A DICKSON COMPANY
OCEASOFT™
Environmental Monitoring + Compliance Experts

Technical Bulletin

OCEAView Solution & Security

Subject:	OCEAView Solution & Security		
Product(s):	OCEAView hardware and software components		
Reference:	ING-MO-055-EN (rev. 01)		
Date:	May 5, 2020	**Updated**:	–

Summary

The OCEAView monitoring solution involves a variety of OCEASOFT hardware and software products, integrated and interconnected with today's cutting-edge wireless, Cloud, and IT technologies. As such, it is important to understand the different security implications involved with the solution.

This document explains the security mechanisms used in the OCEAView solution, including the manner in which customer data is exchanged, handled, secured, and backed up. We include details regarding data encryption, Cloud security, user data security, and password management.

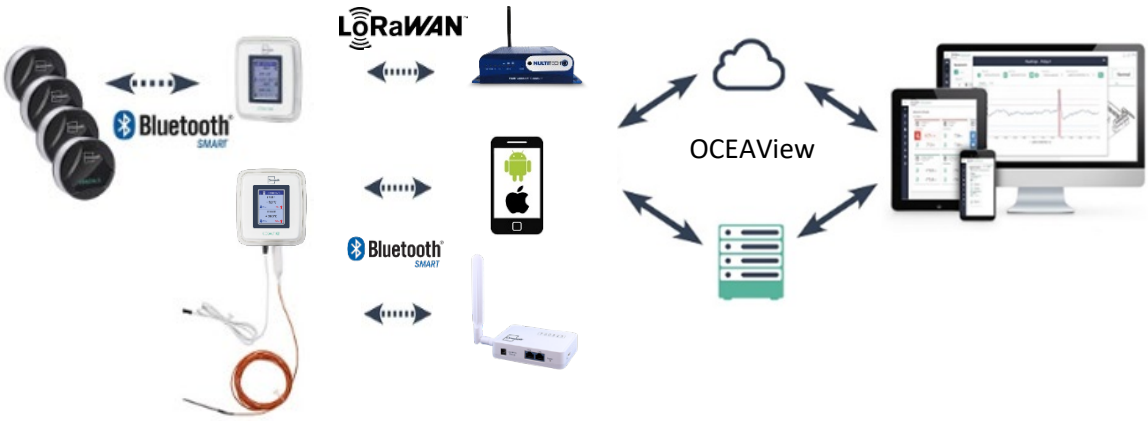
Reference documentation

LoRaWAN wireless technology is an important part of the OCEAView solution. Here is a link to the official LoRaWAN specifications: https://lora-alliance.org/sites/default/files/2018-07/lorawan1.0.3.pdf

Architecture

This chapter presents the security mechanisms used for communication between OCEASOFT products and the OCEAView web application. The same security rules apply to both Cloud installations and on-premise installations.

Here is a high-level diagram showing the current OCEAView architecture and communication protocols used between our different products.



© 2020 OCEASOFT. All rights reserved.

Cobalt X data loggers ➔ LoRaWAN gateway ➔ OCEAView

In LoRaWAN mode, Cobalt X data loggers emit wireless data packets that are captured by all active LoRaWAN gateways within wireless range. The gateways then forward data packets to the OCEAView web server.

Cobalt X data loggers are not associated with a specific gateway, and they have no way of knowing whether any gateway received wireless data packets. As far as the Cobalt X is concerned, packets are simply broadcast and the gateways within range transmit them to the OCEAView web server. The gateways themselves do not integrate any complex embedded business logic. They simply serve as a pass-through tool that converts radio packets into UDP (User Datagram Protocol) packets and vice-versa.

All Cobalt X data transmissions are encrypted and signed using AES128, as described in the LoRaWAN specifications.

The Cobalt X uses the "OTAA Join" (over-the-air-activation) mechanism to reach the LoRaWAN server hosted on the OCEAView Cloud. Unique AES (Advanced Encryption Standard) keys are exchanged between the LoRaWAN server and the Cobalt X device during the Join procedure. As a result, the LoRaWAN server is the only entity able to decrypt and handle packets from that device. Furthermore, each Cobalt X data logger has a unique AES key that is completely private and not shared with other modules.

The gateway transmits packets via the UDP protocol to the server: UDP packets are not encrypted and they encapsulate a readable JSON packet with radio information such as frequency, spreading factor, and other details. The global payload from a Cobalt X device remains encrypted using AES and is transmitted as-is to OCEAView Cloud.

In additional to encryption, LoRaWAN packet are signed to guarantee their integrity and ensure that data cannot be altered. This is described in detail in the section "Message Integrity Code or MIC" in the LoRaWAN specifications.

OCEASOFT Bluetooth device ➔ OCEAView Mobile application or OCEABridge gateway ➔ OCEAView

OCEASOFT Bluetooth devices, namely Emerald and Atlas data loggers, as well as Cobalt X running in Bluetooth mode, use the Bluetooth Low Energy (BLE) protocol to communicate with the OCEAView Mobile application and OCEABridge gateway. OCEASOFT implements proprietary controls for communication so that standard Bluetooth devices and applications cannot interact with any OCEASOFT Bluetooth-enabled products. Only OCEASOFT applications have the technology to encode, decode, and interpret Bluetooth packets from OCEASOFT Bluetooth hardware devices.

The BLE protocol itself is not encrypted. Data is transmitted "in clear text" between OCEASOFT products.

Once data is extracted from the BLE device, it is transmitted to the OCEAView web platform through an iOS or Android mobile application or OCEABridge. Communication between applications and the OCEAView Cloud takes place via HTTPS using OAuth 2.0. This means that only OCEASOFT applications can transmit packets to the OCEAView Cloud platform.

© 2020 OCEASOFT. All rights reserved.

Emerald/Atlas data loggers as remote (Bluetooth) sensors for Cobalt X

OCEASOFT Emerald and Atlas modules can be connected and associated with a Cobalt X data loggers over a BLE link, thus behaving as a remote or wireless sensor. Their role is to periodically read their integrated sensor and broadcast values via a BLE advertising frame. The BLE frame is not encrypted and readings are sent in clear text. Any BLE device within wireless range can "listen" and catch this frame. As a very simple sensor, Emerald and Atlas modules do not contain any sensitive information and are not responsible for computing alarms. Their role is limited to reading sensors and broadcasting readings to be picked up by the paired Cobalt X, just like a standard sensor or OCEASOFT Smart-Sensor connected by wire.

OCEASOFT LoRaWAN gateway security

The OCEASOFT LoRaWAN gateway is based on a hardware platform provided by Multitech, using the official Multitech AEP 5.x firmware. However, OCEASOFT has its own firmware version based on the official firmware, notably including default settings to prevent customers from making configuration mistakes and for simplicity purposes. The changes made to the Multitech firmware by OCEAOSFT are as follows:

- Added a LoRaWAN server Test button in LoRaWAN page for debugging purpose
- Preconfigured LoRa frequencies in LoRaWAN page with OCEASOFT supported frequencies
- Preconfigured network interfaces in order to have a working fallback setup by default
- Preconfigured Wi-Fi settings to scan and list Wi-Fi networks upon first boot

OCEASOFT does not make any changes to Multitech security rules and implementations, relying on Multitech firmware for security. Only required firewall ports are opened, according to the customer's server configuration. OCEASOFT makes every effort to keep our products current with respect to Multitech updates.

The official AEP 5.X release notes are available here:

- http://www.multitech.net/developer/downloads/
- https://www.multitech.com/documents/publications/sales-flyers/PCN%20062619-AEP-01_mPower%20-AEP%20and%20mLinux-.pdf

© 2020 OCEASOFT. All rights reserved.

OCEAView Cloud Security for IT

This chapter describes OCEAView Cloud security aspects, notably with respect to IT considerations. Some of the sections do not apply to on-premise installations. Furthermore, on-premise installations are not directly under OCEASOFT's responsibility. In particular, our on-premise customers are responsible for **Securing** and **Backing-up** their own servers.

Hosting

All OCEAView production servers are hosted on Amazon Web Services (AWS). As of this writing, all AWS servers are located at the same data center in America.

Network security

All OCEAView production servers are located inside a VPC (Virtual Private Cloud) where only the front server is open to the outside world. The platform is accessible to customers over HTTPS using TLS v1.2 (non-secure HTTP is entirely banned).

For support and maintenance access, only the OCEASOFT Public IP is authorized to access Amazon server over RDP. This means that only people physically present at OCEASOFT can reach our server for maintenance. In addition, only an extremely limited number of trusted people have access to this RDP account.

Each virtual machine used by the solution is equipped with:

- Its own operating system firewall with only required ports opened
- Its own AWS security group setup, only opening the exact ports needed
- IP filtering applied to the opened ports

The database instance is only accessible through the back-end server inside the VPC.

System security

- Our system is updated regularly, with Windows Defender anti-virus set up for real-time protection and automatic updates.
- Server passwords are generated.
- A strong password policy is enforced on each server (including password history, minimum password age, maximum password age, password complexity…)
- Only authorized users can access the servers (RDP only) and AWS console
    - Servers: lead developers and system administrators
    - AWS console: system administrators only
- If a developer requires RDP access to one of ours servers, an Administrator provides a password, which is changed as soon as the developer's tasks are complete.

© 2020 OCEASOFT. All rights reserved.

Software data security

- Data Privacy Laws: the overall OCEAView solution is fully compliant with regulations applicable to our business (GDPR)
- Encryption in Transit: data is encrypted in transit using the SSL/TLS protocol to reduce the risk of a third-party intercepting data as it moves to and from the Cloud
- Data integrity: checksum is performed on the Audit Trail (we also plan to run checksum on sensor readings)
- Data retention period: defined by customer contract/SLA (Service Level Agreement)

Application security

- Anonymous Use Policy: the service only allows usage by authenticated users with valid accounts
- Identity Federation Method: OAUTH protocol
- Password policy for customer accounts: 8 alphanumeric characters, mixed case, no default password, expiration policy defined by customer
- Security for data at rest: IdentityServer 4 (SSO with OpenID Connect and OAuth 2.0 - token with expiration defined by scope) + HTTPS
- SSL certificate

Scalability

The OCEAView solution is scalable both horizontally and vertically to meet customer needs.

- Horizontal scalability (increasing capacity by adding more machines) is achieved by implementing additional back-end servers and database servers depending on server usage.
- Vertical scalability (increasing capacity by adding more power to existing machines) is achieved by upgrading our server capacity using AWS, notably with respect to CPU, RAM, and storage.

Monitoring

The server infrastructure is monitored attentively using Zabbix. Monitoring is performed at the hardware level (disk I/O, disk usage, RAM, CPU, bandwidth…) and software level (services, URL access, database size…). If any of these components reaches the limit of malfunction, an e-mail alert is triggered and sent to appropriate people in charge of proactively taking care of the problem to prevent it from occurring.

In addition, AWS alarms are also set at a per-instance level.

© 2020 OCEASOFT. All rights reserved.

Backups

All of OCEASOFT's AWS instances are backed up 4 times a day, from Monday to Friday (8:00 AM, 12:00 PM, 4:00 PM, and 8:00 PM GMT +1) and 1 time per day on Saturday and Sunday (12:00 PM GMT +1).

The entire instance is backed up each time and stored on AWS S3 Cloud storage.

All backups are kept for 31 days. We test these backups regularly in a separate environment to make sure backups are coherent and data integrity is preserved.

Password management

Cobalt X module

Cobalt X data loggers do not store any password information.

When a user enters their PIN code on the data logger screen to access advanced functions, such as alarm acknowledgment, the validity of the 6-digit PIN code is checked locally by checking that the last two digits are the result of a hash algorithm applied to the first four digits. This hash algorithm is specific and unique to every company: a PIN code used by a user at one company does not work for another company.

OCEASOFT LoRaWAN gateway

The OCEASOFT LoRaWAN gateway does not contain or require any password information related to OCEAView or Cobalt X.

A password is used to connect the Web configuration UI. That password must be defined upon first use, as there is no default password. The user is prompted to set the password after the very first boot. This password is strictly local to the gateway, used only by the gateway, and managed by the gateway's proprietary software.

OCEAView server

OCEASOFT has implemented a dedicated identity server to handle user credentials for both authorization and authentication. The identity server communicates with the OCEAView application server via https.

The server is based on the industry-standard OAuth 2.0 protocol, with the OpenID Connect framework layer on top. Once a user's credentials are validated, a specific token is generated for further API calls.

Passwords must be at least 8 characters long and contain a combination of upper- and lower-case letters with at least one number and one special character. The account is automatically locked after 3 failed login attempts and the user must reset their password.

© 2020 OCEASOFT. All rights reserved.

OCEAlert notification system

OCEAlert involves password management. The OCEAlert alert system's functionality is activated based on a license key provided by OCEASOFT and the customer's e-mail address. The license key is given to the customer, and a unique identifier (password) is created automatically based on the customer's e-mail address and a hash calculation using the license key in order to enable calls to OCEAlert services. The e-mail address and unique identifier are used for API calls.

© 2020 OCEASOFT. All rights reserved.