



User Manual

Trulifi Controller 6800 – User Manual

1 Introduction

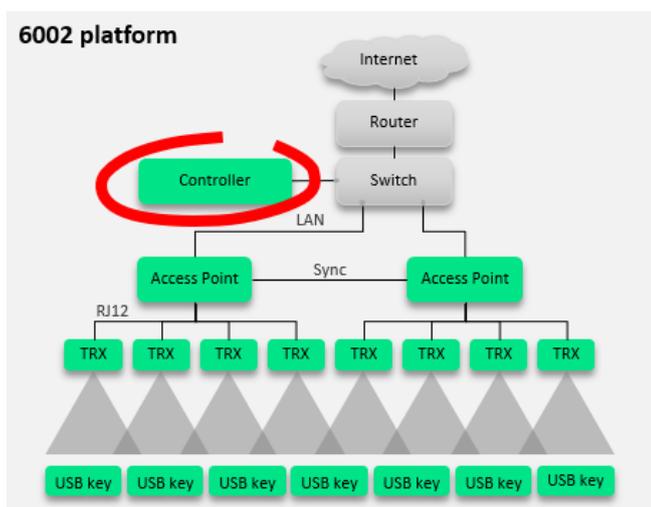
The Trulifi 6002 platform can be extended (licensed) with a LiFi controller, both as system (=Controller HW + SW) or as Virtual Machine/SW-only. The LiFi-controller enables roaming of USB-Keys between multiple Trulifi 6002.2 Access Points installed in network or building. The LiFi controller application 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-hardware:

- Access Point 6002.1
- Access point 6002.2
- Transceiver 6002.1
- USB Key 6002.1

Optionally, the LiFi controller can be licensed with a roaming functionality, to enable the roaming of USB keys through multiple domains. 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 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 V2C. The SNMP functionality will be further described in Chapter 7 of this document.

Signify makes the LiFi Controller Application available on pre-configured hardware and as Virtual Machine (SW-only) version.



Example set-up of 6002 based system.

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

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

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

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 Virtual Machine version (Trulifi 6800 Controller Application).

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 customer-care.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.

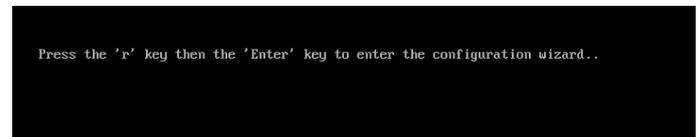
Step 2 : Open the VM application on your client.

Step 3 : Open the [trulifi_controller_application](#) ovf-file in your virtual machine.

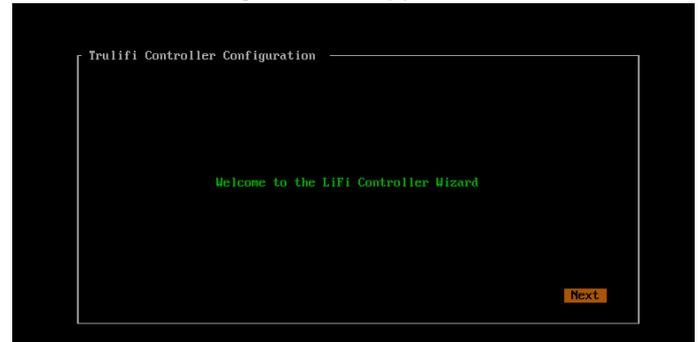
Step 4 : Import "[trulifi_controller_application](#)" on your client.

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.



Wait for the following screen to appear:



Select **Next**

The following screen appears:



For Automatic configuration select **Yes**

For Manual Installation Select **No** and 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

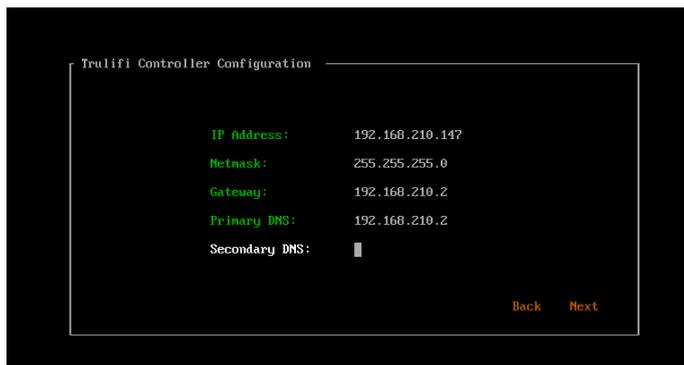
If you select to configure the system manually you can choose how to configure the Network interface, either using DHCP or setting the network addresses manually.



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



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

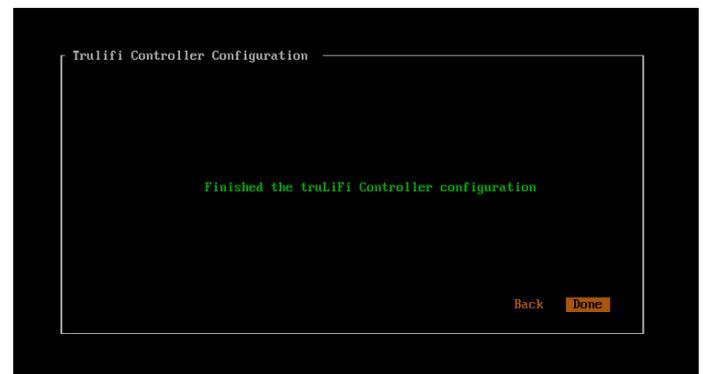
After network settings are configured, configure Time Settings:



Configure your **Time Settings** and select **Next**:



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



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.

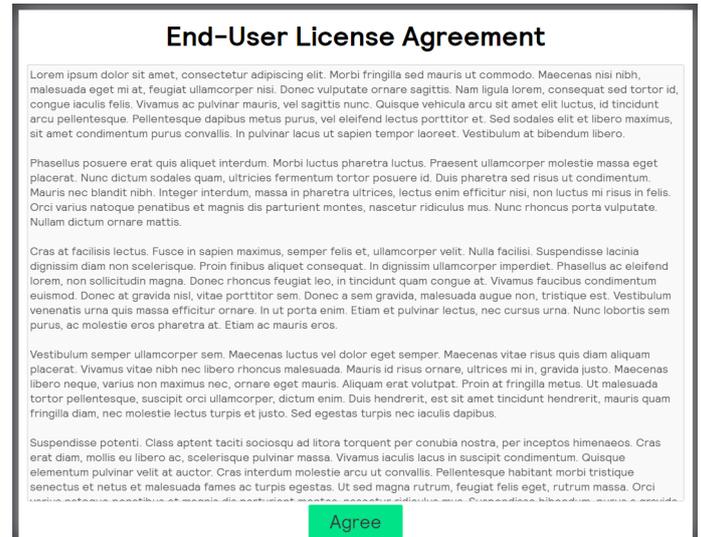
Before installing and configuring the LiFi controller make sure that you have obtained a license and stored the license file on a known location (eg. Desktop) on your client connected to the same network. If you have not obtained a license file please contact :

Step 1 Controller (GUI) access

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

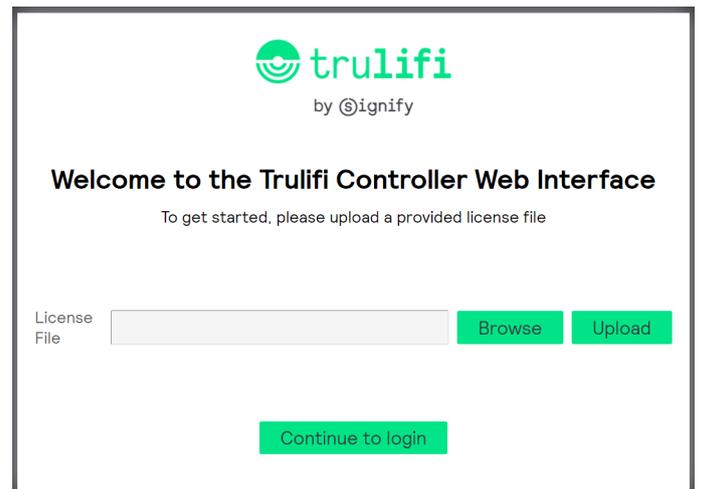
Alternatively you can connect your Client PC to the same network as the Controller Unit or Virtual Machine and browse to <http://trulifi-controller.local>.

The following login page appears:



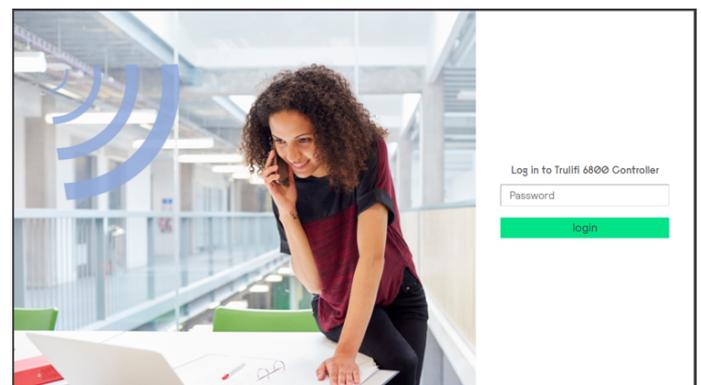
Scroll through the End-User License Agreement and select **Agree**

The following page appears:



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:

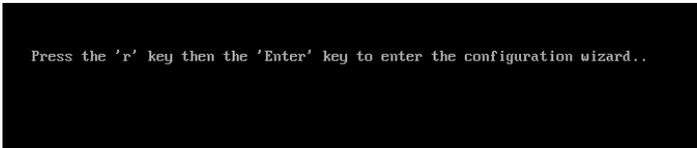


The default password of the user-interface is **admin**.

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 its 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 and then **Enter** to reset the system to factory defaults.

Step 2: 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.

Step 3: 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**.

The default password for every 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.

Step 4: Login password

The Controller UI is protected by a password that can be changed:

- 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**.

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.

Step 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 **Timezone** 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.

Step 6: Logout

To logout from the controller:

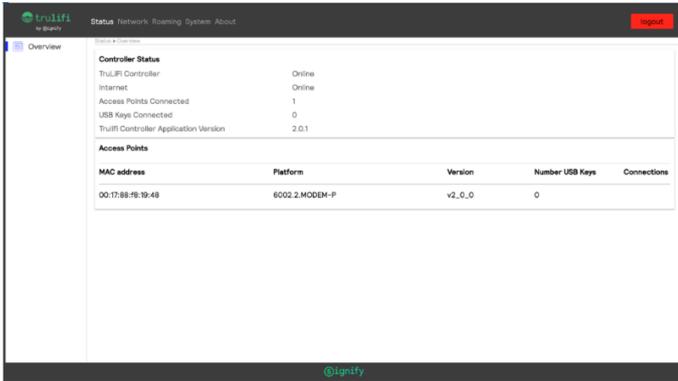
- Click Logout in the top right corner of the page to complete the log out process and prevent unauthorized users from accessing the controller GUI.

Note: automatic logout after 15 min of user inactivity with redirection to the login page.

6 Advanced configuration

6.1 Controller status

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



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.

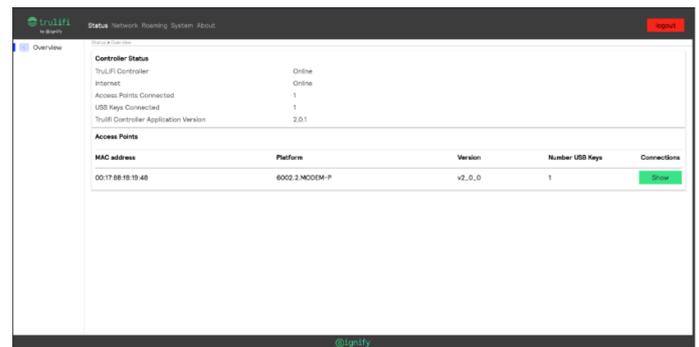
It is not possible to create separate VLAN's managed by one controller or Access Point.

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

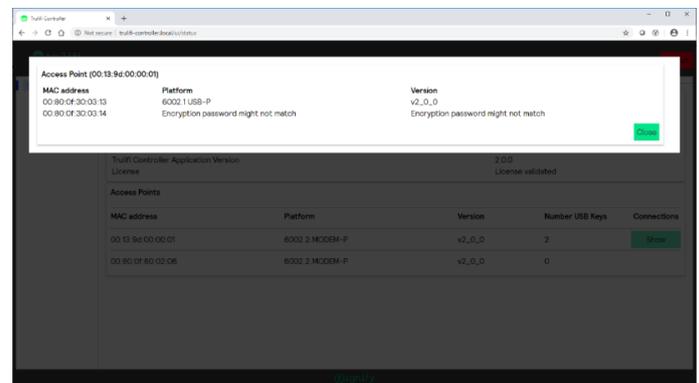
- **Access Points Connected** text field indicates the number of access points connected and associated to the controller.
- **USB Keys Connected** text field indicates the number of USB keys connected to the domain.

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



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:



For every USB key, you can find:

- 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.

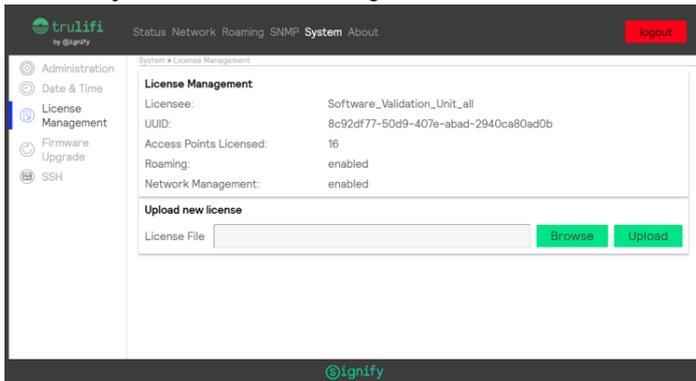
6.2 Roaming overview

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.

6.2.1 Activation of ROAMING license

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

Choose **System > License Management**



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

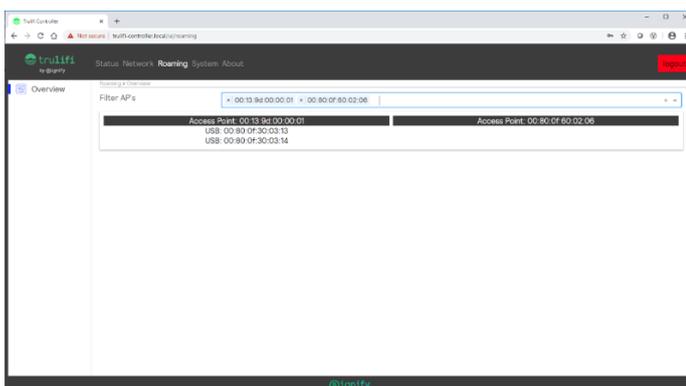
Select **Upload**

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

6.2.2 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.



6.3 Firmware upgrades

The controller can upgrade the following Trulifi devices:

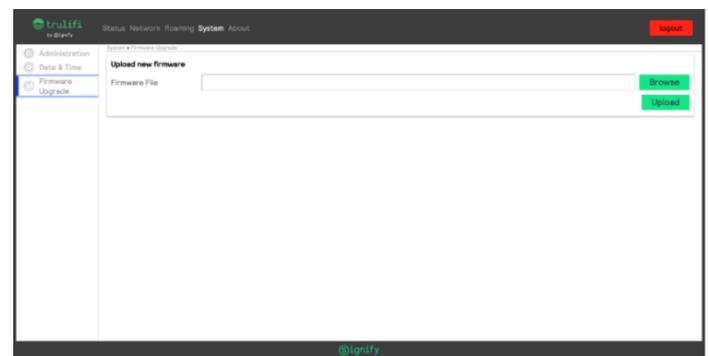
- Controller
- USB key
- Access Point

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

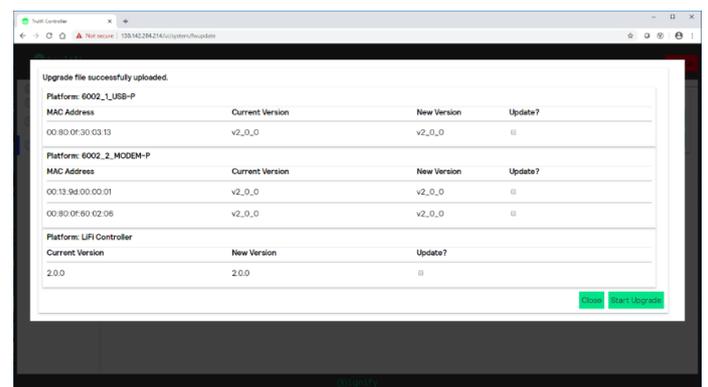
After the new firmware is downloaded and stored on the client on a known location (eg. Desktop) files the LiFi controller can be upgraded .

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.



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

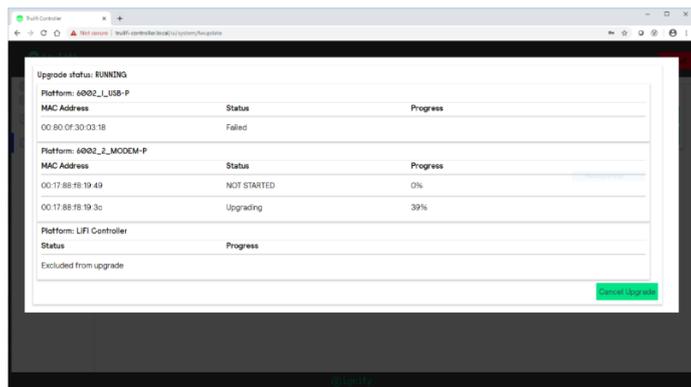


In this new window, the current and new version columns give a status of the current firmware/software version per Trulifi device family:

- 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.



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.



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.

6.4 Legal

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

7 SNMP MIB Integration

7.1 SNMP functionality

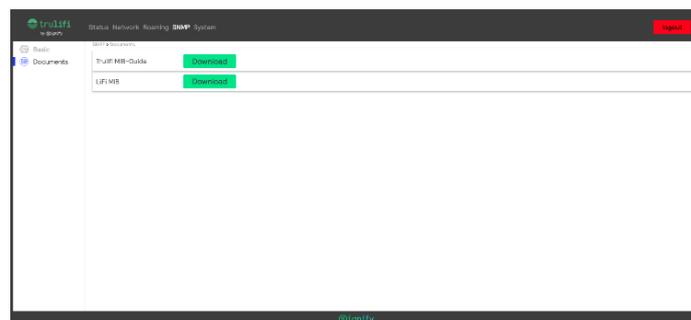
The Trulifi Controller application can be extended with a SNMP license. This allows users to monitor the status of their Controllers and the respective connected Trulifi Access Points through Network Management Systems (NMS) via Simple Network Management Protocol (SNMP). The LiFi MIB exposes over 360 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.

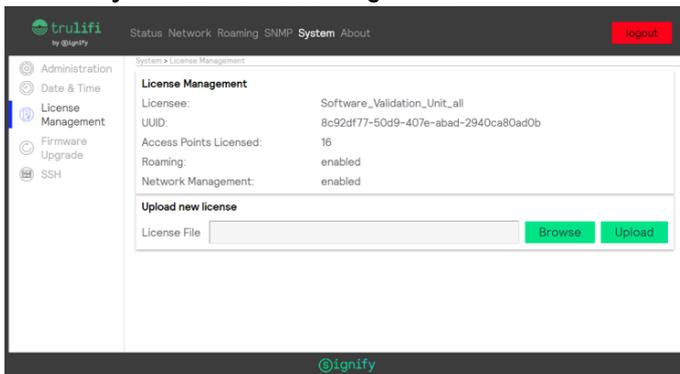


To obtain a SNMP license please contact customer-care.trulifi@signify.com

7.2 Activation of SNMP license

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

Choose **System > License Management**



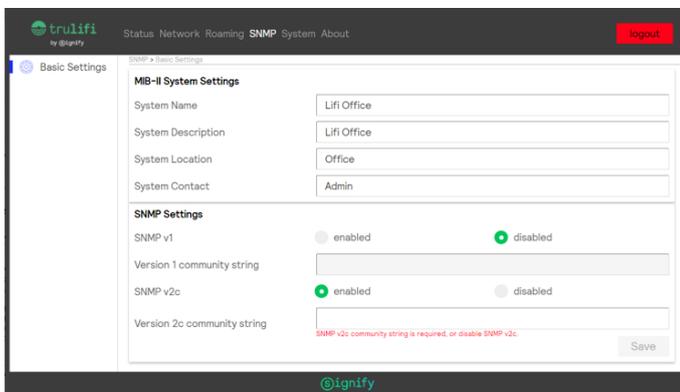
Select the *xxxxxx.lic* license file from the saved location.

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 > Basic Settings** to configure the mandatory MIB-II system parameters. Additionally, you can enable the specific SNMP Version 1 or 2c and define the respective community string. Choose **Save** after completion.



7.4 Trulifi MIB Guide and LiFi MIB file

The full functionality and MIB Guide can be downloaded by selecting **SNMP > Documents**. Select **Trulifi MIB-Guide** and select **Download**.

The LiFi MIB file can be downloaded by selecting **SNMP > Documents**. Select **LiFi MIB** and select **Download**.

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

7.5 RFC's

This following RFCs are supported by the Trulifi SNMP :

- RFC 1155 – SMiv1
- RFC 1157 – SNMPv1
- RFC 1212 – SMiv1
- RFC 1901 – SNMPv2c
- RFC 1908 – SNMP Version Coexistence
- RFC 2576 – SNMP Version Coexistence
- RFC 2578 – SMiv2
- RFC 2579 – SMiv2 TC
- RFC 2580 – SMiv2 CONFORMANCE
- RFC 3418 – MIB-II (SNMP, SYSTEM)
- RFC 3584 – SNMP Version Coexistence

8 Configuration of SSH

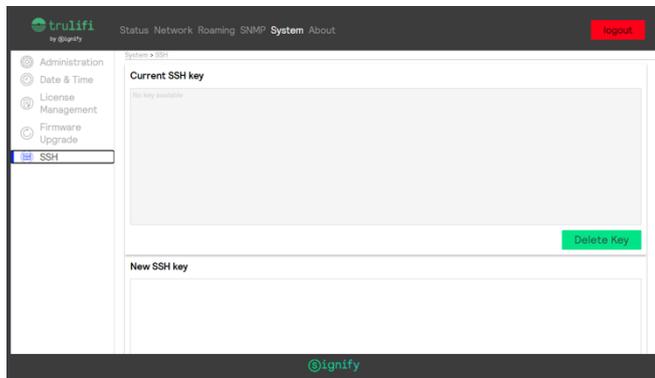
8.1 Introduction to SSH

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 1809.

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.

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.

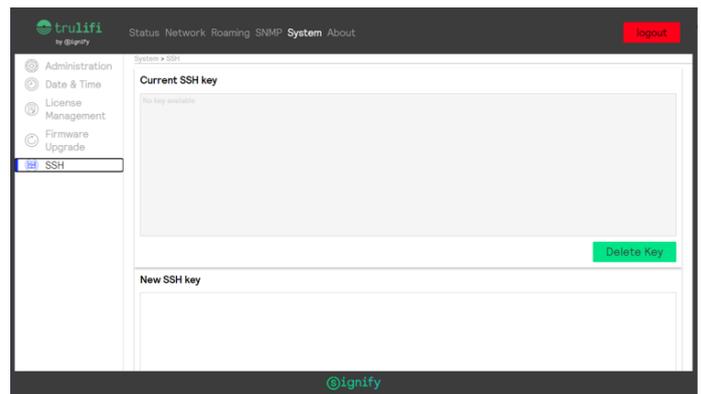
C:/Users/<user name>/.ssh/id_rsa

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

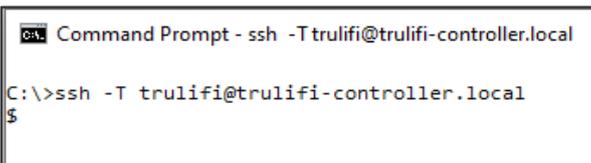
Enter or paste the rsa key pair in the New SSH key dialog box and press upload. When the key has been successfully uploaded, it shows the status: **“Successfully saved new SSH key”**.

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
```

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 CommandLine application and the command line application will present the user its command prompt.



```
Command Prompt - ssh -T 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 a MIB parameter. Chapter 8.5 describe the commands supported by the LiFi command line application.

8.5 Command line utilities

The following commands supported:

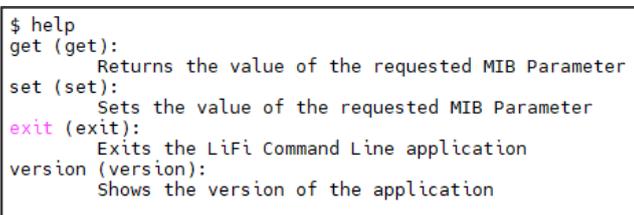
- [Help](#)
- [Get](#)
- [Set](#)
- [Exit](#)

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.