD ADDRESS

Configuration

+ ADD CONFIGURATION



DHCP State

None

APPLY

This section is a listing of all currently configured WiFi NICs.

You can:

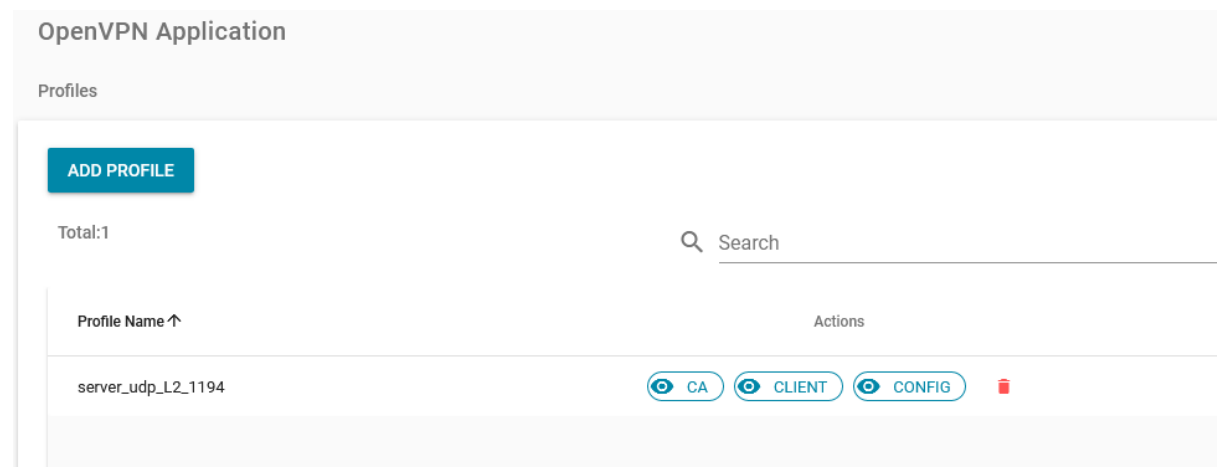
- Switch the **Data** option to use this interface to carry data (rather than as a management interface).
- Add a new IP address:
Click **Add Address** and enter the IP address, subnet, gateway and DNS.
- Delete an IP address:
Click the  icon at the end of the row.
- Add a new configuration:
Click **Add Configuration** and enter the security type and state.
- Delete a configuration:
Click the  icon at the end of the row.
- Configure **DHCP**:
Choose client or server role. Or if DHCP is not applicable, choose **None**.
- After making any of these changes, click **Apply** for the change to take effect.

Applications

Use this module to configure the OpenVPN application.

NOTE: When you create an OpenVPN profile with Layer 2 configuration selected, the system creates a bridge between the ETH0 interface and the VPN NICs.

OpenVPN Application



The screenshot shows the 'OpenVPN Application' interface. At the top, there's a header 'OpenVPN Application' and a sub-header 'Profiles'. Below this, there's a blue button labeled 'ADD PROFILE'. Underneath, it says 'Total:1'. To the right of this is a search bar with a magnifying glass icon and the word 'Search'. Below the search bar is a table. The table has two columns: 'Profile Name ↑' and 'Actions'. There is one row in the table with the profile name 'server_udp_L2_1194'. In the 'Actions' column for this profile, there are three buttons: 'CA', 'CLIENT', and 'CONFIG', each with an eye icon. To the right of these buttons is a red trash can icon.

The authentication information required for an OpenVPN connection is contained in a profile. The profile contains the following:

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

Click on a file button  to display the contents of the file.

When a hub or host endpoint is a VPN, you must specify the VPN profile in the relevant application rule (see the [diolC t gis/E eiitGgre UoPr f//EP](#)). A profile **MUST** also be created here on the device **BEFORE** it can be used in an application rule.

- Make sure that the profile name is *exactly* the same here and in the relevant application rule. The profile name is case sensitive.
- It does not matter which is created first, the profile here or the profile name in the application rule in the Cloud Platform configuration.

To add an OpenVPN profile:

Add OpenVPN Profile

Profile Name

CA Certificate

Client Certificate

Client Key

Configuration Source

Standard

Encryption Type

Blowfish

Compression Type

LZO

Layer Type

Layer 2

CANCEL

ADD

1. Enter a valid name for the profile. (Alphanumeric characters only, no spaces.)
2. Browse to import the required certificate and key files.
3. 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
4. Click **Add**.

Maintenance

Serial

Z26709NCJ3UCN

Firmware

Running Version

Base Package: 0.0.0

Core Package: 1.0.1.0

Web Package: 1.0.0.0

Installed Version

Base Package: 0.0.0

Core Package: 1.0.1.0

Web Package: 1.0.0.0

SHUTDOWN
REBOOT

Browse... No file selected.

UPDATE

Realm

☒ Elsight Cloud
☐ On-Premises

SETUP

Environment

Associated environment:

Environment name

ASSOCIATE

Use this module to the following:

- Manage the device firmware version.
- Configure the realm and environment.
- Shut down the device.
- Reboot the device.

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.

To install a new firmware version:

1. Browse to find and select the firmware version file.
2. Click **Update**.

Realm

including all services under the cloud, Elsiht cloud is installed total is the location where the m realm

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 **T**SUM be defined via the Elsiht Cloud Platform and the device **T**SUM be associated to that environment using the proper device serial number as displayed above (see the [Elsight Cloud Platform User Guide](#)). In addition, you **T**SUM 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 Elsiht Cloud Platform (see the [Elsight 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**.

Appendix: Connectors Description

This appendix describes pinouts for the following connectors located on *The Halo 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
2	DC in (12 v)