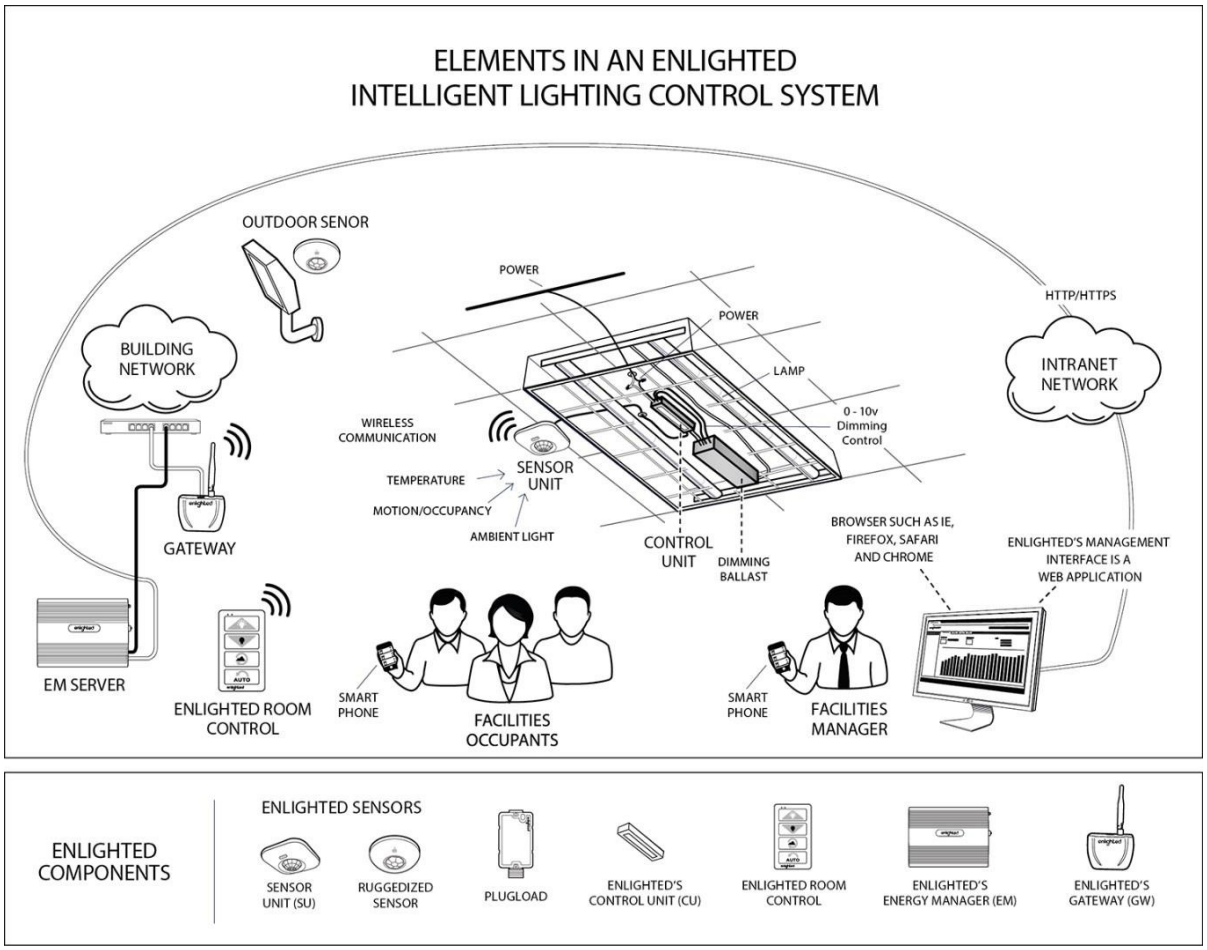
GENERIC SECURITY REQUIREMENTS

Enlighted provides a state of the art intelligent lighting solution, providing the right illumination to meet our customer needs. The Enlighted solution optimizes energy savings while enhancing occupant productivity, well-being, and security. The illustration below shows the fundamental physical components of an Enlighted intelligent lighting control system.



The feature that most differentiates Enlighted Lighting Control from other wireless, networked building management solutions is the autonomy of Enlighted Smart Sensors. Each Enlighted Sensor is a full-fledged computing and communications device that controls light levels locally. With the bulk of control instructions transmitted over a wired connection to the Control Unit and ballast, traffic on the Enlighted wireless network is kept to a minimum.

Wireless networking is used for data gathering and transport of energy, environmental, and occupancy data to the central Enlighted Energy Manager (EM) system. The EM provides an interface to the sensor

network, simplifying configuration and management of lighting behavior, as well as data monitoring and reporting.

Enlighted Smart Sensors communicate to the Enlighted Energy Manager through the Enlighted Gateway using the IEEE 802.15.4 wireless communication protocol that includes AES encryption to ensure secure links.

The Enlighted Energy Manager's intuitive graphical user interface can be accessed via a standard secured browser connection. The figure below shows an example of an Enlighted Energy Manager installation in an office environment.

Describe any hardware included in the service

The Energy Manager appliance is mounted in a wiring or electrical closet and can be on the IT network or a stand-alone network or can be hosted on the Cloud. For Cloud customers, the Energy Manager will be deployed in the Google Cloud.

1. What operating systems is it running?
   Linux (Ubuntu 14.04). Starting with EM 3.9.14, Ubuntu 18.04 is supported.
2. How does this hardware physically communicate?
   Physical communication is over Ethernet (TCP/IP)

3. What protocol does the device use to communicate?
   SSHv2, HTTPS, TLS
4. What does it need to communicate? (other devices, the server)
   The Energy Manager needs Enlighted Gateways to communicate with the building sensor network and a Client PC to access the application through a browser.
5. Are there placement requirements for these devices?
   The Energy Manager will be hosted on Google Cloud.

Describe any software included with the service

The Enlighted Energy Manager's intuitive graphical user interface can be accessed via a standard secured browser connection (Chrome & Firefox are supported)

1. Is an application installed on a computer?
   No, access is through a browser.
2. What operating systems are supported?
   MS windows, Mac OS for the Client.
3. What are the minimum requirements (i.e., CPU's, memory, etc.)
   Any primary PC/Mac (1 core, 2 GB memory)
4. Is a mobile application included?
   No
5. How are application updates handled? What is the update frequency for this application? Who will be using the software? Who will be responsible for ownership of controlling that access?
   New releases are made approximately once a quarter and provided as a Debian update. Some users will have restricted access. The Customer lighting management team will be the user and will have ownership of controlling access.
6. What are the primary ways that the service will be interacted with?
   Application access is through browser web pages.
7. What are the applications/software frameworks used by this application?
   Postgres, Java, Apache, Tomcat, Flex

   Stage 2 (December 2020): Cassandra, Java, Apache Storm, Kafka, Tomcat, AngularJS

Security

1. Is data stored in an encrypted format? How is it encrypted?
   No. Data is stored in the Postgres database. Passwords are encrypted using one-way encryption

2. Is data transmitted in an encrypted format? How is it encrypted?
   Yes. AES 128-bit encryption for wireless data transmission and TLS for TCP/ IP along with the use of 2048-bit certificates and SHA-256 ciphers.

3. What protocol(s) are used in any network communications? What are the security measures in this protocol used? (if any)
   - HTTPS (with 2048-bit certificates) is used to access the Energy Manager.
   - TLS with AES 128-bit encryption is used for Gateway to Energy Manager communication.
   - SSH (SCP/SFTP) is used for upgrading Gateway Firmware.

4. What is the vendor's response to security issues? Are updates pushed on a fixed schedule? Are updates pushed as needed?
   Updates are typically pushed along with every Energy Manager release, which happens about once a quarter. If there are P1 issues discovered, the updates are pushed as needed.

5. How is access to the application handled? Are local accounts created and managed manually? Does the application integrate with Oauth?
   Currently, access to the application is handled manually using local accounts. When the Amaze platform is available (Dec. 2020), the application will integrate with Oauth.

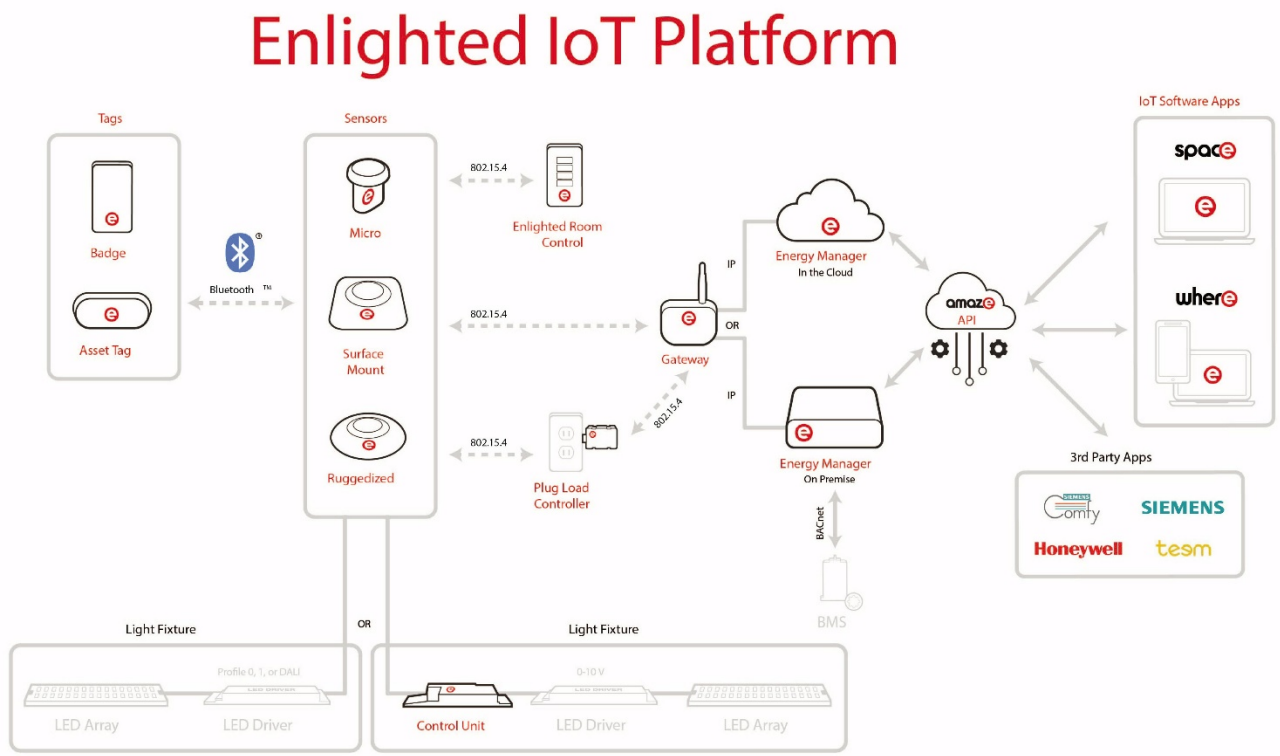
6. Has a vendor security audit been conducted?
   If not conducted, Enlighted can share the Qualys scan reports and work with the customer to get the security audit conducted

Data

1. Can all data be exported in a common format? CSV, XML etc.
   No. The energy consumption report can be exported in CSV from the application. Other common reports can be exported in PDF. A RESTful API provides access to the consumable user data.
2. Is there an API to access the data?
   Yes
3. Does this API meet customer's reporting needs such as latency, specific points of data, open format?
   Enlighted has published APIs for the Energy Manager, which can be shared with the customer for review. When the Amaze platform becomes available in December 2020, we will add real-time event change reporting.
4. Where is the data physically stored?
   Data is physically stored in Enlighted Cloud
5. Is this data shared with third parties? For example, geolocation services to identify the location of users?
   No
6. Are cloud services being used to host the data?

   Yes
7. Provide a diagram showing the flow of data from source to consumer?

   For example, the flow of data from a sensor device to a gateway, processing server, and a visualization server.



User management will be owned by the customer. Enlighted DevOps will be provided with login's which can be audited

9. How frequently is data processed (if handled in batches)
   The data from the sensors is received at a 5-minute interval by the Energy Manager. Data aggregation occurs hourly and daily.
10. How is the data backed up?
    Currently, back-up's are generated nightly for each Energy Manager instance.

    When the Amaze platform becomes available, the Cloud infrastructure will provide high availability and reliability.

Privacy

1. Is any personally identifiable information (PII) used or stored by this application?
   No PII information is saved by the application. Currently, Enlighted stores user credentials. With the Amaze platform (Dec. 2020), we will use OAuth so that no credentials will be stored.

Safety

1. Is there a risk of harm to people or the environment if a component in this service fails? Provide all details on how this risk is mitigated and what measures can be taken to minimize or mitigate the risk.

No. The feature that most differentiates Enlighted Lighting Control from other wireless, networked building management solutions is the autonomy of Enlighted Smart Sensors. Each Enlighted Sensor is a full-fledged computing and communications device that controls light levels locally, so even if the Energy Manager or the Gateways fail, the lights will continue to function. If a sensor fails, the lights will operate as if the sensors are not installed.