trulifi
by signify

Trulifi Controller Unit 6800
Trulifi Controller Application 6800

User Manual

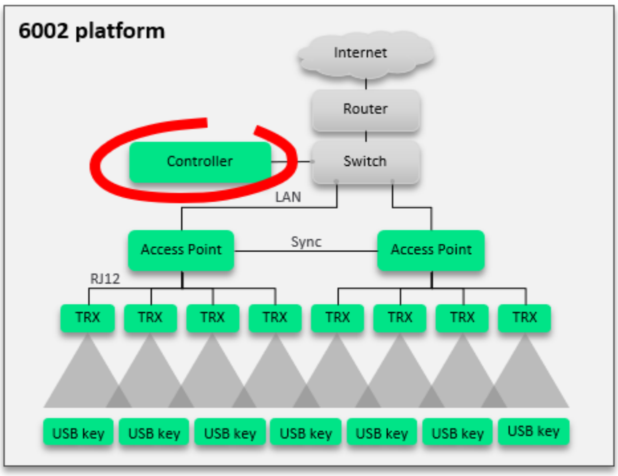
Trulifi Controller 6800 - User Manual

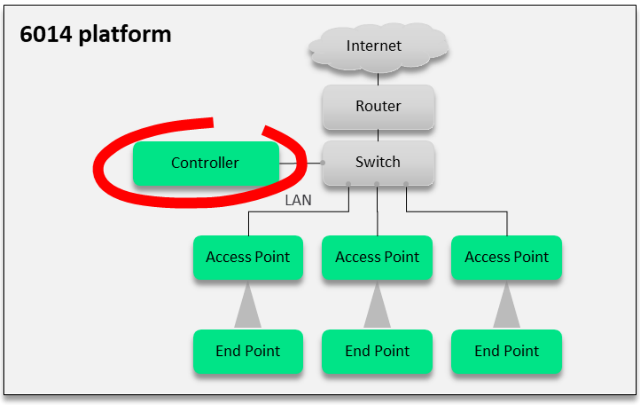
1 Introduction

The Trulifi 6002 and the 6014 platform can be extended (licensed) with a LiFi controller, both as system (=Controller HW + SW) or as Virtual Machine/SW-only. The LiFi-controller enables roaming of USB-Keys between multiple Trulifi 6002.2 Access Points installed in network or building. Also, the Trulifi controller can be extended with a License for Network Monitoring and Control for the Trulifi 6002 and Trulifi 6014 platform.
The LiFi controller application is available pre-installed on a hardware unit or as Virtual Machine version. In both instances the controller application still requires to be licensed.

The Trulifi 6800 controller will support the following LiFi-systems:

- Access Point 6002.1 (NMC)
- Access point 6002.2 (NMC and Roaming)
- USB Key 6002.1 (NMC)
- USB Key 6002.22 (NMC)
- Trulifi 6014.xx (NMC)





Example set-ups of 6002 and 6014 based system.

Pre-requisites for using the LiFi controller and NMC functionality:

- Advanced Networking knowledge
- System/Network administrator rights
- SNMP application such as SolarWinds, MIB Browser etc.
- Licensed system

This document describes the Controller Application, Roaming and SNMP configuration, for Firmware version **v4.1.0** and higher. This document is intended for IT professionals responsible for installation and management of enterprise IT systems and assumes Network Management and configuration knowledge.

1.1 Interference Management and hand-over.

The Trulifi 6002.2 system supports interference management and hand-over (=roaming), between multiple 6002.2 domains. In order to activate the interference management and hand-over, the controller needs to be licensed with a roaming functionality, to enable the roaming of Trulifi 6002 USB keys through multiple domains. The roaming license enables the interference management and hand-over from users (USB-keys) in-between domains and/or moving from one domain to the next domain. Please consult 6002.2 specifications and user manual on the Interference Management and Hand-over functionality.

1.2 Network Monitoring and Control.

Furthermore, SNMP based Network Management & Control function is available as a license option. This supports IT managers and/or IT Service Providers to control their LiFi installed base actively and efficiently, up to 64 Trulifi 6002 or Trulifi 6014 Access Points.

The LiFi Network Management and Control license can be purchased together with the Controller Unit or Application or as a future functionality extension.
Signify supports SNMP up to version V3. The SNMP configuration will be further described in Chapter 7 of this document. Please consult the MIB User Guide for more details and information on the supported SNMP parameters.

2 Hardware installation

The mechanical and electrical installation of the Controller Unit is described in the Quick Start guide packed with the Trulifi Controller Unit, please refer to this document.

The LAN wiring of the Controller Unit is described in the Installation Instructions included with the Trulifi 6002 system.

Once you have completed the mechanical, electrical and LAN installation steps, please proceed with this manual. In the remainder of this document, we describe the configuration of the controller. The LiFi controller application is pre-installed on the controller hardware, however, still requires to be licensed.

A maximum of 16 Access Points can be connected to 1 Trulifi 6800 Controller Unit. If more LiFi Access points need to be controlled, please add a LiFi controller or switch over to the Trulifi 6800 Controller Application (Virtual Machine version).

3 Trulifi Controller Application (Virtual Machine)

The LiFi controller application runs on VM-ware version 15 or higher.

3.1 Minimum hardware requirements:

	≤ 16 AP's	≤ 64 AP's
Minimum number of virtual CPUs	2 (≥ 3,2 GHz) x86 platform	4 (≥ 3,2 GHz) x86 platform
Min. RAM	4Gb	8Gb
Min. storage	8Gb	8Gb
NIC	1Gbps	1Gbps
Other	Client PC	Client PC

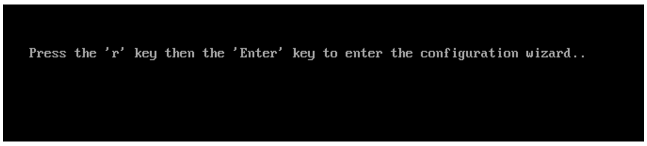
3.2 Purchase and activate licenses

In case you would like to extend the LiFi-controller system with additional licenses, please contact your local Signify reseller or representative or customercare.trulifi@signify.com

3.3 Installation instruction Virtual Machine version and Trulifi Controller Application 6800

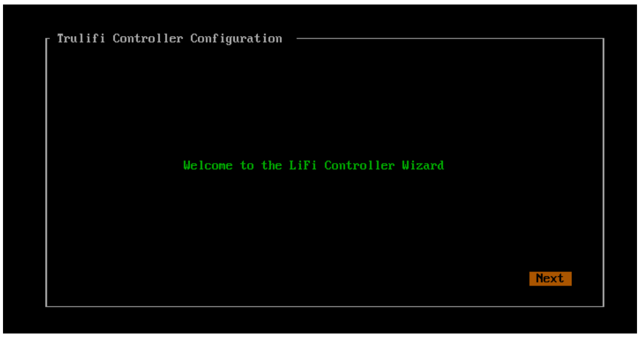
- Step 1: Save the **`trulifi_controller_application`** ovf-file on your client.
- Step 2: Open the VM application on your client.
- Step 3: Open the **`trulifi_controller_application`** ovf-file in your virtual machine.
- Step 4: Import "**`trulifi_controller_application`**" on your client.
- Step 5: Start your virtual machine application

When the virtual machine application is started, you will first see the following screen. This can be used in case the password of the Trulifi controller application is lost or if the Trulifi 6800 Controller application requires a reset.



```
Press the 'r' key then the 'Enter' key to enter the configuration wizard..
```

Wait for the following screen to appear:

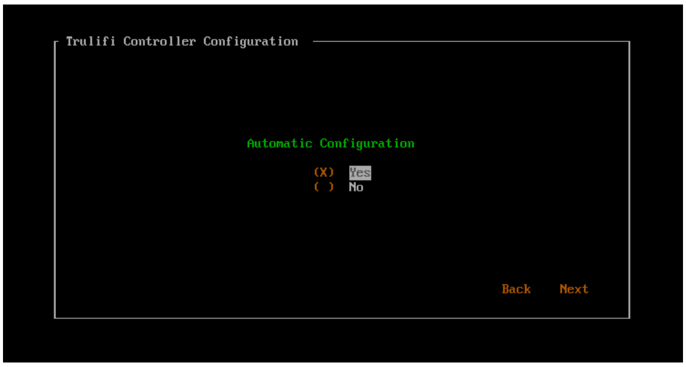


Trulifi Controller Configuration

Welcome to the LiFi Controller Wizard

Select **`[Next]`**

The following screen appears:



Trulifi Controller Configuration

Automatic Configuration

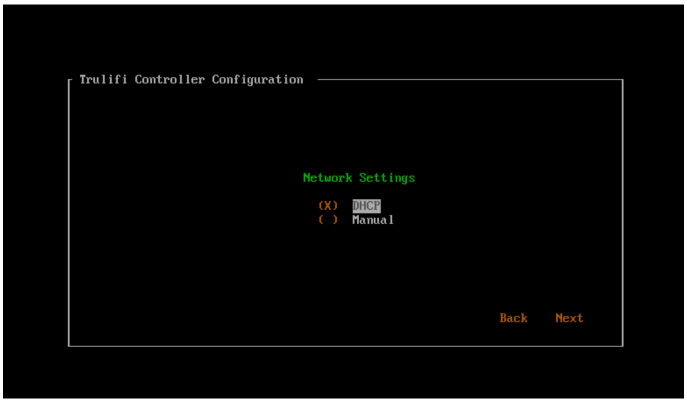
(X) Yes
( ) No

For Automatic configuration select **[Yes]**
For Manual Installation Select **[No]** and then select **[Next]**

In case Automatic configuration is selected, the application will be configured with the following settings:

```
1. Network Settings => DHCP
2. Time Settings =>
      a.  Timezone = Amsterdam
      b.  NTP Server 1 = time-a-g.nist.gov
      c.  NTP Server 2 = time-a-b.nist.gov
3. Admin Password => admin
```

If you select to configure the system manually you can choose how to configure the Network interface, either using DHCP or setting the network addresses manually.



Trulifi Controller Configuration

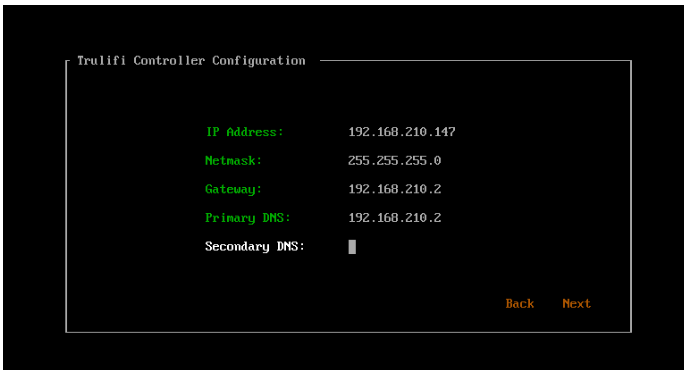
Network Settings

(X) DHCP
( ) Manual

Select Network Setting **[DHCP]** or **[Manual]** and select **[Next]**

In case Manual configuration is selected you need to configure the following parameters:

- IP Address
- Netmask
- Gateway
- Primary DNS
- Secondary DNS

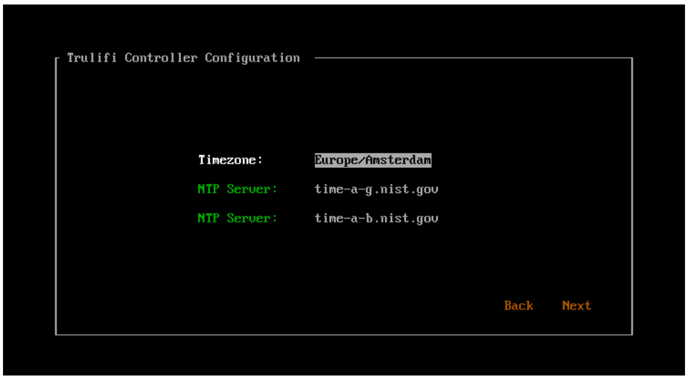


Trulifi Controller Configuration

IP Address: 192.168.210.147
Netmask: 255.255.255.0
Gateway: 192.168.210.2
Primary DNS: 192.168.210.2
Secondary DNS:

Enter your **Network settings** and select **[Next]**

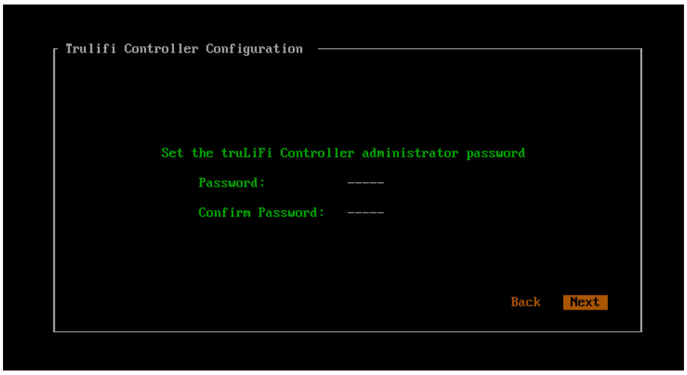
After network settings are configured, configure Time Settings:



Trulifi Controller Configuration

Timezone: Europe/Amsterdam
NTP Server: time-a-g.nist.gov
NTP Server: time-a-b.nist.gov

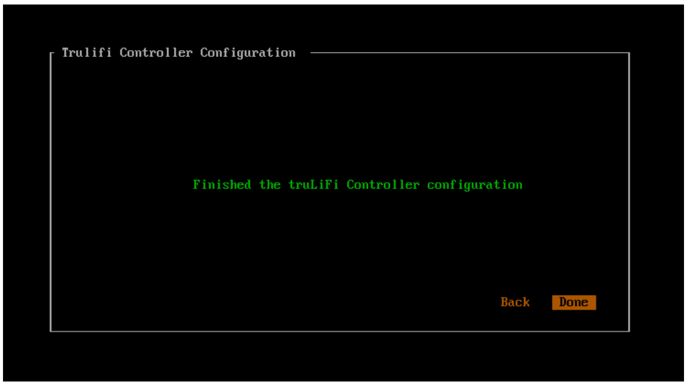
Configure your **Time Settings** and select **[Next]**



Trulifi Controller Configuration

Set the truLiFi Controller administrator password
Password: -----
Confirm Password: -----

Set your **Administrator password** and select **[Next]**



Trulifi Controller Configuration

Finished the truLiFi Controller configuration

You have finished your configuration. Select **[Done]**

After your configuration wizard is completed, open your web-browser and go to: `http://trulifi-controller.local` to enter the Trulifi controller General User Interface.

4 Using the controller GUI

4.1 Using LiFi controller

The Trulifi controller user interface and functionality is the same for the VM version as for the controller application pre-installed on the Trulifi Controller Unit

The Trulifi Controller Unit comes with the application software pre-installed. A browser-based GUI is built into the Trulifi Controller.

The controller management pages enable to configure parameters and to monitor the operational status of the controller and its associated access points.

The controller GUI is supported by the following web browsers:

- Microsoft Edge Version 87.x or higher (Windows)
- Mozilla Firefox, Version 84 or higher (Windows, Mac)
- Google Chrome, Version 87.x or higher (Windows, Mac)
- Apple Safari, Version 14 or higher (MacOS)

Note: Please ensure that your screen resolution is set to 1280x800 or more. Lower resolutions are not supported.

5 Configuring the controller

This section describes the required steps at first-time setup of the Controller Unit.

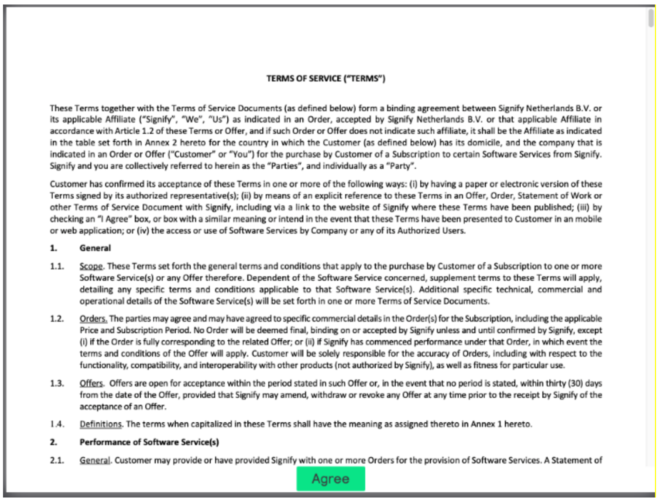
Before installing and configuring the LiFi controller make sure that you have obtained a license and stored the license file on a known location (e.g. Desktop) on your client connected to the same network. If you have not obtained a license file please contact: customercare.trulifi@signify.com

5.1 Controller (GUI) access

You can configure the Trulifi Controller Unit by connecting a keyboard and a monitor directly to the Trulifi Controller Unit.

Alternatively, you can connect your Client PC to the same network as the Controller Unit or Virtual Machine and browse to `http://trulifi-controller.local`.

The following login page appears:



TERMS OF SERVICE ("TERMS")

These Terms together with the Terms of Service Documents (as defined below) form a binding agreement between Signify Netherlands B.V. or its applicable Affiliate ("Signify", "We", "Us") as indicated in an Order, accepted by Signify Netherlands B.V. or that applicable Affiliate in accordance with Article 1.2 of these Terms or Offer, and if such Order or Offer does not indicate such affiliate, it shall be the Affiliate as indicated in the table set forth in Annex 2 hereto for the country in which the Customer (as defined below) has its domicile, and the company that is indicated in an Order or Offer ("Customer" or "You") for the purchase by Customer of a Subscription to certain Software Services from Signify. Signify and you are collectively referred to herein as the "Parties", and individually as a "Party".

Customer has confirmed its acceptance of these Terms in one or more of the following ways: (i) by having a paper or electronic version of these Terms signed by its authorized representative(s); (ii) by means of an explicit reference to these Terms in an Offer, Order, Statement of Work or other Terms of Service Document with Signify, including via a link to the website of Signify where these Terms have been published; (iii) by checking an "I Agree" box, or box with a similar meaning or intend in the event that these Terms have been presented to Customer in an mobile or web application; or (iv) the access or use of Software Services by Company or any of its Authorized Users.

1. General

1.1. Scope. These Terms set forth the general terms and conditions that apply to the purchase by Customer of a Subscription to one or more Software Service(s) or any Offer therefore. Dependent of the Software Service concerned, supplement terms to these Terms will apply, detailing any specific terms and conditions applicable to that Software Service(s). Additional specific technical, commercial and operational details of the Software Service(s) will be set forth in one or more Terms of Service Documents.

1.2. Orders. The parties may agree and may have agreed to specific commercial details in the Order(s) for the Subscription, including the applicable Price and Subscription Period. No Order will be deemed final, binding on or accepted by Signify unless and until confirmed by Signify, except (i) if the Order is fully corresponding to the related Offer; or (ii) if Signify has commenced performance under that Order, in which event the terms and conditions of the Offer will apply. Customer will be solely responsible for the accuracy of Orders, including with respect to the functionality, compatibility, and interoperability with other products (not authorized by Signify), as well as fitness for particular use.

1.3. Offers. Offers are open for acceptance within the period stated in such Offer or, in the event that no period is stated, within thirty (30) days from the date of the Offer, provided that Signify may amend, withdraw or revoke any Offer at any time prior to the receipt by Signify of the acceptance of an Offer.

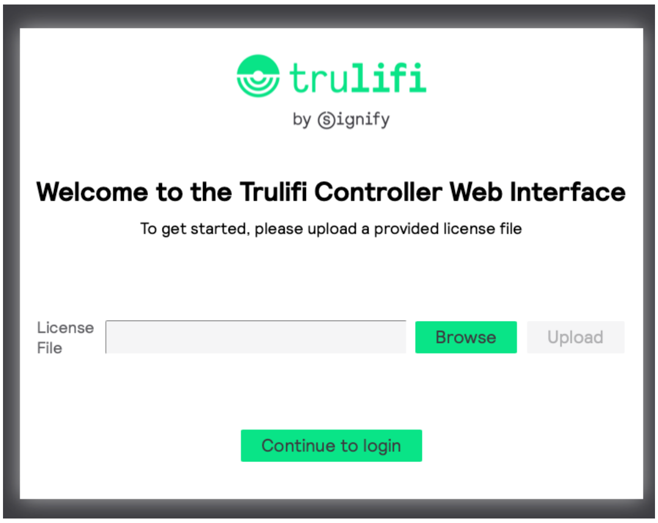
1.4. Definitions. The terms when capitalized in these Terms shall have the meaning as assigned thereto in Annex 1 hereto.

2. Performance of Software Service(s)

2.1. General. Customer may provide or have provided Signify with one or more Orders for the provision of Software Services. A Statement of

Scroll through the End-User License Agreement and select **`[Agree]`**

The following page appears:



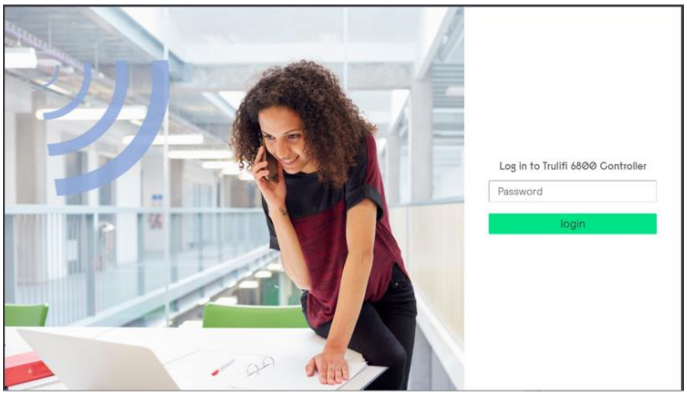
Welcome to the Trulifi Controller Web Interface

To get started, please upload a provided license file

Browse to the location where you have stored your license file and select the license file. Select **`[Upload]`**

After approximately 10-15 seconds you will receive a message that the license is correctly uploaded.

After that the following screen appears:

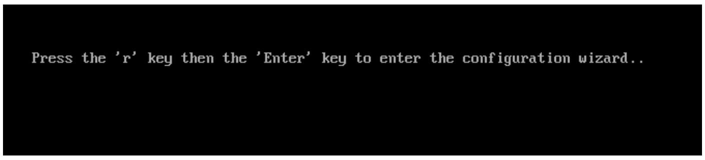


The default password of the user-interface is `admin`.

It is strongly recommended to change/update this password and store it in a secure location. Please make sure that you document and store this password in a secure place.

If the password is lost, you can reset the LiFi Controller Unit to it's default state by connecting a keyboard and monitor to the LiFi Controller Unit and reboot it.

When the following screen appears:



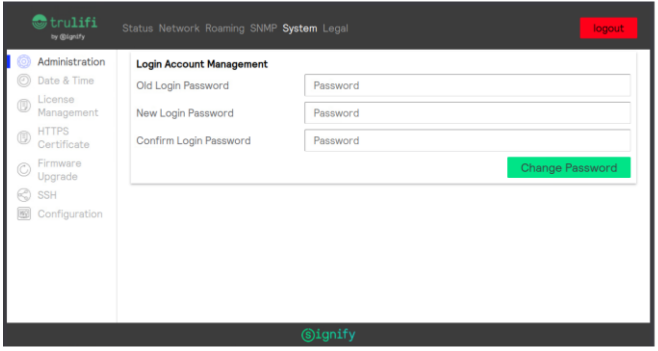
```
Press the 'r' key then the 'Enter' key to enter the configuration wizard..
```

Click the ' `r` ' key and then `Enter` to reset the system to factory defaults.

5.2 Login password

The Controller UI is protected by a password that can be changed:
The default login password is `admin`.
It is strongly recommended to change/update this login password and store it in a secure location. If the login password is lost the controller application needs to be returned to its default settings.

- Choose **System > Administration** to open the administration page.



- Enter the **previous password**, the **new password** and **confirm** the password. Passwords are case-sensitive and can contain from 7 to 32 ASCII characters. Password can contain spaces and special characters.
- Click `[Change Password]`

5.3 LAN settings

The controller can obtain an IP address from a DHCP server, or you can assign a static IP address. To select your preferred IP address method:

- Choose **Network > LAN Settings** to open the LAN Settings page.
- Depending on your network configuration select Dynamic or Static.
- In case of a dynamic IP address, all fields are filled-in automatically by the DHCP server and cannot be changed. Click the `[Dynamic]` button to validate your choice.
- In case of a static IP address, after having selected the `[Static]` button you are requested to provide the **IP Address, Subnet Mask, Gateway, DNS Server, Alternative DNS Server** information and then confirm your selection by clicking the `[Save]` button. Your selection is not confirmed as long as all fields are not correctly filled in.

By default, the Controller will use dynamic IP address.

5.4 Trulifi Encryption password

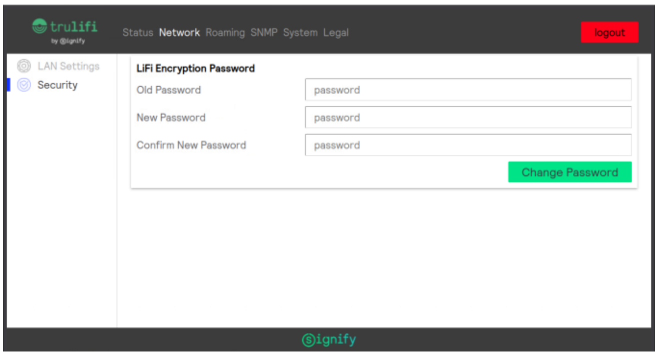
To create a secure connection between a LiFi access point and a USB key, the LiFi link is encrypted using a password. This LiFi encryption password must be configured in each access point and each USB key in the LiFi domain.

To facilitate this task, the controller can populate the new password in each access point in your LiFi domain. This automatic password change can only be performed on access points that are associated to your LiFi domain (the status page lists the associated access points). In case an access point is not connected or associated at that moment, the access point will be blocked i.e. no LiFi communication will be possible by this access point after reconnecting it. To unblock this access point, you need to resynchronize the passwords between the controller and this access point. Go to the web interface of the access point and change the LiFi encryption password manually (see "Trulifi 6002 USB key - User Manual).

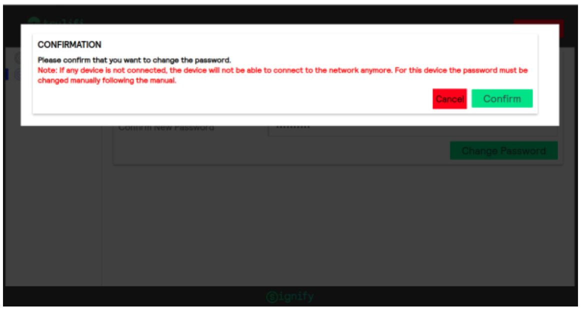
The controller cannot change the passwords of the USB keys. The passwords of the USB keys have to be configured manually (see "Trulifi 6002 USB key - User Manual").

To change the LiFi encryption password from the controller:

- Choose **Network > Security** to open the security page.
- Enter the **previous password**, the **new password** and **confirm** the password. Passwords are case-sensitive and can contain from 7 to 32 ASCII characters. Password can contain spaces and special characters.



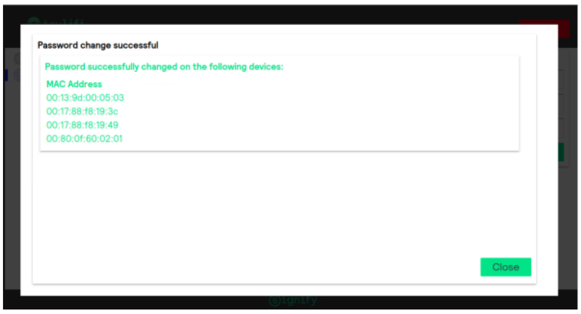
Click **`[Change Password]`**.



CONFIRMATION

Please confirm that you want to change the password.

Note: If any device is not connected, the device will not be able to connect to the network anymore. For this device the password must be changed manually following the manual.



Password change successful

Password successfully changed on the following devices:

MAC Address
00:13:9d:00:05:03
00:17:88:f8:19:3c
00:17:88:f8:19:49
00:80:0f:60:02:01

The default password for every 6002 Access Point, USB key and controller is **`trulifi`**.

It is strongly recommended to change/update the encryption password and store it in a secure location.
If the encryption password is lost the controller application needs to be returned to its default settings.

5.5 Date and time

The system time on your controller is based on the Universal Time Clock. The UTC is automatically set up from an internet time server. Two server URL addresses can be selected. The time zone can be manually adjusted to reflect your current region. To change the time setting:

- Choose **System > Date & Time** to open the date page.
- From the **Time zone** drop-down list, choose the Country/City.
- In the **Time-Server** text box, enter an internet time server.
- In the **Alternative Time-Server** text box, enter a second internet time server.
- Click **`[Save]`** to confirm the change.

The controller is provided with two default Time server URL addresses.

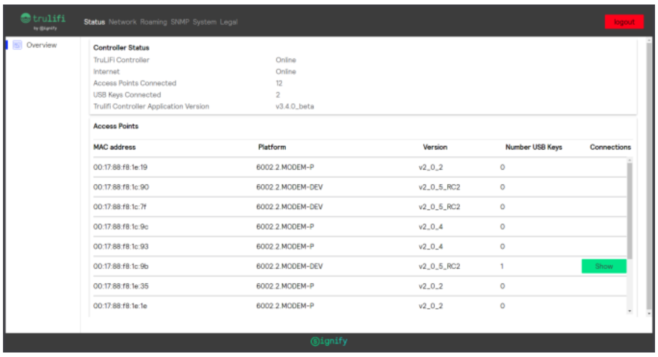
After setting al parameters, logout from the controller:

- Click Logout in the top right corner of the page to complete the log out process and prevent unauthorized users from accessing the controller GUI.
- System will automatically logout the user after 15 minutes of inactivity.

6 Advanced configuration

6.1 Controller status

The controller status page provides information about the controller and the LiFi domain.



Controller Status

TruLiFi Controller	Online
Internet	Online
Access Points Connected	12
USB Keys Connected	2
Trulifi Controller Application Version	v3.4.0_beta

Access Points

MAC address	Platform	Version	Number USB Keys	Connections
00:17:88:f8:1e:19	6002.2.MODEM-P	v2_0_2	0	
00:17:88:f8:1c:90	6002.2.MODEM-DEV	v2_0_5_RC2	0	
00:17:88:f8:1c:7f	6002.2.MODEM-DEV	v2_0_5_RC2	0	
00:17:88:f8:1c:9c	6002.2.MODEM-P	v2_0_4	0	
00:17:88:f8:1c:93	6002.2.MODEM-P	v2_0_4	0	
00:17:88:f8:1c:9b	6002.2.MODEM-DEV	v2_0_5_RC2	1	Show
00:17:88:f8:1e:35	6002.2.MODEM-P	v2_0_2	0	
00:17:88:f8:1e:1e	6002.2.MODEM-P	v2_0_2	0	

Controller status information

The Controller text field can be:

- Detecting: Network internet connection detection is ongoing.
- Offline: Something went wrong during the start-up of the controller. An additional pop-up message on the bottom side screen will give the user further information (e.g.: no network detected, ….).
- Online: Everything is up and running.

The Internet text field can be:

- Detecting: Network internet connection detection is ongoing.
- Offline: Controller is not connected to a network backbone.
- Online: Network backbone connection found.

LiFi domain devices information

The controller manages one or more LiFi domains. Domains consists of one access point and one or more USB keys. To allow for USB Keys to connect to multiple domains, all domains must be protected with the same LiFi encryption password. This password must be the same for every access point and USB key in the domain. Any access point or USB key that does not have the same LiFi encryption password will be rejected from the domain.

- Access Points without the correct password will not be authorized to communicate with a USB key, even with USB keys configured with the same password as the controller
- USB keys without the correct password will not be able to connect to any access points, even with access points configured with the same password as the controller.

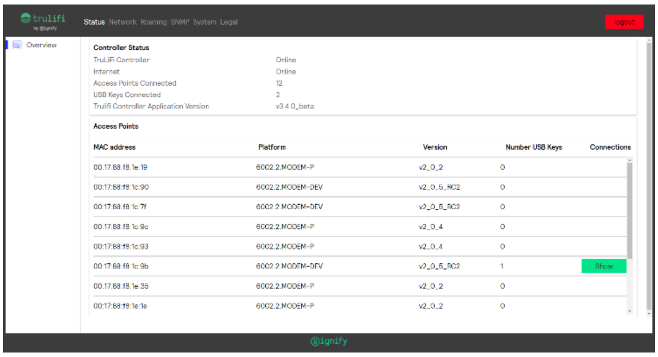
It is not possible to create separate VLANs managed by one controller or Access Point.

The following text fields indicate the number of devices associated to the domain:

- **Access Points Connected** text field indicates the number of access points connected and associated to the controller.
- **USB Keys Connected** text field indicates the number of USB keys connected to the domain.

Further details per access point can be found in the Access Points table at the bottom of status page:

- Access point MAC address
- Access point platform revision
- Firmware version of the Access point
- Number of USB keys associated with the access point.



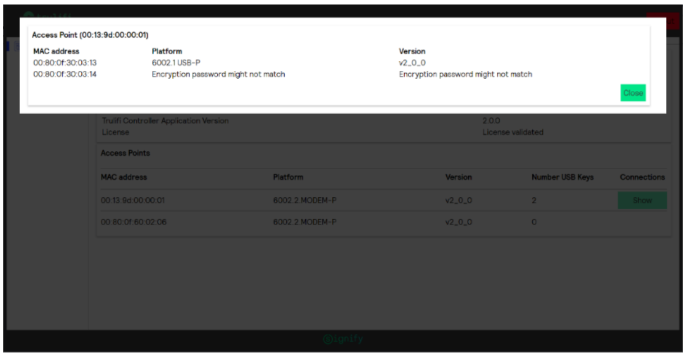
Controller Status

TruLiFi Controller	Online
Internet	Online
Access Points Connected	12
USB Keys Connected	2
Trulifi Controller Application Version	v3.4.0_beta

Access Points

MAC address	Platform	Version	Number USB Keys	Connections
00:17:88:f8:1e:19	6002.2.MODEM-P	v2_0_2	0	
00:17:88:f8:1c:90	6002.2.MODEM-DEV	v2_0_5_RC2	0	
00:17:88:f8:1c:7f	6002.2.MODEM-DEV	v2_0_5_RC2	0	
00:17:88:f8:1c:9c	6002.2.MODEM-P	v2_0_4	0	
00:17:88:f8:1c:93	6002.2.MODEM-P	v2_0_4	0	
00:17:88:f8:1c:9b	6002.2.MODEM-DEV	v2_0_5_RC2	1	Show
00:17:88:f8:1e:35	6002.2.MODEM-P	v2_0_2	0	
00:17:88:f8:1e:1e	6002.2.MODEM-P	v2_0_2	0	

If at least one USB key is attached to the access point, a green button **Show** can be clicked to open an extra window giving further details for every USB key associated with it:



Access Point (00:13:9d:00:00:01)

MAC address	Platform	Version
00:80:0f:30:03:13	6002.1 USB-P	v2_0_0
00:80:0f:30:03:14	Encryption password might not match	Encryption password might not match

Trulifi Controller Application Version	2.0.0
License	License validated

Access Points

MAC address	Platform	Version	Number USB Keys	Connections
00:13:9d:00:00:01	6002.2.MODEM-P	v2_0_0	2	Show
00:80:0f:60:02:06	6002.2.MODEM-P	v2_0_0	0	

For every USB key, you can find the following information:

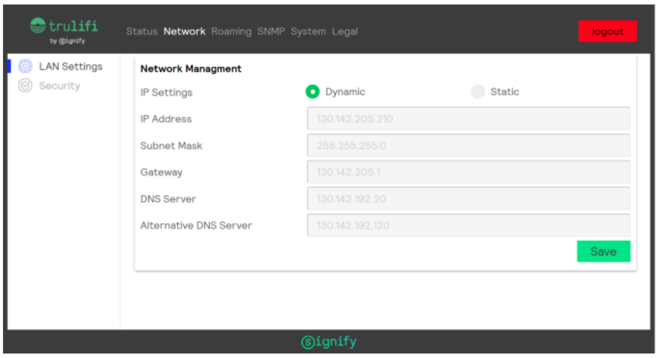
- USB key MAC address
- USB key platform revision
- Firmware version of the USB key

Note: every USB key that is not configured with the correct LiFi encryption password is detected and reported as: **Encryption password might not match**.

The access point table is not refreshed automatically. Please click the refresh button of your web browser to update the information. Use the Roaming overview page to track the devices in the LiFi domain in real-time.

6.2 Network Settings

In the tab **Network** the Network Management settings of the network can be seen.



Network Managment

IP Settings	● Dynamic	○ Static
IP Address	130.142.205.210	
Subnet Mask	255.255.255.0	
Gateway	130.142.205.1	
DNS Server	130.142.192.20	
Alternative DNS Server	130.142.192.120	

Trulifi Controller 6800 network settings are standard pre-configured with DHCP on. If required by selecting **Static**, the IP settings (IP-address, Subnet-mask, Gateway and DNS server) can be changed.
Select **[Save]** to save any changes made.

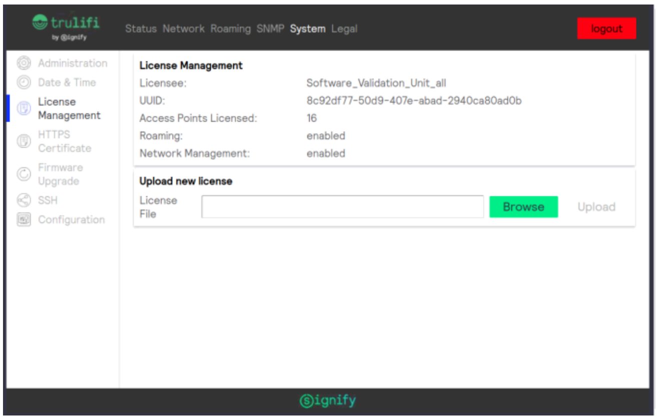
6.3 Roaming overview

Roaming allows the system operator to configure larger LiFi systems and have users roam from one domain (Access Point) to another domain. Roaming requires a license and is only available on the Trulifi 6002.2 Access Point.

6.3.1 Activation of ROAMING license

If a ROAMING license has been obtained, please save this license key file ***xxxxxxxx.lic*** in a known location, eg. Desktop.

Choose **System > License Management**



License Management
Licensee: Software_Validation_Unit_all
UUID: 8c92df77-50d9-407e-abad-2940ca80ad0b
Access Points Licensed: 16
Roaming: enabled
Network Management: enabled

Upload new license
License File

Select the ***xxxxxx.lic*** license file from the saved location.

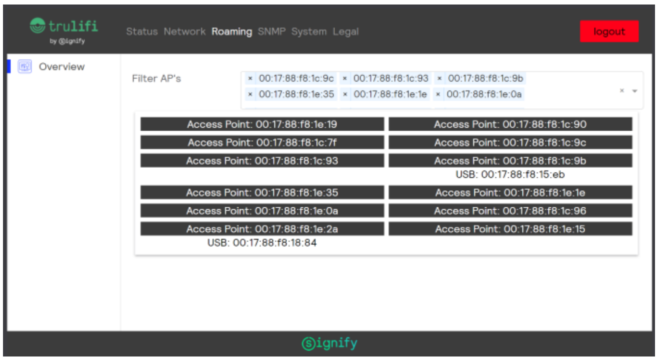
Select **[Upload]**

Once the license file is uploaded the available functions are visible in the **License Management** screen.

6.3.2 ROAMING settings

The roaming page gives an overview of the LiFi domain devices in real-time. The roaming screen shows the access points and USB keys currently associated with the LiFi domain.

A filter can be used to select which access points you want to display. A drop-down list and two buttons can be used to configure this filter. The buttons **[clear all]** and **[select all]** allow to quickly select/unselect the full list. It is also possible to select the access points one by one by ticking the checkbox associated to each access point's MAC address.



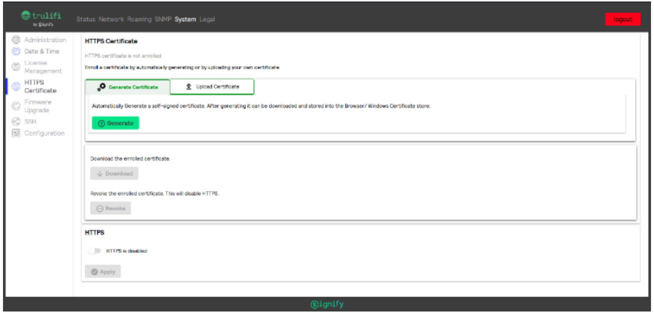
Filter AP's: × 00:17:88:f8:1c:9c × 00:17:88:f8:1c:93 × 00:17:88:f8:1c:9b × 00:17:88:f8:1e:35 × 00:17:88:f8:1e:1e × 00:17:88:f8:1e:0a

Access Point: 00:17:88:f8:1e:19
Access Point: 00:17:88:f8:1c:90
Access Point: 00:17:88:f8:1c:7f
Access Point: 00:17:88:f8:1c:9c
Access Point: 00:17:88:f8:1c:93
Access Point: 00:17:88:f8:1c:9b
USB: 00:17:88:f8:15:eb
Access Point: 00:17:88:f8:1e:35
Access Point: 00:17:88:f8:1e:1e
Access Point: 00:17:88:f8:1e:0a
Access Point: 00:17:88:f8:1c:96
Access Point: 00:17:88:f8:1e:2a
USB: 00:17:88:f8:18:84
Access Point: 00:17:88:f8:1e:15

6.4 Installing HTTPS-certificate

6.4.1 Introduction

This paragraph describes the usage of the HTTPS settings webpage from the LiFi-Controller found under "System -> HTTPS Certificate". The purpose of this webpage is to set-up an encrypted HTTPS connection to the LiFi-Controller. By default, the webserver uses an unencrypted HTTP connection. HTTPS is enabled by enrolling a HTTPS certificate into the LiFi-Controller. This process as well as the certificate handling will also be described in this document.



HTTPS Certificate
HTTPS certificate is not enrolled
Enroll a certificate by automatically generating or by uploading your own certificate.
Automatically Generate a self-signed certificate. After generating it can be downloaded and stored into the Browser/ Windows Certificate store.
Download the enrolled certificate.
Revoke the enrolled certificate. This will disable HTTPS.
HTTPS
HTTPS is disabled

Picture: HTTPS certificate Web UI, no certificate enrolled

6.4.2 Enrolling a certificate

There are two ways how to enroll a certificate into the LiFi-Controller. A certificate can be automatically generated by the LiFi-Controller, or an existing certificate can be uploaded to the LiFi-Controller. After enrolling the certificate, the switch to enable HTTPS will become available.

6.4.2.1 Automatically generate a certificate

A certificate will be generated by the LiFi-Controller when clicking the "Generate" button on the webpage. This option is applicable for users that do not have the capability to generate their own trusted certificate. The generated certificate will be self-signed, and it uses a 4096-bit RSA keypair. The Common Name of the certificate subject is "**trulifi-controller.local**", which is the domain name of the LiFi-Controller.

6.4.2.2 Upload a certificate

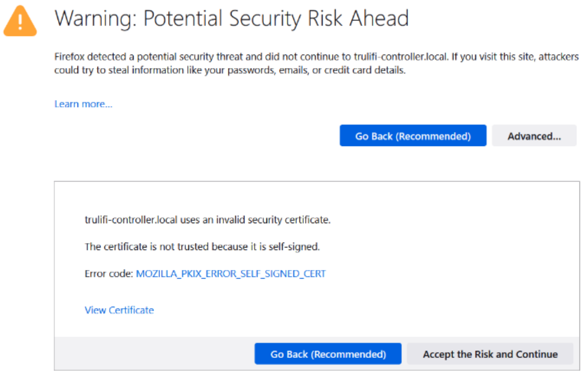
This option makes sense for users that already have their own certificate chain. An organization that has a certificate signed by a trusted Certificate Authority (CA) can generate and sign their own application certificates. The application certificates can then be verified by the organization certificate. An application certificate that will be used for the LiFi-Controller should use "**trulifi-controller.local**" as its Common Name. A certificate bundle file in PEM format must be created. This file consists of certificates and a private key concatenated in the following order:

1. Application certificate for the LiFi-Controller.

2. (If applicable) Intermediate certificates from the certificate chain. Each certificate should be verifiable by the following one. The last certificate should be verifiable by a certificate trusted by the browser.
3. Private key that was used to sign the application certificate.

6.4.3 Trusting a certificate

To be able to access the website via HTTPS, it should be ensured that the enrolled certificate is trusted by the browser. The procedure for trusting a certificate will be explained for Mozilla Firefox, Google Chrome, and Microsoft Edge. Firefox uses its own certificate store whereas Chrome and Edge are using the certificate store from Windows.
When enabling HTTPS on the webpage before the certificate is trusted, a warning page will show. When HTTPS is enabled, the website will always try to redirect to HTTPS.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to trulifi-controller.local. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...

Go Back (Recommended) | Advanced...

trulifi-controller.local uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

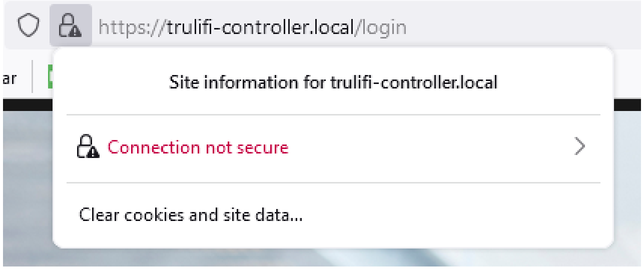
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

Go Back (Recommended) | Accept the Risk and Continue

Picture: Warning page Firefox (untrusted self-signed certificate)

An exception for the website can always be made for every browser, even when the certificate is not trusted. On the Warning Page click on “Advanced…” and on “Accept Risk and Continue”. This way the LiFi-Controller website can be accessed via HTTPS, but a warning in the lock icon in the address bar will be displayed.



https://trulifi-controller.local/login

Site information for trulifi-controller.local

Connection not secure

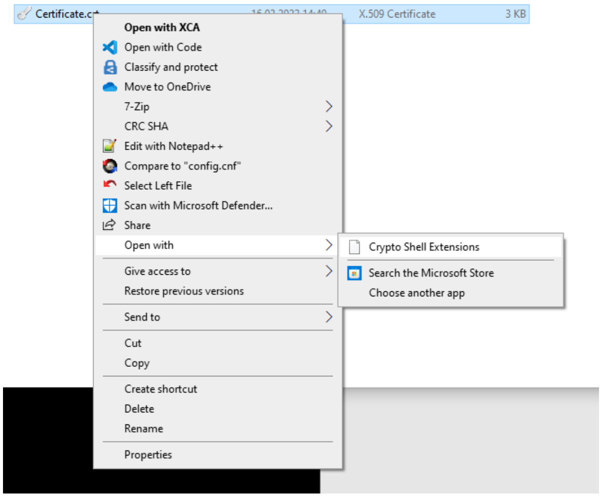
Clear cookies and site data...

Picture: Address Bar Warning Firefox

The following sections will describe how to set-up the automatically generated certificate so the warning will not show, if possible. In the case of the uploaded certificate, it should be ensured that the organization certificate is correctly set-up in the browser/ Windows certificate store, so it can be used to verify the uploaded application certificate.

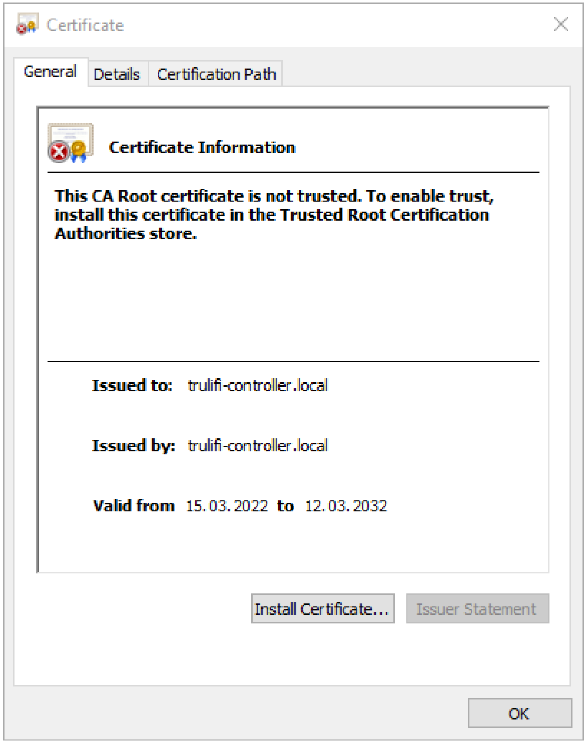
6.4.3.1 Setting up a certificate for Chrome/ Edge

The enrolled certificate can be downloaded by using the **`[Download]`** button on the webpage. After downloading, right-click on the downloaded .crt file. In the context menu click on **`[Open with]`** and on **`[Crypto Shell Extensions]`**.



Picture: Certificate Context Menu

On the opened window click on **`[Install Certificate…]`**.



Certificate

General | Details | Certification Path

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: trulifi-controller.local

Issued by: trulifi-controller.local

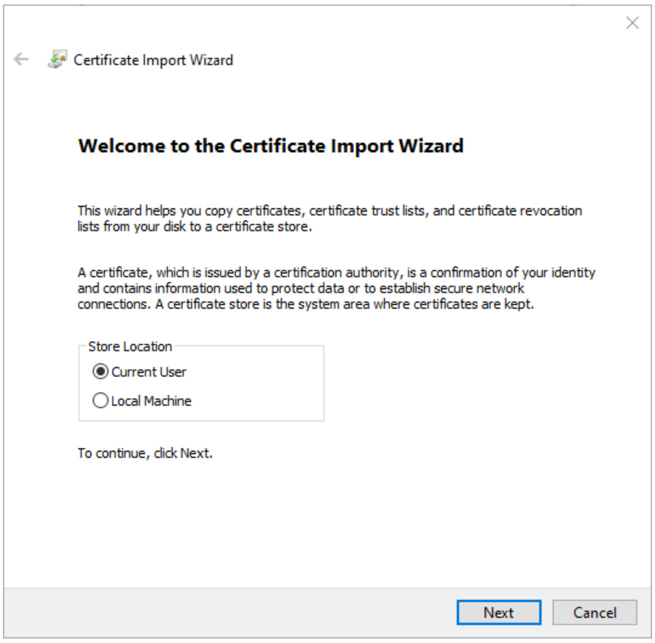
Valid from 15. 03. 2022 **to** 12. 03. 2032

Install Certificate... | Issuer Statement

OK

Picture: Install certificate step 1

Select whether the certificate should be stored at the user or machine level. Click **`[Next]`**.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

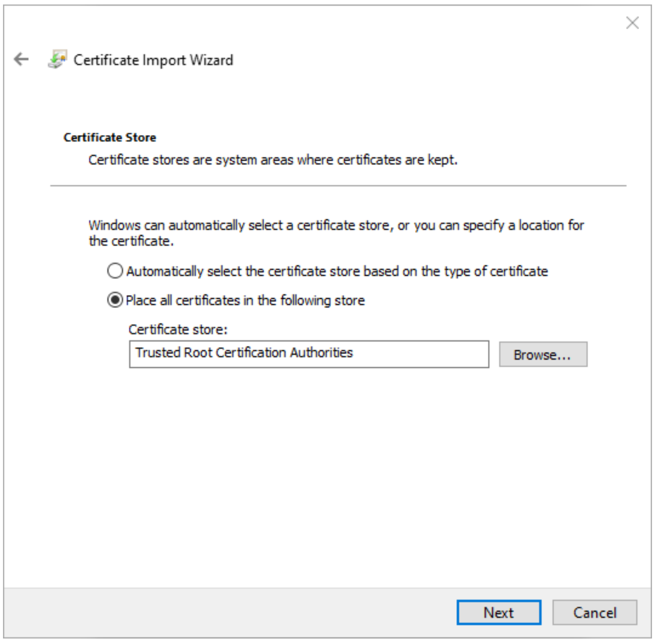
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
● Current User
○ Local Machine

To continue, click Next.

Picture: Install certificate step 2

Select `[Place all certificates in the following store]`. Click on `[Browse]` and select `[Trusted Root Certification Authorities]`. Click `[Next]`.



Certificate Store
Certificate stores are system areas where certificates are kept.

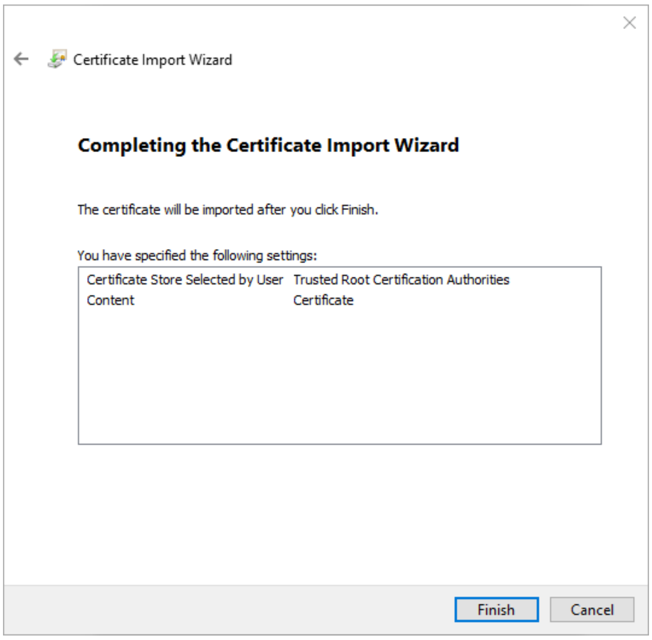
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

Picture: Install certificate step 3

Click `[Finish]`.



Completing the Certificate Import Wizard

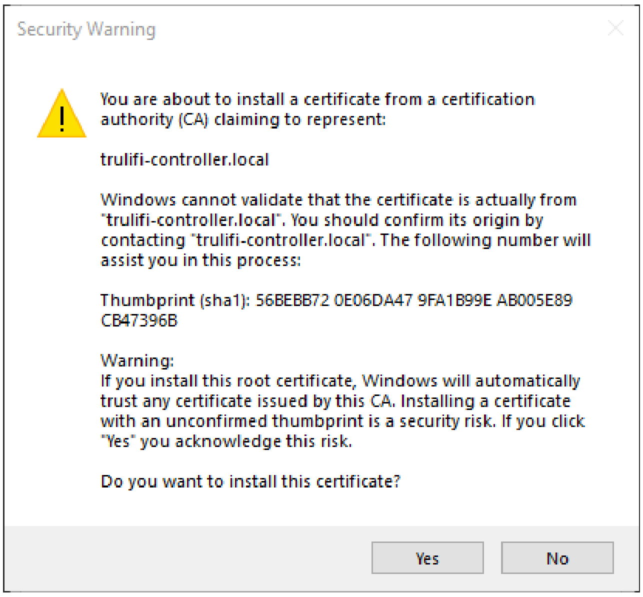
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Picture: Install certificate step 4

Accept the warning by clicking on `[Yes]`.



You are about to install a certificate from a certification authority (CA) claiming to represent:

trulifi-controller.local

Windows cannot validate that the certificate is actually from "trulifi-controller.local". You should confirm its origin by contacting "trulifi-controller.local". The following number will assist you in this process:

Thumbprint (sha1): 56BEBB72 0E06DA47 9FA1B99E AB005E89 CB47396B

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

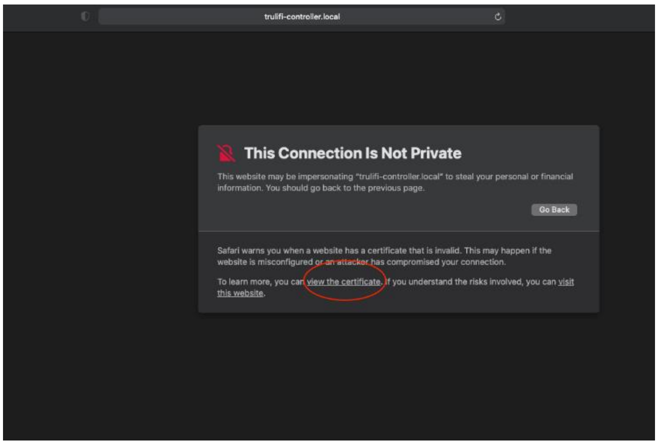
Picture: Install certificate step 5

After the certificate is installed in Windows, HTTPS can be enabled on the LiFi-Controller webpage. The browser will redirect to HTTPS without showing a warning page. The lock icon in the address bar will say that the connection is secure.

6.4.3.2 Setting up a certificate in Safari

Safari does not trust the automatically generated self-signed certificate. It only makes the website accessible.

First enable HTTPS on the webpage by toggling the HTTPS switch and Clicking the **`[Apply]`** button. The browser should redirect and show a warning page.



trulifi-controller.local

This Connection Is Not Private

This website may be impersonating "trulifi-controller.local" to steal your personal or financial information. You should go back to the previous page.

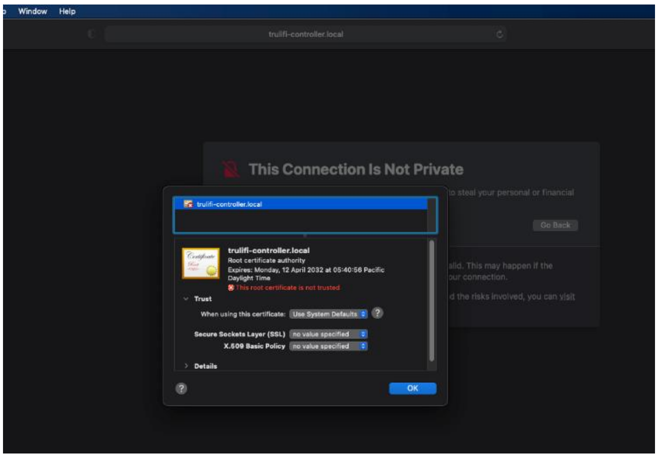
Go Back

Safari warns you when a website has a certificate that is invalid. This may happen if the website is misconfigured or an attacker has compromised your connection.

To learn more, you can view the certificate. If you understand the risks involved, you can visit this website.

Picture: *Warning page safari (untrusted self-signed certificate)*

Click on **`[View Certificates…]`**.



This Connection Is Not Private

trulifi-controller.local

trulifi-controller.local
Root certificate authority
Expires: Monday, 12 April 2032 at 05:40:56 Pacific Daylight Time
This root certificate is not trusted

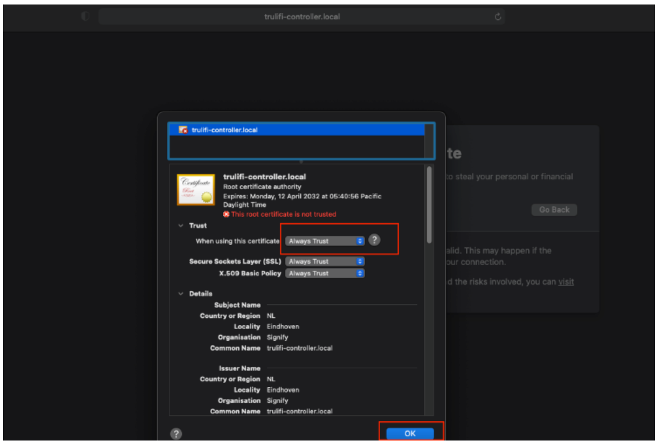
Trust
When using this certificate: Use System Defaults
Secure Sockets Layer (SSL) no value specified
X.509 Basic Policy no value specified

Details

OK

Picture: safari certificate settings

Click on the "Trust" -> "when using this certificate" and select **`[Always Trust]`** and click **`[ok]`** to Confirm certificate Exception.



trulifi-controller.local

trulifi-controller.local
Root certificate authority
Expires: Monday, 12 April 2032 at 05:40:56 Pacific Daylight Time
This root certificate is not trusted

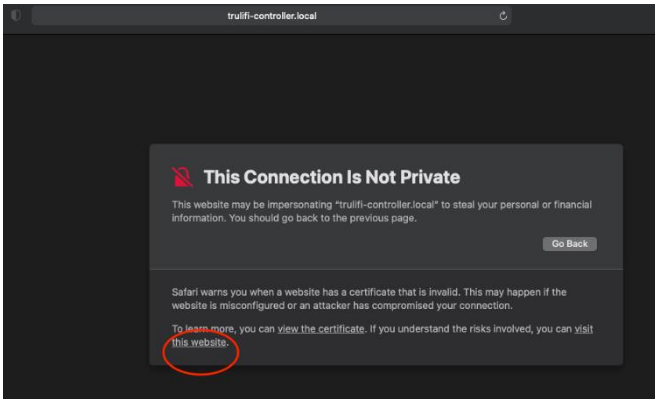
Trust
When using this certificate Always Trust
Secure Sockets Layer (SSL) Always Trust
X.509 Basic Policy Always Trust

Details
Subject Name
Country or Region NL
Locality Eindhoven
Organisation Signify
Common Name trulifi-controller.local

Issuer Name
Country or Region NL
Locality Eindhoven
Organisation Signify
Common Name trulifi-controller.local

OK

Picture: safari certificate trust settings



trulifi-controller.local

This Connection Is Not Private

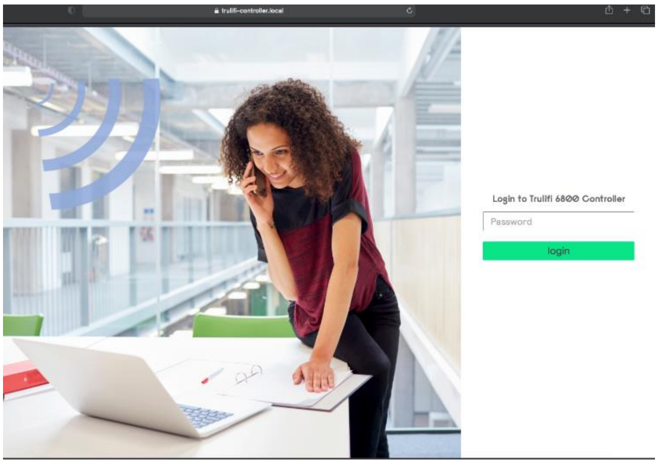
This website may be impersonating "trulifi-controller.local" to steal your personal or financial information. You should go back to the previous page.

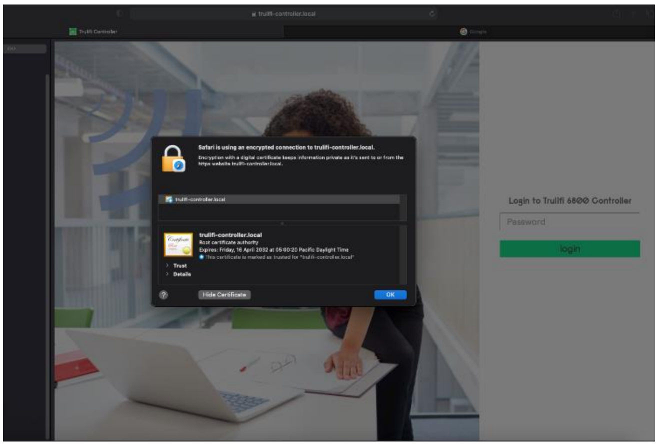
Go Back

Safari warns you when a website has a certificate that is invalid. This may happen if the website is misconfigured or an attacker has compromised your connection.

To learn more, you can view the certificate. If you understand the risks involved, you can visit this website.

Click on **`[you can visit this website]`**, the LiFi-Controller website the warning page will go away, and the website can be accessed and no warning in the address bar.





Safari is using an encrypted connection to trulifi-controller.local.

Encryption with a digital certificate keeps information private as it's sent to or from the https website trulifi-controller.local.

trulifi-controller.local

trulifi-controller.local
Root certificate authority
Expires: Friday, 16 April 2032 at 05:00:20 Pacific Daylight Time
This certificate is marked as trusted for "trulifi-controller.local"

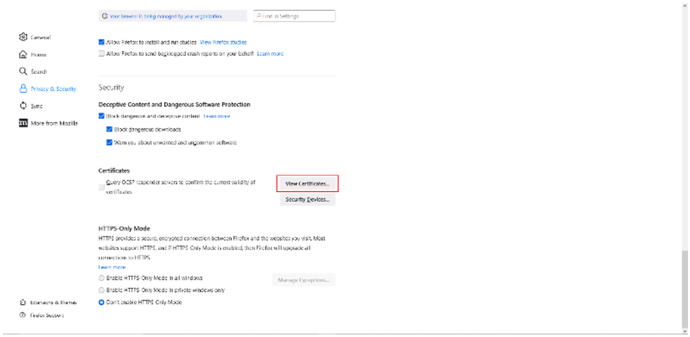
Click on **`[view certificate]`**

6.4.3.3 Setting up a certificate in Firefox

The following description will have the same effect as clicking on "**Accept Risk and Continue**" on the warning page. Firefox will never trust the automatically generated self-signed certificate. It only makes the website accessible.

First enable HTTPS on the webpage by toggling the HTTPS switch and clicking the **`[Apply]`** button. The browser should redirect and show a warning page.

Open the Firefox Settings. Click on **`[Privacy & Security]`** on the left. Scroll down and click on **`[View Certificates…]`**.



Your browser is being managed by your organization

☑ Allow Firefox to install and run studies View Firefox studies
□ Allow Firefox to send backlogged crash reports on your behalf Learn more

Security

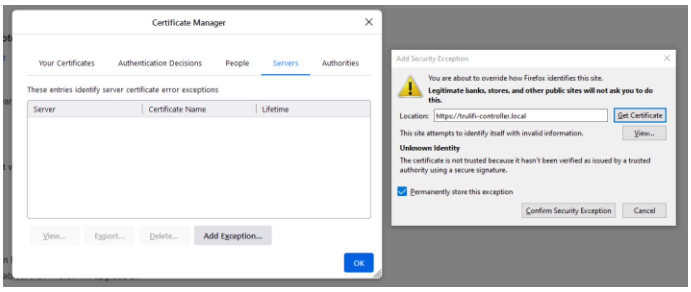
Deceptive Content and Dangerous Software Protection
☑ Block dangerous and deceptive content Learn more
☑ Block dangerous downloads
☑ Warn you about unwanted and uncommon software

Certificates
□ Query OCSP responder servers to confirm the current validity of certificates

HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.
Learn more
○ Enable HTTPS-Only Mode in all windows
○ Enable HTTPS-Only Mode in private windows only
● Don't enable HTTPS-Only Mode

Picture: Firefox Settings

Click on the **`[Servers]`** tab and then on **`[Add Exception…]`**. Enter "**https://trulifi-controller.local**" into the location text field. Click on **`[Get Certificate]`** and then on **`[Confirm Security Exception]`**. This will create an exception for the website. The certificate will also be automatically listed in the "Authorities" tab.



Certificate Manager

These entries identify server certificate error exceptions

Server	Certificate Name	Lifetime

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://trulifi-controller.local

This site attempts to identify itself with invalid information.

Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

Picture 1: Add a website exception in Firefox

When reloading the LiFi-Controller website the warning page will go away and the website can be accessed. The warning in the address bar will show regardless.

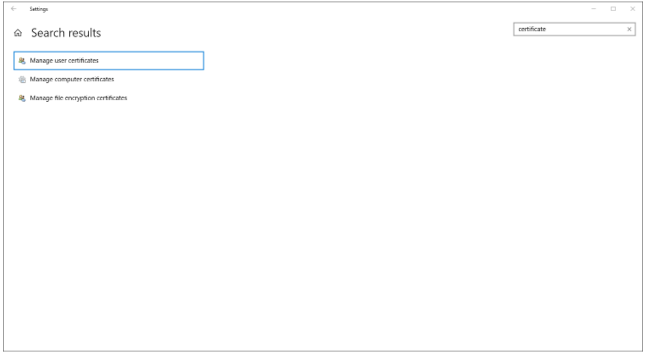
6.4.4 Revoking a certificate

6.4.4.1 Revoking a certificate on the website

After a certificate is enrolled on the HTTPS webpage, the "Revoke" button becomes available. After Clicking the button, the enrolled certificate inside the LiFi-Controller will be deleted and the website will be redirected to HTTP again. If the revoked certificate was stored inside the browser or Windows certificate store, it should also be deleted from there.

6.4.4.2 Revoking a certificate in Windows

Open the Windows Settings and search for "**certificate**".



Settings

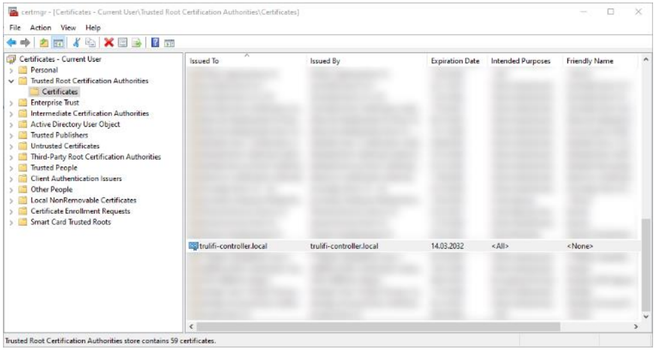
Search results

certificate

Manage user certificates
Manage computer certificates
Manage file encryption certificates

Picture: Certificate Windows Settings

Depending on if the certificate was stored in the user certificate store or the machine-wide certificate store, click **on `[Manage user certificates]`** or on **`[Manage computer certificates]`**. In the certificate manager open the folder "**Trusted Root Certification Authorities/Certificates**".



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

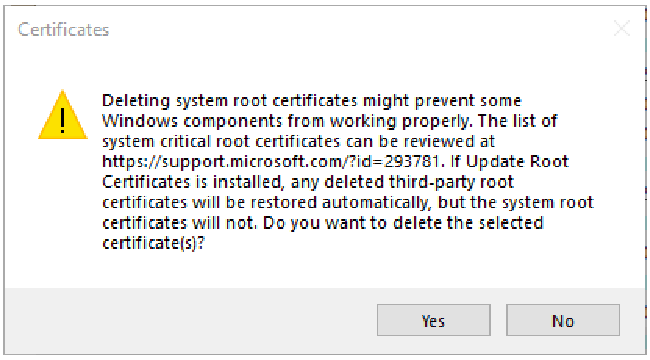
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Other People
Local NonRemovable Certificates
Certificate Enrollment Requests
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
trulifi-controller.local	trulifi-controller.local	14.03.2032	<All>	<None>

Trusted Root Certification Authorities store contains 59 certificates.

Picture: Windows certificate store

Find the certificate issued to "**trulifi-controller.local**". Right-click on the entry and click on **`[Delete]`**. Accept the warning by clicking on **`[Yes]`**.



Certificates

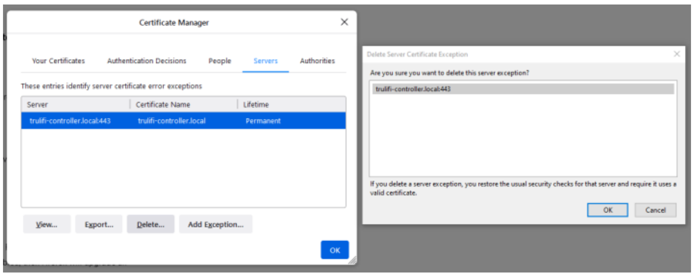
Deleting system root certificates might prevent some Windows components from working properly. The list of system critical root certificates can be reviewed at https://support.microsoft.com/?id=293781. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?

Picture: Windows delete certificate warning

6.4.4.3 Revoking a certificate in Firefox

Open the certificate settings in Firefox like described in paragraph "6.4.3.2. Setting up a certificate in Firefox". Select the entry "**trulifi-**

controller.local” in the “**Servers**” tab and click on `[Delete…]`. Accept by clicking on `[OK]`.



Certificate Manager

These entries identify server certificate error exceptions

Server	Certificate Name	Lifetime
trulifi-controller.local:443	trulifi-controller.local	Permanent

Delete Server Certificate Exception

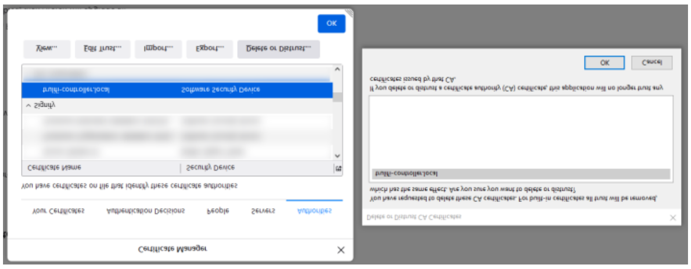
Are you sure you want to delete this server exception?

trulifi-controller.local:443

If you delete a server exception, you restore the usual security checks for that server and require it uses a valid certificate.

Picture: Delete website exception in Firefox

Select the entry “**trulifi-controller.local**” in the “Authorities” tab and click on `[Delete or Distrust…]`. Accept by clicking `[OK]`.



Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌃ Signify	
trulifi-controller.local	Software Security Device

Delete or Distrust CA Certificates

You have requested to delete these CA certificates. For built-in certificates all trust will be removed, which has the same effect. Are you sure you want to delete or distrust?

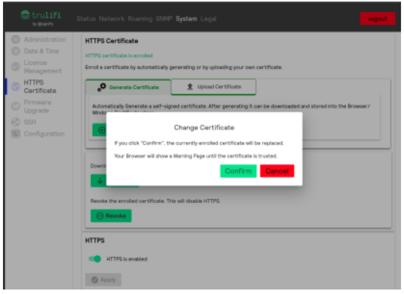
trulifi-controller.local

If you delete or distrust a certificate authority (CA) certificate, this application will no longer trust any certificates issued by that CA.

Picture: Delete authority certificate in Firefox

6.4.4.4 Changing a certificate

When uploading or generating a certificate on the HTTPS webpage while a certificate is already enrolled, the old certificate will be deleted. The old certificate should also be deleted from the browser or Windows certificate store. The new certificate may be stored in the browser or Windows certificate store as described above to prevent the browser warning from showing



HTTPS Certificate

HTTPS certificate is enrolled

Enroll a certificate by automatically generating or by uploading your own certificate.

Automatically Generate a self-signed certificate. After generating it can be downloaded and stored into the Browser/ Windo…

Change Certificate

If you click "Confirm", the currently enrolled certificate will be replaced.

Your Browser will show a Warning Page until the certificate is trusted.

Revoke the enrolled certificate. This will disable HTTPS.

HTTPS

HTTPS is enabled

After generating or uploading the new certificate, the page will be refreshed.

6.5 Firmware upgrades

The controller can upgrade the following Trulifi devices:

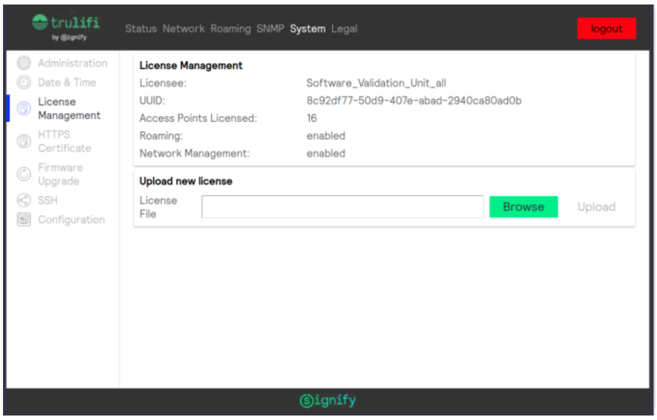
- Controller
- USB key
- Access Point

Registered customers will be notified in case a new firmware file is available for download.

After the new firmware is downloaded and stored on the client on a known location (eg. Desktop) files the LiFi controller can be upgraded.

To upgrade the Trulifi devices:

- Choose **System > Firmware Upgrade** to open the firmware update page.
- Click the **Browse** button, a file section appears.
- In the File Name to Install text box, enter the path to the firmware (*.zip)
- Click **Upload** to launch the upload.



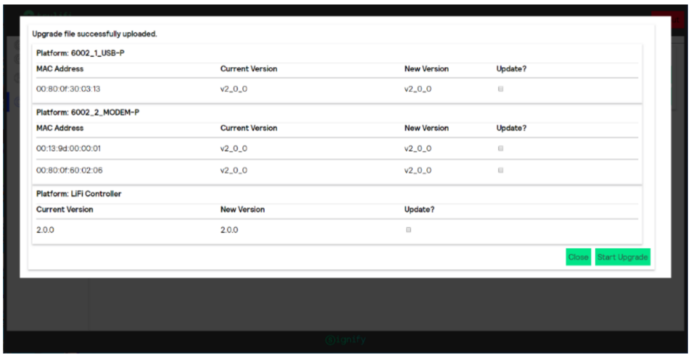
License Management

Licensee:	Software_Validation_Unit_all
UUID:	8c92df77-50d9-407e-abad-2940ca80ad0b
Access Points Licensed:	16
Roaming:	enabled
Network Management:	enabled

Upload new license

License File

The upload process might take several seconds before a new window appears showing the versioning status for the Trulifi devices.



Upgrade file successfully uploaded.

Platform: 6002_1_USB-P

MAC Address	Current Version	New Version	Update?
00:80:0f:30:03:13	v2_0_0	v2_0_0	□

Platform: 6002_2_MODEM-P

MAC Address	Current Version	New Version	Update?
00:13:9d:00:00:01	v2_0_0	v2_0_0	□
00:80:0f:60:02:06	v2_0_0	v2_0_0	□

Platform: LiFi Controller

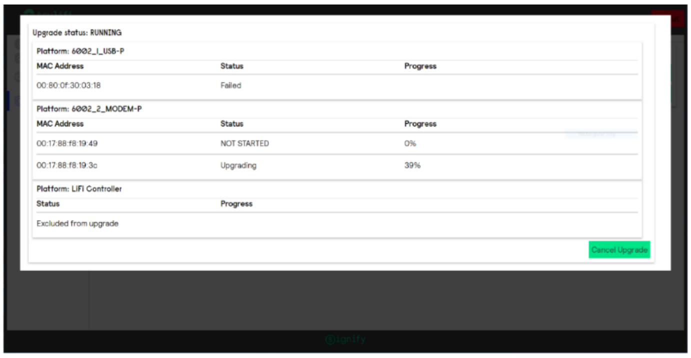
Current Version	New Version	Update?
2.0.0	2.0.0	□

In this new window, the current and new version columns give a status of the current firmware/software version per Trulifi device family:

- USB Key (6002_1_USB-P platform name)
- Access point (6002_2-MODEM-P platform name)
- LiFi controller

It is possible to select which device should be upgraded by ticking the corresponding checkbox in the update column and then click on the `[Start Upgrade]` button.

When the USB keys and access points are being updated, a percentage text gives information about the progress status.



Upgrade status: RUNNING

Platform: 6002_1_USB-P

MAC Address	Status	Progress
00:80:0f:30:03:18	Failed	

Platform: 6002_2_MODEM-P

MAC Address	Status	Progress
00:17:88:f8:19:49	NOT STARTED	0%
00:17:88:f8:19:3c	Upgrading	39%

Platform: LiFi Controller

Status	Progress
Excluded from upgrade	

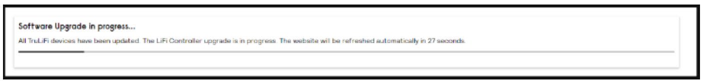
The Status column provides information about the upgrading steps:

- NOT STARTED
- Upgrading: progress indicates in percentage in the Progress column
- Succeeded
- Failed

Note 1: the controller performs the upgrade sequentially device per device and always in the same order: USB key, access point, Controller. If any of this device families are empty, it is skipped.

Note 2: the USB key upgrade is performed over the air, which means that any interruption of the LiFi link during this process will result in a failure, which will be reported in the progress status column with a **failed** status. In case of an access point or USB key upgrade failure, you have first to finish the current upgrade session. Then restart the complete upgrade procedure but this time selecting only the previously failing devices.
The same process applies for any USB keys not connected to the Access Point at the time of the firmware upgrade.

When the controller is being upgraded, a progress bar in a new window is displayed. After 30 seconds, when the upgrade is correctly finished, the login page appears.



Software Upgrade in progress...

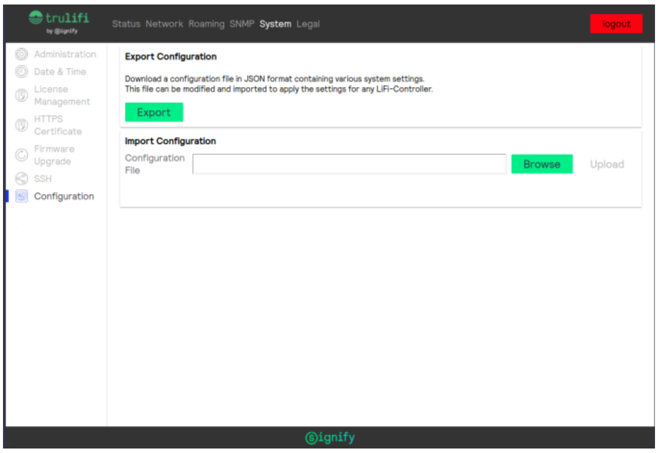
All TruLiFi devices have been updated. The LiFi Controller upgrade is in progress. The website will be refreshed automatically in 27 seconds.

When the upgrade session has terminated, click on the bottom right **close** button.

For any USB keys which were not connected to the LiFi-system during upgrade, a new firmware version needs to be pushed manually once these USB-keys are connected to the LiFi system.

6.6 Configuration export and import

The LiFi controller various system settings like network and time can be modified and imported to apply the settings for any LiFi-Controller.



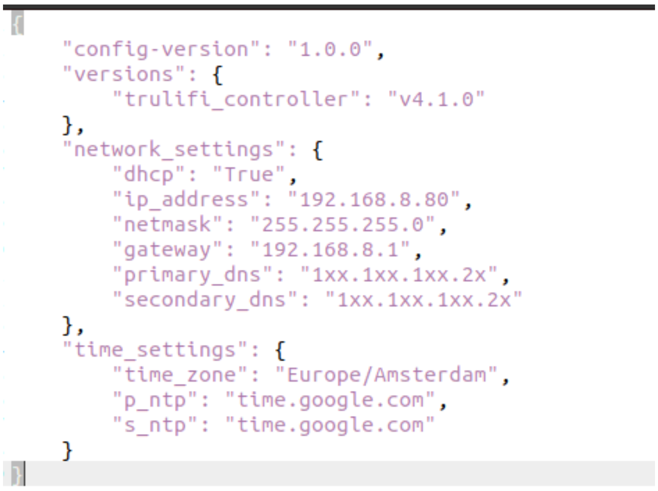
Export Configuration

Download a configuration file in JSON format containing various system settings.
This file can be modified and imported to apply the settings for any LiFi-Controller.

Import Configuration

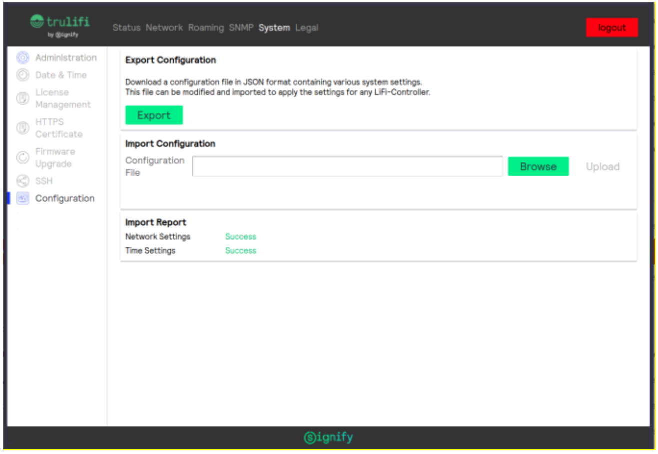
Configuration File

Export:
Click on the Button "Export”
A file “config.json” will be downloaded and contains LiFi controller "time_settings" and "network_settings”



```
{
    "config-version": "1.0.0",
    "versions": {
        "trulifi_controller": "v4.1.0"
    },
    "network_settings": {
        "dhcp": "True",
        "ip_address": "192.168.8.80",
        "netmask": "255.255.255.0",
        "gateway": "192.168.8.1",
        "primary_dns": "1xx.1xx.1xx.2x",
        "secondary_dns": "1xx.1xx.1xx.2x"
    },
    "time_settings": {
        "time_zone": "Europe/Amsterdam",
        "p_ntp": "time.google.com",
        "s_ntp": "time.google.com"
    }
}
```

Import:
create a copy of the exported “config.json” or modify settings and upload.



Export Configuration

Download a configuration file in JSON format containing various system settings.
This file can be modified and imported to apply the settings for any LiFi-Controller.

Import Configuration

Configuration File

Import Report

Network Settings	Success
Time Settings	Success

6.7 Legal

The LiFi controller is built upon several Open-Source Software packages. The complete list with the license details can be found in the “**Legal**” page.

7 SNMP MIB Integration

7.1 SNMP functionality

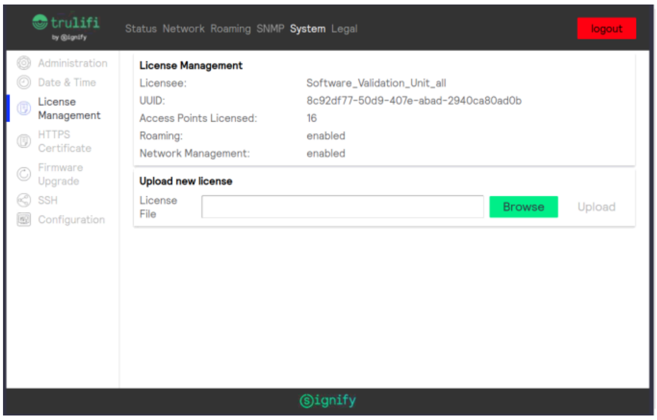
The Trulifi Controller application can be extended with a SNMP license. This allows system administrators to monitor the status of their Controllers and the respective connected Trulifi Access Points through Network Management Systems (NMS) via Simple Network Management Protocol (SNMP).
The LiFi MIB exposes over 360 Trulifi related parameters. These can be retrieved by an SNMP Management Application Platform or by Management Command-line Utilities, issuing SNMP GET Requests to the Trulifi Controller.

Additional, over 60 parameters can be modified using SNMP. These can be changed by an SNMP Management Application or by Management Command-line Utilities, issuing SNMP SET Requests to the Trulifi Controller.

The SNMP MIB provides access to among others the following parameters on the Access Point and/or dongle:

- General system information, memory status and CPU status of Access Point.
- Ethernet settings
- Interface objects and status
- DNS, DHCP and QoS settings.

If the controller is licensed with SNMP this will be shown in the Controller user interface.



License Management

Licensee: Software_Validation_Unit_all
UUID: 8c92df77-50d9-407e-abad-2940ca80ad0b
Access Points Licensed: 16
Roaming: enabled
Network Management: enabled

Upload new license

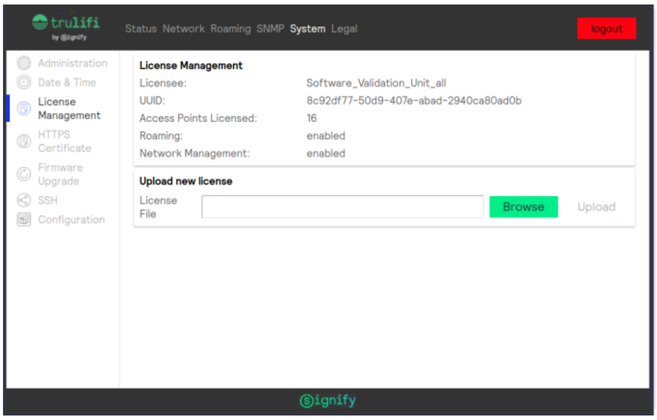
License File

To obtain a SNMP license please contact: customercare.trulifi@signify.com

7.2 Activation of SNMP license

If a SNMP license has been obtained, please save this license key file *xxxxxxxx.lic* in a known location, eg. Desktop.

Choose **System > License Management**



License Management

Licensee: Software_Validation_Unit_all
UUID: 8c92df77-50d9-407e-abad-2940ca80ad0b
Access Points Licensed: 16
Roaming: enabled
Network Management: enabled

Upload new license

License File

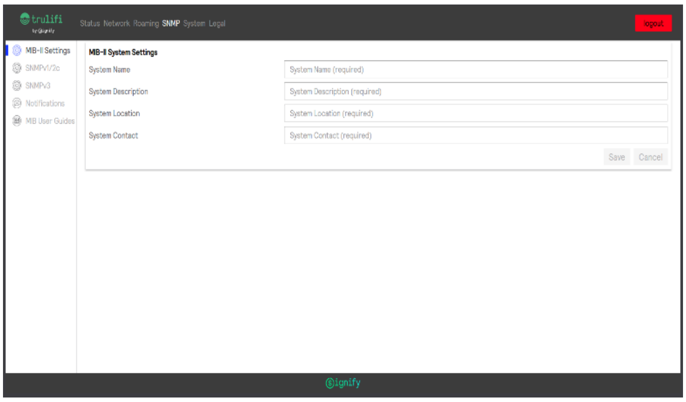
Select the xxxxxx.lic license file from the saved location.

Select **`[Upload]`**

Once the license file is uploaded the available functions are visible in the **License Management** screen.

7.3 Configuration of SNMP

After the SNMP license is uploaded and activated, select **SNMP > `MIB-II System Settings`** to conPicture the mandatory MIB-II system parameters.

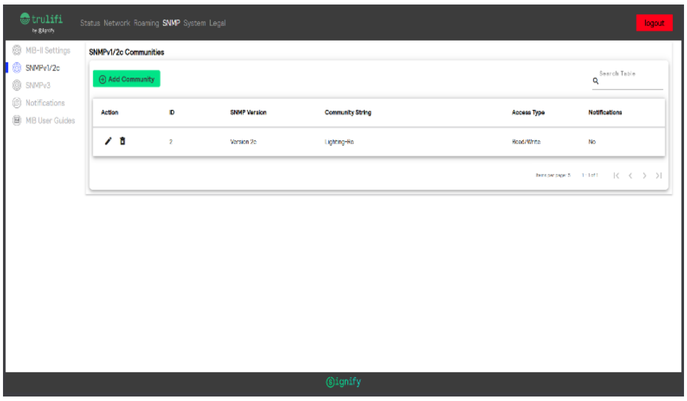


MIB-II System Settings

System Name: System Name (required)
System Description: System Description (required)
System Location: System Location (required)
System Contact: System Contact (required)

Community Strings for specific SNMP Version 1, 2c or 3 can be enabled by selecting **`SNMP> SNMPv1/2c`** and or **`SNMPv3`**. Select **`[Save]`** after entering in the parameters.

`SNMPv1/2c`

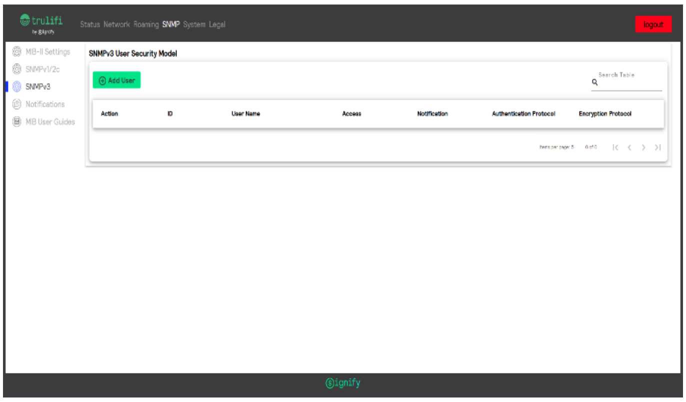


SNMPv1/2c Communities

Action	ID	SNMP Version	Community String	Access Type	Notifications
✎ 🗑	2	Version 2c	Lighting-Ro	Read/Write	No

Items per page: 5 1 - 1 of 1

SNMPv3

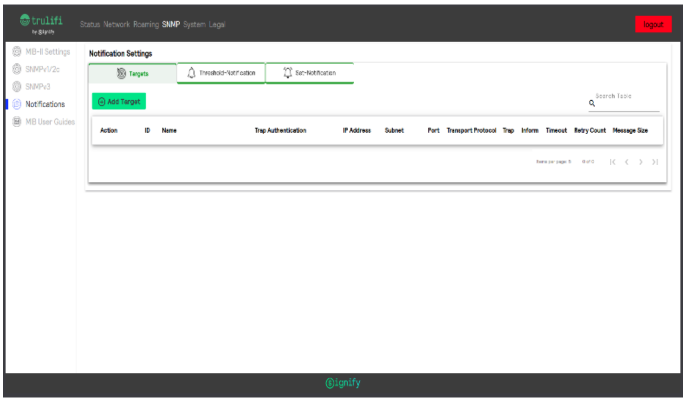


SNMPv3 User Security Model

Action	ID	User Name	Access	Notification	Authentication Protocol	Encryption Protocol

Configuring notifications such as target traps, thresholds and notifications can be set by selecting **SNMP> Notifications.**

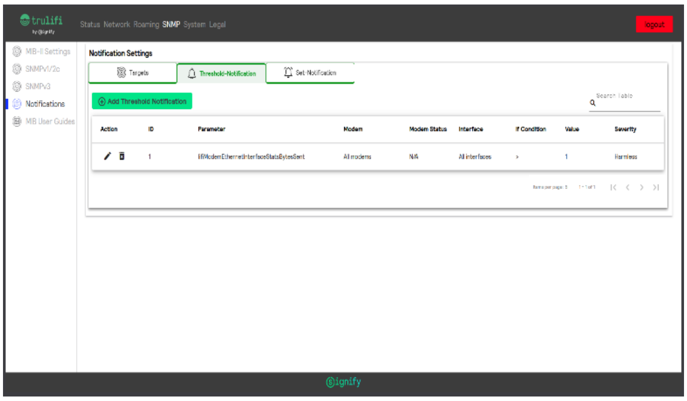
To add a target, select **`SNMP> Notifications > Targets`**. Select **`Add Target`** and enter parameters then select save.



Notification Settings

Action	ID	Name	Trap Authentication	IP Address	Subnet	Port	Transport Protocol	Trap	Inform	Timeout	Retry Count	Message Size

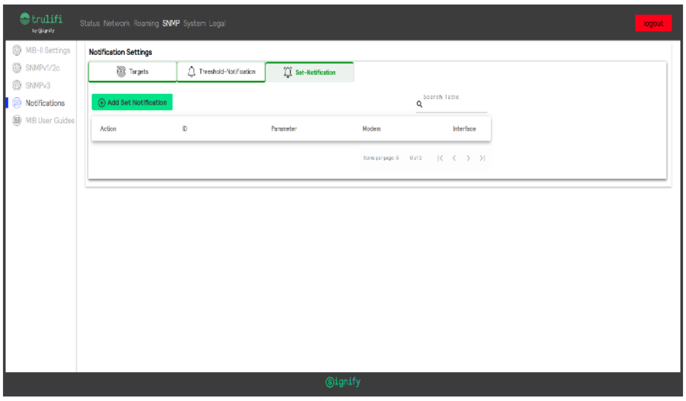
To add a threshold notification, select **`SNMP> Notifications > Threshold-Notification`**. Select **Add Threshold Notification** and enter parameters then select **`[Save]`** **.**



Notification Settings

Action	ID	Parameter	Modem	Modem Status	Interface	If Condition	Value	Severity
	1	lifiModemEthernetInterfaceStatsBytesSent	All modems	N/A	All interfaces	>	1	Harmless

To set a notification, select **`SNMP> Notifications > Set-Notification`**. Select **`Add Set-Notification`** and enter parameters then select **`[Save]`**.



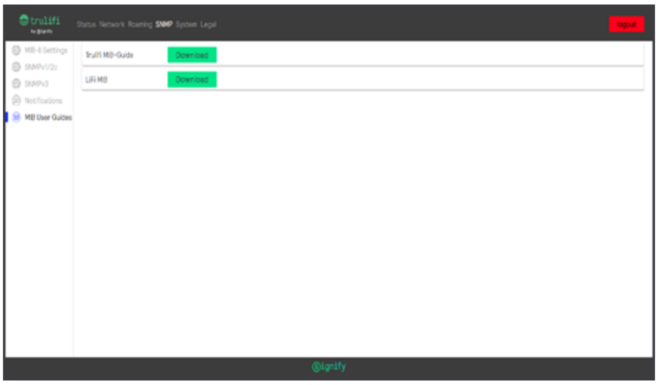
Notification Settings

Action	ID	Parameter	Modem	Interface

7.4 Trulifi MIB Guide and LiFi MIB file

The full functionality and MIB Guide can be downloaded by selecting **SNMP > `MIB User Guides`** and select **`[Download]`**.

The LiFi MIB file can be downloaded by selecting **`SNMP > MIB User Guides`** and select **`[Download]`**.



The LiFi MIB file can then be imported in the SNMP Management application.

8 Configuration of SSH

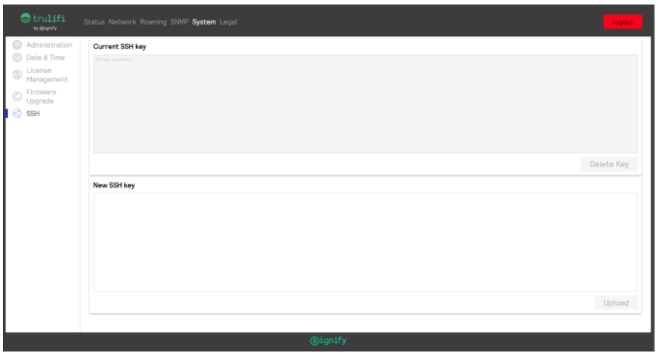
8.1 Introduction to SSH

The LiFi Controller runs the SSH client software. After successful authentication with the SSH server, the SSH client enables a secure connection to the LiFi command line application running in the Life Controller system.
When a secure connection is established with the remote server running on the LiFi Controller system, user can be able to retrieve or modify various Trulifi parameters exposed through the LiFI MIB.

Procedure outlined in the sections below, uses the OpenSSH client software available in Windows operating system. OpenSSH is the open-source version of the Secure Shell (SSH) tools available in Windows 10 and Windows Server 2019. If the OpenSSH Client is not available in Windows 10, it can be installed as separately installable components in Windows Server 2019 and Windows 10.

Steps described are to be performed irrespective of the user's operating system. The steps described below uses the OpenSSH client software available in the Windows operation System. These steps are very similar to the SSH client implementations available in the other operating systems.

Select **System > SSH** to enter/update the SSH keys



8.2 RSA key pair generation.

Secure connection to the LiFi Command Line application uses public key authentication available in SSH. This method of authentication uses public-key/private-key pairs to drive the authentication. Public key authentication is a way of logging into an SSH account using a cryptographic key rather than a password. In case no SSA keys are available, these need to be generated.

Generate the key pair on the machine where the SSH client is running. With OpenSSH on Windows OS, an SSH key is created using ssh-keygen. This step generates a new key pair.

Generate the public\private RSA key pair as described below.

On successful completion of this command, the client will connect to the SSH server running on the Li-Fi controller.
After successful connection to the SSH server, the SSH client will be connected to the LiFi Command Line application and the command line application will present the user its command prompt.

Open the Windows command prompt or Windows power shell. In the simplest form, just run the command ssh-keygen with the following command:

```
C:\ssh-keygen.exe:
```

The key files are usually stored in the ~/.ssh directory. Once an SSH key has been created, copy the rsa key pair from the file where the key pair is stored. If the default location is used to store the key pair, below file contains the key pair.

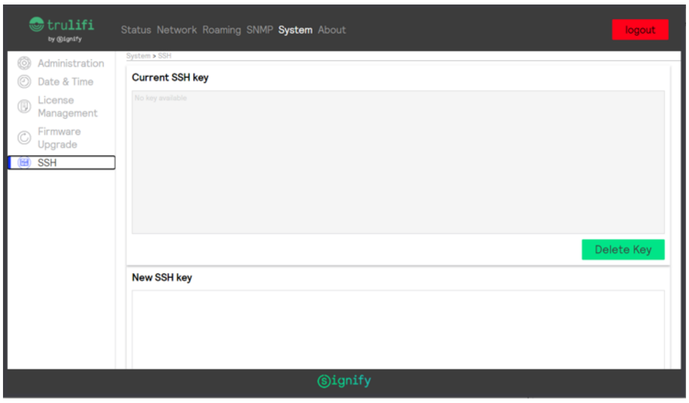
```
C:/Users/<user name>/.ssh/id_rsa
```

8.3 SSH key upload

To provision access without requiring a password for Secure shell to the command line application, SSH key generated as outlined in chapter 8.2, is required to be installed on the SSH server as an authorized key. Once the key has been authorized for SSH, it grants access to the SSH server without a password. This facilitates automated, password less logins and single sign-on using the SSH protocol.

To copy the generated SSH key, Login into the below URL using the web browser.

```
http://trulifi-controller.local/login
```



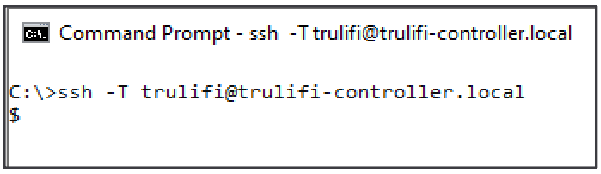
Select **System > SSH** to enter the generated SSH keys

Enter or paste the rsa key pair in the New SSH key dialog box and Click upload. When the key has been successfully uploaded, it shows the status: "**Successfully saved new SSH key**".

8.4 SSH Terminal

To connect to an SSH server, OpenSSH client software needs to be used. On a Windows-based operating system, a OpenSSH client can be invoked from Window command prompt or Windows Powershell. To connect to an SSH server from the Microsoft Windows OS, type the following command into the Windows command prompt:

```
ssh trulifi@trulifi-controller.local
```



```
C:\>ssh -T trulifi@trulifi-controller.local
$
```

The LiFi command Line application provides set and get commands to retrieve or modify an MIB parameter. Chapter 8.5 describe the commands supported by the LiFi command line application.

8.5 Command line utilities

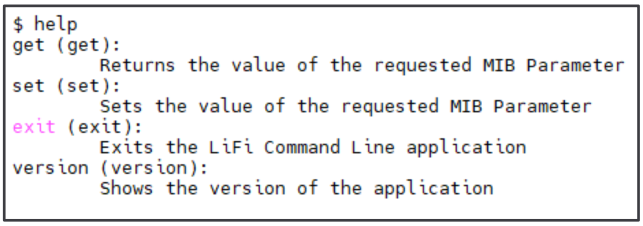
The following commands supported:

- **`Help`**
- **`Get`**
- **`Set`**
- **`Exit`**

8.5.1 HELP command

The “**Help command**” can be used to see the list of commands supported and what each command can do.

To invoke the “**help**” command, type: “ **`help`** ” in the command line.
Below is the screenshot of the Help command.



```
$ help
get (get):
        Returns the value of the requested MIB Parameter
set (set):
        Sets the value of the requested MIB Parameter
exit (exit):
        Exits the LiFi Command Line application
version (version):
        Shows the version of the application
```

8.6 GET command

The “**Get command**” can be used to retrieve the value of a given MIB parameter from the LiFi controller.
For the list of MIB parameters supported, refer to the MIB parameter user guide described in the related documents section.

The format of the “**get** “ command is:

```
get --name=<Parameter Name> {--device=<MAC
Address>} {--index=index identifier}
```

Where:

- **Parameter Name**: Mandatory parameter. Only parameters listed in the Trulifi MIB-Guide are accepted
- **Device**: Optional Parameter. MAC-Address of the device from which the specified parameter is requested. Can be found either on the device, or a list of all MAC addresses in the LiFi-Network can be requested by using the following command: **`get --name=lifiModemEthernetInterfaceMACAddress`**
- **Index**: Optional. Refers to the interface of a specific parameter, e.g. one of the two ethernet interfaces, or a specific NTP time server. Described in more detail in the Trulifi MIB-Guide.

8.6.1 SET command

The “**Set command**” can be used to set the value of a given MIB parameter. For the detailed list of MIB parameters, refer to the Trulifi MIB-Guide.

The format of the “**set** “ command is:

```
set --name=<Parameter Name> {--device=<MAC
Address>} {--index=index identifier} --
value=<value>
```

Where:

- **Parameter Name**: Mandatory parameter. Only parameters listed in the Trulifi MIB-Guide are accepted.
- **Device**: Optional Parameter. MAC-Address of the device from which the specified parameter is requested. Can be found either on the device, or a list of all MAC addresses in the LiFi-Network can be requested by using the following command: **`get --name=lifiModemEthernetInterfaceMACAddress`**. If not defined, parameter will be set for all devices.
- **Index**: Optional. Refers to the interface of a specific parameter, e.g. one of the two ethernet interfaces, or a specific NTP time server. Described in more detail in the Trulifi MIB-Guide. If not defined, value will be set for all indexes of the specified parameter.
- **Value**: Mandatory. Acceptable values are dependent on the data type of a specific parameter. More details can be found in the Trulifi MIB-Guide

8.6.2 EXIT command

The “**Exit command**” is used to close the application and terminate the SSH connection.

Type : “ **`exit`** ” and hit enter.