Product presentation

Speed
LiFiMAX® offers 100Mbps downlink and 100Mbps uplink speeds, providing seamless network access for you and your colleagues during your work sessions.

Security
With LiFiMAX® you no longer need to sacrifice mobility for safety. LiFi is based on non-visible light transmission. Since light cannot pass through walls, your network cannot be accessed from outside the room, giving you a highly secure connection.
A 128-bit AES real-time encryption feature is now available and allows you to pair dongles with access points for an increased level of security.

Reliability
The LiFiMAX® technology is based on high lifetime Infrared LED components operating in the non-visible spectrum, to work in any room lighting. This technology also makes your working environment safer because it does not use radio waves.

Multi-user
LiFiMAX® can support up to 16 simultaneous users per Access point, providing each of them with fast and reliable network access. All users need to do is connect their LiFiMAX® USB dongle to their device.

Ease of use
LiFiMAX® can be installed very simply and quickly, for example in a conference or meeting room. You can either connect it to a ceiling bracket or integrate it directly into a suspended ceiling. The LiFiMAX® access point simply requires a PoE connection, while users simply need to connect the USB dongle. LiFiMAX® to their device to be connected.

LiFiMAX® has been tested and validated by ORANGE.

The LiFIMAX® Cybersecurity Solutions product suite consists, among other things, of separate hardware and software devices that allow a user device to be connected to a network in a secure and controllable manner :

1. The LiFiMAX® Access Point,
2. The LiFiMAX® dongle,
3. The LiFiMAX® Controller.

Figure 1 shows a typical installation of these three components to provide network access in one or more rooms (two in Figure 1) to one or more user equipment (three in Figure 1).

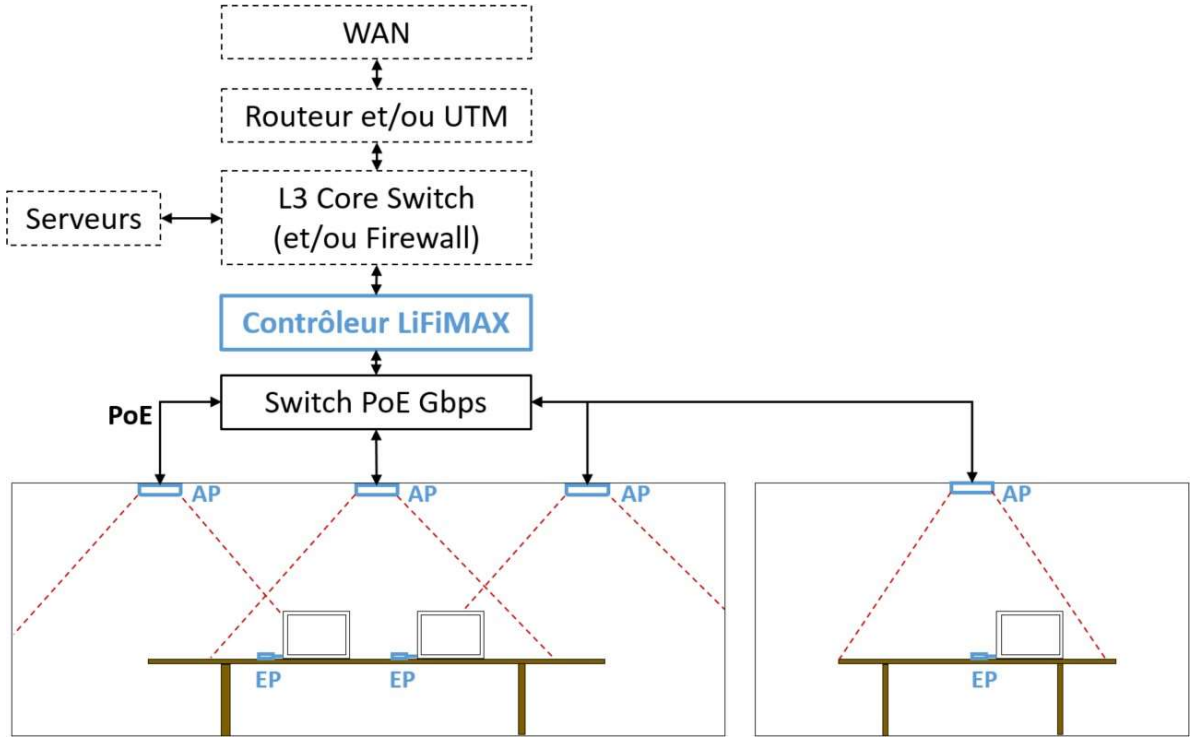

Figure 1: Typical installation of the LiFiMAX® suite in offices. LiFiMAX® equipment is shown in blue (AP = Access Point, EP = End Point or dongle).

Each device has a specific role that will be explained below.

The LiFiMAX® Access Point (or AP)

The LiFiMAX® access point allows a user equipment connected to an authorized dongle to access the network, as shown in Figure 1. Each access point covers a circular area of approximately 10 m² at a height of 2 m (80 degree opening angle), can accept up to 16 users simultaneously, and offers a total download speed (user-to-user access point) of 100Mbps and a total upload speed (user-to-access point) of 100Mbps.

LiFi communication is based on the ITU-T international G.vlc standard and is secured (optional) by AES 128 encryption.

Figure 2: Top (left) and bottom (right) view of the LiFiMAX® access point.

The LiFiMAX® access point has a single Power over Ethernet (PoE, IEEE 802.3af standard) interface, in the form of an RJ45 connector, allowing it to be powered and to exchange data with the controller and therefore the network. It can be fixed to the ceiling in two different ways: as a smoke detector (see figure 3) or directly recessed in a false ceiling (see figure 4).

Figure 3: Smoke detector type mounting.

Figure 4: Flush mounting

The LiFiMAX access point complies with the CE mark certifications, and in particular :

The IEC/EN 62471 standard on photobiological safety. The LiFiMAX® access point is class 0 ("no photobiological risk") and is also equipped with an automatic optical signal cut-off mechanism when the access point/dongle link is cut off (e.g. when a person is looking closely and axially at the access point).

- The IEC/EN 61000 standard on electromagnetic compatibility (EMC).
- In addition, the wavelength used for LiFi communication is 940 nm (infrared), a value at which the spectrum of natural sunlight is at a low point and therefore interference due to it is very low. The system is also protected from other light radiation by a powerful optical filtering system, making it robust to natural and artificial light interference.
- Given the initially envisaged deployment (4.00 m x 6.25 m x 2.58 m room), two access points will be required to ensure coverage of the entire room.

Table 1 below summarizes all the technical characteristics of the AP LiFiMAX.

The LiFiMAX access point complies with the CE mark certifications, and in particular :

The IEC/EN 62471 standard on photobiological safety. The LiFiMAX® access point is class 0 ("no photobiological risk") and is also equipped with an automatic optical signal cut-off mechanism when the access point/dongle link is cut off (e.g. when a person is looking closely and axially at the access point).

- The IEC/EN 61000 standard on electromagnetic compatibility (EMC).
- In addition, the wavelength used for LiFi communication is 940 nm (infrared), a value at which the spectrum of natural sunlight is at a low point and therefore interference due to it is very low. The system is also protected from other light radiation by a powerful optical filtering system, making it robust to natural and artificial light interference.
- Given the initially envisaged deployment (4.00 m x 6.25 m x 2.58 m room), two access points will be required to ensure coverage of the entire room.

Table 1 below summarizes all the technical characteristics of the AP LiFiMAX.

Characteristics	Values
Dimensions	⌀ 110 mm / height 30 mm
Weight	150 g
Protection class	IP30
Interfaces	PoE (IEEE 802.3af) donc plug-and-play
connection	RJ45 (femelle)
optical technology	LED optical technology (infrared)
LiFi communication standard	ITU-T G.vlc
Security	AES 128 encryption
Continuity of connection	Assured under access points by the LiFiMAX® Controller from version V1 onwards
Surface de couverture	Circular cover area, 10 m² at 2 m vertical distance
Maximum number of users	16 users per access point
Total throughput	100Mbps downlink / 100 Mbps uplink
Power consumption	< 7W
Certifications	CE marking including RoHS, IEC/EN 61000 (EMC) and IEC/EN 62471 (eye safety) standards
Mounting	Type smoke detector or flush-mounted

The LiFiMAX® Dongle

The LiFiMAX® dongle makes the user equipment to which it is connected compatible with LiFi data transmission. Thus, if the dongle connected to the user equipment is placed in the coverage area of an access point, then the user will be able to benefit from a connection with a maximum upload and download speed of 100Mbps, secured by AES 128 encryption if necessary.

Figure 5 shows a LiFiMAX® dongle. This device consists of a single USB interface for power and data exchange with the user equipment..

The LiFiMAX® dongle is compatible with Windows operating systems (7 and later), MacOS, Linux for computers, Android for smartphones and tablets. It is completely plug-and-play and therefore requires no driver software installation or configuration by the user.

The LiFiMAX® dongle is compatible with iOS and a Lightning type connector, as long as an external power supply such as a battery or equivalent is added to the dongle.

Like the access point, the LiFiMAX® dongle complies with CE mark certifications, in particular :

- The IEC/EN 62471 standard on photobiological safety. The LiFiMAX® dongle is class 0 ("photobiologically safe") and is also equipped with a mechanism for automatically cutting off the optical signal when the access point/dongle link is cut off (for example when a person is looking closely and axially at the dongle).
- The IEC/EN 61000 standard on electromagnetic compatibility.

In addition, the wavelength used for LiFi communication is 940 nm (infrared), a value at which the spectrum of natural sunlight is at a low point and therefore interference due to it is very low. The system is also protected from other light rays by a powerful optical filtering system, making it robust to natural and artificial light interference..

Characteristics	Value
Dimensions	⌀ 63 mm / hauteur 17 mm
Weight	100 g
Protection class	IP30
Interfaces	USB 2.0
Connectique	USB-C connection (female), USB-C/USB-C and USB-C/USB-A cables included
Compatible with	with Windows OS (from 7), MacOS, Linux, Unix, Android
Installation	Plug-and-play
Optical technology	940 nm LED (infrared)
LiFi communication standard	ITU-T G.vlc
Security	AES 128 encryption
Continuity of connection	Assured connection under an access point and between access points (roaming) with the LiFiMAX® Controller from version V1 onwards
Total throughput	100Mbps downlink / 100 Mbps uplink
Power consumption	< 2W
Certifications	CE marking including RoHS, IEC/EN 61000 (EMC) and IEC/EN 62471 (eye safety) standards

Table 2: Summary of the technical characteristics of the LiFiMAX® dongle.

The LiFiMAX® Controller

General Description of the LiFiMAX® Controller

The LiFiMAX® Controller is at the heart of the LiFIMAX® Cybersecurity Solutions suite by allowing LiFiMAX® access points to interface with the corporate network, secure and manage them remotely, while providing additional connectivity features.

Important note: Version V1 of the LiFiMAX® Controller will be available on March 30, 2020, therefore the features presented below are subject to change according to ongoing developments.

Figure 6 shows a view of the hardware onboard the LiFiMAX® Controller.

Figure 6: LiFiMAX® Controller Appliance

It has a network card for connection to the WAN and as many network cards as there are LANs and thus connected access points. As the maximum speed per access point is 100Mbps, it is desirable to have a dedicated bandwidth of 100Mbps per LAN.

It should be noted that this appliance is only "on premise" (installed on site) at first, with the possibility to upgrade to a cluster mode from May 15, 2020 with the LiFiMAX® Controller version V2.

Translated with www.DeepL.com/Translator (free version)

Based on this architecture, several levels of network segregation are possible:

- In a first step, we will propose to establish an identical "Guest" network for all (employees and visitors). All you need is a LiFiMAX® dongle and to be in the coverage area of a LiFiMAX® access point to be able to connect to the network. We then propose you to extend the company's internal security policy (if there is an End Point User policy via Forticlient, Pulse or NAC).

- In a second step, from May 15, 2020, we plan to implement a real segregation of LiFi networks in order to allow an employee to connect to the employee network while visitors will only be able to connect to a "Guest" network without any company service.

Features offered by the LiFiMAX® Controller

Active directory: With the LiFiMAX® Controller, it is possible to declare the connection to an active directory (AD) to authenticate some or all users in order to delegate firewall administration.

It is thus possible, for example, to assign rights to a specific group, which then corresponds to a group in the AD, allowing it to configure the captive portal part of the firewall. Similarly, a second group can be defined that can only access the firewall logs.

It is also possible to create local groups on the controller, with local users, although it is recommended to query the AD directly to avoid having to change the login and/or password.

This part is set up via our integration service, following these steps

- Declaration of the AD directory on the controller,
- Authentication tests,
- Statement from a group to make the link with the DA,
- Allocation of rights to this group,
- Setting the AD server for authentication.

Graphical User Interface: The LiFiMAX® Controller provides a web-based graphical user interface similar to the one shown in Figure 8.

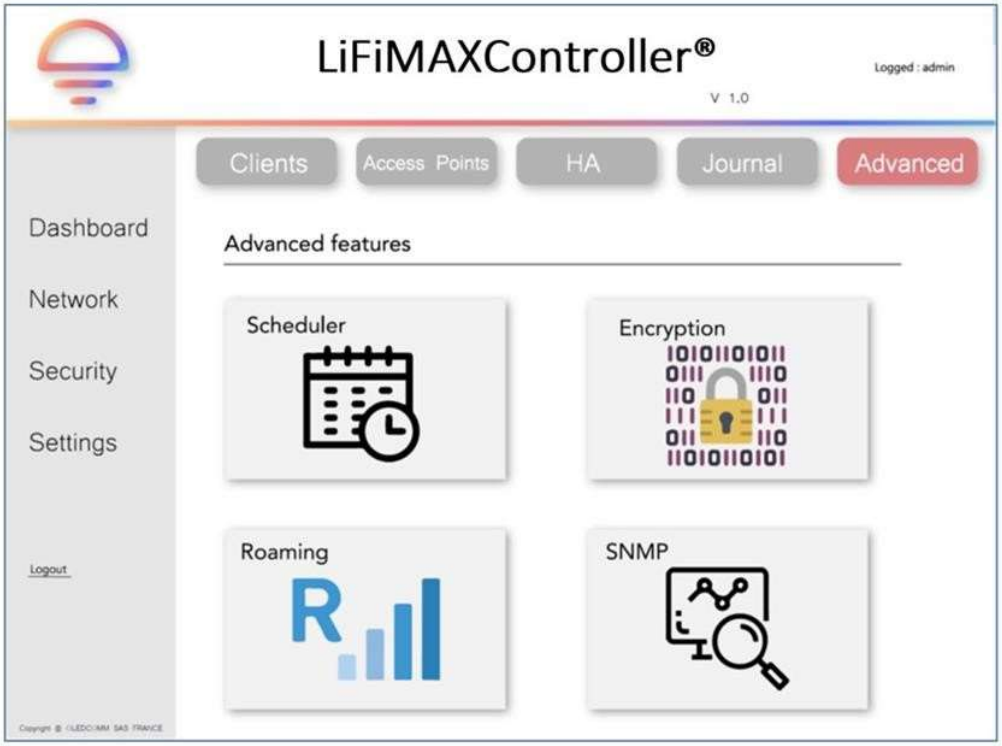

Figure 8: Graphical user interface offered with the LiFiMAX Controller®.

Access to this interface is not limited in the number of simultaneous users of the system but can be finely controlled via the controller.

This interface is supported by the Firefox and Chrome browsers and can be offered in English and French. Other languages may be added from June 2020.

Reporting: The LiFiMAX® Controller can provide numerous analysis reports via its EventLog Analyzer module:

- LiFiMAX® Controller Firewall Traffic Reports: EventLog Analyzer processes the LiFiMAX® Controller traffic logs and provides information on allowed and denied traffic with source, destination, port and protocol details.

- LiFiMAX® Controller Connection Reports: Monitor successful and unsuccessful LiFiMAX® Controller logins. Identify which devices are used most and which users are accessing your LiFiMAX® Controller devices the most. Access monitoring helps you control device usage and activity.

- LiFiMAX® Controller IDS/IPS Reports: Protect your network from attacks with security reports based on LiFiMAX® Controller IDS/IPS logs. View a list of positively identified attacks as well as potential threats to your network that merit investigation.

- LiFiMAX® Controller Threat Reports: These reports detail various types of attacks, such as URL filtering, flooding attacks, spyware downloads, and more, that are useful in protecting the network from intrusion attempts.

- LiFiMAX® Controller Severity Reports: These reports classify log information by severity and are useful for accessing all events (including emergency, error, critical, alert, warning, notification, information and debugging events) with a single click.

- LiFiMAX® Controller Configuration Reports: These reports help you ensure that your LiFiMAX® Controller firewalls are properly configured and track changes in link status.

- LiFiMAX® Controller System Events: These reports help you track system restarts, starts and stops, and ensure that your LiFiMAX® Controller firewalls are running smoothly, with no unplanned shutdowns or restarts.

VPN: The LiFiMAX® Controller supports SSL TLS and includes the ability to set up a VPN Tunnel, OpenVPN or IPSEC. VPN access is therefore possible.

Administration and Monitoring: As shown in the previous sections, administration and monitoring of the LiFiMAX® network is easily performed via the graphical user interface and analysis reports of the LiFiMAX® Controller.

In addition to these tools, we provide :
o Training in the use of the controller.
o Integration service for the implementation in your environment, mandatory to have access to the Gold Support (by phone).
o Implementation of a Grafana type monitoring interface accessible in HTTPS with secure access.
o The optional possibility to set up a VPN Tunnel between your controller and our secure control center to keep an encrypted version of your configuration (in case of loss) as well as a Log capture if needed.

Web services and API: In its initial version, the LiFiMAX® Controller does not integrate web services and APIs. However, we can develop such solutions if needed in order to add functionalities to the LiFiMAX® Controller via the GUI interface of the appliance.

LiFiMAX® Controller deployment schedule

The LiFiMAX® Controller has been designed as a scalable solution that adapts and expands as needed. Therefore, we propose a deployment of the LiFiMAX® Controller solution according to the following schedule :

- March 30, 2020: delivery of the LiFiMAX® Controller V1 in "premise" mode.
- May 15, 2020 : LiFiMAX® Controller V2 with the possibility of a cloud and virtual machine version.15

Prerequisites for deployment

The description of the previous technical solution reveals a number of prerequisites

- The presence of a DHCP server on the test network.
- The availability of 12 IP leases,
- The need for the switch port on which the AP will be plugged to be in UNTAG mode in the correct test VLAN,
- The ability to save the IP frame in a .pcap format in case troubleshooting is required.
- The possibility to plug and play USB dongles on user equipment (no policy to block USB ports for example, no blocking by antivirus software...).
- Knowledge of the type of network security in place, for example IEEE 802.1x with certificate.