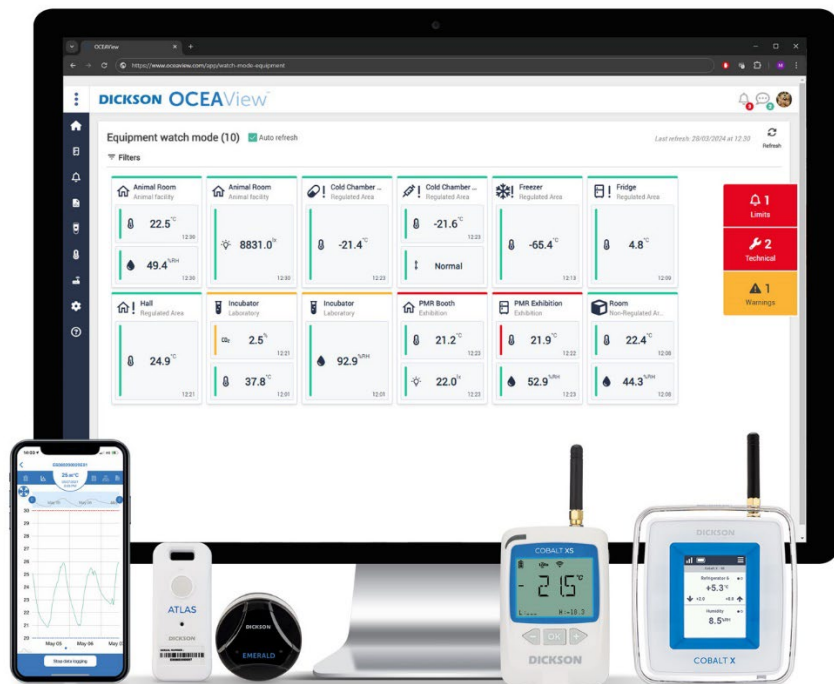


# OCEAView™

## Monitoring Solution

Web application  
for Dickson data loggers



## General notices and safety

### Disclaimer and limitation of liability

Dickson assumes no liability for any loss or claims by third parties which may arise through the use of this product. Users must not use the product in any manner not specifically indicated by Dickson. Dickson shall not be held liable for improper use of this product. This document is non-contractual and subject to change without notice.

### Safety instructions

**IMPORTANT SAFETY NOTE:** Do not use this product for protection or as part of an automated emergency system or for any other application that involves protecting people and/or property. This product is designed for use in environments where children are not likely to be present. Customers and users of Dickson products are responsible for making sure that the product is fit for the intended usage. Do not open the product casing and do not disassemble or modify internal components in any manner. Dickson products do not contain any internal components that require user intervention or repair. If the device shows signs of improper operation, disconnect it immediately from its power source or remove the battery and contact Dickson technical services.

#### Dickson Europe

Montpellier – France  
+33 499 13 67 30  
contact@dicksondata.fr

#### Dickson North America

Addison, IL – USA  
+1 (630) 543-3747  
contact@dicksondata.com

#### Dickson Asia-Pacific

Petaling Jaya – Malaysia  
+603 749 40758  
contact@dicksondata.my

© 2025 Dickson. All rights reserved. Dickson, the Dickson logo, Cobalt XS, Cobalt XS Wi-Fi, Cobalt X1, Cobalt X2, Cobalt L3, Cobalt ML3, and OCEAView are the exclusive property of Dickson. The LoRa® name and associated logo are trademarks of Semtech Corporation or its subsidiaries. Semtech, the Semtech logo and LoRa® are registered trademarks of Semtech Corporation. LoRaWAN® is a trademark of Semtech Corporation. The Bluetooth® word mark and logos are owned by Bluetooth SIG, Inc. All other brands are the property of their respective owners. Specifications subject to change without notice. Images are non-contractual.

Document updated for OCEAView 1.19.x.

November 2025

Ref: ING-INS-178-EN

Rev. 25

## Table of contents

General notices and safety .....	2
<b>1 Introduction.....</b>	<b>9</b>
1.1 Welcome to OCEAView .....	9
1.2 About this manual.....	9
1.2.1 Terminology used in this document.....	10
1.3 Overview of OCEAView .....	11
1.3.1 OCEAView feature highlights .....	12
1.3.2 Prerequisites for using OCEAView.....	13
1.3.3 OCEAView Cloud access requirements .....	13
1.3.4 OCEAView On-premises access.....	13
<b>2 Getting started.....</b>	<b>14</b>
2.1 OCEAView login.....	14
2.1.1 Logging in (internal authentication, LDAP, or SSO).....	17
2.2 Creating your OCEAView company account.....	21
2.2.1 Company information .....	23
2.2.2 User information for the first Application Manager.....	26
2.2.3 First login to the application .....	28
2.3 Forgot your password? .....	30
<b>3 Using OCEAView .....</b>	<b>32</b>
3.1 Presentation of the user interface .....	32
3.1.1 Main menu .....	33
3.1.2 Side-bar indicators .....	35
3.1.3 Using filters .....	38
<b>4 Home screen overview .....</b>	<b>39</b>
4.1 Plan view.....	40
4.2 Equipment and sensor watch mode .....	41
4.2.1 Equipment tile presentation .....	42
4.2.2 Sensor status indication color codes.....	42
4.2.3 Equipment status color codes .....	43
4.2.4 Examples .....	44
4.2.5 Sensor details with and without warnings or alarms .....	45
4.2.6 Alarms and warnings panels .....	49
4.2.7 Sensor display for dry contact input sensors (Cobalt X1/X2 only).....	50
<b>5 Users and authentication modes.....</b>	<b>51</b>

<b>5.1</b>	<b>Connection authentication modes .....</b>	<b>51</b>
5.1.1	Default integrated user authentication.....	52
5.1.2	Adding an external identity provider .....	52
5.1.3	Editing an external authentication platform .....	59
5.1.4	Options for external authentication platforms .....	61
<b>5.2</b>	<b>User accounts .....</b>	<b>63</b>
5.2.1	Creating a new account .....	63
5.2.2	Menu access based on profiles, permissions, and roles .....	67
5.2.3	User details overview .....	69
<b>5.3</b>	<b>Editing an account.....</b>	<b>70</b>
5.3.1	Assigning application permissions to "User" profile accounts .....	72
5.3.2	Note about notifications related to account permissions .....	75
5.3.3	Updating contact details .....	76
5.3.4	Personalizing an account picture .....	78
<b>5.4</b>	<b>Managing "Out of Office".....</b>	<b>80</b>
<b>5.5</b>	<b>Managing passwords (internal authentication only).....</b>	<b>82</b>
5.5.1	Changing your own password .....	82
5.5.2	Resetting another user's password .....	82
5.5.3	Resetting your own password.....	84
<b>5.6</b>	<b>Adding user roles .....</b>	<b>85</b>
5.6.1	Overview: role permissions vs. application permissions .....	85
5.6.2	Creating new roles .....	85
<b>6</b>	<b>Setting up your organization.....</b>	<b>88</b>
<b>6.1</b>	<b>Updating company information .....</b>	<b>88</b>
6.1.1	General information .....	88
6.1.2	Enabling the report review & approval process.....	90
6.1.3	Managing license keys.....	91
6.1.4	Renewing or expanding your current license .....	93
6.1.5	License expiration e-mail reminders.....	93
6.1.6	Renewing an expired OCEAView license .....	94
<b>6.2</b>	<b>System security settings.....</b>	<b>95</b>
6.2.1	Password policy .....	95
6.2.2	Granting access to external applications .....	97
<b>6.3</b>	<b>Organizing your system with sites and departments.....</b>	<b>99</b>
6.3.1	Adding sites.....	101
6.3.2	Adding departments.....	102
6.3.3	Editing / deleting a site or department.....	103
6.3.4	Assigning a user role in your organization's hierarchy .....	103

6.3.5	Viewing equipment and infrastructure in your organization.....	106
<b>6.4</b>	<b>Site plan images.....</b>	<b>107</b>
6.4.1	Adding a plan.....	107
6.4.2	Editing or deleting a plan .....	109
6.4.3	Placing equipment on the plan.....	110
<b>7</b>	<b>Infrastructure: Wireless gateways .....</b>	<b>111</b>
7.1	Note about LoRaWAN gateway as infrastructure .....	111
7.2	Adding a LoRaWAN or OCEABridge gateway .....	113
7.3	Editing infrastructure information .....	115
<b>8</b>	<b>Infrastructure: Siren &amp; Dry Contact alert devices .....</b>	<b>116</b>
8.1	Adding a Dickson LoRaWAN Siren.....	117
8.1.1	Testing your LoRaWAN Siren.....	120
8.1.2	Other LoRaWAN Siren functions .....	121
8.2	Adding a Dickson LoRaWAN Dry Contact device.....	122
8.2.1	Testing your LoRaWAN Dry Contact device.....	125
8.2.2	Other LoRaWAN Dry Contact device functions.....	126
8.2.3	Terminal wiring on Dry Contact device .....	127
<b>9</b>	<b>Data loggers.....</b>	<b>129</b>
9.1	Adding data loggers.....	129
9.1.1	Adding a data logger manually .....	129
9.1.2	Importing a batch of data loggers.....	132
9.1.3	Adding Atlas and Emerald data loggers with OCEAView Mobile.....	134
9.2	Viewing the data logger list .....	135
9.3	Viewing data logger details .....	136
9.4	Data logger actions .....	139
9.5	Editing data logger details (transfer/retransfer interval).....	140
<b>10</b>	<b>Sensors .....</b>	<b>143</b>
10.1	Sensor summary list .....	144
10.2	Individual sensor details.....	145
10.3	Filtering the sensor list display .....	147
10.4	Calibration parameters.....	149
10.4.1	Editing parameters for calibrated sensors.....	149
10.4.2	Calibration reminder frequency.....	151
10.4.3	Importing CSV file with calibration information .....	152
10.4.4	Error messages when importing a calibration CSV file .....	155
10.4.5	Exporting sensor information.....	156

10.5	Using the Cobalt X1/X2 dry contact input sensor.....	157
10.6	Using Dickson 0-4 mA / 0-5 V / 0-10 V Smart-Sensors .....	158
10.6.1	Mapping values for meaningful readings .....	158
10.7	Simulating a sensor alarm for testing.....	159
10.8	Removing a sensor .....	159
10.9	Disabling /enabling a sensor .....	160
<b>11</b>	<b>Equipment.....</b>	<b>161</b>
11.1	Adding equipment.....	161
11.1.1	Associating sensors with equipment.....	163
11.1.2	Dissociating sensors from equipment.....	165
11.2	Viewing equipment details .....	166
11.3	Modifying / managing equipment.....	168
11.4	Deleting equipment.....	169
<b>12</b>	<b>Data logging .....</b>	<b>170</b>
12.1	How does it work?.....	170
12.2	Setting up data logging.....	171
12.2.1	Environmental sensors (temperature, humidity, CO <sub>2</sub> , etc.) .....	174
12.2.2	Dry contact input sensors (Cobalt X1/X2 only) .....	178
12.3	Changing data logging settings on-the-fly.....	180
12.4	Stopping data logging.....	182
12.5	Note regarding reading interval vs transfer interval .....	184
12.6	Mobile monitoring considerations for Cobalt ML3 .....	185
12.6.1	Setting the sensor reading interval.....	185
12.6.2	Setting the data transfer interval.....	185
<b>13</b>	<b>Viewing sensor data.....</b>	<b>186</b>
13.1	Displaying sensor graphs .....	187
13.1.1	Displaying corrected limits on graphs .....	188
13.1.2	Selecting the display period.....	189
13.1.3	Adding annotations to graph points .....	189
13.1.4	Including events in graph display .....	192
13.1.5	Viewing paused alarm period .....	193
13.1.6	Zoom and control tools .....	194
13.1.7	Exporting sensor data .....	196
13.1.8	Multigraph views across different equipment.....	197
13.2	Listing and filtering sensor readings.....	203
<b>14</b>	<b>Generating reports.....</b>	<b>205</b>

<b>14.1</b>	<b>Downloading reports</b>	<b>205</b>
14.1.1	Sensor reading reports	206
14.1.2	Dry contact input sensor report	208
<b>14.2</b>	<b>Reviewing and approving reports</b>	<b>209</b>
14.2.1	Activating report review/approval for your company	209
14.2.2	Generating, reviewing, and approving reports	211
14.2.3	Accessing archived reports	216
<b>14.3</b>	<b>Alarm report subscriptions</b>	<b>217</b>
14.3.1	Scheduling a report	217
14.3.2	Editing scheduled reports and subscriptions	220
<b>14.4</b>	<b>Audit trail</b>	<b>222</b>
14.4.1	Exporting the audit trail	224
14.4.2	Filtering the audit trail	225
<b>15</b>	<b>Alarms &amp; alerts</b>	<b>227</b>
<b>15.1</b>	<b>Handling alarms</b>	<b>227</b>
15.1.1	Alarms highlighted in the watch mode screen	227
15.1.2	Viewing alarm details	230
15.1.3	Filtering alarms and warnings	231
15.1.4	Acknowledging alarms	234
15.1.5	Editing acknowledged alarms	237
<b>15.2</b>	<b>Alert rules and notifications</b>	<b>238</b>
15.2.1	Configuring alert rules	238
15.2.2	Alert rules with users	242
15.2.3	Alert rules with LoRaWAN Siren or Dry Contact devices	243
15.2.4	Modifying or deleting alert rules	245
<b>15.3</b>	<b>Filtering the alert rules display</b>	<b>246</b>
<b>15.4</b>	<b>Time slots</b>	<b>248</b>
15.4.1	Adding a time slot	248
15.4.2	Modifying or deleting time slots	249
15.4.3	Setting days off (weekends and non-working days)	250
15.4.4	Modifying or deleting weekends and days off	252
<b>16</b>	<b>Getting help / FAQ</b>	<b>253</b>
<b>16.1</b>	<b>User manuals</b>	<b>253</b>
<b>16.2</b>	<b>Contacting Dickson technical support</b>	<b>253</b>
<b>16.3</b>	<b>Viewing OCEAView version release notes</b>	<b>254</b>
<b>16.4</b>	<b>FAQ</b>	<b>255</b>
16.4.1	Data loggers & data logging	255

16.4.2 System & support.....	257
<b>17 Appendix 1 – Sensor reading report details.....</b>	<b>259</b>
17.1 Downloading reports .....	259
17.2 Applying filters.....	261
17.3 Understanding the alarms & warnings summary.....	261
17.4 Data logging details.....	265
17.5 Alarms & Warnings.....	266
17.6 Reading summary and reading detail.....	266
<b>18 Appendix 2 – Tracking OCEAView Cloud system status .....</b>	<b>268</b>
18.1 Overview of the OCEAView Status Dashboard .....	268
18.2 The different statuses.....	269
18.3 Accessing the OCEAView Status Dashboard.....	269

# 1 Introduction

## 1.1 Welcome to OCEAView

Congratulations! Thank you for choosing OCEAView.

This user guide describes how to use the OCEAView web application to manage and monitor Dickson wireless data loggers featuring LoRaWAN™ long-range wireless connectivity and supported data loggers offering Bluetooth wireless connectivity.

Dickson data loggers collect data automatically from connected sensors and transmit that data to the Cloud. These data loggers are part of Dickson's latest generation of wireless IoT devices.

## 1.2 About this manual

This user guide describes how to use the many features offered by the OCEAView application.

Before using OCEAView, you must configure at least one of the following:

- Dickson LoRa gateway for data loggers using the LoRaWAN protocol in a Cloud or private (on-premises) network. LoRaWAN is supported by Cobalt XS, Cobalt X1/X2, Cobalt L3, and Cobalt ML3 data loggers, as well as Dickson's Alert Siren and Alert Relay devices.
- Dickson OCEABridge gateway for data loggers using Bluetooth connectivity. Bluetooth is supported by Cobalt X1/X2 data loggers.

See Dickson LoRaWAN gateway or OCEABridge gateway instructions for more details.

### 1.2.1 Terminology used in this document

Here is a list of terms frequently used when working with the OCEAView solution.

<b>Alarm</b>	An alarm is a state that occurs when the system observes a sensor reading that is outside its target range (an "excursion"), such as a temperature reading, humidity level, or CO <sub>2</sub> value that is too high or too low with respect to programmed limits. The system can notify users when alarms occur by sending alerts. Alarms must be acknowledged by an authorized user. See also: <b>Warning</b> .
<b>Alert</b>	An alert is a notification sent by the system to users when the system observes an alarm or warning condition or potential problem. Alerts can be sent by e-mail, SMS, or voice calls.
<b>Bluetooth®</b>	Bluetooth Low Energy, also known as Bluetooth Smart® or BLE, offers point-to-point wireless connectivity with a practical range of up to about 30 meters (about 100 feet).
<b>Data logger</b>	Refers to Cobalt and/or other Dickson wireless data logger devices
<b>Equipment</b>	The material or space that you are monitoring with a data logger and sensor.
<b>LoRaWAN®</b>	Very-long-range wireless communication protocol available with public or private network connectivity. Free-field wireless range can reach up to nearly 10 miles (about 15 km).
<b>Organization</b>	Refers to your company and its organizational structure based on sites and departments created within the solution.
<b>Profile</b>	The term "profile" in OCEAView refers explicitly to Application Manager and User profiles. Every account is assigned one of these two profiles. Accounts with an Application Manager profile can control every aspect of the system (including changing other users' profiles, but not their own). Accounts with a User profile start with view-only permissions, and additional application-wide permissions can be added to their individual account as well as to a "role" (see <i>below</i> ) assigned within the organizational structure.
<b>Role</b>	The "role" represents a very flexible feature that grants users further permissions so they can perform a variety of day-to-day tasks at their organizational level.
<b>Warning</b>	A warning alerts users when a sensor reading reaches a programmed limit during data logging. Unlike alarms, warnings do not need to be acknowledged by a user.

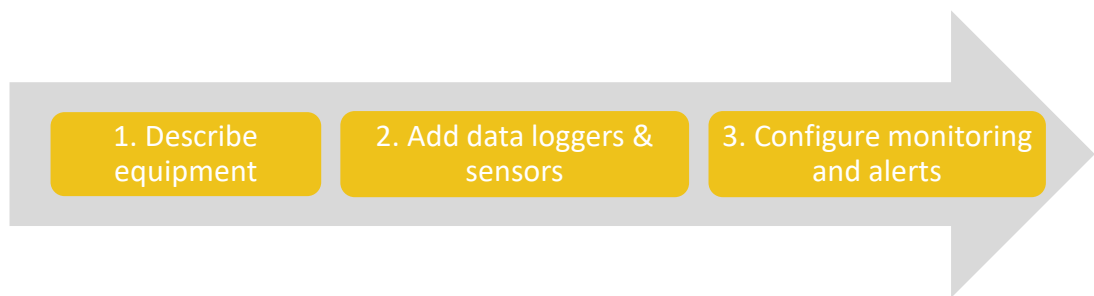
## 1.3 Overview of OCEAView

The OCEAView concept is based on managing sensors that are assigned to entities called "equipment". Equipment refers to any assets (such as refrigerators and freezers), rooms, or locations in/on which sensors may be placed.

The overall process for using OCEAView is divided into distinct steps:

1. You must first order a **license key** to cover the number of sensors you will be using. Please contact your sales representative for more information.
2. Then, use OCEAView to create your company account, add users, and set up your equipment.

The general process for configuring OCEAView, as detailed in this user guide, is as follows:



*Figure 1 - Process overview*

Understanding these three aspects is important for using OCEAView, as summarized below:

### 1. Describe equipment

The notion of equipment is the central principle for sensor monitoring with OCEAView. This approach is based on the idea that you are more likely concerned about the assets you are monitoring than the tool used to accomplish the task. For example, you monitor equipment, such as a cold room, refrigerator, deep freezer, or incubator. You therefore must add these entities to your system.

### 2. Add data loggers & sensors

Equipment is monitored by one or more sensors attached to data loggers, for recording temperature, humidity, CO<sub>2</sub>, etc. at regular intervals. Sensors are listed automatically in OCEAView when the data logger to which they are attached is added to the system.

### 3. Configure monitoring

Different equipment may have different needs in terms of monitoring. Sensors must therefore be configured to monitor different ranges, at different reading frequencies, with different alert strategies, etc.

### 1.3.1 OCEAView feature highlights

OCEAView enables you to visualize supported Dickson data logger sensors and data, with a complete management interface for configuration and system administration.

Key application features:

#### **User and license management**

- Create company and user accounts
- Internal, LDAP, or SSO authentication (including support for multifactor and passwordless authentication, and Federated SSO)
- Manage users, roles, and application permissions
- Manage license keys
- Manage your company's organization with different sites and departments
- Benefit from FDA 21 CFR Part 11 guideline compatibility
  - o Readings and settings stored in secure database
  - o Password protection and configurable policy

#### **Data**

- Configure sensors, gateways, and infrastructure components
- View data recorded by Dickson data loggers
- Monitor equipment and associated sensors
- Manage data transmitted by Dickson data loggers
- View detailed sensor readings, history, single- and multi-sensor graphs, and more
- Manage sensor calibrations and reminders
- Import / export sensor calibration information
- Access a detailed audit trail

#### **Alarms & warnings**

- Configure and send alerts when alarms and/or warnings are detected
- Manage alarms and warnings: high/low limits, technical alarms (sensor or communication problems), alert devices, and more
- Pause alarms and warnings from 30 minutes to 72 hours
- Set up flexible user notification scheduling for days, nights, and weekends according to user level and desired contact methods
- Receive notification by e-mail; SMS/text message and voice call with optional OCEAlert subscription

#### **Reports**

- Generate reports for all key parameters, including configuration, status, events, and alarms
- Schedule reports
- Review and approve reports

### 1.3.2 Prerequisites for using OCEAView

OCEAView is a web application designed to work with standard web browsers.

The minimum system requirements are as follows:

- Personal computer
- Internet connection
- Screen resolution 1280 x 900 pixels minimum
- Recommended browsers:

Web browser applications evolve quickly, and we do our best to keep the OCEAView application compatible with the latest releases. The following were used to test the current version:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Opera

### 1.3.3 OCEAView Cloud access requirements

When using OCEAView as a Cloud solution, the following ports must be added to your network's safelist according to the physical location of your OCEAView data center:

Purpose	URL	Port	Protocol
For users: OCEAView web application	<b>Americas:</b> <a href="https://app-us.oceaview.com/">https://app-us.oceaview.com/</a> <b>Europe:</b> <a href="https://app-eu.oceaview.com/">https://app-eu.oceaview.com/</a> <b>Asia-Pacific:</b> <a href="https://app-asia.oceaview.com/">https://app-asia.oceaview.com/</a>	443	HTTPS
For infrastructure: LoRaWAN gateway and/or OCEABridge gateway connection	<b>Americas:</b> <a href="https://connect-us.oceaview.com">connect-us.oceaview.com</a> <b>Europe/EMEA:</b> <a href="https://connect-eu.oceaview.com">connect-eu.oceaview.com</a> <b>Asia-Pacific:</b> <a href="https://connect-asia.oceaview.com">connect-asia.oceaview.com</a>	1700	UDP

These ports are used for two-way communications between the OCEAView web application running in your browser and the server platform on the Cloud.

### 1.3.4 OCEAView On-premises access

With your OCEAView solution running on your company's internal network, simply connect using the URL provided to you by your IT department.

## 2 Getting started

This section describes how to:

1. Create an account on the OCEAView web application
2. Login to OCEAView



This section assumes that you have purchased a license key and that you have that number available. Please contact your sales representative if you need more information.

---

### 2.1 OCEAView login

As for most web applications, you must login to the OCEAView web platform to use the software.

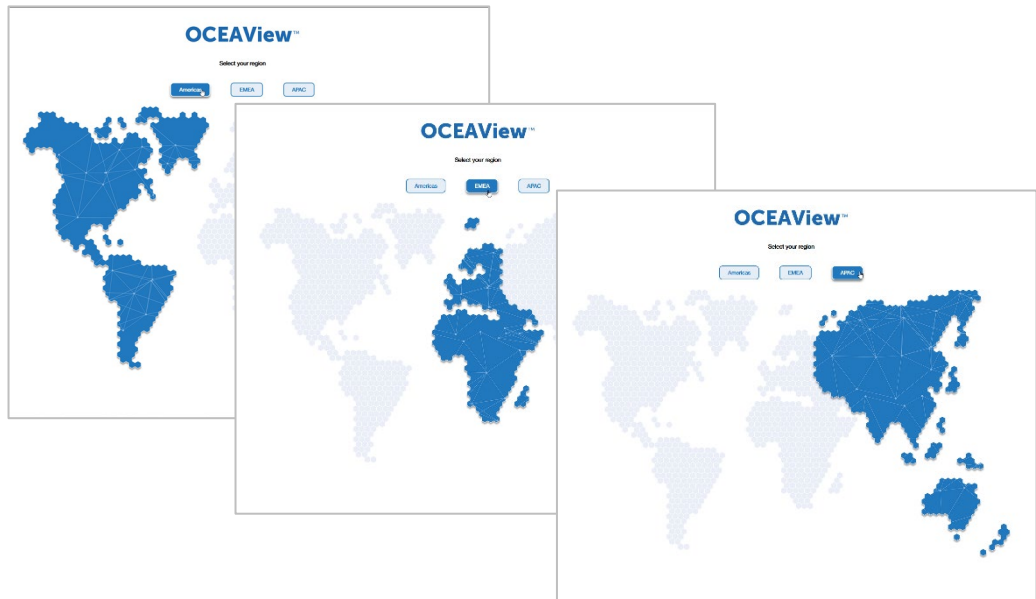
1. Launch your Internet browser application.
2. Open the URL for the region in which your company was created:  
app-us.oceaview.com (North America and South America)  
app-eu.oceaview.com (Europe)  
app-asia.oceaview.com (Asia-Pacific)
3. Alternatively, you can go to the address: [www.oceaview.com](http://www.oceaview.com) and select your region:



Figure 2 – Selecting your region



You must choose the correct region here, otherwise your username will not be recognized and you will not be able to log in to the system.



*Figure 3 – Choose the region corresponding to your organization's platform*

## Getting started

4. The application detects your browser language automatically and displays the login window either in English, French, German, Italian, Spanish, or Portuguese. For all other languages, English is used:

**DICKSON**  
Environmental Monitoring + Compliance Experts

**OCEAView™**

Username \*

Password \*

[Forgot password?](#)

**Log in**

or

**Use your organization's login**

[Not registered? New company](#)

Figure 4 – General login window (login)

### 2.1.1 Logging in (internal authentication, LDAP, or SSO)

OCEAView supports different authentication methods as described below:

Authentication type	Supported OCEAView platform(s)	Comments
<b>Internal</b>	OCEAView Cloud and OCEAView On-Premises	Username and password are created and managed within OCEAView
<b>SSO</b> (Single Sign-On)	OCEAView Cloud and OCEAView On-Premises	Username and password are defined at an organization-wide level, outside OCEAView, and thus are the same as those used for other everyday applications. SSO must be configured correctly on your authentication server, including the first name, last name, e-mail address, and username. See the FAQ section in this guide for more details.
<b>LDAP</b> (Lightweight Directory Access Protocol)	OCEAView On-Premises	Username and password are managed from a centralized active directory service outside OCEAView.



For your LDAP or SSO connection, you will need to know the *authentication mode name* configured in OCEAView, as determined by the Application Manager who sets up the identity providers on your OCEAView platform.

#### Logging in with integrated OCEAView authentication

1. Enter your assigned username and password.
2. Click on **Log in** to enter the application.

Passwords are case sensitive and encrypted. If you forgot your password, click on **Forgot password**.

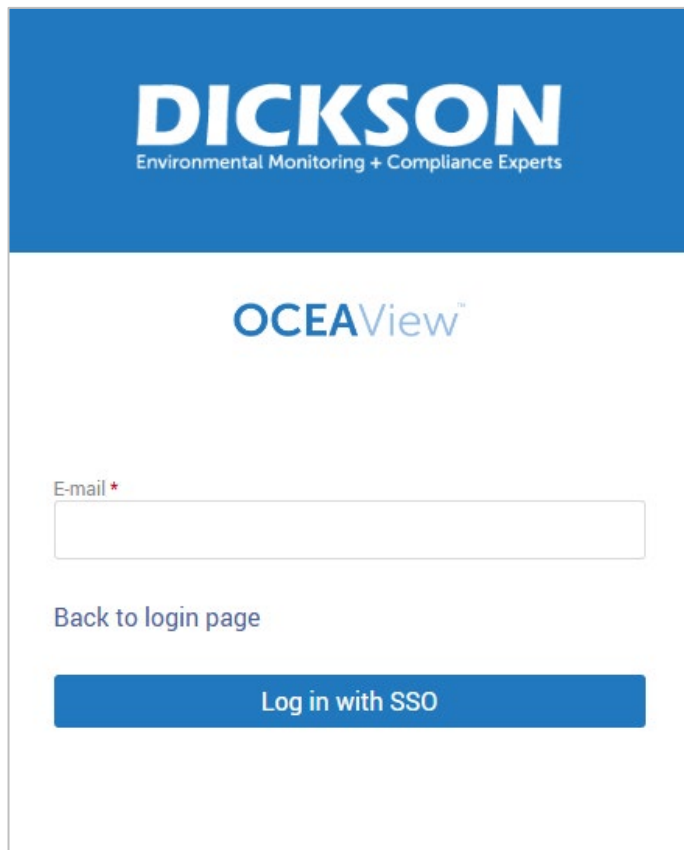
As a security measure, the account can be locked if **User lockout** is enabled in **Security → Password policy** (described in section 6.2 – *System security settings*, p. 95) and you enter an incorrect password the specified number of times consecutively. The only way to unlock the account is to reset the password. Proceed with the **Forgot password** procedure or contact an Application Manager to have them initiate the reset (which you must then complete in order to actually change the password).

### Logging in with LDAP (Lightweight Directory Access Protocol, available for on-premises solutions only)

1. Enter login details in the form "authentication\_mode\_name/username" and then enter your password.
2. Click on **Log in** to enter the application.

### Logging in with SSO (Single Sign-on)

1. Click on **Use your organization's login**. You will see this window:



The screenshot shows a web application login window. At the top, there is a blue banner with the 'DICKSON' logo in white, with the tagline 'Environmental Monitoring + Compliance Experts' underneath. Below this banner, the 'OCEAView™' logo is centered. Underneath the logo is an 'E-mail' input field with a red asterisk to its left. Below the input field is a blue link that says 'Back to login page'. At the bottom of the window is a prominent blue button with the text 'Log in with SSO' in white.

Figure 5 – SSO login window

2. Enter your enterprise e-mail address.
3. For your first login, you must provide the **Authentication mode name**, as configured by an Application Manager when setting up the authentication mode (described in section 5.1.2 – *Adding an external identity provider*, p. 52). On subsequent logins, you do not have to enter this information.

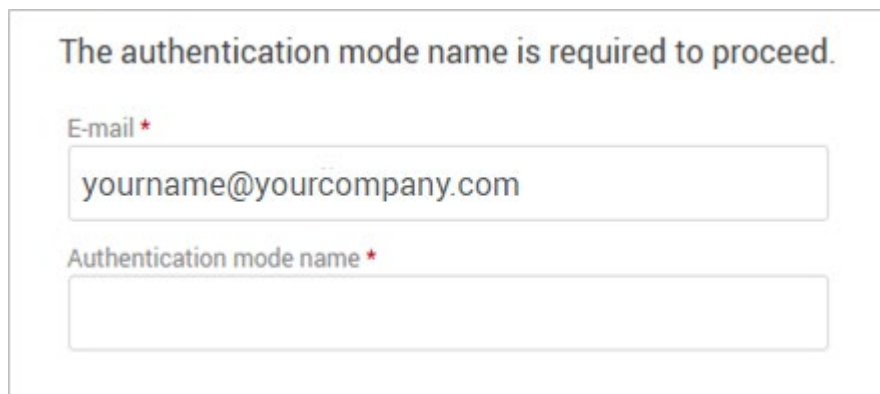


Figure 6 – Entering the OCEAView authentication mode name in the SSO login window

4. Click on **Log in with SSO** → complete the sign-in with your enterprise system e-mail address, password, and/or other multifactor mechanisms. to enter the application. Here is an example using Microsoft Entra as the identity provider:

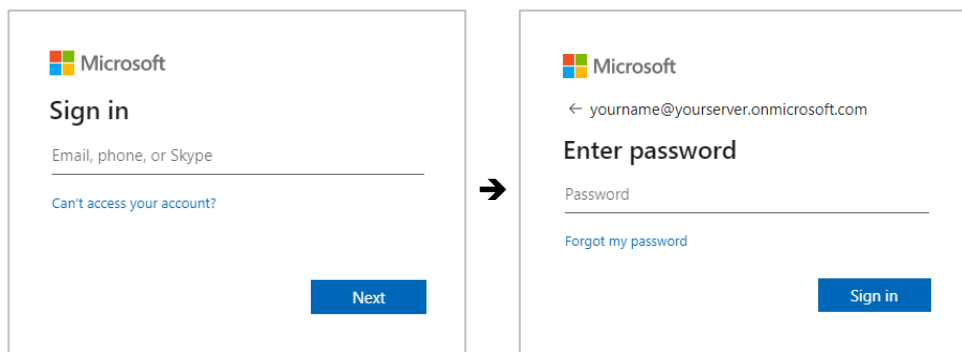


Figure 7 – Microsoft SSO authentication window



- For more information about users and setting up authentication modes, see chapter 5 – *Users and authentication modes*, p. 51.
-

## Changing the display language

The initial language used by OCEAView depends on your browser settings.

Once connected to OCEAView, you can change the application to a supported language at any time:

1. Click on your user account avatar at the top right-hand corner of the screen.
2. Click on **My account** → **More** (⋮) → **Edit localization settings**
3. Click on the **Language** and select the desired language from the list. You must log out and log back in to apply the change.

## Automatic system logout after inactivity

You will automatically be logged out of the OCEAView application after a period of inactivity, as follows:

- If you remain on one of the Watch Mode screens and the **Auto refresh** option is selected, you will be logged out after 12 hours of inactivity
- Anywhere else in the application, you will be logged out after 1 hour of inactivity
- If your session is used periodically and remains active, you will be logged out after 12 hours

To reconnect to the platform, enter your login credentials in the authentication screen.



The OCEAView application version is shown at the bottom of the login window. Move your mouse cursor over the version number if you want to see more information. This information may be requested if you need to contact the technical support team.

---

## 2.2 Creating your OCEAView company account

If you do not yet have an OCEAView account, you must create one to interact with and manage your data loggers.

You may add as many users as you want to an existing account at any time (more details are provided in section 5.2 – *User*, p. 63).



When you create your company in OCEAView, you also create the first user. That user has Application Manager rights and is authorized to create additional users via **Configuration → Users**.

---

### To create your company account: choose your region and create a first Application Manager user:

1. Use your web browser to open one of the addresses in the table below, according to the region in which you want your system to be hosted physically.



OCEAView datacenters operate on three distinct regional platforms to best serve customers around the world. The URL you use when creating your company in OCEAView determines which physical location is used.

The datacenter location has no impact on your local, national, and international use of the OCEAView solution. Your users must simply log in using the URL corresponding to the chosen region.

---

URL	Datacenter location
app-us.oceaview.com	United States (Ohio)
app-eu.oceaview.com	Europe (Ireland)
app-asia.oceaview.com	Asia-Pacific (Singapore)

Getting started

2. Beneath the login fields, click on **New company?**

**DICKSON**  
Environmental Monitoring + Compliance Experts

OCEAView™

Username \*

Password \*

[Forgot password?](#)

**Log in**

or

[Use your organization's login](#)

Not registered? **New company**

Figure 8 – Authentication window (login)

### 2.2.1 Company information

OCEAView includes a 2-step setup process for creating your company account and a first user account. That account has *Application Manager* rights and can configure the entire system and add other user accounts. The fields marked with \* are required.

The screenshot shows the 'Create a new account' form in the OCEAView application. The header includes the DICKSON logo (Environmental Monitoring + Compliance Experts) and the OCEAView logo. The form is titled 'Create a new account' and features a progress indicator with two steps: '1 Company' (active) and '2 User'. The form contains several input fields and dropdown menus:

- Company name \*** (text input)
- Platform \*** (text input)
- Company address** (text input)
- City** (text input)
- Postal code** (text input)
- Country** (text input)
- International phone no.** (text input, starting with '+...')
- Language** (dropdown menu, currently set to 'English')
- Time zone** (dropdown menu, currently set to '(UTC+01:00/+02:00) Brussels, Copenhagen, Ma...')
- Date format** (dropdown menu, currently set to 'dd/MM/yyyy')
- Time format** (dropdown menu, currently set to '12h AM-...')
- Unit** (dropdown menu, currently set to '°C')
- Decimal separator** (dropdown menu, currently set to ', (comma)')
- License key \*** (text input)

At the bottom of the form, there is a checkbox labeled 'I accept the [Subscription Terms](#)'. Below this, there are two buttons: 'Back to login page' and 'Next'.

Figure 9 – Filling in company information

1. Fill in the required fields (marked with **\***) as appropriate. You can change or update most of this information later if necessary:

<b>Company name</b>	Enter the name of your company. This name cannot be changed later.
<b>Platform</b>	Unique company identifier, filled in automatically based on the company name you enter.
<b>Company address...</b>	...City, Postal code, Country, International phone number: enter the relevant information for your company.



---

Make sure you enter the telephone number in international format, with the prefix "+country code", such as: +14153817894

Do not include any extra digits, characters, or leading zeros.

---

The following settings apply as the defaults for your system. They can be overridden by each person's individual settings for local operation and display purposes, but this information is used as a common reference for the company in case people have conflicting settings for shared actions. For example, if you have e-mail alerts sent to people in different regions, English could be the default company language for a same alert message.

<b>Language</b>	Choose the desired default language for your company. Users are free to choose their own personal preference at any time.
<b>Time zone</b>	Select the time zone based on the primary geographical area for the company.
<b>Date format</b>	Select how dates are displayed in the application.
<b>Time format</b>	Select how time is displayed in the application. Readings can be displayed in the <b>12-hour (AM/PM)</b> or <b>24-hour</b> format.
<b>Unit</b>	Temperature can be displayed in degrees <b>Celsius (°C)</b> or <b>Fahrenheit (°F)</b> .
<b>Decimal separator</b>	Select the character to use as a decimal separator in numerical values, either a period (.) or a comma (,).
<b>License key</b>	Enter your license key in this field. Based on the number of measurement points (sensors) in your system, this key is provided to you when you subscribe to OCEAView. License management is discussed in further detail in section <i>6.1 – Updating company information, p. 88</i> .

## Getting started

2. After completing all the company information, you must click the checkbox to accept the **Subscription Terms**, then click on **Next** to fill in your user information as described in the next section.
3. The system then confirms the region in which your company account is being created (where its datacenter is physically located). Click on **Continue** if the region is correct and you are ready to move on to the next step, or on **Cancel** to return to the company creation page.

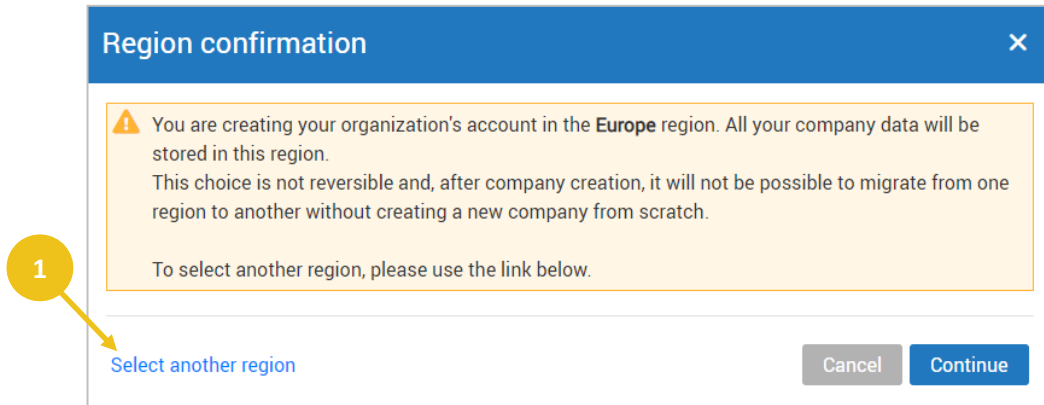


Figure 10 – Confirming the region when creating your company

If the indicated region is incorrect, click on **Select another region** ( 1 ) and choose the one that applies to your situation. Your license key will not be affected if you interrupt the process at this point. Click on **New company** again ( 2 ) and repeat the process.

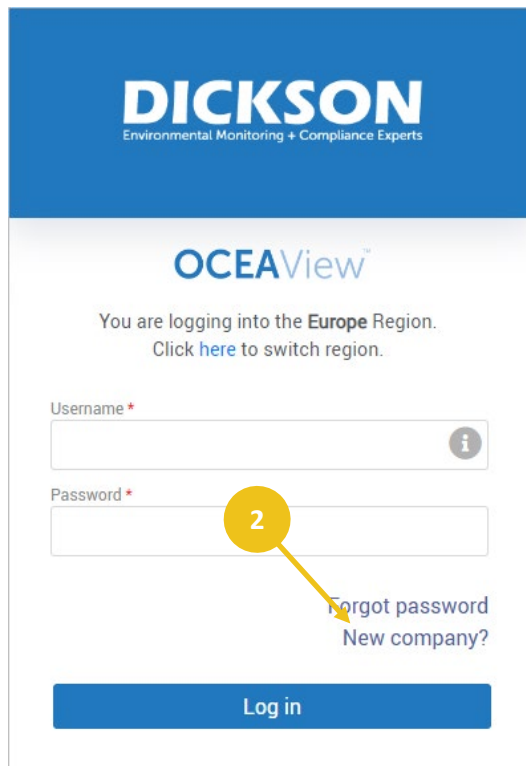


Figure 11 – Switching regions to use a different OCEAView datacenter

## 2.2.2 User information for the first Application Manager

Continue with the setup process by entering basic information for the first Application Manager user (with permissions to control the entire solution).



The e-mail address you enter here is the only information that you cannot change subsequently for your company account. We recommend using an e-mail address that is not strictly tied to a single person, that is, an impersonal address such as "oceaview@your\_company.name"

The screenshot shows the 'Create a new account' form. The header includes the 'DICKSON Environmental Monitoring + Compliance Experts' logo and the 'OCEAView' logo. The form title is 'Create a new account'. A progress bar indicates two steps: '1 Company' and '2 User'. The '2 User' step is active. The form contains the following fields: 'First name \*', 'Last name \*', 'E-mail \*', and 'Job title'. Below these fields is a checkbox labeled 'I accept the Terms of Use and the Privacy Policy Terms.' with a yellow callout '1' pointing to it. At the bottom, there are three buttons: 'Back to login page', 'Previous', and 'Proceed'.

Figure 12 – Entering user information

1. Fill in the required fields (marked with \*) as appropriate:

**First name / Last name** The user's full name.

**E-mail** The user's e-mail address, which is used to login to the system and receive e-mail alerts and confirmations sent by the system. The e-mail address must be unique and may not be edited once entered. A message is displayed if the e-mail address is already in use.

**Job title** The user's job function within their company.

2. After completing the information, click on the “**I accept the Terms of Use and the Privacy Policy Terms**” checkbox at the bottom of the screen <sup>1</sup> (you may click on **Terms of Use** and/or **Privacy Policy Terms** to see the detailed text) and then click on **Proceed**.

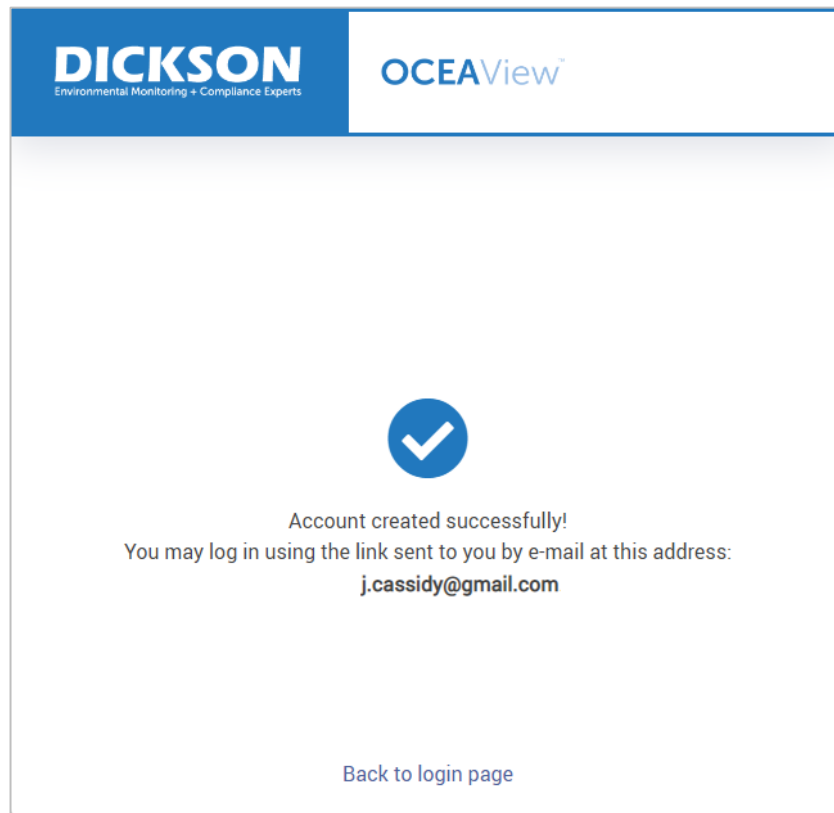


Figure 13 – OCEAView confirmation of account creation

3. Your account is created and confirmation e-mail is sent to the address you entered. Click on the link in the e-mail to activate the account.

## 2.2.3 First login to the application



This section applies to systems using OCEAView's internal authentication (based on the username and password). When using external identity providers, namely LDAP or SSO, use your regular enterprise login credentials.

If your system uses OCEAView's internal authentication mode, you are prompted to create a password the first time you login to the application.

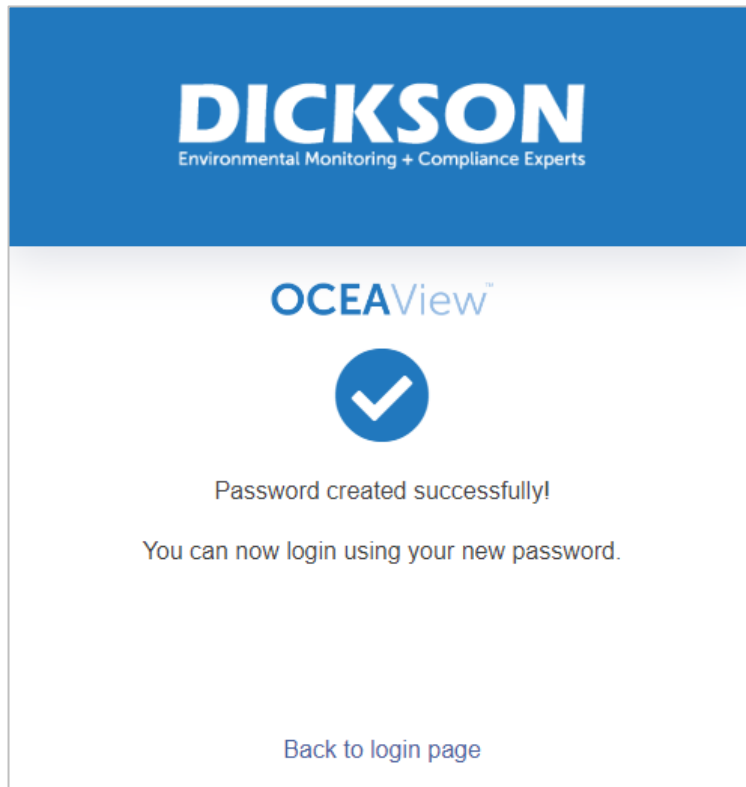
1. Check your e-mail inbox for the confirmation e-mail and click on the link provided. If you do not see the e-mail, check your spam or junk e-mail folders in case your e-mail application filtered it automatically.
2. After you click on the link, the following window opens so you can set your password:

The screenshot shows a web application window for creating a password. The header is blue with the 'DICKSON' logo and the tagline 'Environmental Monitoring + Compliance Experts'. The main content area is white and contains the text 'OCEAView™ Create password'. There are three input fields: 'E-mail \*' with the value 'jen.smith@gmail.com', 'Choose password \*', and 'Confirm password \*'. At the bottom right, there are 'Cancel' and 'OK' buttons.

Figure 14 – Creating a password upon first connection

3. Enter a new password. Passwords must respect your organization's password security policy (as described in section 6.2 – *System security settings*, p. 95).
4. Confirm the new password by re-typing it in the bottom field.

5. Click on **OK** when done to reset the password.



*Figure 15 – Successful password creation*

6. Click on **Back to login page** to connect to the application using your e-mail address and the password you created.

## 2.3 Forgot your password?



This section describes password recovery for systems using OCEAView's internal authentication mechanism. For external identity providers, namely LDAP or SSO, please check with your system administrator if you need help resetting a forgotten password.

If you are unable to access OCEAView or if you cannot remember your username or password, the system can send password reset instructions to you by e-mail.

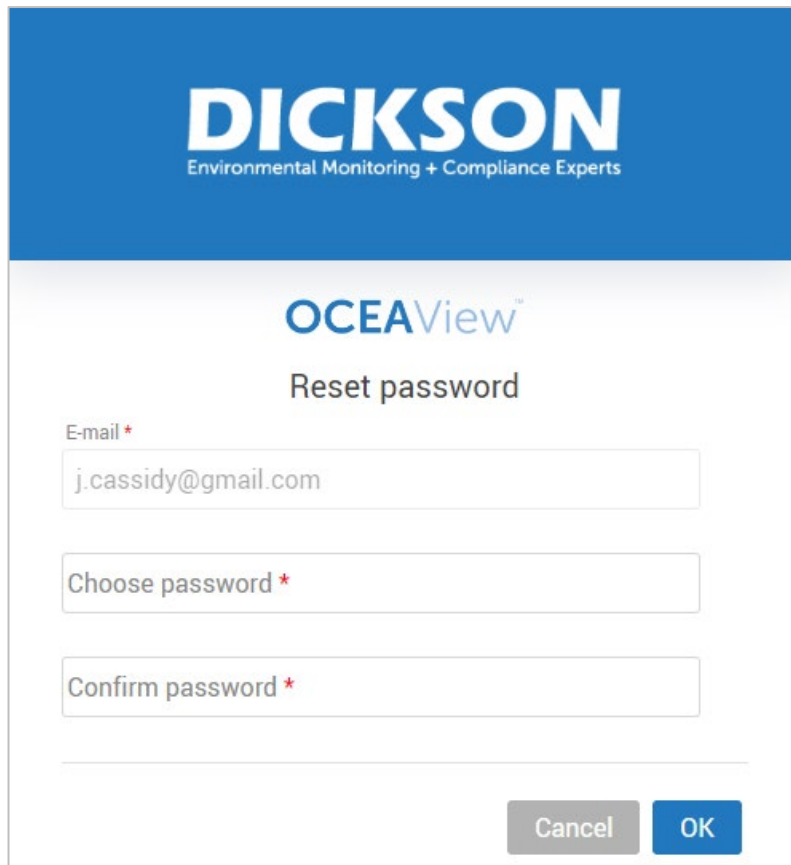
Follow these instructions if you need to reset your OCEAView password:

1. Use your browser to open the correct URL:  
app-us.oceaview.com, app-eu.oceaview.com, or app-asia.oceaview.com
2. Click on **Forgot password** on the login screen.
3. Enter your OCEAView account e-mail address and click on **OK**:

Figure 16 shows a dialog box titled "Password recovery" with a close button (X) in the top right corner. The main text inside the dialog says "Enter your e-mail address to receive a new password." Below this text is a text input field labeled "E-mail \*". At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

Figure 16 – Entering an e-mail address to receive a new password

4. Check your e-mail inbox and click on the link in the email you receive to assign a new password.



The screenshot shows a web application interface for password reset. At the top, there is a blue header with the 'DICKSON' logo in white, and the tagline 'Environmental Monitoring + Compliance Experts' below it. The main content area has a white background with the 'OCEAView' logo in blue. Below the logo, the text 'Reset password' is centered. There are three input fields: the first is labeled 'E-mail \*' and contains the text 'j.cassidy@gmail.com'; the second is labeled 'Choose password \*'; and the third is labeled 'Confirm password \*'. At the bottom right of the form, there are two buttons: a grey 'Cancel' button and a blue 'OK' button.

Figure 17 – Assigning a new password

5. Enter the new password in the first field, then retype it in the second field to confirm.
6. Click on **OK** to assign the new password, or on **Cancel** to keep your old password.

## 3 Using OCEAView

### 3.1 Presentation of the user interface

The OCEAView interface consists of the following main zones:

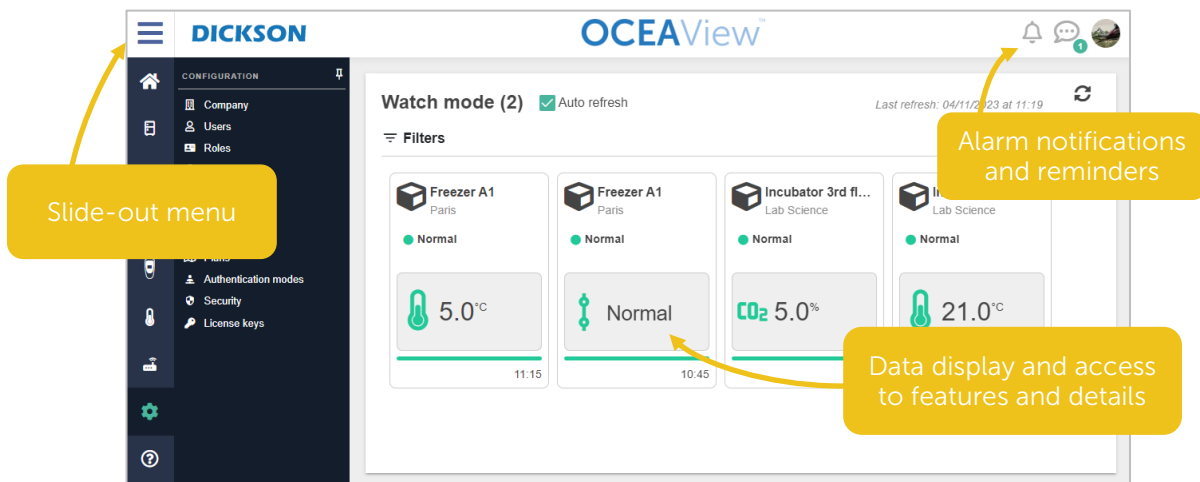


Figure 18 – Overview of OCEAView user interface

The Watch mode screen shown here gives you direct access to key features in your monitoring system.

### 3.1.1 Main menu

The main menu is located on the left-hand side of the screen, folded by default to save space on the screen. Click on the left-side menu links to access OCEAView features.

Depending on the context, the menu item will display a statistics pane or a sub-menu with additional features or information:

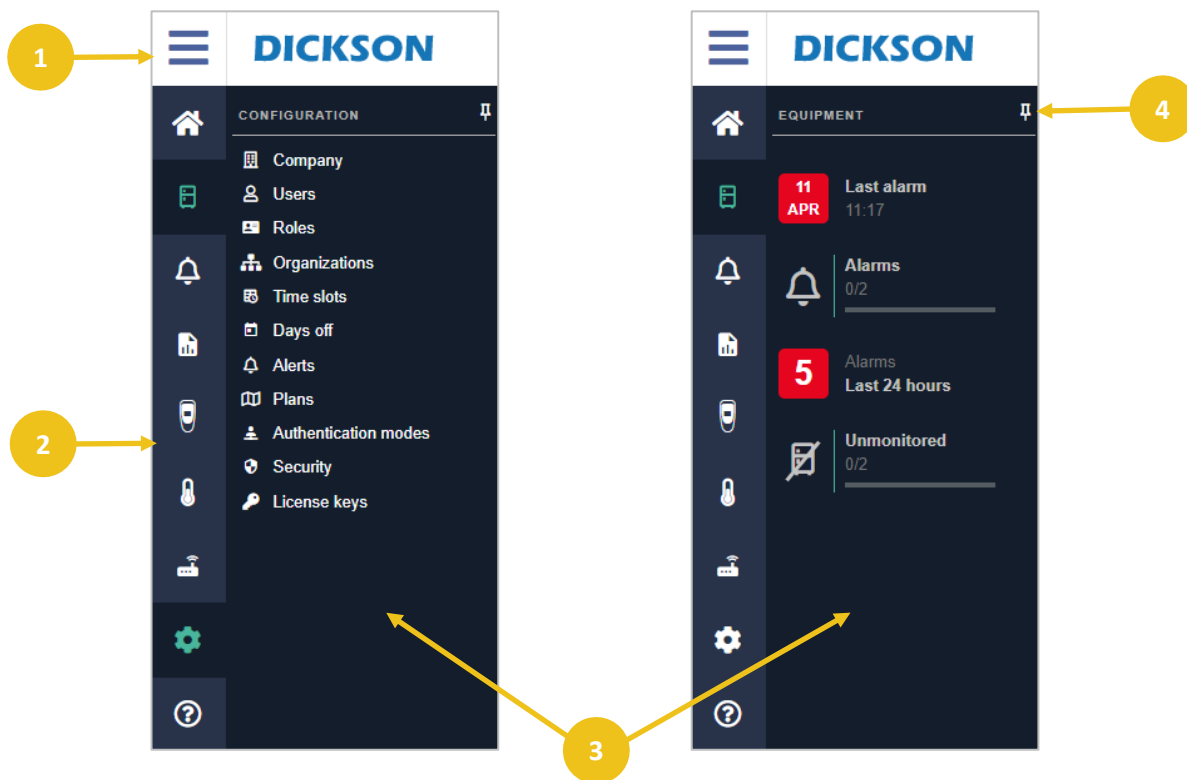











Figure 19 – General layout of OCEAView main menu

Main menu features:

Description	
1	Fold or unfold the menu
2	Navigation menu:  Home  Equipment  Alarms  Reports  Data loggers  Sensors  Infrastructure  Configuration  Help
3	Sub-menu with additional features or information, depending on the context (described in the next section).
4	Toggle the thumbtack to <b>Pin</b> or <b>Unpin</b> the menu (keep it open or allow it to slide back automatically).

The background color changes as you pass your mouse over each feature and after you select it.

### 3.1.2 Side-bar indicators

Your system constantly monitors the health of all its components so you can take action if necessary. As you unfold the main menu on the left-hand side of the screen, sidebars with key indicators are displayed for several items.

Some icon colors vary according to status, such as (Alarms) **To acknowledge**, which turn from green to red when alarms need your attention.

**Equipment:** This information pertains specifically to the status of your equipment.

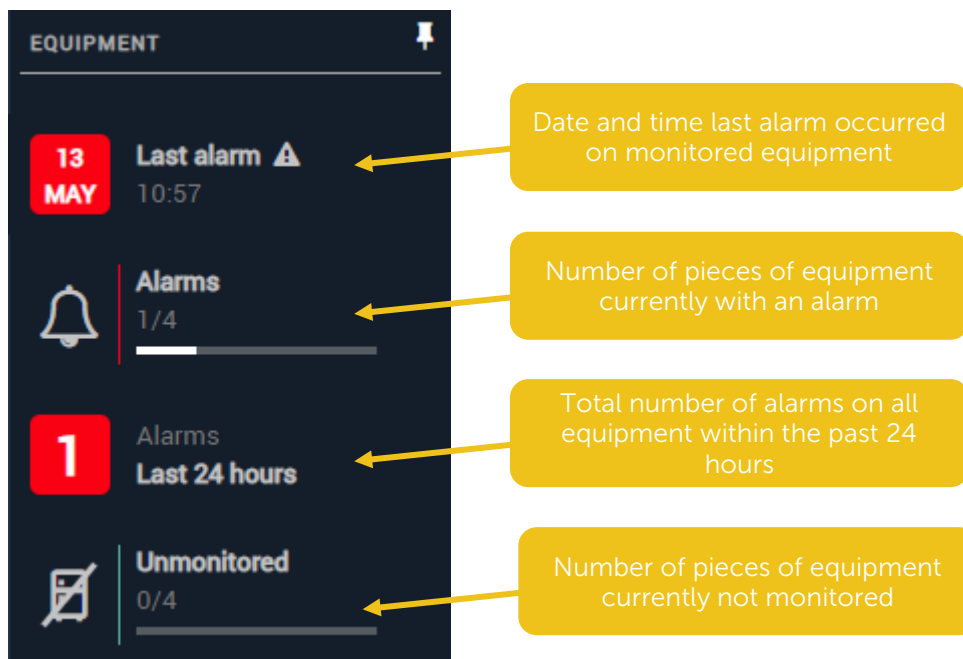


Figure 20 – Equipment side-bar indicators

**Alarms:** This information pertains specifically to alarms detected by the system.

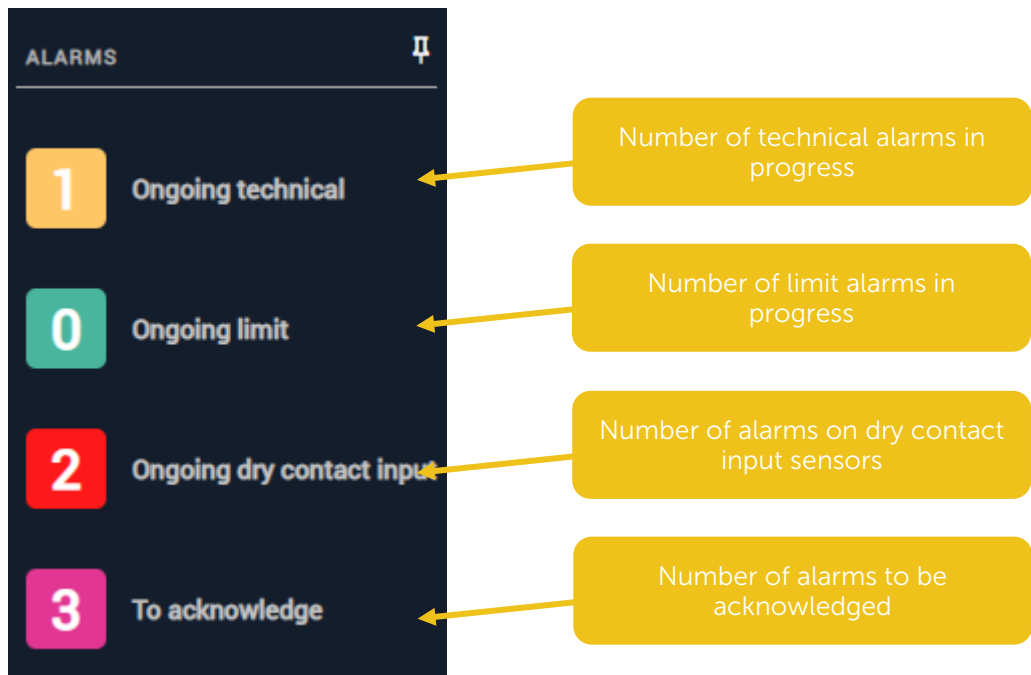


Figure 21 – Alarms side-bar indicators

**Data loggers:** This information pertains specifically to the status of your data loggers, not their sensors or equipment to which they are assigned.

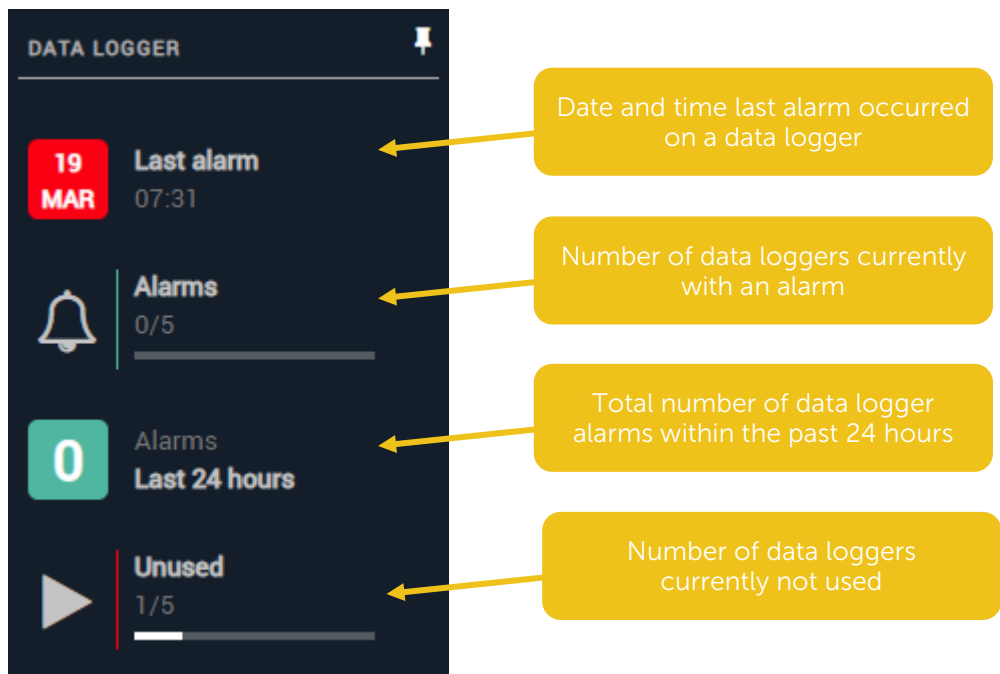


Figure 22 – Data logger side-bar indicators

**Sensors:** This information pertains specifically to the status of the sensors connected to your data loggers.



Figure 23 – Sensor side-bar indicators

**Infrastructure:** This information pertains specifically to the status of your infrastructure devices, such as gateways and dry contact or siren alert devices.

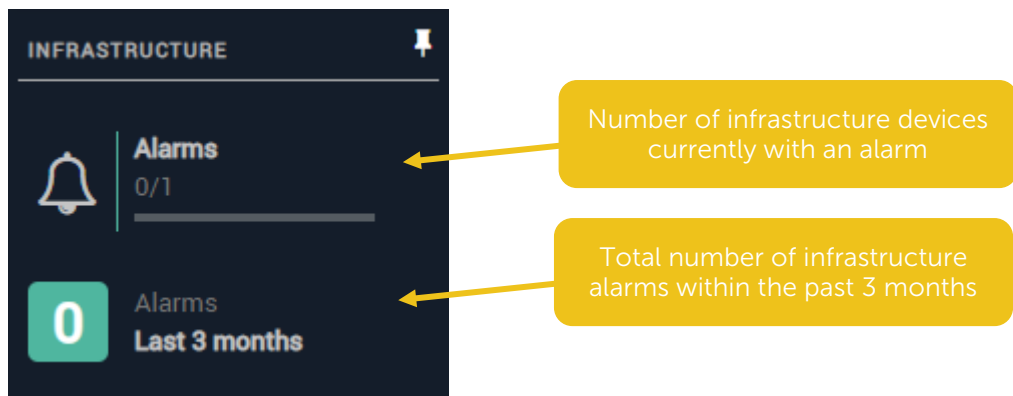


Figure 24 – Infrastructure side-bar indicators




If you pin these side-bars open and make certain changes in the main screen, you must refresh the page – press the F5 key or **Refresh** button (🔄) to update the various indicators.

### 3.1.3 Using filters

Many OCEAView screens include a **Filters** option at the top of the display. You may use various fields and search criteria to adapt lists displayed on screen or sort data in different ways. Filters can be particularly useful for finding specific information quickly or limiting long lists.

The **Filters** feature always works as described below, though perhaps with slightly different options depending on the context.

To use **Filters**:

1. Click on **Filters**  and use the pull-down menus to choose the information you want to display. These examples show the filters options on the **Equipment** and **Sensors** screens:

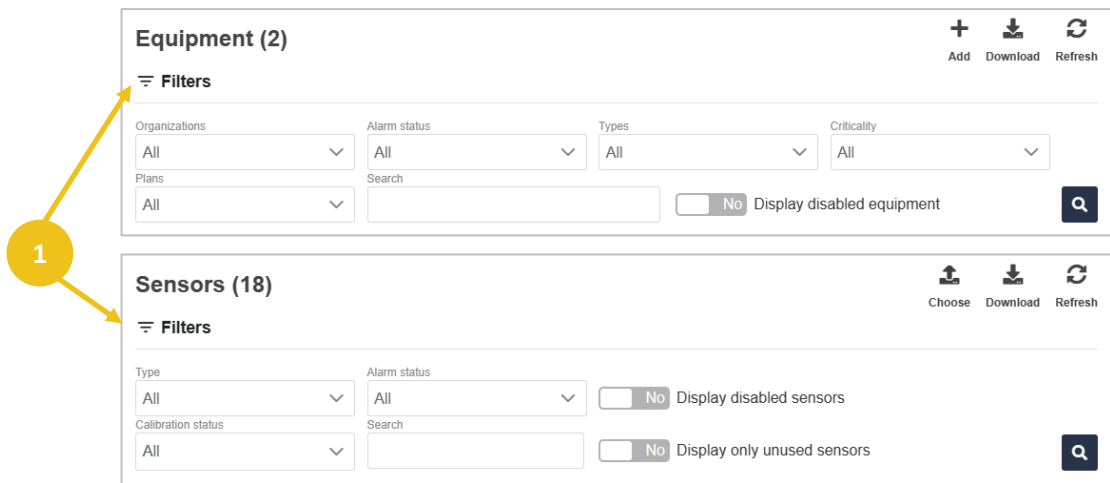





Figure 25 – Using filters in OCEAView to refine lists

2. You may filter by entering text into the **Search** field.
3. Apply the filters by clicking on the search icon (  ). The resulting list only displays items related to the criteria you specified.
4. To clear the active filter(s), simply click on **Refresh** (  ) or uncheck the selected options and click on the search icon (  ).

## 4 Home screen overview

The OCEAView home screen contains the equipment monitoring dashboard, giving you quick access to the information you need concerning your system. The home screen features several display modes:

<b>Plan View</b>	Displays an image of your facility's floor plan, on which you can place the equipment you are monitoring according to its physical location (described in section 6.4 – <i>Site plan images</i> , p. 107).
<b>Equipment watch mode</b>	Allows you to visually check the status of all your equipment as well as the most important information, such as the last recorded reading, sensor status, alarm status, and more. With this view, each tile shows one piece of equipment with up to two sensors.
<b>Sensor watch mode</b>	Nearly identical to <b>Equipment watch mode</b> , but only shows one sensor per piece of equipment.
<b>Multigraph view</b>	Enables you to display multiple sensor readings from different pieces of equipment on a single graph.

You may choose your default view using the “Favorites” bookmark (🔖), as shown below. To pin your preferred view to your home screen, simply click on the desired bookmark icon <sup>1</sup>:

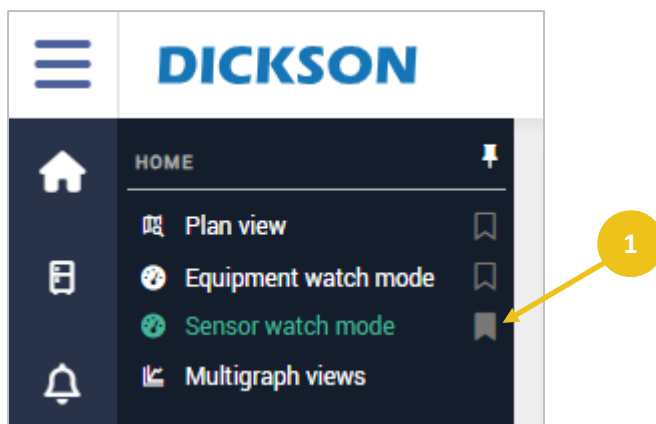


Figure 26 – Customizing OCEAView home screen

The selected view is reopened automatically the next time you login to OCEAView (note: this does not apply to the **Multigraph views** feature).

## 4.1 Plan view

OCEAView enables you to load a floor plan for a quick visual indication of where your equipment and data loggers are located.

Here is an example showing equipment at various locations on the floor plan 1:

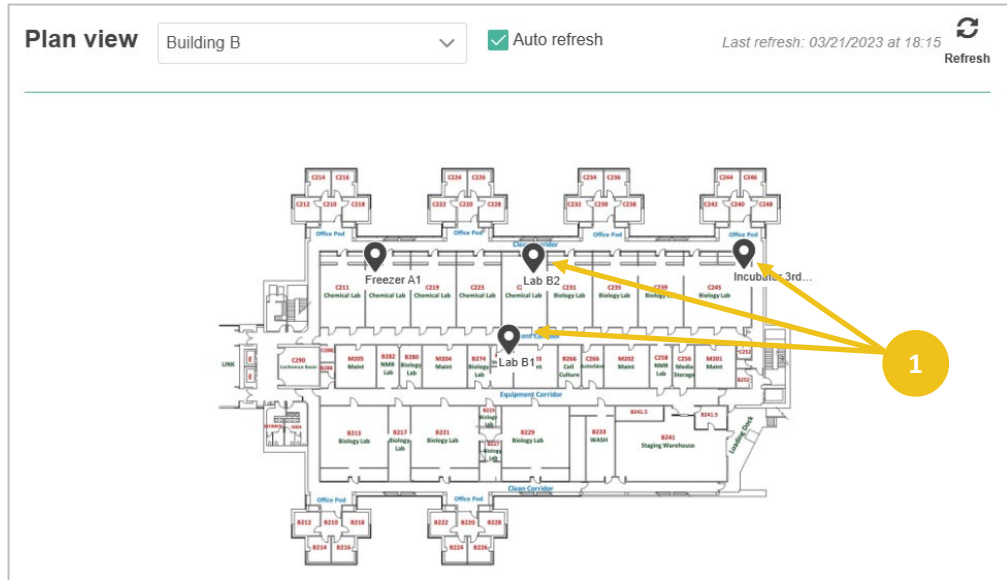


Figure 27 – Viewing your equipment on a floor plan of your site

For more details, please see section 6.4 – *Site plan images*, p. 107.

## 4.2 Equipment and sensor watch mode

The **Watch mode** screens show the status of all the equipment your profile allows you to view. The tiles on the dashboard provide an instant view of your equipment as well as the physical parameters recorded by your data loggers.

Enable **Auto refresh** <sup>1</sup> to update the data on your dashboard automatically every five minutes.

Sensor watch mode (one sensor per piece of equipment):

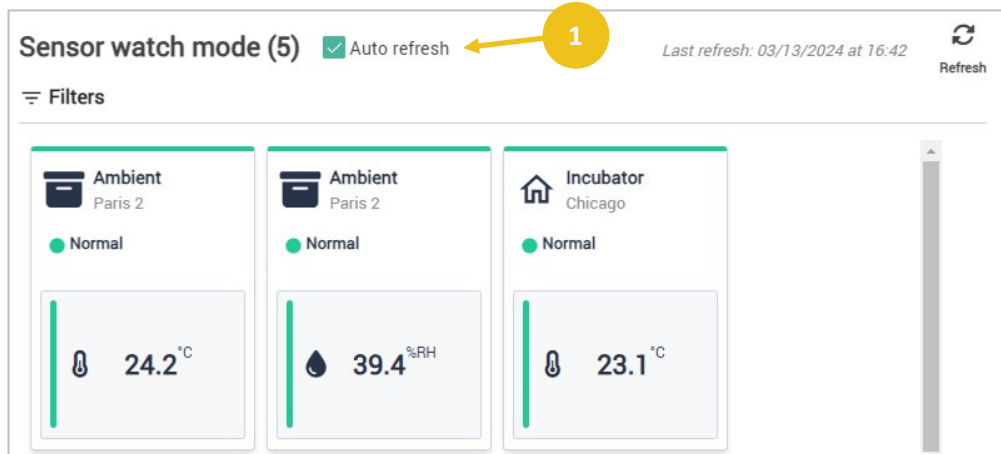


Figure 28 – Overview of the Sensor watch mode dashboard

Equipment watch mode (up to two sensors per piece of equipment):

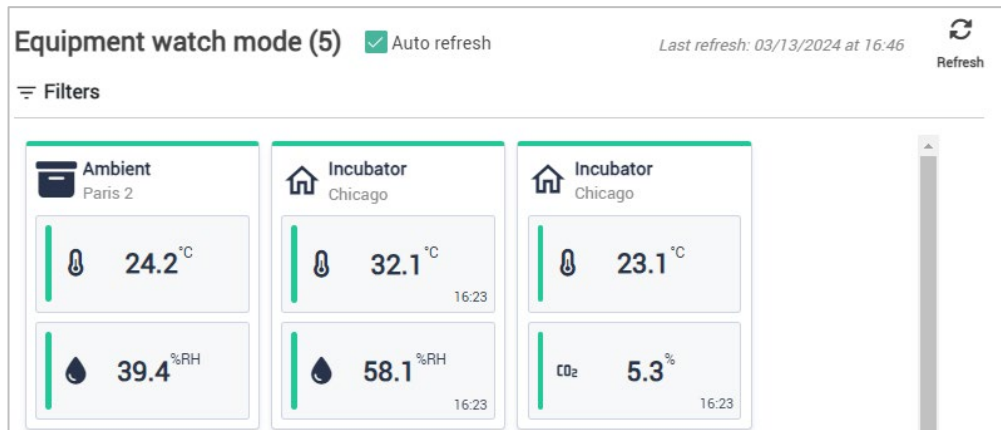


Figure 29 – Overview of the Equipment watch mode dashboard



Actions and updates concerning remote data loggers might not always be visible instantaneously in OCEAView. As data transfer is based on the configured transfer interval, you may observe a reading on a data logger screen that has not yet been transferred to the system.

### 4.2.1 Equipment tile presentation

Each tile shows key information about a piece of equipment and its sensors.

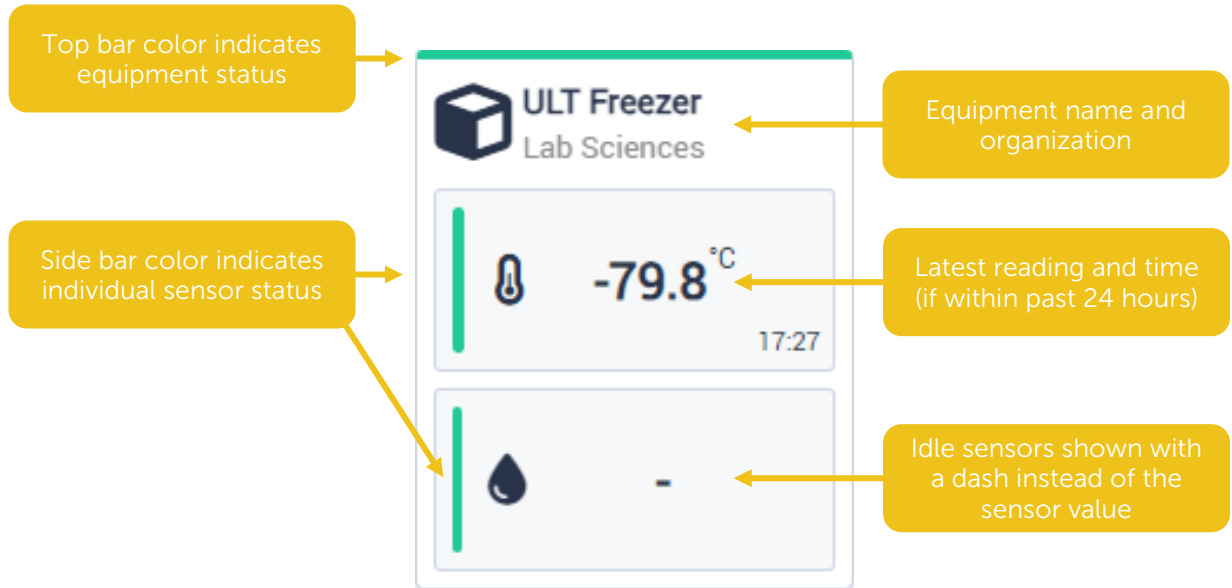
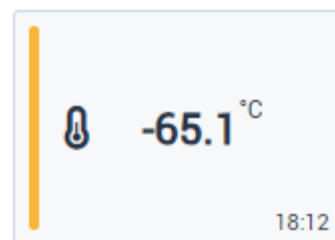
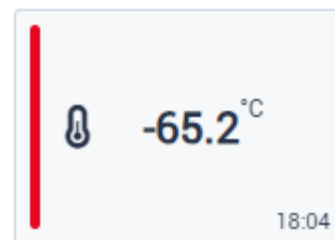
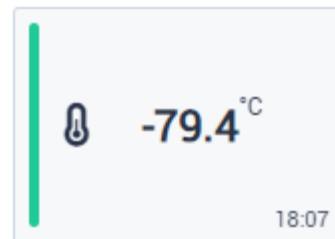


Figure 30 – Sensor watch mode tile with key details

### 4.2.2 Sensor status indication color codes

Sensor status is indicated by the vertical bar to the left of the tile. Three colors are used:

- **Green**
  - There are currently no errors or alarms.
  - If high and/or low limits are programmed, the reading is within the target range.
- **Red**
  - The sensor is currently in an alarm state.
  - The sensor reading has gone outside programmed high or low alarm limits, or there is a technical error such as a sensor problem or low battery.
- **Orange**
  - The sensor is currently in a warning state.
  - The sensor reading has gone outside programmed high or low warning limits.



### 4.2.3 Equipment status color codes

The horizontal bar across the top of the tile indicates the overall status of the piece of equipment. The colors are as follows:

- **Green**

- There are no errors.
- The sensors and datalogger(s) associated with the equipment are working correctly.



- **Red**

- One or more of the equipment's **sensors** has triggered an alarm.
  - or -
- One or more of the equipment's **data loggers** have triggered a technical alarm, such as low battery, sensor error, or communication problem.



- **Orange**

- One or more of the equipment's **sensors** has triggered a warning.



### 4.2.4 Examples

Here are some examples to illustrate the use of colors on the dashboard tiles. Note: this piece of equipment ("Incubator") has four associated sensors and therefore uses two tiles.

#### Example 1: Sensor with warning returns to normal

(1) Top bar indicates that a sensor has a warning. Side bar indicates which sensor.

(2) Top bar and side bar indicate that sensor reading has returned to normal.

#### Example 2: Sensor with alarm returns to normal

(1) Top bar indicates that an element associated with the equipment has an alarm. Side bar indicates a sensor alarm, and which sensor.

(2) Top bar and side bar indicate that sensor reading has returned to normal.

#### 4.2.5 Sensor details with and without warnings or alarms

You can click on a tile to see more details about a particular sensor.

##### Example 1: Sensor details without warnings or alarms

Here is an example with a sensor running within the programmed target range.



Figure 31 – Sensor details panel without alarm or warning

- 1 Equipment name and associated organizational node.
- 2 Sensor serial number. Click to access the sensor directly.
- 3 Latest sensor reading and alarm status.
- 4 High and low alarm limits (red dashed line) and warning limits (orange dashed line). Click in this zone to open the full readings window, with filters and the possibility to create and download reports. See *Chapter 13 – Viewing sensor data, p. 186* for more details.

### Example 2: Sensor details with warning

If the sensor exceeds a reading value that is programmed as warning limit, the color coding changes to orange, as shown below. Warnings do not have to be acknowledged with a PIN code and cause in OCEAView.

You may click on the orange button to open the Alarms & Warnings window and see details about the warning.

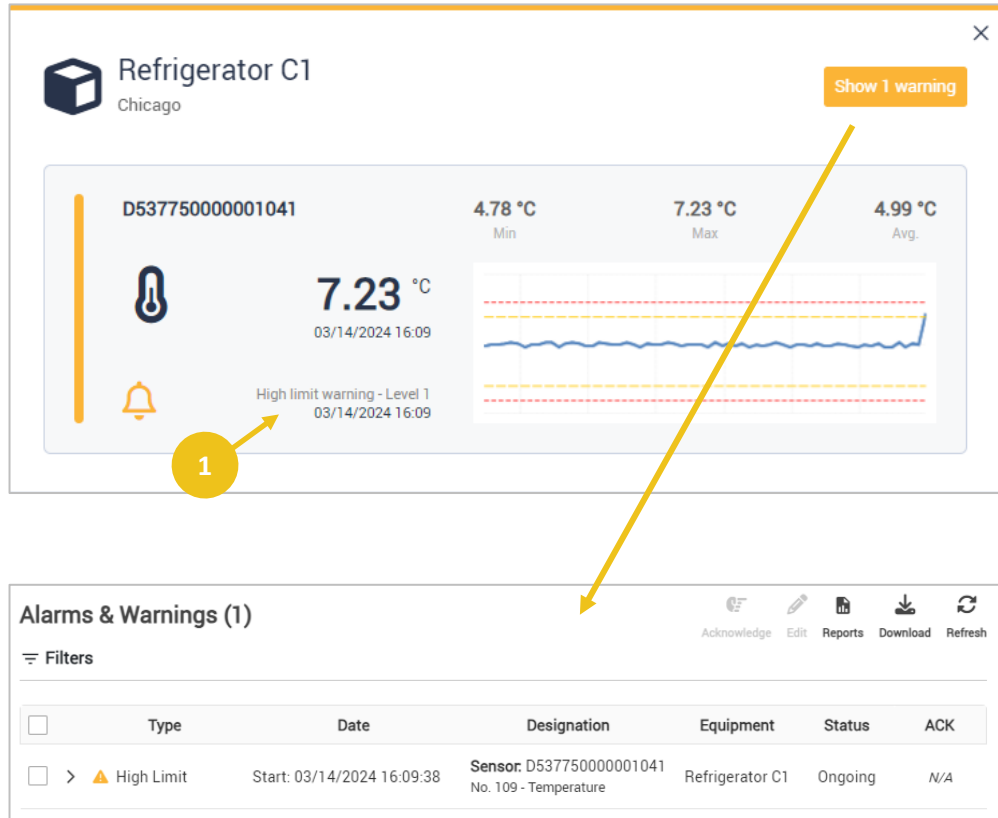


Figure 32 – Sensor details panel with a current warning

- 1 The type of warning and timestamp are indicated here.

### Example 3: Sensor details with alarm

The color-coding changes to red if the sensor reading exceeds a limit programmed as an alarm, or if there is a technical alarm such as a sensor problem or low battery.

You may click on the red button to open the Alarms & Warnings window and see details about the alarm. The button indicates the number of alarms or warnings associated with the sensor (in the example below, the button indicates 2 alarms/warning because it takes the previous warning into account).

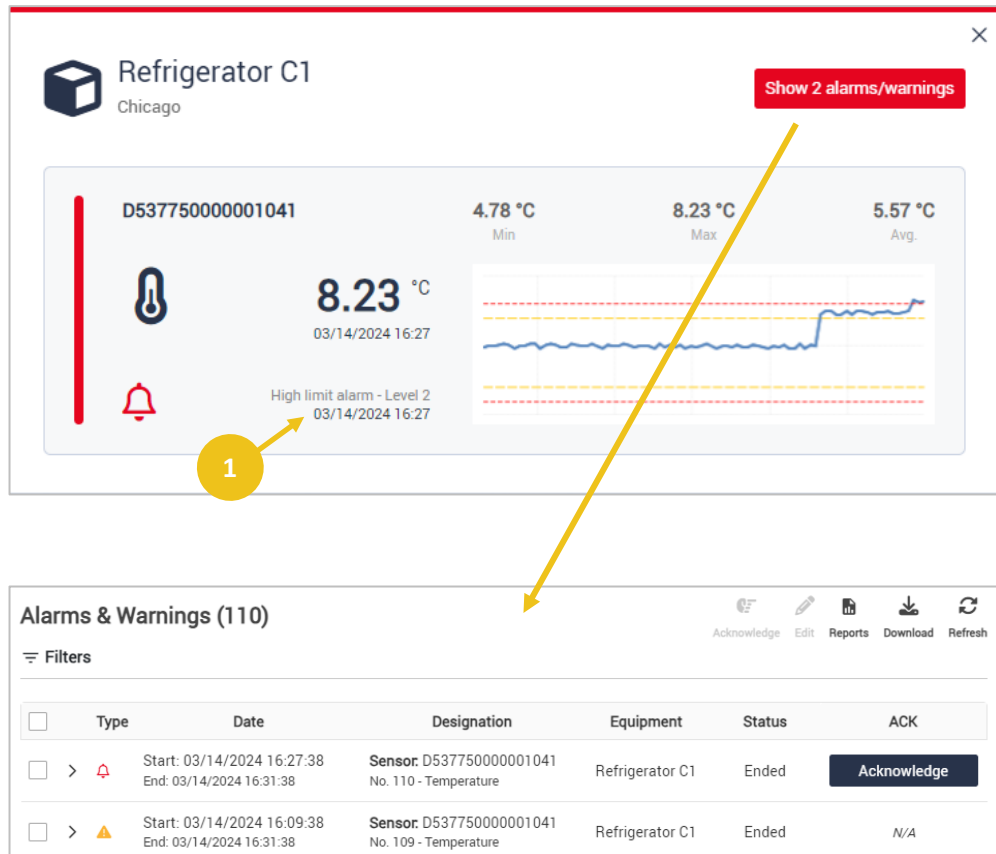


Figure 33 – Sensor details panel with an alarm

- 1 The type of alarm and timestamp are indicated here.

More details about the Alarms & Warnings list are provided in *Chapter 15 – Alarms & alerts, p. 227*.

#### Example 4: Sensor details with paused alarms

Cobalt X1 and Cobalt X2 data loggers have a feature to pause alarms from 30 minutes to 72 hours. This feature can only be activated using the interface on the data logger itself.



Figure 34 –Sensor details panel showing alarm pause is activated on the data logger

- 1 Paused alarms are indicated here.

#### 4.2.6 Alarms and warnings panels

When alarms or warnings occur, panels are displayed on the right-hand side of the screen <sup>1</sup>, with counters to indicate the number of alarms and warnings currently active in your monitoring system.

This information is updated dynamically to inform you right away if there are any critical incidents. The panels are cleared automatically as problems are resolved.

Click on the red or orange boxes to open the alarm management window (more details are provided about this in section 15.1.2 – *Viewing alarm details*, p. 230):

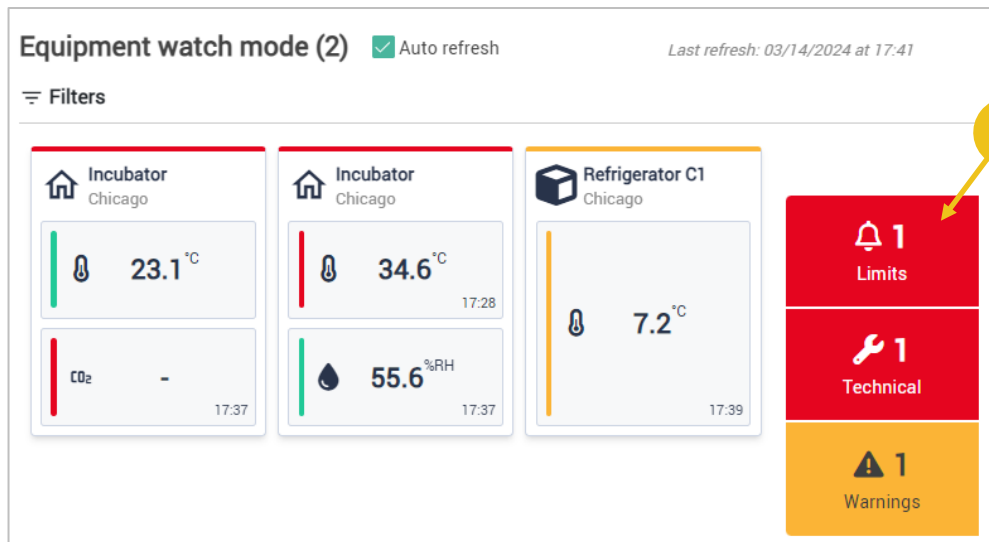


Figure 35 – Pop-up for alarm notification

#### 4.2.7 Sensor display for dry contact input sensors (Cobalt X1/X2 only)

In Watch Mode, dry contact input sensor tiles show an icon indicating the current configuration (which is defined in settings on the Cobalt X1/X2 data logger), with alarm colors depending on the open-close state. Each state shows the icon corresponding to the “normal” configuration.

If the dry contact input sensor is defined as “normally closed”:

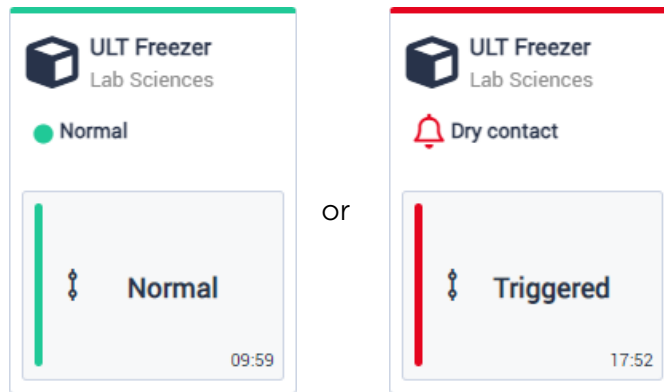


Figure 36 – “Normally closed”: dry contact loop is closed for normal operation, in an alarm state (“triggered”) if the loop is open

If the dry contact sensor is defined as “normally open”:

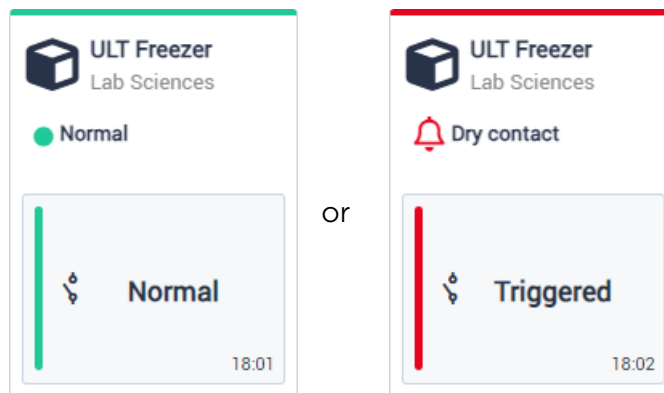


Figure 37 – “Normally open”: dry contact is open for normal operation, in an alarm state (“triggered”) if closed

Dry contact sensor configuration is covered in more detail in section 12.2.2 – Dry contact input sensors (Cobalt X1/X2 only), p. 178.

## 5 Users and authentication modes

OCEAView provides a complete user management interface. When you first create your company in OCEAView (as described in section 2.2 – *Creating your OCEAView company account, p. 21*) you also create the first user account. That user has an Application Manager profile and is thus allowed to control every aspect of the system, its organization, and other user accounts. Every company must have at least one user with an Application Manager profile.

### 5.1 Connection authentication modes

OCEAView supports several user authentication modes:

- OCEAView's own **integrated user authentication mechanism**, which identifies users by their username (which can be an e-mail address) and password.
- **LDAP** (Lightweight Directory Access Protocol), an external authentication protocol to identify users by their corporate, network, or system login name and password. Generally used by large organizations, this option centralizes user management, while offering a broader range of user permissions and password control within corporate IT tools.

*LDAP is supported by OCEAView On-premises solutions.*

- **SSO** (Single sign-on) is an authentication method that uses an external identity provider to enable users to access multiple enterprise applications with a single set of login credentials, thus eliminating the need for multiple passwords.

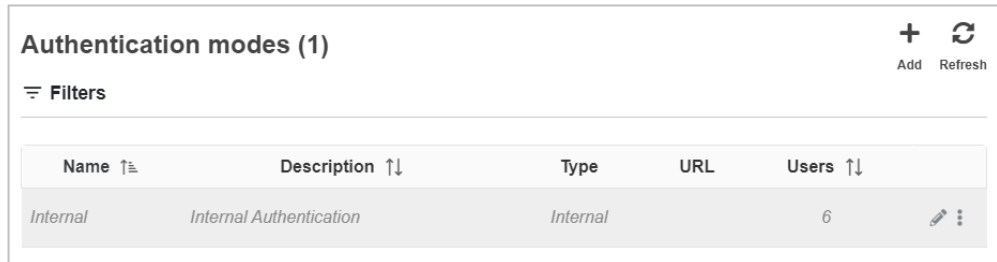
*SSO is supported by both OCEAView Cloud and OCEAView On-premises solutions.*

Technical bulletins for using SSO with OCEAView are available via these links

- Microsoft Entra ([click here for PDF](#))
- Okta ([click here for PDF](#))

### 5.1.1 Default integrated user authentication

By default, OCEAView system uses its own internal authentication mechanism. You can see the authentication mode(s) used by your system by clicking on Configuration (⚙️) → Authentication modes:



Name ↑	Description ↑↓	Type	URL	Users ↑↓
Internal	Internal Authentication	Internal		6

Figure 38 – Default OCEAView authentication platform



The internal authentication mode may not be disabled, deleted, or edited.

### 5.1.2 Adding an external identity provider

For your system to access an external SSO identity provider or LDAP active directory, you must add one or more authentication modes to OCEAView and configure it as described in this section.



#### Assistance from your IT department is highly recommended



The configuration process for adding an LDAP or SSO identity provider can be somewhat complicated, as technical information needs to be coordinated between your OCEAView system and the identify provider. This involves the OCEAView-specific information discussed here, but it also requires access to an external identity provider platform as well as in-depth knowledge of application and user management.

The specific details of third-party identity provider services and interfaces may vary and are therefore outside the scope of this document.

### 5.1.2.1 Adding LDAP authentication (OCEAView On-Premises only)



Before you add LDAP authentication in OCEAView, you must make sure that your active directory contains the necessary *groups* specific to OCEAView. All other information is standardized and does not require any particular attention. More information on this is provided in the OCEAView On-Premises Installation User Guide.

1. In the main menu, click on **Configuration** (  ) → **Authentication modes**
2. Click on **Add** (  ) and choose **LDAP**
3. Fill in the fields below for LDAP settings:

The screenshot shows a dialog box titled "Create authentication mode" with a close button (X) in the top left corner. It contains three input fields: "Name \*" (required), "Description", and "URL \*" (required). To the right of the "URL \*" field is a "Connect" button, which is currently disabled. At the bottom right of the dialog are "Cancel" and "Save" buttons.

Figure 39 – Adding an external LDAP identity provider

**Name** Assign a name for the authentication mode. This name is used as a reference within OCEAView only and must be unique. You will receive an error message if the name is already in use.

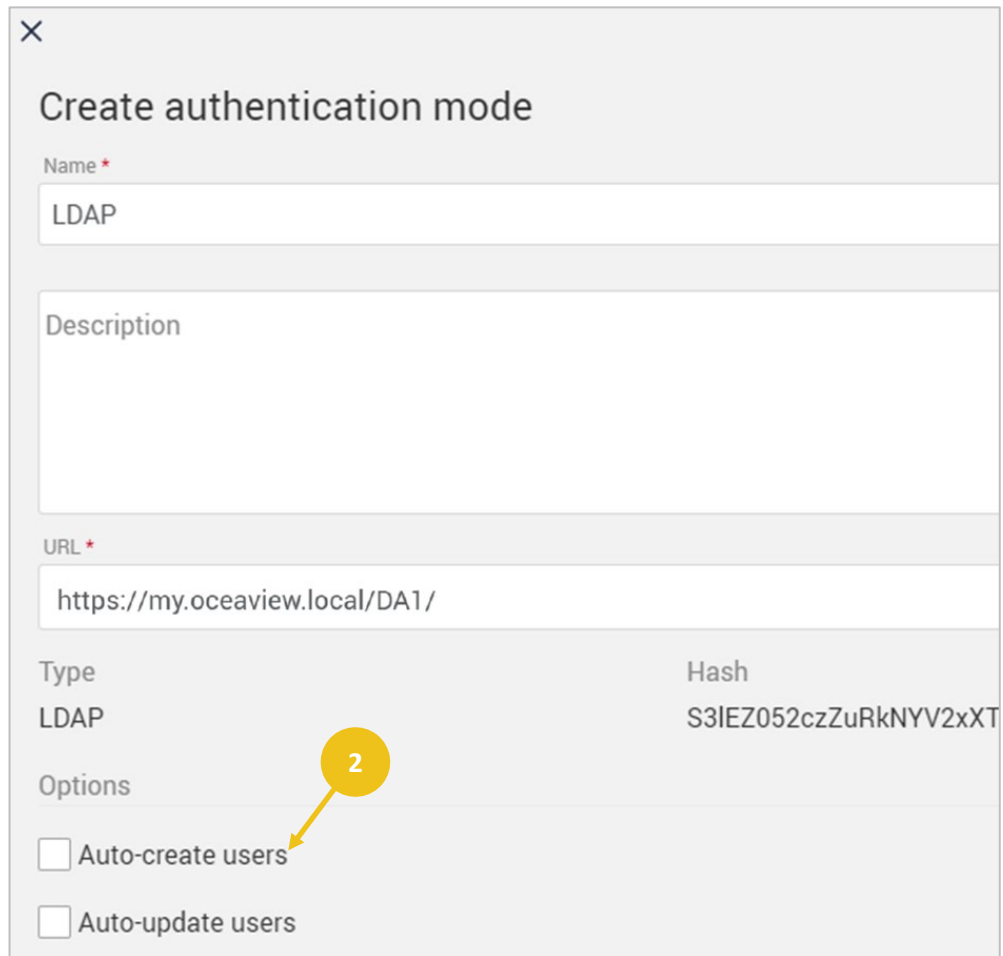
To log in, the user enters this name along with their username, in the format:

`authentication_mode_name/username`

**Description** You may enter general information in this optional field.

**URL** Enter the exact URL for connecting to your platform's LDAP authentication agent.

4. Click on **Connect** <sup>1</sup> to verify that the URL is correct and connection to the LDAP authentication agent can be established. If connection is successful, additional information is displayed <sup>2</sup>:



×

### Create authentication mode

Name \*

LDAP

Description

URL \*

https://my.oceaview.local/DA1/

Type	Hash
LDAP	S3IEZ052czZuRkNYV2xXT

Options

Auto-create users

Auto-update users

Figure 40 – Automatic options with LDAP

The following two options are available:

**Auto-create users** If this option is activated, OCEAView creates new users automatically when they login with their enterprise username and password. The authentication mode name is indicated in their user account settings (i.e., the name assigned in step 1 above).

**Auto-update users** With this option, information in user settings is automatically updated based on information in the external directory. Changes made in the external Active Directory are applied next time the user logs in.



The user's e-mail address must be:

1. Present in the LDAP directory, otherwise the user will not be imported into OCEAView.
  2. Unique in the system (the same e-mail address cannot be used more than once).
- 

### 5.1.2.2 Adding SSO authentication

---

Before you add SSO authentication in OCEAView, you must first set up the application, users, and "claims rules" on the identity provider side to define which attributes are sent to OCEAView from your identity provider platform and which fields they correspond to in OCEAView. Among other information, it is essential to include the username, first name, last name, and e-mail, otherwise you will not be able to log in to OCEAView.



In addition, you must create a group and a claim specifically for OCEAView "Application Manager" users. Otherwise, the OCEAView "User" user type is applied by default.

#### **TECHNICAL BULLETINS AVAILABLE**

We have created detailed technical bulletins on implementing SSO for:

- Microsoft Entra (Azure) ([click here for PDF](#))
- Okta ([click here for PDF](#))

For more information, feel free to contact your Dickson OCEAView representative for a technical bulletin on this topic.

---

To set up SSO authentication in OCEAView:

1. In the main menu, click on **Configuration** (⚙️) → **Authentication modes**
2. Click on **Add** (+) and choose **SSO**
3. Fill in the fields below for SSO settings:

×

### Create authentication mode

Name \*

Type

-

Identity Provider metadata URL

Metadata URL \*

 Connect

Entity ID

-

Login URL

-

Logout URL

-

Token validation certificate

-

Request Signing certificate

-

Renew certificate Remove certificate

Cancel Save

Figure 41 – Adding an SSO identity provider

**Name** Assign a name for the authentication mode. This name is used as a reference within OCEAView only and must be unique. You will receive an error message if the name is already in use. The first time users log in, they must enter their username as well as this authentication mode name.

**Identity provider metadata URL** You will find this URL in the identity provider’s configuration console for the application. Copy the full path from the console into this field in OCEAView.

4. Click on **Connect** (1) to verify that the URL is correct and connection can be established and to obtain the other technical information required to complete configuration on the identity provider side.

After connecting, the screen is updated with information for the following:

- Entity ID
- Login URL
- Logout URL
- Token Validation Certificate
- Request signing certificate

You must then copy/paste that information, as shown on the screen below, to your identity provider.

The screenshot shows a dialog box titled "Create authentication mode" with a close button (X) in the top left. The form contains the following fields and values:

- Name \***: YourSSO
- Type**: SSO
- Identity Provider metadata URL**: Metadata URL \*  
https://login.microsoftonline.com/ed46sdf654dfgf4556-4fabd693-ef5e-48c4-bf1d-7
- Entity ID**: https://sts.windows.net/ed46545682d45655dace23cd693-ef5e-31c4-bf45-765465554130c05a8ba/
- Login URL**: https://login.microsoftonline.com/ed46655545473cd693-ef5e-48c4-bf1d-74130c05a8ba/saml2
- Logout URL**: https://login.microsoftonline.com/e23cd693-ef5e-48c4-bf1d-74130c05a8ba/saml2
- Token validation certificate**: CN=Microsoft Azure Federated SSO Certificate  
E3DD452B5844BC56D7A01A666F26972A955 (sha256RSA)  
05/06/2024 10:55 → 05/06/2027 10:55
- Request Signing certificate**: CN=noclaims  
F60DC645A4554B54555E6FA20F1AD1655AE3 (sha256RSA)  
05/06/2024 14:22 → 05/06/2025 14:22

At the bottom of the dialog, there are two buttons: "Renew certificate" and "Remove certificate".

Figure 42 – Details to copy to your SSO identity provider settings



With SSO, OCEAView manages user session connection certificates. These certificates are valid for one year, as indicated by the date ( 2 ) in the above screen and are renewed automatically. If you want to end the current sessions for users logged in with this SSO mode, press the **Remove certificate** and **Renew certificate** ( 3 ).

- On this same screen, you can activate or deactivate the following options, depending on your needs:

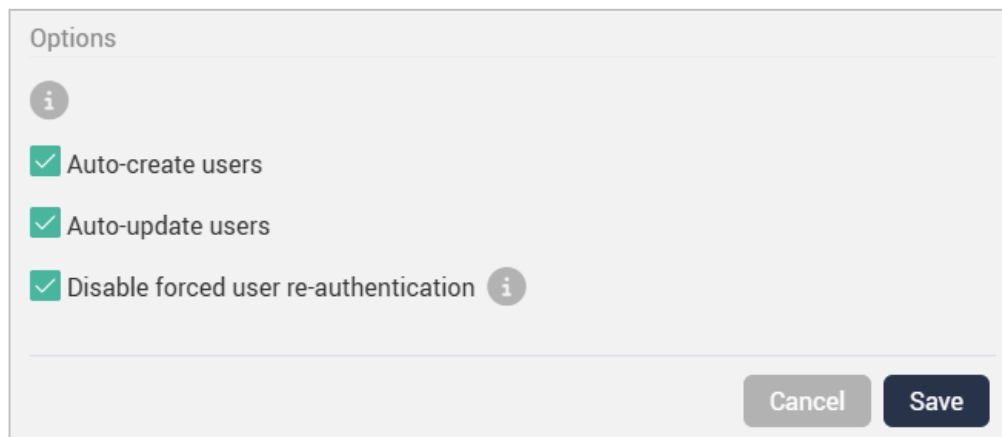



Figure 43 – Enabling auto-create and/or auto-update functionality

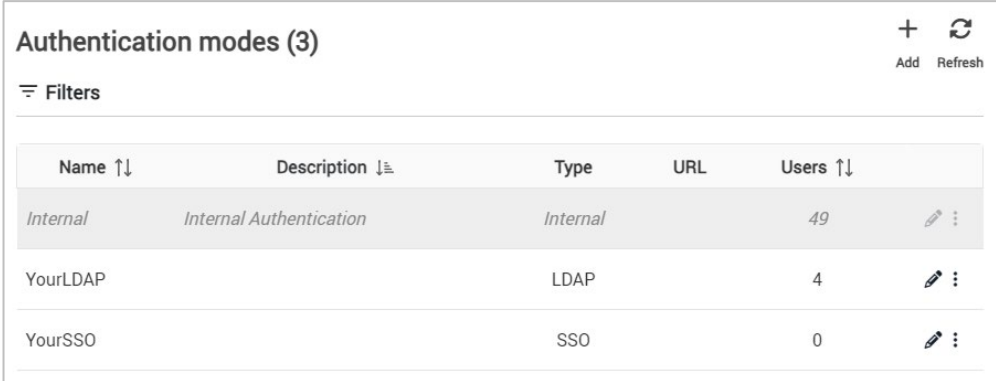
- Auto-create users** If this option is activated, OCEAView creates new users automatically when they login via SSO. Your users must be created on the identity provider platform and assigned to the application.
- Auto-update users** With this option, information in user settings is automatically updated based on information sent by the identity provider. Changes made on the identity provider side are applied the next time the user logs in.
- Disable forced user re-authentication** With this option, SSO users do not have to re-authenticate when confirming sensitive actions in OCEAView. Instead, the application uses existing session cookies for a smoother user experience.

- Press **Save** when done or **Cancel** to close this window without saving changes.

### 5.1.3 Editing an external authentication platform

You can edit an LDAP or SSO authentication mode that you have added to the system, but not OCEAView's internal authentication:

1. Click on **Configuration** (  ) → **Authentication modes**

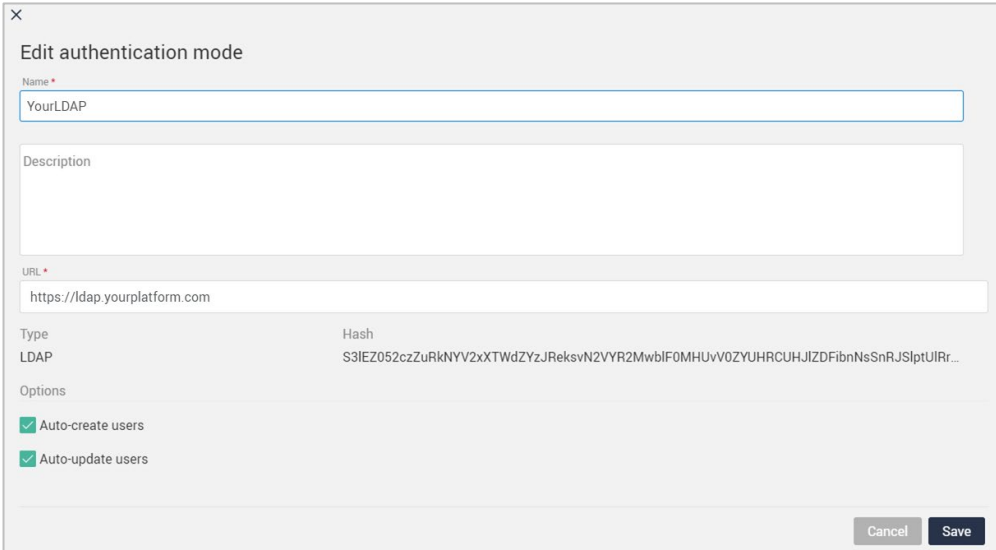


Name ↑↓	Description ↓≡	Type	URL	Users ↑↓
Internal	Internal Authentication	Internal		49
YourLDAP		LDAP		4
YourSSO		SSO		0

Figure 44 – Sample list of authentication platforms

2. To change information, click on **Edit** (  ) on the line containing the authentication mode you want to change.

#### LDAP



**Edit authentication mode**

Name \*  
YourLDAP

Description

URL \*  
https://ldap.yourplatform.com

Type  
LDAP

Hash  
S3IEZ052czuRkNYV2xXTWdZYzJReksvN2VYR2MwblF0MHUvV0ZYHRCUHJIZDFibnNsSnRJSltUIRr...

Options

Auto-create users

Auto-update users

Cancel Save

Figure 45 – Editing an LDAP authentication mode

If you change the URL for LDAP authentication, the system checks to make sure that the new URL corresponds to the same agent as before. If not, an error message informs you that the changes will not be taken into account.

## SSO

**Edit authentication mode**

Name \*  
YourSSO

Type  
SSO

Identity Provider metadata URL  
Metadata URL \*  
https://login.microsoftonline.com/e454cd78693-458215948c4-bf1d0c05a8ba/fe... **Connect**

Entity ID  
https://sts.windows.net/ef5e-48c4-bf1d-74130c05a8ba/

Login URL  
https://login.microsoftonline.com/ef5e-48c4-bf1d-74130c05a8ba/saml2

Logout URL  
https://login.microsoftonline.com/ef5e-48c4-bf1d-74130c05a8ba/saml2

Token validation certificate  
CN=Microsoft Azure Federated SSO Certificate  
E3DD42A3A73D3FA7AC5E01A6AC6366F26972A955 (sha256RSA)  
05/06/2024 10:55 → 05/06/2027 10:55

Request Signing certificate  
CN=noclaims

**Cancel** **Save**

Figure 46 – Editing an SSO authentication mode

If you change the **Metadata URL** field, use the **Connect** button to make sure that the connection works correctly. Also, update the information on the identity provider side if necessary. Scroll down if you want to change the **Auto-create users** and **Auto-update users** options.

3. Click on **Save** to save any changes you made, or on **Cancel** to discard changes.

### 5.1.4 Options for external authentication platforms

Several options are available when you have configured one or more external authentication platforms.



You cannot edit or delete the system's internal authentication mechanism.

To access options for external authentication platforms:

1. Click on **Configuration** (⚙️) → **Authentication modes**

Name ↑↓	Description ↓≡	Type	URL	Users ↑↓	
Internal	Internal Authentication	Internal		49	⋮
YourLDAP		LDAP		4	⋮
YourSSO		SSO		0	⋮

Figure 47 – Access authentication platform options

2. Click on **Options** (⋮) 1 to access additional features, depending on the authentication type.

**For LDAP:**

**Synchronize** This option connects to your LDAP agent and fetches all the users configured as Users or Application Managers for OCEAView and creates them automatically. Notably, this allows you to include users in Alert Rule definitions even if they have not yet connected to OCEAView (which would create those users upon their first login if you enable the Auto-create option described previously). A message is displayed to confirm the operation, informing you if required information is missing from a person's LDAP settings, or if the connection could not be established.

**Note:** if **Auto-create users** and **Auto-update users** are not selected, the Synchronize button only updates the status of existing users (Enabled, Disabled, Expired).

- Disable** Prevents associated users from connecting to the system.
- Delete** Deletes the authentication mode. You may only delete an existing authentication mode if there are no associated users.

For SSO:

- SSO settings** Opens a read-only pop-up with SSO information. You can use this screen to copy information for your identity provider configuration.

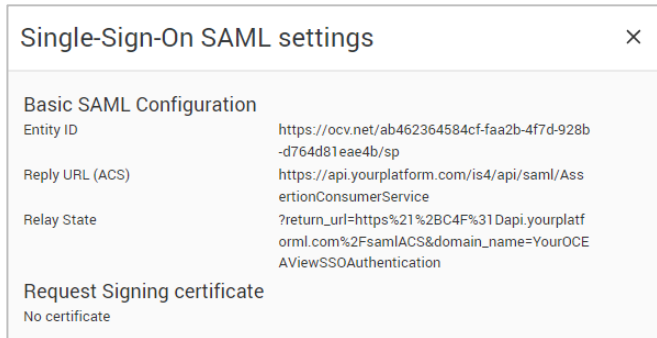


Figure 48 – SSO details, for reference only

- Disable** Prevents associated users from connecting to the system.
- Delete** Deletes the authentication mode. You may only delete an existing authentication mode if there are no associated users.

## 5.2 User accounts

### 5.2.1 Creating a new account

To add a new user account, login to OCEAView with your **Application Manager** account, or as a user whose application permissions include **Manage other users**, and follow these steps:




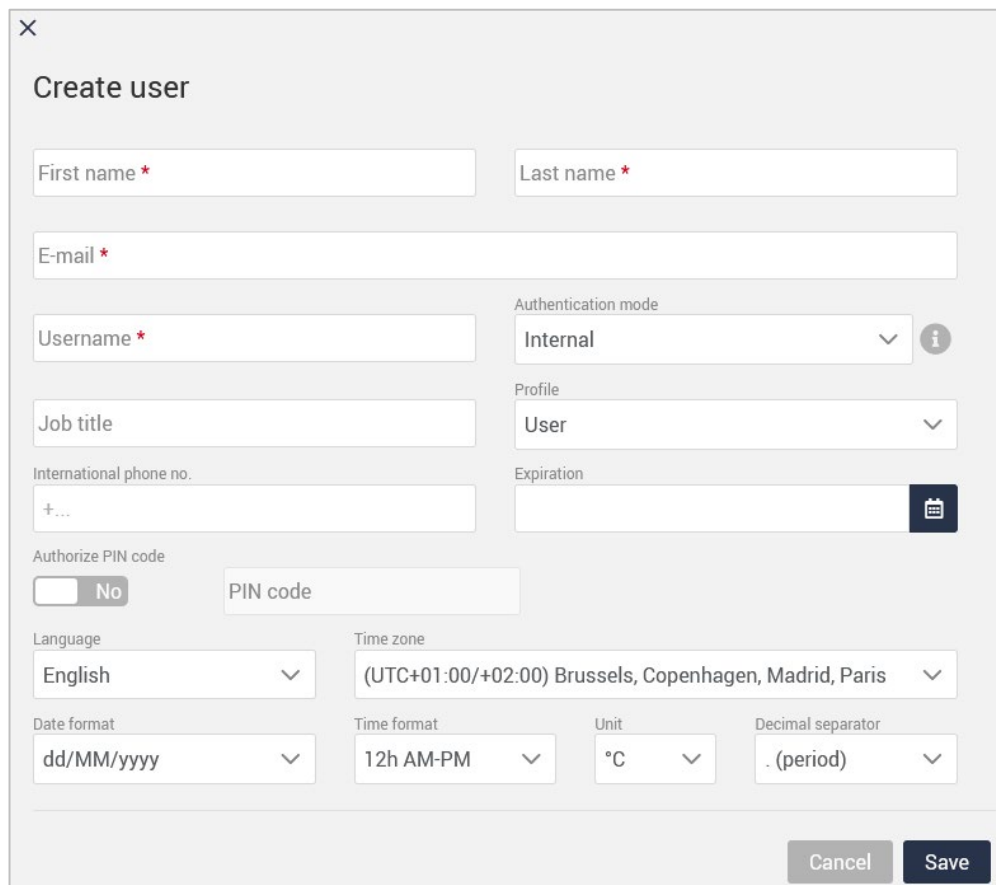
1. In the main menu, click on **Configuration** (  ) → **Users**. You may either click on **Add** (  ) or click on an existing username in the list and then **Create from...** (  ) to use that account as a template for creating a new one.



Figure 49 – Adding a new user

2. The **Create user** window opens as shown below, with fields either empty or already containing information, depending on your choice in step 1:


 A screenshot of the 'Create user' window. The window has a close button (X) in the top left. The title is 'Create user'. The form contains the following fields:
 

- First name \* (text input)
- Last name \* (text input)
- E-mail \* (text input)
- Username \* (text input)
- Authentication mode (dropdown menu, currently set to 'Internal')
- Profile (dropdown menu, currently set to 'User')
- International phone no. (text input, starting with '+...')
- Expiration (text input with a calendar icon)
- Authorize PIN code (checkbox, currently unchecked, with a 'No' button and a 'PIN code' text input)
- Language (dropdown menu, currently set to 'English')
- Time zone (dropdown menu, currently set to '(UTC+01:00/+02:00) Brussels, Copenhagen, Madrid, Paris')
- Date format (dropdown menu, currently set to 'dd/MM/yyyy')
- Time format (dropdown menu, currently set to '12h AM-PM')
- Unit (dropdown menu, currently set to '°C')
- Decimal separator (dropdown menu, currently set to '. (period)')

 At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 50 – User account details

3. Enter information to identify the user. The fields marked with a red asterisk (\*) are required:

**First name / Last name\*** The user's first and last names.

**E-mail\*** The user's e-mail address, which is used to login to the system and receive e-mail alerts and confirmations sent by the system.

**Username\*** If you are using OCEAView's internal authentication, the username can either be the same as the e-mail address or it may be a name that you enter here.



You must use the information provided in the **Username** field to log in.

---


If you are using SSO or LDAP authentication, the username is your regular corporate system username.

**Authentication mode** This field enables you to choose whether to use OCEAView's internal authentication (based on username and password), or an external authentication platform using your regular corporate system credentials. The option specified when creating the company account is displayed here by default.

When you select LDAP or SSO, a "Connect" button is displayed so that you can test access directly from this screen.

**Job title** The person's job within the company.

**International phone** Enter the telephone number in international format, with the prefix "+[country code]", such as: +14153817894. Do not include any extra digits or leading zeros.

**Expiration date** When using OCEAView's internal authentication mode, you may set a date at which this user account will expire. For external authentication platforms, you may not change the expiration date here. Expired accounts are indicated by this icon in the user list: 

## Profile

User control in the OCEAView system is based on two foundation profiles:

- **Application manager**

Users with this profile can control all aspects of the entire system for your entire organization, including changing other users' profile settings (but not their own).

- **User**

This profile is generally assigned to all other accounts. Most accounts in your system will be **User** accounts. Additional control abilities are then assigned by an **Application manager** or other authorized user on an as-needed basis by activating system-wide *application permissions* and/or creating organization specific roles in sites and departments.



You may not change the profile directly via OCEAView when using external authentication platforms.

---

## Authorize PIN code

This option lets you determine whether the account is allowed to perform actions that require the use of a PIN code, namely:

- Acknowledging alarms via the Cobalt X1/X2 data logger screen
- Acknowledging telephone alerts
- Accessing advanced settings menus on the Cobalt XS/X1/X2 data logger screen.



means the user can have a PIN code.



means the user will not have a PIN code.


## PIN code

If the user is authorized to have a PIN code, enter 4 digits into this field. The system will complete the PIN code with 2 additional digits after you close the window.



Only the account holder can see their own full 6-digit code in their account (**PIN code** → **Show**). Nobody else, including Application Managers, can see someone else's full PIN code.

---

<b>Language</b>	You may change the application language at any time. Select your default language from the <b>Language</b> pull-down menu.
<b>Time zone</b>	Select the time zone based on the user's geographical area when first logged in. <hr/>  If this user is included in an alert rule, their time zone is taken into account to determine the local time slot, and thus whether or not they will be notified. <hr/>
<b>Date format</b>	Select how dates are displayed in the application.
<b>Hour format</b>	Select how time is displayed in the application. Readings can be displayed in 12-hour (AM/PM) or 24-hour format.
<b>Unit</b>	Temperature unit can be displayed in degrees Celsius (°C) or Fahrenheit (°F).
<b>Decimal separator</b>	Select the character (period or comma) to use as a decimal separator in numerical values in the OCEAView display.

4. Click on **Save** to create the user account or **Cancel** to return to the previous screen.
5. The new user will receive an e-mail with a link to create their new password. Upon their first login, they must accept the Terms of Use and Privacy Policy Terms to continue.

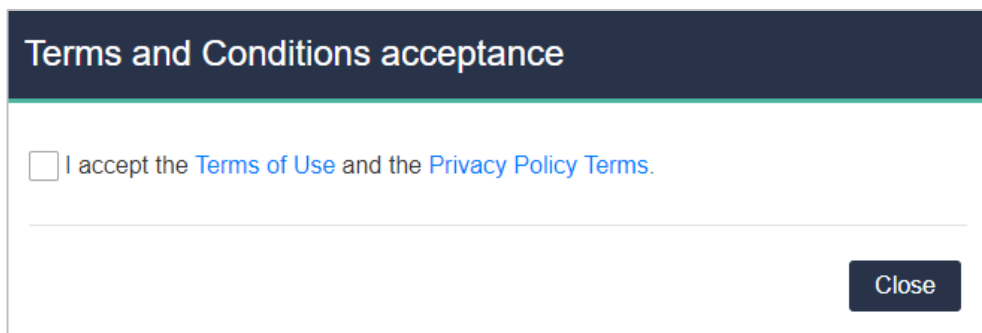
















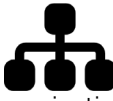











Figure 51 – New users must accept Terms and Conditions upon first login

### 5.2.2 Menu access based on profiles, permissions, and roles

The table below summarizes system access according to account profiles, as well as functionality that can be granted using roles and individual permissions.

Main menu	Sub-menu	Profiles			
		Application manager	User		
			Default	Can be added by permissions	Can be added by roles
 Home	 Plan view	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
	 Watch mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
 Equipment		<input checked="" type="checkbox"/>	-	-	<input checked="" type="checkbox"/>
 Alarms		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
 Reports	 Audit trail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
	 Report subscriptions	<input checked="" type="checkbox"/>	-	-	-
	 Review & approval	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
 Data loggers		<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
 Sensors		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
 Infrastructure		<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
		<input checked="" type="checkbox"/>	-	-	-

Main menu	Sub-menu	Profiles			
		Application manager	User		
			Default	Can be added by permissions	Can be added by roles
 Configuration	Company				
	 Users	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
	 Roles	<input checked="" type="checkbox"/>	-	-	-
	 Organizations	<input checked="" type="checkbox"/>	-	-	<input checked="" type="checkbox"/>
	 Time slots	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
	 Days off	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
	 Alerts	<input checked="" type="checkbox"/>	-		<input checked="" type="checkbox"/>
	 Plans	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	-
	 Authentication modes	<input checked="" type="checkbox"/>	-	-	-
	 License keys	<input checked="" type="checkbox"/>	-	-	-
	 Security	<input checked="" type="checkbox"/>	-	-	-
	 Online help	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-




Main menu	Sub-menu	Profiles			
		Application manager	User		
			Default	Can be added by permissions	Can be added by roles
Help	 About	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
	 Release notes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-
	 Legal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-


Figure 52 – Access differences between Application Managers and Users


Users may have view-only access to certain menu options, without being able to perform actions related to them.

### 5.2.3 User details overview

To view and/or edit your general account information:

1. Click on your user account image in the upper right-hand corner of the screen, then click on **My account**. The screen contains two main sections:

**Information** This section indicates the status of your account (Active / Inactive), its creation date and expiry date (if entered), your user level, the language selected and the PIN code to be typed on a Cobalt X1/X2 data logger screen to acknowledge alarms. You may edit this information by clicking on **Edit** (  ).

**Localization settings** Display format for time zone, time format, date format, measurement unit, and decimal separator. You may edit this information by clicking on **More** (  ) → **Edit localization settings**.

2. In either case, you may click on **Save** to record your changes, or on **Cancel** to return to the previous screen without saving changes.

## 5.3 Editing an account

To change any of the details for a user account in your OCEAView system:

1. Click on **Configuration** (⚙️) → **Users**
2. Click on a line in the table to open the account:

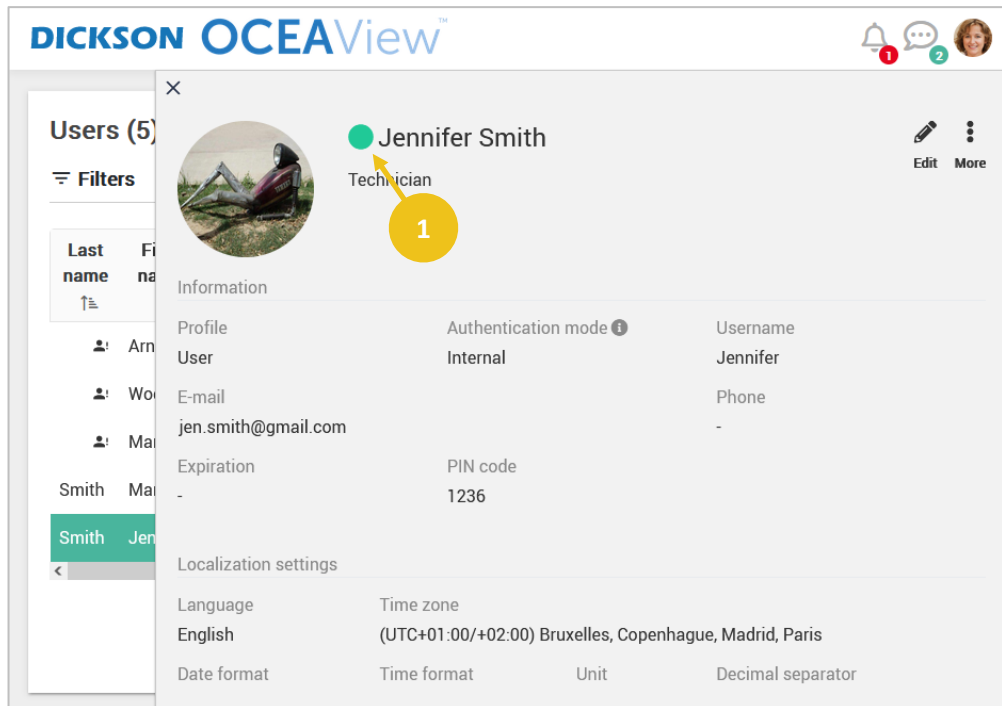


Figure 53 – Details for selected user account

3. The account status is indicated next to the person's name <sup>1</sup>:  
 Green (●) if the status is OK; red if the account is expired or locked (●) or gray (●) if the account is deactivated.

**Locked account** If the account using internal authentication is locked because **User lockout** is activated in **Security** → **Password** settings (described in section 6.2 – *System security settings*, p. 95) and the user entered an incorrect password the specified number of times (three, by default), a padlock is also displayed next to the user's name in the user list:

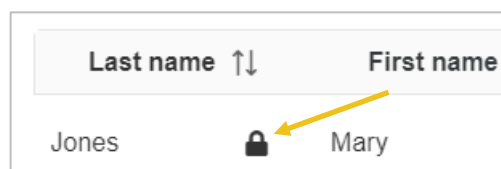


Figure 54 – Account locked after consecutive failed password attempts

You must reset the password to reactivate a locked account. When using SSO, the authentication provider handles password rules.

**Expired account**

If an account has an expiration date that has been reached, an icon is displayed next to the user's name and they will no longer be able to login.

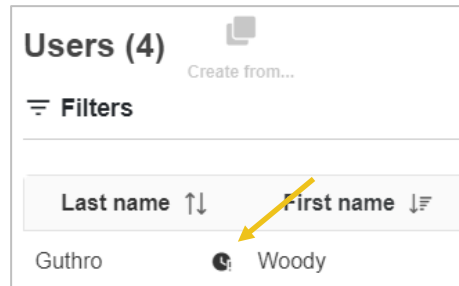




Figure 55 – Expired user account indicated next to name


To set a new expiration date for this user, you must login with an Application Manager account, or as a user with application permissions to manage other users, then **Edit** (  ) the account.

4. To change account information, click on **Edit** (  ) in the top right-hand corner of the window and edit the fields as needed.
5. Click on **Save** to save your changes or **Cancel** to exit this screen without saving changes.

---

Notes regarding changes made to an existing account:



1. The account's e-mail address cannot be changed, as it serves as a unique identifier for this user in the system.
  2. Some information presented here may not be modified if an external authenticational mode (LDAP) is being used by the system, and the option "Auto-update users" is activated. If you change the **Authentication mode**, test to make sure the user's account is valid by clicking on the test button: 
  3. Changes take effect the next time the user logs in to the system.
  4. An account cannot be deleted, it can only be disabled (and then hidden). For traceability reasons, it is not possible to delete a user account from the system.
-

### 5.3.1 Assigning application permissions to “User” profile accounts



Each person with a “User” profile can have their own set of “Application permissions” to perform a variety of different application-wide actions that apply to the entire system. An Application Manager typically assigns these permissions to a limited group of people within an organization, as they enable significant changes to be made regarding global operation. Application permissions are therefore assigned at the individual account level and generally only on an as-needed basis.



People who do not require these global application-wide permissions can be granted rights to perform many other “day-to-day” actions within their site or department within the organization (described in section 5.6 – *Adding user roles*, p. 85).

---

To assign application permissions to an account with a User profile:

1. Login with an **Application Manager** profile.
2. Click on **Configuration** (  ) → **Users**
3. Click on a line in the list to open that user’s account → **More** (  ) → **Edit application permissions**

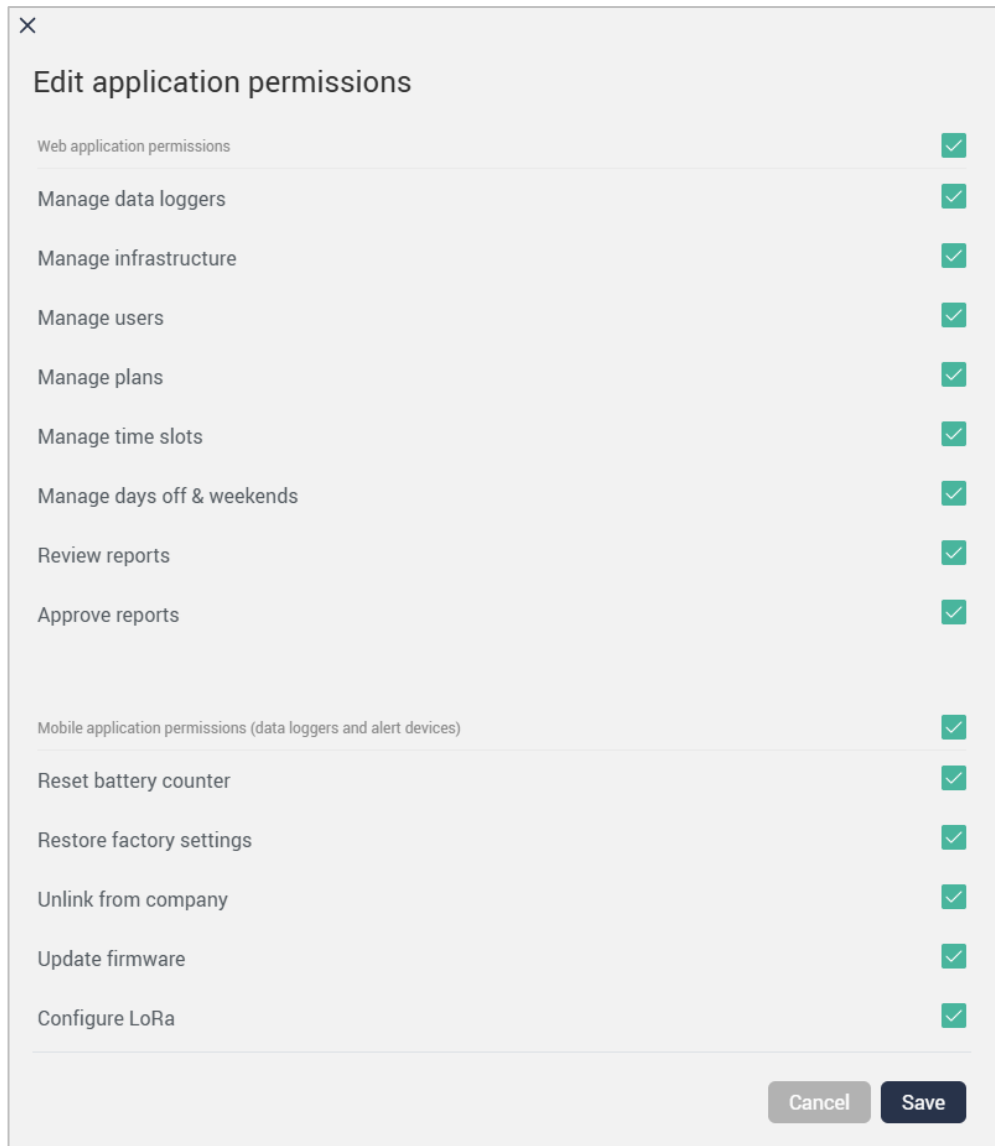


Figure 56 – Editing application permissions for a user account

Web application permissions:

<b>Manage data loggers</b>	Add, delete, and modify data loggers.
<b>Manage infrastructure</b>	Add, delete, and modify infrastructure devices such as gateways, wireless alert sirens, and wireless dry contact alert relay.
<b>Manage users</b>	Add, delete, and modify user accounts, including contact information and password reset.
<b>Manage plans</b>	Add, delete, and modify floor plan images used to identify equipment locations.
<b>Manage time slots</b>	Add, delete, and modify the time slots used in alert rules.

## Users and authentication modes

<b>Manage days off &amp; weekends</b>	Add, delete, and modify workdays and other days used in alert rules.
<b>Review reports</b>	Sign reports as a reviewer.
<b>Approve reports</b>	Sign reports as an approver.

Mobile application permissions (data loggers and alert devices):

<b>Reset battery counter</b>	Resetting the device's battery to 100% after a battery change.
<b>Restore factory settings</b>	Restoring original factory settings (clearing all information from device memory).
<b>Unlink from company</b>	Removing a device's association with a particular company.
<b>Update firmware</b>	Using OCEAView Mobile to perform firmware upgrades.
<b>Configure LoRa</b>	Using OCEAView Mobile to configure LoRa on Cobalt XS/X1/X2 and L3/ML3 data loggers, as well as Dickson LoRa sirens and dry contact alert devices.



Users can see their own applications permissions at any time (**My account → Options → Show user permissions**) but they cannot edit them.

---

### 5.3.2 Note about notifications related to account permissions

The above permissions grant application functionality on a system-wide level to a specific user. OCEAView displays a warning message if that user makes changes that represent a potential conflict with current configuration elsewhere in the system. Nonetheless, the system *does* allow the user to make the change.

For example:

- A team in your California laboratory uses a plan image to identify data logger location at their site.
- A user in Sweden with "Manage plans" permissions could delete that plan image from the system, though a warning message is displayed.

The same principle applies to the other application permissions, which could enable users to impact current configurations elsewhere in the system.

The benefit of this feature is that it enables the main Application Manager(s) to grant limited administrative roles to some user accounts. As with any computer system, these permissions must be granted only on an as-needed basis to qualified people.

### 5.3.3 Updating contact details

Contact information in OCEAView is used specifically for the purposes of notifying users in case of warnings and alarms.

You may only add contact information as described in this section if the user is assigned to an alert rule. This enables you to customize alert rules as needed for your organization, and then assign specific contact methods for a wide variety of situations.



If you want the user to receive alert notifications by e-mail and/or SMS text message, you must first assign that user to an alert rule as described in section 15.2.2 – *Alert rules with users*, p. 242.

---

To edit contact details for yourself or another user that is already associated with an alert rule:

1. For yourself, click on your account image → **My account**  
For other users, click on **Configuration** (⚙️) → **Users**  
Click on a line in the table to edit that user's account.
2. Click on **More** (⋮) → **Edit contact information**.



Contact information contained in OCEAView is independent from any external authentication (LDAP) platform information.

---

3. Enter the telephone numbers and/or e-mail addresses for the different time slots and different types of alerts configured in alert rules, as described in section 15.2.1 – *Configuring alert rules*, page 238

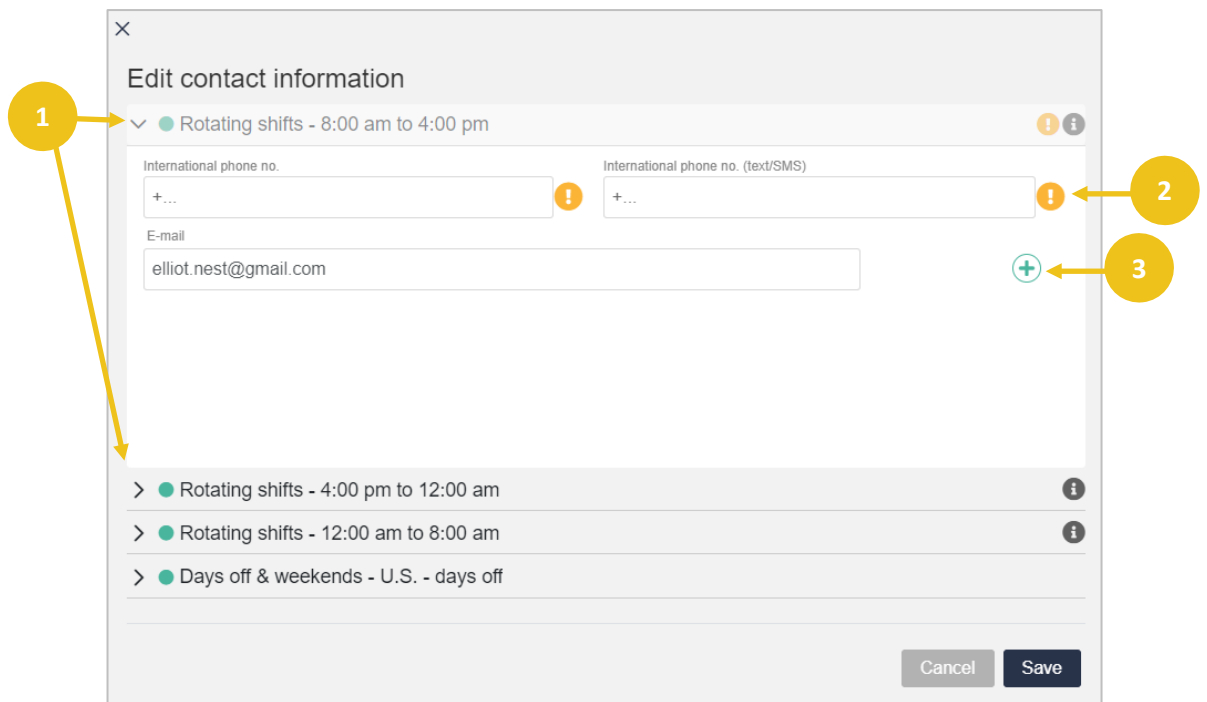




Figure 57 – Editing contact information to receive alert notifications

Description	
<b>1</b>	All time slots used in alert rules that include this user are displayed. In the above example, there are three work time slots and one time slot for days off and weekends.
<b>2</b>	An icon  is displayed wherever required information is missing. The user in the above screen is associated with an alert rule for voice and SMS/text message, so that information must be entered here. Telephone numbers must be entered in international format using the “+” sign and country code prefix.
<b>3</b>	You may add up to 3 email addresses for each time slot by clicking on <b>Add</b> (  ).



1. OCEAlert alert notification via voice messaging works with most types of mobile phones in many regions. SMS/text messages are supported on a large majority of mobile phones on the market today.
2. Remember to include the “+” sign and country code prefix for both your mobile and land-line phone numbers.
3. You cannot disable a user account if that user is associated with an alert rule.



### 5.3.4 Personalizing an account picture

OCEAView can personalize your display with a picture when you are logged in to the system. The picture is shown in the upper right-hand corner of the screen.

Picture recommendations:

- Maximum size: < 1 MB
- JPG or PNG format

To add a picture:

1. Click on the user image icon (  ) in the upper right-hand corner of the screen, then click on **My account** to open your profile directly (or click on **Users** in the left-hand menu and select your name in the user list).
2. Click on **More** (  ) and then select **Edit photo**.
3. Click on **Choose file**:

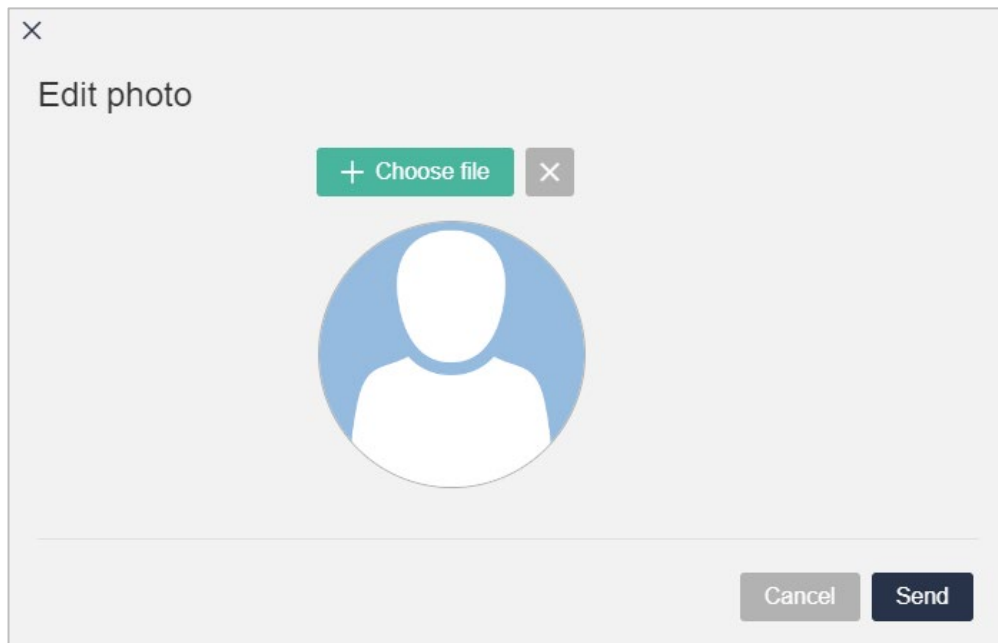


Figure 58 – Selecting a profile picture

4. Browse your computer to locate the image you want to use and then click on **Open**.
5. The image is uploaded and displayed in OCEAView.

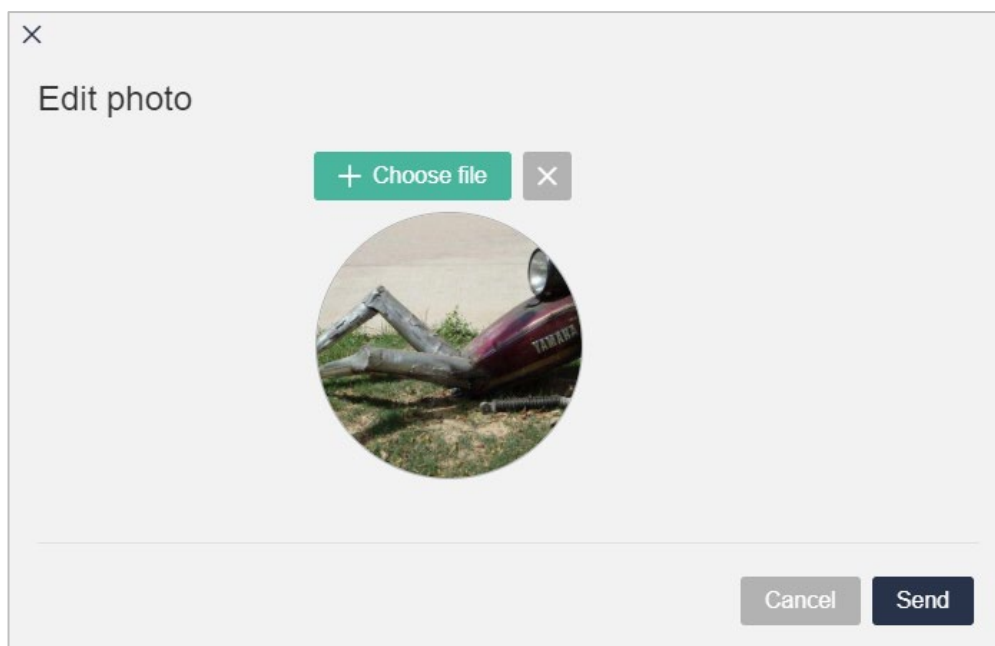



Figure 59 – Editing an account picture

6. Click on **Send** to save your changes and update your account.
7. If you want to delete the picture linked with the user account, click on  in the screen shown above.

## 5.4 Managing “Out of Office”

OCEAView includes an Out of Office feature that lets you inform the system that you (or a user you are configuring) are absent and should not receive notifications until a specified date and time.



If you choose to use this feature, make sure any alert rules that include this user also have a backup recipient.

To turn on Out of Office:

1. For yourself, click on your account image → **My account**  
For another user, click on **Configuration (⚙️)** → **Users**  
Click on a line in the table to edit that user’s account.
2. Click on **More (⋮)** → **Turn on Out of Office**
3. Click on the calendar icon (📅) and select the date and time until which Out of Office is activated.

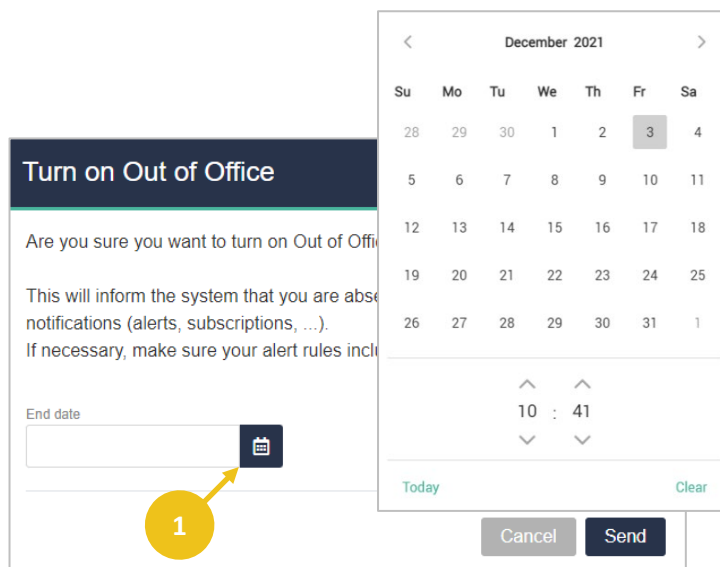


Figure 60 – Activating Out of Office functionality

4. Click on **Send** to activate Out of Office, or on **Cancel** to close this window without making any changes.  
Out of Office deactivates automatically at the date/time you set.

5. A suitcase icon (🧳) is displayed next to the user's name in the My account screen and in the User list:

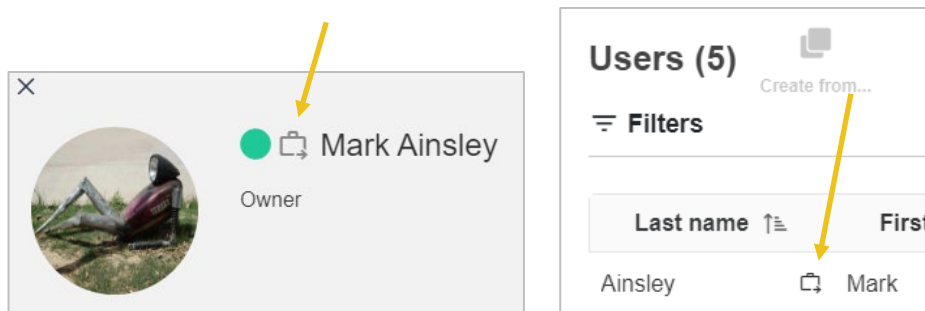


Figure 61 – Indication that Out of Office is turned on

6. You may edit the current Out of Office end date and time by selecting **More (⋮) → 🧳 Edit Out of Office**
7. You may deactivate Out of Office by selecting **More (⋮) → 🧳 Turn off Out of Office**
8. If you reconnect to OCEAView while Out of Office is turned on, the system asks whether you want to turn it off or leave it on.  
Select **No** to leave it on.  
Select **Yes** to turn it off.

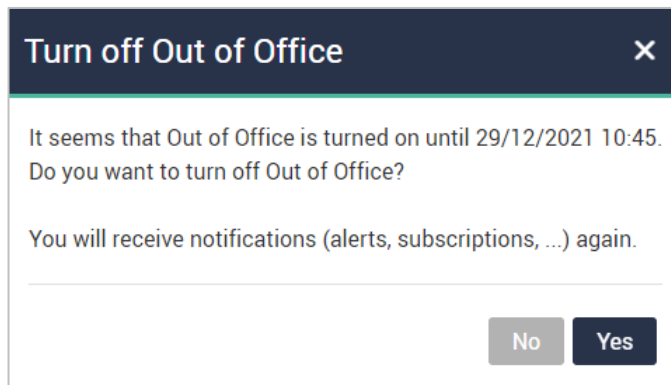


Figure 62 – System prompt if you log back in while Out of Office is still on

## 5.5 Managing passwords (internal authentication only)

### 5.5.1 Changing your own password



This section does not apply to users in systems using external authentication (LDAP or SSO).

---

Users can change their own passwords when using OCEAView's internal authentication.

#### To change your own password:

1. Click on your user profile in the upper right-hand corner of the screen then click on **My account**.
2. Click on **More** (⋮) in the top right-hand corner of the window and select **Change password**.
3. Enter the new password in the first field and type it again in the second field to confirm.
4. Click on **OK** to save your changes or **Cancel** to return to the previous screen.



Passwords must respect your organization's password security policy (as described in section 6.2 – System security settings, p. 95).

---

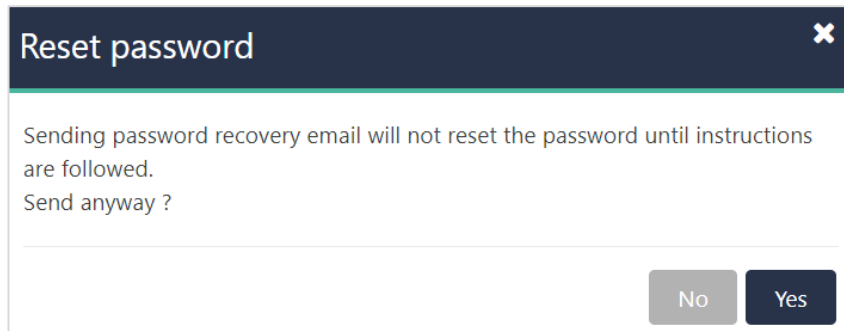
### 5.5.2 Resetting another user's password

Users with Application Manager rights can initiate a password *reset* for other people, when using OCEAView's internal authentication, but they cannot set the password for someone else. In all cases, users must set up their own passwords.

#### To change a password:

1. Click on **Configuration** (⚙️) → **Users**
2. Click on the user profile for which you want to reset the password.
3. The user details appear at the right of the screen.
4. Click on **More** (⋮) and then select **Reset password**.

5. In the password reset window, click on **Yes** to proceed with the process or **No** to return to the previous screen:



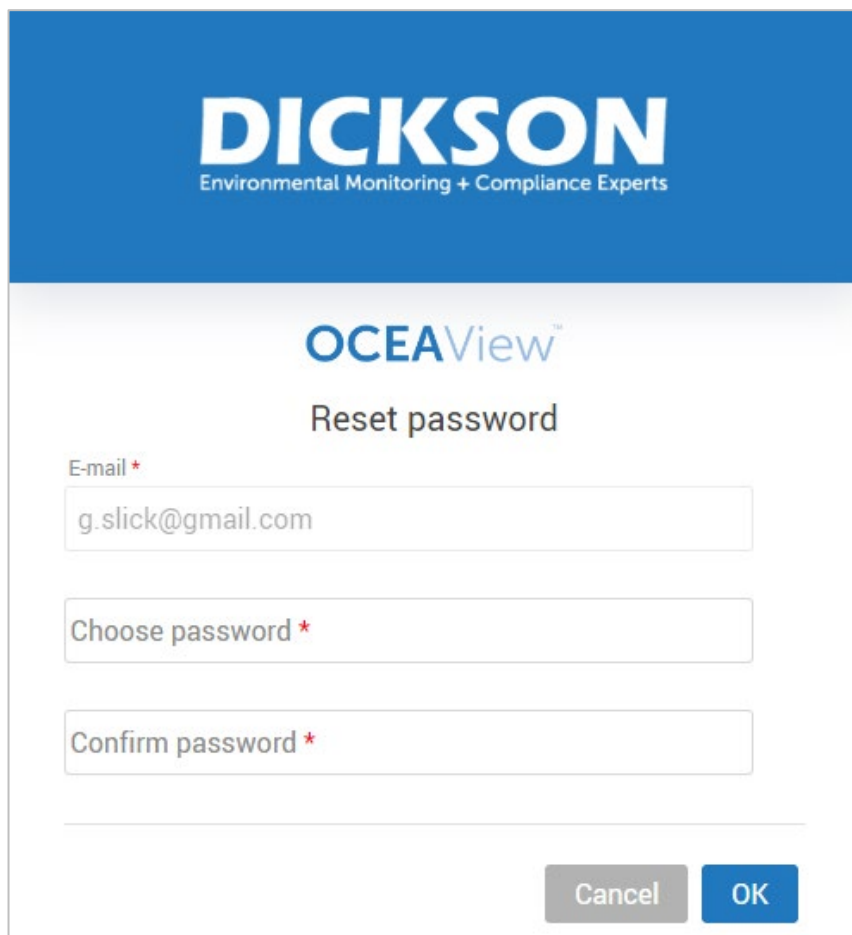
Reset password

Sending password recovery email will not reset the password until instructions are followed.  
Send anyway ?

No Yes

Figure 63 – Password reset confirmation

6. The password recovery email is sent to the user with instructions to reset his/her password as shown here:



DICKSON  
Environmental Monitoring + Compliance Experts

OCEAView™  
Reset password

E-mail \*  
g.slick@gmail.com

Choose password \*

Confirm password \*

Cancel OK

Figure 64 – Resetting a user's password

7. The change is taken into account when the user clicks on **OK**.

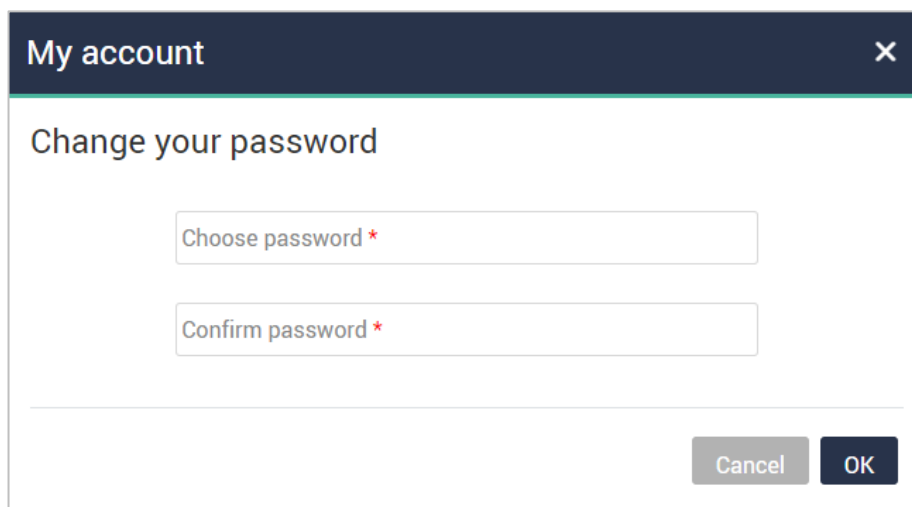
8. The regular login screen is displayed the next time the user logs in, and they are prompted to enter the new password. The user cannot login without changing the password.

**Note:** If the user's account is not locked or expired, it is still possible to connect with the old password even if the password has not been reinitialized.

### 5.5.3 Resetting your own password

A user may reset their own password, when using OCEAView's internal authentication, at any time as follows:

1. Click on the profile icon in the upper right-hand corner of the screen, then select **My account** → **Options** → **Change password**



The screenshot shows a modal dialog box titled "My account" with a close button (X) in the top right corner. Below the title bar, the heading "Change your password" is displayed. There are two text input fields: the first is labeled "Choose password \*" and the second is labeled "Confirm password \*". At the bottom right of the dialog, there are two buttons: "Cancel" (light gray) and "OK" (dark blue).

Figure 65 – Changing your own password

2. Enter a password in the first field, then enter the same password in the second field. The passwords must match and must respect your password security settings (Configuration → Security → Password policy).
3. Click on **OK** to save the new password, or on **Cancel** to close the window without saving.

## 5.6 Adding user roles

### 5.6.1 Overview: role permissions vs. application permissions

As mentioned previously, most user accounts in your system are created with a “User” profile. This account profile starts by giving people view-only access to specific parts of the application. Remember, the “Application manager” profile is generally limited to a few super-users who need complete access to every aspect of the application.

For individual users, you may assign application-wide permissions (as described in section 5.3.1 – *Assigning application permissions to “User” profile accounts, p. 72*) in order to give those people more administrative abilities in terms of system set up and management.

Nonetheless, people with a “User” profile account often need to manage a variety of day-to-day tasks, typically within their part of the organization (described in detail in chapter 6 – *Setting up your organization, p. 88*). OCEAView therefore enables you to create different roles that can be assigned to those accounts for this purpose.

Role permissions enable you to fine-tune responsibilities and application access within your organization for:

- Managing organization / equipment
- Start data logging
- Stop data logging
- Acknowledge alarms
- Manage metrology parameters
- Manage alert rules

### 5.6.2 Creating new roles

Roles are used to allow people with user-level accounts to perform to a variety of different actions that can be considered as “daily” types of actions. Roles are assigned to people as they are associated with sites and/or departments, and a person may have different roles in different parts of the organization. For example, they could be limited to viewing information in one department and only be allowed to acknowledge alarms in another.

OCEAView starts with three default roles: **Manager**, **Acknowledger**, and **View only**.

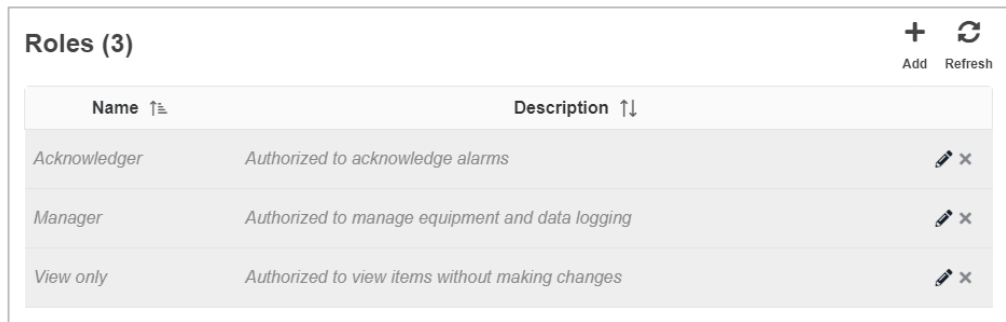


Only Application Managers can add or customize user roles.

---

To add a new user role and assign permissions:

1. In the main menu, click on **Configuration** (  ) → **Roles**










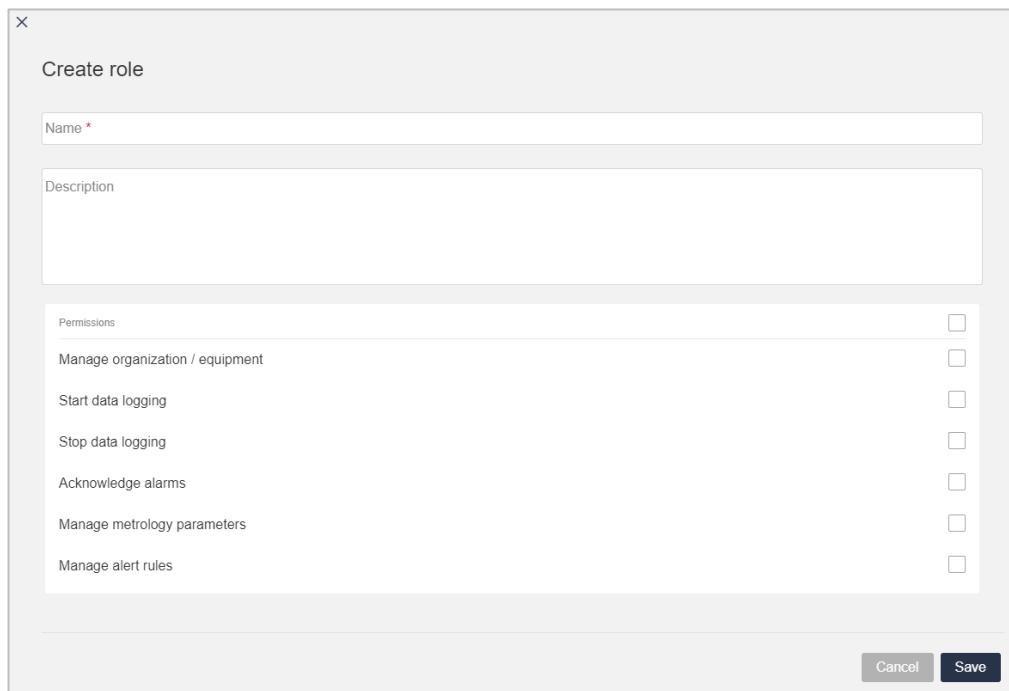
Name ↑↓	Description ↑↓	
Acknowledger	Authorized to acknowledge alarms	 
Manager	Authorized to manage equipment and data logging	 
View only	Authorized to view items without making changes	 

Figure 66 – Default user roles in OCEAView

The default system roles are shown with a gray background and may not be edited.

2. Then click on **Add role** (  ), which opens the **Create role** window shown here:



Create role

Name \*

Description

Permissions

- Manage organization / equipment
- Start data logging
- Stop data logging
- Acknowledge alarms
- Manage metrology parameters
- Manage alert rules

Cancel Save

Figure 67 – Adding a new user role within your organization

3. Fill in the fields as required:

**Name** Enter a name for the new user role.

**Description** Enter a description for the user role (optional).

**Permissions** The permissions listed here define what a user is allowed to do in one or more parts of the organization. To grant permissions, check the permission(s) you want to assign to the role:

**Manage organization:**

The user can set up and configure the system's organizational structure and include other users as allowed.

**Start data logging:**

The user can start data logging for equipment.

**Stop data logging:**

The user can stop data logging for equipment.

**Acknowledge alarms:**

The user can acknowledge alarms.

**Manage metrology parameters:**

The user can update calibration settings.

**Manage alert rules:**

The user can create, edit, and update alert rules.

If you want to assign all these permissions at once, click on the checkbox above the list to select all the checkboxes.

4. Click on **Save** to apply your changes or on **Cancel** to discard your changes. Here is an example after adding a role called "Calibration".

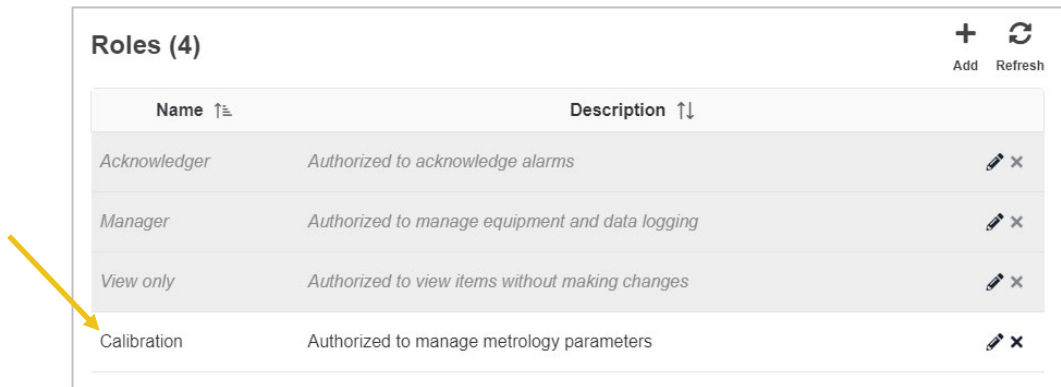


Figure 68 – Custom role displayed in role list

Once the role is created, you may use it when assigning users to sites and departments in your organization, as described in section 6.3.4 – *Assigning a user role in your organization's hierarchy*, p. 103.

## 6 Setting up your organization

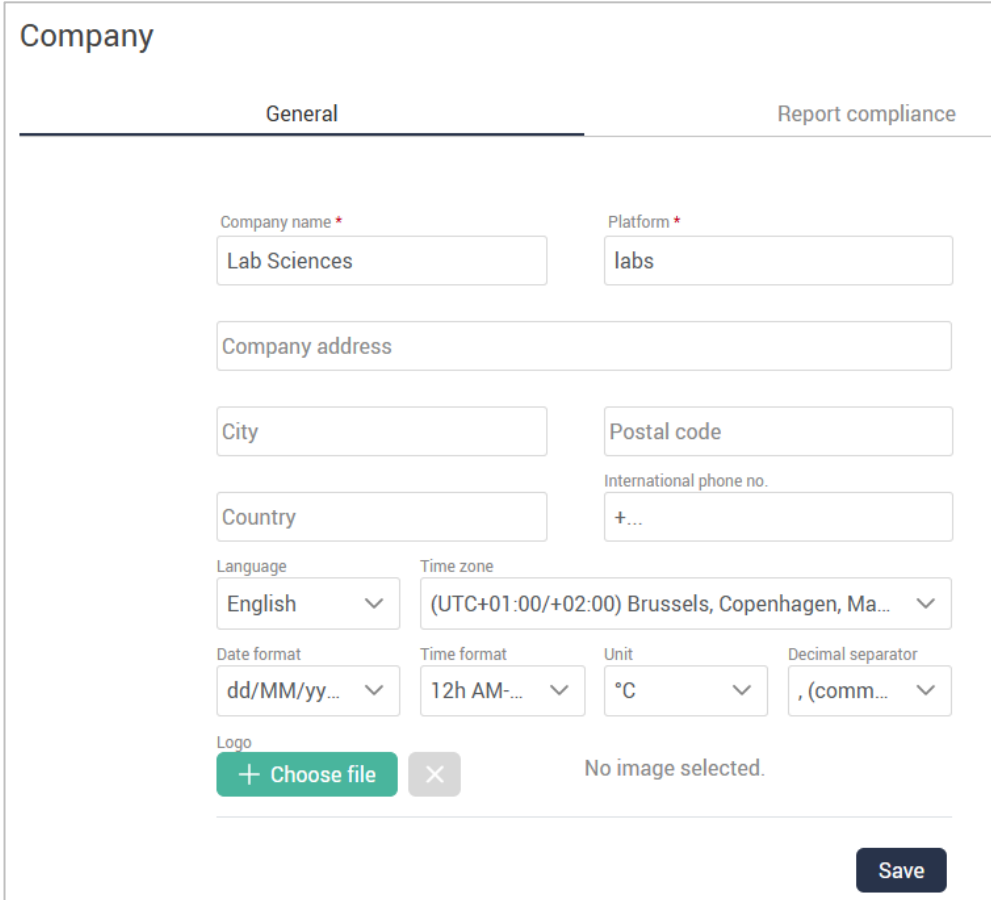
### 6.1 Updating company information

You may update all company information at any time, except for the main contact e-mail address.

#### 6.1.1 General information

To update the general information regarding your company account:

1. Click on **Configuration** (  ) → **Company**



The screenshot shows the 'Company' configuration screen with two tabs: 'General' (selected) and 'Report compliance'. The 'General' tab contains the following fields:

- Company name \***: Text input field containing 'Lab Sciences'.
- Platform \***: Text input field containing 'labs'.
- Company address**: Text input field.
- City**: Text input field.
- Postal code**: Text input field.
- Country**: Text input field.
- International phone no.**: Text input field containing '+...'. A small '+' icon is visible to the left of the field.
- Language**: Dropdown menu showing 'English'.
- Time zone**: Dropdown menu showing '(UTC+01:00/+02:00) Brussels, Copenhagen, Ma...'. A small '+' icon is visible to the left of the field.
- Date format**: Dropdown menu showing 'dd/MM/yy...'. A small '+' icon is visible to the left of the field.
- Time format**: Dropdown menu showing '12h AM-...'. A small '+' icon is visible to the left of the field.
- Unit**: Dropdown menu showing '°C'. A small '+' icon is visible to the left of the field.
- Decimal separator**: Dropdown menu showing ', (comm...'. A small '+' icon is visible to the left of the field.
- Logo**: A file upload area with a green '+ Choose file' button, a grey 'x' button, and the text 'No image selected.'.

A dark blue 'Save' button is located at the bottom right of the form.

Figure 69 – Company information screen

2. Fill in the required fields (marked with \*) as appropriate.

<b>Company name</b>	Enter the name of your company.
<b>Platform</b>	This unique company identifier is filled in automatically based on the company name you enter.
<b>Company address...</b>	...City, Postal code, Country, International phone number: enter the relevant information for your company.



Make sure you enter the telephone number in international format, with the prefix “[country code]”, such as: +14153817894

Do not include any extra digits or leading zeros.

---

The settings below apply as a default for your system. They can be overridden by each person’s individual settings for local operation and display purposes, but this information is used as a common reference for the company in case people have conflicting profile settings for shared actions. For example, if you have e-mail alerts sent to people in different regions, English could be the default company language for a same alert message.

<b>Language</b>	Choose the desired default language for your company. Users are free to choose their own personal preference at any time.
<b>Time zone</b>	Select the time zone based on the primary geographical area for the company.
<b>Date format</b>	Select how dates are displayed in the application.
<b>Hour format</b>	Select how time is displayed in the application. Readings can be displayed in the <b>12-hour (AM/PM)</b> or <b>24-hour</b> format.
<b>Unit</b>	Temperature can be displayed in degrees <b>Celsius (°C)</b> or <b>Fahrenheit (°F)</b> .
<b>Decimal separator</b>	Select the character to use as a decimal separator in numerical values.
<b>Logo</b>	If you want to add a logo image for your company, click on <b>Choose file</b> (JPG or PNG format, maximum size 1 MB). This image is used to personalize exports in Word and PDF formats.

3. Make the desired changes directly in the form and then click on **Save** to save the information.

### 6.1.2 Enabling the report review & approval process

The options on the **Report compliance** tab activate the report review and approval feature in the specified areas of the application.

Category	Enabled
Enable report review & approval cycle	<input checked="" type="checkbox"/>
Equipment	<input checked="" type="checkbox"/>
Alarms & warnings	<input checked="" type="checkbox"/>
Audit trail	<input checked="" type="checkbox"/>
Data loggers	<input checked="" type="checkbox"/>
Readings	<input checked="" type="checkbox"/>
Infrastructure	<input checked="" type="checkbox"/>

Save

Figure 70 – Activating report review and approval functionality

Reviewing and approving reports is described in detail in section 14.2 – *Reviewing and approving reports*, p. 209.

### 6.1.3 Managing license keys

Access to OCEAView is based on one or more service subscriptions linked with the number of sensors in your system. The following services require a subscription:

- **OCEAView web application** and all integrated features (including 24/7 alerts by e-mail only) for a specified number of measurement points.
- **OCEAlert alert notification system**, an additional service that provides 24/7 alert notification by telephone voice call and/or SMS-text message (to a cellular telephone). OCEAlert is included by default in the OCEAView Cloud platform version, though a license key is still provided.



Please contact your authorized Dickson representative for more information regarding subscriptions.

When you sign up for one (or both) of these subscriptions, you will receive the associated license key number(s) to enter in OCEAView.

To view information about your OCEAView solution or add a new license key:

1. Click on **Configuration** (⚙️) → **License keys**

This page shows information related to your licenses, such as activation key codes and expiration dates. The Dickson technical support team may ask you to provide this information if you contact them for assistance.

2. To enter a new license key number, click on **Add** (+):

License key	Product	Description	Expiration ↓
XXXXX-XXXXX-XXXXX-XXXXX-P2AAA-YDDCE	OCEAView	100 measurement points	02/12/2025

Figure 71 – Current list of license keys

3. Enter your new license key number in the pop-up window:

**Add license key** [X]

License key \*

Cancel Save

Figure 72 – Entering the new license key number

## Setting up your organization

4. Click on **Save** to register your license or **Cancel** to discard changes and return to the previous screen.
5. Once the license key is registered, the activation key number is shown in the table, along with the license type and expiration date. In this example, we added an OCEAlert license:


License keys (2) <span style="float: right;">+ Add   ↻ Refresh</span>			
License key	Product	Description	Expiration ↓
XXXXX-XXXXX-XXXXX-XXXXX-P2AAA-YDDCE	OCEAView	100 measurement points	02/12/2025
XXXXX-XXXXX-XXXXX-XXXXX-JICAA-AHKK4	OCEAlert		04/14/2023

Figure 73 – Your monitoring system's licenses

### 6.1.4 Renewing or expanding your current license

If you need to renew one of your licenses or upgrade your current license (such as to expand the number of authorized measurement points), simply click on **Add license key** ( **+** ) and enter the new license number as described above in section 6.1.3 – *Managing license keys, 91*.

### 6.1.5 License expiration e-mail reminders

As the expiration date for any of the licenses in your OCEAView solution draws closer, a message is displayed in the upper right-hand corner of the screen, with a reminder in the **Notifications** menu. Click on the  icon to open the menu:

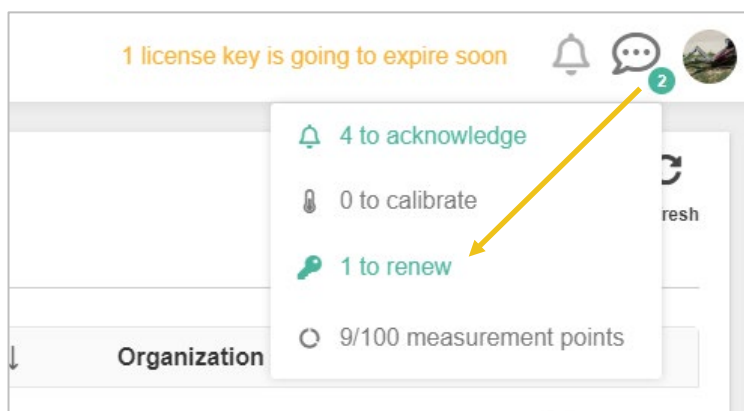


Figure 74 – First reminder to renew license 90 days before expiration

This reminder is displayed, and the first e-mail is sent starting 90 days before the license expiration date.

---

E-mail reminders are sent regularly up until the expiration date and after, as follows:



- 90, 60, 30, 21, 14, 7, 6, 5, 4, 3, 2, and 1 day(s) before expiration
  - On the expiration date
  - Once a day for 7 days after expiration
-

The e-mail reminders are no longer sent after 7 days following expiration. Lines in the license key table containing keys that have reached their expiration date are shown in grey with *italic text*:



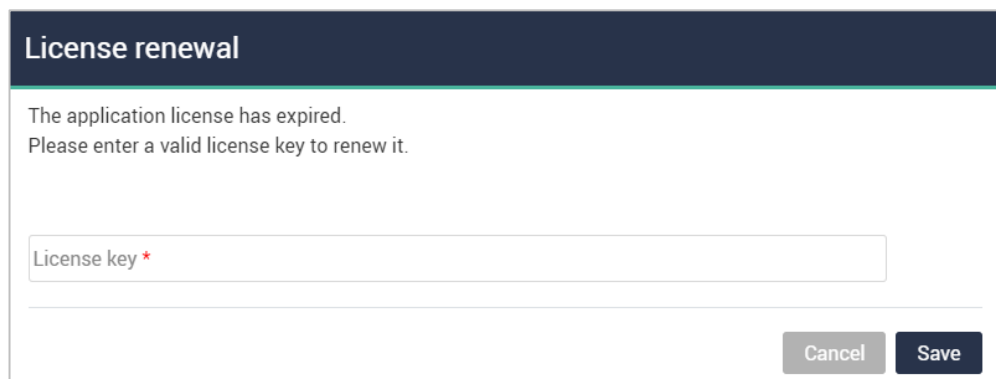
License key	Product	Description	Expiration ↓
XXXXX-XXXXX-XXXXX-XXXXX-P2AAA-YDDCE	OCEAView 2.0	100 measurement points	02/12/2025
XXXXX-XXXXX-XXXXX-XXXXX-JICAA-AHKK4	OCEAlert		04/14/2023

Figure 75 – Expired license(s) indicated in grey and italics

### 6.1.6 Renewing an expired OCEAView license

If your OCEAView license expires, you will not be able to connect to the system unless you enter a new license key.

If you attempt to log in to a company account whose license has expired, you will see this screen, prompting you to enter a new license key:



**License renewal**

The application license has expired.  
Please enter a valid license key to renew it.

License key \*

Cancel Save

Figure 76 – Entering a new license key for an expired company account

To continue, you must enter a new license key. Please contact your Dickson representative to obtain a new key. Simply enter the new key and click on **Save** to log in.

## 6.2 System security settings

OCEAView allows you to configure several system-wide security options according to your needs and situation:

- Password policy (when using internal user authentication)
- OCEAView Mobile application access

Security settings apply to all users.

### 6.2.1 Password policy

To control password settings:

1. Click on **Configuration** (⚙️) → **Security**
2. Select the appropriate settings in the **Password policy** tab.

The screenshot shows the 'Security' configuration page with the 'Password policy' tab selected. The page is divided into two sections: 'Password policy' and 'Application'. The 'Password policy' section includes the following settings:

- Password strength**
  - Require capitals and lowercase
  - Require special characters
  - Minimum number of characters:
- Password reuse**
  - Allow password reuse
  - Prevent password reuse of last  passwords
- Password expiration**
  - Password never expire
  - Password will expire after  days
- User lockout**
  - Users will never get locked out
  - Users will be locked out after  failed login attempts
    - Lockout lasts for  hours

A 'Save' button is located at the bottom right of the form.

Figure 77 – Configuring your system's password policy

Here is a description of the options in this screen:

---

<b>Password strength</b>	
Require capitals and lower case	Passwords must contain both capital and lower-case letters.
Require special characters	Passwords must include at least one special character (punctuation, symbols, etc.)
Minimum number of characters	The password must contain the indicated number of characters or more.

---

<b>Password reuse</b>	
Allow password reuse	When creating a new password, the user may reassign one that has been used previously.
Prevent password reuse of last [ X ] passwords	When creating a new password, the user may not assign a password that has been used within the past "X" password changes.

---

<b>Password expiration</b>	
Passwords never expire	Passwords do not expire and therefore do not need to be changed by users.
Passwords will expire after [ X ] days	Users will be prompted to change their password when the indicated number of days has passed.

---

<b>User lockout</b>	
Users will never get locked out	The system will not lock out users after several failed login attempts.
Users will be locked out after [ X ] failed login attempts	When this option is selected, users will be locked out of the system if they enter the wrong password the specified number of times.
Lockout lasts for [ X ] hours	This field indicates how long the user's account remains locked if an incorrect password is entered too many times, mainly as a measure to prevent automated attacks. The system unlocks the user's account after the specified number of hours, or the user may choose to reset their password instead of waiting.

---

## 6.2.2 Granting access to external applications

### 6.2.2.1 Access for OCEAView Mobile users

Dickson provides an iOS and Android mobile application for OCEAView called OCEAView Mobile. Among other features, the mobile application enables users to push data from Dickson Atlas and Emerald Bluetooth-enabled data loggers.


#### Important notes about OCEAView synchronization

In the OCEAView Mobile app, users must be connected (logged in) to the OCEAView web platform to:



1. **Start data logging**, as Atlas and Emerald data loggers must correspond to equipment present in the OCEAView web platform
2. **Push data** via their smartphone

To allow connected OCEAView Mobile users to push Atlas and Emerald data to the OCEAView web platform:

1. Click on **Configuration** (  ) → **Security**
2. Click on the **Application** tab.

Security

Password policy      Application

Mobile application access

Yes  Users can access from the mobile application      Save

Communication key




 .....  

Figure 78 – Authorizing access for OCEAView Mobile users

3. Use the slider to determine whether users are allowed to push (synchronize) data:

Yes

Users **may push** data from their smartphone.

No

Users **may not push** data or login to their company account from their smartphone.

4. Click on **Save**.


**Note:** see also section 5.3.1 – *Assigning application permissions to “User” profile accounts, p.72* for related mobile application settings.

### 6.2.2.2 Communication key allowing access for Cobalt 2 Bridge

Cobalt 2 Bridge is a software connectivity tool provided by Dickson that allows you to integrate previous-generation data loggers with the OCEAView web platform.

During the installation process, you will be asked to enter the “Communication key”, which is provided in OCEAView.

To access the communication key:

1. Click on **Configuration** (  ) → **Security**
2. Click on the **Application** tab.

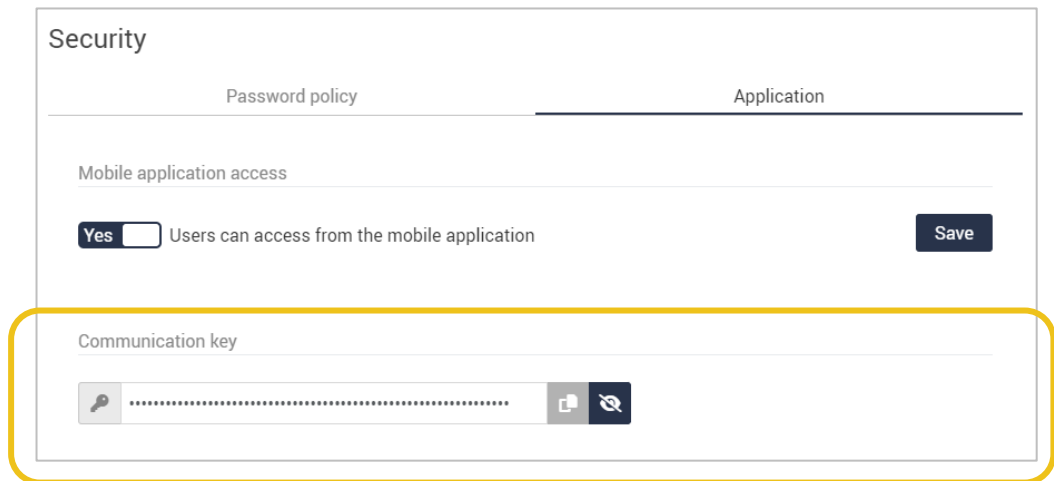




Figure 79 – Accessing the OCEAView communication key

The communication key information is read-only. You may click on  to copy the text to the clipboard, or on  to display the text in the field.

## 6.3 Organizing your system with sites and departments

Your OCEAView monitoring system is comprised of one **Organization**, which may be sub-divided into **Sites** and **Departments**.

This feature enables you to create a logical hierarchy for managing your system based on geographical, operational, or any other criteria that may be useful to you. For example, you could create a hierarchy such as this:

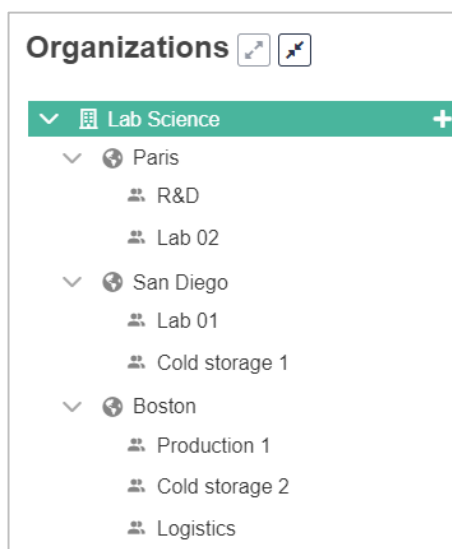


Figure 80 – Creating a hierarchy that is appropriate for your organization

Equipment, data loggers, users, and infrastructure devices are assigned to the various nodes within the overall organization.

Users may even have different roles (as described in section 5.6 – *Adding user roles, p. 85*) in different parts of the organization. For example, a user could be a site manager in a specific laboratory, but be limited to view-only rights for a facility in another location.

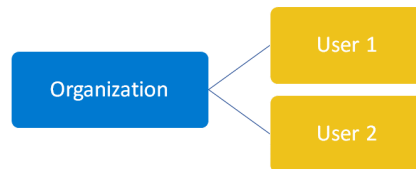


Equipment and infrastructure devices (such as gateways) can only be assigned to one entity in the hierarchy.

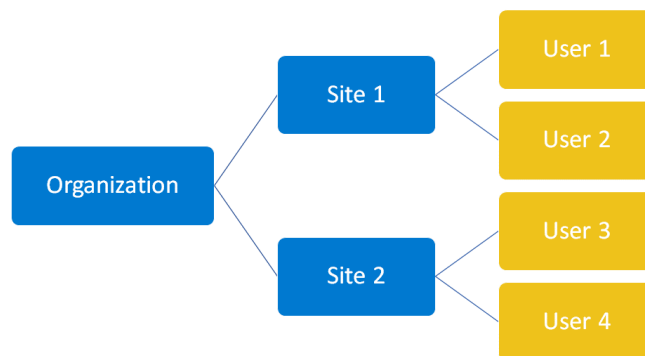
## Setting up your organization

An organization can have from one to three levels – Organization, Site, and Department – (shown in **blue** below). You are not required to create sub-divisions with this feature, though it tends to make management much more intuitive than a “flat” structure, especially for large organizations. You may associate users (shown in **yellow**) at whichever level of the organization works best for you. Here are three examples:

Ex. 1: Users directly attached to Organization:



Ex. 2: Users assigned to sites in the Organization:



Ex. 3: Users assigned to departments and sites in the Organization:

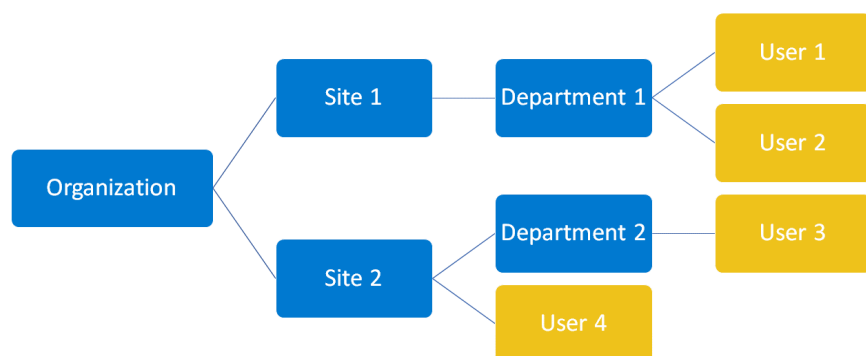


Figure 81 – Sample organizational structures with users assigned at different levels

### 6.3.1 Adding sites

To add a new site:

1. Click on **Configuration** (⚙️) → **Organizations**
2. Click on the name of your company account and then click on **Add site** 1

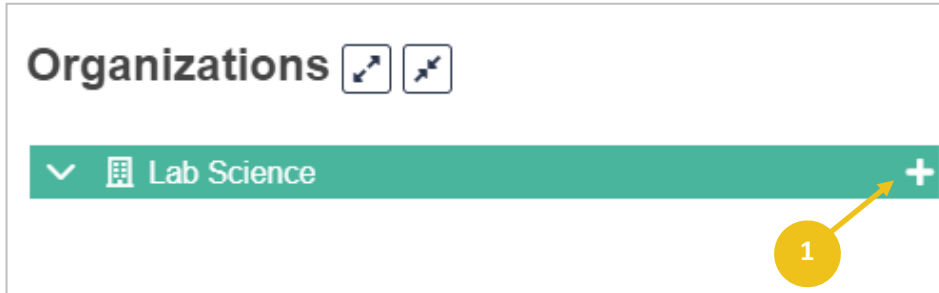


Figure 82 – Adding a new site

3. Enter a name for the new site in the pop-up window and click on **Save**:

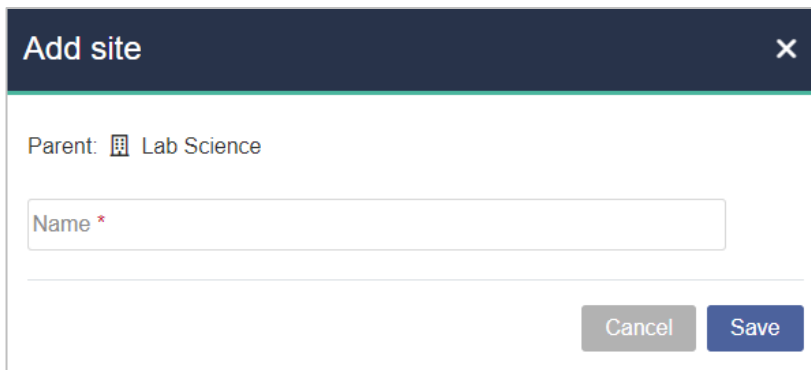





Figure 83 – Entering the new site name

The new site appears in your organization's tree structure. You may click on   or the triangles (  ) in the tree to expand and contract the view. Add as many sites as necessary for your organization.

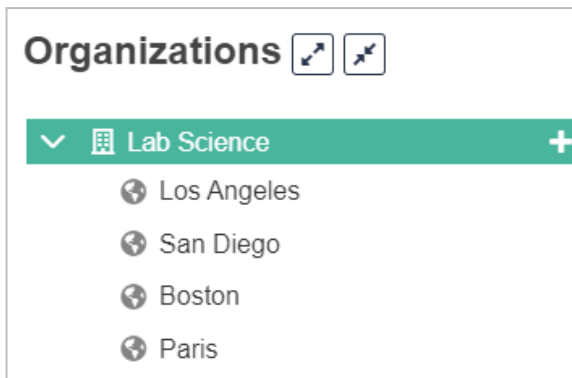


Figure 84 – Adding sites to set up your organization

### 6.3.2 Adding departments

To add a new department:

1. Click on **Configuration** (⚙️) → **Organizations**.

In your organization's tree structure, click on the site and then on **Add department** (+) 2:

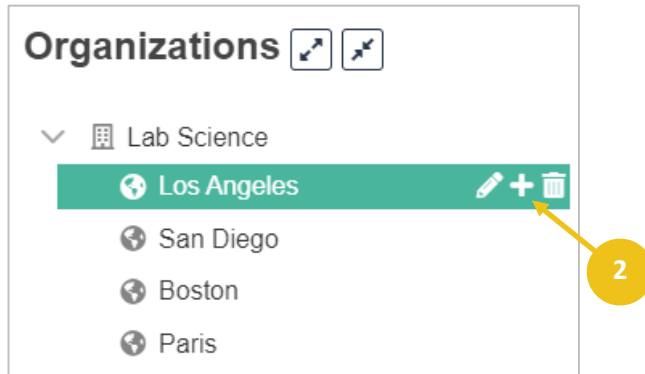


Figure 85 – Adding a new department

2. Enter a name in the pop-up window for the new department and click on **Save**:

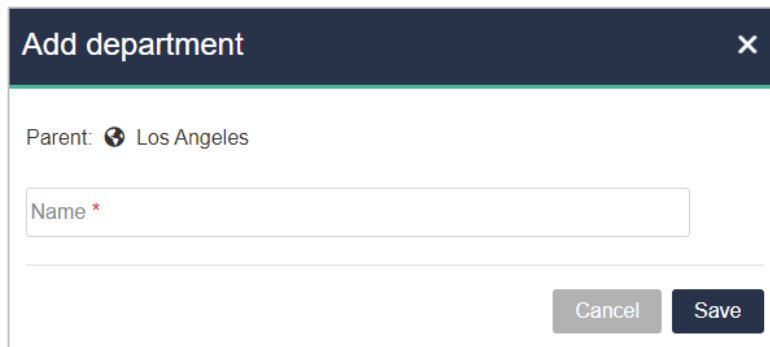


Figure 86 – Entering the new department name

3. The new department is listed in your organization's tree structure:

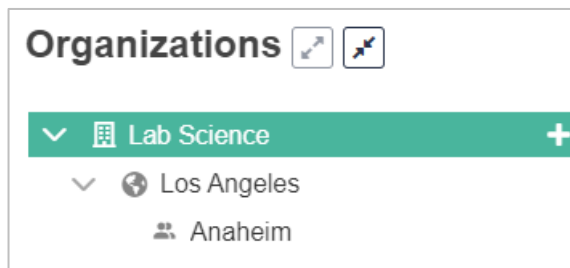






Figure 87 – Organizational structure

### 6.3.3 Editing / deleting a site or department

To manage your different sites and departments, click on the desired node in the organizational structure and use the available options:

- New** To add a new site or department, click on 
- Delete** To delete a site or department, click on 
- Edit** To edit a site name, click on . Modify or enter a new name and then, confirm your changes by clicking on 

### 6.3.4 Assigning a user role in your organization's hierarchy

When you first start, you have one organization with the Application Manager – the person who created the company account – listed with a manager role. Application managers are associated automatically with all the nodes in your organizational structure. Those users cannot be removed. Other users must be added here.

You must create users (see *chapter 5 – Users and authentication modes, p. 51*) before you can add them to your sites and departments.

To associate a user with the organization or a site or department:

1. Click on **Configuration** → **Organizations** → **Associate users** ( .

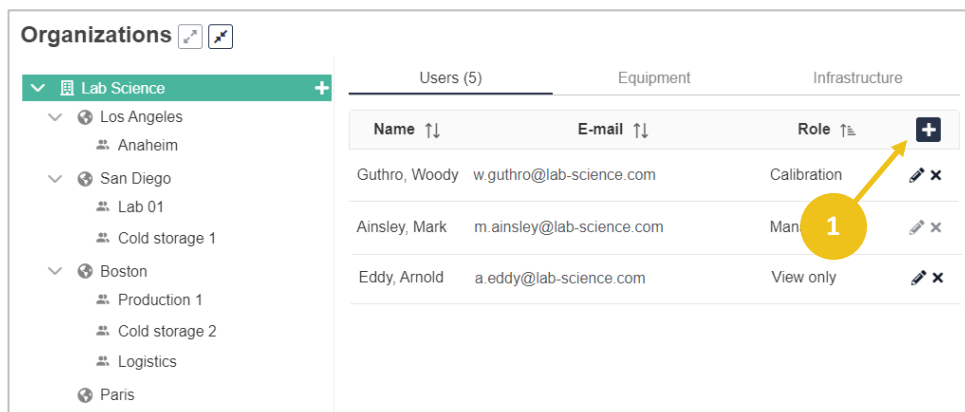


Figure 88 – Adding users to the organization's hierarchy

2. The **Associate user** window opens as shown here:

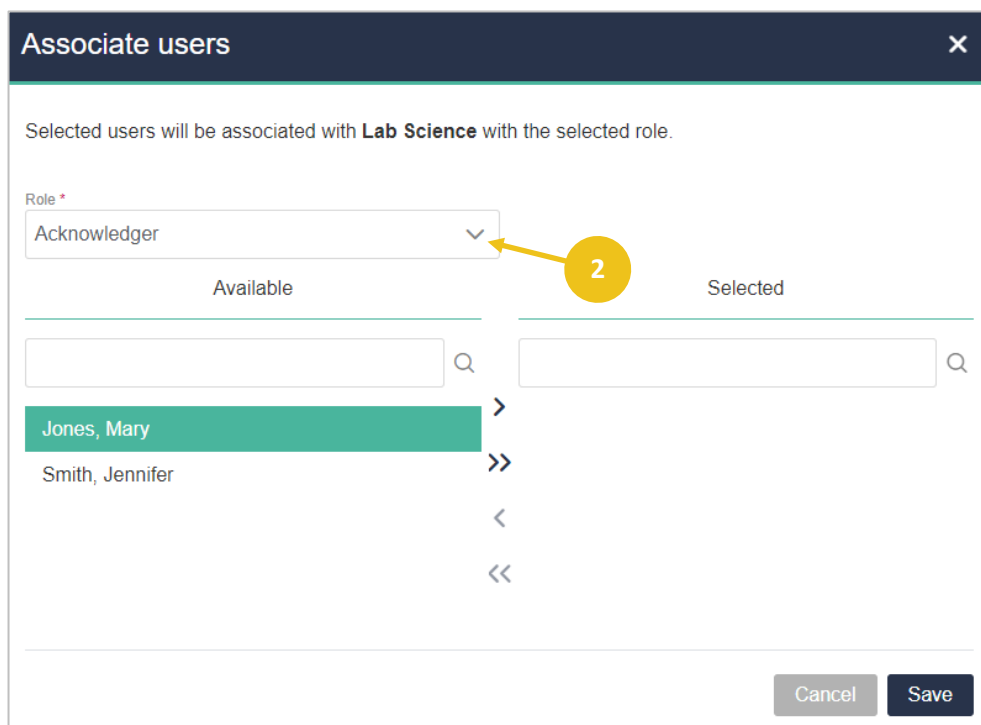


Figure 89 – Associating a user within the organization hierarchy


In the role drop-down list **2**, select the role you want to assign to this user depending on your needs for the site or department. A role determines the actions that the user can perform and the objects that they can manage in OCEAView.


There are three roles by default:

- **Acknowledger**  
User profiles with **acknowledgement** rights can acknowledge alarms issued by the system for the sensors they are monitoring. They may also disable those sensors if necessary.
- **Manager**  
User profiles with Manager rights can manage other users and access all application features, except for license and authentication mode management.
- **View only**  
User rights are limited to viewing only. These users do not have access to management and configuration windows.

Other roles may be added, as described previously in section 5.6 – *Adding user roles, p. 85*.


3. Add users to your organization:


**Available** Select a user from the list of **Available** users. Then click on  to move the user to the list of **Selected** users on the right-hand side.

To select multiple users at a time, press and hold the **Ctrl** key and click on each of the users you want to select. Click on  to add them to the list of **Selected** users.

To select all available users, click on .

**Selected** To remove a user from your organization, click on that user in the list of **Selected** users and then click on  to move the user to the list of **Available** users on the left-hand side.

To remove multiple users, press and hold the **Ctrl** key and, while holding down the key, click on each of the other users you want to remove. Then click on  to move them to the list of **Available** users on the left.

To remove all users, click on .

4. Click on **Save** to save your changes or **Cancel** to exit this screen without saving changes.

### 6.3.5 Viewing equipment and infrastructure in your organization

The table on the Organizations screen also contains tabs **1** that you can use to list Equipment and Infrastructure assigned to sites and departments.

The example below shows the equipment and infrastructure elements assigned to the “Los Angeles” site:

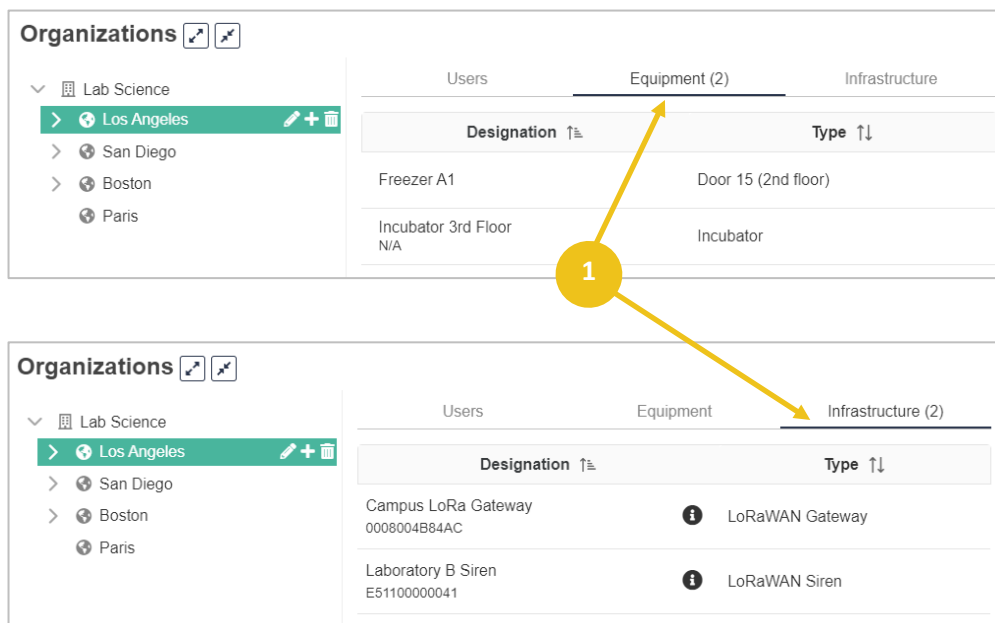




Figure 90 – Listing the equipment and infrastructure in your organization

## 6.4 Site plan images

OCEAView allows you to visually place your equipment on floor plan representing the layout of your organization. Plans are useful for identifying the locations of the sensors associated with the equipment you are monitoring. You may add as many plans as necessary.

### 6.4.1 Adding a plan

To add a plan:

1. In the main menu, click on **Configuration** (  ) → **Plans**
2. Click on **Add** (  ) to import a plan image:

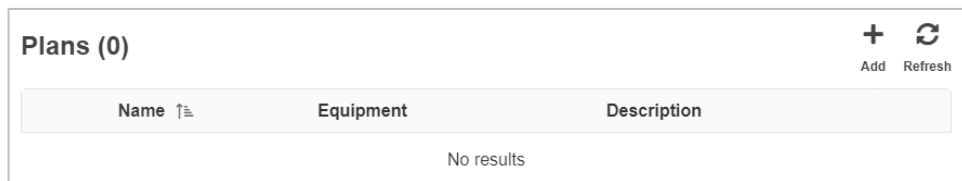
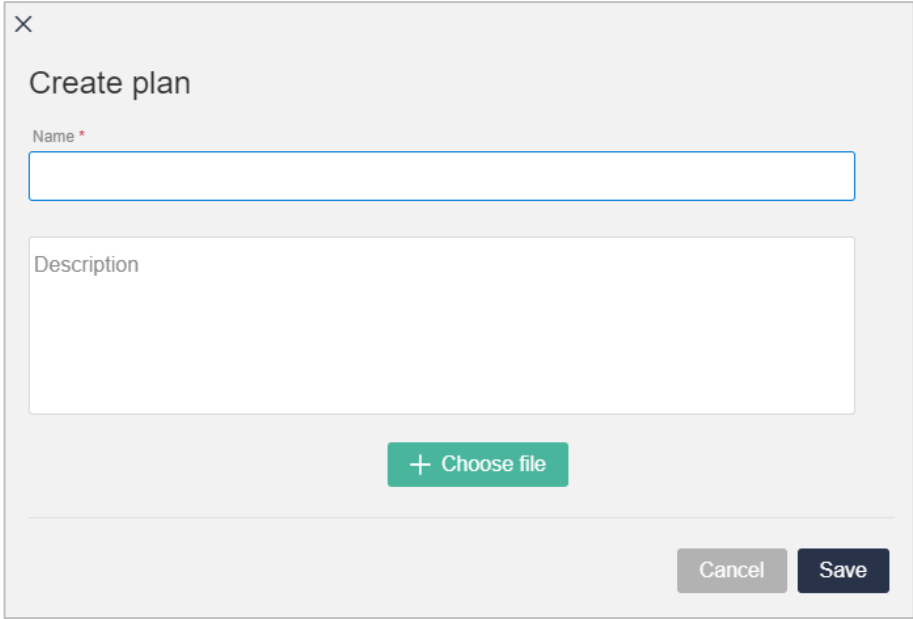


Figure 91 – Managing plans

3. The **Create plan** window opens as shown here:



×

### Create plan

Name \*

Description

+ Choose file

Cancel Save

Figure 92 – Adding a new floor plan

4. Enter a name for the floor plan in the **Name** field.
5. You may add a description in the **Description** field (optional).
6. Click on **Choose file** and select the desired image of your premise (JPG, PNG, or GIF format up to 1 MB maximum size).
7. A preview image is displayed after you load the floor plan:

## Setting up your organization

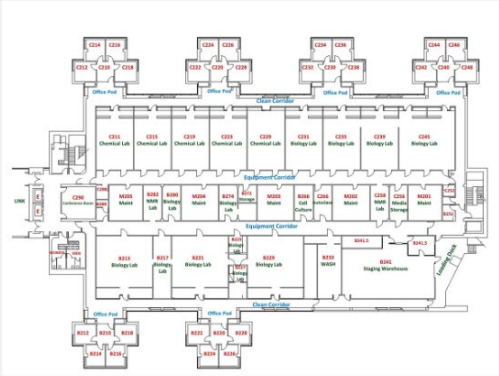
×

### Create plan

Name \*

Description

+ Choose file



Cancel Save

Figure 93 – Adding a new floor plan



8. You may click on the image to enlarge it on the screen.
9. Click on **Save** to add the floor plan to your system, or on **Cancel** to close this window and discard your changes.

## 6.4.2 Editing or deleting a plan

You may edit (replace) or delete plan images from your system by clicking on the icons on the right-hand side of the screen :








Figure 94 – Editing or deleting an existing plan

-  Allows you to change the name, description, or plan image as described in the previous section.
-  Allows you to delete the plan from your system.

### 6.4.3 Placing equipment on the plan

Once you have loaded one or more floor plan images, you may place your equipment on the image according to its physical location.

To place equipment on the plan:

1. In the main menu, click on **Equipment** (  ).
2. Select the equipment you want to place on the plan.
3. The equipment details are shown on the right-hand side of the screen.
4. Click on **More** (  ) in the upper right-hand corner of the equipment window and then click on **Edit location**.
5. Select the desired floor plan from the list using the **Plan** drop-down list  to display the image.
6. Click on the desired location to place your equipment on the image. The colored pin (  ) moves to show the new position . If the equipment was already present, the grey pin remains in place to show the previous position, which disappears after you save the new equipment location.

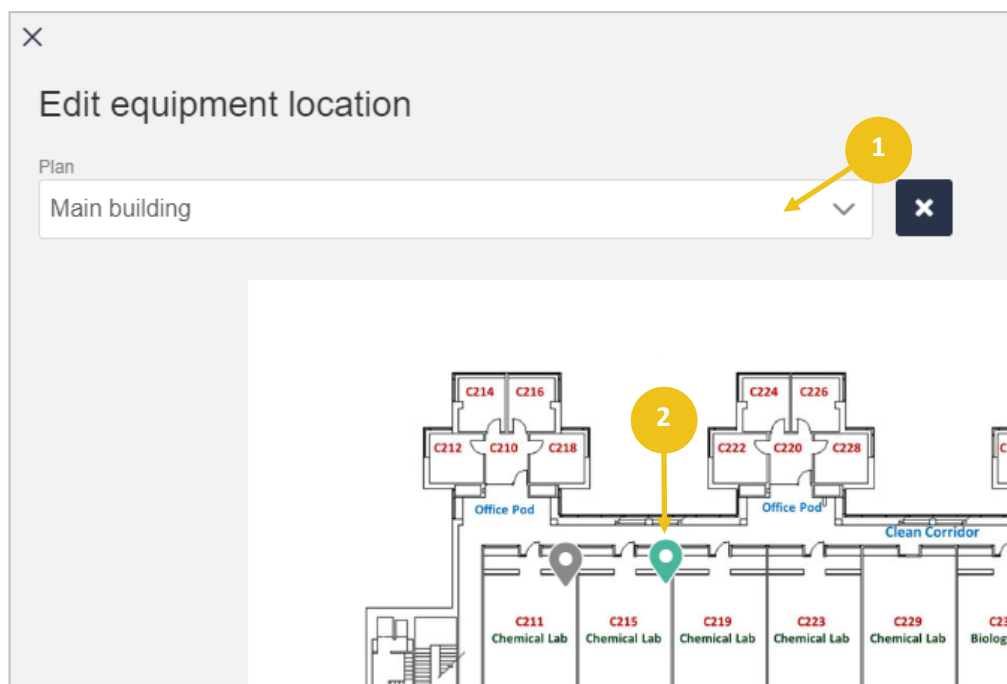



Figure 95 – Placing an equipment on the plan

If you want to remove the equipment from the image, you may click on the **Remove association** button (  ).

7. Click on **Save** to save the equipment location (or removal) or click on **Cancel** to return to the previous screen without saving the changes.

## 7 Infrastructure: Wireless gateways

This section describes how to include wireless gateways as infrastructure devices in your monitoring system. One or more wireless gateway must be up and running to set up your data loggers and collect data from them. OCEAView supports the following gateways:

- Dickson LoRaWAN Gateway
- OCEABridge Bluetooth Gateway



Siren and Dry Contact alert devices are also handled as infrastructure in OCEAView, and are covered in chapter 8 – *Infrastructure: Siren & Dry Contact alert devices, p. 116.*

---

### 7.1 Note about LoRaWAN gateway as infrastructure

The Dickson LoRaWAN gateway is entirely configured in an administrator interface integrated in the gateway itself, as described in the Dickson LoRaWAN Gateway User Guide. You may access the User Guide via the **Help** menu in the OCEAView web application.

You are not *required* to configure the gateway in the OCEAView web application for functional purposes. However, if you want to receive alerts in case a technical problem arises, you must add the gateway to your OCEAView infrastructure as described in this chapter.





Even if it is not technically required to add your gateways as infrastructure in OCEAView, we recommend that you do include them in order to receive technical alerts in case of problems.

---



## 7.2 Adding a LoRaWAN or OCEABridge gateway

Follow these steps to add a gateway (gateway) to your system configuration:

1. Click on **Infrastructure** (  ) in the main menu and then click on **Add** (  ):

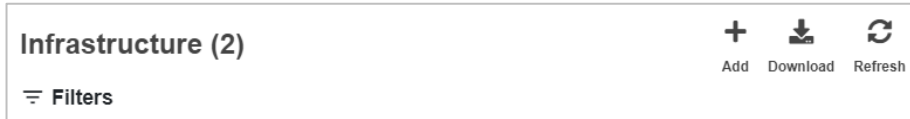
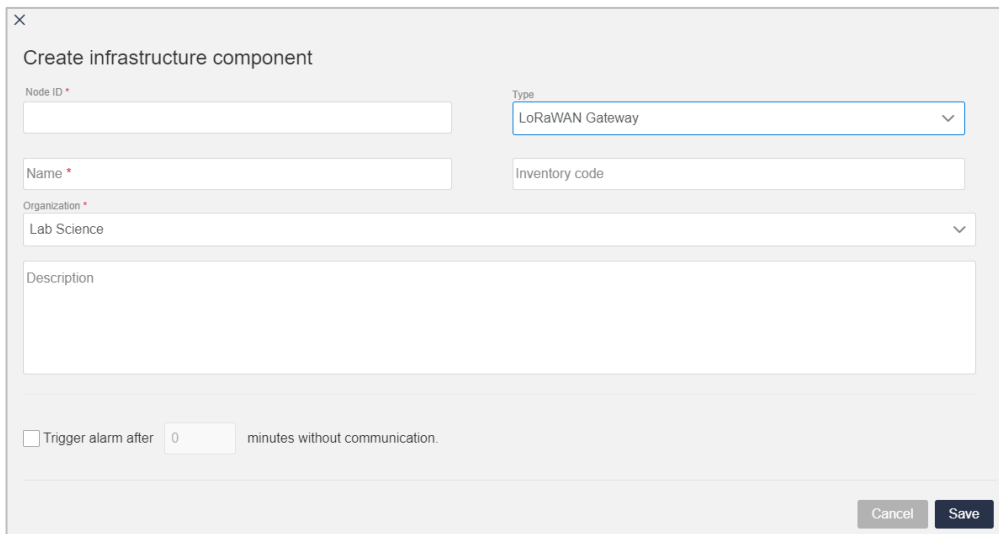


Figure 96 – Click to add infrastructure

2. The **Create infrastructure component** window opens as shown below.



The screenshot shows a form titled "Create infrastructure component" with the following fields and options:

- Node ID \***: A text input field.
- Type**: A dropdown menu with "LoRaWAN Gateway" selected.
- Name \***: A text input field.
- Inventory code**: A text input field.
- Organization \***: A dropdown menu with "Lab Science" selected.
- Description**: A large text area.
- Trigger alarm after**: A checkbox followed by a text input field containing "0" and the text "minutes without communication."

At the bottom right, there are "Cancel" and "Save" buttons.

Figure 97 – Adding gateway details

3. Enter the gateway details in this screen. Fields marked with a red asterisk (\*) are required:

<b>Serial number</b>	Enter the serial number provided on the back of your gateway. The system identifies the device based on its serial number. If you enter an incorrect serial number, a red exclamation mark is shown in front of the corresponding field. Check the serial number and try again.
<b>Type</b>	The Type is assigned automatically based on the serial number you enter.
<b>Name</b>	Enter a name for the infrastructure component. This name is used as the reference in all lists.
<b>Inventory code</b>	(Optional) You may enter the inventory code of the infrastructure element for information purposes.
<b>Organization</b>	Use the drop-down list to select the department to which the infrastructure element is associated. It may be helpful to associate the gateway with a

specific node in your organization in order to manage precise alert management and alarm acknowledgement rights.

Note: to add other departments, follow the procedure described in section 6.3 – *Organizing your system with sites and departments*, p. 99

**Description** (Optional) You may enter a description of the component for information purposes.

**Trigger alarm after...** Check this option and enter the delay (in minutes) after which the system will trigger an alarm if the infrastructure component is not responding. This mechanism ensures early notification in case of problems or a communication error.

4. Click on **Save** to add your gateway to the system, or on **Cancel** to close this window without saving changes.

## 7.3 Editing infrastructure information

To manage existing infrastructure, use the following options:

1. In the main menu, click on **Infrastructure**.
2. Click on a line in the table to view or edit the desired device.

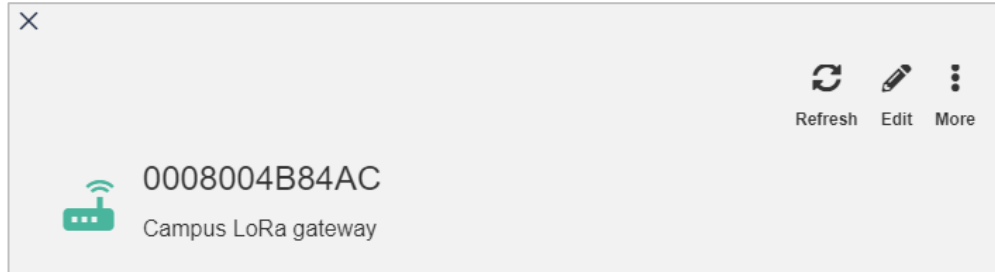









Figure 98 – Editing infrastructure details

3. Click on **Edit** (  ) on the right-hand side of the screen and edit information directly as necessary.
4. Several other functions are available in this screen:

<b>More</b> 	 <b>Alarm history</b>	Opens the Alarm list so you can see any alarms involving this device (a filter is applied to show "Infrastructure" with the device's serial number).
	 <b>Simulate an alarm</b>	You may use this function to simulate an alarm for testing purposes.
	 <b>Disable</b>	Click to disable the device's functionality (in the Infrastructure list, a filter enables you to display or hide disabled infrastructure).
	 <b>Remove</b>	Click to remove the device from your system. The device is marked as "removed" in the Infrastructure list. If you wish to restore the same device, you must create it again by entering the serial number.
<b>Refresh</b> 		Refreshes the infrastructure information window.

5. Click on **Save** to keep your changes, or on **Cancel** to return to the previous screen without saving changes.

## 8 Infrastructure: Siren & Dry Contact alert devices

The OCEAView system supports several “digital” alert notification mechanisms, notably:

- E-mail (integrated in all OCEAView systems)
- SMS/Text message (optional via OCEAlert)
- Automated voice call (optional via OCEAlert)

In addition, you may use hardware alert devices via LoRaWAN® wireless technology:

- **LoRaWAN Alert Siren**  
(audio & visual alerts)



- **LoRaWAN Alert Relay device**  
(triggers a connected external dry contact device)



This chapter describes how to add these hardware devices to your system.



## 8.1 Adding a Dickson LoRaWAN Siren



### Audio warning

Siren devices may emit sound levels that could damage hearing. Please use caution when using the Dickson LoRaWAN Siren by turning down the volume and then adjusting it as appropriate.

To add a LoRaWAN Siren to your system:

1. Click on **Infrastructure** (  ) in the left-hand menu, then on **Add** (  ).
2. Fill in the fields to create the new LoRaWAN Siren:

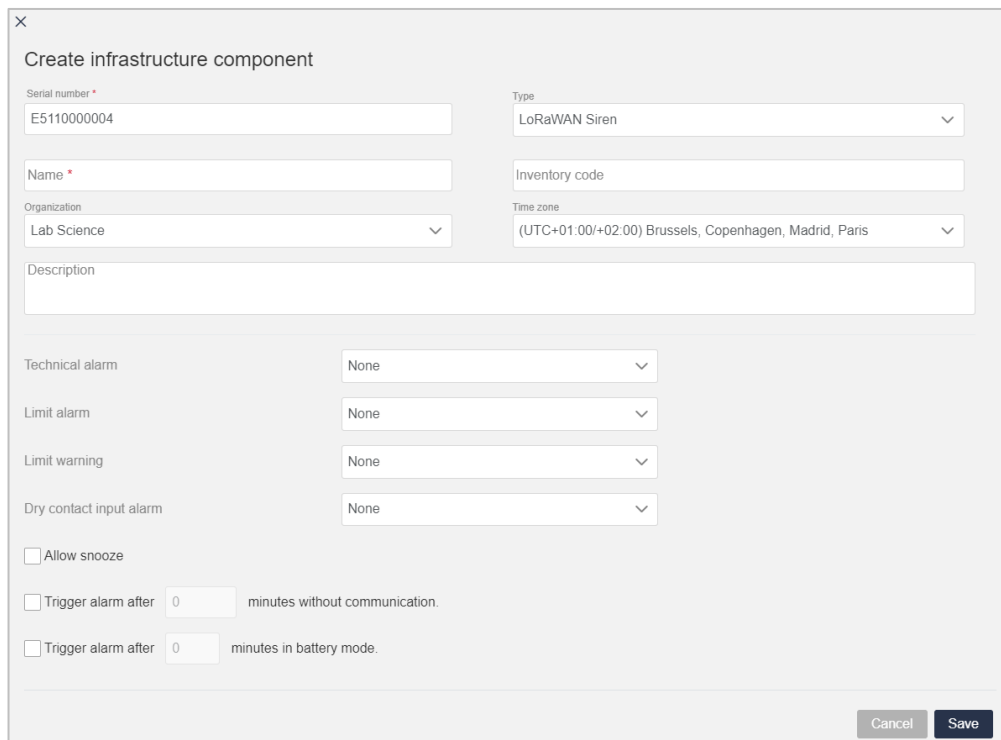



Figure 99 – Adding a LoRaWAN Siren to your system

**Serial number** Enter the serial number provided on your product.

**Type** Select LoRaWAN Siren. If you select the incorrect type of device here, it will be adjusted automatically upon the system's first connection.



We recommend that you test new alert devices by simulating alerts. You may test the siren directly by clicking on **More** (  ) → **Simulate an alarm** once the device has been created, and/or in the full context of testing an alert rule by simulating a sensor alarm.

<b>Name</b>	Enter a "friendly name" to use as a reference in your system.
<b>Inventory code</b>	Enter an inventory code for this device (optional).
<b>Organization</b>	You must assign the device to a branch of your organization. Choose the level that is appropriate for your hierarchy.
<b>Time zone</b>	Enter the time zone in which the device is located in order to make sure that it is activated at the right moment (as defined in Alert rules).
<b>Description</b>	You may enter information here as desired (optional).
<b>Technical alarm</b>	Choose how the siren should react when receiving a technical alarm, such as a low data logger battery:  <b>None</b> = no reaction  <b>Buzzer and light</b> = Audio sound + red siren light  <b>Light only</b> = Red siren light only
<b>Limit alarm</b>	Choose how the siren should react when receiving a limit alarm, such as a temperature excursion (None, Buzzer and light, Light only)
<b>Limit warning</b>	Choose how the siren should react when receiving a limit warning, such as a temperature excursion (None, Buzzer and light, Light only)
<b>Dry contact alarm</b>	Choose how the siren should react when receiving a dry contact input alarm from a Cobalt X1/X2 data logger (None, Buzzer and light, Light only)
<b>Allow snooze</b>	Enables you to press the snooze button on the siren to turn off the light and/or buzzer for 12 hours for a given alarm.

**Trigger alarm after  minutes without communication**

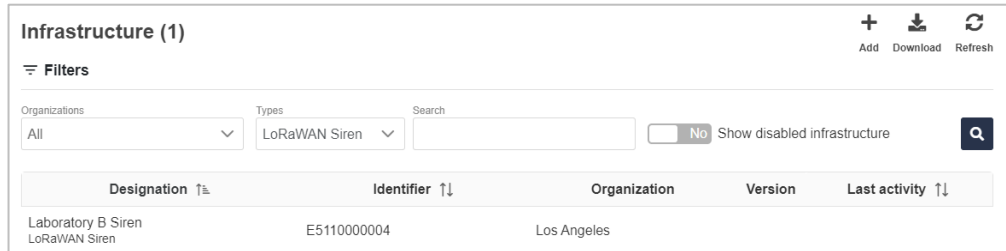
The system checks communication with all devices periodically. If the system fails to communicate with the siren, and then fails again after "X" minutes that you specify, an alarm is triggered (such as an e-mail or text message).

**Trigger alarm after  minutes on battery mode**

## Infrastructure: Siren & Dry Contact alert devices

If the siren switches from AC power to battery mode, an alarm is triggered after the number of minutes you specify here.

3. The new siren is listed in the Infrastructure list shown here:



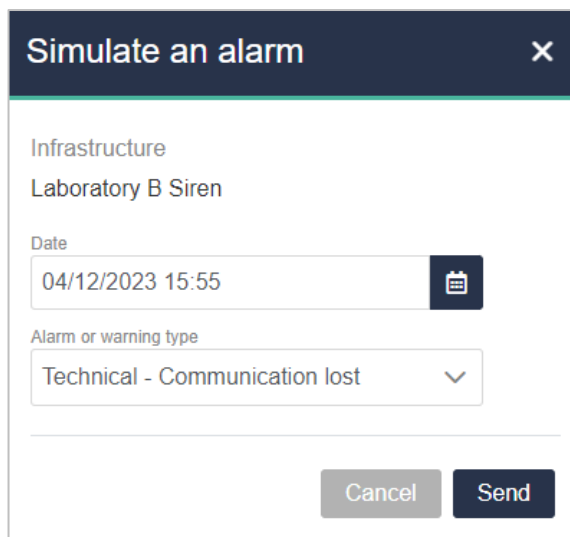
Designation ↑↓	Identifier ↑↓	Organization	Version	Last activity ↑↓
Laboratory B Siren LoRaWAN Siren	E511000004	Los Angeles		

Figure 100 – Siren shown in Infrastructure list

### 8.1.1 Testing your LoRaWAN Siren

We recommend that you test any newly installed alert devices to ensure proper operation in your context. To test the siren:

1. Click on the siren name in the list.
2. Click on **More** (⋮) → **Simulate an alarm** (🔔)  
**Note:** this alarm is useful for testing the siren device itself, outside the context of any alert rules.
3. Confirm details in the window that opens:



The screenshot shows a modal window titled "Simulate an alarm" with a close button (X) in the top right corner. The window contains the following elements:

- Text: "Infrastructure" and "Laboratory B Siren"
- Date field: "Date" with a calendar icon, showing "04/12/2023 15:55"
- Alarm or warning type dropdown: "Alarm or warning type" with a dropdown arrow, showing "Technical - Communication lost"
- Buttons: "Cancel" and "Send" at the bottom right.

Figure 101 – Details for simulating an alarm

Use the pull-down list to choose one of the available alarm types for the siren: "Technical – Communication lost", "Technical – Power lost", or "Technical – Low Battery".

4. Click on **Send** to launch the test, or on **Cancel** to return to the previous window without taking any action.

### 8.1.2 Other LoRaWAN Siren functions

Once you have added the siren to your system, you may include it in alert rules to notify users in case of alarms. chapter 15 – *Alarms & alerts*, p. 227 provides details on how to configure alerts. Other functions 1 are available by clicking on the siren in the list, which opens the siren details as shown here:

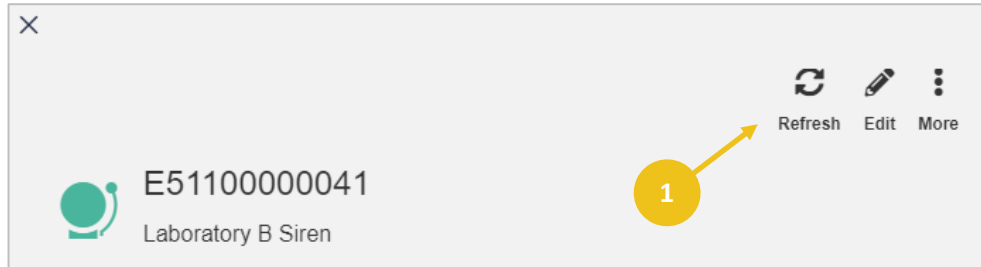











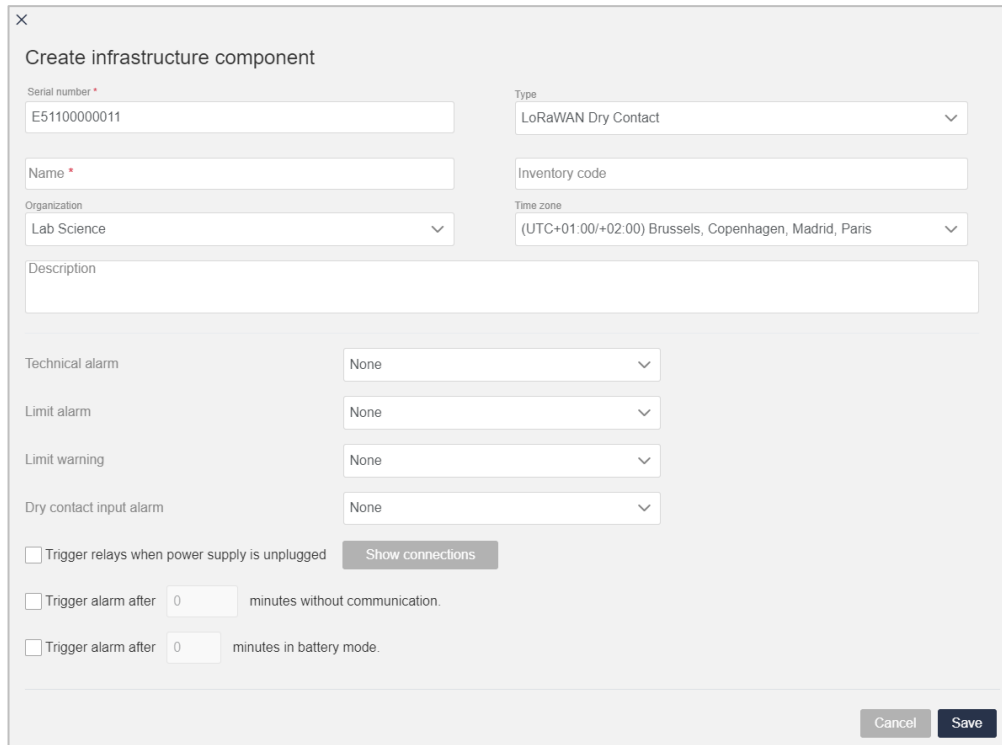
Figure 102 – Additional options for LoRaWAN Siren management

More 	<p> <b>Alarm history</b> Opens the Alarm list so you can see any alarms involving this device (a filter is applied to show "Infrastructure" with the siren's serial number)</p> <p> <b>Simulate an alarm</b> You may use this function to simulate an alarm as described in the previous section.</p> <p> <b>Disable</b> Click to disable the siren's functionality (in the Infrastructure list, a filter enables you to display or hide disabled infrastructure).</p> <p> <b>Remove</b> Click to remove the siren from your system. The siren is marked as "removed" in the Infrastructure list. If you wish to restore the same siren, you must create it again by entering the serial number.</p>
Refresh 	Refreshes the siren information window.
Edit (  )	Opens the <b>Edit infrastructure</b> window in which you may modify all the same details you entered when creating the siren.

## 8.2 Adding a Dickson LoRaWAN Dry Contact device

To add a LoRaWAN Remote Contact alert relay device to your system:

1. Click on **Infrastructure** (  ) in the left-hand menu, then on **Add** (  ).
2. Fill in the fields to create the new LoRaWAN Dry Contact device:



The screenshot shows a web form titled "Create infrastructure component" for a "LoRaWAN Dry Contact" device. The form includes the following fields and options:

- Serial number \***: Text input field containing "E51100000011".
- Type**: Dropdown menu set to "LoRaWAN Dry Contact".
- Name \***: Empty text input field.
- Inventory code**: Empty text input field.
- Organization**: Dropdown menu set to "Lab Science".
- Time zone**: Dropdown menu set to "(UTC+01:00/+02:00) Brussels, Copenhagen, Madrid, Paris".
- Description**: Empty text area.
- Technical alarm**: Dropdown menu set to "None".
- Limit alarm**: Dropdown menu set to "None".
- Limit warning**: Dropdown menu set to "None".
- Dry contact input alarm**: Dropdown menu set to "None".
- Trigger relays when power supply is unplugged. **Show connections** button.
- Trigger alarm after 0 minutes without communication.
- Trigger alarm after 0 minutes in battery mode.


Buttons for "Cancel" and "Save" are located at the bottom right of the form.

Figure 103 – Adding a Dry Contact alert relay device to your system

**Serial number** Enter the serial number provided on your product.

**Type** Select LoRaWAN Dry Contact. If you select the incorrect type of device here, it will be adjusted automatically upon the system's first connection.



We recommend that you test new alert devices by simulating alerts. You may test the dry contact device directly via **More** (  ) → **Simulate an alarm** once the device has been created, and/or in the full context of testing an alert rule by simulating a sensor alarm).

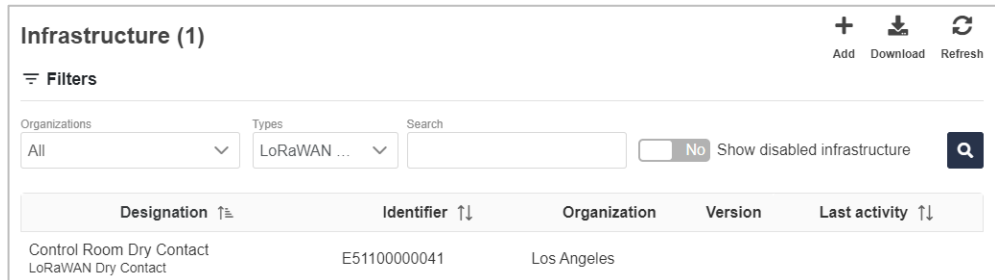
**Name** Enter a "friendly name" to use as a reference in your system.

<b>Inventory code</b>	If you have an inventory code for this device, you may enter it here (optional).
<b>Organization</b>	You must assign the device to a branch of your organization. Choose the level that is appropriate for your hierarchy.
<b>Time zone</b>	Enter the time zone in which the device is located in order to make sure that it is activated at the right moment (as defined in Alert rules).
<b>Description</b>	You may enter information here as desired (optional).
<b>Technical alarm</b>	Choose how the remote dry contact device should react when receiving a technical alarm, such as a low data logger battery:  <b>None</b> = no reaction  <b>Relay 1</b> = Triggers state change on relay 1 (terminals 1-2-3)  <b>Relay 2</b> = Triggers state change on relay 2 (terminals 4-5-6)  <b>Relay 1 &amp; relay 2</b> = Triggers state change on both relays
<b>Limit alarm</b>	Choose how the device should react when receiving a limit alarm, such as a temperature excursion (None, Relay 1, Relay 2, or Relay 1 & relay 2)
<b>Limit warning</b>	Choose how the device should react when receiving a limit warning, such as a temperature excursion (None, Relay 1, Relay 2, or Relay 1 & relay 2)
<b>Dry contact alarm</b>	Choose how the device should react when receiving a limit alarm, such as a temperature excursion (None, Relay 1, Relay 2, or Relay 1 & relay 2)
<b>Trigger relays when power supply is unplugged</b>	Determines relay behavior if AC power is lost. You may click on <b>Show connections</b> to see images of the different wiring options (details on relay open and closed configuration are provided below in section 8.2.3 – <i>Terminal wiring on Dry Contact device, p. 127</i> ).
<b>Trigger alarm after</b> <input type="text" value="X"/>	<b>minutes without communication</b>  The system checks communication with all devices periodically. If the system fails to communicate with the device, and then fails again after "X" minutes that you specify, an alarm is triggered (such as an e-mail or text message).
<b>Trigger alarm after</b> <input type="text" value="X"/>	<b>minutes on battery mode</b>

## Infrastructure: Siren & Dry Contact alert devices

If the remote contact device switches from AC power to battery mode, an alarm is triggered after the number of minutes you specify here.

3. The new remote contact device is listed in the Infrastructure list as shown here:



The screenshot shows the 'Infrastructure (1)' interface. At the top right are icons for '+ Add', 'Download', and 'Refresh'. Below these are 'Filters' for 'Organizations' (set to 'All'), 'Types' (set to 'LoRaWAN ...'), and a 'Search' field. A toggle switch for 'Show disabled infrastructure' is set to 'No'. The table below has columns for 'Designation', 'Identifier', 'Organization', 'Version', and 'Last activity'. The data row shows 'Control Room Dry Contact' as the designation, 'LoRaWAN Dry Contact' as the sub-designation, 'E5110000041' as the identifier, and 'Los Angeles' as the organization.

Designation ↑↓	Identifier ↑↓	Organization	Version	Last activity ↑↓
Control Room Dry Contact LoRaWAN Dry Contact	E5110000041	Los Angeles		

Figure 104 – Dry contact alert relay shown in Infrastructure list

### 8.2.1 Testing your LoRaWAN Dry Contact device

We recommend that you test any newly installed alert devices to ensure proper operation in your context. To test the remote contact device:

1. Click on the LoRaWAN Dry Contact name in the list.
2. Click on **More** (⋮) → **Simulate an alarm** (🔔)

**Note:** this alarm is useful for testing the remote contact device itself, outside the context of any alert rules.

3. Confirm details in the window that opens:

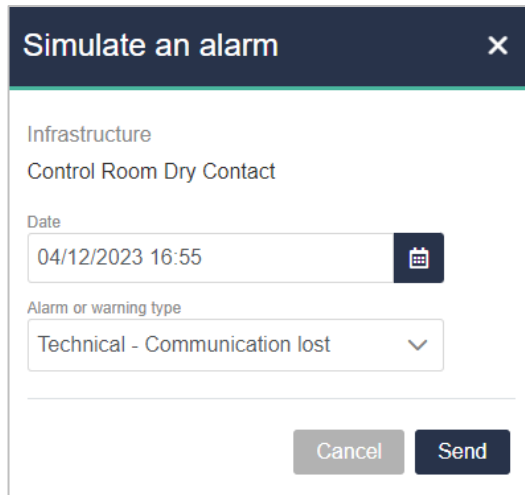


Figure 105 – Details for simulating an alarm

Use the pull-down list to choose one of the available alarm types for the siren: “Technical – Communication lost”, “Technical – Power lost”, or “Technical – Low Battery”.

4. Click on **Send** to launch the test, or on **Cancel** to return to the previous window without taking any action.

## 8.2.2 Other LoRaWAN Dry Contact device functions

Once you have added the remote contact device to your system, you may include it in alert rules to notify users in case of alarms. Other functions <sup>1</sup> are available by clicking on the device in the list, which opens details as shown here:

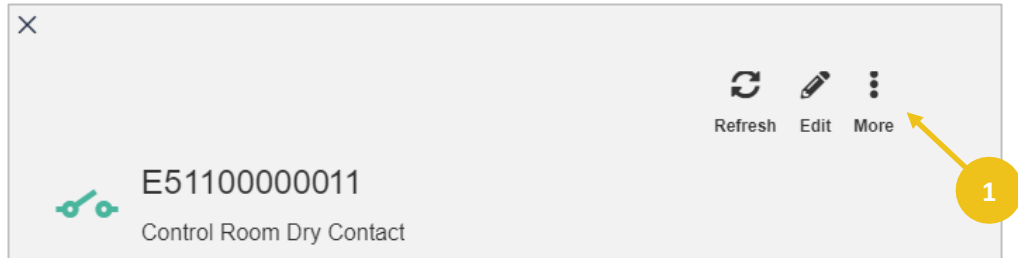









Figure 106 – Additional options for LoRaWAN Remote Contact management

<p>More </p>	<p> <b>Alarm history</b> Opens the Alarm list so you can see any alarms involving this device (a filter is applied to show "Infrastructure" with the device's serial number)</p> <p> <b>Simulate an alarm</b> You may use this function to simulate an alarm as described in the previous section.</p> <p> <b>Disable</b> Click to disable the device's functionality (in the Infrastructure list, a filter enables you to display or hide disabled infrastructure).</p> <p> <b>Remove</b> Click to remove the remote contact device from your system. The device is marked as "removed" in the Infrastructure list. If you wish to restore the same siren, you must create it again by entering the serial number.</p>
<p>Refresh </p>	<p>Refreshes the LoRaWAN Dry Contact information window.</p>
<p>Edit </p>	<p>Opens the Edit infrastructure window in which you may modify all the same details you entered when creating the device.</p>

### 8.2.3 Terminal wiring on Dry Contact device

The terminal is wired as follows (the images are shown in the OCEAView web application):



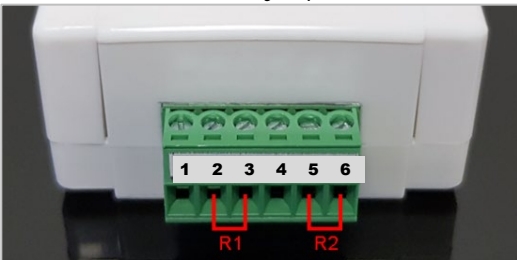
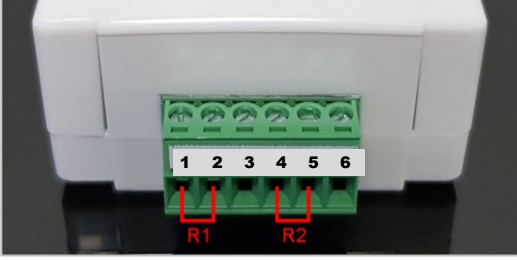


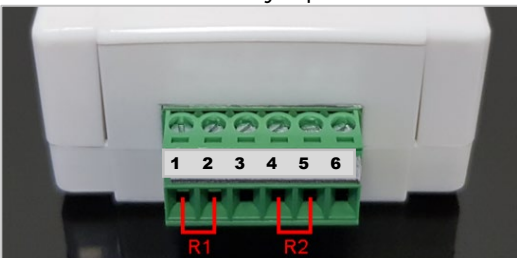
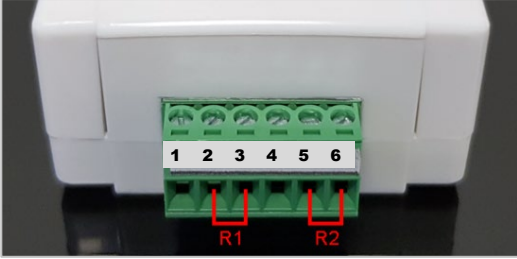
Blocks & states	Wiring
<p>Option in OCEAView: <input checked="" type="checkbox"/> Trigger relays when power supply is unplugged</p>  	<p>Normally open</p>  <p>Normally closed</p> 
<p>Option in OCEAView: <input type="checkbox"/> Trigger relays when power supply is unplugged</p>  	<p>Normally open</p>  <p>Normally closed</p> 

Figure 107 – Terminals for open and closed relays

Connect the wires of your external devices to the terminal poles as appropriate for your needs.



The two blocks (1-2-3 and 4-5-6) may be cabled differently from each other.

For example, with **Trigger relays when power supply is unplugged** selected, 1-2-3 may be cabled for "Normally open" and 4-5-6 may be cabled for "Normally closed".

---



## 9 Data loggers

The features described in this section are reserved for users with an Application Manager profile and users with application permission to manage data loggers.

### 9.1 Adding data loggers

#### 9.1.1 Adding a data logger manually

Follow these steps to add a supported Dickson data logger to the system manually:

1. In the main menu, click on **Data loggers** (  ) and then click on **Add** (  ) to enter all the details for a new data logger:

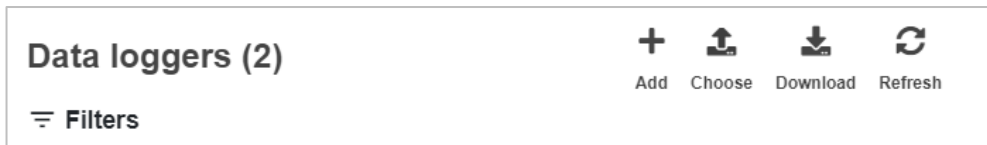


Figure 108 – Adding a new data logger

2. The **Create data logger** window opens as shown here:

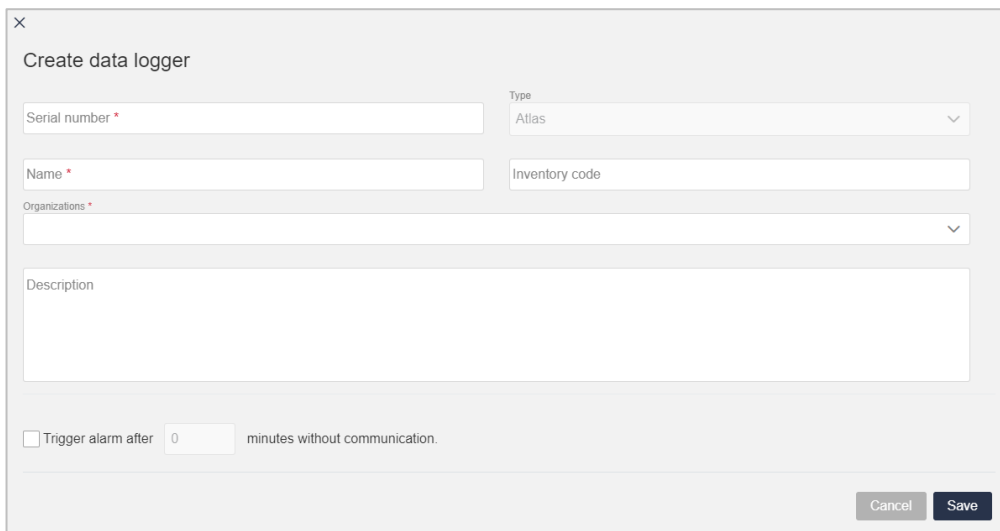
A screenshot of a 'Create data logger' window. The window has a title bar with a close button (X). The form contains several fields: 'Serial number \*' (text input), 'Name \*' (text input), 'Organizations \*' (dropdown menu), 'Type' (dropdown menu with 'Atlas' selected), 'Inventory code' (text input), and 'Description' (text area). At the bottom, there is a checkbox labeled 'Trigger alarm after' followed by a text input containing '0' and the text 'minutes without communication.'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 109 – Create data logger window before entering serial number

3. As you type in the data logger serial number, additional fields are displayed:

The screenshot shows a 'Create data logger' dialog box. It contains the following fields and options:

- Serial number \***: Text input field containing 'E61C00000124F3'.
- Type**: Dropdown menu showing 'X2'.
- Name \***: Text input field.
- Inventory code**: Text input field.
- Organizations \***: Dropdown menu.
- Description**: Large text area.
- Trigger alarm after** 0 minutes without communication.
- Trigger alarm after** 0 minutes in battery mode.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom right.

Figure 110 – Adding a new data logger

4. Fill in complete data logger details as required. Options are displayed according to the type of data logger. The fields marked with a red asterisk (\*) are required:

<b>Serial number</b>	Enter the serial number from the back of your data logger. If you enter an incorrect serial number, a red exclamation mark is shown in front of the corresponding field. Check the serial number and try again. Contact technical support if the problem persists.
<b>Type</b>	The device type is filled in automatically by the system based on the serial number you enter.
<b>Name</b>	Enter a name for the data logger. This name is used as the reference in lists throughout the application.
<b>Inventory code</b>	(Optional) You may enter an inventory code for the data logger for information purposes.
<b>Organizations</b>	Data loggers must be assigned to one or more nodes in your site organization. If you assign them to the root of your organization, all users can see them. If you assign them to a specific node, only the users assigned to that node will see them. This helps keep individual people’s dashboards relevant for their daily work. Site organization is described in section 6.3 – <i>Organizing your system with sites and departments</i> , p. 99.
<b>Description</b>	(Optional) You may enter a description of the data logger for information purposes.

**Trigger alarm after...**

These settings help ensure early notification in case of communication errors or power failure:

**[##] minutes without communication:** This option determines how long the system waits before triggering an alarm if the data logger is not communicating.



A general rule is to set this value to allow 3 communication failures before triggering an alarm. You may then control how to handle notification for communication problems as described in section 15.2 – *Alert rules and notifications, p. 238.*

**[##] minutes on battery mode:** this additional checkbox is displayed if the type of device you are creating also runs on battery power. The alarm is triggered after the specified number of minutes after the device switches to battery power (i.e., due to a power failure).

5. Click on **Save** to save the data logger in the database.
6. Before any communication takes place, the data logger is shown as follows, without any sensors:

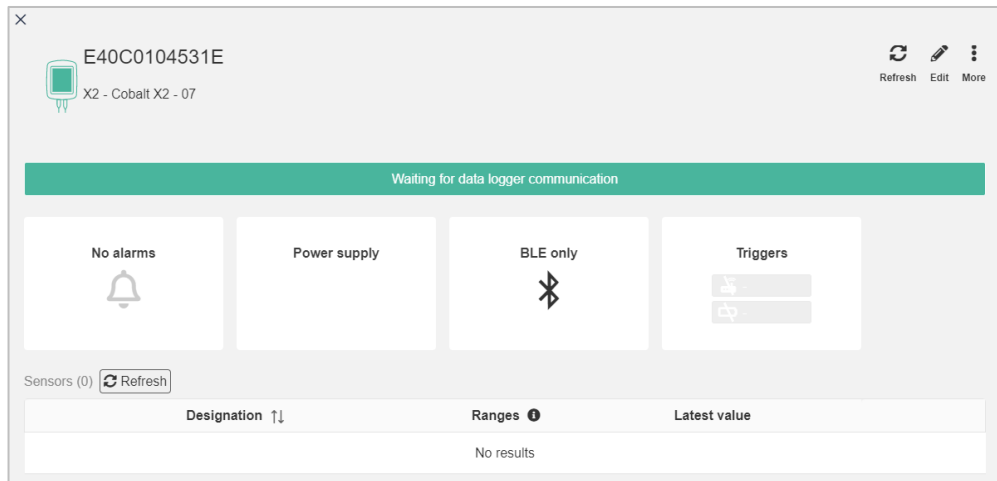




Figure 111 – Freshly added data logger

7. On your data logger, make sure that sensors are correctly connected and detected:
  - **Cobalt XS/X1/X2:** open the menu and select **Sensors** → **Refresh sensors**
  - **Cobalt L3 or ML3:** press the button on the front of the data logger and hold it for three seconds to refresh sensors.

8. Then, in OCEAView:

Click on the **Refresh sensors on data logger**  icon **1** to send an update request to the data logger. Wait a few moments, then press **Refresh** () update the screen.

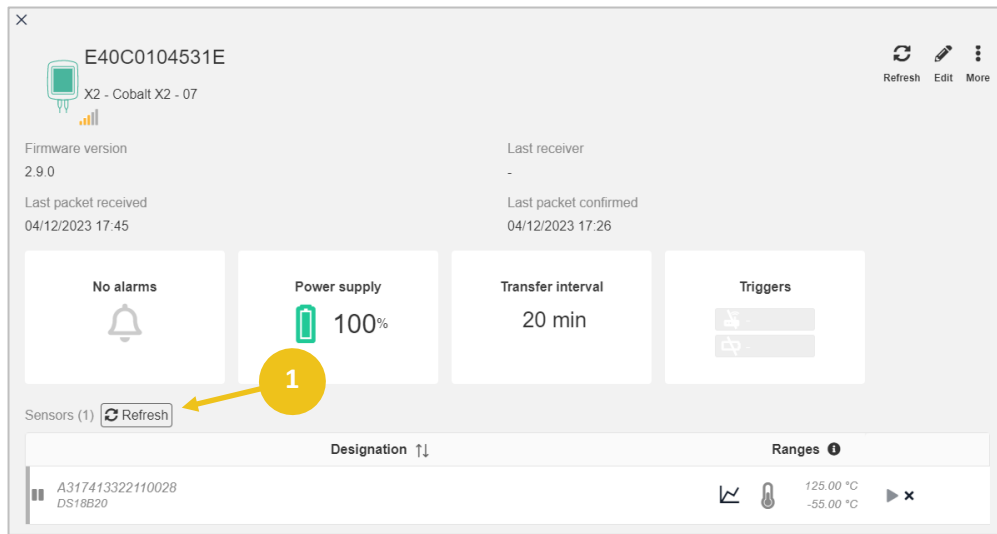


Figure 112 – Example of data logger information after refresh

### 9.1.2 Importing a batch of data loggers

If you would like to set up several data loggers at once, you may import a .TXT or .CSV text file with values separated by a semi-colon character (;). You must include at least the data logger serial number and name, as shown here:

```
SerialNumber;Name;
E40C0104###1;Incubator 1
E40C0104###2;Incubator 2
E40C0104###3;Incubator 3
E40C0104###4;Incubator 4
E40C0104###5;Incubator 5
E40C0104###6;Incubator 6
E40C0104###7;Incubator 7
E40C0104###8;Incubator 8
E40C0104###9;Incubator 9
E40C0104###10;Incubator 10
E40C0104###11;Incubator 11
```


Figure 113 – Sample .CSV import file with data logger serial numbers and names

## Data loggers

You may also include the inventory code and data logger description as shown here:

```
SerialNumber;Name;InventoryCode;Description;  
E40C0104576D;Incubator 1;123451;Lab data logger 1;  
E40C01045731;Incubator 2;123452;Lab data logger 2;  
E40C0104576F;Incubator 3;123453;Lab data logger 3;  
E40C0104577B;Incubator 4;123454;Lab data logger 4;  
E40C0104577A;Incubator 5;123455;Lab data logger 5;
```

Figure 114 – Sample .CSV file with additional information

1. Click on the  icon to import a batch file.
2. Browse to locate the .TXT or .CSV file on your computer.
3. Click on **Open** to import the list.

### 9.1.3 Adding Atlas and Emerald data loggers with OCEAVIEW Mobile

The OCEAVIEW web platform allows you to synchronize data from Dickson Atlas and Emerald data loggers using the OCEAVIEW Mobile application on a smartphone or tablet.

You may add your Atlas and Emerald data loggers either as described in the previous sections of this guide or add them directly using OCEAVIEW Mobile, which also allows you to associate the sensors with equipment already configured in the OCEAVIEW web application.

Data logging with Atlas and Emerald is controlled by the mobile application.

The OCEAVIEW Mobile companion app for the OCEAVIEW web solution is available for:

- iOS devices via the Apple App Store®
- Android devices via Google Play®

Visit the appropriate store for your device to install OCEAVIEW Mobile.

Please read the user guide provided with the application for more information about synchronizing Atlas and Emerald data loggers with the OCEAVIEW web application.



The OCEAVIEW web application only allows you to view Atlas and Emerald data logger information that is pushed by OCEAVIEW Mobile. The data loggers are managed entirely using the OCEAVIEW Mobile application.

---

## 9.2 Viewing the data logger list




All the data loggers you add to the system are shown in the **Data loggers** screen:

Type	Designation	Serial number	Version	Sensors	Last activity	Power Status
X2	Cobalt X2 - 07	E40C0104531E	2.9.0	1	PR:04/13/2023 11:14 PC:04/13/2023 09:44	Gray
X2	Lab B1	E40C0104571C	2.9.0	4	PR:04/13/2023 11:13 PC:04/13/2023 11:13	Green
X2	Storage Room	E40C0104589D	2.9.0	5	PR:04/13/2023 10:54 PC:04/13/2023 10:53	Red






Figure 115 – List of data loggers in OCEAView

This screen displays all data loggers in the system, with columns containing the information below.

Data logger status is indicated by color coding on left-hand edge of the table (this does not indicate alarms related to sensor readings, just the data logger itself):

 X2	Gray indicates that the data logger is not yet configured.
 X2	Green indicates that the data logger is configured and operating correctly.
 X2	Red indicates a technical issue with the data logger, such as a sensor failure, low battery, or communication problem

You may click on the up/down arrows (↑↓) in a column header to sort the list by that column and apply ascending or descending order. The column used for sorting is indicated by ↓≡ or ↑≡.

<b>Type</b>	Type of data logger
<b>Designation</b>	Friendly name for the data logger. You may click on the graph icon (  ) to see a data graph and other sensor information.
<b>Serial number</b>	Data logger serial number
<b>Version</b>	Firmware version running on data logger
<b>Sensors</b>	Number of sensors connected to the data logger
<b>Last activity</b>	Date and time of last communication with the data logger
	Power status: plugged into AC adapter (  ), or battery level (  or  ).



The number of sensors that you may use in your system is determined by your license. Your system may be configured to contain a total number of sensors that is greater than that which the license allows, but you can only use the allowed number of sensors simultaneously.

### 9.3 Viewing data logger details

Regardless of your OCEAVIEW user level, you may always check the data for the data loggers you are authorized to view.

To view the details for a given data logger:



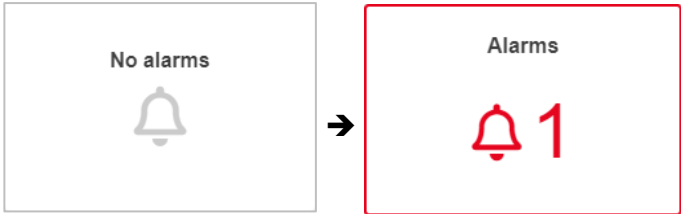








1. Click on **Data loggers** (  ) in the main menu.
2. Select a data logger.
3. The data logger details are shown on the right-hand side of the screen, with several sections:

Figure 116 – Data logger details

Description	
<p>1</p>	<p>Data logger's serial number, name, and inventory code (if present). The LoRaWAN wireless signal quality is shown next to the data logger icon.</p> 
<p>2</p>	<p>Alarm counter indicating data logger status (i.e., no technical errors, low battery, or other aspects not related to sensor readings). In case there is an alarm concerning the data logger itself, the icon changes color and shows the number of alarms, for example:</p> <div style="text-align: center;">  </div> <p><i>Figure 117 – Alarm counter in data logger details</i></p> <p>Hover over the alarm counter with your mouse to view alarm details.</p> <p>Click on the alarm counter to get more information, acknowledge one or more alarms, or generate an alarm report. You will be directed to the alarm management screen (see <i>chapter 15 – Alarms &amp; alerts, p. 227</i>).</p>
<p>3</p>	<p>Indicator showing the power source being used and estimated remaining battery level.</p>
<p>4</p>	<p>For LoRaWAN communications, the <b>Transfer interval</b> indicates the frequency with which data is transmitted by the data logger to the OCEAView system. That information is not relevant when the data logger is used for Bluetooth communications, in which case <b>BLE only</b> is displayed instead:</p> <div style="text-align: center;">  </div>
<p>5</p>	<p>Alarm trigger rules defined when adding or editing the data logger. Hover over the alarm counter with your mouse to view alarm details.</p>
<p>6</p>	<p>All the sensors associated with the data logger.</p>

	<p>The active icon (  ) indicates sensors with data logging in progress.</p> <p>Sensors not yet programmed are greyed out, as indicated by the inactive icon (  ).</p>
7	<p>You may click on <b>Readings</b> (  ) to view a graph of sensor readings over time (measurements and associated events...) or download the report in PDF, CSV, or Excel format (see section 13 – Viewing sensor data, page 186).</p>
8	<p>Sensor operating range.</p>
9	<p>Icons to start (  ), stop (  ) or edit (  ) data logging, or remove a sensor from the data logger.</p>
10	<p>When datalogging is running, you may click on the right arrow (  ) to unfold a complete summary of the data logging configuration:</p> <div data-bbox="529 878 1375 1070" style="border: 1px solid #ccc; padding: 5px;"> <p>1A5544332211003B Freezer A1 SmartDS   Freezer A1</p> <p style="text-align: right;">125.00 °C -55.00 °C</p> <hr/> <p>Name: <b>Freezer A1</b>      Level 1: <span style="color: blue;">↓</span> 3.00 °C    <span style="color: orange;">↑</span> 7.00 °C      Start: 04/13/2023 14:18:33      Use drift/uncertainty: <b>Yes</b></p> <hr/> <p>Status: <b>Running</b>      Level 2: <span style="color: red;">↓</span> 2.00 °C    <span style="color: red;">↑</span> 8.00 °C      End: -      Allow ACK from data logger: <b>Yes</b></p> <hr/> <p>Start mode: <b>Immediate</b>      Reading interval: 1 min      Use buzzer: <b>Yes</b></p> </div>

## 9.4 Data logger actions

You may use the options on the data logger details screen to manage data loggers.

1. Click on **Data loggers** (📱) in the main menu and select a data logger.
2. Click on **More** (⋮) <sup>1</sup> in the upper right-hand corner to access available options:



Figure 118 – Data logger options menu

<b>Alarm history</b>	Opens the alarm page for the data logger).
<b>Simulate an alarm</b>	Allows you to simulate the occurrence of an alarm on this data logger for testing purposes. The simulation generates a Technical alarm (your choice of Communication lost, Data logger mismatch, Low Battery, Power lost), listed in the Audit Trail as an “Alarm simulation”.
<b>Communication settings</b>	This menu provides technical information regarding data logger communications. In case of problems, Technical Support may ask you for this information.
<b>Disable</b>	Deactivates data logger and stops data logging.
<b>Remove</b>	Enables you to completely remove this data logger from your system and stops data logging. You may need to do this in the event of a data logger swap or hardware problem. If you choose this option, you must enter your password to confirm the operation (or press <b>Send</b> if you are logged in with SSO).





You may remove a data logger if data logging is active, if necessary. Only do this if there is a problem with the data logger and you cannot stop data logging in OCEAVIEW. The action is tracked in the Audit Trail.

3. Click on **Save** to keep your changes, or on **Cancel** to return to the previous screen without saving changes.

## 9.5 Editing data logger details (transfer/retransfer interval)

Follow these steps if you need to change the information or default values for your data logger:

1. Click on **Data loggers** (  ) in the main menu and select a data logger.
2. Click on **Edit** (  ) icon. This action opens a window nearly identical to that described in section 9.1 – *Adding data loggers, p. 129*). **Note:** You may not edit the Serial number or data logger Type fields.
3. When editing a data logger, there is some information present that was not displayed earlier:

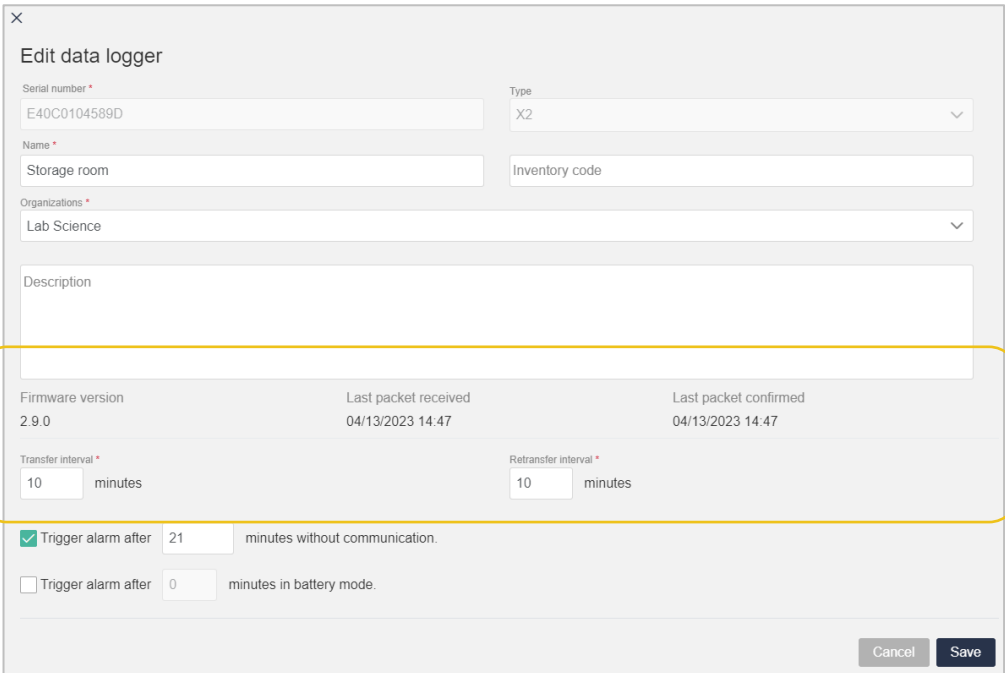


Figure 119 – Editing data logger details

**Firmware version** Indicates the data logger firmware version number (not editable).

### Last packet received

This indicates the last time the server received communication from the data logger (“uplink”). The server triggers an alarm if it does not receive communication from the data logger within the configured number of minutes allowed without communication (described below).

### Last packet confirmed

This indicates the last time the data logger confirmed communication from the server (“downlink”). The server triggers an alarm if data logging is running and

the data logger does not receive acknowledgment from the server within a period (calculated automatically) equal to eight times the number of minutes allowed without communication.

### Transfer interval

For LoRaWAN communications, you may specify how often the data logger should transmit its data via the LoRaWAN network. The minimum period is 10 minutes for all Cobalt **XS/X1/X2**, Cobalt L3, and Cobalt ML3 data loggers. You may change this value even while data logging is running.



Alarms are always sent in real-time. The data logger does not wait for the programmed transfer interval to send alarms.

---

### Retransfer interval

For LoRaWAN communications, you may specify how long the data logger should wait to try again in case data was not transferred successfully. The minimum duration is 5 minutes for all Cobalt **XS/X1/X2**, Cobalt L3, and Cobalt ML3 data loggers. You may change this value even while data logging is running.

### Trigger alarm after...

These settings help ensure early notification in case of communication errors or power failure:

**[##] minutes without communication:** This option sets the uplink delay time, that is, the number of minutes that the server can wait before triggering an alarm that it has not received communication from the data logger.

---

As of OCEAView 1.11, we recommend setting the number of minutes to:

**2 x (transfer interval + 1 minute)**



For example, with a transfer interval of 20 minutes, we recommend setting this value to 42 minutes.

You may then control how people are notified for communication problems as described in section 15.2 – *Alert rules and notifications*, p. 238.

---

**[##] minutes on battery mode:** this additional checkbox is displayed if the type of device you are

creating also runs on battery power. The alarm is triggered after the specified number of minutes after the device switches to battery power (i.e., due to a power failure).

4. Click on **Save** to keep your changes, or on **Cancel** to return to the previous screen without saving changes.

## 10 Sensors

Sensors that are connected to supported data loggers are added to the OCEAView web application automatically.

For OCEAView to recognize the sensor(s) connected to a data logger:

- **Cobalt XS/X1/X2:** open the menu and select **Sensors** → **Refresh sensors**
- **Cobalt L3 or ML3:** Press the button on the front of the data logger and hold it for three seconds to refresh sensors.

Once detected by the system, these sensors are shown in the sensor management window. From the sensor management window, you may:

- Access detailed information about the sensor
- Filter the sensor list according to various criteria
- Display readings in a graph, along with other information about the selected sensor
- Manage calibration parameters

## 10.1 Sensor summary list

All the sensors connected to data loggers in your system are listed in the **Sensors** screen (  ):

















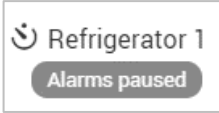
Type	Designation	Data logging	Equipment	Calibration	Latest value
	1A5544332211003B SmartDS   Storage Room	 Freezer A1	Freezer A1 Door 15 (2nd floor)		04/13/2023 15:06:33 5.49 °C
	863412000001741_C SmartCO2   Storage Room	 Incubator 3rd	Incubator 3rd floor Incubator		04/13/2023 14:26:31 5.00 %
	863412000001741_T SmartCO2   Storage Room	 Incubator 1	Incubator 1 Incubator		04/13/2023 15:04:12 5.56 °C
	863412000001741_H SmartCO2   Storage Room		-		-
	E40C0104589D Internal Sensor   Storage Room	 Amb. storage	Freezer A1 Door 15 (2nd floor)		04/13/2023 14:18:37 Normal

Figure 120 – Sensor list in OCEAView

This screen displays the following information for all the sensors in your system:

- Type** Visual indication of the sensor type
- Designation** Sensor serial number, sensor type, and associated data logger
- Data logging** Data logging status: running (  ) or idle (  ). Move your mouse over the icon to see data logging settings.  
  
If alarms and warnings are paused (Cobalt X1/X2 only), the status is displayed like this:  
  

- Equipment** The equipment associated with the sensor.
- Calibration** Hover your mouse over the field to see calibration parameters or click to open the calibration management window.
- Latest value** Date and value of the most recently recorded reading.

## 10.2 Individual sensor details

Regardless of your account permissions in OCEAView, you may always check the data for sensors you are authorized to view.

To view detailed information about a sensor:

1. In the main menu, click on **Sensors** (🌡️).
2. Click on the desired sensor.
3. The sensor details are shown on the right-hand side of the screen, with several sections:

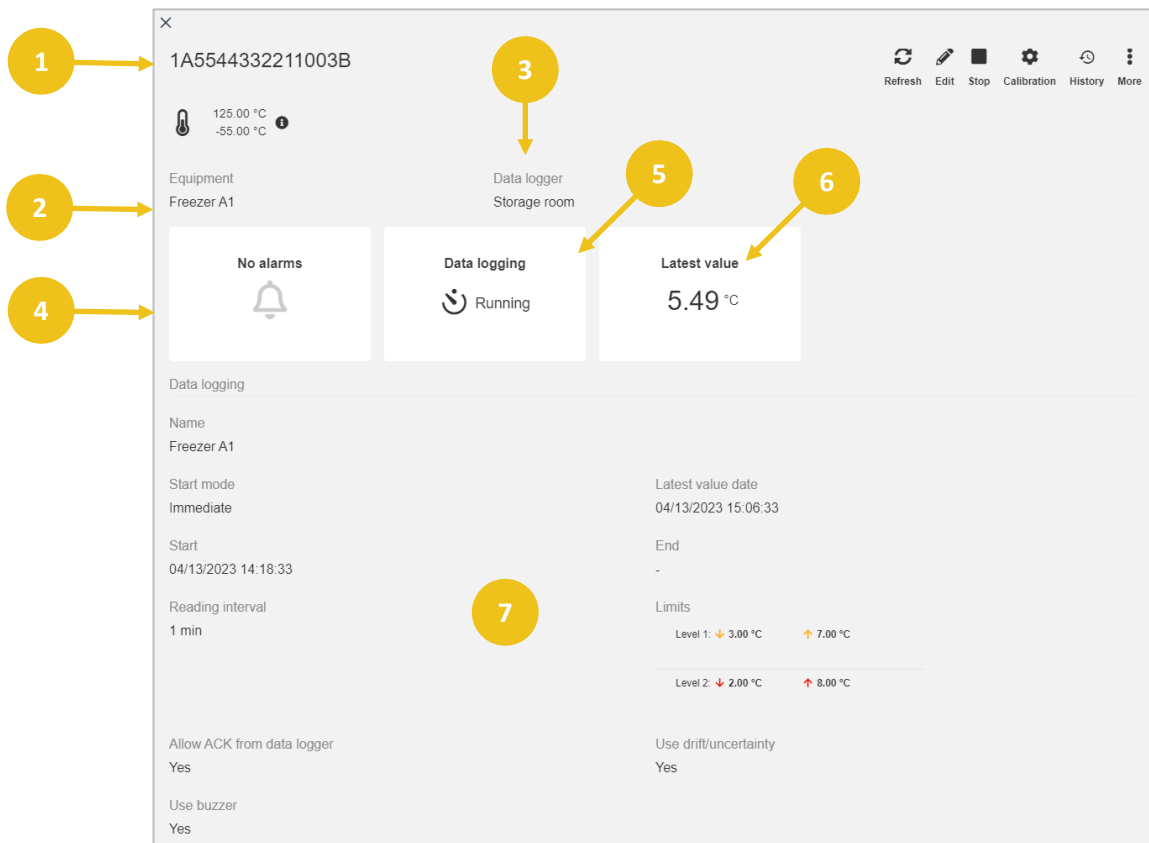
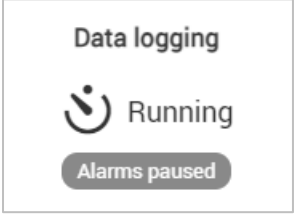


Figure 121 – Sensor details

Description	
1	Sensor serial number and type.
2	Name of the equipment with which the sensor is associated.
3	Name of the data logger on which the sensor is physically attached.

4	Alarm indicator (excursions with respect to programmed limits). Click on this indicator or on <b>History</b> (🕒) for detailed information or to acknowledge an alarm.
5	Data logging status for this sensor: <b>Running</b> or <b>Idle</b> If alarms and warnings are paused (Cobalt X1/X2 only), the status is displayed like this:  A screenshot of a data logging status display. It shows the text "Data logging" at the top, followed by a circular icon with a play symbol and the word "Running". Below that is a grey button with the text "Alarms paused".
6	Last recorded reading.
7	Data logging configuration parameters.

## 10.3 Filtering the sensor list display

When looking at the sensor list, you may wish to filter the display to see specific sensors or sensors that meet certain criteria.

To filter the list:

1. Click on **Filters** ( 1 ) to unfold the options, and then select the filter(s) you would like to apply ( 2 ):

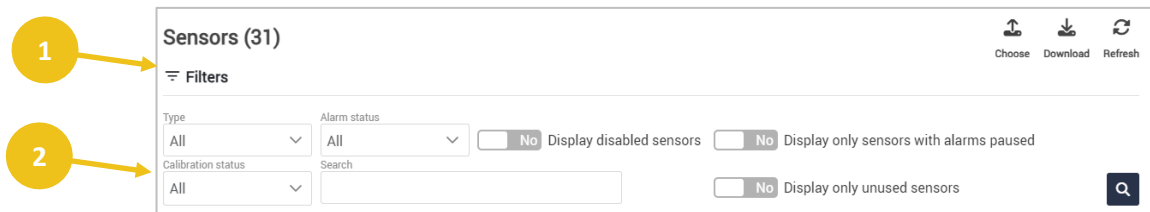
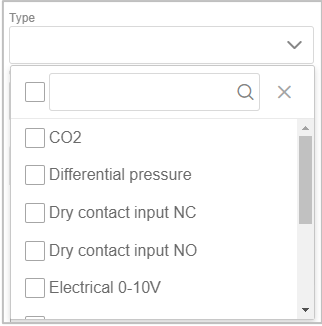




Figure 122 – Filtering the sensor list

The available filters are as follows:

Filter option	Description
<b>Type</b>	By default, this is set to <b>All</b> , to display all sensors. Use the pull-down menu to select one or more specific types of sensors (or type the first letters of the sensor type in the search field at the top of the list): 
<b>Calibration status</b>	By default, this is set to <b>All</b> , to display all sensors regardless of their calibration status. Select <b>Overdue</b> to see those sensors whose calibrations have expired.
<b>Alarm status</b>	By default, this is set to <b>All</b> , to display all sensors regardless of their alarm status. Select <b>No alarms</b> to show sensors without alarms, or <b>Ongoing</b> to see sensors that currently are in an alarm state.
<b>Search</b>	You may enter any text here, such as all or part of a sensor serial number in this field.

<b>Display disabled sensors</b>	Set this option to <b>Yes</b> to see all sensors. Set this option to <b>No</b> to exclude those sensors that are disabled.
<b>Display only sensors with alarms paused</b>	Set this option to <b>Yes</b> if you want to see only those sensors on Cobalt X1/X2 data loggers for which alarms are paused. Set this option to <b>No</b> to see all sensors.
<b>Display only unused sensors</b>	Set this option to <b>Yes</b> to see all sensors. Set this option to <b>No</b> to see only those sensors that are not currently being used for data logging.

2. Apply filters by clicking on the magnifying glass (  ).

You may clear all applied filters by clicking on **Refresh** (  ). Filters are also reset to their default settings when you refresh the page (pressing the F5 key in most browsers) or when you go to another page in the application.

## 10.4 Calibration parameters

It is important to calibrate the sensors on your Dickson data loggers to fine-tune reading accuracy. The calibration procedure is often handled by Dickson's in-house metrology laboratory, which determines precise correction coefficients. OCEAView users are also free to manage calibration according to their own standard operating procedures.



Calibration parameters, also referred to as "correction coefficients", are stored directly in Dickson Smart-Sensors. This means that all sensor readings are adjusted for maximum accuracy. You may edit calibration parameters as necessary. However, you may only use the OCEAView Mobile application to change calibration parameters on remote (Bluetooth wireless) sensors.

---

### 10.4.1 Editing parameters for calibrated sensors




OCEAView allows you to correct the parameters and calibration information of your data loggers from the information provided sensor calibration certificates.




Calibration parameters may only be corrected if data logging is not currently running on the sensor(s) in question. If necessary, you must first stop data logging before you can change calibration parameters.

---

#### To update calibration information:

1. Login to OCEAView using an Application manager account, or with a user account whose role includes "Manage metrology parameters" access (as described in section 5.6 – *Adding user roles*, p. 85).
2. In the main menu, click on **Sensors** (  ) and click on the sensor you want to update.
3. If calibration information has already been provided, you may click on **Calibration** (  ) → **Edit** (  ).

Otherwise, click on **Add** (  ) to enter and save new information.

The screenshot shows a 'Create calibration parameters' dialog box with the following fields and values:

- Sensor:** Serial number: 1A57443322110028, Unit: °C
- Parameters (°C):**
  - Coefficient A: 1.0000
  - Coefficient B: 0.000
  - Coefficient C: 0.000000
  - Drift: 0.00
  - Uncertainty: 0.00
- Certificate:**
  - Laboratory: Unknown (dropdown menu)
  - Identifier: (empty text field)
  - Date: 04/13/2023 (calendar icon)


Buttons for 'Cancel' and 'Save' are located at the bottom right of the dialog.

Figure 123 – Creating or adding sensor calibration parameters

- Coefficient A, B, C** The A, B, and C correction coefficients are used to improve the accuracy of sensor readings mathematically. It is possible to only use A and B when calibrating sensors, in which case C is set to 0. The C coefficient comes into play when you have 3 or more points, where you can either use A and B for a linear calculation ( $y=Ax+B$ ), or A, B, and C to determine coefficients based on a curve ( $y=Cx^2 + Ax+B$ ). Enter the correction coefficients in the A, B, and C fields. To ensure the accuracy of readings, it is extremely important to enter only valid parameters in these fields.
- Drift** This value represents reading accuracy loss over time. Values may drift lower by a few hundredths per year, which can impact programmed data logging limits. Enter the **Drift** value from your calibration certificate.
- Uncertainty** Uncertainty is the loss of calibration accuracy with respect to the reference sensor, thus having an impact on alarm generation and notification. Enter the **Uncertainty** value provided on calibration certificate.
- Laboratory** Using the drop-down list, select the calibration laboratory that issued the calibration certificate.
- Identifier** Enter reference information, such as a certificate number or lab technician's name.
- Date** Click on the calendar to choose the date on which the sensor was calibrated. The current date is displayed by default.
- Note:** if calibration certificate information had been entered previously for this sensor, the date you enter here must not be earlier than that of the previous certificate.

### 10.4.2 Calibration reminder frequency

Once you have added calibration information, you may choose to receive notification as a reminder to recalibrate the sensor by a given date.

In the **Calibration** screen, click on **Edit** (  ) and then enter the number of months after the certificate date at which the system will remind you to recalibrate the sensor:

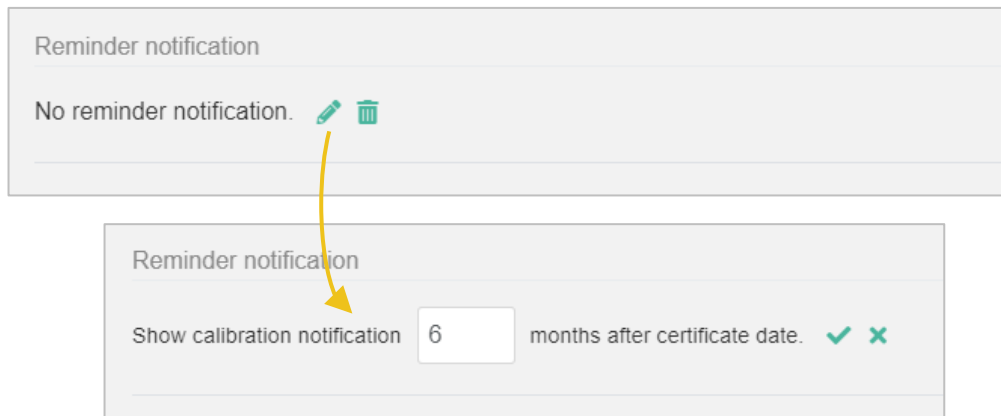





Figure 124 – Sensor calibration reminder

Click on **Save** (  ) to update sensor information, on **Cancel** (  ) to undo any changes you may have made, or on **Delete** (  ) to remove notification.



Calibration is not used for dry contact input sensors (on Cobalt X1/X2 data loggers), as the only two possible sensor values are "open" or "closed", as described in the next section.

### 10.4.3 Importing CSV file with calibration information

You may import calibration information from a CSV format text file. This feature offers a practical way to update batches of sensors without having to manually edit each one.



You must be logged in with an Application Manager account, or as a user whose role includes "Manage metrology parameters".

Data logging must not be currently using the sensor(s) to be updated.

#### Sample text file

Here is text from a sample CSV file with the required header line and details for one sensor:

```
ProbeSerialNumber;Number;CalibrationDate;CertificateId;CoefA;CoefB;CoefC;Drift;Uncertainty
8634120000001741;3;2020-12-15;John;1.2;0.1;0;0.25;0.3
```

Field names must be separated by a semi-colon ( ; ). All the fields below must be present:

<b>ProbeSerialNumber</b>	The serial number of the sensor to be updated. If a probe has several sensors, its serial number is displayed in OCEAVIEW with a suffix of "_T", "_H", or "_C" (e.g., 8634120000001741_T).  Do not include the suffix in the CSV file.
<b>Number</b>	Identifies the specific sensor with these numbers, notably for multi-sensor probes:  <b>Single</b> sensor probes: 1  <b>Dual</b> temperature + relative humidity probes:  T° = 1      RH% = 2  <b>Triple</b> CO <sub>2</sub> + temperature + relative humidity probes:  CO <sub>2</sub> = 1    T° = 2    RH% = 3
<b>CalibrationDate</b>	The date the calibration was performed. This date must be more recent than the previous calibration date.  The date format is YYYY-MM-DD
<b>CertificateId</b>	An identifier to indicate the document (certificate) containing calibration information.
<b>CoefA</b>	Correction coefficient A, using a period ( . ) as the decimal separator.

## Sensors

<b>CoefB</b>	Correction coefficient B, using a period ( . ) as the decimal separator.
<b>CoefC</b>	Correction coefficient C, using a period ( . ) as the decimal separator.
<b>Drift</b>	Drift value
<b>Uncertainty</b>	Uncertainty value

### To import a CSV file with sensor calibration parameters:

1. Login to OCEAView using an Application manager account, or as with a user account whose role includes "Manage metrology parameters" access (as described in section 5.6 – *Adding user roles*, p. 85).
2. In the main menu, click on **Sensors** (🌡️) and click on **Choose** (📁) <sup>1</sup>.

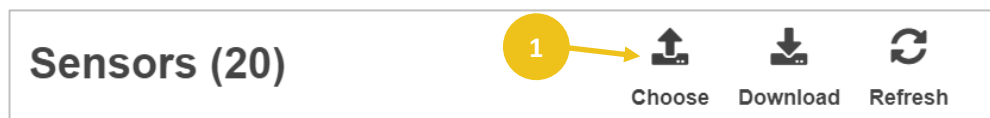

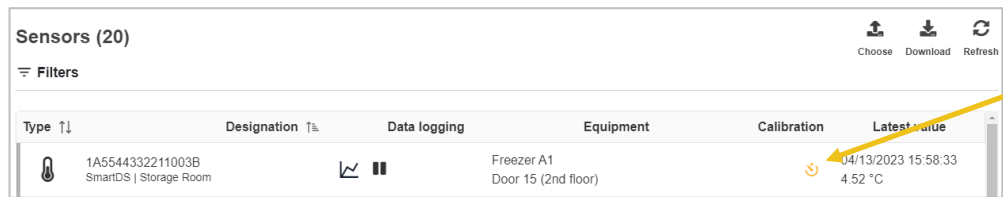


Figure 125 – Click to import a CSV file with sensor calibration parameters

3. Browse to locate the CSV file on your computer.
4. Enter your password (or press **Send** if you are logged in with SSO) to import the file.

- Confirmation is displayed on the screen if no errors are encountered. Each updated sensor has a temporary icon  in the **Calibration** column to indicate that calibration is pending.



The screenshot shows a table titled "Sensors (20)" with columns: Type, Designation, Data logging, Equipment, Calibration, and Latest value. A yellow arrow points to a clock icon in the Calibration column of the first row.





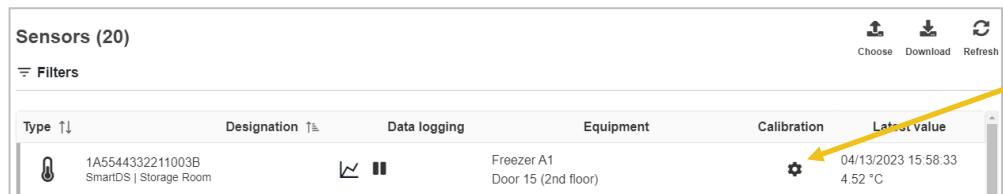
Type	Designation	Data logging	Equipment	Calibration	Latest value
	1A5544332211003B SmartDS   Storage Room		Freezer A1 Door 15 (2nd floor)		04/13/2023 15:58:33 4.52 °C

Figure 126 – After import but before synchronization with data logger

- Calibration parameters are updated automatically on the data logger upon the next schedule data transfer interval. For the update to be taken into account right away, you may use the **Synchronize** function on the data logger. The normal calibration icon  is displayed in the Calibration column once the update is complete.



The screenshot shows the same table as Figure 126, but the gear icon in the Calibration column indicates that synchronization is complete. A yellow arrow points to the gear icon.




Type	Designation	Data logging	Equipment	Calibration	Latest value
	1A5544332211003B SmartDS   Storage Room		Freezer A1 Door 15 (2nd floor)		04/13/2023 15:58:33 4.52 °C

Figure 127 – After synchronization with data logger

#### 10.4.4 Error messages when importing a calibration CSV file

Errors may occur when you import a CSV file with calibration parameters. In that case, each error is indicated with the corresponding line number in the CSV file, as shown here:

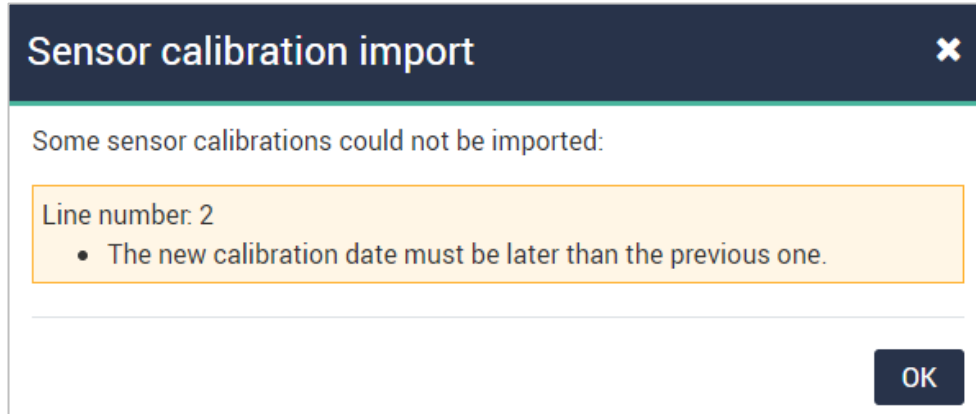


Figure 128 – Example of error while importing CSV file

Possible errors are as follows:

Message	Description
Not allowed. Sensor is not plugged into a data logger.	The sensor must be physically plugged into a connected data logger in your system.
Not allowed. Sensor is currently being used for data logging.	Calibration parameters may not be loaded for a sensor that is currently being used for data logging.
Action not allowed for this probe type.	The probe does not support correction parameter management from OCEAView.
Sensor not found.	The sensor is not present in your OCEAView system.
The new calibration date must be later than the previous date.	The calibration date provided in the CSV file cannot be earlier or the same as the previous date.
Invalid file content	The fields and/or data in the CSV file do not respect the required format.
Not allowed. Sensor has been recycled.	The sensor has been removed from operation and is no longer valid.
Action not allowed for this data logger firmware version.	The data logger firmware does not support correction parameter management from OCEAView.

### 10.4.5 Exporting sensor information

From the sensor list you may export detailed sensor information, including calibration parameters, in CSV file format with values separated by a semi-colon (;).

To export sensor details:

1. In the main menu, click on **Sensors** (🌡️).
2. Click on **Download** (📄) in the upper right-hand corner 1.



Figure 129 – Creating a CSV file with complete sensor details

3. Depending on your browser and/or download settings, you may need to choose the desired download location for the CSV file on your computer. By default, the file name is presented as follows:  
`Sensors - 01-12-2021 1235 PM.csv`
4. Click on **Save** to download the file (if necessary).

## 10.5 Using the Cobalt X1/X2 dry contact input sensor

The Dickson dry contact input sensor is used with Cobalt X1/X2 data loggers to provide fast dry contact loop detection for a variety of situations. Typical uses include door open-close monitoring systems and specialized equipment such as ultra-low-temperature freezers that offer a dry contact output terminal.

The dry contact input sensor is different from sensors that monitor ranges of different readings, such as temperature or humidity. The dry contact sensor simply shows the open-close status of a low-current loop, with the data logger configured to detect either a “normally closed” or “normally open” state to correspond with the device or equipment to be monitored.



For more details on dry contact sensor usage, cabling, and data logger configuration, please see the Cobalt X1/X2 User Guide.

In the **Sensors**, **Data loggers**, and **Equipment** menus, dry contact sensors are shown as follows (with slight variations depending on the context):








Type ↑↓	Designation ↑≡	Data logging
	E40C0104589D Internal Sensor	 
	E40C0104589D Internal Sensor   Storage R...	 

Figure 130 – Dry contact sensor display



For each physical dry contact sensor, you will see two sensors listed. This is done to ensure traceability in case you use both configuration options. The sensor with the  icon and “Internal Sensor” label corresponds to the current setting on the data logger. Data logging is described in detail in chapter 12 – *Data logging*, p. 170.

Configuration is indicated by the following icons (  ):



The electric current loop is configured for “normally closed”.



The electrical current loop is configured for “normally open”.

## 10.6 Using Dickson 0-4 mA / 0-5 V / 0-10 V Smart-Sensors

The Dickson sensor for 4-20 mA (*intensity*) and 0-5 V / 0-10 V (*voltage*), for Cobalt X1/X2 data loggers, is physically the same product. You will therefore see both sensors listed in OCEAView and you must choose the right one for your needs.

- The 4-20 mA sensor is indicated by “\_I” in the serial number.
- The 0-5 V / 0-10 V sensor is indicated by “\_U”.

Type ↑↓	Designation ↑≡	Data logging	Equipment	Calibration
	8135120000001441_I 4-20mA   Cobalt X - Electrical		-	
	8135120000001441_U 0-5V/0-10V   Cobalt X - Electrical		-	

Figure 131 – Selecting the 4-20 mA / 0-5 V / 0-10 V Smart-Sensor

### 10.6.1 Mapping values for meaningful readings

For sensor readings to be relevant in your context, you must map the *low values* (0 V or 4 mA) and *high values* (10 V or 20 mA) to match the limit values produced by your connected device. For example, on a 4-20 mA device, the low 4 value could correspond to a CO<sub>2</sub> level of 0% and the high 20 mA value could correspond to 10% CO<sub>2</sub>. In that case, you would map 4 to 0, and 20 to 10 in OCEAView. You may use other units to meet your needs.

To map values:

1. Click on **Sensors** () in the left-hand menu.
2. Select the sensor you wish to modify from the sensor list.
3. Click on **Calibration** () → **Edit** ()
4. Edit the values in the **Range** zone to meet your needs:

**Low** the lower value output by your device

**High** The higher value output by your device

**Unit** The measurement unit you would like to display in OCEAView

Range		
Low (4 mA)	High (20 mA)	Unit
<input type="text" value="0.00"/>	<input type="text" value="10.00"/>	<input type="text" value="CO²"/>

Figure 132 – Mapping 4-20 mA / 0-10 V values

5. Click on **Save** to save your changes, or on **Cancel** to close this window without saving changes.

The unit you specify here is shown in the OCEAView web application as well as on the data logger.





The mapping from 4 to 20 mA or 0 to 10 V is strictly linear.

The 0-10 V sensor is also used for 0-5 V output devices. Simply adjust your Low and High values accordingly.

---



## 10.7 Simulating a sensor alarm for testing

You may trigger a limit alarm on a sensor for testing purposes, notably to ensure that related alert rules and user contact work properly. To test a sensor alarm:

1. Login to OCEAView as an Application manager.
2. In the main menu, click on **Sensors** (  ) for a list of the sensors in your system.
3. Click on the sensor you want to test.
4. Click on **More** (  ) and select **Simulate an alarm** from the drop-down menu. You will then be able to see the alarm in the Alarm list and Audit trail (indicated as "Simulation" in both places). Any related alert rules for the sensor are triggered, such as e-mail or telephone alerts.

## 10.8 Removing a sensor

You may remove sensors from the system, for example if they are no longer used or if they have been replaced on the data logger. To remove a sensor:

1. Login to OCEAView as an Application manager.
2. In the main menu, click on **Sensors** (  ) for a list of the sensors in your system.
3. Click on the sensor you want to remove.
4. Click on **More** (  ) and select **Remove** from the drop-down menu. To remove a sensor, data logging must not be running. If you choose this option, you must enter your password (or press **Send** if you are logged in with SSO) to confirm the operation.





Supported data loggers update sensor information in OCEAView automatically based on connected sensor(s). When you plug in a new sensor (or even plug the same one back in if it had been removed by mistake), the sensor(s) will appear again in the OCEAView web application.

---

## 10.9 Disabling /enabling a sensor

You may disable a sensor so that it cannot be used for data logging, or you can enable a sensor that has been disabled. To do this:

1. Login to OCEAView as an Application manager.
2. In the main menu, click on **Sensors** (  ) for a list of the sensors in your system.
3. Click on the sensor you want to disable or enable.
4. Click on **More** (  ) and select **Disable** (or **Enable**) from the drop-down menu. To disable a sensor, data logging must not be running.



Disabled sensors are no longer shown in the sensor list. To enable a disabled sensor, use the **Filter** option in the sensor list and select Display disabled sensors. You may then choose to enable it as described above.

---

## 11 Equipment



This chapter describes how to manage equipment in your OCEAView system and how to assign sensors to that equipment.

It is important to remember the underlying notion in OCEAView that your goal is to monitor equipment, rather than just activate data logging using sensors. With that understanding, you must define your equipment and then assign sensors to monitor it.

As mentioned earlier, the term “equipment” in OCEAView refers to the temperature-controlled chambers, cabinets, refrigerators, tanks, enclosures, and other spaces you may choose to monitor with your data loggers.

### 11.1 Adding equipment

To add equipment:

1. Click on **Equipment** (  ) in the left-hand menu to open the Equipment window. There are two options for creating new equipment:
2. Click on **Add** (  ) to enter details.

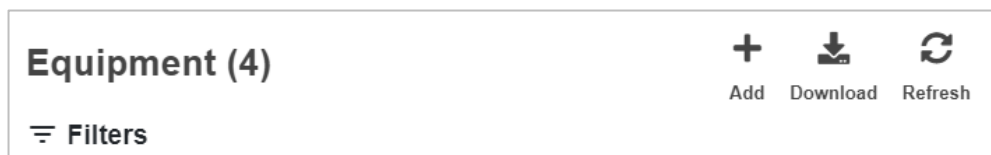


Figure 133 – Equipment management window

- The **Create equipment** window opens as shown here:

Figure 134 – Adding new equipment

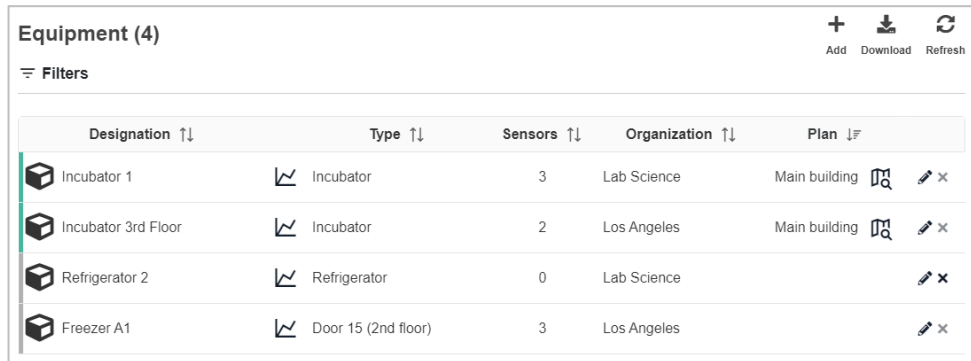
- Fill in complete equipment details. The fields marked with a red asterisk (\*) are required:

<b>Name</b>	Enter a name for your equipment. This name is used in all lists.
<b>Inventory code</b>	(Optional) You may enter an inventory code for the equipment for information purposes.
<b>Type</b>	Enter a type of equipment in the field.
<b>Icon</b>	Click on the icon and select the most appropriate symbol to visually represent the equipment.
<b>Organization</b>	Equipment must be assigned to either the entire (root) organization or to individual sites or departments. Equipment can only be located in one of those nodes.  Assign your equipment to an organization using the pull-down menu. Details on setting up your organizational structure are provided in section 6.3 – <i>Organizing your system with sites and departments</i> , p. 99.
<b>Critical/Not critical</b>	Determine the criticality level for the equipment by clicking on the appropriate option.  This information is used to fine-tune the data logging mode and alert rules based on equipment criticality.
<b>Mobile/Static</b>	Indicate whether the equipment is dedicated to a static environment (refrigerators, freezers, water-baths...) or a mobile environment (coolers, packages...).

- Click on **Save** to save the equipment or on **Cancel** to close this window without saving changes.

## Equipment

Once created, the equipment is listed in the equipment management screen:





Designation ↑↓	Type ↑↓	Sensors ↑↓	Organization ↑↓	Plan ↓↕
Incubator 1	Incubator	3	Lab Science	Main building
Incubator 3rd Floor	Incubator	2	Los Angeles	Main building
Refrigerator 2	Refrigerator	0	Lab Science	
Freezer A1	Door 15 (2nd floor)	3	Los Angeles	

Figure 135 – Equipment list in OCEAView

### 11.1.1 Associating sensors with equipment

This section describes how to assign one or more sensors to monitor equipment.

To associate a sensor with equipment:

1. Click on **Equipment** (  ) in the left-hand menu to see the list of equipment you are authorized to manage.
2. Click on the equipment to which you want to add a sensor.
3. Click on **Associate sensor** (  ) 1:

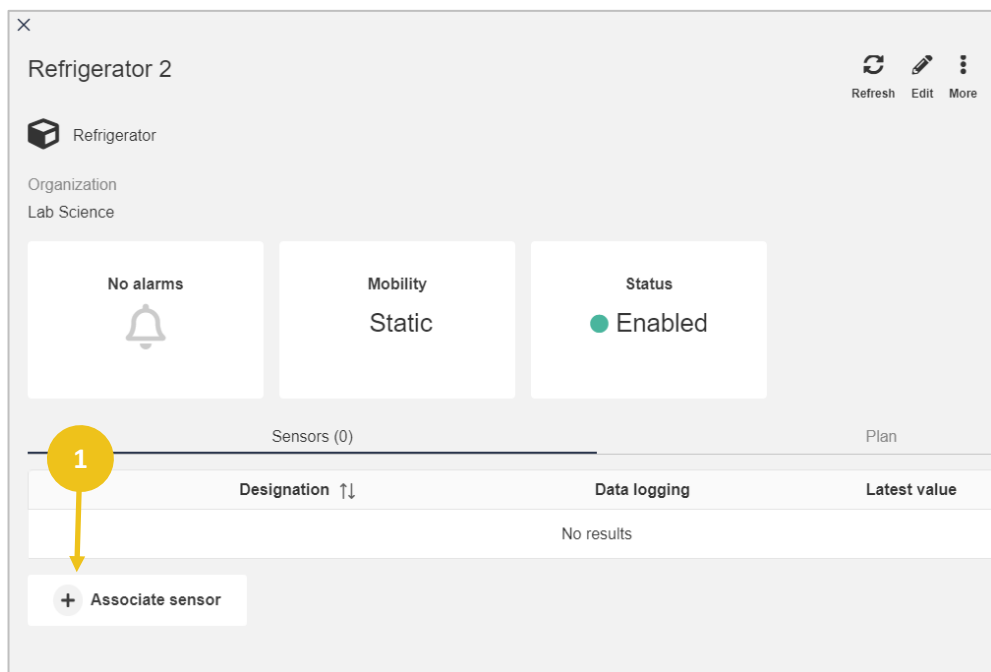


Figure 136 – Equipment details

4. Tick one or more checkboxes 2 to select the desired sensor(s):

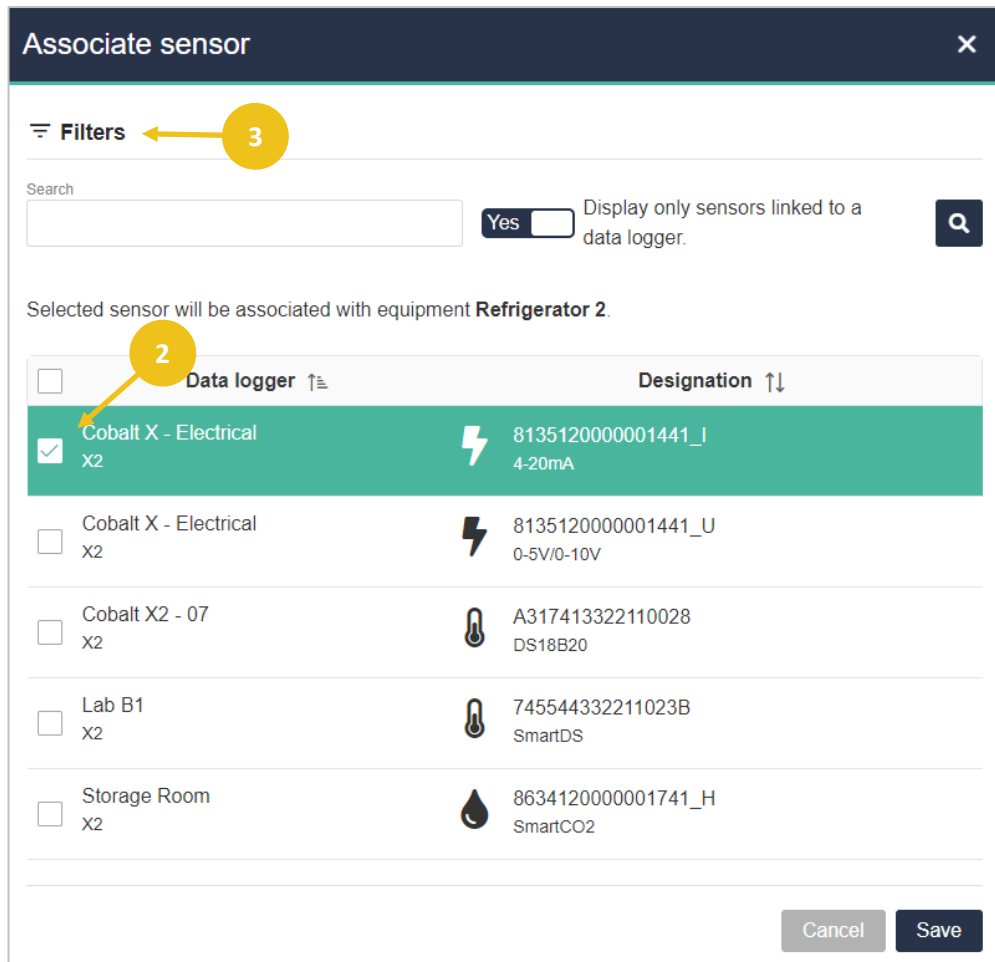





Figure 137 – List of available sensors

- If you have many sensors in your system, you may click on **Filters** 3 to search for specific data loggers. Type all or part of the data logger name in the **Search** field and then click on the magnifying glass (  ) to refresh the list.

**Note:** sensors that have been unplugged from a data logger may still be in the system. If you would like to list only those sensors that are currently linked to a data logger, click the **Yes**  toggle switch to **Yes** and click on the magnifying glass (  ). Otherwise, to list all sensors, toggle the switch to  **No** and click on the magnifying glass (  ).




- Click on **Save** after selecting one or more sensors, or on **Cancel** to exit this screen without saving changes.

### 11.1.2 Dissociating sensors from equipment



You may only dissociate sensors from equipment if they are not being used for data logging. If the sensor is being used for data logging, you must first stop data logging and then dissociate the sensor from the equipment

#### To dissociate a sensor from equipment:

1. Click on **Equipment** (  ) in the main menu to see the list of equipment you are authorized to manage.
2. Click on the equipment from which you want to remove a sensor.
3. Click on **Remove association** (  )  next to the sensor you want to remove:

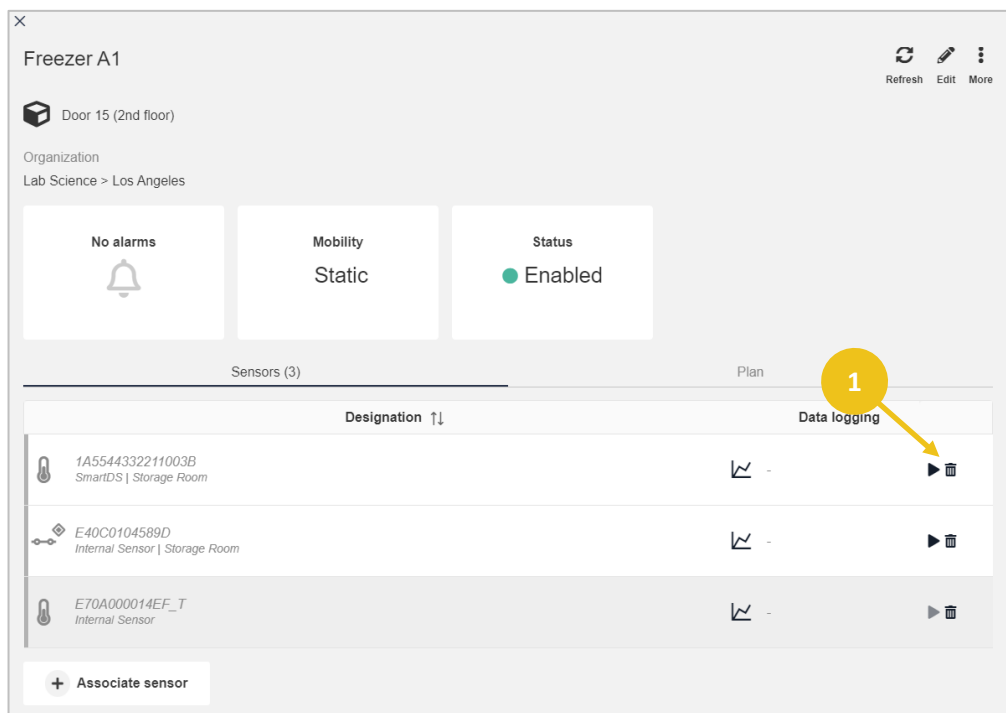


Figure 138 – Dissociating a sensor from equipment

4. Click on **Yes** and confirm the operation when prompted, if you really want to remove the sensor, or click on **No** to return to the previous screen without making any changes.

## 11.2 Viewing equipment details

Regardless of your user level in OCEAView, you may always check the data for the equipment you are authorized to view.

For a complete view of all equipment details, including sensor readings:

1. Click on **Equipment** (📦) in the main menu.
2. Select the desired equipment.
3. The equipment details are displayed as shown below:

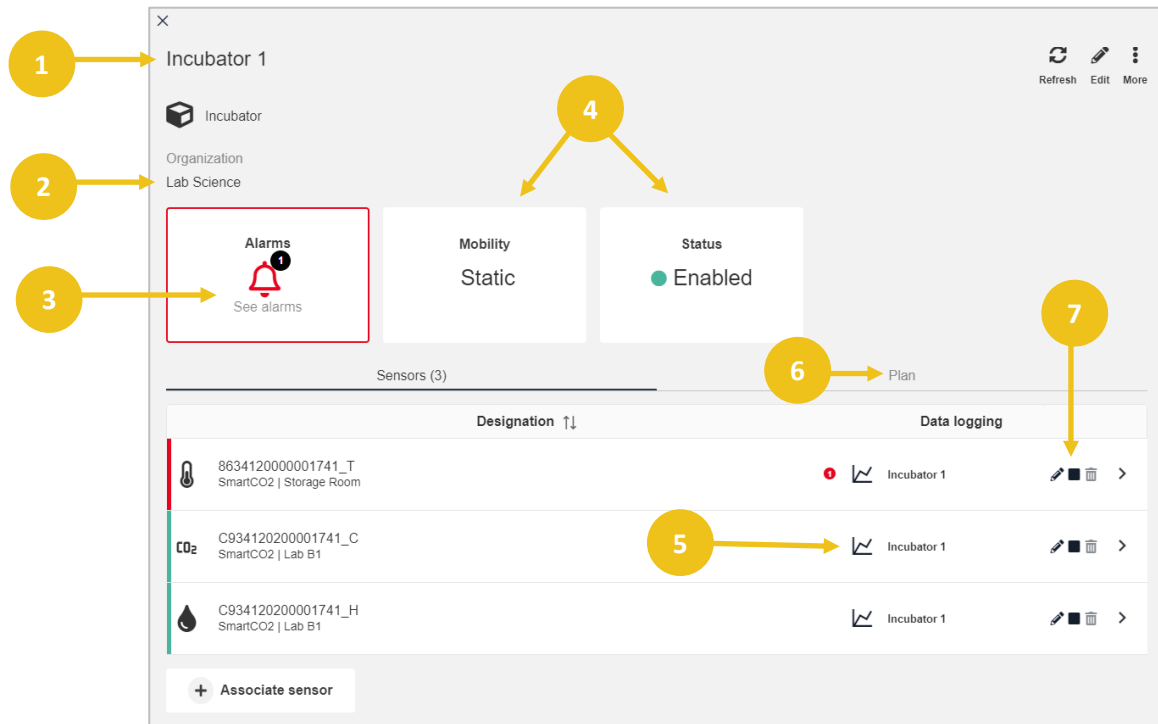







Figure 139 – Equipment details




Description	
1	Equipment name and type.
2	Organization and department (if configured) to which the equipment is associated.
3	Current alarm indicator. Hold your mouse over the indicator or click on it for details or to acknowledge an alarm.
4	Mobility indicator (Mobile or Static) and equipment status (Enabled or Disabled).

<p>5</p>	<p>Opens a graph with all sensor readings.</p>
<p>6</p>	<p>If you have placed the equipment on a plan as described in section 6.4.2 – <i>Editing or deleting a plan, p. 109</i>, click on the <b>Plan</b> tab to view the exact location of the equipment on the map.</p>
<p>7</p>	<ul style="list-style-type: none"> <li data-bbox="531 465 1385 544">  Click to edit current data logging settings (starting with OCEAView 1.11)         </li> <li data-bbox="531 555 1385 600">  Click to remove the sensor from its current equipment.         </li> <li data-bbox="531 611 1385 689">  Click to set sensor settings and start data logging (password required).         </li> <li data-bbox="531 701 1385 745">  Click to <b>stop data logging</b> (password required).         </li> </ul>

## 11.3 Modifying / managing equipment

You may use the options available in the equipment details screen to manage the equipment in your OCEAView system.

1. Click on **Equipment** () in the main menu.
2. Select the desired equipment.
3. Several options are available in the upper right-hand corner:

<p>More ()</p>	<p><b>Alarm history</b> Opens the alarm page for the selected equipment (described in section <i>15.1.2 – Viewing alarm details, p. 230</i>).</p> <p><b>Edit location</b> This option is only available for “<b>Static</b>” equipment, allowing you to locate the equipment on a floor plan or change its position on the plan (described in section <i>6.4.2 – Editing or deleting a plan, p. 109</i>).</p> <p><b>Disable / Enable</b> Select this option to disable equipment or enable equipment that has been disabled. Disabled equipment is no longer shown in the equipment list or as a tile in the Watch Mode display. Note: equipment cannot be disabled if data logging is currently running on one of its sensors. To enable disabled equipment, use the Filter option in the equipment list and select <b>Display disabled equipment</b> to enable it.</p> <p><b>Delete</b> Removes the selected equipment from the system.</p>
<p>Edit ()</p>	<p>To modify the information for existing equipment. Click on <b>Save</b> to keep your changes, or on <b>Cancel</b> to return to the previous screen without saving changes.</p>
<p>Refresh ()</p>	<p>Click to Refresh to update the information in this window.</p>

## 11.4 Deleting equipment

You may only delete equipment if no sensors are associated with it, and which have never been used for data logging (for traceability reasons). You may deactivate equipment to no longer display it (**Options** → **Deactivate**)

If one or more sensors are associated with the equipment, you must first unpair the sensor(s) before deleting the equipment. See section 11.1.2 – *Dissociating sensors from equipment*, p. 165 for more details on this feature.

To remove equipment:




1. Click on **Equipment** (  ) in the main menu.
2. Select the desired equipment.
3. Click on **Delete** (  )  to remove the selected equipment:



Figure 140 – Equipment management window

4. Click on **Yes** to confirm the operation when prompted if you really want to remove the equipment or click on **No** to return to the previous screen without making any changes.

## 12 Data logging

You must program data logging on your data loggers in order to record sensor readings and upload data to OCEAView.



Data logging revolves around the equipment you wish to monitor. You must therefore assign one or more sensors to equipment in order to set up and start data logging (described in section 11.1.1 – *Associating sensors with equipment, p. 163*).

Data logging consists of recording physical parameters (such as temperature and humidity) over time. Sensor readings are recorded based on a set of configuration options that are used to manage your data logger while data logging.

Data logging parameters include:

- The sensor reading frequency
- High and low alarm limits

### 12.1 How does it work?

Here is a quick overview of the data logging flow with OCEAView:

1. The Dickson data logger equipped with sensors is installed on the equipment to be monitored.
2. Sensor readings are collected by the data logger and sent data to the Cloud or your server via LoRaWAN or Bluetooth wireless connectivity.
3. If programmed limits are exceeded, or other anomalies are detected, an alert is displayed on the data logger and you can receive alerts 24/7 by e-mail, SMS/text message, or voice message.

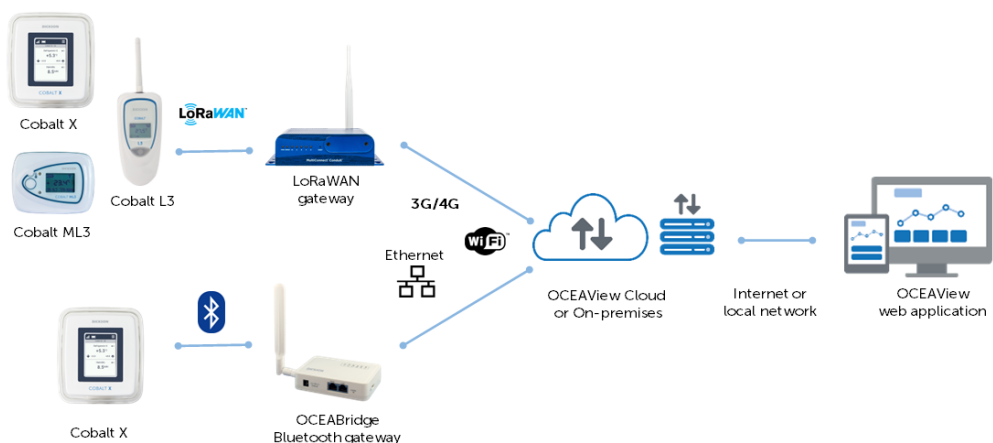


Figure 141 – Communication with OCEAView via LoRaWAN or Bluetooth

## 12.2 Setting up data logging



A sensor must be associated with equipment to start data logging.

To configure data logging:

1. You can start data logging via **Equipment** (📁), **Data loggers** (📡), or **Sensors** (🔧) in the left-hand menu for sensors associated with equipment. The instructions below are identical in all three cases.

2. **From Equipment** (📁):

Click anywhere on the line with the desired equipment **1** for which you want to start data logging:

Designation	Type	Sensors	Organization	Plan
Freezer A1	Room 5 (2nd floor)	2	Chicago	
Incubator 1	Incubator	3	Berlin	Main building

Figure 142 – Click on equipment for data logging

Click on the **Start data logging** button (▶) **2** on the desired sensor to continue:

Freezer A1

Room 5 (2nd floor)

Organization: Lab Science > Chicago

No alarms

Mobility: Static

Status: Enabled

Sensors (2)

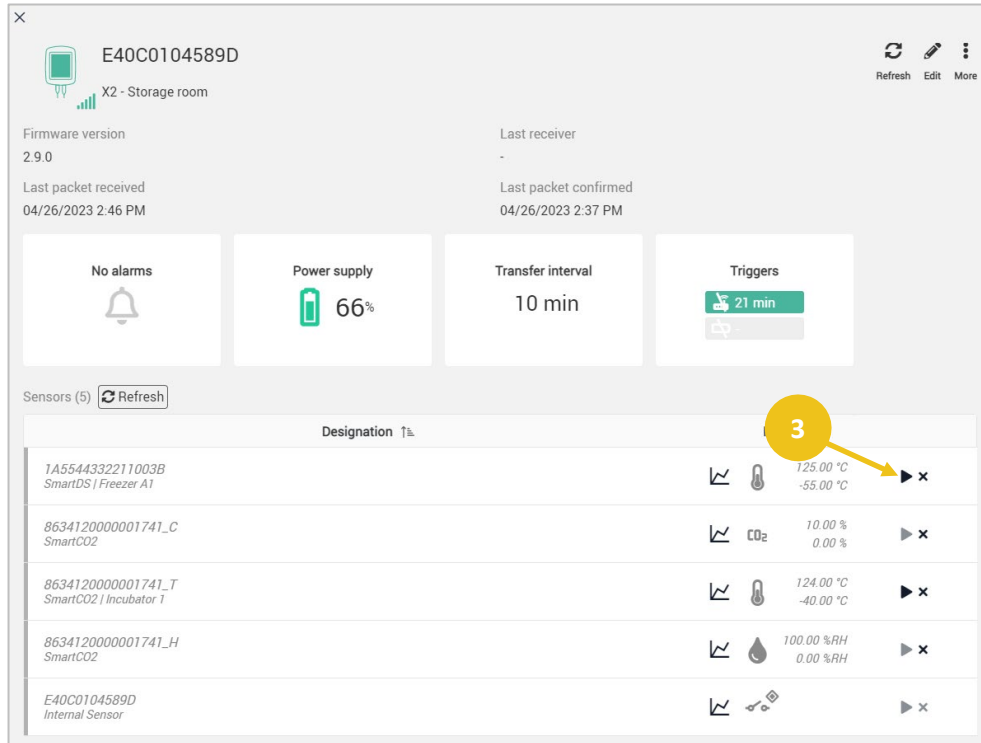
Designation	Start data logging
1A5544332211003B SmartDS   Storage Room	▶
E70A000014EF_T Internal Sensor	▶

+ Associate sensor

Figure 143 – Choosing a sensor for data logging

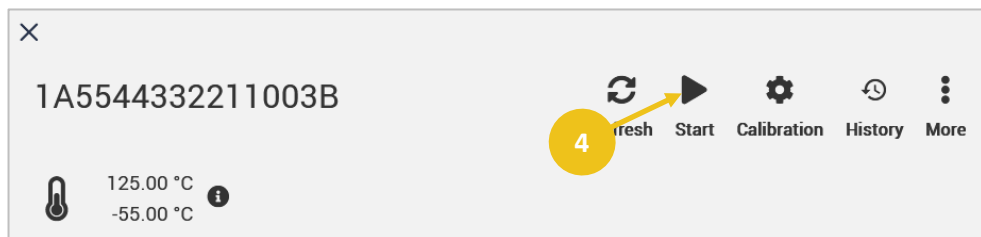
From **Data loggers** (📱):

Click on the desired data logger in the list. Available sensors are shown on the right-hand side of the screen. Click on the **Start data logging** button (▶) 3 for data logging settings:



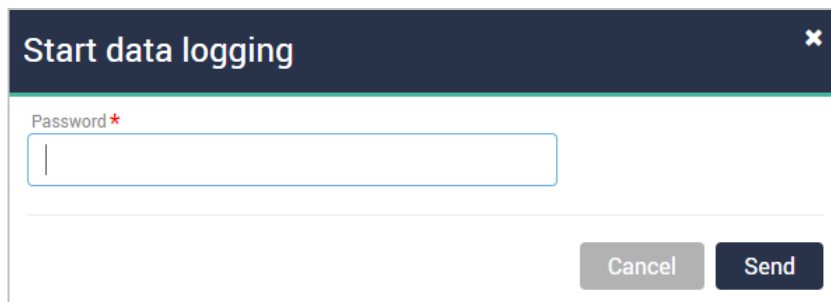
From **Sensors** (🌡️):

Click on the desired sensor, then click on **Start** (▶) 4.



3. Enter your password to continue.

With internal authentication, enter the password and press **Send**:



With SSO, press Send and complete the process displayed by your identity provider:

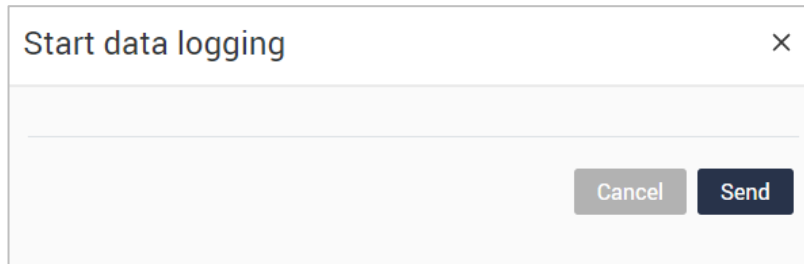


Figure 144 – Entering password to access data logging settings screen

4. The **Start data logging** window opens, as shown below:

- General sensor properties ( 1 ), for information only
- Entering specific parameters ( 2 ), with information that varies according to sensor type

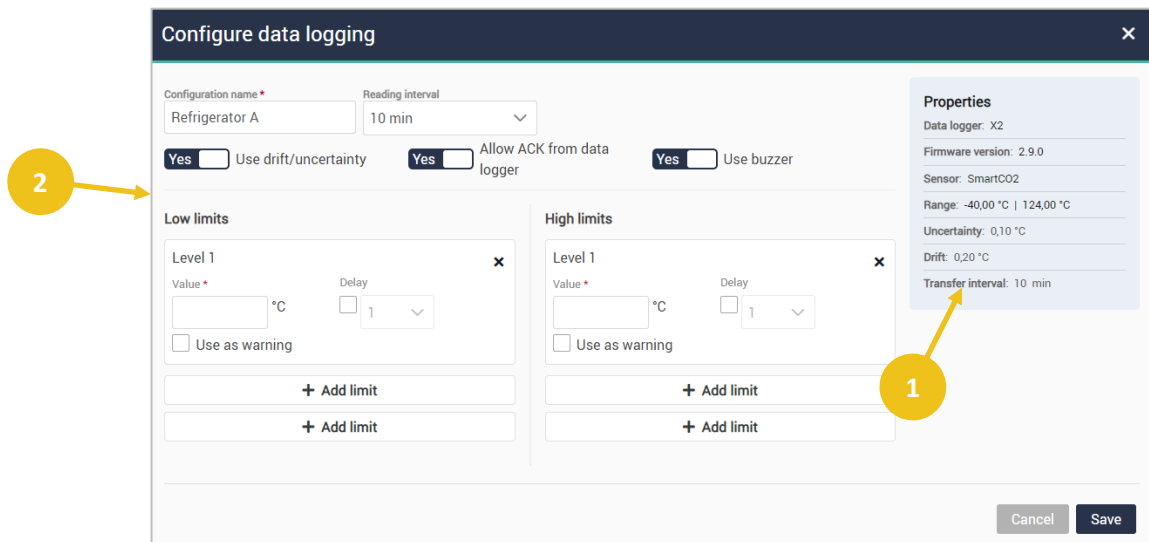


Figure 145 – Defining data logging settings (example with temperature sensor)

5. Define the settings for a new data logging session as described in the next sections or reuse the existing values (if present from a previous data logging session).

### 12.2.1 Environmental sensors (temperature, humidity, CO<sub>2</sub>, etc.)

For sensors that take readings across a range of values, such as temperature or humidity, the data logging options in the **Start data logging** window shown above are as follows:

1. Set the following information:

**Configuration name** Assign a name for the data logging session. This name will be displayed on the data logger screen.

**Reading interval** Indicates the frequency with which the sensor records a reading. Use the drop-down list to select the value that meets your needs.

**Use drift/uncertainty** Select this checkbox if you want to take into account the drift and uncertainty values provided for the sensor (see section 10.4.1 – *Editing parameters for calibrated sensors, page 149*). These values will diminish read value tolerance: for example, if you set low and high limits at 2°C and 8°C, with drift of 1°C and uncertainty of 1°C, the effective target range is considered by the system as being as the “worst case scenario”, or 4°C to 6°C). Drift and uncertainty values can be shown on sensor graphs (described in section 13.1 – *Displaying sensor graph, p. 187*)

**Allow ACK from data logger**

[Cobalt X1/X2 only] Select this checkbox if you want users to be able to acknowledge alarms via the data logger screen. If you deselect this checkbox, acknowledgment cannot be performed via the data logger screen.

**Use buzzer**

[Cobalt X1/X2 only] Select this checkbox if you want the buzzer on your data logger to buzz in case of an alarm. The data logger must be running on AC power for the buzzer to function.

2. You may set low and high limits to ensure that the physical parameter(s) in the monitored environment remain(s) within a specific range of values.



---

With Cobalt XS/X1/X2 data loggers, you may enter up to three high limits and three low limits to benefit from multiple warnings if excursions persist, and each limit may either be treated as a warning or an alarm (see below). You may enter the limits in any order that you choose. The first one you enter is displayed on the data logger display.

Cobalt L3 and Cobalt ML3 data loggers only support one high limit and one low limit.

---

### Low limits

<b>Value</b>	The lowest acceptable sensor reading (lowest temperature, lowest humidity level, etc.). Any readings below the limit(s) will trigger an alarm or warning. Click on <b>+</b> to set up additional limits, or <b>X</b> to remove limits you may have added.
<b>Delay</b>	Indicates how many readings lower than the low limit can be observed before triggering an alarm. The maximum number for this field is 200 readings.  The corresponding duration in terms of time is simply the number of readings indicated here, multiplied by the read interval. This information is shown in a tooltip that is displayed when you hold your cursor over the <b>i</b> icon.
<b>Use as warning</b>	Starting with OCEAView version 1.12, you can configure limits as a "warning" rather than an "alarm". The only difference is that a warning does not require acknowledgement (either in OCEAView or by entering a PIN code on a Cobalt X1/X2 data logger)

### High limits

<b>Value</b>	The highest acceptable sensor reading. Any readings above the limit(s) will trigger an alarm. Click on <b>+</b> to set up additional limits, or <b>X</b> to remove limits you may have added.
<b>Delay</b>	Indicates how many readings above the high limit can be observed before

triggering an alarm. The maximum number for this field is 200 readings.

The corresponding duration in terms of time is simply the number of readings indicated here, multiplied by the read interval.

**Use as warning** Starting with OCEAView 1.12, you can configure limits as a “warning” rather than an “alarm”. The only difference is that a warning does not require acknowledgement (either in OCEAView or by entering a PIN code on a Cobalt X1/X2 data logger)

When configuring delays as described above, you may hold your mouse over the **i** icon next to the **Delay** field (1) to see a tooltip showing the exact duration in terms of time. The value indicated here is updated to reflect any changes you make for **Reading interval** or **Delay**.

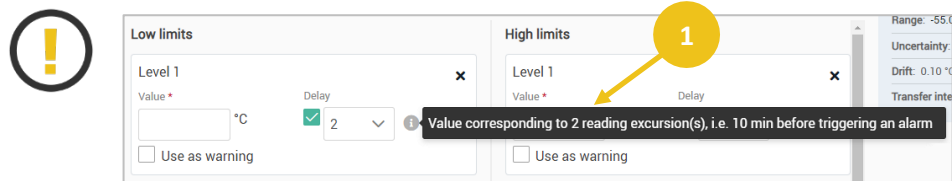


Figure 146 – Dynamic calculation of time before alarm occurs

If a reading exceeds the specified limits when data logging is running (and the delay is reached, if configured), you receive notification as configured by your Alert rules (described in section 15.2 – Alert rules and notifications, p. 238 ), and you will see visual notification of the alarm condition on your data loggers as follows:

**Cobalt X1/X2** The data logger screen changes color, the outer ring flashes, and the system’s alert mechanism notifies you as configured. As long the data logger remains in an alarm state, the data logger buzzer will also emit an audio alarm when plugged into AC power.

**Cobalt XS** The LED in the upper left-hand corner of the casing blinks as long as the alarm condition persists.

**Cobalt L3/ML3** The pushbutton (L3) or LED (ML3) flashes and the system’s alert mechanism notifies you as configured.

## Data logging

3. Click on **Save** in the lower right-hand corner of the **Start data logging** screen to begin recording sensor readings. The system sends the command to the data logger and then waits for synchronization. Data logging begins at the next programmed transfer interval.

### 12.2.2 Dry contact input sensors (Cobalt X1/X2 only)

To start data logging for a dry contact input sensor on a Cobalt X1/X2 data logger:

1. Click on the **Start data logging** button (▶) in the Equipment, **Data loggers**, or **Sensors** screens.
2. Enter your system password and click on **Send** to continue.
3. The **Start data logging** window opens, with several zones (*shown below*):
  - General sensor properties (1), including indication of current sensor configuration (NO = Normally Open; NC = Normally Closed)
  - Specific parameters for this data logging session (2)

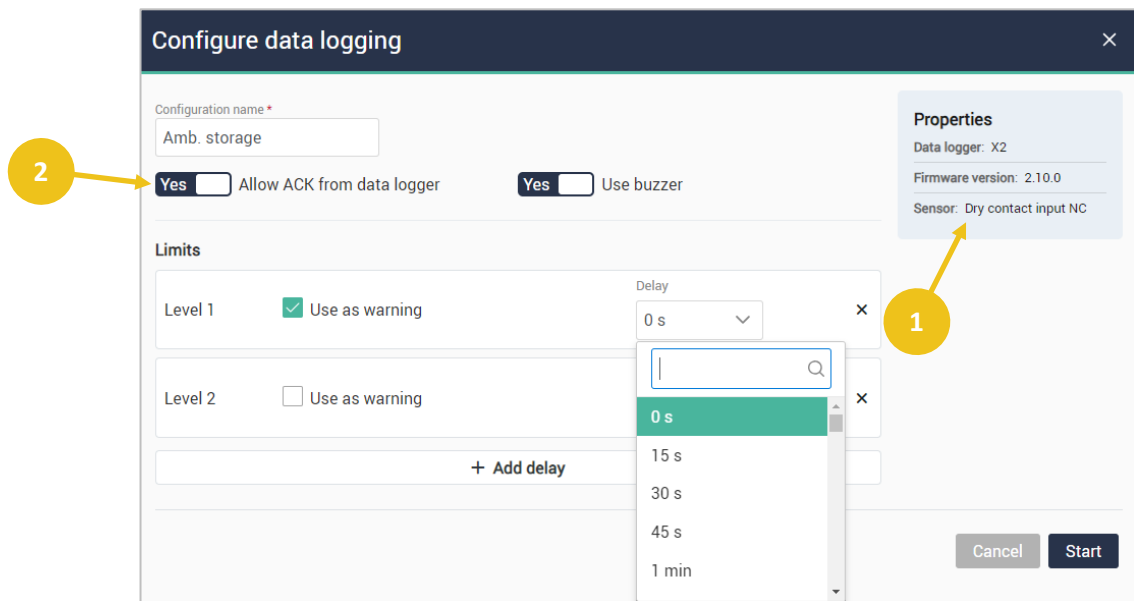


Figure 147 – You may configure up to three alarm and warning delay times

4. Define the settings as described for the fields as follows:
 

<b>Configuration name</b>	Assign a name for the data logging session.
<b>Allow ACK from data logger</b>	Select this checkbox if you want users to be able to acknowledge alarms via the Cobalt X1/X2 screen. If you deselect this checkbox, acknowledgment cannot be performed via the data logger screen.
<b>Use buzzer</b>	Select this checkbox if you want the buzzer on your Cobalt X1/X2 data logger to buzz in case of an alarm. The data logger must be running on AC power for the buzzer to function.
<b>Limits</b>	Check the <b>Use as warning</b> checkbox if the alarm level should be a warning (in which case acknowledgement is not required).

Select the desired time from the pull-down list (from 0 seconds to 60 minutes). You may click on **+ Add delay** to add up to three delay levels. Each delay may be assigned to a different alert notification (as described in section 15.2.1 – *Configuring alert rules, p. 238*).



If you do not set any delay, the sensor never enters an alarm state. The tile in Watch Mode does not turn red when the sensor state changes.

---

Reading is continuous, with every loop opening and closing action recorded in data logging. That information is sent to the server at the programmed transfer interval.

If the loop remains open for a period of time specified for an alert, then the alert is sent immediately upon detection. For example, if data logging is set with a 1-minute alarm delay, and the loop remains open for 1 minute, then the alarm condition is transmitted right away to OCEAView and the alert notification is sent by the system as defined by alert rules.



If you want to change the configuration between “Normally closed” and “Normally open”, you must first stop data logging in OCEAView before making the change on the Cobalt X1/X2 data logger.

---

5. Click on **Start** in the lower right-hand corner of the **Configure data logging** screen to begin recording sensor readings. The system sends the command to the data logger and then waits for synchronization. Data logging begins at the next programmed transfer interval.

## 12.3 Changing data logging settings on-the-fly

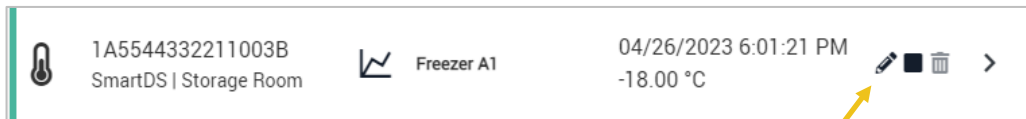
If your user role allows you to start and stop data logging, you may change data logging settings at any time, even while data logging is running. For example, you can change high or low limits or the data logging session name without stopping data logging. This makes it easy to handle changes and while ensuring continuity in your data logging records.



This feature is available for Cobalt data loggers with firmware 2.7 or higher. In order to change data logging on-the-fly, your user role must allow you to both "Start data logging" and "Stop data logging", as described in section 5.6 – *Adding user roles*, p. 85.

You may change data logging settings from the **Equipment** (📁), **Data loggers** (📱), or **Sensors** (🌡️) screens. When data logging is running, you will see the **Edit** icon (✎) 1 as shown below.

Equipment screen:



Data logger screen:



Sensor screen:

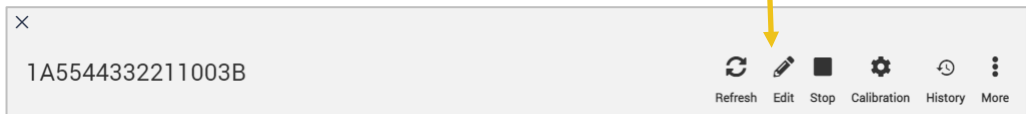


Figure 148 – Editing settings without stopping data logging

To change data logging settings:


1. Click on the **Edit** icon (  ).
2. Enter your password and press **Send** (or press **Send** if you are logged in with SSO). This opens the **Configure data logging** window with your current settings (in this example, 3°C low limit and 10°C high limit):

Figure 149 – Editing data logging settings

3. Simply change the limit values as desired, for example changing the low limit to 2°C and the high limit to 8°C  :

Figure 150 – Assign new values for low and high limits

**Note:** you can also change the data logging session name, but not the reading interval, drift/uncertainty, acknowledgment, or buzzer options. You can change the transfer interval in **Data logger** → **Edit data logger**.

4. Press **Save** to apply your changes, which will take effect the next time the data logger is synchronized (either manually via the data logger menu or at the next programmed transfer interval). It may take one or two synchronization cycles to be completely taken into account.

## 12.4 Stopping data logging



Data logging can be stopped via the Equipment, Data logger, or Sensor screens.

To stop data logging that is currently running:

1. Click on **Equipment** (📦), **Data loggers** (📊), or **Sensors** (🌡️) in the left-hand menu. The instructions below are identical in all three cases.
2. Click on the name of the equipment or data logger that you want to stop.
3. Sensors for which data logging is in progress have a **Stop data logging** button (⏸️). Click on that button **1** to stop data logging:

Refrigerator A1

Room 5 (2nd floor)

Organization  
Lab Science > Chicago

No alarms

Mobility  
Static

Status  
Enabled

Sensors (2)

Designation ↑↓	Data logging	Latest value	
🌡️ 1A5544332211003B SmartDS   Storage Room	📊 Refrigerator A	04/26/2023 6:27:37 PM 5.10 °C	⏸️ 🗑️ ➤
🌡️ E70A000014EF_T Internal Sensor	📊 -	04/05/2023 4:24:11 PM 26.13 °C	▶️ 🗑️

Figure 151 – Stopping data logging (example shown in Equipment screen)

4. You will be prompted to confirm your action by entering your password in the pop-up window:

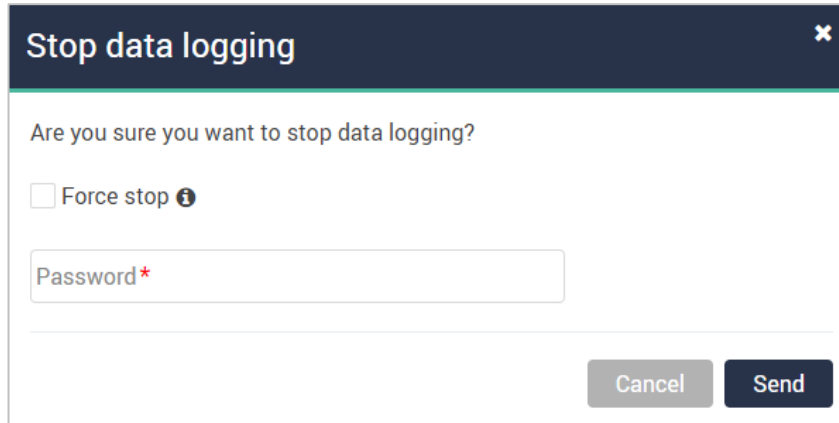


Figure 152 – Entering your password to stop data logging

If you select **Force stop**:

Data logging is stopped at the next programmed transfer interval without retrieving the latest information from the data logger (readings and other information). Any unretrieved information is lost.

If you do not select **Force stop**:

Data logging is stopped at the next programmed transfer interval, but all the information is retrieved from the data logger at that time. The operation may take longer with this option.

5. Click on **Send** to stop data logging, or on **Cancel** to return to the previous screen without making any changes.

## 12.5 Note regarding reading interval vs transfer interval

With LoRaWAN wireless communications, do not confuse the data logger's wireless data "transfer" interval, with the sensor "reading" interval configured for each sensor.

Sensor data is first stored in the data logger's internal memory and then transferred wirelessly to the OCEAView platform at programmed intervals. To preserve data logger battery life under normal operation, transmission to the server occurs periodically, but not at every reading. If you modify settings in OCEAView, the values on the data logger screen are updated when the next transfer interval occurs.

The wireless transfer interval refers to the frequency with which the data logger sends its collected information to the server. The reading interval refers to the frequency with which the data logger reads its connected sensors.

For example, the data logger could read its sensors every 5 minutes and then send the data every 20 minutes.

Reading intervals can also depend on the data logger type and transfer interval. Here are some specific cases:

- In Bluetooth (BLE) mode, the minimum sensor reading interval for some sensors on Cobalt X1 is 5 seconds (Pt100, 4-20 mA).
- In Bluetooth (BLE) mode, the minimum sensor reading interval on Cobalt X2 is 15 seconds.
- In LoRaWAN mode: the minimum reading time depends on the transfer interval:  $minimum\ read\ time = transfer\ interval / 20$  (results are rounded up to the nearest minute). For example, with Cobalt X1/X2:
  - A transfer interval of 40 minutes supports a minimum read time of 2 minutes.
  - A transfer interval of 20 minutes (default value) supports a minimum read time of 1 minute.
  - A transfer interval of 15 minutes (the minimum value), the minimum read value is 1 minute, due to rounding.



The minimum transfer interval with LoRaWAN connectivity is 10 minutes.

---

## 12.6 Mobile monitoring considerations for Cobalt ML3

This section is mainly an excerpt from the Cobalt ML3 User Guide, as Cobalt ML3 usage for mobile monitoring is slightly different than that for fixed data loggers. OCEAView is optimized to handle LoRaWAN communications efficiently for Cobalt ML3 data loggers that are on the move during most of their duty cycle.

### 12.6.1 Setting the sensor reading interval

With data logger internal memory limited to 4,000 readings, make sure that you leave enough margin when setting the sensor reading interval in OCEAView to cover the entire journey. After 4,000 readings, new data overwrites the oldest data (first-in first-out FIFO mechanism). Here are some examples of memory capacity based on the sensor read interval:

Read interval	Memory limit reached
1 minute	66 hours
10 minutes	Almost 28 days
15 minutes	Almost 42 days

### 12.6.2 Setting the data transfer interval

The data transfer interval is configurable in OCEAView, with two elements: *transfer* and *retransfer* intervals.

The *transfer* interval represents the time between data transmissions when the data logger can connect to a gateway, with a typical value of 10 minutes for Cobalt ML3.

The *retransfer* interval represents the time before the data logger tries to communicate with a gateway after not being able to establish communication at the regular transfer interval.

This setting is important with mobile data loggers, which spend a large part of their time outside the wireless range of your LoRaWAN gateway(s). The default retransfer time for Cobalt ML3 is 5 minutes.

Practically speaking, this implies:

- For a data logger to transfer collected data *automatically* upon reaching a destination site (there could be several), you would need to wait at least the *retransfer* time (for the data logger to first connect to a new gateway), plus potentially the next transfer cycle (for example, 10 minutes, depending on settings).
- You may trigger data synchronization manually when within gateway range by pressing the pushbutton on the ML3 data logger for one second (first to connect to the server), then again for one second (to force immediate data synchronization).

## 13 Viewing sensor data

To access the list of the readings recorded by a sensor:

1. Click on **Readings** (📈) in any of the **Equipment**, **Data loggers**, or **Sensors** screens.
2. A color graph is displayed showing readings recorded by the selected sensor:

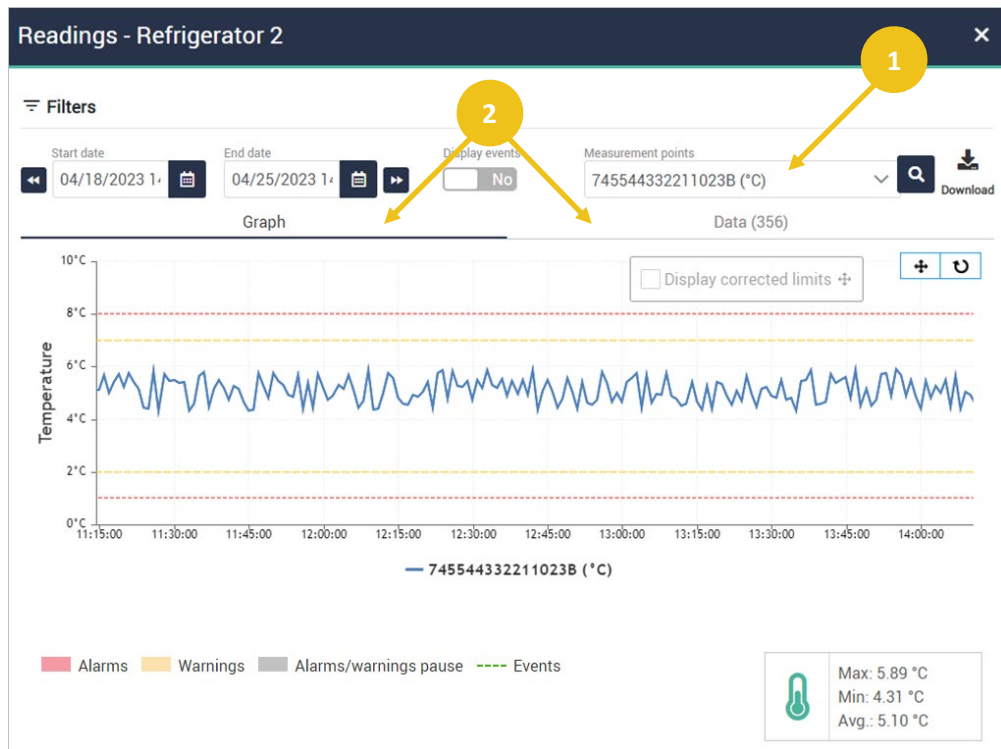


Figure 153 – Example of a sensor graph

You can display information from several sensors running data logging in a given piece of equipment at the same time by clicking on the **Measurement points** drop-down menu (1):

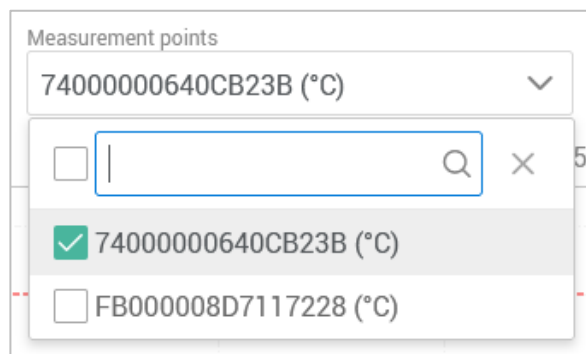


Figure 154 – Displaying several sensors simultaneously

The **Readings** window contains two tabs (2):

<b>Graph</b>	The graph shows readings in a visual format over time.
<b>Data</b>	A list is displayed showing all data and events that occurred throughout the data logging session (readings, timestamps, start, stop, limits exceeded, technical alarm, etc.).

## 13.1 Displaying sensor graphs

All sensor readings are shown on a graph, providing an easy way to track variations over time:

- The vertical axis shows the reading value.
- The horizontal axis shows the time scale.
- High and low alarm and warning limits
  - High and low alarm limits are by horizontal red dotted lines.
  - High and low warnings are indicated by horizontal orange dotted lines.
  - Limits can be displayed with Drift and Uncertainty corrections (described in the next section)
- Alarms (high and low limits) and events (technical alarms) are displayed in red. A key describing the different colors is shown at the bottom of the graph.
- Minimum, maximum, and average readings calculated during the data logging cycle are shown at the bottom right-hand side of the graph.

### 13.1.1 Displaying corrected limits on graphs

When you start data logging, you have the option to take **Drift** and **Uncertainty** values into account. These values are stored for each sensor via the **Calibration** function.

Here is an example of a sensor graph for data logging programmed with one high and low alarm limit, and one high and low warning limits, indicated by horizontal red and orange lines **1**:

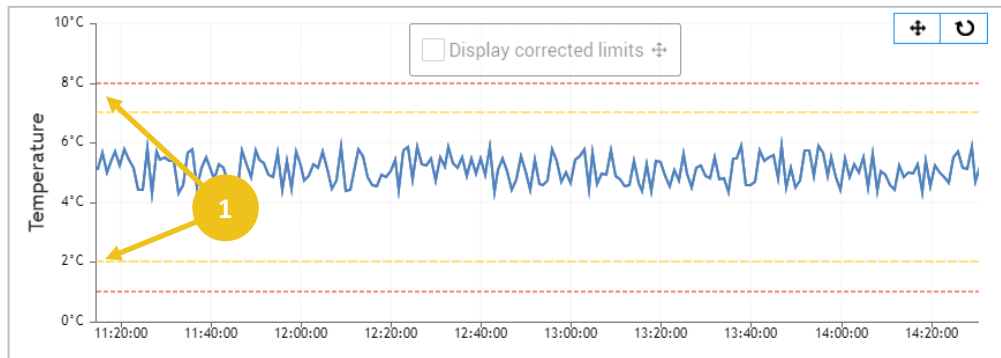


Figure 155 – High and low limits shown if programmed

The screen below shows the same information with the limit values adjusted by clicking on **Display corrected limits** **2** to take drift and uncertainty into account.

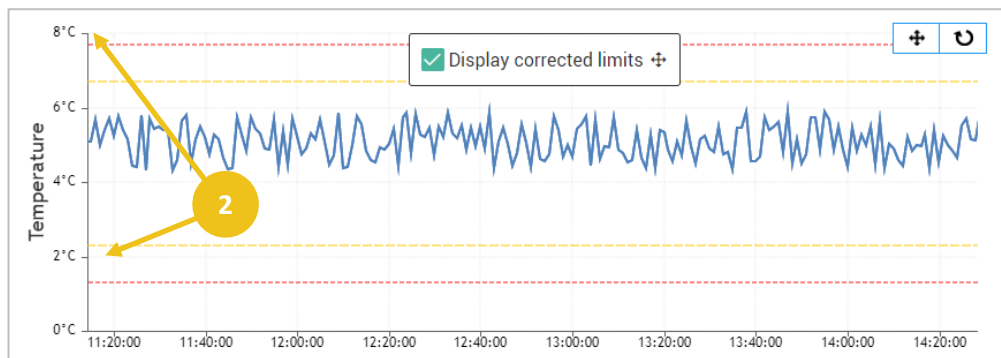


Figure 156 – High and low limits corrected for drift and uncertainty

Limit values are shifted by "inwards" by the total of drift plus uncertainty, thus adapting the theoretical target value to reflect the sensor's specific properties.

### 13.1.2 Selecting the display period

By default, the graph shows readings for the past 7 days. To adjust the dates for the graph display:

1. Click in the **Start date** and/or **End date** fields **1** and choose a month, day, and year from the date selection calendars. The date range must not exceed one month.

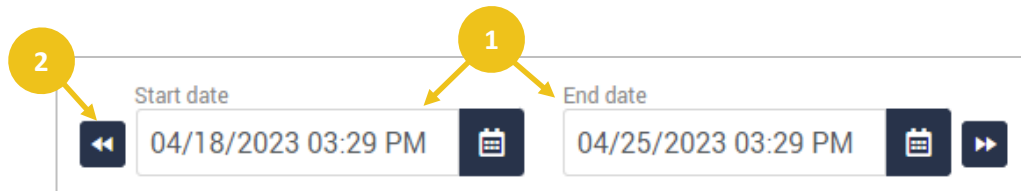


Figure 157 – Selecting the display period

2. Click on **Q** to confirm your choice and refresh the graph.
3. The scroll buttons next to the **Start** and **End** dates **2** are used to change the period for which you would like to display graphs. Click the arrows to move back or forward by one week.

### 13.1.3 Adding annotations to graph points

You may click on sensor values to add comments to a graph, for example to explain an unexpected situation or excursion in the data logging session.

1. As you move the mouse cursor along a graph, each reading point is indicated by a triangle (▲).

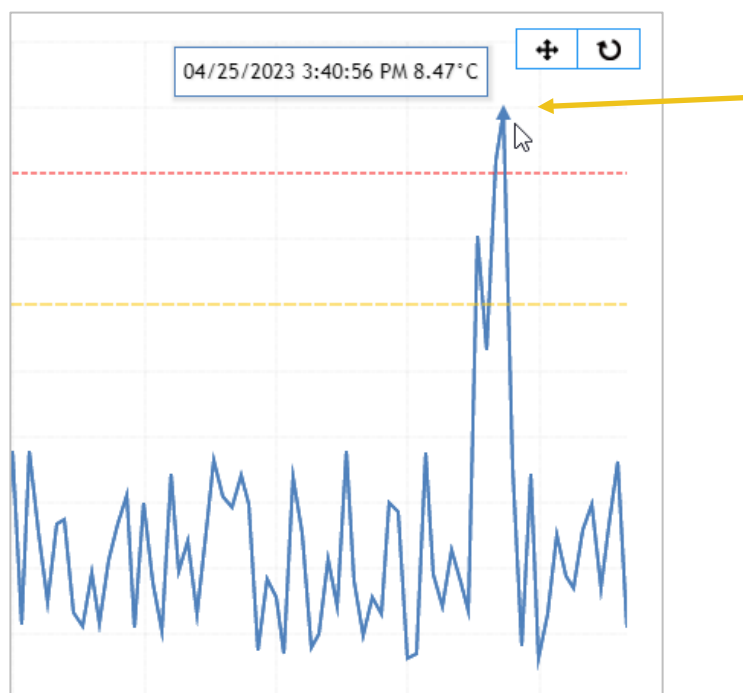


Figure 158 – Pop-up label indicates the reading's date / time stamp

## Viewing sensor data

2. When you place the cursor directly over the triangle, the cursor becomes a hand (👉).

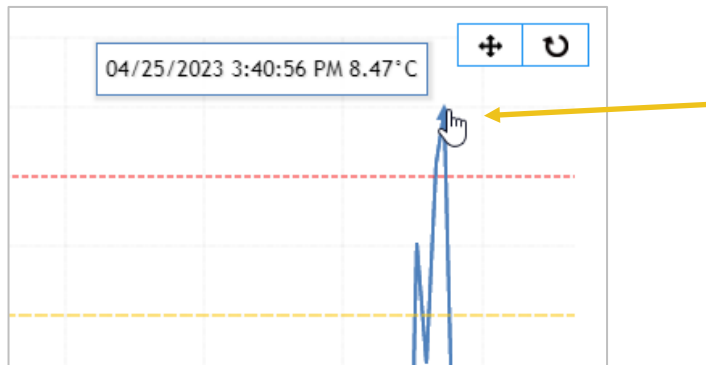


Figure 159 – Mouse cursor becomes a hand to click and add a comment

3. Click on the desired point and enter your text in the comment field.

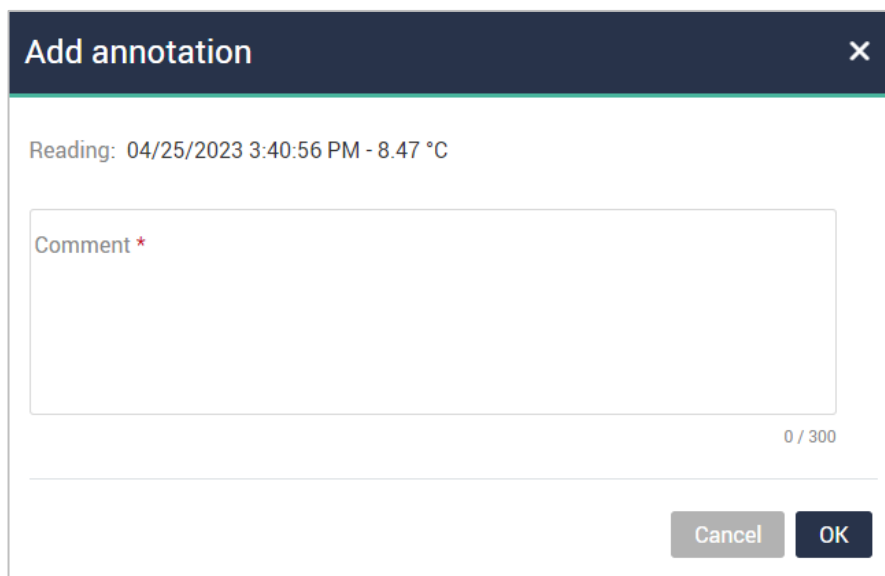
A dialog box titled "Add annotation" with a close button (X) in the top right corner. The dialog contains the text "Reading: 04/25/2023 3:40:56 PM - 8.47 °C". Below this is a text input field labeled "Comment \*". At the bottom right of the input field, the text "0 / 300" is displayed. At the bottom of the dialog are two buttons: "Cancel" and "OK".

Figure 160 – Enter your text in the Comment field

4. Click on **OK** when done, or on **Cancel** to close the window without saving changes. Reading points with annotations are indicated by a blue triangle that remains in place.



Figure 161 – Blue triangle remains on graph to indicates an annotation

5. When your mouse cursor hovers over the blue triangle, the details of the reading point and the annotation are displayed in a pop-up window.

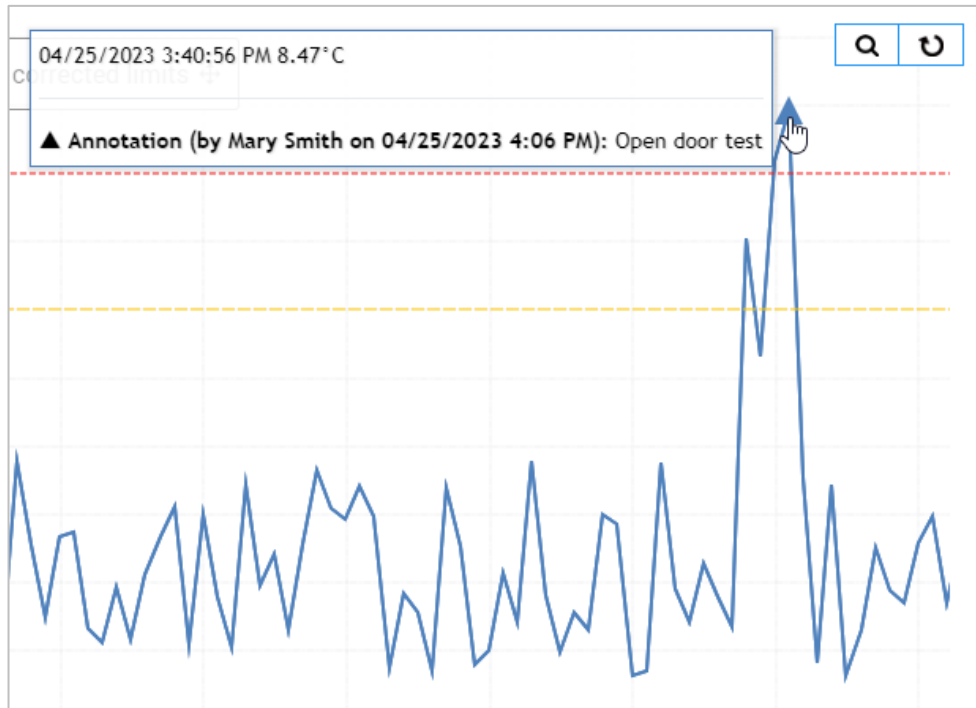


Figure 162 – Annotation displayed in pop-up in graph window



If a graph contains more than 50,000 readings, you must zoom in before you can add an annotation.

The annotation is also displayed in the **Data** tab. The annotation is time-stamped with the time it was created, and placed on the line corresponding to the reading in question.

Filters			
Graph		Data (448)	
Date	Value (°C)	Additional information	Type
04/25/2023 3:42:56 PM	4.41		Reading
04/25/2023 3:41:56 PM	5.78		Reading
04/25/2023 3:40:56 PM	8.47	▲ Annotation (by Mary Smith on 04/25/2023 4:06 PM): Open door test	Reading
04/25/2023 3:39:56 PM	8.10		Reading

Figure 163 – Annotation under *Additional information* in Data tab

#### To edit or remove a comment:

1. Click on the blue triangle ( ▲ ).
2. You may edit the text in the Comment field as desired.

Click on **Remove** to delete the annotation, on **Cancel** to close the window, or on **OK** to save any changes.



Actions to create, edit, and remove annotations are recorded in the audit trail.

#### 13.1.4 Including events in graph display

You may choose to include events in the graph displays, such as “Data logging started”, “Data logging stopped”, “Low battery alert”, etc.

To show events, click on  to access Filters if necessary, then use the **Display events** toggle switch at the top of the window to adjust the display:



Figure 164 – Event display toggle switch

### 13.1.5 Viewing paused alarm period

A feature to pause alarms and warnings was introduced in Cobalt X1/X2 firmware version 2.10 (released September 2023), allowing you to pause alarm and warning generation for a specified period of time ranging from 30 minutes to 72 hours. This can be useful when moving equipment or preparing for cleaning operations that would lead to unnecessary alarms and/or warnings. You may resume normal alarm/warning functionality manually at any time from the data logger.



This feature is controlled exclusively via the Cobalt X1/X2 user interface. You will find more details in the Cobalt X1/X2 user guide.

To see the paused period when viewing graphs in OCEAView, you must include events in the graph display as described in the previous section:

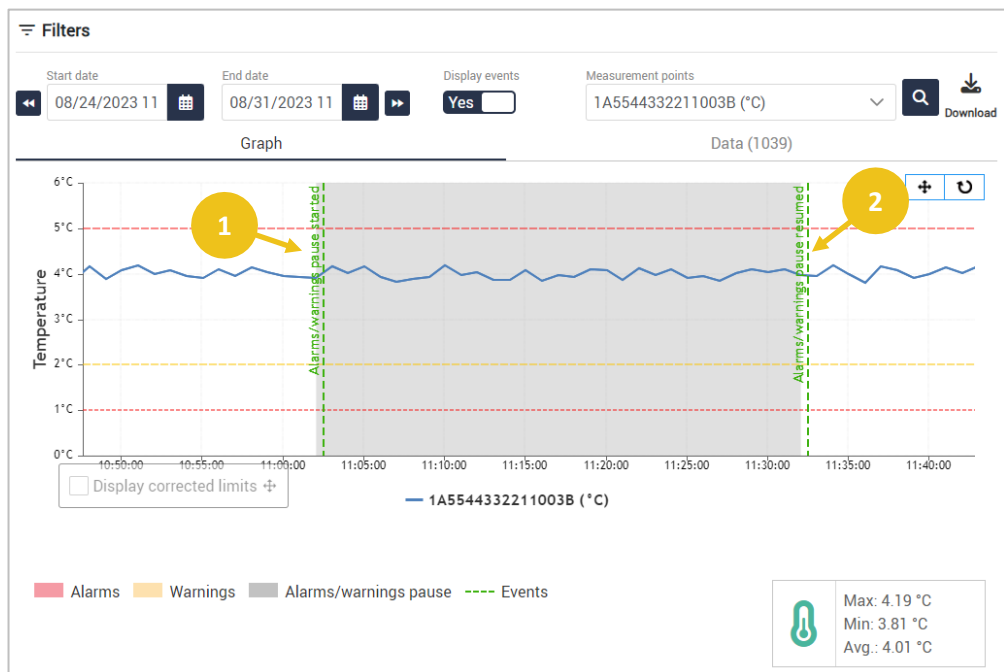


Figure 165 – Gray zone shows period when alarms were paused

You can see when the alarm pause was taken into account by the system **1** and when it ended **2**. This information is also recorded in the audit trail.

### 13.1.6 Zoom and control tools

When you move the mouse cursor **1** over the graph, a tooltip displays reading values and timestamps:

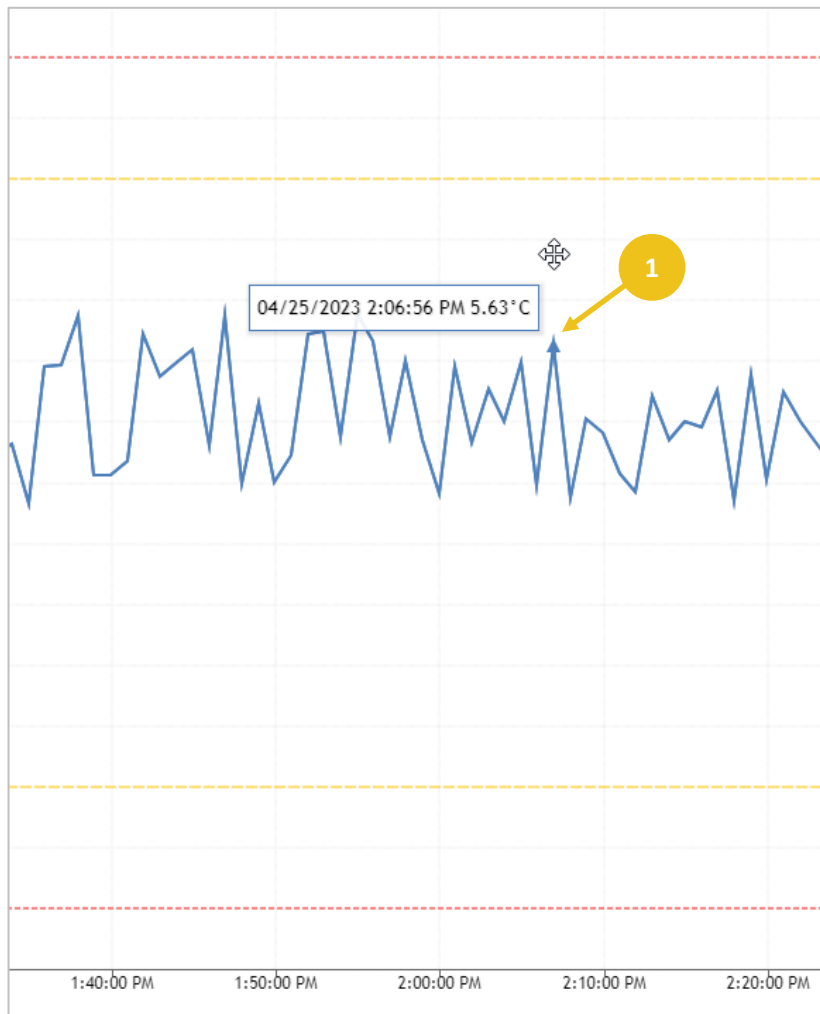


Figure 166 – Graph with reading details

If **Display events** is selected, events are indicated with the appropriate background color for warnings and alarms (light orange for warnings or light red for alarms) on the graph. Move the cursor over the graph to see event details **2**:

## Viewing sensor data

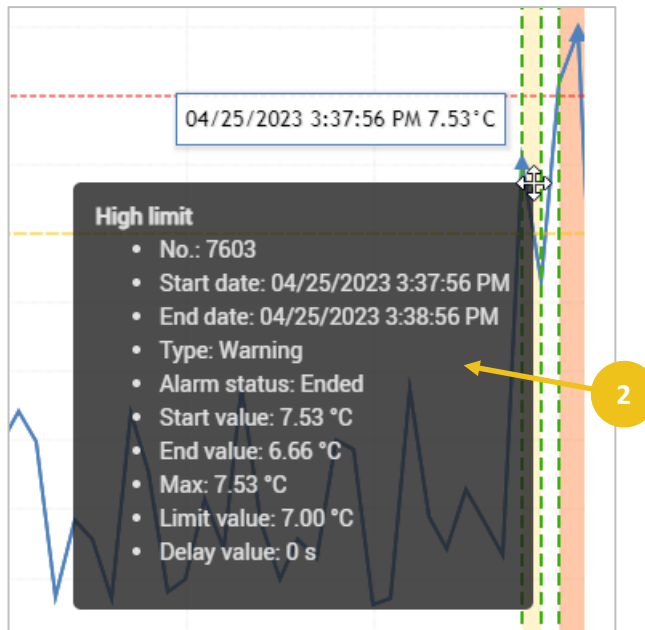


Figure 167 – Graph with event details

You may zoom into the graph to examine details more closely:

1. Left click and hold the mouse button and drag the cursor over the desired location in the graph.
2. Release the mouse button to zoom in on the selected area 3.

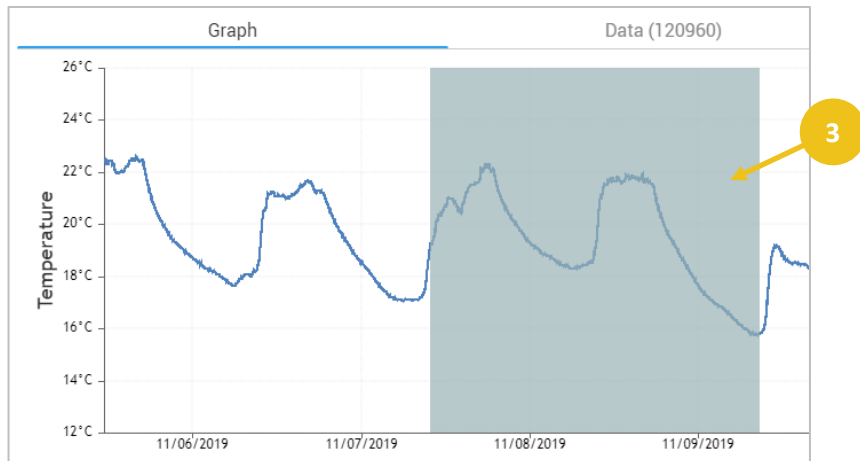


Figure 168 – Selecting the zoom area

3. The selected area is enlarged.
4. Repeat these steps to get a higher zoom level if needed.

As you zoom in on the graph, additional tools are shown in the upper right-hand corner of the graph <sup>4</sup>:

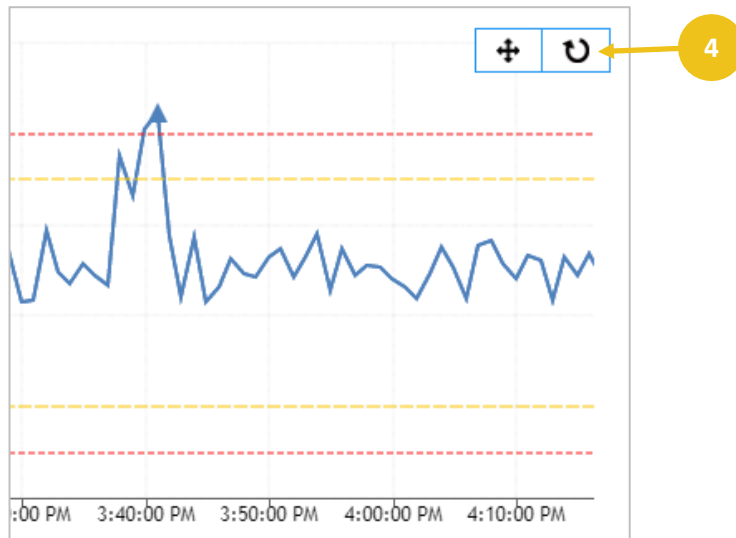


Figure 169 – Zoom and control tools



Enables you to use your mouse to scroll right and left through the graph. When you click on this button, the mouse cursor turns into a multidirectional arrow. Then click anywhere on the graph and drag right or left while holding the mouse button to focus on specific areas of the graph.




Turns off panning mode.



Clears zoom or pan effects and restores the graph to its original scale.

### 13.1.7 Exporting sensor data

You may generate a report based on the filters applied to the graph display by clicking on the **Download** button (  ) at the top of the screen and selecting the format (Excel, PDF, Word, or text). This is described in more detail in section 14.1.1 – *Sensor reading reports*, p. 206, and reports are described in detail in *Appendix 1 – Sensor reading report details*, p. 259.

### 13.1.8 Multigraph views across different equipment

OCEAView features a multigraph view that enables you to superimpose readings from multiple pieces of equipment or different dataloggers at the same time. This offers a practical way to compare equipment performance over a given period of time, and export a report in PDF format.

Here is a sample multigraph view:

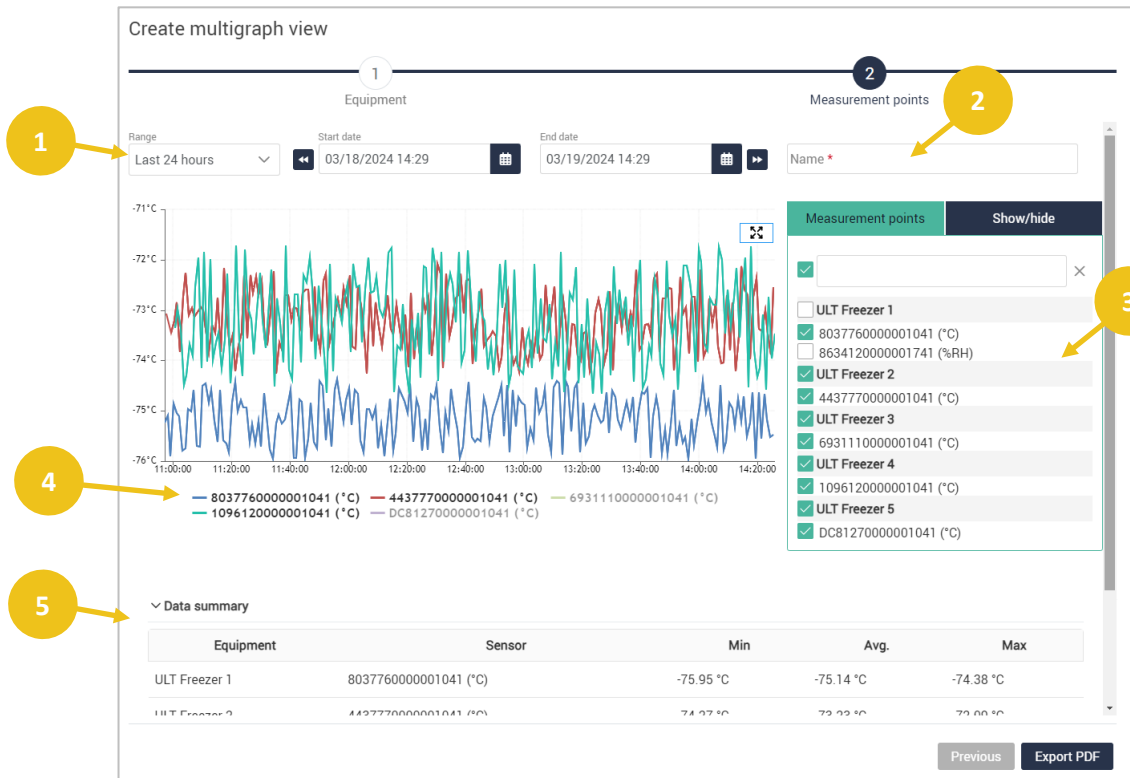




Figure 170 – Overview of multigraph display

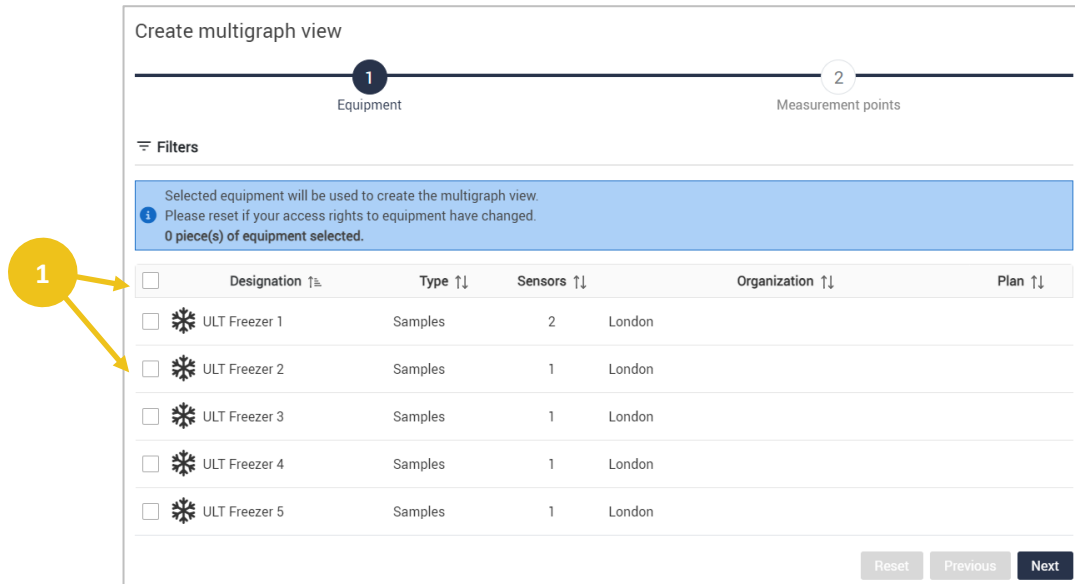
The key elements on this screen are:

- 1 Date and time range
- 2 Name to use when exporting graphs in PDF format
- 3 Measurement points to display
- 4 Serial numbers are clickable to show or hide curves
- 5 Summary with key data for each measurement point

## Viewing sensor data

Follow this two-step process to create a multigraph view:

1. In the main menu, select **Home** →  **Multigraph views**.
2. Click on the top checkbox  to select all displayed equipment, or select individually by clicking in the checkbox(es) for the equipment you want.



Create multigraph view

1 Equipment 2 Measurement points

Filters

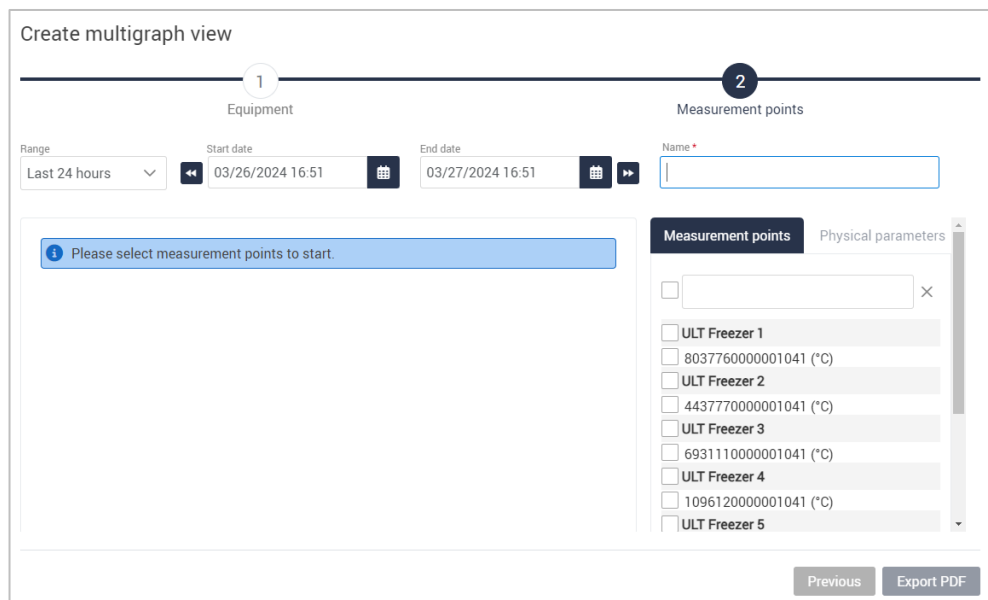
Selected equipment will be used to create the multigraph view.  
Please reset if your access rights to equipment have changed.  
0 piece(s) of equipment selected.

<input type="checkbox"/>	Designation ↑↓	Type ↑↓	Sensors ↑↓	Organization ↑↓	Plan ↑↓
<input type="checkbox"/>	ULT Freezer 1	Samples	2	London	
<input type="checkbox"/>	ULT Freezer 2	Samples	1	London	
<input type="checkbox"/>	ULT Freezer 3	Samples	1	London	
<input type="checkbox"/>	ULT Freezer 4	Samples	1	London	
<input type="checkbox"/>	ULT Freezer 5	Samples	1	London	

Reset Previous Next

Figure 171 – Selecting equipment for multigraph display

3. You can click on **Reset** to clear your selection, or select the desired equipment and click on **Next** to continue:



Create multigraph view

1 Equipment 2 Measurement points

Range: Last 24 hours Start date: 03/26/2024 16:51 End date: 03/27/2024 16:51 Name \*

Please select measurement points to start.

Measurement points Physical parameters

- 
- ULT Freezer 1
- 8037760000001041 (°C)
- ULT Freezer 2
- 4437770000001041 (°C)
- ULT Freezer 3
- 6931110000001041 (°C)
- ULT Freezer 4
- 1096120000001041 (°C)
- ULT Freezer 5

Previous Export PDF

Figure 172 – Selecting date range and measurement points

- Select the desired date and time range:

Here, you may choose a preset range (from 24 hours to 1 month), or enter start and end dates using the calendar icons (📅). Use the arrow buttons (⏪ ⏩) buttons to shift the selected period back or forward in time, with a maximum range of one month.

- Then select the measurement points to include:

Figure 173 – Selecting measurement points for multigraph display

- Click on the top checkbox ① to select all displayed equipment and measurement points, or make individual selections.



You can display up to ten measurement points simultaneously.

- Enter a sensor serial number in the field ② if you want to filter the list. You may click on the ✕ icon to clear the field.

Figure 174 – Filtering by sensor serial number

## Viewing sensor data

- If you have included different sensor types, such as temperature and humidity, the **Physical parameters** tab allows you to select which types you want to display on the fly by clicking on the buttons:

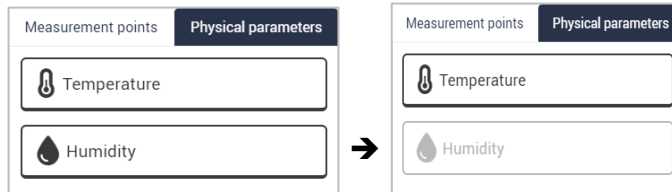


Figure 175 – Filtering by sensor serial number

- Graphs are added as you select measurement points (sensors). Here is an example with three sensor reading curves:

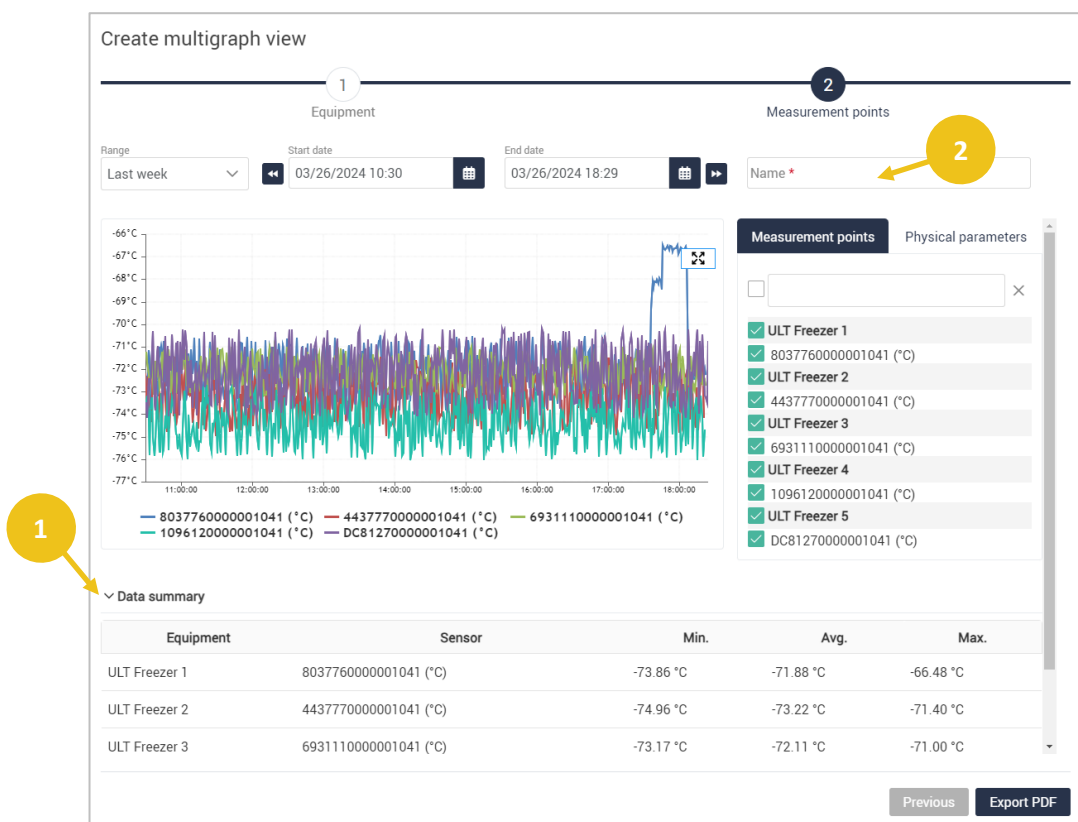


Figure 176 – Superimposed measurement point graphs

- Click on **Data summary** (1) to fold or unfold key details about each sensor, notably the minimum, average, and maximum values.
- To create a report, enter a name for the report in the **Name** field (2), then click on **Export PDF**. The PDF will be generated with the name in your computer's downloads folder.

12. For your convenience, you may click on the sensor numbers beneath the graphs **3** to show them or erase them from the display. Even when hidden from the display, data from the selected sensors will still be included in the summary and report.

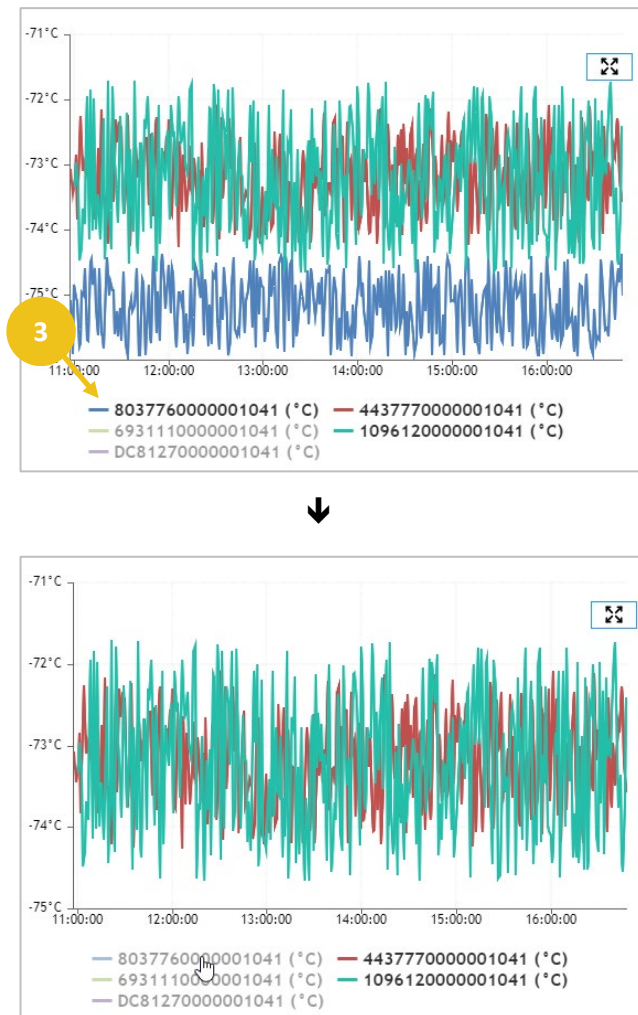


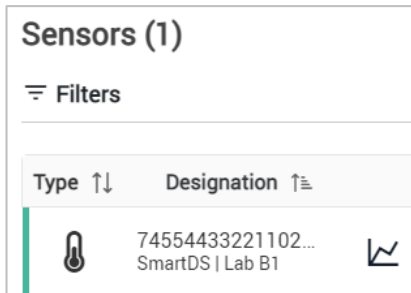
Figure 177 – Superimposed measurement point graphs

Viewing sensor data

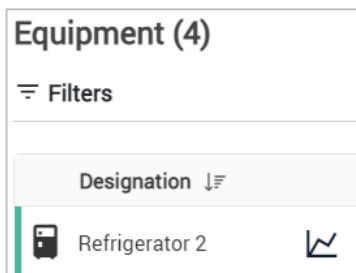
## 13.2 Listing and filtering sensor readings

To display detailed sensor readings:

1. Click on **Readings** (📈) in any of the **Equipment**, **Data loggers**, or **Sensors** screens.



or



or

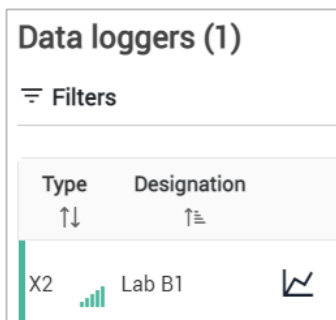
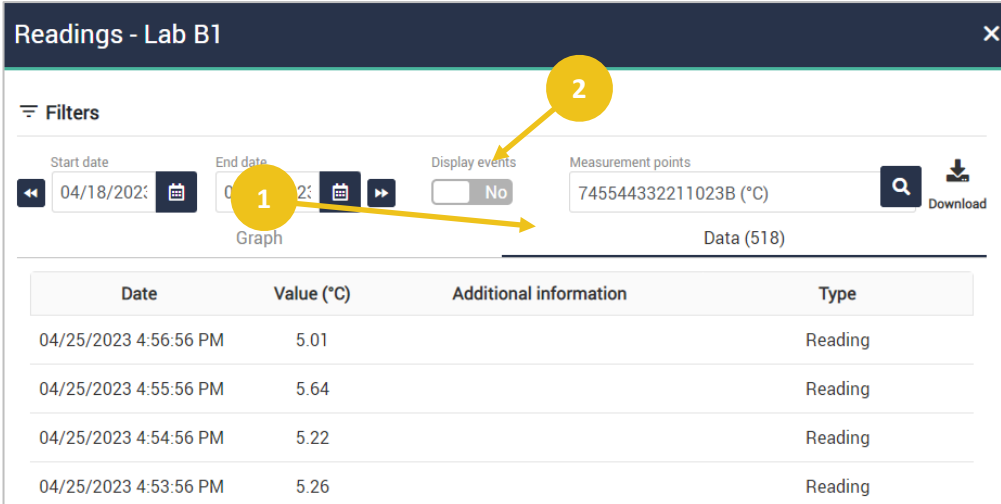


Figure 178 – Accessing sensor data

## Viewing sensor data

2. Click on the Data tab **1**:



The screenshot shows the 'Readings - Lab B1' interface. At the top, there is a 'Filters' section with 'Start date' (04/18/2023) and 'End date' (04/25/2023) selectors, a 'Display events' toggle set to 'No', and a 'Measurement points' search box containing '745544332211023B (°C)'. Below the filters, there are two tabs: 'Graph' and 'Data (518)'. The 'Data' tab is active, displaying a table with the following data:

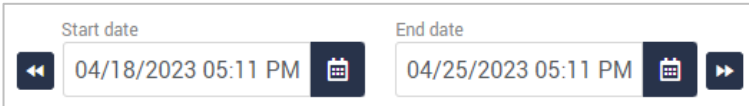
Date	Value (°C)	Additional information	Type
04/25/2023 4:56:56 PM	5.01		Reading
04/25/2023 4:55:56 PM	5.64		Reading
04/25/2023 4:54:56 PM	5.22		Reading
04/25/2023 4:53:56 PM	5.26		Reading

Figure 179 – List of readings/events

3. You may include the list of events for the selected sensor using the **Display events (Yes/No)** toggle button **2**.

The table includes the following information:

- Event date
  - Reading value
  - Event details
  - Event type
4. You may use the date range selector to adjust the dates for displaying events. The date range must not exceed one month.



The screenshot shows the date range selector with 'Start date' (04/18/2023 05:11 PM) and 'End date' (04/25/2023 05:11 PM). Navigation arrows are visible on both sides of the date inputs.

Figure 180 – Selecting the date range for displayed data

Use the right and left arrow buttons ( **◀** and **▶** ) to move forwards or backwards through the calendar.

## 14 Generating reports

OCEAView enables you to create list reports for the various elements of your solution. This includes downloading data as well as managing a review and approval process with electronic signatures.

### 14.1 Downloading reports

Many screens in the application offer a **Download** button (  ) <sup>1</sup>, notably those presenting lists of equipment, sensors, alarms, etc..

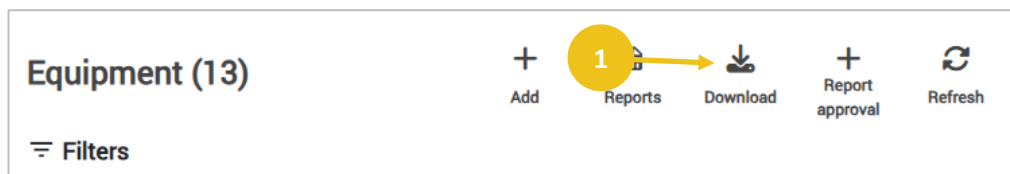









Figure 181 – Data download tools

Several file format options are displayed when you click on the download button. Depending on the context, the available options are:

<b>Excel (.xlsx)</b>	Creates an XLSX format file that you can open with Microsoft Excel, including summary and detailed sensor data.
<b>PDF (.pdf)</b>	Creates a complete PDF file of the information displayed on the screen, including summary and detailed sensor data.
<b>PDF - Summary (.pdf)</b>	Creates a two-page PDF file with summary information about the sensor, but not the detailed data.
<b>Word (.docx)</b>	Creates a DOCX format file that you can open with Microsoft Word, including summary and detailed sensor data.
<b>Data (.txt)</b>	Creates a text file in CSV format with detailed sensor readings.

The following table indicates the report format options available in the different sections of the application:

Application screen	MS Excel (.xlsx)	.CSV	PDF	PDF summary pages only	MS Word (.docx)	Data (.txt)
Equipment list (  )	X		X		X	
Alarms (  )	X		X		X	X
Audit trail (  )	X		X		X	
Data logger list (  )	X		X		X	X
Sensor list (  )		X				
Sensor readings (  )	X		X	X	X	X
Infrastructure list (  )	X		X		X	




### 14.1.1 Sensor reading reports

This section describes the different options for creating sensor reports. These reports are described in detail in *Appendix 1 – Sensor reading report details, p. 259*.



If you plan to generate several copies of your report in different file formats, or multiple different reports, make sure your browser is not configured to block multiple downloads from the site.

To create a sensor report:

1. Click on **Readings** (  ) in any of the Equipment, Data loggers, or Sensors screens to open the sensor readings screen described in the previous section.
2. The default date range covers the past week. You may use the filters to select a different date range, then click on  to apply the change.
3. Click on **Download** (  ) and choose from the available options:

**Excel (.xlsx)**

Creates an XLSX format file that you can open with Microsoft Excel. The file includes a summary and the sensor data

**PDF (.pdf)**

Creates a complete PDF file of the information displayed on the screen, including detailed sensor data.

**PDF – Summary (PDF)**

Creates a two-page PDF file with summary information about the sensor, but not the data.

**Word (.docx)**

Creates a DOCX format file that you can open with Microsoft Word, including a summary and the sensor data.

**Data (.txt)**

Creates a text file in CSV format.

```
Sensor S/N;YYYY-MM-DDThh:mm:ss (UTC);Value;Unit;Status
370000095CED1028;2021-08-17T10:00:42Z;24.70;°C;
370000095CED1028;2021-08-17T10:01:42Z;24.70;°C;
370000095CED1028;2021-08-17T10:02:42Z;24.70;°C;
370000095CED1028;2021-08-17T10:03:42Z;24.70;°C;
370000095CED1028;2021-08-17T10:04:42Z;24.70;°C;
370000095CED1028;2021-08-17T10:05:42Z;24.75;°C;
370000095CED1028;2021-08-17T10:06:42Z;24.70;°C;
```

Figure 182 – Sample CSV report with sensor data

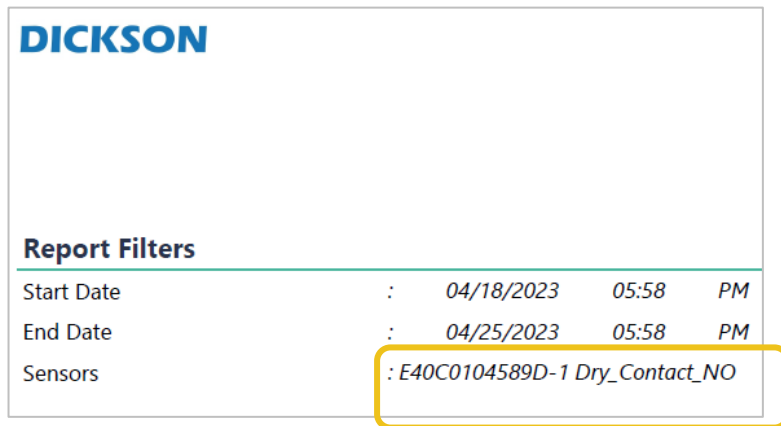


Figure 183 – Sample report with summary pages and sensor data

### 14.1.2 Dry contact input sensor report

When downloading readings in Excel, PDF, or Word format for dry contact input sensors, the sensor serial number has a suffix of "-1" or "-2".

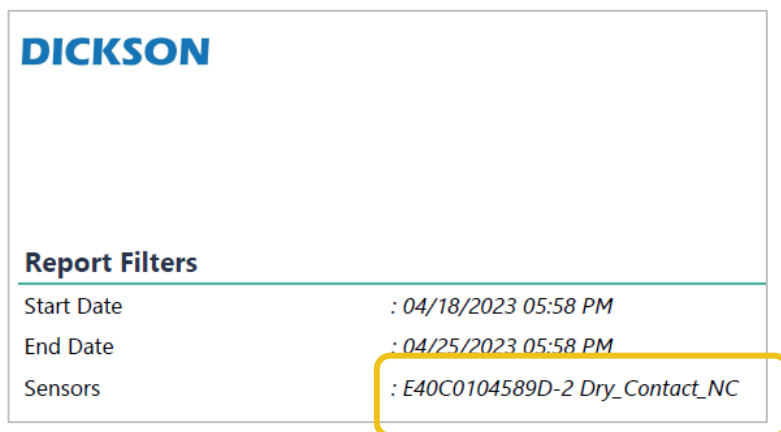
As indicated below, Normally Open (NO) corresponds to the "-1" suffix, and Normally Closed (NC) corresponds to "-2".



The screenshot shows a report filter table for a DICKSON sensor. The table has a header 'Report Filters' and three rows of data. The 'Sensors' row is highlighted with a yellow box and shows the sensor ID 'E40C0104589D-1' followed by the suffix 'Dry\_Contact\_NO'.

DICKSON			
Report Filters			
Start Date	:	04/18/2023	05:58 PM
End Date	:	04/25/2023	05:58 PM
Sensors	:	E40C0104589D-1 Dry_Contact_NO	

or



The screenshot shows a report filter table for a DICKSON sensor. The table has a header 'Report Filters' and three rows of data. The 'Sensors' row is highlighted with a yellow box and shows the sensor ID 'E40C0104589D-2' followed by the suffix 'Dry\_Contact\_NC'.

DICKSON			
Report Filters			
Start Date	:	04/18/2023	05:58 PM
End Date	:	04/25/2023	05:58 PM
Sensors	:	E40C0104589D-2 Dry_Contact_NC	

Figure 184 – Dry contact input sensor serial number with suffix in report

## 14.2 Reviewing and approving reports

OCEAView enables users to create PDF reports with a review and approval cycle. These reports are stored directly in the OCEAView platform. Authorized users can then access the reports to review or approve them by signing with their system password. All actions related to reports are included in the audit trail.

### Key points about the review and approval workflow:


- If the Review/Approve Reports feature is activated for your company (accessible to Application Managers in **Company** → **Report compliance**), then any user belonging to an organization node in common with the target of the report (i.e. equipment, data logger, etc.) can create a report for review and approval.
- You cannot review or approve a report you created, but you can reject one.
- If your individual user profile does not allow you to manage reviews and approvals (in **My account** → **More** → **Show application permissions**), you will only see reports that you created.

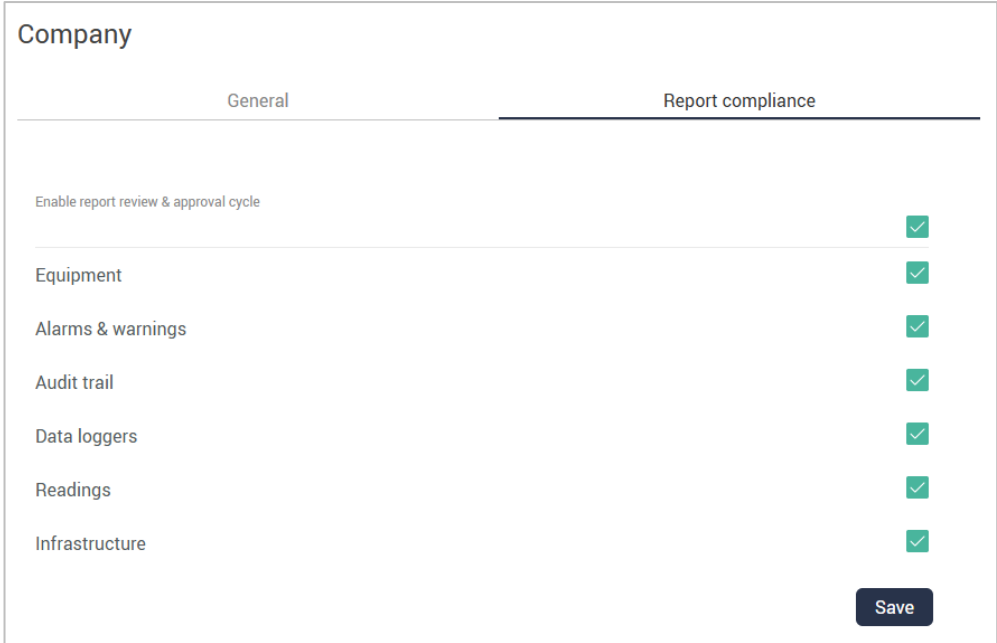
Application Managers and users specifically allowed to manage and review reports will see all reports.

- Report review/approval requires three different users to complete the cycle: one to create the report, one to review it, and one to approve it.
- Reviewed and approved reports are stored in the system and are completely secure and unalterable.

### 14.2.1 Activating report review/approval for your company

To activate this feature for your company:

1. Click on **Configuration** (  ) → **Company** → **Compliance**




General	Report compliance
Enable report review & approval cycle <input checked="" type="checkbox"/>	
Equipment	<input checked="" type="checkbox"/>
Alarms & warnings	<input checked="" type="checkbox"/>
Audit trail	<input checked="" type="checkbox"/>
Data loggers	<input checked="" type="checkbox"/>
Readings	<input checked="" type="checkbox"/>
Infrastructure	<input checked="" type="checkbox"/>

Save

Figure 185 – Select the items for which you want to enable report approval/review

## Generating reports

- The pages corresponding to the items you select here will then have a Report approval icon  in the upper right-hand corner:

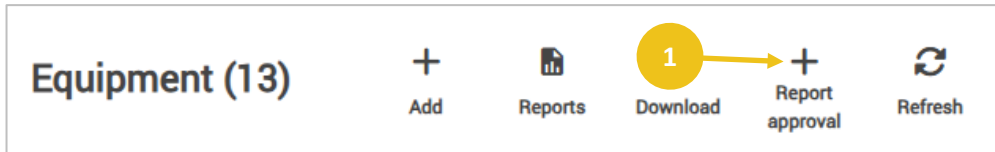


Figure 186 – Icon showing that review/approval is available in this section

Users currently logged in to the system will see the additional functionality next time they log in.

- Press **Save** when done.

## 14.2.2 Generating, reviewing, and approving reports



All application managers can access report review and approval functions. Other users, however, must be authorized to review and/or approve reports in their individual application permissions settings, as described in section 5.3.1 – *Assigning application permissions to “User” profile accounts, p. 72.*

### Creating a report (first user)

- Before you begin, remember that you may use filters to determine the contents of your report. The items displayed on the screen are those that will be contained in the report.

In this example, the text “C.3” is entered in the **Search** field ( 1 ) to specifically target this piece of equipment.

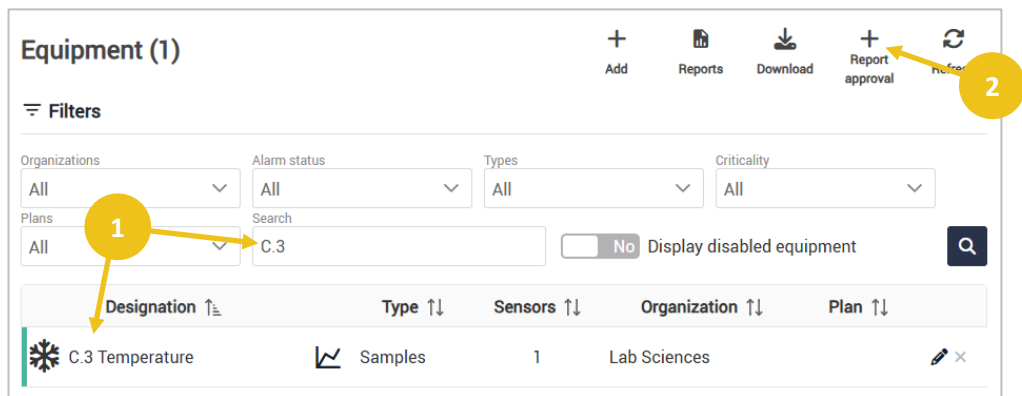


Figure 187 – Click to create a report

- To start the report review/approval cycle, click on the **Report approval** icon ( 2 ) in the upper right-hand corner of the screen:
- Enter a name for the report, then press **Send**.

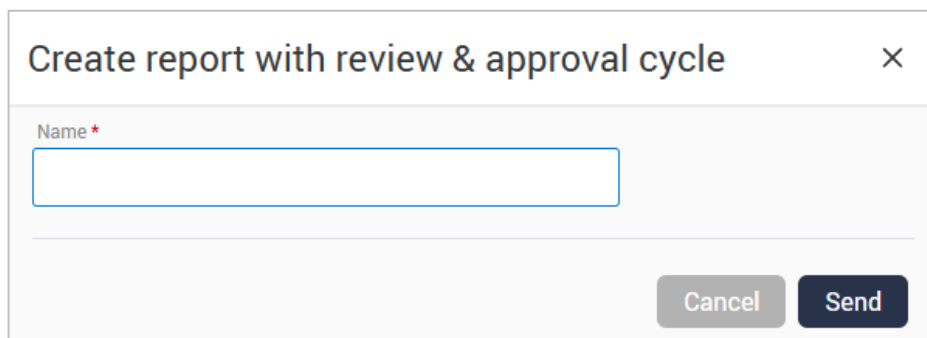


Figure 188 – Name the report

- This creates and stores the report in PDF format, which you may access by selecting **Reports** ( 📄 ) → **Review & approval** → **View** ( 3 )

## Generating reports

The screenshot illustrates the 'Review & approval (1)' interface. At the top, there is a 'Refresh' button. Below it, a 'Filters' section is visible. The main table lists reports with columns for Name, Type, Creation date, Date range, Status, and Actions. A yellow callout '3' points to the 'View' button in the Actions column for the 'C.3 Temp Report'.


Name ↑↓	Type	Creation date ↓	Date range ↑↓	Status	Actions
C.3 Temp Report	Equipment	14/01/2025	-	Pending review	<a href="#">View</a>

Below the table, a downward arrow indicates the next step. The detailed view of the 'C.3 Temp Report' is shown. It includes a 'Back to list' link, the DICKSON logo, and the report title 'C.3 Temp Report'. A yellow callout '4' points to the 'Reject report' button. The report content is displayed in a preview window, showing a table titled 'Equipment listing' with columns for Type, Name, Inventory Code, Organization, Data Logging, Alarm Status, Disabled, Criticality, and Sensors. The table contains one row of data for 'C.3 Temperature'.

Type	Name	Inventory Code	Organization	Data Logging	Alarm Status	Disabled	Criticality	Sensors
Samples	C.3 Temperature		Lab Sciences	Monitoring	No Alarm	0	0	1

Additional details on the right side of the report view include the Status (Pending review), Created by (Mark Jones), Created on (1/14/2025 at 06:26 PM), Report type (Equipment), and a Download PDF button. An Activity section shows that Mark Jones created the report 2 minutes ago.

Figure 189 – PDF reports are stored and accessible in the system

As the creator of the report, you may not sign a report as reviewed or approved, but you can reject it if necessary by clicking on **Reject** (  ). You can also download the file by clicking on **Download PDF**.

### Reviewing a report (second user)

The next step in the cycle is for a different user to review the report and sign it as reviewed, or reject it.

Users with permission to review reports will see notification in the upper right-hand corner of the screen:

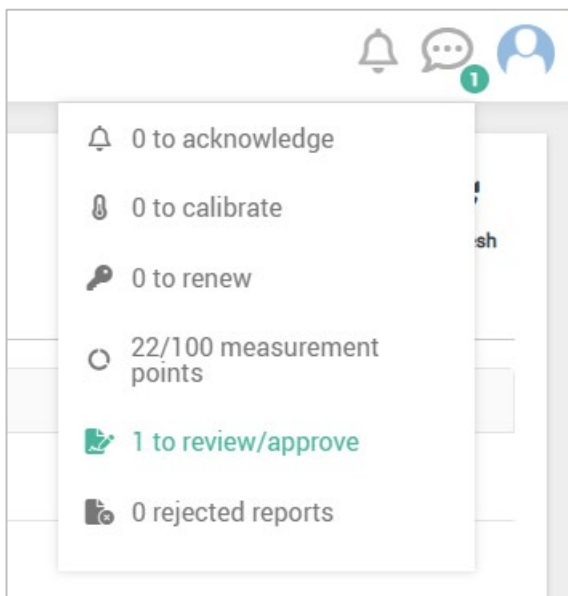


Figure 190 – Users are notified when reports are ready for review

### To review a report:

1. Access reports to be reviewed either by clicking on the notification menu (as shown above), or select **Reports** (📄) → **Review & approval**

After a report is generated, it is shown with “**Pending review**” in the list:

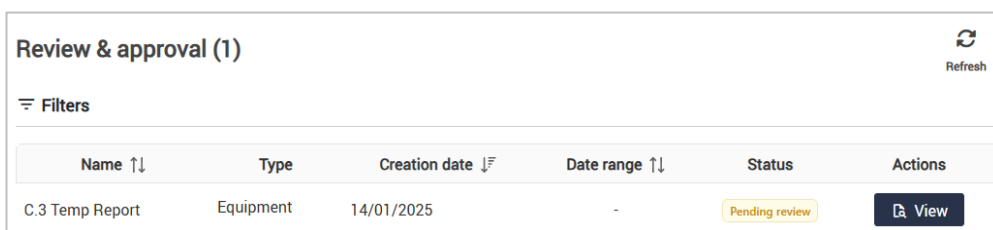


Figure 191 – Report is pending review

2. Click on **View**
3. The report opens with a **Mark as reviewed** button (🟡):

## Generating reports

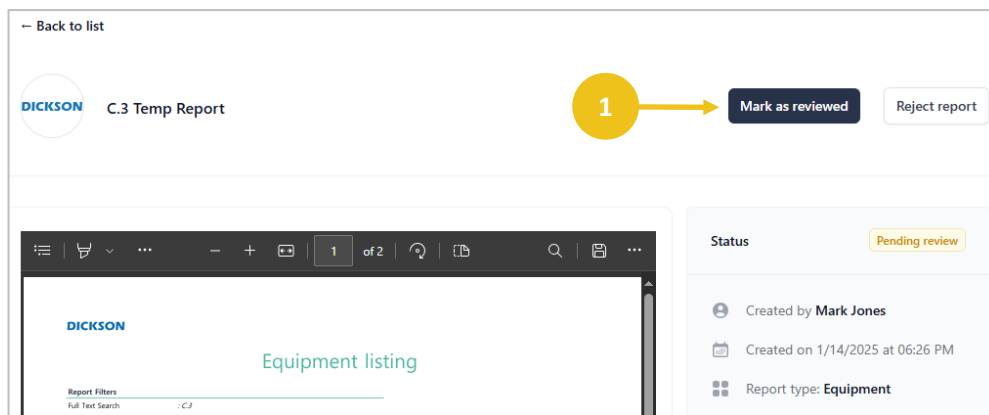


Figure 192 – The report is ready for review

4. You may check the contents of the report directly in the interface, or download the file PDF to read it locally.
5. If you are satisfied with the report, click on **Mark as reviewed** to enter your system password (which is used to create an electronic signature in your name on the report).

You can reject the report by clicking on **Reject**.

### Approving a report (third user)

The final step is for a different user to approve the report and sign it as approved, or reject it. The report must be approved by a different user, as you cannot both review and approve a report.

Users with permission to approve reports will see notification in the upper right-hand corner of the screen:

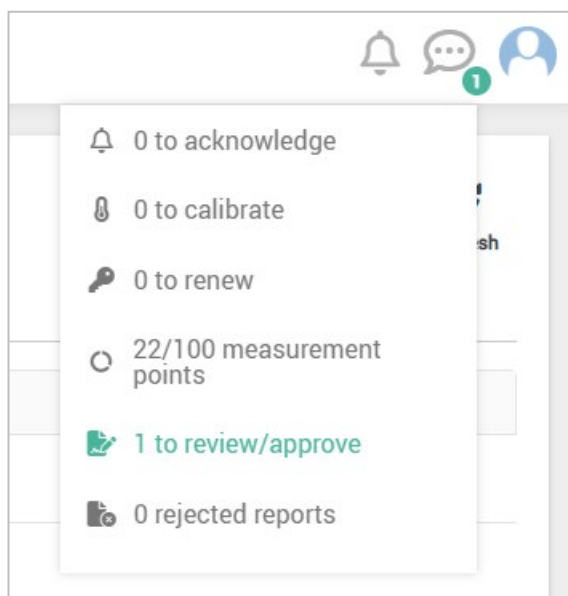



Figure 193 – Users are notified when reports are ready for approval

## Generating reports

1. Access reports to be reviewed either by clicking on the notification menu (as shown above), or select **Reports** (  ) → **Review & approval**  
After a report is reviewed, it is shown with “Pending approval” in the list:



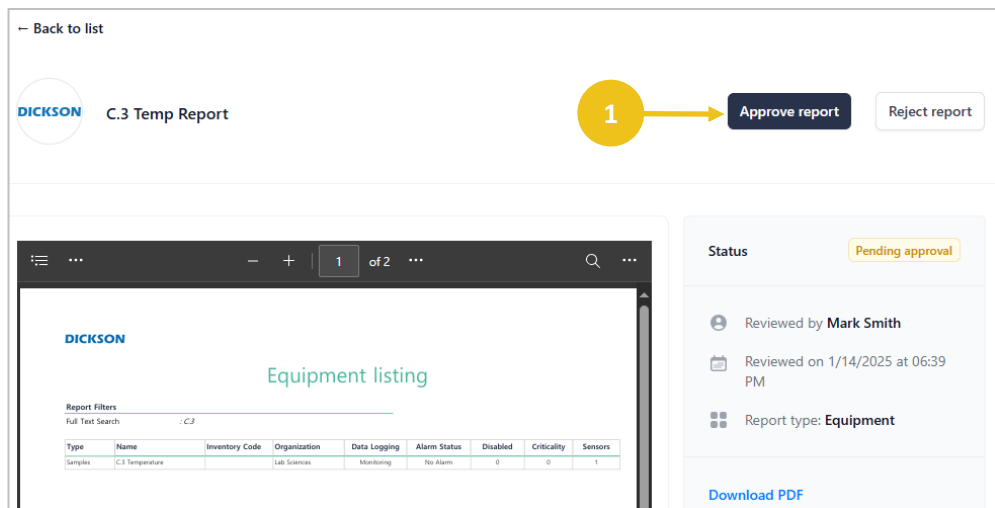
**Review & approval (1)** Refresh

Filters

Name ↑↓	Type	Creation date ↓	Date range ↑↓	Status	Actions
C.3 Temp Report	Equipment	01/14/2025	-	Pending approval	<a href="#">View</a>

Figure 194 – The report is ready for approval

2. Click on **View**
3. The report opens with an **Approve report** button (  ):



Back to list

**DICKSON** C.3 Temp Report **1** → Approve report Reject report

Status Pending approval

Reviewed by **Mark Smith**

Reviewed on 1/14/2025 at 06:39 PM

Report type: **Equipment**

[Download PDF](#)

Equipment listing

Report Filters

Full Text Search

Type	Name	Inventory Code	Organization	Data Logging	Alarm Status	Disabled	Criticality	Sensors
Samplex	C.3 Temperature		Lab Sciences	Monitoring	No Alarm	0	0	1

Figure 195 – Click to approve the report

4. You may check the contents of the report directly in the interface, or download the file PDF to read it locally.
5. If you are satisfied with the report, click on **Approve report** to enter your system password (which is used to create an electronic signature in your name on the report).  
You can reject the report by clicking on **Reject**.

### 14.2.3 Accessing archived reports

You can access reviewed, approved, and rejected reports at any time by selecting **Reports** (🏠) → **Review & approval** → **View**

Reports that have gone through the approval cycle contain information regarding the process.

The archived PDF contains the names of the users who generated, reviewed, and approved the report (having signed their action with their system password).

The screenshot displays the 'C.3 Temp Report' interface. At the top, there is a 'Back to list' link and the DICKSON logo. The main content area shows a preview of the report titled 'Equipment listing' with a table of data. The table has columns for Type, Name, Inventory Code, Organization, Data Logging, Alarm Status, Disabled, Criticality, and Sensors. The data row shows 'Temp', 'C.3 Temperature', 'Lab Services', 'Monitoring', 'No Alarm', '0', '9', and '1'. Below the table, it says 'Created by Mark Jones (michael.mcg@lab-services.com)'. To the right of the report preview, there is a 'Status' section with a green 'Approved' badge, 'Approved by Martin Miller', 'Approved on 1/14/2025 at 06:44 PM', and 'Report type: Equipment'. Below that is a 'Download PDF' button. At the bottom left, there is an 'Activity' section with three entries: 'Martin Miller approved the report.' (1 min. ago), 'Mark Smith reviewed the report.' (6 min. ago), and 'Mark Jones created the report.' (19 min. ago). A yellow arrow points from the 'Approved' status to the 'Approval' entry in the activity log.

**Generation**  
By Mark Jones  
On 14/01/2025 06:26 PM

**Review**  
By Mark Smith  
On 14/01/2025 06:39 PM

**Approval**  
By Martin Miller  
On 14/01/2025 06:44 PM

Figure 196 – Electronic signatures and details permanently added to the report

## 14.3 Alarm report subscriptions

OCEAView can generate reports automatically for the following items and send them at programmed intervals:


- Equipment
- Alarms
- Audit trail
- Data loggers
- Sensors
- Infrastructure



Users with Application Manager rights can assign reports to be sent to other users, whereas regular Users can only create reports for themselves, without being able to assign them to other users.

### 14.3.1 Scheduling a report

To schedule a report and assign users:

1. Go to one of the pages mentioned above and apply any filters you may want to use for your report. The report is created using the selection criteria in your filters.
2. Click on **Reports** (  ) in the upper right-hand corner of the screen:

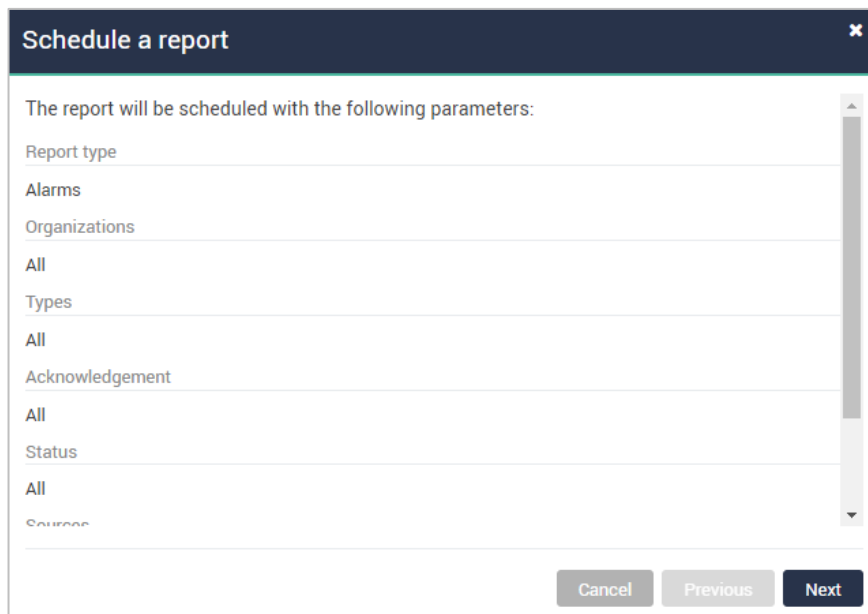


Figure 197 – Report parameters (example for Alarms)

3. Click on **Next** and edit details for the report:

Figure 198 – Set up the report to meet your needs

**Name** Enter a name to refer to this report.

**Periodicity** Select whether the report should be produced on a weekly or monthly basis.

**Weekly:** select one or more days to generate the report:

Figure 199 – Report printed on selected days every week

**Monthly:** select the day of the month to print the report:

Figure 200 – Report printed on specified day once a month

**At** Indicate the time for the report to be produced.

**Data range** For alarm/warning and Audit Trail reports, specify the time period for which you want to include data (from “Previous 7 days” to “Previous month”).

4. People with "User" rights in the system can only create reports for themselves, so they must click on **Save** at this point, or **Previous** to return to the scheduling screen, or **Cancel** to close the window without saving changes.
5. People with "Application Manager" rights can have reports sent to other users, and must click on **Next** to select the users (including themselves) to receive the report in PDF format via e-mail:

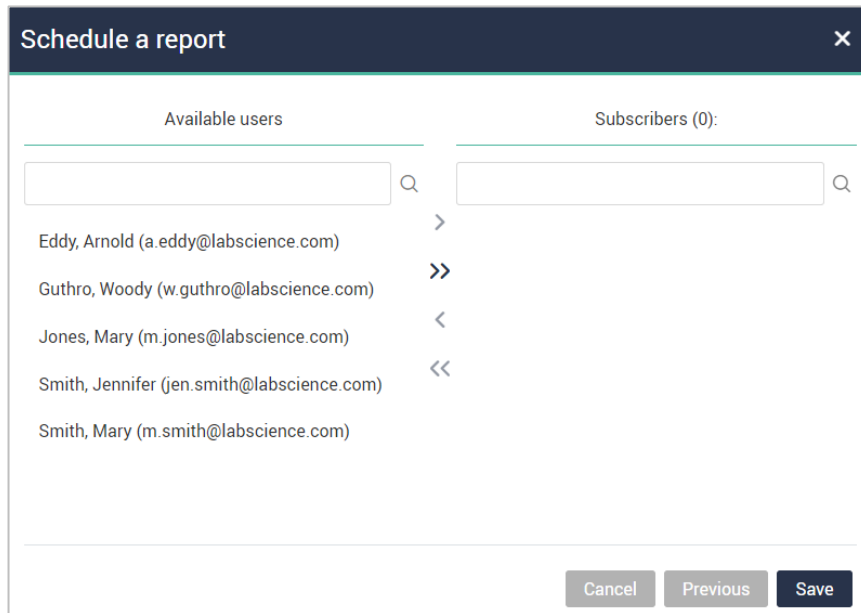


Figure 201 – Include users in report distribution

**To add users:**

Double-click on a username or click on **>** to move the selected user from **Available** to **Subscribers**.

To select multiple users at a time, press and hold the **Ctrl** key and click on each of the users you want to select. Click on **>** to add them to the list of **Subscribers**.

To select all available users, click on **>>**.

**To remove users:**

To remove a user from a report, double-click on a username in the list of **Subscribers** (right-hand side) or click on a user and click on **<** to move the user to the list of **Available** users on the left-hand side.

To remove multiple users, press and hold the **Ctrl** key and, while holding down the key, click on the other users you want to remove. Click on **<** to move them to the list of **Available** users on the left.

To remove all users, click on **<<**.

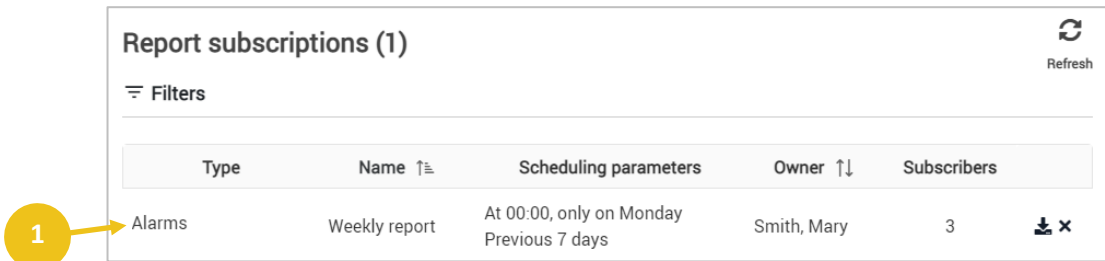
6. Click on **Save** when done, on **Previous** to return to the scheduling screen, or on **Cancel** to close the window without saving your changes.

### 14.3.2 Editing scheduled reports and subscriptions

You may edit and update reports that you have created (as described in the previous section) and reassign users to those reports.

To modify a report:

1. Click on Reports (  ) → Report subscriptions









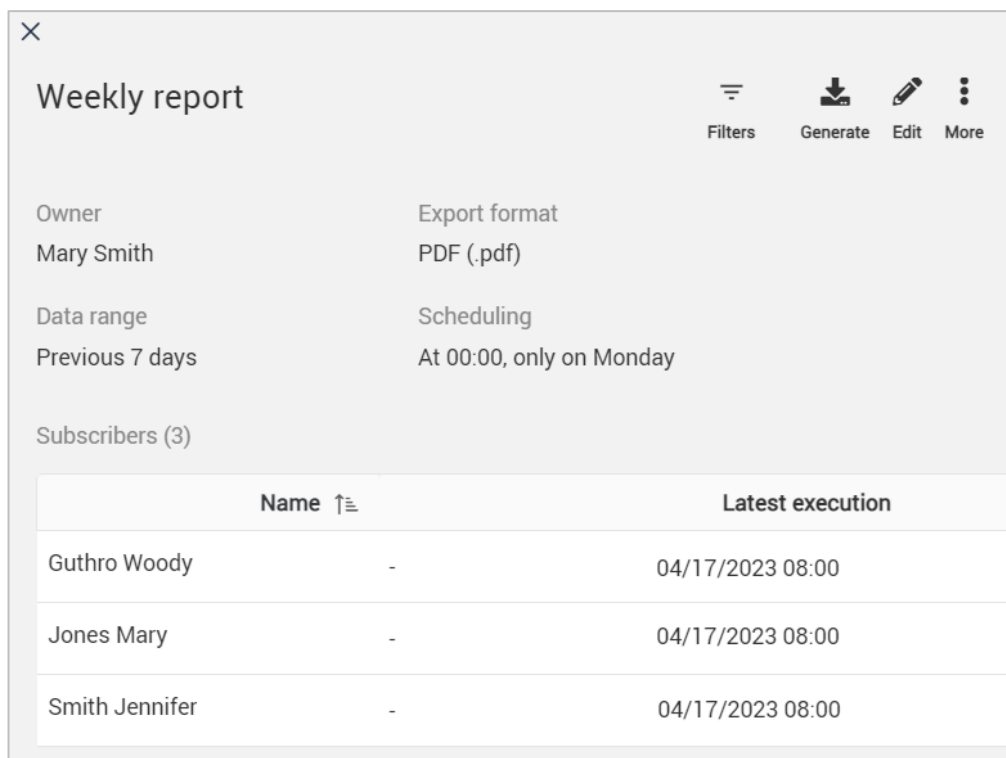
Type	Name ↑	Scheduling parameters	Owner ↑↓	Subscribers	
Alarms	Weekly report	At 00:00, only on Monday Previous 7 days	Smith, Mary	3	 

Figure 202 – Include users in report distribution



Note: the user who created the report is indicated as the “Owner”. You may change the owner via **More** (  ) as described below.









2. To run the report right now, click on 
3. To delete the report, click on 
4. For further report configuration, click on the line with the report .



Weekly report	
Owner	Export format
Mary Smith	PDF (.pdf)
Data range	Scheduling
Previous 7 days	At 00:00, only on Monday
Subscribers (3)	
Name ↑	Latest execution
Guthro Woody	04/17/2023 08:00
Jones Mary	04/17/2023 08:00
Smith Jennifer	04/17/2023 08:00

Figure 203 – Report summary screen

This screen contains several options for managing the report:

	<p><b>Filter</b> – Displays the parameters used to filter data and establish the report.</p>
	<p><b>Generate the report</b> – You may click on this icon to generate the report at any time.</p>
	<p><b>Edit</b> – Enables you to change scheduling options for the report. The options here are the same as those used to create the report (as described in the previous section).</p>
	<p><b>Options</b> – Contains the following items:</p> <ul style="list-style-type: none"> <li data-bbox="555 636 1398 808">  <p><b>Change owner</b> – The report owner is allowed to manage report details. If the report is assigned to multiple subscribers, ownership may only be assigned to another Application Manager. A User profile cannot be the owner of a report that is sent to other people.</p> </li> <li data-bbox="555 824 1398 898">  <p><b>Edit subscribers</b> – Allows Application Managers to edit the list of users who receive the report via e-mail.</p> </li> <li data-bbox="555 913 1398 1086">  <p><b>Disable</b> – Deactivates automatic generation of the report. You may <b>Enable</b> the report subsequently if you want (to show reports that have been disabled, open <b>Filters</b> at the top of the screen and select “<b>Show inactive</b>”)</p> </li> <li data-bbox="555 1102 1398 1176">  <p><b>Remove</b> – Completely removes the report from the system.</p> </li> </ul>




## 14.4 Audit trail

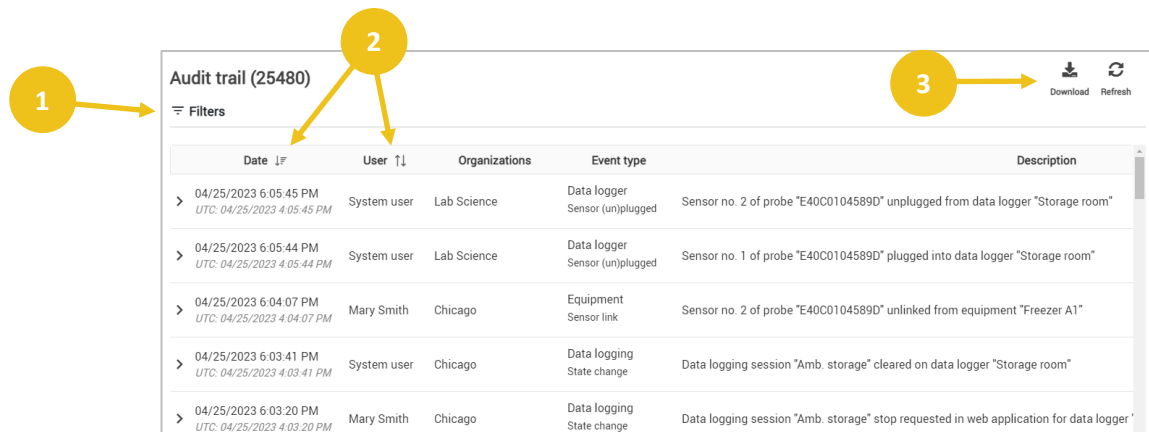
The audit trail is a key feature for traceability in equipment monitoring solutions, notably with respect to regulatory requirements, such as FDA 21 CFR Part 11 guidelines. OCEAView tracks every system action in a non-modifiable list that provides complete details about system events, such as:

- Alarms
- User login and logout
- Configuration changes
- New equipment, data loggers, and sensors
- Profile updates
- Alert rule creation, modification, and testing
- Data logging start and stop
- System messages
- Password changes
- Application version updates
- Etc.

To view your system's audit trail:

1. Click on Reports (  ) → Audit trail
2. Here you may click on:

- 1 **Filters:** to open filter options and refine the display by choosing the types of information you want to see.
- 2 **Sort:** click on the icons to sort by **Date** (  or  ) or **User name** (  ):
- 3 **Download:** to download an XLSX, PDF, or DOCX version of the displayed list.



**Audit trail (25480)**

Filters

Date	User	Organizations	Event type	Description
04/25/2023 6:05:45 PM UTC: 04/25/2023 4:05:45 PM	System user	Lab Science	Data logger Sensor (unplugged)	Sensor no. 2 of probe "E40C0104589D" unplugged from data logger "Storage room"
04/25/2023 6:05:44 PM UTC: 04/25/2023 4:05:44 PM	System user	Lab Science	Data logger Sensor (unplugged)	Sensor no. 1 of probe "E40C0104589D" plugged into data logger "Storage room"
04/25/2023 6:04:07 PM UTC: 04/25/2023 4:04:07 PM	Mary Smith	Chicago	Equipment Sensor link	Sensor no. 2 of probe "E40C0104589D" unlinked from equipment "Freezer A1"
04/25/2023 6:03:41 PM UTC: 04/25/2023 4:03:41 PM	System user	Chicago	Data logging State change	Data logging session "Amb. storage" cleared on data logger "Storage room"
04/25/2023 6:03:20 PM UTC: 04/25/2023 4:03:20 PM	Mary Smith	Chicago	Data logging State change	Data logging session "Amb. storage" stop requested in web application for data logger

Download Refresh

Figure 204 – Audit trail

## Generating reports

- The header fields show the event Date, User, Type, and a Description. You may sort the list by Date or User by clicking on those headers with your mouse.
- You may expand any event item by clicking on the arrow ( > ) **3** to show complete details, as shown here:

**Audit trail (25480)** Download Refresh

Filters

04/25/2023 3:39:58 PM System user Singapore Alarm Creation Alarm # 7605: limit 8.00 °C exceeded (8.10 °C) on equipment "Refrigerator 2" (data logging "Refrigerator 2")  
UTC: 04/25/2023 1:39:58 PM

**Details**

- Alarm identifier: 7605
- Data logger: Lab B1
- Data logger S/N: E40C0104571C
- Data logging: Refrigerator 2
- Equipment: Refrigerator 2
- Limit value: 8.00 °C
- Physical parameter: Temperature
- Probe S/N: 745544332211023B
- Sensor number: 1
- Trigger value: 8.10 °C

Property name	Old value	New value
Alarm identifier	7605	
Creation date	04/25/2023 03:39:58 PM	
Start date	04/25/2023 03:39:56 PM	
Type	High limit - Level 2	

Figure 205 – Complete details for a specific event

For some audit trail items, the **Old value** and **New value** fields **4** show information that has changed:

04/25/2023 3:28:51 PM System user User Log in User "Mary Smith" logged in  
UTC: 04/25/2023 1:28:51 PM

**Details**

- E-mail: m.smith@labscience.com
- Name: Mary Smith

Property	Old value	New value
Last connection	04/25/2023 02:23 PM	04/25/2023 03:28 PM

Figure 206 – Old and new values shown when relevant

### 14.4.1 Exporting the audit trail

As described above in section 14.1 – *Downloading reports* (p. 205), you may also download audit trail information in XLSX, PDF, or DOCX format. Here is a sample first page from a PDF download:

**DICKSON**
Audit Trail

---

**Report Filters**

Start Date : 04/18/2023 06:48 PM  
 End Date : 04/25/2023 06:48 PM

**04/25/2023 06:05:45 PM - System user**  
**Data logger > Sensor (un)plug > Sensor no. 2 of probe "E40C0104589D" unplugged from data logger "Storage room"**

Details:	Property	Old value	New value
<b>Connection type</b> : Internal	Unplugged on		04/25/2023 06:05 PM
<b>Data logger</b> : Storage room			
<b>Data logger S/N</b> : E40C0104589D			
<b>Physical parameter(s)</b> : Dry contact NC			
<b>Plugged in on</b> : 03/28/2023 10:31 AM			
<b>Probe S/N</b> : E40C0104589D			
<b>Sensor number</b> : 2			
<b>Type</b> : Internal sensor			
<b>Organizations</b> :			
Lab Science			



Created by Mary Smith (m.smith@labscience.vom)
1/173
04/25/2023 06:48 PM (GMT +02:00)

Figure 207 – Downloading an audit trail report

### 14.4.2 Filtering the audit trail

When looking at the audit trail, you may wish to filter the display to see specific events that meet certain criteria.

To filter the list:

1. Click on Filters (  ) and select the filter(s) you would like to apply (  ):

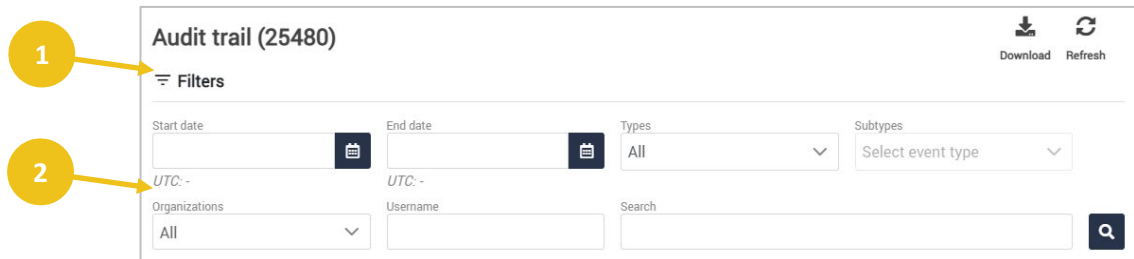





Figure 208 – Filtering the audit trail display

The available filters are as follows (click on the magnifying glass button (  ) to apply:

Filter option	Description
<b>Start date</b>	Indicate the date and time at which you would like the list to start. The maximum date range is one month.
<b>End date</b>	Indicate the date and time at which you would like the list to end. The maximum date range is one month.
<b>Organizations</b>	By default, this is set to <b>All</b> , to display all events across your entire organization.  You may type the first characters or full name of the organizational node(s) you are looking for and or scroll through the pull-down menu to select the organizational node(s) you want.
<b>Username</b>	You may type the first characters or full name of the User associated with the event.
<b>Types</b>	By default, this is set to <b>All</b> , to display all entries.  The pull-down list contains many options, such as <b>Alarm</b> , <b>Alert rule</b> , <b>Authentication mode</b> , <b>Company</b> , and more.
<b>Subtypes</b>	By default, this is set to <b>All</b> , to display all event subtypes.  You may specify various criteria related to your choice for <b>Types</b> .
<b>Search</b>	You may enter text to use as search criteria.

## Generating reports

2. Apply filters by clicking on the magnifying glass (  ).
3. You may clear all applied filters by clicking on **Refresh** (  ). Filters are also reset to their default settings when you refresh the page (pressing the F5 key in most browsers) or when you go to another page in the application.

## 15 Alarms & alerts

The OCEAVIEW monitoring system features an alert mechanism that notifies you if your sensors go outside their expected range or if some type of technical error occurs. For example, if a temperature sensor is configured to monitor a cold-storage unit between 2°C and 8°C, and the sensor reads a temperature of 9°C, then an alarm is shown in OCEAVIEW. The system can also send an alert to one or more users if an alarm is detected. It is therefore important to understand the distinction between alarms and alerts.

### 15.1 Handling alarms

#### 15.1.1 Alarms highlighted in the watch mode screen

Alarms are visible throughout OCEAVIEW, wherever sensors and equipment are displayed. Typically, the first place you will see visual indication of an alarm is in the **Watch mode** screen.

When there are no errors, the equipment tile color is green and **Normal** is displayed. Here is a “healthy” system dashboard and equipment details window:

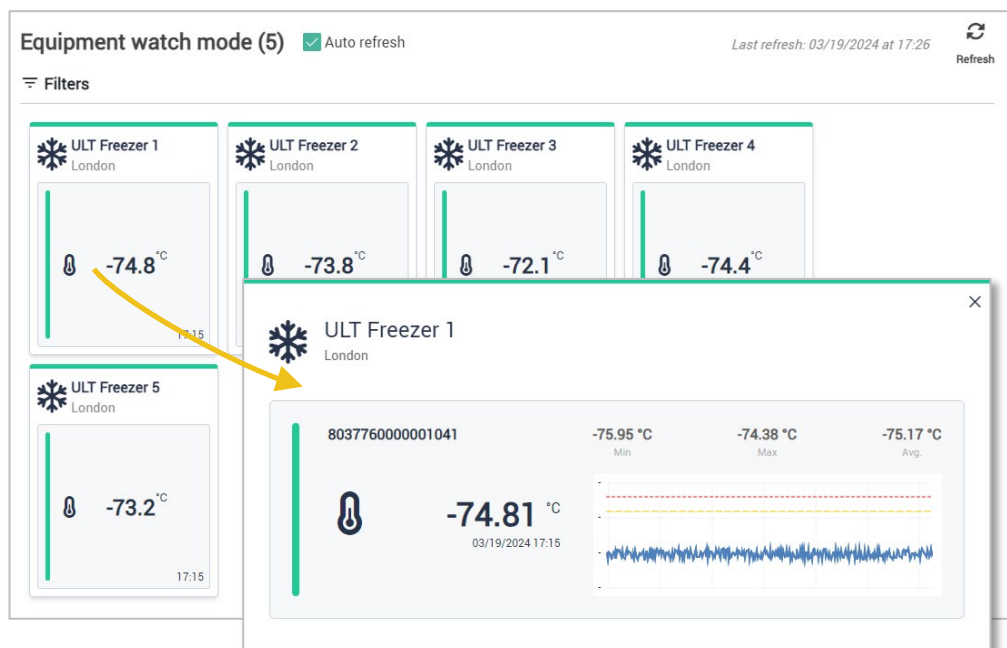


Figure 209 – Watch mode screen and equipment details with no alarms

## Alarms & alerts

When an alarm occurs, the equipment's color code changes from **green** to **red** for excursions and technical problems, or **orange** for warnings, which do not require acknowledgment.

The alarm indicators **1** show:

- On the main screen, the number of pieces of equipment currently with an alarm
- On the equipment details screen, the type of alarm

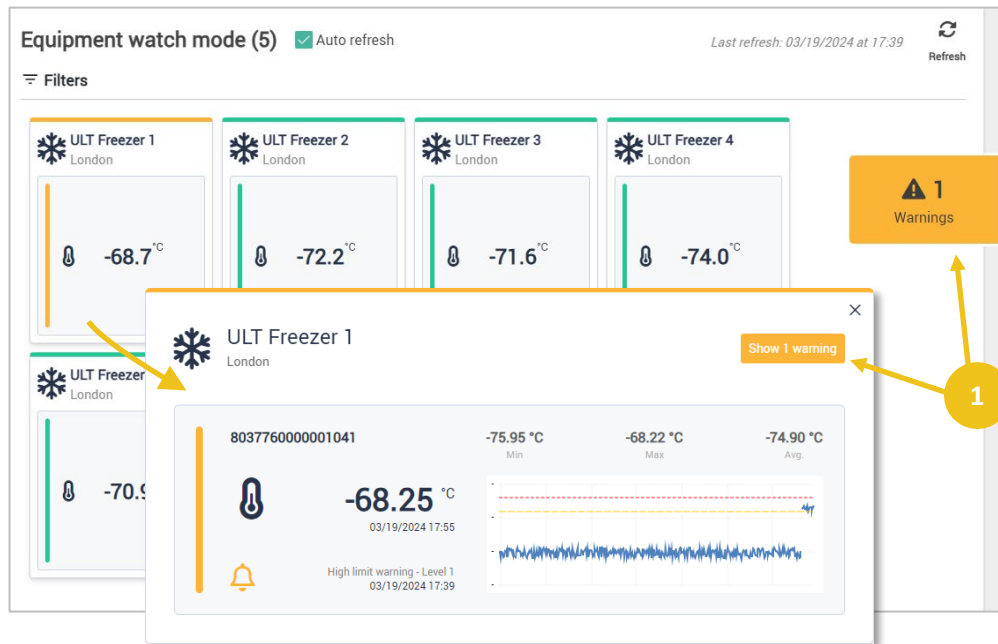


Figure 210 – Dashboard and equipment details with a limit **warning**

Alarms & alerts

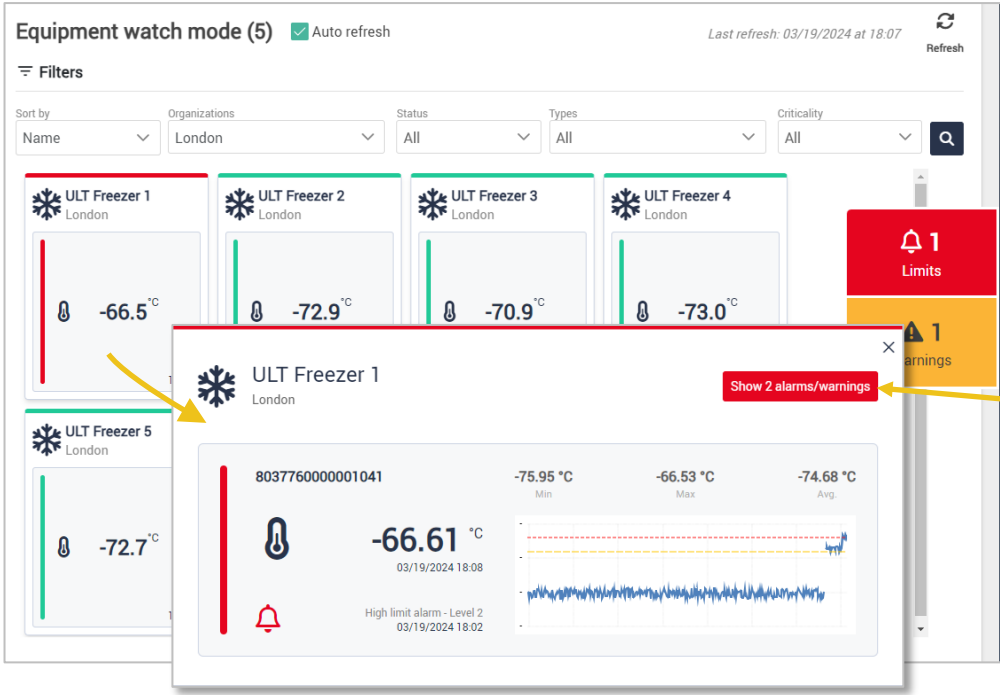


Figure 211 – Dashboard and equipment details with a limit *alarm*

### 15.1.2 Viewing alarm details

When you see that you have equipment with errors:

1. Click on one of the alarm indicators mentioned above 1 or open the alarm list by clicking on **Alarms** (🔔) in the left-hand menu.
  - If you click on the counter in the Watch mode window or on **Alarms** (🔔) in the menu, you will see current alarms. Note: when clicking from Watch Mode, a filter is applied you will only see the type of alarms or warnings indicated on the counter.
  - If you click on an alarm in the equipment tile, you will access that alarm directly.
2. The **Alarm** list opens and shows the alarm events for the selected equipment. Unfold alarm details by clicking on the arrow (➤) 2.

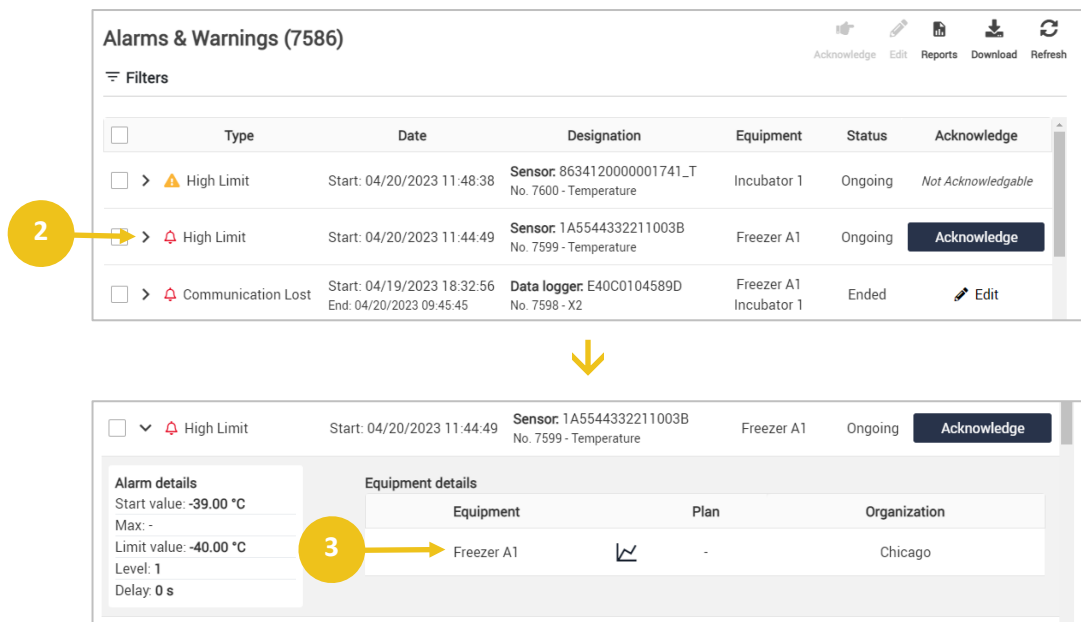




Figure 212 – Displaying alarm details

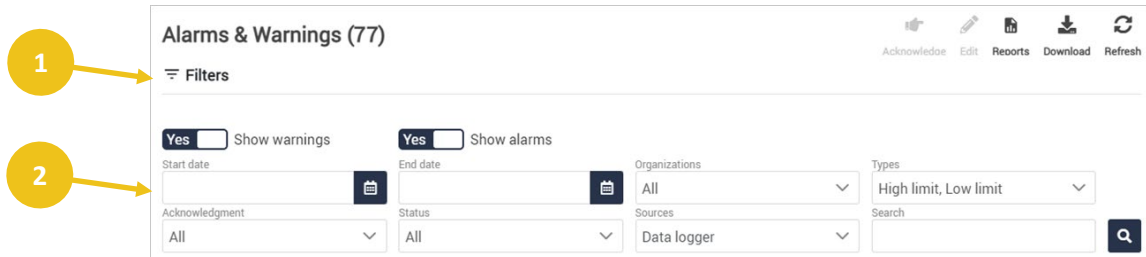
- Clicking on the graph icon (📈) opens the sensor graph to show one hour before the alarm started and one hour after the alarm ended.
- You may access the equipment directly by clicking on the link in the **Equipment** name 3.

### 15.1.3 Filtering alarms and warnings

The OCEAVIEW alarm list presents all the different alarms that have occurred in the system. The **Filters** feature on the **Alarms & Warnings** screen enables you to display alarms according to various criteria, as described below.


To filter the list:

1. Click on **Filters** (  ) and select the filter(s) you would like to apply (  ):



The screenshot shows the 'Alarms & Warnings (77)' interface. At the top right, there are icons for Acknowledge, Edit, Reports, Download, and Refresh. Below the title, there is a 'Filters' section. A yellow circle with the number '1' points to the 'Filters' header. Below the header, there are two toggle switches: 'Show warnings' and 'Show alarms', both currently set to 'Yes'. A yellow circle with the number '2' points to these toggle switches. Below the toggles, there are several filter options: 'Start date' and 'End date' (both with calendar icons), 'Organizations' (set to 'All'), 'Types' (set to 'High limit, Low limit'), 'Acknowledgment' (set to 'All'), 'Status' (set to 'All'), 'Sources' (set to 'Data logger'), and a search box with a magnifying glass icon.

Figure 213 – Filtering the list of alarms and warnings

The available filters are as follows (click on the magnifying glass button (  ) to apply:

Filter option	Description
<b>Show warnings</b>	Set toggle switch to <b>Yes</b> or <b>No</b> to display or not display warnings.
<b>Show alarms</b>	Set toggle switch to <b>Yes</b> or <b>No</b> to display or not display alarms.
<b>Start date</b>	Indicate the date and time at which you would like the list to start. The maximum date range is one month.
<b>End date</b>	Indicate the date and time at which you would like the list to end. The maximum date range is one month.
<b>Organizations</b>	By default, this is set to <b>All</b> , to display all events across your entire organization.  You may type the first characters or full name of the organizational node(s) you are looking for and or scroll through the pull-down menu to select the organizational node(s) you want.
<b>Types</b>	The options under <b>Types</b> are:  <b>Communication lost:</b> This alarm is generated if the server does not receive communication from the data logger or alert device after the period of time defined for "Trigger alarm after X minutes without communication".

---

**Data logger mismatch:** This alarm may be generated if you delete a data logger on which data logging is currently running, without stopping data logging, and you then add that data logger back into OCEAView. On the rare chance that you encounter this error: remove the data logger from OCEAView, perform a factory reset on the device, then add the data logger back into OCEAView.

**Dry contact triggered:** This alarm indicates that the dry contact input sensor detected a state change for which an alarm was configured.

**High limit:** This alarm is generated when a reading exceeds programmed high limit alarm/warning levels 1, 2, and/or 3.

**Invalid sensor type:** This alarm is generated if data logging is running and you swap the sensor with a sensor type that is not identical to the original.

**Low battery:** This alarm is generated by the data logger if the battery consumption counter indicates that the remaining battery level has reached 10%. Note: though it is not in this list, you may encounter a **Battery level low** alarm, which is generated by the data logger if the CPU detects a drop in voltage that could cause device failure. In either case, you should replace the batteries and reset the battery counter.

**Low limit:** This alarm is generated when a reading is below programmed low limit alarm/warning levels 1, 2, and/or 3.

**MKT:** Reserved for future use.



**Power lost:** This alarm occurs if a data logger's AC adapter is no longer receiving power (for example, if electricity in the building goes off or if the adapter is unplugged). The alarm is generated based on your choice for the "Trigger alarm after [X] minutes in battery mode".

**Sensor failure:** A sensor failure alarm indicates that a sensor connected to a data logger did not respond when an attempt was made to read the sensor. This could be due to a malfunctioning wired connection, out-of-range situation for a wireless sensor, or a hardware failure. Check the connection and try swapping the sensor with an identical sensor to see if the problem is resolved.

**Unexpected stop:** This alarm may be generated if the data logger stops data logging unexpectedly, for example if the batteries were changed in a device (and it completely lost power), and data logging was not restarted in OCEAView. As of OCEAView 1.11, data logging restarts automatically once the data logger reconnects to the server (Cobalt XS/X1/X2, Cobalt L3, or Cobalt ML3).

---

<b>Acknowledgment</b>	Select <b>ACK</b> to show acknowledged alarms, or <b>Not ACK</b> to show alarms that have not yet been acknowledged. Select <b>All</b> to show all alarms.
<b>Status</b>	Select <b>Ongoing</b> to show alarms that are still active, or <b>Ended</b> to show alarms that are no longer active.
<b>Sources</b>	<p>The <b>Sources</b> are the devices or equipment in your system that may generate alarms, with the following options:</p> <p><b>Data logger:</b> Alarms related to data loggers</p> <p><b>Equipment:</b> Alarms for equipment you are monitoring</p> <p><b>Infrastructure:</b> Alarms concerning various devices in your system, notably:</p> <ul style="list-style-type: none"> <li>• LoRaWAN Dry Contact (alert relay)</li> <li>• LoRaWAN Gateway</li> <li>• LoRaWAN Siren (alert device)</li> <li>• OCEABridge Bluetooth gateways</li> </ul> <p><b>Sensor:</b> Alarms related to sensors connected to data loggers</p>
<b>Search</b>	You may enter text to use as search criteria.

2. Apply filters by clicking on the magnifying glass (  ).
3. You may clear all applied filters by clicking on **Refresh** (  ). Filters are also reset to their default settings when you refresh the page (pressing the F5 key in most browsers) or when you go to another page in the application.

### 15.1.4 Acknowledging alarms


When alarms are displayed for your equipment, you must acknowledge the alarm in OCEAView and take care of the problem so that further alarms do not continue to occur.

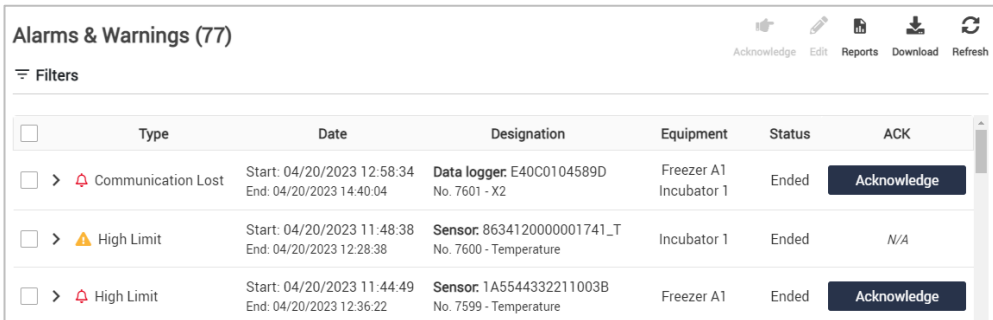
Warnings shown in orange do not need to be acknowledged. The color will revert to green once the sensor reading is back within the programmed range (unless it persists or worsens and becomes an alarm shown in red).



This section describes how to acknowledge alarms in OCEAView, but it is important to realize that the alarm status is still red in the dashboard until the next reading transmitted by the data logger no longer indicates the alarm condition. More importantly, acknowledging the alarm in the software does not actually fix any physical or technical problem on the data logger and the equipment could still be in an alarm state.

Follow these instructions to acknowledge an alarm:

1. Click on Alarms (  ) in the main menu, or on the alarm counter in the dashboard or equipment details screens.
2. The alarm management screen displays equipment with alarms:



Type	Date	Designation	Equipment	Status	ACK
Communication Lost	Start: 04/20/2023 12:58:34 End: 04/20/2023 14:40:04	Data logger: E40C0104589D No. 7601 - X2	Freezer A1 Incubator 1	Ended	Acknowledge
High Limit	Start: 04/20/2023 11:48:38 End: 04/20/2023 12:28:38	Sensor: 8634120000001741_T No. 7600 - Temperature	Incubator 1	Ended	N/A
High Limit	Start: 04/20/2023 11:44:49 End: 04/20/2023 12:36:22	Sensor: 1A5544332211003B No. 7599 - Temperature	Freezer A1	Ended	Acknowledge

Figure 214 – Alarm management and acknowledgement screen



To organize the display of unacknowledged alarms, click on **Filters** and select **Not ACK** from the **Acknowledgement** drop-down list, or select any other criteria depending on your needs.

3. To acknowledge a single alarm, click on **Acknowledge** on the line with the alarm you want to acknowledge. Enter your password to continue (or press **Send** if you are connected via SSO).

- You may acknowledge several alarms at once by clicking on their checkboxes in the first column:

<input type="checkbox"/>	Type	Date	Designation	Equipment	Status	ACK
<input checked="" type="checkbox"/>	Communication Lost	Start: 04/20/2023 12:58:34 End: 04/20/2023 14:40:04	Data logger: E40C0104589D No. 7601 - X2	Freezer A1 Incubator 1	Ended	Acknowledge
<input checked="" type="checkbox"/>	High Limit	Start: 04/20/2023 11:44:49 End: 04/20/2023 12:36:22	Sensor: 1A5544332211003B No. 7599 - Temperature	Freezer A1	Ended	Acknowledge

Figure 215 – Acknowledging several alarms at the same time

Then click on **Acknowledge** (👉) at the top of the screen. If one of the alarms in your selection has already been acknowledged, it will be deselected automatically and thus not affected by the current acknowledgment.

- The Alarm acknowledgment screens opens:

✕

### Acknowledge alarm

Alarm or warning type: High limit      Alarm status: Ended



Cause \* ▼

Corrective action 1

Preventive action

Cancel
Save

Figure 216 – Enter the details to acknowledge an alarm

6. To acknowledge the alarm, you must enter a reason for the incident in the **Cause** field. The 30 most recent entries in this field are stored and may be reused by clicking on the drop-down list .
7. The **Corrective action** and **Preventive action** fields are optional and can be used to include further information with the acknowledgment. This information is included in alarm reports that you generate.
8. Click on **Save** to save your changes (and confirm by entering your password) or **Cancel** to discard changes and return to the previous screen.
9. Once the alarm has been acknowledged, the alarm line shows " **Edit**".






Remember, acknowledging an alarm does not eliminate any physical problems at the sensor, data logger, or equipment levels.

---

### 15.1.5 Editing acknowledged alarms

You may edit alarm acknowledgments even after they have been saved. You may only edit your own acknowledgements, not those of another user.

To edit a single acknowledgment:

1. Click on **Alarms** (  ) in the main menu, or on the alarm counter in the dashboard or equipment details screens to open the alarm list.
2. Choose an alarm to edit by clicking on  **Edit** (  ).








<input type="checkbox"/>	>		Start: 04/19/2023 18:32:56 End: 04/20/2023 09:45:45	<b>Data logger:</b> E40C0104589D No. 7598 - X2	Freezer A1 Incubator 1	Ended	 Edit
<input type="checkbox"/>	>		Start: 04/19/2023 17:15:16 End: 04/19/2023 18:11:07	<b>Sensor:</b> 1A5544332211003B No. 7597 - Temperature	Freezer A1	Ended	 Edit

Figure 217 – Selecting a single acknowledgment to edit

3. In the **Acknowledgment** screen that opens, click on **Edit** (  ), make the desired changes, then click on **Save** to keep the changes or on **Cancel** to leave the previous information as it was.

To edit several acknowledgments at the same time:

1. Select checkboxes in the left-hand column and then click on **Edit** (  ) in the upper right-hand corner (  ):










Alarms & Warnings (773)							 Acknowledge  Edit  Reports  Download  Refresh			
Filters										
<input type="checkbox"/>	Type	Date	Designation	Equipment	Status	ACK				
<input checked="" type="checkbox"/>	>  Communication Lost	Start: 04/19/2023 18:32:56 End: 04/20/2023 09:45:45	<b>Data logger:</b> E40C0104589D No. 7598 - X2	Freezer A1 Incubator 1	Ended	 Edit				
<input checked="" type="checkbox"/>	>  High Limit	Start: 04/19/2023 17:15:16 End: 04/19/2023 18:11:07	<b>Sensor:</b> 1A5544332211003B No. 7597 - Temperature	Freezer A1	Ended	 Edit				

Figure 218 – Selecting multiple acknowledgments to edit

2. In the **Edit alarm acknowledgments** screen, make the desired changes and then click on **Save** to keep the changes or on **Cancel** to leave the previous information as it was.



When you edit multiple acknowledgments, the new information overwrites the old information contained in all selected acknowledgments.

## 15.2 Alert rules and notifications

OCEAView offers several alert notification mechanisms:

- By default, the system provides alert notification via e-mail and every user account is required to include an e-mail address.
- **OCEAlert** is a web-based solution that provides SMS/text messaging and automated voice call support. You must enter a valid license key in order to use **OCEAlert** notification features, as described in section 6.1.3 – *Managing license keys, p. 91*.

OCEAlert is included with the OCEAView Cloud solution, and optional with an OCEAView On-premises solution.

OCEAView sends alerts to one or more users configured in alert rules. Each user is configured with an e-mail address for this purpose. To implement alerts, you must therefore create one or more alert rules to determine the equipment and data loggers for which those groups will receive alert e-mails.

### 15.2.1 Configuring alert rules



In order to create and configure alert rules, your user *role* must allow you to “Manage alert rules”, as described in section 5.6 – *Adding user roles, p. 85*.

---

An alert is a notification sent by the system to users when the system observes an alarm condition or potential problem in the monitored environment.

Alert rules can be configured and assigned to different call lists in order to notify, by telephone and/or e-mail, users designated to handle an alarm category. You may define different criteria for the nodes in your organization, or according to the geographical areas, or sensor categories. Alert rules are based on “Time slots” and “Weekends and holidays”, defined in the system. These entities enable you to handle a variety of different cases, including Day/Night and weekend modes.

Follow these steps to configure an alert rule:

1. Click on **Configuration** (⚙️) → **Alerts** → **Add** (+)
2. The **Create alert rule** screen is displayed:

Figure 219 – Setting up an alert rule (step 1)

3. Fill the in fields according to your needs. The fields marked with a red asterisk (\*) are required:

- Name** Assign a friendly name to identify the alert rule.
- Description** Enter a description of the alert, for your information.
- Alarm or warning types** Select one or more types of alert (Limits, Dry Contact, or Technical).
  - Limit alerts** are the high and low limit values that you may configure for sensor readings.
  - Technical alerts** concern technical issues with your sensors and gateways, such as low battery and communication errors. A given rule can only apply to one or the other of these types of alerts.

**Dry contact triggered (Level 1, 2, 3)** corresponds to the time delays configured when starting data logging for the dry contact sensor on a Cobalt X1/X2 data logger. See section 12.2.2 – Dry contact input sensors (Cobalt X1/X2 only), p. 178 for more details. This enables

you to have a different alert notification for each different time delay.

**Items in organizations** Choose the relevant organization(s) and/or department(s).

**Alerts for** Select the type of equipment for which alerts will be sent: Infrastructure, mobile equipment, Shipments, or Static equipment.

**Criticality** Select the criticality level(s) for which the alert rule applies (critical and/or not critical), as configured for equipment. Criticality does not apply to alerts for infrastructure components.

**If the alarm or warning persists, repeat phone call alert every [ XX ] minutes (5 repetitions max.)**

Check this option to set the repeat frequency for this alert notification if the alarm/warning condition persists and specify the desired time interval between calls.

Note: only voice phone calls are repeated, *not e-mail and SMS/text message notifications.*

**Stop repetition when user has entered PIN code on their phone**

If you *do not check* this option, the phone call notification cycle repeats up to 5 times at the specified interval if the alarm remains active. If the alert rule is configured for the system to call several people, calling stops when the first person enters their PIN code. The call cycle then resumes after XX minutes if the alarm persists.

If you *check* this option, the first user to enter their PIN code stops the call cycle and subsequent users are not called.



Phone call alerts can be repeated up to a maximum of five (5) times. This means a total of 6 calls: the original call, and 5 repetitions. If no user has entered a PIN code by the 6<sup>th</sup> call, the phone call alert process stops automatically.

---

4. Click on **Next** to set up the users who will be notified, and when, as described below.

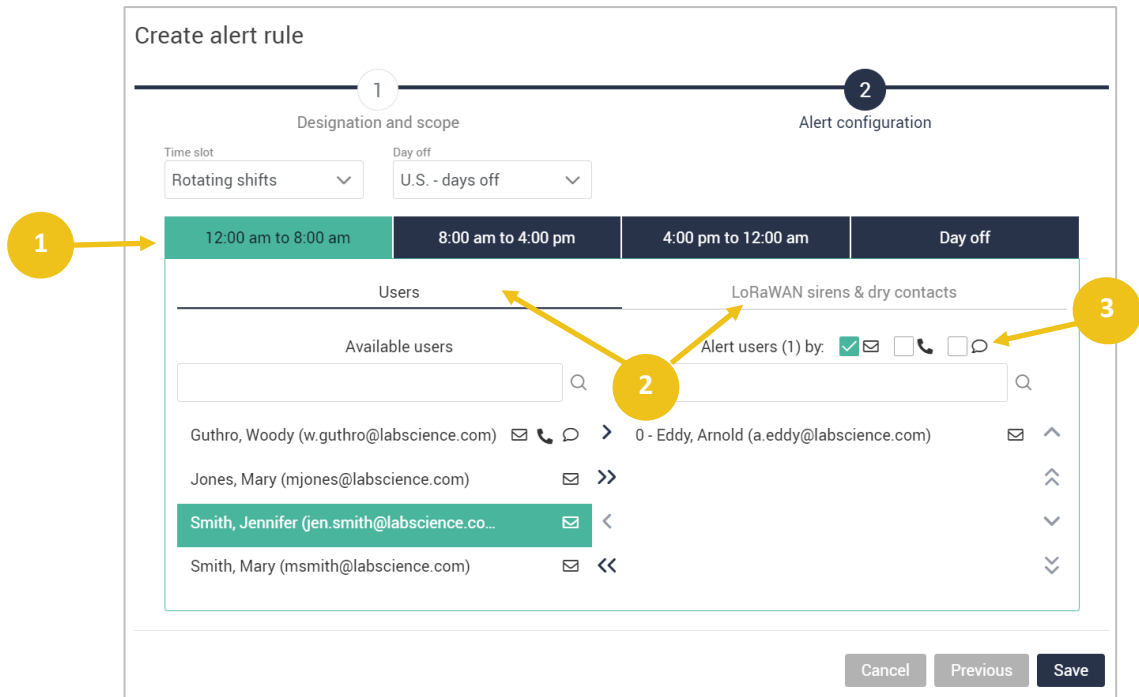


Figure 220 – Assigning users to time periods in an alert rule (step 2)

In the above example, time periods are shown on four tabs (1). Remember to assign users and/or alert devices to each period.

For each period, you may configure notifications to be sent to users and/or devices to trigger (2), notably Dickson LoRaWAN Sirens and/or Dry Contact alert relay devices configured in your system.





5. Select the **Time slot** and **Days off** for the alert:

**Time slot** Use the drop-down menu to select the alarm period from the available options. Other time slots may be added as described in section 15.4 – *Time slots*, p. 248.

**Days off** Use the drop-down list to select **Days off** periods (such as weekends and holidays) so they can be handled differently if necessary. Other days off may be added as described in section 15.4.3 – *Setting days off (weekends and non-working days)*, p. 250.


### 15.2.2 Alert rules with users


Add or remove users in the **Users** tab (  ) of the screen in Figure 220 above:


1. Determine how users will be alerted (  ): via e-mail (  ), automated voice call (  ), or SMS/Text message (  ).

Click the checkbox  →  to assign one or more alert types.


2. To add users:


Double-click on a username or click on  to move the selected user from **Available** to **Alerted**.

To select multiple users at a time, press and hold the **Ctrl** key and click on each of the users you want to select. Click on  to add them to the list of **Selected** users.

To select all available users, click on .

3. To remove users:

To remove a user from a rule, double-click on a username in the list of **Alerted** users (on the right-hand side) or click on a user and click on  to move the user to the list of **Available** users on the left-hand side.


To remove multiple users, press and hold the **Ctrl** key and, while holding down the key, click on each of the other users you want to remove. Then click on  to move them to the list of **Available** users on the left.

To remove all users, click on .

4. To change the contact sequence:

Users are contacted in the order in which they are listed in the alert rule. The top user is contacted first, etc.

You may click on the  and  icons to move the selected user up or down one line at a time.

You may click on the  and  icons to move the selected user to the very top or bottom, respectively.

5. Click on **Save** to save the rule (or add alert devices, as described in the next section), on **Previous** to return to step 1, or on **Cancel** to close this window without saving any changes.









When including a user in an alert rule, make sure their time zone is configured correctly in their profile to ensure that they are notified in the correct time slot(s) based on their local time.


---

### 15.2.3 Alert rules with LoRaWAN Siren or Dry Contact devices

To add or remove alert devices, click on the **LoRaWAN sirens & dry contacts** tab ( **5** ) of the alert rule screen:

Figure 221 – Assigning alert devices to time periods in an alert rule (Step 2)

1. Select one or more sirens (  ) or dry contact devices (  ) in the “Available” column.
2. To add devices:  
 Double-click on a device name or click on  to move the selected device from **Available** to **Alerted**.  
 To select multiple devices at a time, press and hold the **Ctrl** key and click on each of the devices you want to select. Click on  to add them to the list of “Triggered” devices.  
 To select all available devices, click on .
3. To remove devices:  
 To remove a device from a rule, double-click on a device name in the list of **Triggered** devices (on the right-hand side), or single-click on a device name and click on  to move the device to the list of **Available** devices on the left-hand side.


To remove multiple devices, press and hold the **Ctrl** key and, while holding down the key, click on each of the other devices you want to remove. Then click on  to move them to the list of **Available** devices on the left.

To remove all devices, click on .

4. To change the trigger sequence:

Devices are triggered in the order in which they are listed in the alert rule. The top device is triggered first, etc.

You may click on the  and  icons to move the selected device up or down one line at a time.

You may click on the  and  icons to move the selected device to the very top or bottom, respectively.


5. Click on **Save** to save the rule, on **Previous** to return to step 1, or on **Cancel** to close this window without saving any changes.



When including an alert device in an alert rule, make sure the rule's time zone is configured correctly to ensure that the device is triggered in the correct time slot(s) based on local time.

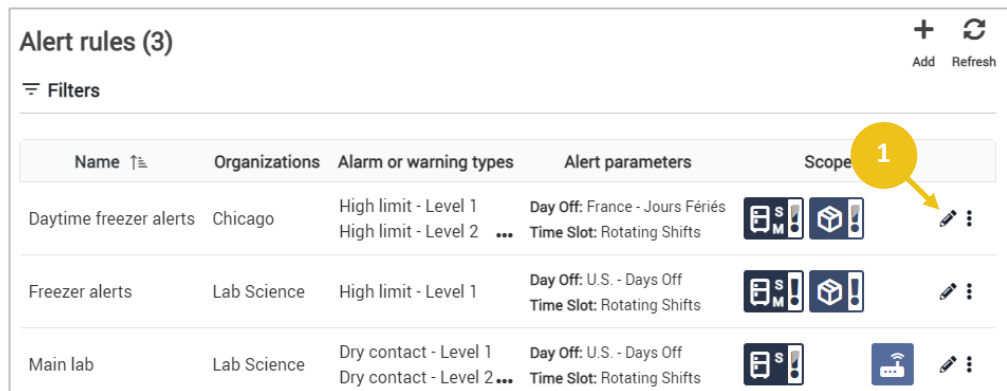
---

### 15.2.4 Modifying or deleting alert rules

To disable or change the conditions or recipients of an alert rule, click on **Configuration** (  ) → **Alerts**.

The alert rules you defined earlier are shown in the table with the configuration parameters and characteristics of the equipment involved.

1. To modify an alert rule, click on **Edit** (  ) for the rule you wish to modify  :














Name ↑	Organizations	Alarm or warning types	Alert parameters	Scope 
Daytime freezer alerts	Chicago	High limit - Level 1 High limit - Level 2 ...	Day Off: France - Jours Fériés Time Slot: Rotating Shifts	  
Freezer alerts	Lab Science	High limit - Level 1	Day Off: U.S. - Days Off Time Slot: Rotating Shifts	  
Main lab	Lab Science	Dry contact - Level 1 Dry contact - Level 2 ...	Day Off: U.S. - Days Off Time Slot: Rotating Shifts	  

Figure 222 – List of alert rules saved in the system

2. Make the desired changes (with all the same options as described in the previous sections when creating the rule).
3. Click on **Save** to save your changes or on **Previous** to return to the previous screen without saving changes.
4. For more options, click on **Options** (  ) for a drop-down menu with the following:

**Create using as template** This option enables you to create a new alert rule based on the currently selected rule.

**Simulate an alarm** Enables you to validate the alarm scenario by sending a test alert using the selected rule. No alert is listed in the Alarm list, but people are contacted and/or devices are triggered as if an alarm occurred.



**Disable** Deactivates the alert rule. You may reactivate it at any time selecting the alert rule and clicking on "Enable" in the drop-down menu.

**Delete** Deletes the alert rule from the system.

## 15.3 Filtering the alert rules display

When looking at the alert rules list, you may wish to filter the display to see specific rules that meet certain criteria.

To filter the list:

1. Click on Filters (  ) and then select the filter(s) you would like to apply (  ):

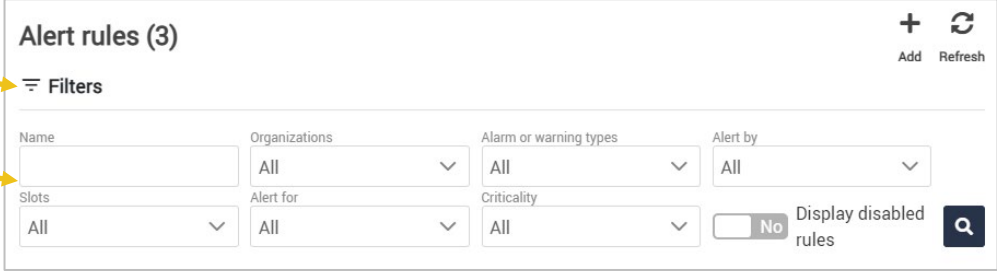




Figure 223 – Filtering the alert rules display

The available filters are as follows (click on the magnifying glass button (  ) to apply:

Filter option	Description
<b>Name</b>	Type in the first characters or full name of the alert rule you are looking for.
<b>Organizations</b>	By default, this is set to <b>All</b> , to display all rules across your entire organization.  You may type the first characters or full name of the organizational node(s) you are looking for or scroll through the pull-down menu to select the organizational node(s) you want.
<b>Alarm or warning types</b>	By default, this is set to <b>All</b> , to display all rules.  You may specify <b>Dry contact input alarm</b> , <b>Limits</b> , or <b>Technical</b> .
<b>Alert by</b>	By default, this is set to <b>All</b> , to display all rules.  You may specify <b>Call</b> , <b>E-mail</b> , or <b>SMS</b> (text message).
<b>Slots</b>	By default, this is set to <b>All</b> , to display all rules. Use the pull-down menu to select one or more rules from your list of configured rules.
<b>Alerts for</b>	By default, this is set to <b>All</b> , to display all rules.  You may specify <b>Infrastructure elements</b> , <b>Mobile equipment</b> , <b>Shipments</b> , or <b>Static equipment</b> .

<b>Criticality</b>	By default, this is set to <b>All</b> , to display all rules. You may specify <b>Critical</b> or <b>Not critical</b> .
<b>Display disabled rules</b>	Set this to <b>No</b> to not show disabled rules. Set this to <b>Yes</b> to show disabled rules.

2. Apply filters by clicking on the magnifying glass (  ).

You may clear all applied filters by clicking on **Refresh** (  ). Filters are also reset to their default settings when you refresh the page (pressing the F5 key in most browsers) or when you go to another page in the application.

## 15.4 Time slots

As described earlier in section 15.2.1 – *Configuring alert rules*, p. 238, you may configure specific time slots during which your system will send alerts to users. These time slots may then be used in the context of one or more alert rules.

### 15.4.1 Adding a time slot

To add a time slot:

1. In the main menu, click on **Configuration** (⚙️) → **Time slots**
2. Click on **Add** (+).

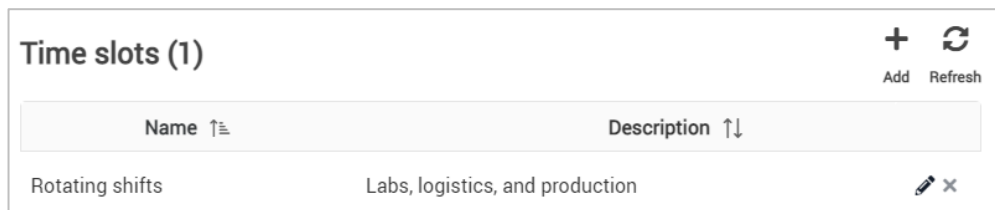


Figure 224 – Adding a new time slot

3. The **Create time slot** window opens on the right-hand side of the screen:

×

Create time slot

Name \*

Description

Slots

Name \*

From 00:00 To 00:00

Cancel Save

Figure 225 – Time slot details


4. Enter the details of the new time slot. The fields marked with a red asterisk (\*) are required:

<b>Name</b>	Enter a name for the time slot.
<b>Description</b>	Enter a description of the time slot.
<b>Slots</b>	Enter a name for the time slot and then, define the start and end time. These parameters are used by the application to determine the start and end of the alarm period.






To avoid confusion, all times are indicated in local time of the user who will be receiving the alert, or the device to be triggered.

---

5. Click on **Add** (  ) to add up to a total of three time slots, if needed.
6. Click on **Save** to save your changes or on **Cancel** to discard changes and return to the previous screen.

### 15.4.2 Modifying or deleting time slots

To change the time slots of your alert rules:

1. In the main menu, click on **Configuration** (  ) → **Time slots**
2. Click on **Edit** (  ) to modify a time slot.
3. Make the necessary changes.
4. Click on **Save** to save your changes or on **Cancel** to discard changes and return to the previous screen.
5. If you want to delete a time slot, select the time slot, and click on **Delete** (  ).

### 15.4.3 Setting days off (weekends and non-working days)

OCEAView enables you to manage non-working days, such as weekends, public holidays, and other days off. You may then use this feature to fine-tune your system's alert rules.

To add days off:

1. In the main menu, click on **Configuration** (⚙️) → **Days off**



Name ↑	Description ↓	
France - National holidays		✕
U.S. - National holidays		✕

Figure 226 – Adding days off (non-working days)

2. Click on **Add** (+), which opens the **Create days off** window:

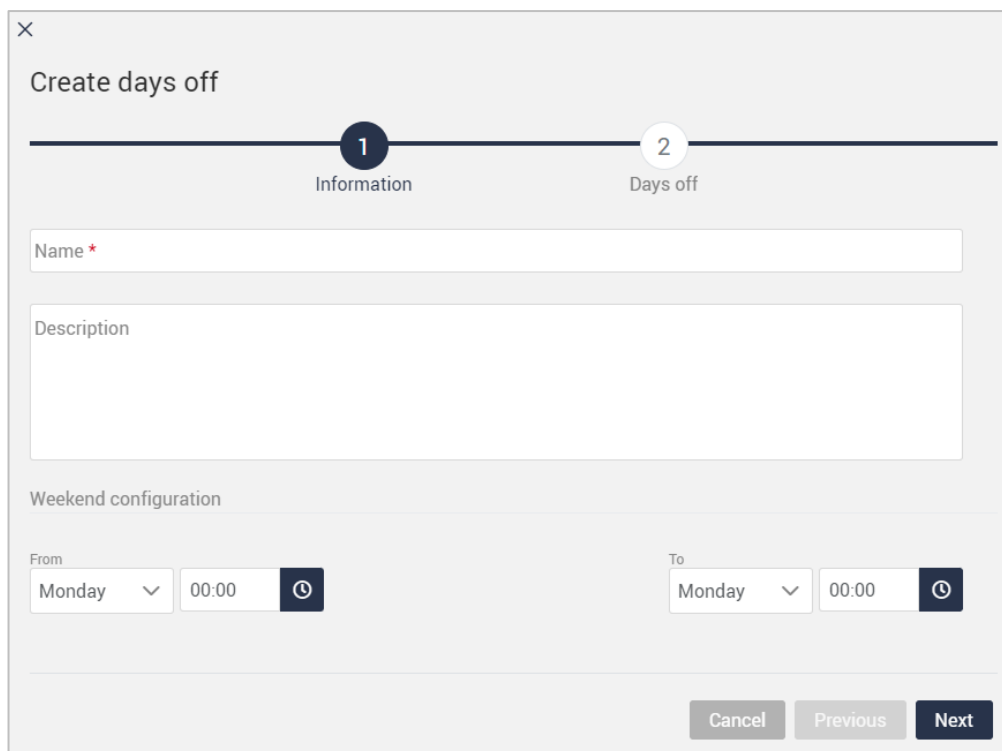


Figure 227 – Entering details for days off

- Fill the in fields according to your needs. The fields marked with a red asterisk (\*) are required:

<b>Name</b>	Enter a name as a reference for the day(s) off. You will be able to use this name when you create alert rules.
<b>Description</b>	(Optional) You may enter a description of the day off for information purposes.
<b>Weekend configuration</b>	Set the start and end times that are considered as part of the weekend, such as for on-call staff. These settings are used to determine the start and end of the weekend alarm period.

- Click on **Next** → **+ Add day off**

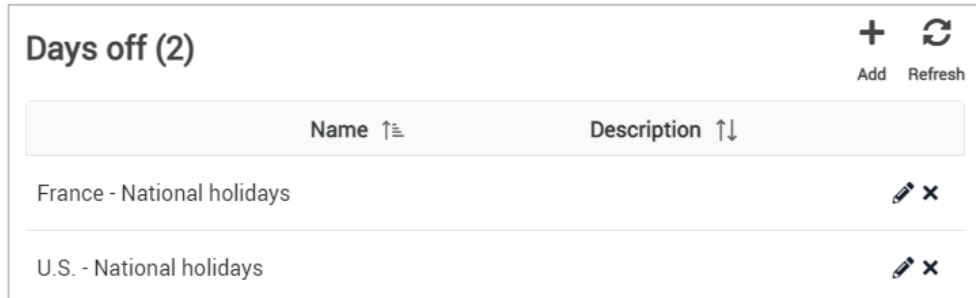
Figure 228 – Adding days off to be used in alert rules

- Select dates in the **From** and **To** fields.
- If the day or range recur every year, click on the **Annually** checkbox.
- You may remove a day or range off by clicking on **Remove** ( - ) next to the item to be deleted, or add a day or range off by clicking on **Add** ( + )
- Click on **Save** to save your changes in the system, on **Previous** to return to the previous, or on **Cancel** to discard your changes and close the window.

### 15.4.4 Modifying or deleting weekends and days off

To edit a weekend or day off:

1. In the main menu, click on **Configuration** (  ) → **Days off**









Name ↑	Description ↑↓
France - National holidays	 
U.S. - National holidays	 

Figure 229 – List of days off in your system

2. Select the line you want to change, then click on **Edit** (  ).
3. Make the desired changes.
4. Click on **Save** to save your changes or on **Cancel** to discard changes and return to the previous screen.
5. If you want to delete a day off configuration, select the desired line and click on **Delete** (  ).

## 16 Getting help / FAQ

### 16.1 User manuals

User manuals for the OCEAView web application and related products are available directly from the application.

Click on **Help** → **Online help** to download the latest documents:



Figure 230 – Access to user guides for OCEAView and companion products

### 16.2 Contacting Dickson technical support

You may send e-mail to Dickson technical support by clicking on **Contact support** in the help screen shown above. This action creates an e-mail message using your computer's default e-mail application, complete with application version information that is useful for the technical support team.

## 16.3 Viewing OCEAView version release notes

If the OCEAView web application has been updated since the last time you logged in, the Release Notes concerning the new version are displayed on your screen:

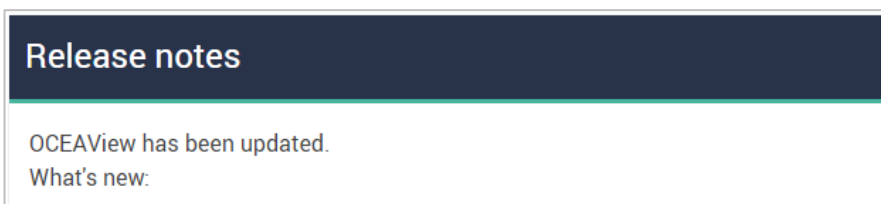


Figure 231 – Latest release notes

This message is not displayed for new users.

You may click on **Do not show these notes again** to stop the message from being displayed when you log in again. Click on **Close** to close the window and continue with OCEAView.




You may show all OCEAView release notes at any time by clicking on **Help** → **Release notes**

---

## 16.4 FAQ

### 16.4.1 Data loggers & data logging

**I just installed a new data logger. It seems to be working fine, but no information is updated in the OCEAView dashboard.**

- Information is automatically sent to the system at the end of each programmed “transfer period”. The transfer period is generally longer than the sensor reading period, so you may simply need to wait for the cycle to begin in order to have data in the web application.
- On the Cobalt XS/X1/X2 data logger, you may use the **Synchronize** feature to trigger communication between the system and the data logger.
- You may also refresh the application screen using the **Refresh** () that is present throughout OCEAView.

**My Cobalt X1/X2 data logger does not seem to be able to detect an Emerald or Atlas Bluetooth module that I want to use as a remote sensor.**

In order to use an Emerald or Atlas module as a wireless sensor on your Cobalt X1/X2 data logger, a few conditions must be met:

- The Atlas or Emerald module must be compatible with the Cobalt X1/X2 solution. Compatible modules are marked with an “X” on the sticker on the module, above the product name.
- The Atlas or Emerald module must not have already been used on the legacy OCEAView system.
- You may need to factory reset the module using the OCEAView mobile application for iOS and Android. See details in the OCEAView mobile application user guide.

**How can I check the battery level of a remote sensor?**

The battery level of Atlas and Emerald devices being used as remote sensors (paired with Cobalt X1/X2 data loggers) is shown in the battery level column of the **Data loggers** screen.

**I used OCEAView to activate data logging on a Cobalt XS/X1/X2 device, which now displays the temperature and session name as expected, but I still do not see any readings in OCEAView. What should I do?**

If the data logger screen shows information other than “Data logger waiting for configuration”, it means that communication from the server was successful. The edges of the tile in the Watch Mode screen (in OCEAView) should no longer be gray. Just wait until sensor readings are uploaded at the next transfer interval.

**My data logger was data logging and it lost power (unplugged or batteries removed). But when we restored power, OCEAView showed an Unexpected Stop alarm. Why?**

Starting with OCEAView 1.11: if a data logger with one or more data logging sessions in progress stops unexpectedly, you will see an "Unexpected Stop" technical alarm in OCEAView. However, once the data logger is turned on again and communication is re-established with the server, data logging settings are restored and data logging restarts.

In versions prior to version 1.11: when you restore power, the data logger is operational but the data logging session is not restarted. The data logger therefore still needs your attention and OCEAView triggers the Unexpected Stop alarm to notify you that your equipment is not being monitored.

**Can I remove a data logger from OCEAView if data logging is currently running?**

Yes, you can remove a data logger from your OCEAView system even if data logging is running. You should only do this in cases where there is a problem with the data logger, or if a data logger had to be swapped while still running. In those cases, OCEAView can no longer stop the data logging session via software.

**The unit or temperature range for my sensor is not displayed correctly in the OCEAView web application. What should I do?**


Under rare conditions, it may happen that the sensor's physical parameter (unit) or temperature does not appear properly in the OCEAView web application. If that occurs, resynchronize the information by unplugging the sensor from the data logger and pressing **Menu → Settings → Refresh Sensors**. Then plug the sensor back into the data logger and press on **Menu → Settings → Refresh Sensors** again to push updated information to the web application.

**I successfully generated a sensor report in MS Excel format, but then I was unable to generate the same report as a PDF. What should I do?**

If you plan on generating several copies of a report in different file formats, or several different reports, make sure your browser is not configured to block multiple downloads from the site. The first download will usually work fine, but subsequent file downloads could be blocked by your browser.

## 16.4.2 System & support

### What is the best way for me to get technical support with OCEAView?

We recommend that you click on **Help** →  to send an e-mail message to the support team. The message includes information that will help us understand your situation faster.

### In terms of GAMP 5 (2008), what is the software category for the OCEAView monitoring solution?

The OCEAView monitoring solution is categorized as a Category 4 (Configured Products) according to GAMP 5 (2008).

The OCEAView web application and related Dickson products, including sensors, data loggers, gateways, alert devices, etc., are configurable software products providing standard interfaces and functions that enable the configuration of user-specific business processes. This typically involves configuring predefined software components to handle users, alarms, alerts, communication, etc.

### Can my IT department safelist the OCEAView server's IP address?

As part of the system's high-availability design, we use load balancing which can result in changes to the system's IP address without advanced warning. For this reason, we HIGHLY discourage the use of IP addresses for safelisting services related to OCEAView.

### What if I have multiple locations across multiple geographic regions?

Any given account can only exist in one region, so you must select a specific region as the location for your datacenter: Europe, North and South America, or Asia-Pacific. Regardless of the region you choose, OCEAView is designed to function in local, national, and international work environments.

### "Reports with approval" is not present in the left-hand menu, and I don't see it in the various screens.

**Reports with approval** is not shown by default in the menu or on pages in the application unless the feature is activated in your company configuration. To activate report review/approval, log in to OCEAView with user having an Application Manager profile, then click on **Configuration** (⚙️) → **Company** → **Compliance**. Select the items for which you would like to manage report reviews and approvals, then save your settings.

Note: As an Application Manager, changes you make in the list of items in the **Compliance** screen are applied on a system-wide level, but they only take effect next time users log in.

### **I'm using SSO, but I cannot log in to OCEAView. What should I do?**

Proper SSO configuration on your identity provider platform is essential and can be quite tricky. It should be handled by an IT specialist.

In particular, care should be taken to properly configure "claims" on the identity provider side, in particular Email, FirstName, LastName, and UserName. User login will fail if OCEAView receives an incomplete response from the identify server.

We have created detailed technical bulletins on implementing SSO for:



- Microsoft Entra (Azure) ([click here for PDF](#))
- Okta ([click here for PDF](#))

For more information, feel free to contact your Dickson OCEAView representative for a technical bulletin on this topic.

## 17 Appendix 1 – Sensor reading report details

This chapter describes the contents of reports generated by the OCEAView web application as of version 1.13. Here, we define the key indicators provided in OCEAView reports and explain how information is presented and derived.

### 17.1 Downloading reports

Sensor reading reports can be downloaded from the Sensor Readings graph screen in OCEAView via the **Download** (  ) button in the upper right-hand corner . Available file formats include MS Excel, PDF, MS Word, and TXT (plain text). The general content is identical in all formats except for plain text, which only includes sensor readings and timestamp information.



In plain text format, timestamps are always expressed in UTC (Coordinated Universal Time).

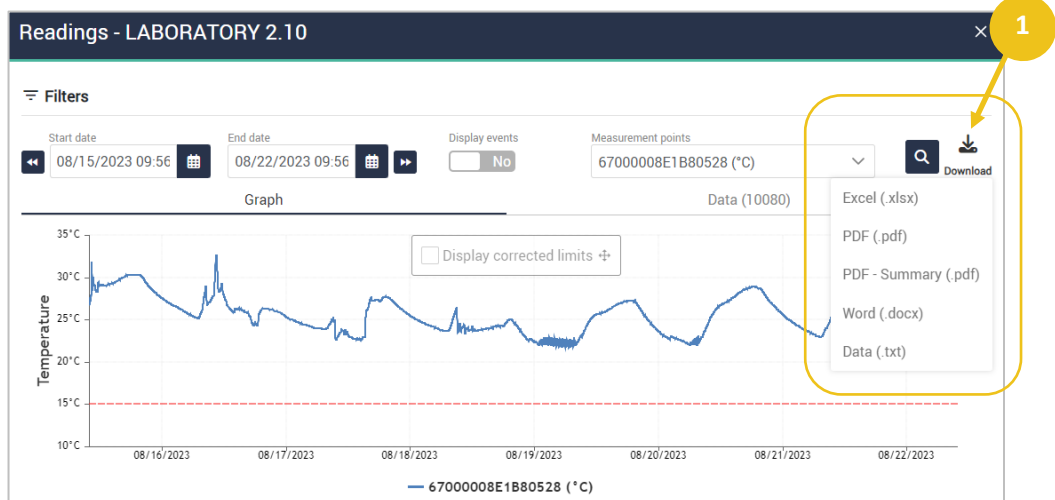


Figure 232 – Generate reports by clicking on the Download button on the sensor readings page

## Appendix 1 – Sensor reading report details

Reports comprise several sections:

- Summary information about filters, alarms, and warnings
- Equipment and data logging details
- One section for each sensor associated with the equipment

**DICKSON** Load [PBLUM]

### Readings

**Report Filters**  
 Start Date : 08/15/2023 09:56  
 End Date : 08/22/2023 09:56  
 Equipment : LABORATORY 2.10 (Dickson Demo)  
 Sensors : 67000006E1880528-1

**Alarms & Warnings**

Type	Status	Ack
High limit alarms	Ended	No
Low limit alarms	Ended	No
High limit warnings	Ended	No
Low limit warnings	Ended	No
Technical alarms	Ended	No
Dry Contact alarms	Ended	No
Dry Contact warnings	Ended	No
Total		

**Data logging Monitoring (Running)** Data logger SN : E69F0001066  
 Reading Interval : 01 min 00 s Start Date : 08/09/2023 11:16:13 End Date :  
 Use drift/uncertainty : Yes Allow acknowledgment from data logger : Yes Use buzzer : Yes

**Sensors**  
 Sensor : 67000006E1880528

**Limits**

Type	Limit
Alarm High limit 1	15.00

**Alarms & Warnings**

Start Date	End Date	Type	Status	Ack
08/12/2023 11:48:13	08/17/2023 08:51:13	Alarm High limit	Ended	No
08/17/2023 09:21:13	08/24/2023 15:21:13	Alarm High limit	Ended	No

**Reading Summary**

Min	Max	Average	Standard Deviation	Activation Energy	MKT
21.63 °C (08/19/2023 07:03:13)	32.63 °C (08/16/2023 10:33:13)	25.35 °C	2.07 °C	83.14472 kJ/mol	25.58 °C

**Readings**

Date	Value	Unit	Date	Value	Unit	Date	Value	Unit	Date	Value	Unit
08/15/2023 09:56:13	26.69	°C	08/15/2023 09:57:13	26.69	°C	08/15/2023 09:58:13	26.69	°C	08/15/2023 09:59:13	26.69	°C
08/15/2023 10:00:13	26.69	°C	08/15/2023 10:01:13	26.75	°C	08/15/2023 10:02:13	26.81	°C	08/15/2023 10:03:13	26.81	°C
08/15/2023 10:04:13	26.88	°C	08/15/2023 10:05:13	26.88	°C	08/15/2023 10:06:13	26.94	°C	08/15/2023 10:07:13	26.94	°C
08/15/2023 10:08:13	27.00	°C	08/15/2023 10:09:13	27.15	°C	08/15/2023 10:10:13	27.31	°C	08/15/2023 10:11:13	27.44	°C
08/15/2023 10:12:13	27.38	°C	08/15/2023 10:13:13	27.44	°C	08/15/2023 10:14:13	27.63	°C	08/15/2023 10:15:13	27.75	°C
08/15/2023 10:16:13	27.63	°C	08/15/2023 10:17:13	27.75	°C	08/15/2023 10:18:13	27.94	°C	08/15/2023 10:19:13	27.94	°C
08/15/2023 10:20:13	27.81	°C	08/15/2023 10:21:13	27.69	°C	08/15/2023 10:22:13	28.00	°C	08/15/2023 10:23:13	29.00	°C
08/15/2023 10:24:13	28.75	°C	08/15/2023 10:25:13	29.81	°C	08/15/2023 10:26:13	30.06	°C	08/15/2023 10:27:13	30.50	°C
08/15/2023 10:28:13	31.13	°C	08/15/2023 10:29:13	31.69	°C	08/15/2023 10:30:13	31.88	°C	08/15/2023 10:31:13	31.25	°C
08/15/2023 10:32:13	30.50	°C	08/15/2023 10:33:13	30.00	°C	08/15/2023 10:34:13	29.56	°C	08/15/2023 10:35:13	29.13	°C
08/15/2023 10:36:13	28.75	°C	08/15/2023 10:37:13	28.56	°C	08/15/2023 10:38:13	28.56	°C	08/15/2023 10:39:13	28.58	°C
08/15/2023 10:40:13	28.81	°C	08/15/2023 10:41:13	29.50	°C	08/15/2023 10:42:13	29.94	°C	08/15/2023 10:43:13	29.56	°C
08/15/2023 10:44:13	29.50	°C	08/15/2023 10:45:13	29.31	°C	08/15/2023 10:46:13	29.75	°C	08/15/2023 10:47:13	29.94	°C
08/15/2023 10:48:13	30.06	°C	08/15/2023 10:49:13	29.81	°C	08/15/2023 10:50:13	29.44	°C	08/15/2023 10:51:13	29.19	°C
08/15/2023 10:52:13	29.19	°C	08/15/2023 10:53:13	29.13	°C	08/15/2023 10:54:13	29.06	°C	08/15/2023 10:55:13	28.94	°C
08/15/2023 10:56:13	28.88	°C	08/15/2023 10:57:13	28.88	°C	08/15/2023 10:58:13	28.84	°C	08/15/2023 10:59:13	29.00	°C
08/15/2023 11:00:13	29.06	°C	08/15/2023 11:01:13	29.06	°C	08/15/2023 11:02:13	29.06	°C	08/15/2023 11:03:13	29.06	°C
08/15/2023 11:04:13	29.00	°C	08/15/2023 11:05:13	28.88	°C	08/15/2023 11:06:13	28.88	°C	08/15/2023 11:07:13	28.81	°C
08/15/2023 11:08:13	28.81	°C	08/15/2023 11:09:13	28.69	°C	08/15/2023 11:10:13	28.63	°C	08/15/2023 11:11:13	28.63	°C
08/15/2023 11:12:13	28.56	°C	08/15/2023 11:13:13	28.50	°C	08/15/2023 11:14:13	28.50	°C	08/15/2023 11:15:13	28.44	°C

Created by M. Mojdeska (mma.ocv@oceasoftware.com) 3/84 08/29/2023 17:21:13 (GMT +0200)

Figure 233 – Reports contain summary pages followed by a listing of sensor readings

## 17.2 Applying filters

Active filters determine the contents of your report, in particular the date range <sup>1</sup> and measurement points (sensors) <sup>2</sup>.

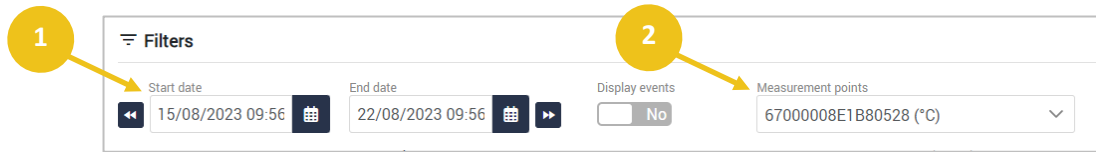


Figure 234 - Reports are generated based on the filters you apply before downloading



If you create a report for multiple sensors at the same time, the information described in the following pages is provided separately and sequentially for each sensor.

Filter criteria are indicated at the beginning of the report:

Report Filters	
Start Date	: 15/08/2023 09:56
End Date	: 22/08/2023 09:56
Equipment	: LABORATORY 2.10 (Dickson Demo)
Sensors	: 67000008E1B80528-1

Figure 235 – Filter information included at the beginning of the report

## 17.3 Understanding the alarms & warnings summary

The first section of the report presents a table that summarizes all the alarms and warnings for sensors associated with the equipment.

Alarms & Warnings Summary						
Type	Total	Ongoing	Acknowledged	Duration	%	Longest Duration
High limit alarms	2	1	0	6 d 23 h 30 min 00 s	99.70%	5 d 00 h 35 min 03 s
Low limit alarms	0	0	0			
High limit warnings	0	0	0			
Low limit warnings	0	0	0			
Technical alarms	0	0	0			
Dry Contact alarms	0	0	0			
Dry Contact warnings	0	0	0			
<b>Total</b>	<b>2</b>	<b>1</b>	<b>0</b>	<b>6 d 23 h 30 min 00 s</b>	<b>99.70%</b>	<b>5 d 00 h 35 min 03 s</b>

Figure 236 – Summary table showing alarms and warnings during the report period

The following information is provided in the summary table:

<b>Type</b>	Description of the various alarm and warning types
<b>Total</b>	Number of alarms or warnings triggered during the report period
<b>Ongoing</b>	Number of alarms or warnings still ongoing when the report was produced
<b>Acknowledged</b>	Number of alarms acknowledged during the report period
<b>Duration</b>	From a system perspective, duration represents the amount of time during which at least one of the events was triggered during the report period, that is, the total amount of time the system showed the corresponding alarms or warnings.



When calculating duration, alarms and warnings occurring at the same moment “overlap”, so duration does not represent the sum of alarms and/or warnings during the report period.

Example: suppose that Equipment A has a temperature sensor and a humidity sensor. The equipment encounters a problem, and the temperature sensor is an alarm state from 8:00 a.m. to 10:00 a.m., and the humidity sensor is an alarm state from 9:00 a.m. to 11:00 a.m. Regardless of the individual alarm durations (with overlapping time periods), the system showed alarms from 8:00 a.m. to 11:00 a.m., that is, 3 hours. The value shown in the Duration column is therefore 3 hours.

**%** Indicates represents the duration value with respect to the total report period.

Example: suppose you create a report for Equipment A covering a 24-hour period. The duration value for Equipment A indicates alarms that alarms were present for 3 hours, which is 12.5% of the report period.

**Longest duration** The longest individual alarm or warning triggered during the report period.

The Total line at the bottom of the report summarizes the information in the columns.

**Total, Ongoing, Acknowledged**

Sum totals of all the events listed above in the columns.

**Duration**

The length of time during which at least one of the alarm or warning events was triggered during the report period.

For example, suppose Equipment B had the following:

- Temperature high limit warning on sensor 1 from 7:30 a.m. to 11:00 a.m.
- Temperature high limit alarm on sensor 2 from 8:00 a.m. to 10:00 a.m.
- Humidity high limit alarm on sensor 3 from 9:00 a.m. to 11:00 a.m.
- A technical alarm from 8:00 p.m. to 9:00 p.m.

The total duration from a system perspective (with alarms occurring during the same period actually overlapping and not cumulated) would be **4 hours 30 minutes** (with alarms 1, 2, and 3 covering 3 hours 30 minutes from 7:30 a.m. to 11:00, and 4 covering 1 hour from 8:00 p.m. to 9:00 p.m.).

**%**

Indicates the percentage represented by the total duration value with respect to the total report period.

Example: if you create a report for Equipment B for a 24-hour period, and the equipment has a total duration of alarms and warnings of 4 hours 30 minutes, the % in this case would be 18.75%.

This illustration shows a visual representation of the above example:





	12:00 a.m.	11:59 p.m.
<b>High limit alarms</b> Temp sensor 2 Humidity sensor 3  <b>Duration</b>	<div style="text-align: center;"> <span style="background-color: red; color: white; padding: 2px;">8:00 – 10:00 a.m.</span>  <span style="background-color: red; color: white; padding: 2px;">9:00 – 11:00 a.m.</span>                        3 hours                 </div>	
<b>High limit warning</b> Temp sensor 1  <b>Duration</b>	<div style="text-align: center;"> <span style="background-color: red; color: white; padding: 2px;">7:30 – 11:00 a.m.</span>                        3 hours 30 mins                 </div>	
<b>Technical alarm</b> Low battery  <b>Duration</b>	<div style="text-align: right;"> <span style="background-color: red; color: white; padding: 2px;">8:00 – 9:00 p.m.</span>                        1 hour                 </div>	
<b>Total duration</b>	<div style="text-align: center;">                     3 hours 30 mins                      1 hour                        4 hours 30 mins                 </div>	

Figure 237 – Illustration of alarm and warning duration example

That same information is included in the summary table as shown here:

Alarms & Warnings Summary						
Type	Total	Ongoing	Acknowledged	Duration	%	Longest Duration
High limit alarms	2	0	2	3 h 00 min 00 s	12.50%	2 h 00 min 00 s
Low limit alarms	0	0	0			
High limit warnings	1	0	0	3 h 30 min 00 s	14.58%	3 h 30 min 00 s
Low limit warnings	0	0	0			
Technical alarms	0	0	0	1 h 00 min 00 s	4.17%	1 h 00 min 00 s
Dry Contact alarms	0	0	0			
Dry Contact warnings	0	0	0			
<b>Total</b>	<b>4</b>	<b>0</b>	<b>2</b>	<b>4 h 30 min 00 s</b>	<b>18.75%</b>	<b>3 h 30 min 00 s</b>

Figure 238 - Equivalent values in summary table

## 17.4 Data logging details

The next section in the report summarizes data logging settings and includes a graph of readings over the report period.



Figure 239 - Data logging session summary

<b>1</b>	Data logging session information.
<b>2</b>	<p>The <b>Sensors</b> table indicates the sensor serial number and data logging start and end dates. This list can contain information for several sensors if the sensor was swapped while data logging was running.</p> <p>The <b>Limits</b> section indicates the alarm and warning limits configured for data logging. The start and end dates allow to</p>

	track any changes made to setting during the data logging session.
<b>3</b>	The graph shows sensor readings over time, with color lines indicating programmed limits.

## 17.5 Alarms & Warnings

The Alarms & Warnings section lists all the alarms and warnings triggered during the report period, along with their current status and whether or not they were acknowledged.

Alarms & Warnings				
Start Date	End Date	Type	Status	Ack
08/23/2023 15:48:42	08/27/2023 08:52:42	Alarm High limit	Ended	Yes
08/27/2023 13:30:42	08/27/2023 13:31:42	Alarm High limit	Ended	No
08/27/2023 13:32:42	08/27/2023 22:00:42	Alarm High limit	Ended	No
08/28/2023 10:49:42	08/29/2023 05:28:42	Alarm High limit	Ended	No
08/29/2023 08:31:42	08/30/2023 03:56:42	Alarm High limit	Ended	No
08/30/2023 10:20:42		Alarm High limit	Ongoing	No

Figure 240 - Alarms and warnings during the report period

## 17.6 Reading summary and reading detail

The Reading Summary section **1** provides information about the overall data contained in the report, such as Minimum and Maximum values (with reading date and time), Average, and Standard Deviation.

1

Reading Summary						
Min	Max	Average	Standard Deviation	Activation Energy	MKT	
22.31 °C (08/28/2023 08:21:42)	31.19 °C (08/23/2023 16:16:42)	25.35 °C	1.20 °C	83.14472 kJ/mol	25.43 °C	

2

Data logging XMF INFORMATION - (Running)											
Date	Value	Unit	Date	Value	Unit	Date	Value	Unit	Date	Value	Unit
08/23/2023 15:48:42		°C	08/23/2023 15:49:42	25.44	°C	08/23/2023 15:50:42	25.38	°C	08/23/2023 15:51:42	25.38	°C
08/23/2023 15:52:42		°C	08/23/2023 15:53:42	25.50	°C	08/23/2023 15:54:42	25.56	°C	08/23/2023 15:55:42	25.38	°C
08/23/2023 15:56:42		°C	08/23/2023 15:57:42	26.06	°C	08/23/2023 15:58:42	25.56	°C	08/23/2023 15:59:42	25.63	°C
08/23/2023 16:00:42	25.56	°C	08/23/2023 16:01:42	25.50	°C	08/23/2023 16:02:42	25.44	°C	08/23/2023 16:03:42	25.44	°C
08/23/2023 16:04:42	25.31	°C	08/23/2023 16:05:42	25.25	°C	08/23/2023 16:06:42	25.25	°C	08/23/2023 16:07:42	25.25	°C
08/23/2023 16:08:42	25.25	°C	08/23/2023 16:09:42	25.25	°C	08/23/2023 16:10:42	25.19	°C	08/23/2023 16:11:42	25.13	°C
08/23/2023 16:12:42	25.06	°C	08/23/2023 16:13:42	25.06	°C	08/23/2023 16:14:42	25.13	°C	08/23/2023 16:15:42	25.13	°C
08/23/2023 16:16:42	31.19	°C	08/23/2023 16:17:42	29.31	°C	08/23/2023 16:18:42	27.94	°C	08/23/2023 16:19:42	27.19	°C
08/23/2023 16:20:42	26.69	°C	08/23/2023 16:21:42	26.31	°C	08/23/2023 16:22:42	26.19	°C	08/23/2023 16:23:42	25.81	°C
08/23/2023 16:24:42	25.63	°C	08/23/2023 16:25:42	25.44	°C	08/23/2023 16:26:42	25.31	°C	08/23/2023 16:27:42	25.31	°C
08/23/2023 16:28:42	25.19	°C	08/23/2023 16:29:42	25.06	°C	08/23/2023 16:30:42	24.94	°C	08/23/2023 16:31:42	24.75	°C
08/23/2023 16:32:42	24.69	°C	08/23/2023 16:33:42	24.69	°C	08/23/2023 16:34:42	24.69	°C	08/23/2023 16:35:42	24.63	°C
08/23/2023 16:36:42	24.56	°C	08/23/2023 16:37:42	24.50	°C	08/23/2023 16:38:42	24.44	°C	08/23/2023 16:39:42	24.44	°C
08/23/2023 16:40:42	24.44	°C	08/23/2023 16:41:42	24.44	°C	08/23/2023 16:42:42	24.38	°C	08/23/2023 16:43:42	24.38	°C
08/23/2023 16:44:42	24.38	°C	08/23/2023 16:45:42	24.31	°C	08/23/2023 16:46:42	24.31	°C	08/23/2023 16:47:42	24.31	°C
08/23/2023 16:48:42	24.31	°C	08/23/2023 16:49:42	24.38	°C	08/23/2023 16:50:42	24.38	°C	08/23/2023 16:51:42	24.38	°C

Figure 241 - Reading summary and detail

The Mean Kinetic Temperature (MKT) value is calculated from the data based on the following equation:

$$T_K = \frac{\frac{\Delta H}{R}}{-\ln\left(\frac{t_1 e^{\left(\frac{-\Delta H}{RT_1}\right)} + t_2 e^{\left(\frac{-\Delta H}{RT_2}\right)} + \dots + t_n e^{\left(\frac{-\Delta H}{RT_n}\right)}}{t_1 + t_2 + \dots + t_n}\right)}$$



100 or more readings are required to calculate MKT. If the report period does not include 100 readings, the MKT value is not included.

---

All the readings for the report period are listed in the last section, **Readings** <sup>2</sup>. Readings are listed chronologically in lines from earliest to oldest and colored in red (high limits) or blue (low limits) if the configured limit(s) is/are crossed.

## 18 Appendix 2 – Tracking OCEAView Cloud system status

As part of our ongoing commitment to transparency and customer satisfaction, Dickson uses the *status.io* service to provide you with real-time updates on the status of our platforms.

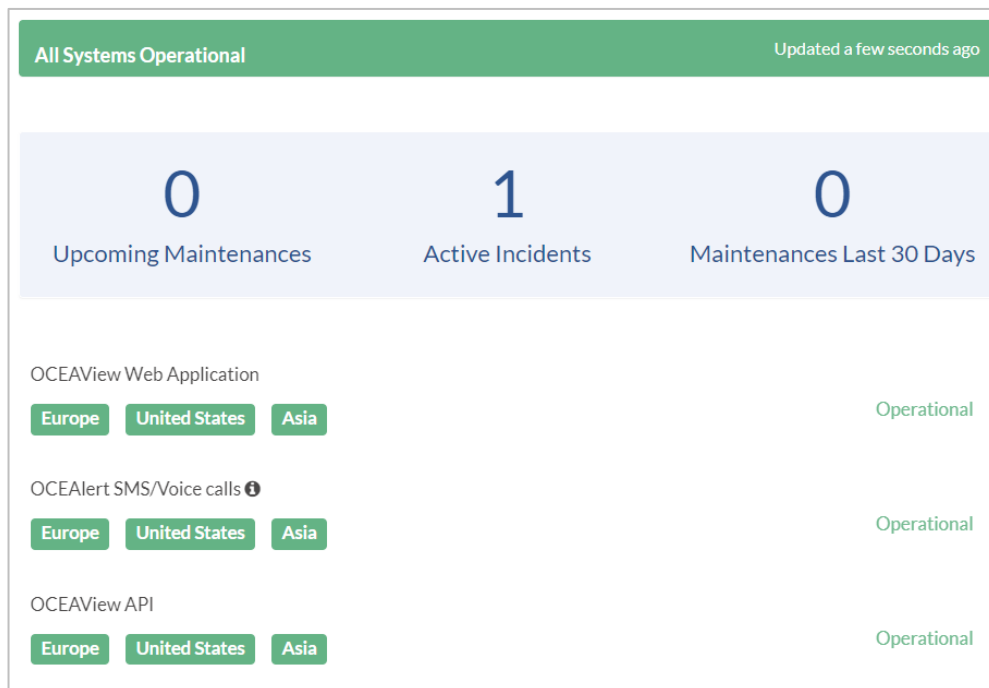


Figure 242 – OCEAView Status Dashboard

### 18.1 Overview of the OCEAView Status Dashboard

The status dashboard is a real-time service status and outage monitoring tool that you can access at this address: [oceaview.status.io](https://oceaview.status.io).

When you subscribe to this free service, you can also opt-in for notifications to receive instant alerts whenever there is an outage, scheduled maintenance, or slowdown affecting our platforms.

We recommend bookmarking the web page for quick access whenever you need the latest updates on our service status.



This service complements Dickson's existing customer notification procedures, allowing you to access real-time information.

It does not, however, replace manual notifications by our team, which will continue to be sent as necessary.

## 18.2 The different statuses

The OCEAView Status Dashboard allows you to check the status of the various Dickson services:

<b>OCEAView Web Application</b>	Access to data on the oceaview.com Cloud platform
<b>OCEAlert Notifications</b>	Sending of OCEAlert notifications by phone call and/or SMS for OCEAView customers.
<b>OCEAView Device Communication</b>	Data logger communication to OCEAView Cloud.

Each service can have different statuses:

<b>Operational</b>	Normal operation
<b>Degraded Performance</b>	All components are working, but slowness and delays may occur. The user experience is not optimal.
<b>Partial Service Disruption</b>	Problem with a specific component (example: access to the platform is possible, but false "Lost Communication" alarms are being triggered)
<b>Service Disruption</b>	Issue blocking normal use of the solution.

## 18.3 Accessing the OCEAView Status Dashboard

You can use the OCEAView Status Dashboard at any time by accessing the site [oceaview.status.io](http://oceaview.status.io).

Feel free to subscribe to be notified immediately in case of a system event occurs. You can subscribe to any specific service and region (we recommend you specifically select the region in which your OCEAView account is registered). This selection can be modified at any time in [oceaview.status.io](http://oceaview.status.io).



# DICKSON

Environmental Monitoring + Compliance Experts

Dickson North America  
Addison, IL - USA

+1 (630) 543-3747  
contact@dicksondata.com

Dickson Europe  
Montpellier - France

+33 (0)4 99 13 67 30  
contact@dicksondata.fr

Dickson Asia-Pacific  
Petaling Jaya - Malaysia

+603 749 40758  
contact@dicksondata.my

[www.dicksondata.com](http://www.dicksondata.com)