Service Kit

Installation and Set-Up Guide

Helvar's data driven Service Kit enables sending of data from a lighting system to a cloud platform where authorised users can access it through a REST API or a web browser interface.

The package also provides an encrypted VPN connection for remote Designer software assistance to ensure optimal lighting system performance with very little downtime.

Helvar's Service Kit consists of the following products:

1. Helvar Cloud Gateway (HCG), a small-form-factor computer that uploads the data from the lighting system to Helvar's Cloud Platform via Ethernet or Wi-Fi.
2. TOSIBOX® Lock 100, a small-form-factor computer that provides an encrypted VPN connection to a lighting site's router systems for remote Designer software assistance.
3. TOSIBOX® Key 200, the cryptoprocessing device that establishes the VPN connection between the PC running Designer software and the TOSIBOX® Lock 100.

Helvar Cloud Gateway

TOSIBOX® Lock 100

TOSIBOX® Key 200

Online FAQs: https://helvarsupport.zendesk.com/hc/en-us

Contents

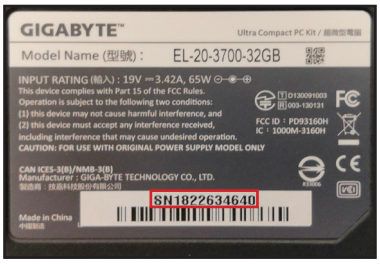
1. Prerequisites and Considerations....2
2. Overview....2
3. DIN-Rail spacing requirements....3
4. Install the Helvar Cloud Gateway....3
   - 4.1 Mount the PSU on the DIN rail....4
   - 4.2 Mount the Helvar Cloud Gateway on the DIN rail....4
   - 4.3 Connect the PSU, the Ethernet cable for the router network, and the Ethernet internet cable and/or Wi-Fi antennas....7
5. HCG Security and Network Configuration....8
   - 5.1 Internet Connectivity....8
   - 5.2 Helvar Cloud Platform....8
   - 5.3 Remote Assistance....8
   - 5.4 Local Connectivity....8
   - 5.5 Controller Admin Tool....9
   - 5.6 Hardware and OS....9
   - 5.7 Summary....9
6. Configure the router network and the workgroup....10
7. Account and Site creation....11
8. Install the TOSIBOX® Lock 100....12
   - 8.1. Mount the PSU on the DIN rail....12
   - 8.2. Mount the TOSIBOX® Lock 100 on the DIN rail....13
   - 8.3. If required, connect the Wi-Fi antennas....13
   - 8.4. Connect the PSU....13
9. Serialise the TOSIBOX® Key 200....13
10. Set up the IP address of the VPN adapter....14
11 Set up the IP address of the TOSIBOX® Lock 100....15
12. Connect the TOSIBOX® Lock 100 to the internet....16
13. Connect the lighting router network to the TOSIBOX® Key 200....18
14. Test the VPN connection....18
15. Technical data....19
    - 15.1 HCG....19
    - 15.2 TOSIBOX® Lock 100....20
    - 15.3 TOSIBOX® Key 200....20
16. System diagram....20

1. Prerequisites and Considerations

Prior to installing and setting up the Helvar Cloud Gateway (HCG) please ensure the following have been taken into consideration:

- HCG kit location - Has been discussed and finalised. Are there any cabling restrictions for the installation?
- Internet Connection - Has the client's IT department confirmed if it is it Ethernet or WiFi?
- Ethernet Cables - Ensure the client has the required number available on-site.
- Router information required:
    i) Workgroup name.
    ii) A free IP address within the same range as the router
    iii) What is the subnet mask?
    iv) What is the broadcast address?
- Firewall - Is it compliant with our requirements? ***Note:*** *Please read section 5 "HCG Security and Network Configuration"* of this document prior to any HCG installation.
- Can Dynamic Host Configuration Protocol (DHPC) be used? If not then:
    i) Confirmation of the allocated IP address is required.
    ii) A default gateway must be specified and manually updated. Contact Helvar Technical Support for assistance.
- Located on the rear of the HCG, above the barcode, is the unique ten digit serial number (highlighted in the picture, right). Ensure this number and the name of the site having the installation/set up are sent to Helvar support (global.tier.support@helvar.com).
  Upon receipt Helvar support will complete the registration, please allow **24 hours** for this process to happen.

  Note: *Make sure the serial number of the HCG is easily obtainable during the installation/set up process as it is required when activating a new Gateway.*



2. Overview

Follow these steps to install and set up Helvar's Service Kit package:

1. Install the Helvar Cloud Gateway. For details, see section 4 on page 3.
2. How to configure HCG Security and Network, page 8
3. Configuring the router network and the workgroup. For details, see section 6 on page 10.
4. Site and account creation, see section 7 on page 11.
5. Install the TOSIBOX® Lock 100. For details, see section 8 on page 12
6. Serialise the TOSIBOX® Key 200. For details, see section 9 on page 13.
7. Set up the IP address of the VPN adapter. For details, see section 10 on page 14.
8. Set up the IP address of the TOSIBOX® Lock 100. For details, see section 11 on page 15.
9. Connect the TOSIBOX® Lock 100 to the internet. For details, see section 12 on page 16.
10. Connect the lighting router network to the TOSIBOX® Key 200. For details, see section 13 on page 18.
11. Testing the VPN connection can be found in section 14, page 18.
12. All technical data is located in section 15, page 19
13. A system diagram is located in section 16, page 20

3. DIN-Rail spacing requirements

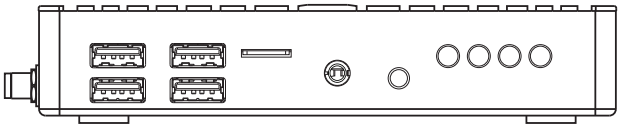
KIT				Dimensions			
Kit Description	Starter	Next Site	Site Expansion	(L / W / D) mm	Unit size	Note	Antenna incl.
HCG	✓	✓	✓	108 / 140 / 28	8	*	W 180 mm
TOSIBOX® Lock 100	✓	✓		99 / 132 / 35	8	*	W 165 mm
TOSIBOX® Key 200	✓			78 / 21.5 / 9	4	**	
PSU 12 V 30 W (HCG)	✓	✓	✓	90 / 35 / 58	2		
PSU 24 V 10 W (TOSIBOX® Lock 100)	✓	✓		91 / 18 / 57	1		

* *If Wi-Fi is used, place the units in such a way that interference between antennas is minimised. Do not place them in close proximity.*

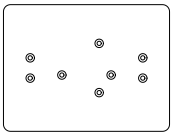
** *The TOSIBOX® Key 200 is a USB device that requires temporary connection to the TOSIBOX® Lock 100 during setup only. It does not require permanent DIR-Rail space.*

4. Install the Helvar Cloud Gateway

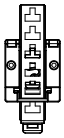
Package contents (HCG1TBLK KIT, HCG1TBL KIT and HCG1 KIT)



Helvar Cloud Gateway



DIN-rail mounting plate



DIN-rail mounting clip

HDR-30-12 PSU

DC feed plug

Wi-Fi antenna

Antenna extension with magnetic base

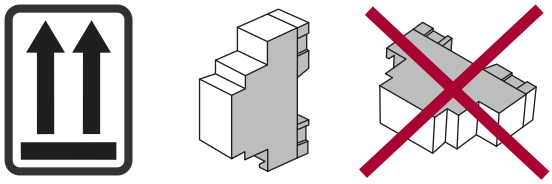
Screws (2)

Washer screws (2)

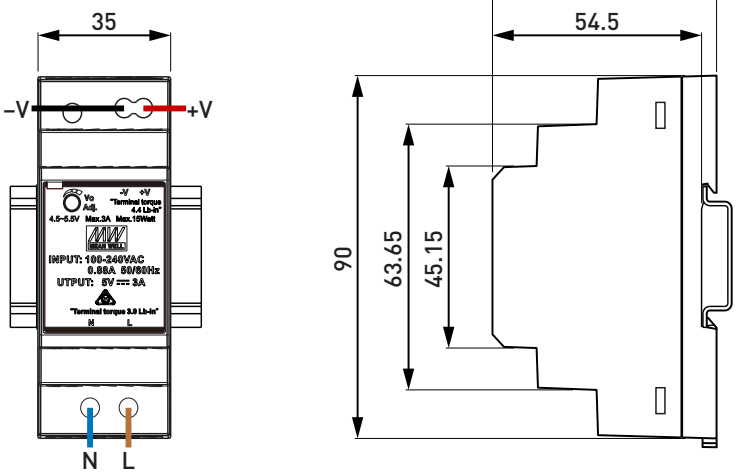
Follow these steps to mount the Helvar Cloud Gateway on a standard DIN rail:

1. Mount the PSU on the DIN rail. For details, see section 4.1.
2. Mount the Helvar Cloud Gateway on the DIN rail. For details, see section 4.2.

4.1 Mount the PSU on the DIN rail



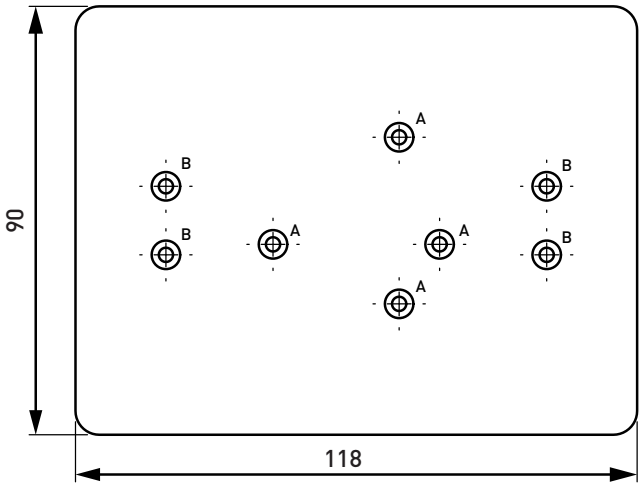
Dimensions (mm) and connections



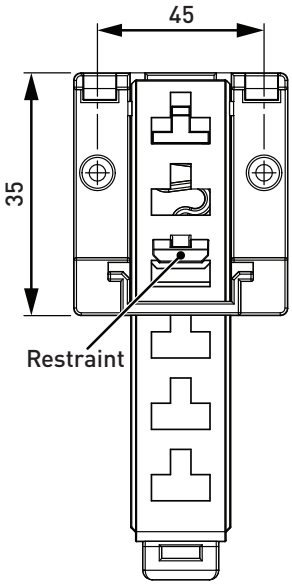
4.2 Mount the Helvar Cloud Gateway on the DIN rail

Mounting dimensions (mm)

Mounting plate

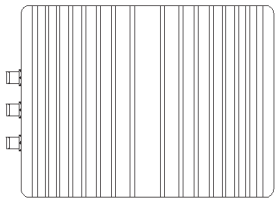
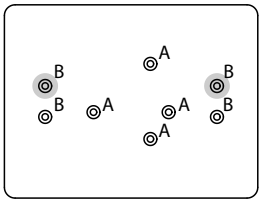
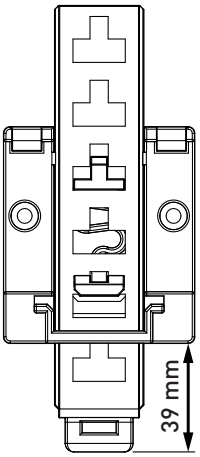
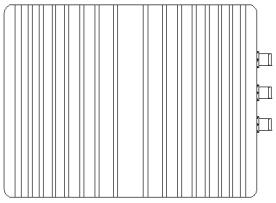
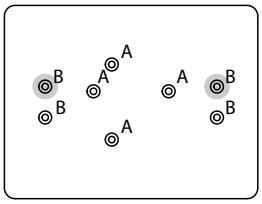
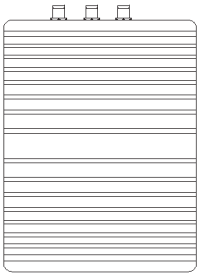
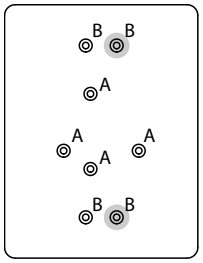
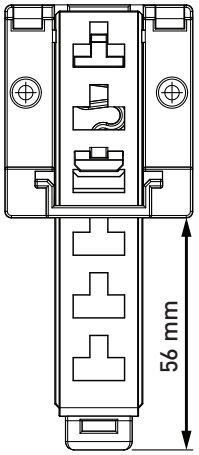
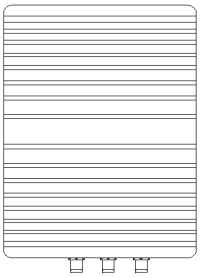
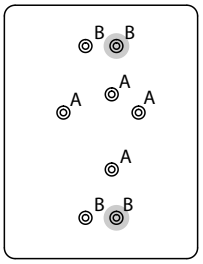


Mounting clip

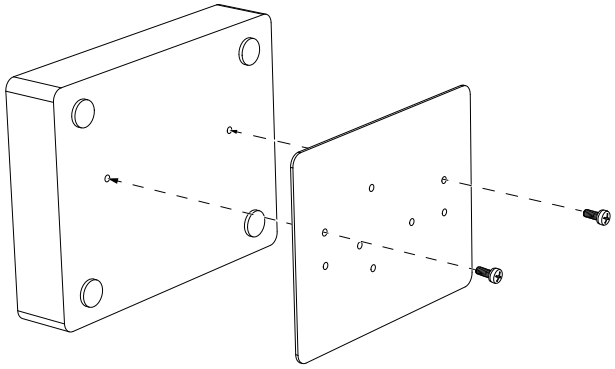


Mounting procedure

1. Determine the mounting position of the HCG and identify in the following table the mounting plate holes that you need to use.

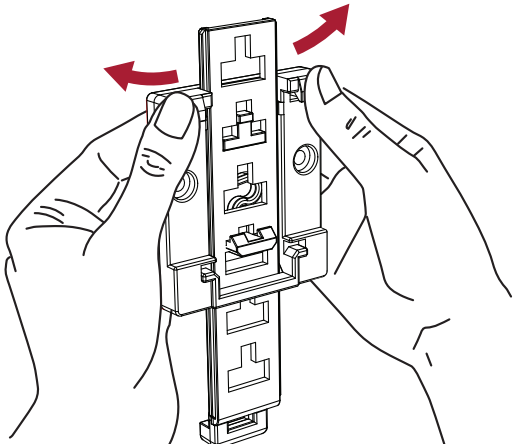
To mount the HCG in this position...			*Use these holes in the mounting plate*	*Length of mounting clip latch*	*DIN-Rail spacing*
Horizontal orientation	Front panel down				4U
	Front panel up				
Vertical orientation	Front panel left				3U
	Front panel right				

2. Screw the mounting plate to the unit using the appropriate holes. For details, refer to the preceding table.



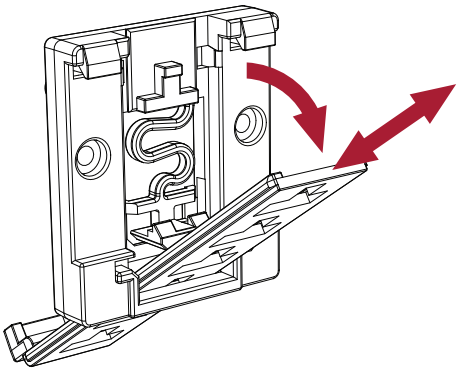
3. Do the following to adjust the mounting clip latch to the length that is appropriate for the required mounting orientation:

   a. Press the upper part of the mounting clip on both sides.

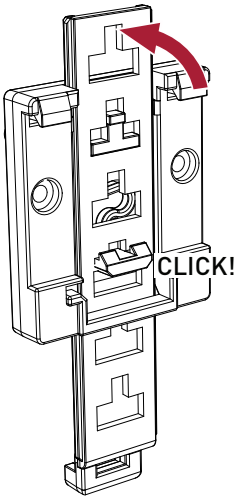


   b. Push the mounting clip latch forwards to unlock it.

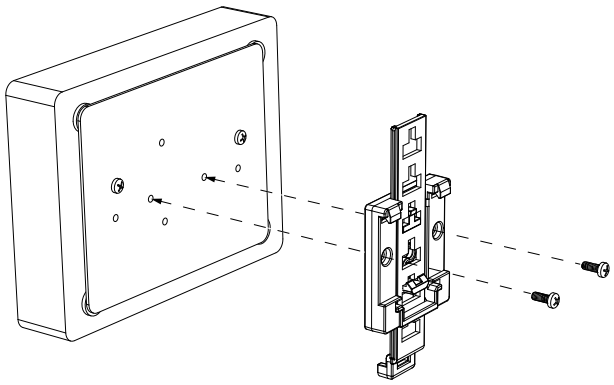
   c. Slide the latch upwards or downwards to the length that is appropriate for your mounting orientation. For details, refer to the table on page 5.



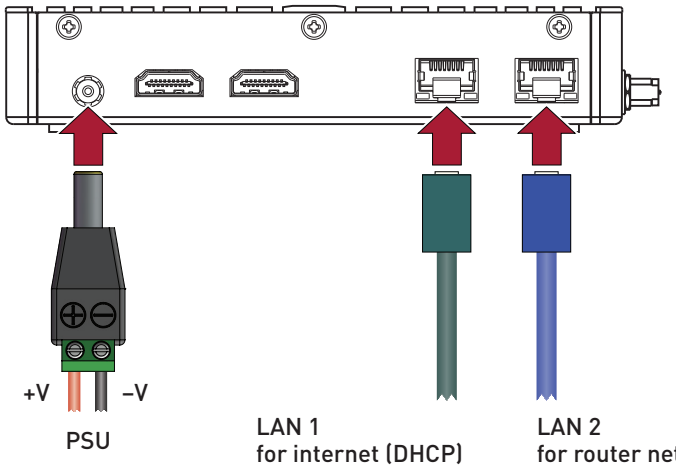
   d. Push the latch backwards to lock it.

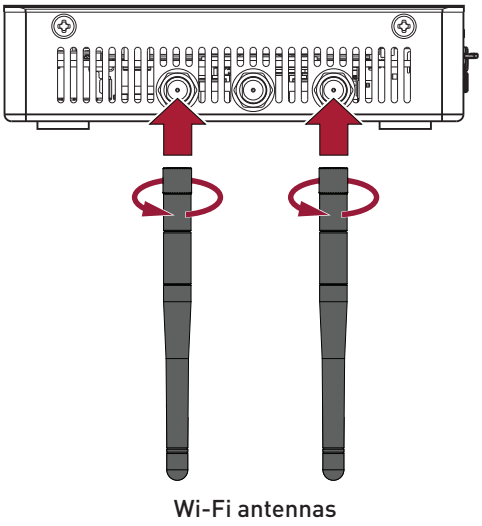


4. Screw the mounting clip to the mounting plate.



4.3 Connect the PSU, the Ethernet cable for the router network, and the Ethernet internet cable and/or Wi-Fi antennas





Follow these recommendations to optimise the performance and reliability of the wireless connection:

a. If required, connect the Wi-Fi antenna to the magnetic base of the antenna extension.
b. Set up your Helvar Cloud Gateway as close as possible to the centre of the area for which you want to provide wireless networking.
c. Keep the antenna away from objects that cause wireless interference. Large metal objects, fluorescent or halogen lights, microwaves, cordless phones and their base stations and wall ducting or vents can block or interfere with wireless signals.
d. Place the antenna in an elevated location.

5. HCG Security and Network Configuration

This section provides information on how the HCG communicates externally to the internet and internally on local networks, the hardware specification, the operating system and software that's installed in respect to what is exposed to the customer. As far as the client is concerned, the HCG should be considered only as a black box.

5.1 Internet Connectivity

The HCG requires internet connectivity in order to facilitate the provision of data to Helvar's Cloud Platform and to allow remote assistance. This can be achieved by connecting the HCG to the LAN, using Ethernet port 1 or wireless, and then configuring the network settings in accordance to the LAN requirements. The network settings can be configured using the 'Control Admin Tool'.

5.2 Helvar Cloud Platform

The Helvar Cloud Platform supports Helvar's Services offering. The Helvar Cloud Gateway is required to connect to the Helvar Cloud Platform that is built on top of AWS (Amazon Web Services). To achieve this it uses both HTTPS and MQTT protocols on ports 443 and 8883 respectively, and the HCG requires that these ports are kept open on any firewalls or internet gateways. The HCG connects to the following AWS IoT Service endpoint: . A connection between the HCG and the Helvar Cloud is established using MQTT, which uses TLS 1.2 along with cypher suite ECDHE-ECDSA-AES128-GCM-SHA256 and is protected using an X.509 certificate, which is stored on the HCG. Once the connection has been authenticated and authorised then subsequent connections are setup, over HTTPS and MQTT, using AWS credentials that use the AWS signature version 4 format. The AWS credentials in the seconds phase are obtained dynamically and are not stored on the HCG.

5.3 Remote Assistance

In order the remotely support issues regarding the HCG Helvar utilises TeamViewer. This service uses port 5938 when trying to establish a connection with the TeamViewer servers. If that port is not open then it will try port 443 (HTTPS) and then finally port 80 (HTTP). Helvar recommends that either ports 5938 or 443 are left open but not port 80 as this in not secure. There are no static IP addresses to whitelist for the TeamViewer servers, however all of their servers IPs have PTR records (used for reverse DNS lookup) that resolve to *.teamviewer.com, and this wildcard address can be used to restrict destination addresses that are allowed through the any firewall. Note that Helvar does not make a direct connection to the HCG when using TeamViewer.

5.4 Local Connectivity

Local communications are concerned with the HCG transmitting messages to and from Helvar routers. There are two main types of internal network in which the Helvar system can exist. For a simple layer 2 network there are no real security concerns for the network as all communications will be contained within the network. For a more complex system, that is integrated into a layer 3 network, there are certain networking requirements that need to be implemented. These are the opening of certain network ports to allow communications between HCG and routers and between routers themselves.

The first of these types of communications are for network discovery and are realised by UDP broadcasting or multicasting using the ports 60000 and 60009 respectively. These message packets must be free to traverse the network segments that contain all routers and the HCG.

The second type of communications are direct messages that are unicast between the HCG and routers and also between routers. These are sent using a combination of UDP and TCP over the following port range 60001-60008.

There are some other communication scenarios that require additional network configuration that are related to the Helvar routers and Helvar Designer software. The scenarios are based around BMS systems are concern Helvar's HelvarNet protocol and also BacNET and OPC which are industry standard protocols. These scenarios are not directly related to the HCG and are not discussed further here, for more information regarding these scenarios contact Helvar support.

5.5 Controller Admin Tool

This is a web page interface on the controller, and can be accessed via port 5000 and a known IP address (assigned via DHCP or a static IP configured manually) for the HCG or the pre-configured IP address of 10.24.15.5, i.e. http://10.24.15.5:5000. The tool can be used to configure both the internet connection and the local network connectivity of the HCG. Currently, the HCG can only be configured to access the internet using DHCP. ***Note***, if a static IP address configuration is required along with a gateway and DNS configuration then this is not currently supported out-of-box and installation will require Helvar support to assist with this. Additionally the internal network can only be statically configured to to a layer network. If layer 3 network configuration is required, then again installation will require Helvar support to assist with this.

5.6 Hardware and OS

The HCG is an GIGABYTE EL-20-3700-32GB IoT Gateway and consists of:

- 2 Ethernet ports that are not secured by a firewall.
- 4 USB ports
- 1 micro USB port
- 1 'COM' port
- MicroSD card slot.

There is no protection for the USB ports or the MicroSD slot and also as the device can be setup as a terminal, Helvar recommends, that the device is installed in a secure location and that access to the device requires authorization and is monitored for auditing.

5.7 Summary

Connectivity	Function	Ports	Protocols	Notes
HCG External	Cloud	443, 8883	HTTPS, MQTT	Required for external access and should be protected by firewall that is administered by the IT team responsible for the LAN.
HCG External	TeamViewer Support	443, 5938 (optional)	UDP, TCP	Required for external access and should be protected by firewall that is administered by the IT team responsible for the LAN, this feature is optional but Helvar support would be required to go to site which is a more expensive option.
HCG Internal	Routers	60000-60009	UDP, TCP	Required by the HCG to connect to the Helvar Router system.
HCG Internal	Controller Admin	5000	HTTP	Required by a commissioner to configure the network settings and the Workgroup (Router system connection) of the HCG.

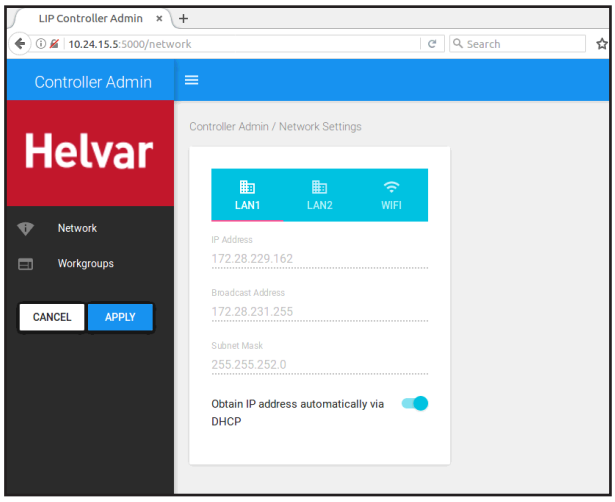
6. Configure the router network and the workgroup

Before the HCG can communicate with the router system, do the following to configure the router network and indicate to which workgroup the HCG should connect on LAN 2.

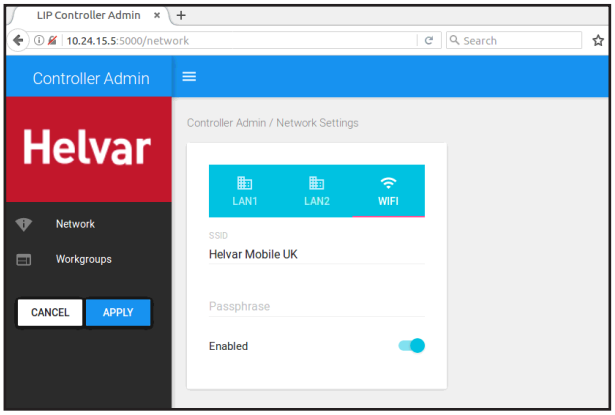
1. Make sure that the HDR-30-12 PSU is on and is connected to the HCG.
2. Connect the PC to the HCG ensuring the Ethernet cable is placed into port 2.
3. Turn on the PC that is connected to the HCG.
4. Set the IP address of this PC to the same IP range as the HCG.

***Note**: The HCG shipping static IP address for LAN 2 is 10.24.15.5, and the subnet mask is 255.0.0.0. Therefore, you could, for example, set your PC to the IP address 10.24.15.99 and to the subnet mask 255.0.0.0.*

5. Open Google Chrome, and navigate to http://10.24.15.5:5000 to access the **Network** configuration pages of the HCG.
6. In the dialog box, specify how you want to connect to the internet:

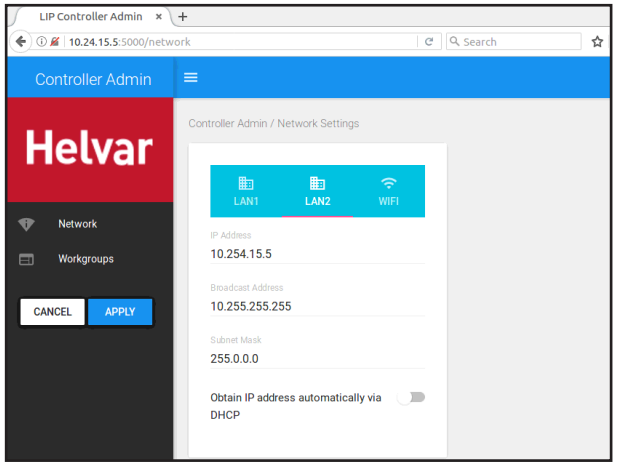


- To connect to the internet over LAN 1, do one of the following on the **Network** tab:
  - To obtain the IP address automatically via the Dynamic Host Configuration Protocol (DHCP), click **APPLY** (default option).
  - To enter the IP address manually, type the required **IP Address**, **Broadcast Address** and **Subnet Mask**, and then click **APPLY**.



- To connect to the internet over Wi-Fi, click the **WIFI** tab, and then do the following:
  a. Type the exact SSID and passphrase for the Wi-Fi network that you want to connect to.
  b. Click **Apply** to save your settings.

7. To change the static IP address for the connection to the router network, click the **LAN2** tab, and then type the new IP address.



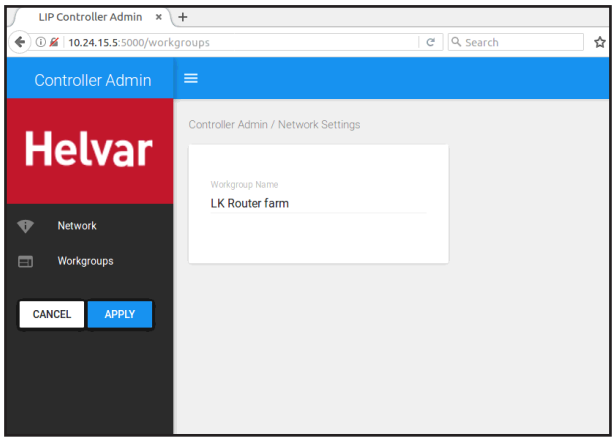
***Note** 1: The static IP address for the connection to the router network must be in the same range as the router workgroup to which the HCG will connect. Check in the Designer software beforehand to ensure all details are correct. Changing this IP address will change the HCG's address for the network configuration pages. For example:*

- *If you change the IP to 10.254.0.100, the network configuration address will change from http://10.24.15.5:5000 to http://10.254.0.100:5000.*
- *If you change the first octet of the HCG to 192.x.x.x, you will need to set the broadcast address of the HCG to match accordingly: 192.255.255.255.*

***Note 2:** The static IP address for the connection to the router network must be a unique IP address that does not conflict with any other devices on the network. Obtain confirmation from the site owner.*

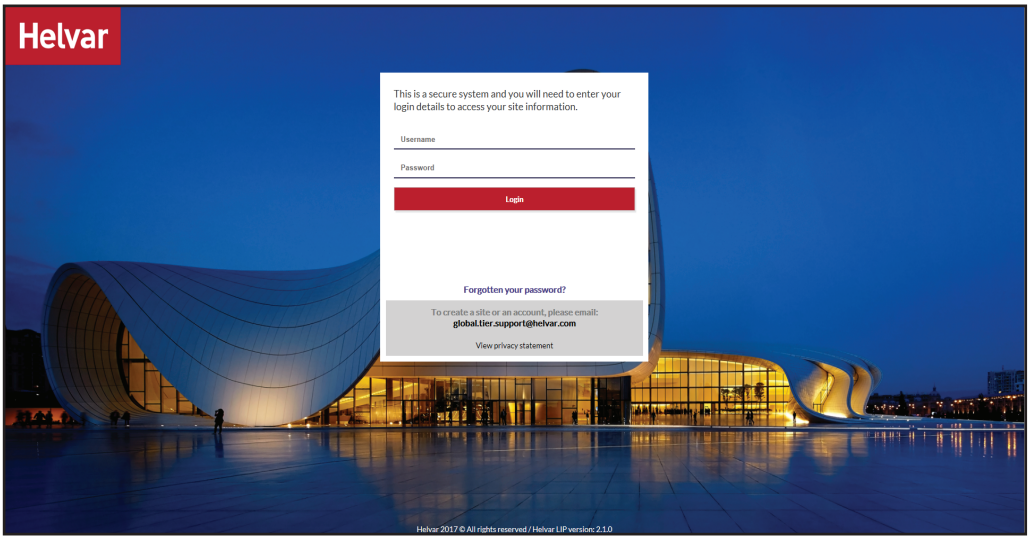
8. Click **Apply** to save your settings.
9. Click **Workgroups**, type the exact name of the workgroup that you want the HCG to connect to (check in the Designer Software beforehand), and then click **Apply**.

***Note**: After the settings that you have entered are saved, a message will appear at the bottom of the browser. This is only an indication that your settings have been saved, not a status that the HCG is connected to the network.*



7. Site and Account creation

When creating a site or an account go to https://service.helvar.io/ and from the login screen, shown below, select the **global.tier.support@helvar.com** address. a new email page will appear.



If the creation of a **new site** is required ensure the email contains the following information:

- Serial Number of the HCG - This is located on the base of the unit, above the barcode and has an SN prefix.
- Site name to be used - Select something logical and relating, for example "Helvar_Espoo".
- Address of the site - Full details are required.
- Company name - Who is the install for?

If the creation of a **new account** (user to access the web Ui) is required ensure the email contains the following information:

- User name.
- User surname.
- Site name and/or Serial number of the HCG the user requires access to.

***Note:** Both of these requests can be put in a single email. Please specify what is required in the title of the email.*

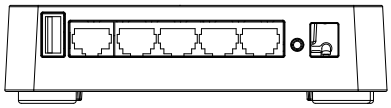
Be aware of the following rules when requesting any site or account creation:

- Helvar policy *does not* allow account creation though delegation (a user requesting site access for a 3rd party)
- Helvar policy *does not* allow site access for generic email addresses (eg.: info@helvar.com)
- Each user wanting to access a site can only make the request through the global tier support address stated above.

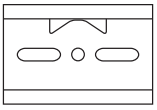
8. Install the TOSIBOX® Lock 100

This section applies only to HCG1TBLK KIT and HCG1TBL KIT.

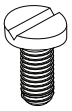
Package contents



TOSIBOX® Lock 100



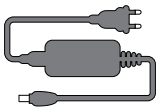
DIN-rail mounting bracket



Screws (2)

AMR1-24 PSU

DC feed plug



12 VDC AC/DC power adaptor

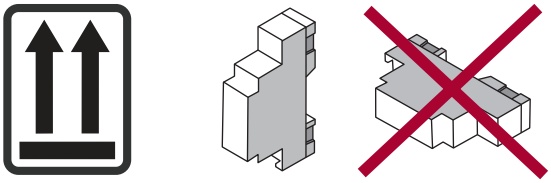
2 × Wi-Fi antenna

Antenna extension with magnetic base

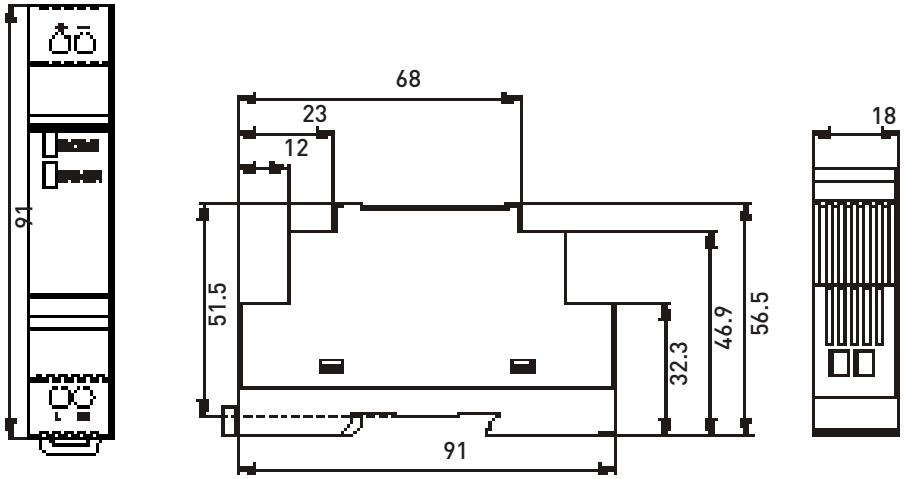
Follow these steps to mount the TOSIBOX® Lock 100 on a standard DIN rail:

1. Mount the PSU on the DIN rail. For details, refer to section 4.1.
2. Mount the TOSIBOX® Lock 100 on the DIN rail. For details, refer to section 4.2.

8.1 Mount the PSU on the DIN rail



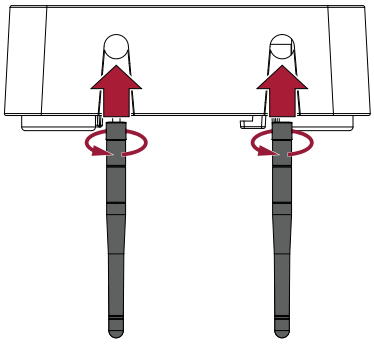
Dimensions (mm) and connections



8.2 Mount the TOSIBOX® Lock 100 on the DIN rail

For information on how to mount the TOSIBOX® Lock 100 on the DIN rail, refer to Tosibox Inc.'s documentation available at www.tosibox.com.

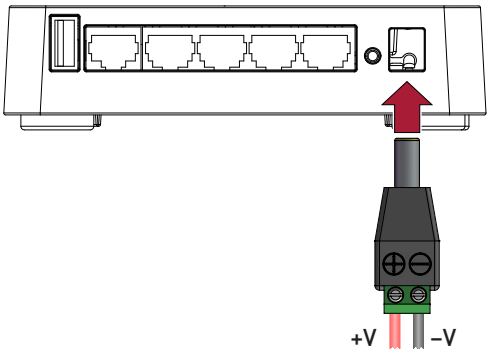
8.3 If required, connect the Wi-Fi antennas



Wi-Fi antennas

For recommendations on how to connect the Wi-Fi antennas, refer to section 4.3 on page 7.

8.4 Connect the PSU and allow a couple of minutes for the unit to boot up.

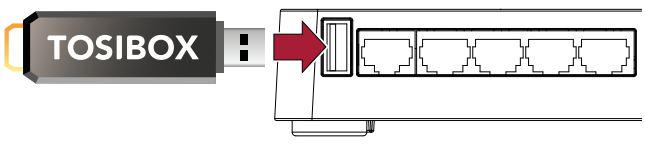


PSU

9. Serialise the TOSIBOX® Key 200

To serialize the TOSIBOX® Key 200, follow these steps:

1. With the TOSIBOX® Lock 100 fully booted up, insert the TOSIBOX® Key 200 into the USB port of the unit. When the TOSIBOX® Key 200 LED stops blinking or shuts off, the serialisation is complete.

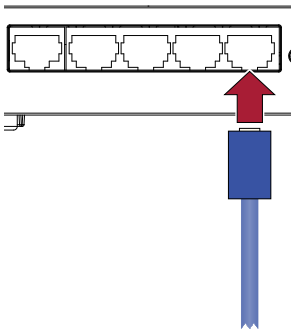


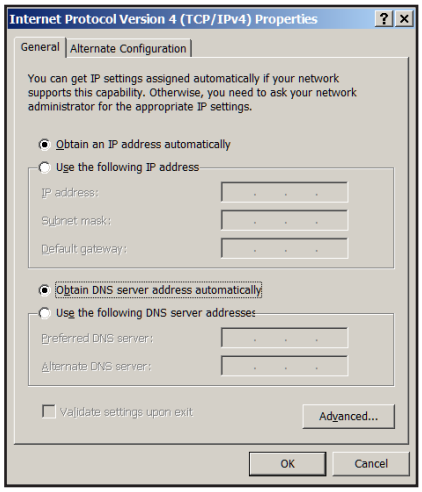
2. Remove the TOSIBOX® Key 200 from the TOSIBOX® Lock 100.

10. Set up the IP address of the VPN adapter

To set up the IP address of the VPN adapter, follow these steps:

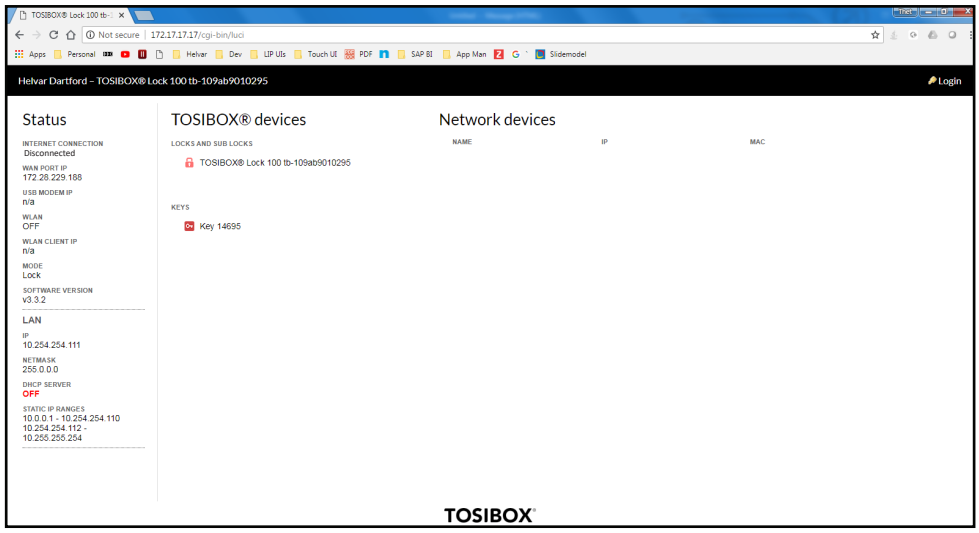
1. Connect a PC to the Service port of the TOSIBOX® Lock 100 via an Ethernet cable.

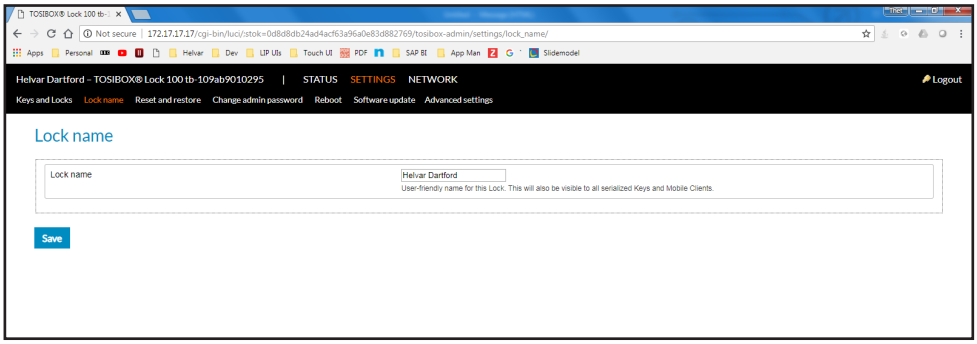




2. Make sure that the Ethernet LAN properties on the PC are set to obtain an IP address automatically.

3. Open the web browser of the PC, type **http://172.17.17.17** (IP address of the Service port) in the address bar, and then press **Enter** to access the TOSIBOX® Lock 100 home page.

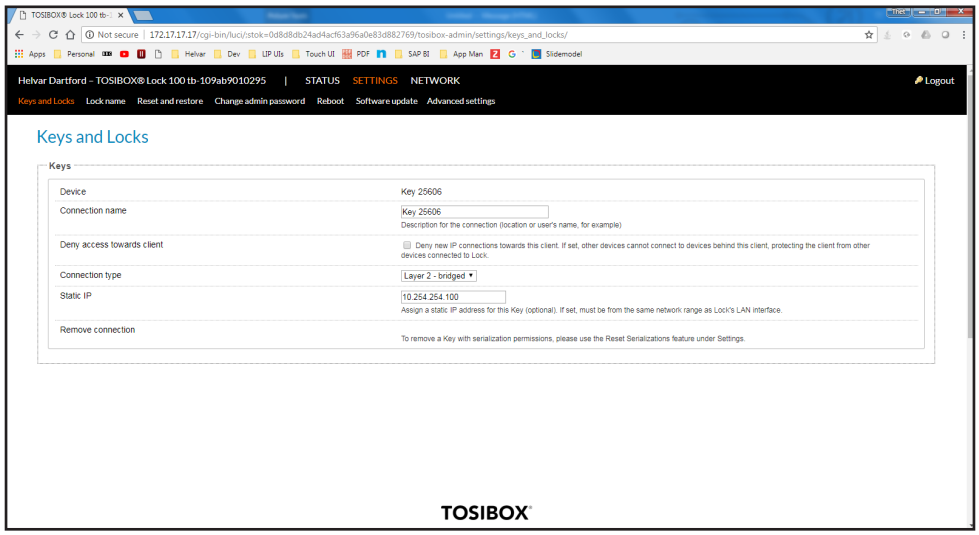




4. Click **Login** in the upper right corner to access the TOSIBOX® Lock 100. Login details are printed on the back of the TOSIBOX® Lock 100.

5. Click **SETTINGS > Lock name**, type an appropriate name for the TOSIBOX® Lock 100 in the **Lock Name** text box, and then click **Save**.

6. Click **SETTINGS > Keys and Locks** to display the **Keys and Locks** page.



7. In the **Connection name** text box, type an appropriate name for this connection.
8. Clear the **Deny new IP connections towards this client** check-box.
9. From the drop-down list, select the **Layer 2 – bridged** connection type.
10. In the **static IP for the connection**, type the IP address that you want the PC to use.

    Examples:

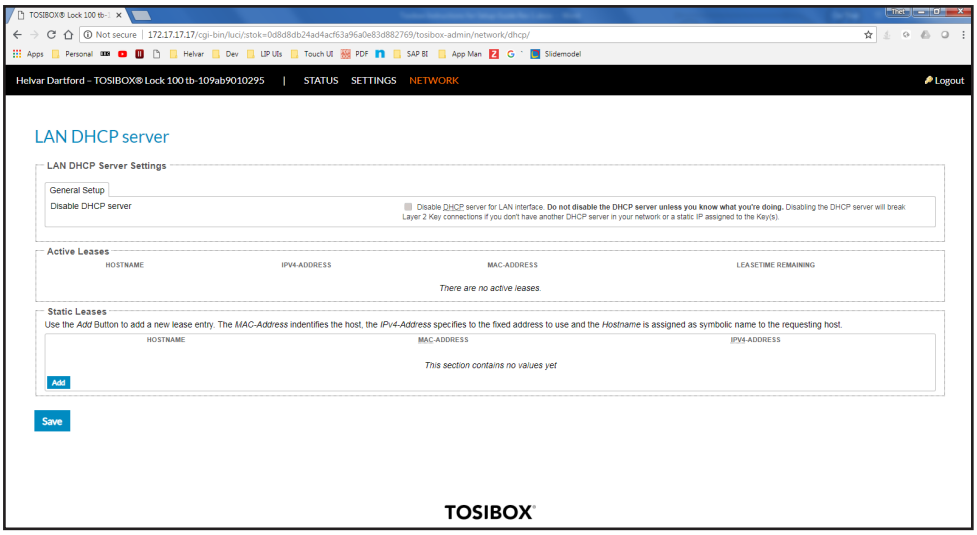
    - *For single-cluster systems: 10.254.1.40 (next key 10.254.1.41, etc.).*
    - For multi-cluster systems: 10.254.254.40 (next key 10.254.254.41 etc.).

***Note**: The static IP address for the connection must be a unique IP address that does not conflict with any other devices on the network.*

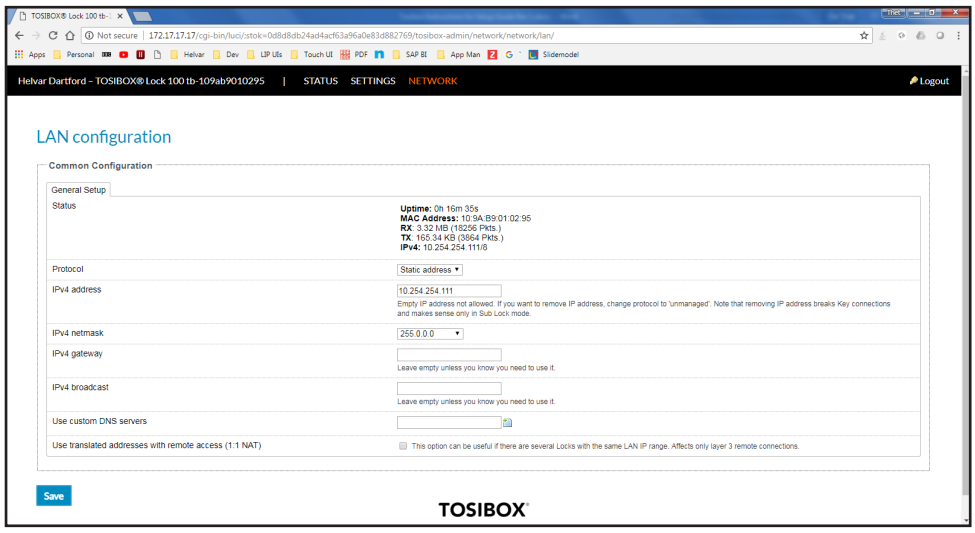
11. Set up the IP address of the TOSIBOX® Lock 100

To set up the IP address of the TOSIBOX® Lock 100, follow these steps:

1. In the TOSIBOX® Lock 100 home page, click **NETWORK > LAN DHCP server** to display the LAN DHCP server page.
2. Clear the **DHCP server for LAN interface** check-box, and then click **Save**.



3. Click **NETWORK** to display the **LAN configuration** page.



4. From the **Protocol** drop-down list, select **Static address**.
5. In the **IPv4 address text** box, type the appropriate IPv4 static IP address. The IP address range and the free IP addresses of the router network can be obtained from the relating Designer software.

   Examples:

   - *For single-cluster systems: 10.254.1.99.*
   - *For multi-cluster systems: 10.254.254.99.*
6. In the **IPv4 netmask** box, type the appropriate IPv4 netmask.

   Example netmask for above IP addresses: 255.0.0.0

***Note**: The static IP address for the connection must be a unique IP address that does not conflict with any other devices on the network.*

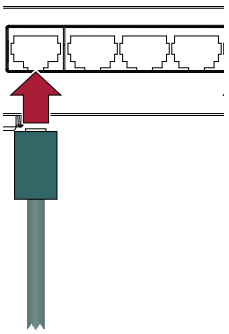
7. Click **Save**.

12. Connect the TOSIBOX® Lock 100 to the internet

To connect the TOSIBOX® Lock 100 to the internet, do one of the following:

- To use a wired connection, follow these steps:

  a. Connect an Ethernet internet cable into the WAN port of the TOSIBOX® Lock 100.



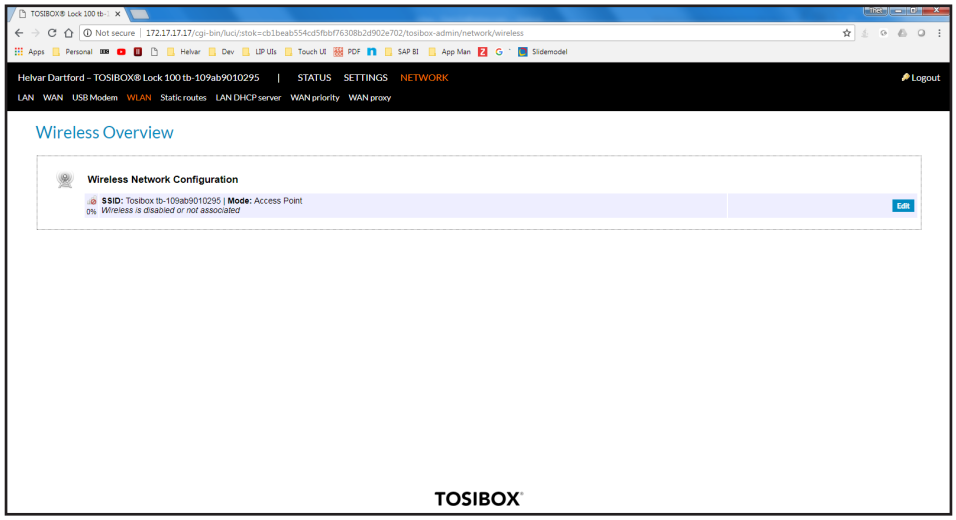
WAN to internet

  b. Go to the TOSIBOX® Lock 100 home page and make sure that the internet connection shown under **Status** is active.

  ***Note**: You should still be connected to the service port, and your browser should still be open to http://172.17.17.17. But if you are not, repeat steps 1–2 in section 11.*

- To use a wireless connection, follow these steps:

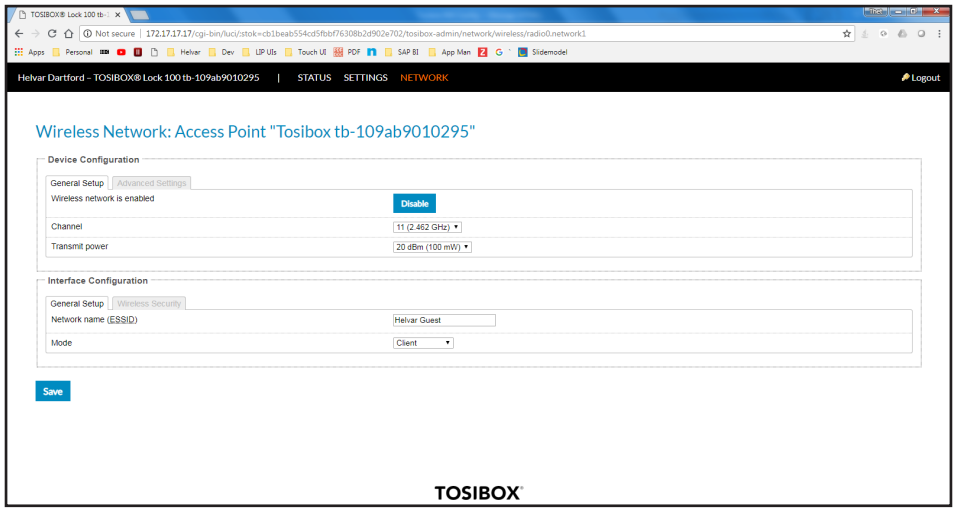
  a. Click **NETWORK > WLAN** to display the **Wireless Overview** page.



  b. Click the **Edit** button on the right side of the screen to display the **Wireless Network** page.

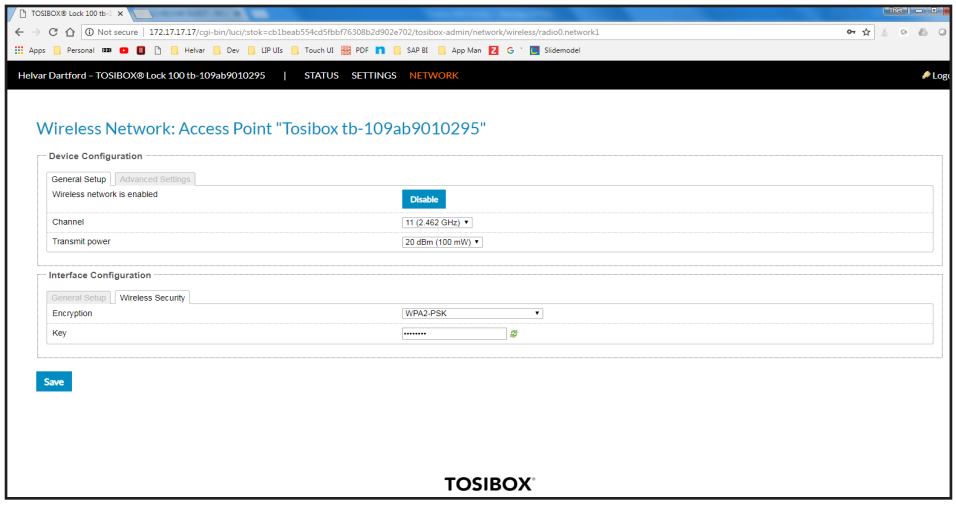
  c. Under **Device Configuration**, click the **Enable** button to active the WLAN.

  d. The **Enable** button toggles to **Disable**.



  e. In the **General Setup** tab, type the name of the wireless network in the **Network Name (ESSID)** text box, and then select **Client** from the **Mode** drop-down list.

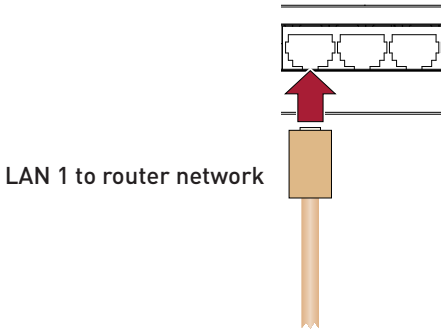
  f. If the wireless network uses encryption and password protection, click the **Wireless Security** tab, select the type of encryption from the **Encryption** drop-down list, and then type the password in the **Key** text box.



  g. Click **Save**.

13. Connect the lighting router network to the TOSIBOX® Key 200

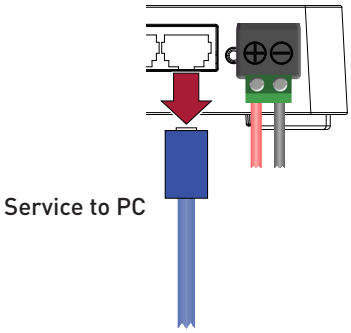
Connect the lighting router network to the LAN 1 port of the TOSIBOX® Lock 100 using an Ethernet cable.



14. Test the VPN connection

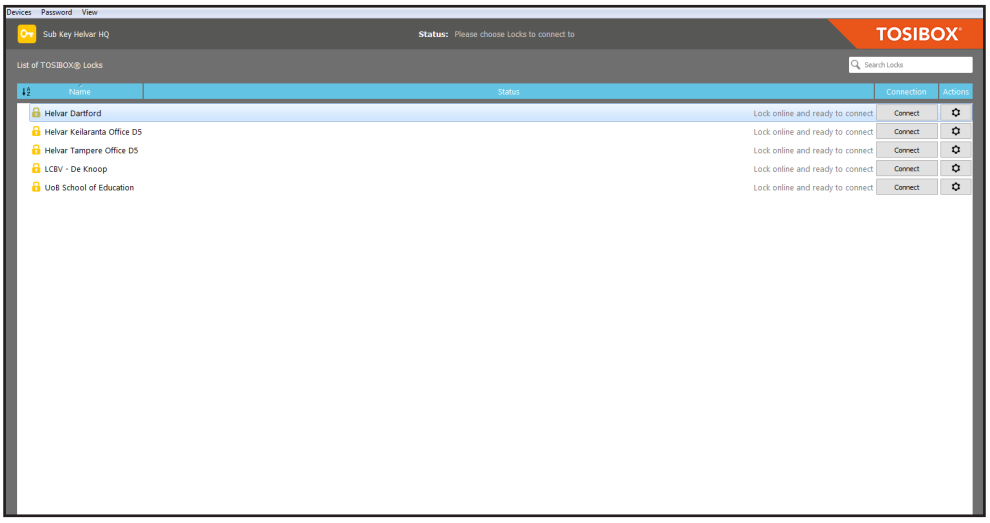
To test the VPN connection between the TOSIBOX® Lock 100 and the PC running Designer do the following:

1. Make sure that the PC running Designer is connected to the Internet.
2. Disconnect the Ethernet cable from the Service port on the TOSIBOX® Lock 100.



3. Insert the TOSIBOX® Key 200 into a USB port on your PC.

   An auto play window will appear with options to install the TOSIBOX® Key 200 software.
4. Complete the installation process of the software.
5. When the **List of TOSIBOX® Locks** window appears, select the appropriate TOSIBOX® Lock 100, and then click **Connect**.
6. Wait a few moments for the TOSIBOX® Key 200 to establish connection to the TOSIBOX® Lock 100.



7. Run Designer software and check that the remote routers appear in the **Devices** tree.
8. Connect to the workgroup and use Designer normally.

15. Technical data

15.1 HCG

Power

Input voltage: 12 VDC – 19 VDC

Connectivity

LAN 1: 10/100/1000 Mbps Intel I210 GbE. For router network.

LAN 2: 10/100/1000 Mbps Intel I210 GbE.

Wi-Fi: 2 × Wi-Fi antenna

I/O interface

HDMI: 2 × HDMI-out, max. resolution: 3840 × 2160 @ 30 Hz, 2560 × 1600 @ 60 Hz, 24 bpp

On/Off: Power button with LED

USB interface: 4 × USB 3.0

Mechanical data

Dimensions: 140.8 mm × 107.5 mm × 28 mm

Mounting: DIN rail (installation in switchgear/controlgear cabinet)

Weight: 0.56 kg

IP code: IP20

Operating and storage conditions

Ambient temperature: 0 °C to +40 °C

Relative humidity: Max. 90 %, noncondensing

Storage temperature: –20 °C to +60 °C

Conformity and standards

EMC: EN 55032
EN 55024

RED: EN 301489-1
EN 301489-17

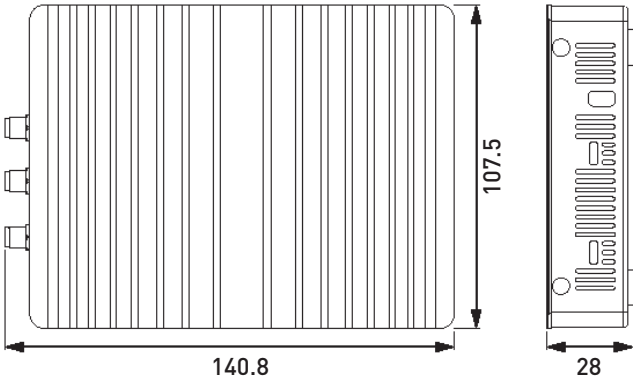
Safety: EN 60950-1

Environment: Complies with WEEE and RoHS directives.

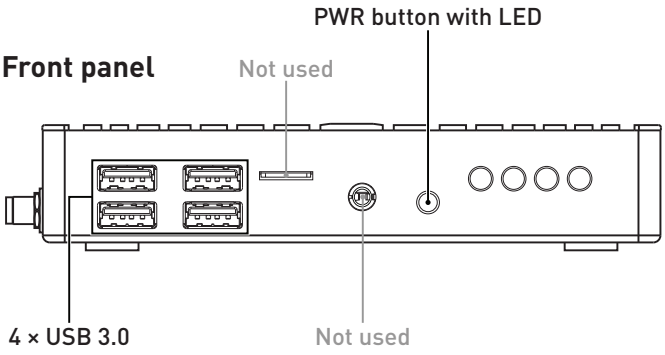
Software compatibility

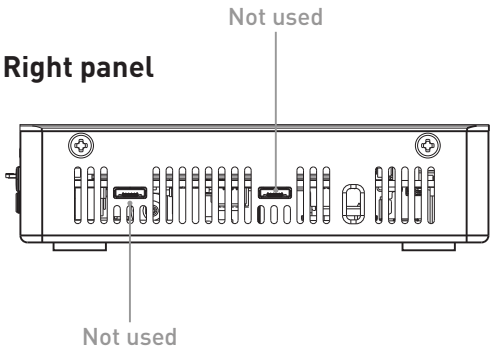
Designer: 5.4.3 or later

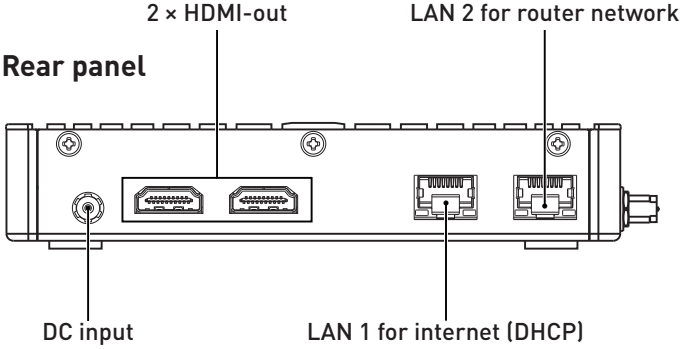
Dimensions (mm)

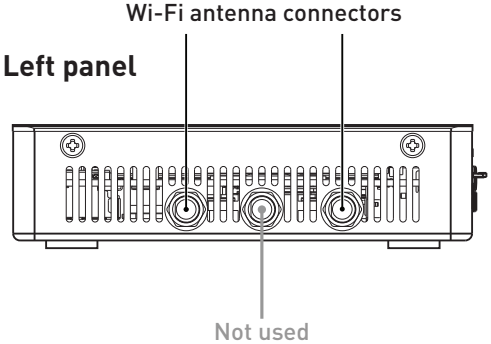


Connections





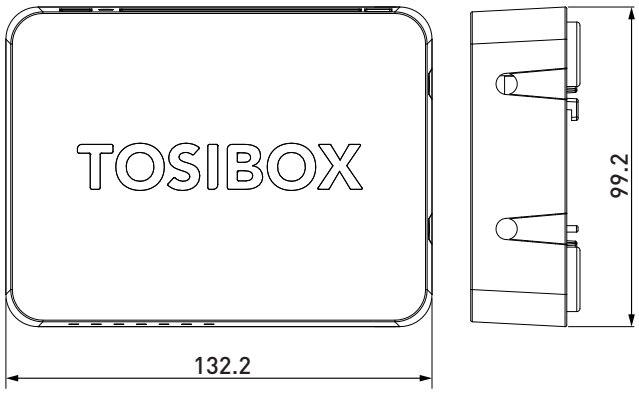




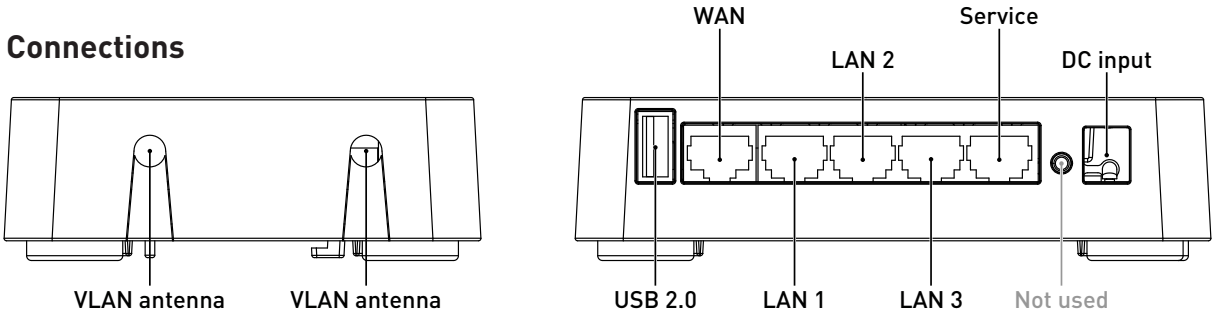
15.2 TOSIBOX® Lock 100

For technical data, refer to Tosibox Inc.'s documentation available at www.tosibox.com.

Dimensions (mm)



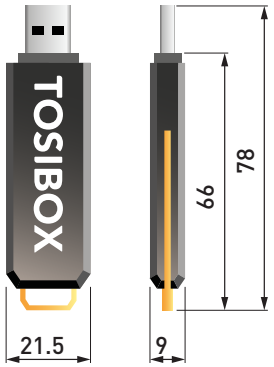
Connections



15.3 TOSIBOX® Key 200

For technical data, refer to Tosibox Inc.'s documentation available at www.tosibox.com.

Dimensions (mm)



16 System diagram