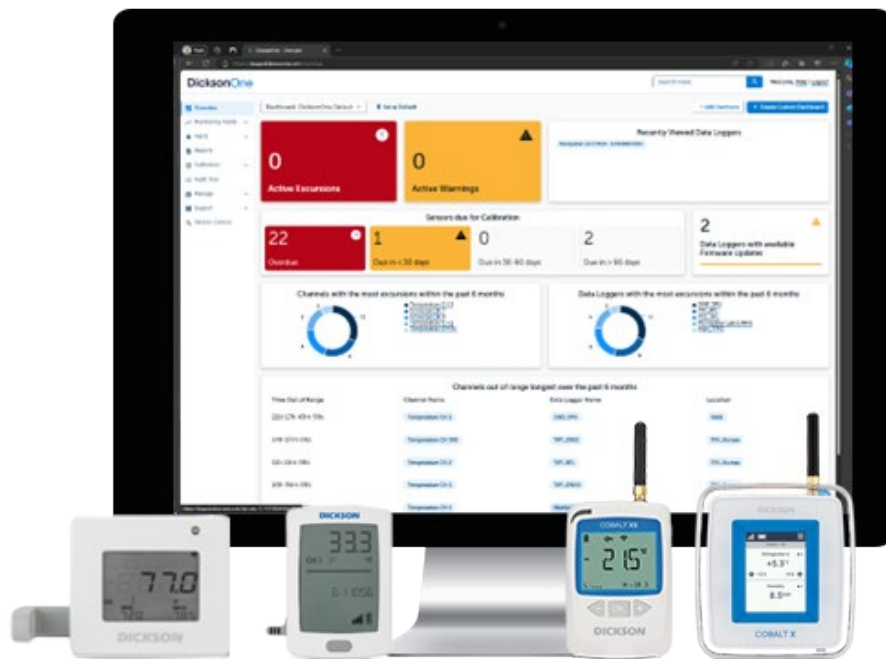


DicksonOne™

Monitoring Solution

Web application essentials
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

© 2024 Dickson. All rights reserved. Dickson, the Dickson logo, DicksonOne, RFL, DWE, and Cobalt X are the exclusive property of Dickson. The LoRa® name and associated logo are trademarks of Semtech Corporation or its subsidiaries. LoRaWAN® is a trademark of Semtech Corporation. All other brands are the property of their respective owners. Specifications subject to change without notice. Images are non-contractual.

Document updated for DicksonOne v1.12.x.

Table of contents

General notices and safety	2
1 Adding data loggers.....	5
1.1 Adding new data loggers to DicksonOne.....	5
1.2 Configuring and registering the data logger	6
2 Adding or deleting a location.....	7
2.1 Adding a location.....	7
2.2 Rearranging and deleting locations.....	8
3 Adding new users.....	9
3.1 Adding a new user	9
3.2 User invitations.....	11
4 Customizing alarms.....	12
4.1 Creating alarms for a data logger	12
5 Alarm templates	17
6 Reviewing and acknowledging alarm alerts	23
6.1 Alert details	24
6.2 Reviewing Alerts.....	25
6.3 Acknowledging Alerts	26
6.4 Commenting on alerts.....	27
7 Creating reports	28
7.1 How to create a report	28
8 Exporting data logger data.....	32
8.1 How to export data in MS Excel format.....	32
8.2 Using CSV or MS Excel files in highly regulated environments.....	34
9 Troubleshooting.....	35
9.1 DWE data logger error codes.....	35
9.1.1 Error codes displayed on the data logger.....	35
9.1.2 LED Functionality.....	36
10 RFL data logger troubleshooting.....	37
10.1 RFL data logger error messages	39
10.2 Understanding how "Not reporting" alarms work	40

11 Credit card payment failed (Stripe)	41
11.1 About credit card payments	41
11.2 Subscription is cancelled in case of failed payment	41
11.3 What to do if credit card payment fails	42
12 IT requirements and notes	43
12.1 Data Loggers (DWE2)	43
12.2 DWE2 and MDIX	44
12.3 RF LoRa data logging system	44
12.3.1 LoRa System Components	44
12.3.2 LoRa System requirements	45
12.4 VLANs	45
12.5 Local IP Addresses	45
12.6 Safe-listing application IP addresses/FQDNs for firewalls	46
12.7 MAC address filtering	47
12.8 Backup data independently from DicksonOne	48
12.9 Integrations & REST APIs	48
12.10 Wi-Fi Access Points	48

1 Adding data loggers

- Dickson Display Data loggers (DWE) must be connected to the Internet via Ethernet or Wi-Fi before you can register the devices. For the RF System, the RF gateway must be connected to the Internet and registered to your account before you can register your RF data loggers.
- All data loggers will display a 6-digit registration code for registration (described in the Quick-start guide provided with your data loggers).

Note: If you are using RF loggers, please see [Register RF Loggers](#) for more detailed instructions.

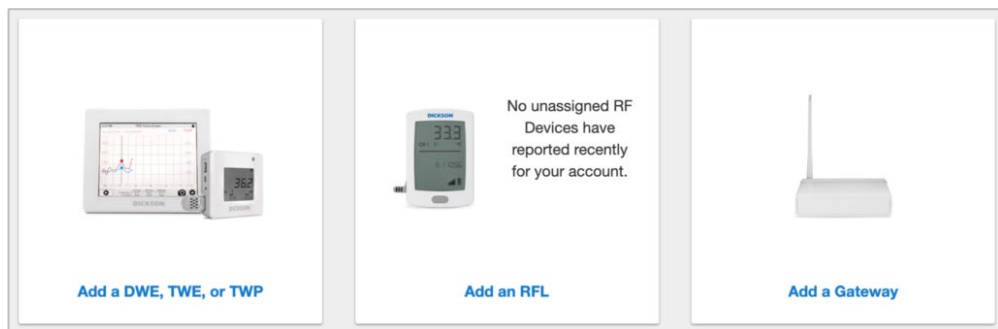
1.1 Adding new data loggers to DicksonOne

1. Log in to On DicksonOne, then click on **+Register New Hardware**.



Note If you need to connect your touchscreen device of display data logger to the Internet, please see [Connect a Device to Wi-Fi](#) or [Connect a Device to Ethernet](#)

2. Click on the device model that you need to register.



For more detailed information on the RF System, please visit [Register RF Loggers](#).

1.2 Configuring and registering the data logger

1. Provide a **Device Name** (i.e., Refrigerator One, Ambient Room 123)
2. Enter the 6-digit registration code found on the device screen (touchscreen devices display the code in the network screen).
3. To select a location for the device:
 - Use the drop-down list to select a **Location** from existing options the drop-down location options, or
 - Create a new location for the device by clicking on **Add New Location**
4. Review the Company Default Settings or Edit them to make adjustments
5. Click **Register Device**

The screenshot shows a web form titled "Register Device". At the top, there are two tabs: "DicksonOne Device" (selected) and "Legacy Device". Below the tabs, there are three required fields: "Device Name", "Registration Code", and "Location". The "Location" field is a dropdown menu currently showing "Cooper Tire". To the right of the dropdown is a button labeled "Add New Location". Below these fields is a section titled "Device Settings" with two links: "Company Default" (selected) and "Edit". At the bottom right of the form is a large blue button labeled "Register Device".

To learn more about DicksonOne features such as how to create alarms, please visit the DicksonOne [Knowledge Base](#).

2 Adding or deleting a location

- Locations allow users to control how devices in the account are organized by location and/or application (e.g. *Laboratory, Refrigerators, Pharma Co., etc.*)
- Locations make it possible to control user permissions that restrict a user to *No Access, Read Only, or Manage Access* for specific locations.
- This function is presented as “Parent-Child” relationship where the account name (e.g. Pharma Co.) is the super location in which locations and sub-locations can be created.

2.1 Adding a location

1. Log in to DicksonOne.com and select **Manage → Locations**
2. Select the **Parent Location** from the drop-down list (**1**) to specify where the location is situated.
3. In the **New location name** field (**2**), provide a name for the location (e.g. Cold Room Storage)
4. Click **Add Location** (**3**).

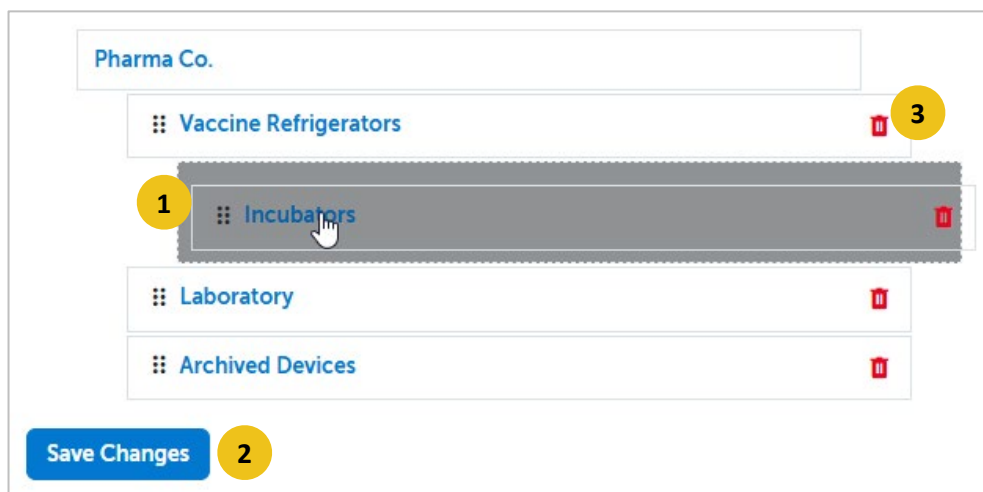
The screenshot shows a web application window titled "Locations". Inside, there is a "New Location" form. The form contains a "Parent location" dropdown menu with "Pharma Co." selected, a "New location name" text input field containing "Cold Room Storage", and a blue "Add Location" button. Three yellow circular callouts with numbers 1, 2, and 3 are overlaid on the form. Callout 1 points to the "Parent location" dropdown, callout 2 points to the "New location name" text field, and callout 3 points to the "Add Location" button. Below the dropdown, there is a small italicized text note: "Locations are nested within other locations. Select the 'Parent' you want to create a location within."

Note You can add as many locations as you want. When archiving devices, we recommend creating a location for those devices to access them easily.

2.2 Rearranging and deleting locations

Follow these steps to manage your list of locations.

1. Log in to DicksonOne and select **Manage** → **Locations** to access the list of locations.



2. To rearrange the list by moving items: hover your mouse over a location name (1), then click and drag the location up or down, or position it as a sub-location beneath another location as desired.
3. To delete a location, click the trash can icon (3).
4. Click **Save Changes** (2) to apply any changes you make to the list, or click on an option in the left-hand menu to leave this page without saving changes.

Deleting a location does **NOT** delete the devices from that location. If a location is deleted, the devices it contains are moved to the parent location.

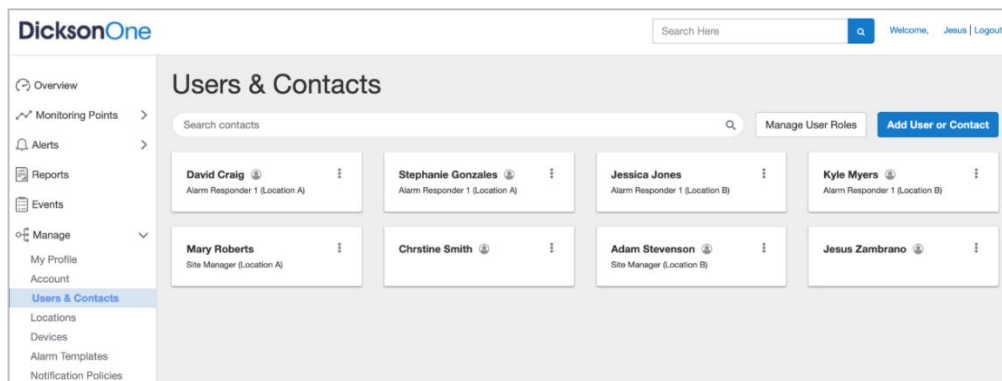
3 Adding new users

In the DicksonOne monitoring solution:

- The term “Users” refers to individuals who log in and out of DicksonOne and are controlled by different User Permissions.
- The account [owner](#) is the individual who created the DicksonOne account. The account owner automatically has all permissions to manage every aspect of the system.
- The account owner can create users with the following permissions:
Manage Access Users who can administer the account.
Read Only Access Users who can view only, based on location permissions.
- You can add an unlimited number of users to your DicksonOne account.

3.1 Adding a new user

1. Log in to DicksonOne and select **Manage → Users & Contacts**
2. Click on **Add User or Contact**



Note about Contacts You can add additional [Contacts](#) to your account. Contacts are individuals who do not have access to the system but may need to be notified during alarm events.

Add User or Contact

1 First Name

Last Name

Role (Optional)
Assign a role to a user/contact if alerts will be configured to send to individuals with specific roles. If no roles are available, contact your account Owner to enable functionality.

2 Choose a role...

Locations (Optional)
Select one or more locations that this user/contact has responsibility over and may receive alerts for.

3 Select locations

Contact Info

Label Email

4 + Add email address
+ Add phone number

5 ☒ Make this contact a user?
They'll be granted access to your account. Their permissions can be configured below.

Location Permissions

The permission level for a child location must be the same as or more permissive than that of its parent.
Select All: No Access | Read Only | Manage

Location	No Access	Read Only	Manage
6 Pharma Co	☒	☐	☐
Incubators	☒	☐	☐
Metrology	☒	☐	☐
Mapping	☒	☐	☐

Submit **Back**

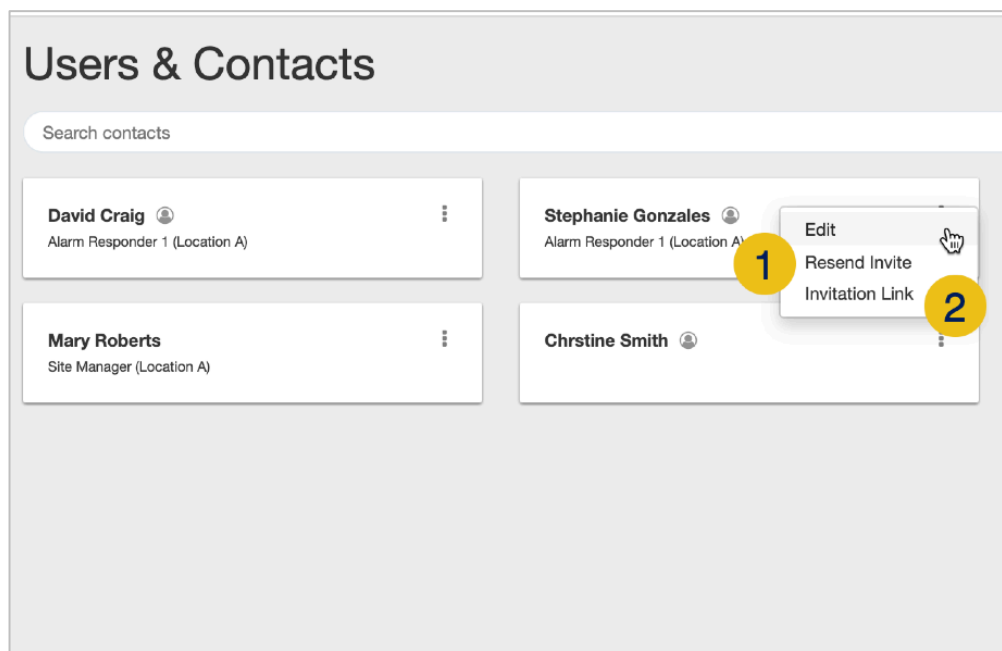
3. In this screen, provide information about the user.
- First Name, Last Name, and Email are required (**1**).
 - Use the drop-down list to determine if you would like to add an optional [Role](#) (**2**) and Location for the user (**3**).
 - Enter the user's email address. You can add additional email addresses by clicking **+Add email address** (**4**).
 - You may optionally add a phone number if you want the user to be notified via SMS or phone call during excursions or warning alerts.

4. Slide the toggle next to **Make this contact a user?** (5) to make the individual a User.
5. Use the Location Permissions zone (6) to assign permissions for the user by selecting **No Access**, **Read Only**, or **Manage** for each specific location.
6. Click **Submit** to save your changes when done.

3.2 User invitations

New users receive an email message with a link to log in and validate their account. After clicking on the link, the user can create a password to log in.

1. If the link in the e-mail expires, you can click on the options (⋮) icon next to the user name and select **Resend Invite** (1) to send a new email and link to the user.
2. You can click on **Invitation Link** (2) to copy the link so you can deliver it to the user in case they do not receive the system email.



You can add as many users as you want in DicksonOne. To learn more about User Permissions, please visit the DicksonOne [Knowledge Base](#).

4 Customizing alarms

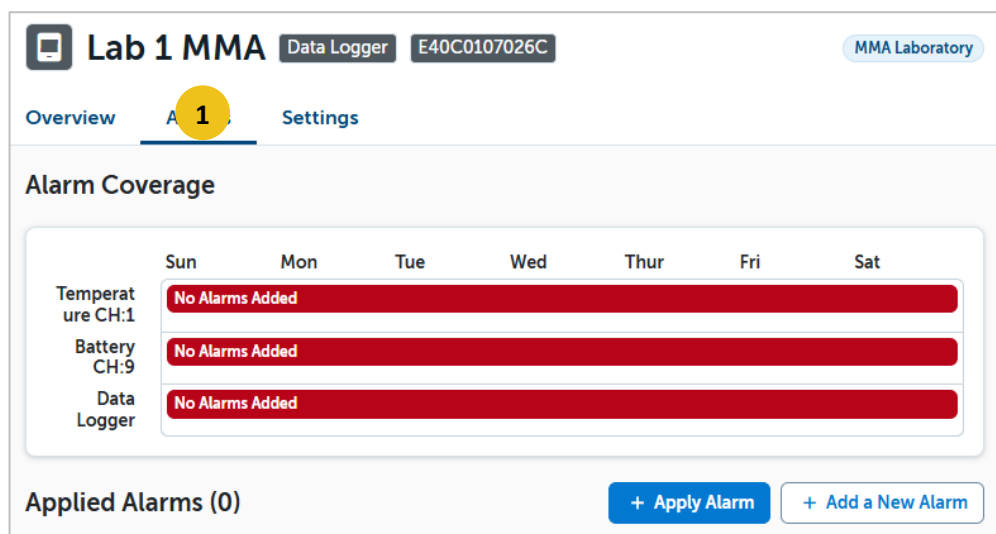
Alarms are a key feature in the DicksonOne monitoring solution, enabling users to be notified in case of excursions recorded by data loggers. To summarize:

- Creating custom alarms allow users to create alarms specifically for a data logger without using an alarm template
- Alarms alert individuals when conditions pre-determined by users are met, such as temperature excursions where the temperature exceeds a specified value.
- Users can be alerted via email, SMS, and/or phone call.

4.1 Creating alarms for a data logger

Note There are several ways to set up alarms and apply them to data loggers. If an alarm template has already been created, you can click on **+Apply Alarm** to use it. To learn more about Alarm Templates, please visit the support section in DicksonOne.

1. Log in to DicksonOne.com, then click on **Manage → Data loggers** to open the desired data logger.
2. Click on the **Alarms** tab (**1**).



3. Click on **+ Add a New Alarm** to define a new alarm.

4. Use the drop-down menus to set the conditions and determine the purpose of the alarm.

This example shows that an alarm will be generated if the sensor on Channel 1 drops below 0.5°C.

1) Set Your Condition

When Select a Channel



1) Set Your Condition

When Temperature CH:1 is below 0.5 °C

☒ Add a reference line to your data logger graph

Alarms can be created for sensor channels or the device itself. The options in the drop-down lists adapt according to your choices. Help and tips are displayed on the right-hand side of the screen to guide you.

Use the **Add a reference line** slider ( ⇌ ) if you want to include a reference line to the indicated value in the data logger graph.

5. In the next zone, set up the notification policy details for the alarm. Use the slider **Audible Alarm** ( ⇌ ) to choose whether to activate an audible alarm:

2) Set Your Notification Policy

☒ Audible Alarm

Escalate as warning or excursion?

☐ Warning

☒ Excursion

When should we sound the alarm?

Wait 0 readings (Will alert Immediately) before triggering the audible alarm.

Audible Alarm

When activated, this triggers a sound alarm on the data logger

Escalate as warning or excursion?

Warnings do not need to be acknowledged in the system; excursions must be acknowledged.

When should we sound the alarm?

This determines how quickly the alarm sound is triggered when the alarm

condition has been met. The value for the **Wait** field is expressed in the number of readings (thus based on the sample interval) to allow before triggering the alarm. If set to “0” readings, the alarm is triggered immediately.

6. If you want to contact people in the event of an alarm, click on **+ Add Custom Escalation Group**. You may add up to three custom escalation groups to meet your needs:

[+ Add Custom Escalation Group](#)



Escalation No. 01

Escalate as warning or excursion?

☐ Warning
☒ Excursion

When should we let your contacts know?

Wait readings (Will alert Immediately) before contacting them.

Who do you want to contact?

Notification No. 01 [Remove](#)

Send SMS to ▼

Fred Nobel ▼

work-phone ▼

[+ Add Another Notification](#)

Escalate as warning or excursion? Warnings do not need to be acknowledged in the system; excursions must be acknowledged. Read more on [Warnings vs. Excursions](#).

When should we let your contacts know? This determines how quickly the alarm sound is triggered when the alarm condition has been met. The value for the **Wait** field is expressed in the number of readings (thus based on the sample interval) to allow before triggering the alarm. If set to “0” readings, the alarm is triggered immediately.

Who do you want to contact?

Specify the person to contact as well as the contact method (SMS, phone call, or email). The options in the drop-down lists adapt according to your choices. Help and tips are displayed on the right-hand side of the screen to guide you.

To add more notifications for this alarm, click on **+ Add Another Notification**. You may add as many notifications as you want to each escalation level.

You can click on **Remove** to clear a notification from this list.

7. Use the slider in the **Set Alarm Schedule** ( ⇌ ) zone to specify when alarms should be managed for the data logger. By default the data logger is set to handle alarms at all times. When you deactivate 24/7 alarms using the slider, you can manage the finer details of alarm scheduling to meet your needs:

3) Set Alarm Schedule

☒ Have this alarm active 24/7

☒ Have this alarm active 24/7

Select the day(s) you'd like this alarm active

Alarm schedules do not support transitions from one day to the next day. A start time and end time must be selected for each day that is added. If more shifts are needed, please click '+Add days and/or Times.'

☐ Sun
☐ Mon
☐ Tue
☐ Wed
☐ Thur
☐ Fri
☐ Sat

Active From:

00 : 00

Until:

23 : 59

+ Add Days and/or Times

☐ Enable Buffer

Applying a buffer to an alarm will allow alerts that begin outside of the scheduled window to trigger notifications immediately once the scheduled period begins. This setting can be used to escalate alerts between alarms and ensure that multiple shifts are covered.

☐ Enable After-Hours Notifications

Enabling after-hours notifications will allow back-to-normal alert notifications to be delivered to users when an alarm is triggered during the scheduled window, but is resolved outside of the alarm schedule. When after-hours notifications are not enabled, the system will not send notifications for alarms resolved outside of the alarm schedule.

Have this alarm active 24/7

Use the slider to set this as desired. If alarms are not active 24/7, the zone expands and you can specify related details.

Select the days you'd like this alarm active

Click in the checkboxes to select days on which alarms should be activated, and indicate the times for each day. You can add more day/time selections by clicking on **+Add Days and/or Times**.

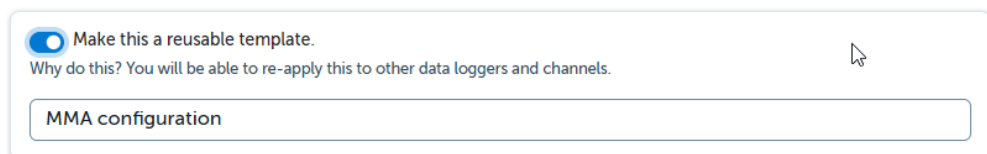
Enable Buffer

Applying a buffer to an alarm allows alerts that begin outside the scheduled window to trigger notifications immediately once the scheduled period begins. This setting can be used to escalate alerts between alarms and ensure that multiple shifts are covered.

Enable After-Hours Notifications

Enabling after-hours notifications will allow back-to-normal alert notifications to be delivered to users when an alarm is triggered during the scheduled window, but is resolved outside of the alarm schedule. When after-hours notifications are not enabled, the system will not send notifications for alarms resolved outside of the alarm schedule.

8. If you want to be able to reuse these same alarm settings for other data loggers, you can use the slider to activate the option **Make this a reusable template**. Then enter a name for the template.



The screenshot shows a configuration window with a toggle switch labeled 'Make this a reusable template.' which is currently turned on. Below the toggle is a text explanation: 'Why do this? You will be able to re-apply this to other data loggers and channels.' At the bottom of the window is a text input field containing the text 'MMA configuration'.

9. Click on **Save Alarm** to save your settings and finalize configuration. If you don't want to save your changes at all, click on **Cancel**.

5 Alarm templates

- An alarm template is a set of conditions and associated notifications (emails, texts, phone calls, etc.) that can be applied to a group of loggers in bulk or to a new logger once it has been added.
- The goal is to reduce the recreation of the same alarm conditions over and over. This feature is particularly helpful for accounts with many loggers and even more so when the loggers are monitoring the same application (a large number of refrigerators and freezers storing vaccines for example).



A two channel temperature device with two probes monitoring different ranges should have two separate alarm templates.

Creating an alarm template

1. Log in to DicksonOne, then click on **Manage → Alarm Templates** in the left-hand menu.
2. To add a new template, click **+Add New Template**
3. Enter a name for the template and click on **Continue**

1) Name Your Template

Name *

Continue

Remember to choose a name that will be meaningful for the people using the template. The name can reflect the assets and monitoring points related to the alarm.

4. In the screen shown below, use the drop-down menus to set the conditions and determine the purpose of the alarm.

This example shows that an alarm will be generated if the sensor on Channel 1 drops below 0.5°C.

The screenshot shows a form titled "2) Set Your Conditions". It contains a "When" label followed by a dropdown menu with the text "Select a Channel". Below this is a blue link "+ Add Another Condition". A downward arrow points to a second, more detailed form. This second form also has a "When" label, followed by a dropdown menu with "Temperature", then another dropdown menu with "is below", then a text input field containing "0.5", and finally a dropdown menu with "°C". Below this second form is also a blue link "+ Add Another Condition".

Alarms can be created for sensor channels or the device itself. The options in the drop-down lists adapt according to your choices. Help and tips are displayed on the right-hand side of the screen to guide you.

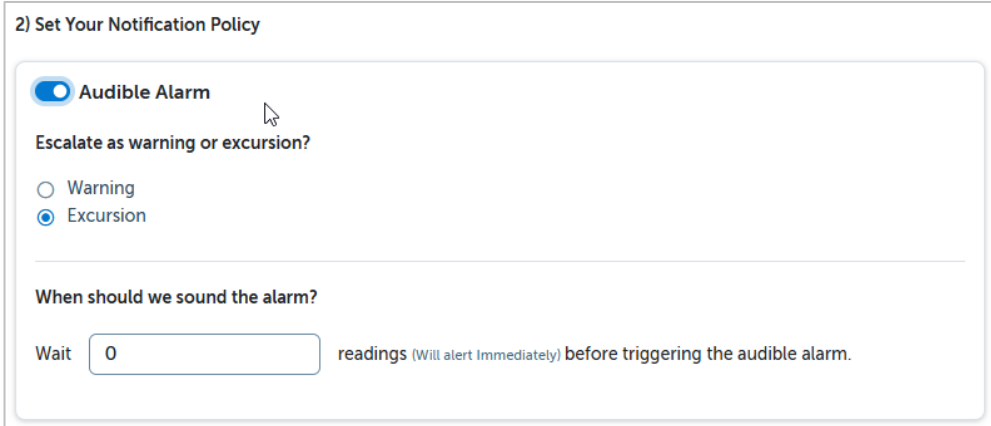
You can add more than one alarm condition by clicking on **+Add Another Condition**.

5. Click on **Continue** to specify the notification policy. A notification policy can have up to three escalations. Each escalation consists of three components: when to send the alert, the method to use, and who to contact. If notification policies have already been set up, you can choose from here.

The screenshot shows a form titled "3) Set Your Notification Policy". It has two tabs: "Use Existing" (which is selected and underlined) and "Create New". To the right of the "Create New" tab is a yellow circle with the number "1". Below the tabs is a dropdown menu with the text "Select an escalation policy..." and a downward arrow.

Otherwise, create new notification settings as described below.

6. Click to open the **Create New** tab (**1**).
7. In the next zone, set up the notification policy details for the alarm. Use the slider **Audible Alarm** ( ⇔ ) to choose whether to activate an audible alarm:



2) Set Your Notification Policy

☒ Audible Alarm

Escalate as warning or excursion?

☐ Warning

☒ Excursion

When should we sound the alarm?

Wait readings (Will alert Immediately) before triggering the audible alarm.

Audible Alarm	When activated, this triggers a sound alarm on the data logger
Escalate as warning or excursion?	Warnings do not need to be acknowledged in the system; excursions must be acknowledged.
When should we sound the alarm?	This determines how quickly the alarm sound is triggered when the alarm condition has been met. The value for the Wait field is expressed in the number of readings (thus based on the sample interval) to allow before triggering the alarm. If set to "0" readings, the alarm is triggered immediately.

8. If you want to contact people in the event of an alarm, click on **+ Add Custom Escalation Group**. You may add up to three custom escalation groups to meet your needs:

[+ Add Custom Escalation Group](#)

↓

Escalation No. 01

Escalate as warning or excursion?

☐ Warning

☒ Excursion

When should we let your contacts know?

Wait readings (Will alert Immediately) before contacting them.

Who do you want to contact?

Notification No. 01 [Remove](#)

Send SMS to ▼

Fred Nobel ▼

work-phone ▼

[+ Add Another Notification](#)

Escalate as warning or excursion? Warnings do not need to be acknowledged in the system; excursions must be acknowledged. Read more on [Warnings vs. Excursions](#).

When should we let your contacts know? This determines how quickly the alarm sound is triggered when the alarm condition has been met. The value for the **Wait** field is expressed in the number of readings (thus based on the sample interval) to allow before triggering the alarm. If set to “0” readings, the alarm is triggered immediately.

Who do you want to contact? Specify the person to contact as well as the contact method (SMS, phone call, or email). The options in the drop-down lists adapt according to your choices. Help and tips are displayed on the right-hand side of the screen to guide you.

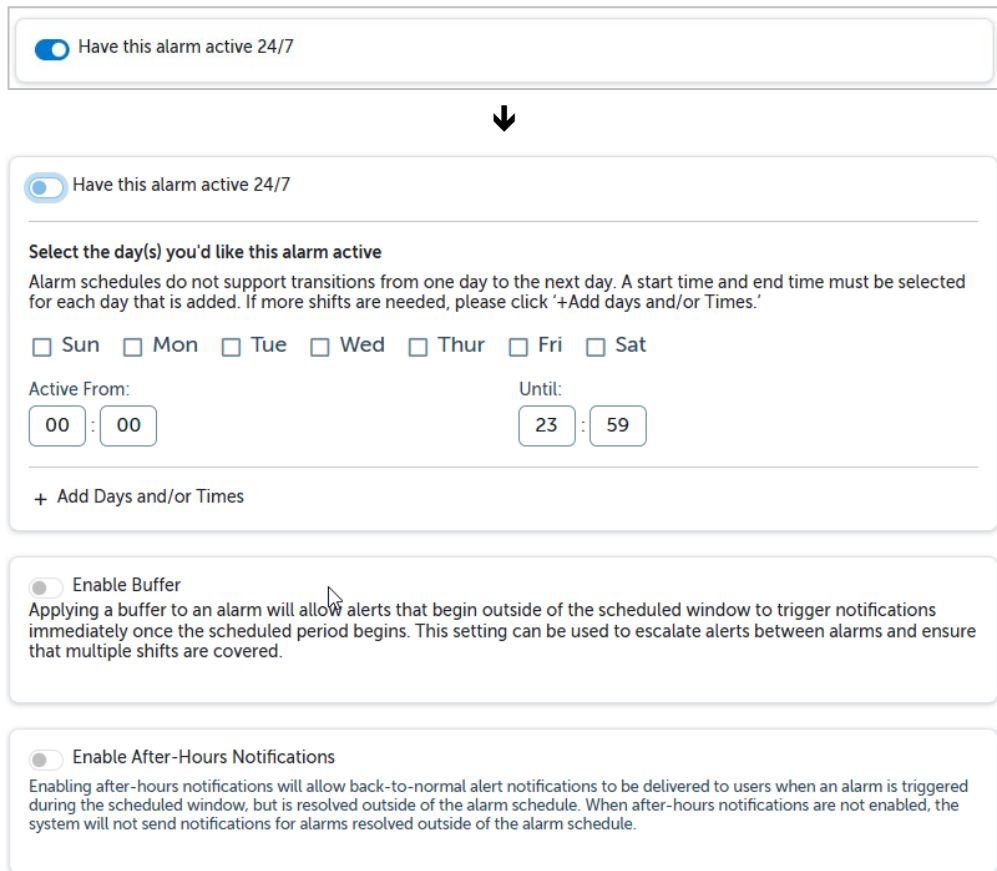
To add more notifications for this alarm, click on **+ Add Another**

Notification. You may add as many notifications as you want to each escalation level.

You can click on **Remove** to clear a notification from this list.

9. Click on **Continue**

10. Use the slider in the **Set Alarm Schedule** ( ⇌ ) zone to specify when alarms should be managed for the data logger. By default the data logger is set to handle alarms at all times. When you deactivate 24/7 alarms using the slider, you can manage the finer details of alarm scheduling to meet your needs:



☒ Have this alarm active 24/7

↓

☐ Have this alarm active 24/7

Select the day(s) you'd like this alarm active
 Alarm schedules do not support transitions from one day to the next day. A start time and end time must be selected for each day that is added. If more shifts are needed, please click '+Add days and/or Times.'

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thur ☐ Fri ☐ Sat

Active From: : Until: :

+ Add Days and/or Times

☐ **Enable Buffer**
 Applying a buffer to an alarm will allow alerts that begin outside of the scheduled window to trigger notifications immediately once the scheduled period begins. This setting can be used to escalate alerts between alarms and ensure that multiple shifts are covered.

☐ **Enable After-Hours Notifications**
 Enabling after-hours notifications will allow back-to-normal alert notifications to be delivered to users when an alarm is triggered during the scheduled window, but is resolved outside of the alarm schedule. When after-hours notifications are not enabled, the system will not send notifications for alarms resolved outside of the alarm schedule.

Have this alarm active 24/7

Use the slider to set this as desired. If alarms are not active 24/7, the zone expands and you can specify related details.

Select the days you'd like this alarm active

Click in the checkboxes to select days on which alarms should be activated, and indicate the times for each day. You can

Enable Buffer

add more day/time selections by clicking on **+Add Days and/or Times**.

Applying a buffer to an alarm allows alerts that begin outside the scheduled window to trigger notifications immediately once the scheduled period begins. This setting can be used to escalate alerts between alarms and ensure that multiple shifts are covered.

Enable After-Hours Notifications

Enabling after-hours notifications will allow back-to-normal alert notifications to be delivered to users when an alarm is triggered during the scheduled window, but is resolved outside of the alarm schedule. When after-hours notifications are not enabled, the system will not send notifications for alarms resolved outside of the alarm schedule.

11. Click on **Continue** to choose which sensor channels and/or data loggers are concerned by the alarm template.

5) Add Channels/Data Loggers

If you'd like to apply this template to the channels on a data loggers now, you can select from the list below or search to narrow down your selection. You can come back and do this at any time or apply a template to channels from a data logger's alarm page.

Search:

Results (1)

- ☒ Refrigerator - Lab 1 MMA - E40C0107026C - Temperature CH:1

Applied to Template (1)

- Refrigerator - Lab 1 MMA - E40C0107026C - Temperature CH:1

[Continue](#) [Back](#)

If you want to apply this template to the channels on one or more data loggers now, you can select from the list or enter text into the search field to narrow down your selection. You can search for devices, channels, or additional tags to apply the template.

You can come back and do this at any time or apply a template to channels from a data logger's alarm page.

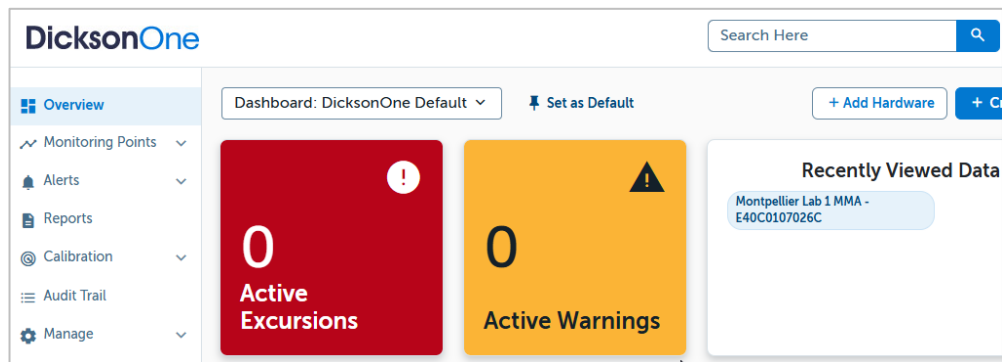
As you select data loggers or channels, they are displayed on the right-hand side of the screen under **Applied to Template**.

12. Click **Continue** to save the template. You may edit templates at any time as described in this section.

6 Reviewing and acknowledging alarm alerts

- In your DicksonOne account, you can review, acknowledge, and add comments to your current and historical alerts.
- Alerts are the result of triggered alarms, which are captured in the Alerts and Events pages of your account.
- Alert notifications are delivered to users via email, text message, and/or phone call based on the alarm configurations.
- Alerts are categorized as either warning alerts or excursion alerts based on alarm configurations.

The count of active alerts is highlighted on the dashboard in the **Active Excursions** and **Active Warnings** tiles, as shown below.



You can navigate to the alert pages by clicking on either of these tile or by using the left-hand menu to select **Alerts → Excursions** or **Alerts → Warnings**

When you click on **Overview**, **Excursions**, or **Warnings**, you are directed to the respective alerts page filtered accordingly to show all active alerts, active excursions, or active warnings.

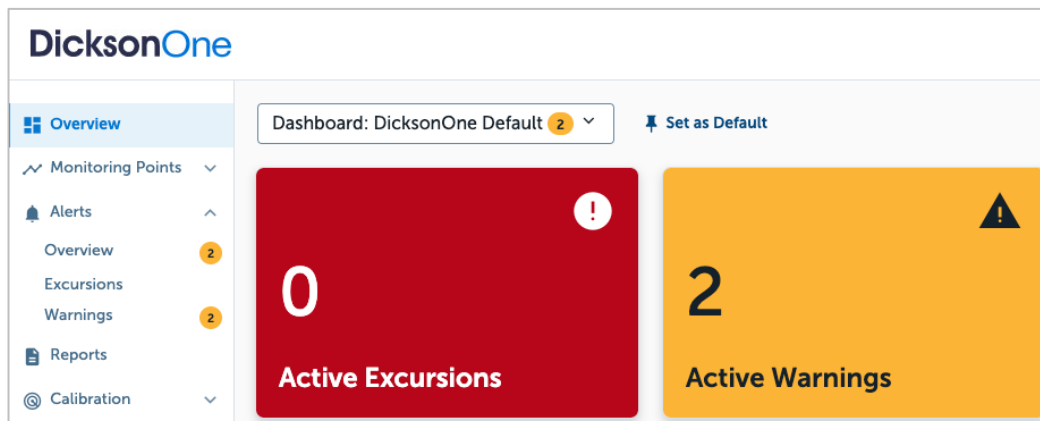
6.1 Alert details

To see the details of an alert, click **View More** (1) to expand the row. To see details for multiple alerts, use the **Expand All** button (2) at the top of the table to quickly expand all the rows.

Clicking on an alert opens a window in which you can acknowledge or snooze the alert. Acknowledge the alert (3) to confirm that it has been seen, or choose Snooze if you do not want the escalation policy to continue. Snoozing the alert automatically acknowledges the alert, limiting the number of clicks needed.

6.2 Reviewing Alerts

The count of active alerts is highlighted on the dashboard in the **Active Excursions** and **Active Warnings** tiles. You can navigate to the alerts pages by clicking on either tile or by clicking on **Alerts** using the left navigation bar.



1. You can filter alerts on various criteria by clicking on **More Filters** (**1**), including alert severity, trigger time, resolution time, affected data loggers, locations, acknowledgment status, and condition.
2. "Active" alerts remain in active status until the alarm conditions return to normal.
3. The full history of alerts, including resolved alerts, can be seen by removing the "Only Active Alerts?" filter that is automatically applied on the Alerts pages. This filter appears at the top of the table and in the **More Filters** pane.

Type	Status	Condition	Duration	Equipment	Logger	Recent Reading	Triggered
Warning	Active & Not Acknowledged	Temperature CH1 is below -5.0°F	6 minutes	Freezer 3		-16.3°F	06/05/2024 3:42:52 pm View More
Excursion	Active & Not Acknowledged	Temperature CH1 is below 35.6°F	6 minutes	Refrigerator 10		36.6°F	06/05/2024 3:42:52 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	a minute	Freezer 3		-16.3°F	06/05/2024 3:40:52 pm View More
Excursion	Active & Not Acknowledged	Temperature CH1 is above 70°C	11 minutes	Refrigerator 1		8.1°C	06/05/2024 3:37:52 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	3 minutes	Freezer 3		-16.3°F	06/05/2024 3:36:52 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	a minute	Freezer 3		-16.3°F	06/05/2024 3:33:52 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	a minute	Freezer 3		-16.3°F	06/05/2024 3:30:52 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	6 minutes	Freezer 3		-16.3°F	06/05/2024 3:21:51 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	4 minutes	Freezer 3		-16.3°F	06/05/2024 3:15:51 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	3 minutes	Freezer 3		-16.3°F	06/05/2024 3:11:51 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	2 minutes	Freezer 3		-16.3°F	06/05/2024 3:06:51 pm View More
Warning	Resolved & Not Acknowledged	Temperature CH1 is below -5.0°F	a minute	Freezer 3		-16.3°F	06/05/2024 3:03:50 pm View More
Excursion	Resolved & Not Acknowledged	Temperature CH1 is below 35.6°F	15 minutes	Refrigerator 6		46.5°F	06/05/2024 3:02:50 pm View More

6.3 Acknowledging Alerts

In the Alerts pages, you can acknowledge the alerts by clicking on the alert and then clicking **Acknowledge** at the top of the Alert Details window. When an alert is acknowledged, the system will log the user and timestamp of the event. Acknowledgments can be done for all current and historical alerts.

The screenshot shows the 'RFL' Alert Details window. At the top, there are two buttons: 'Acknowledge' (highlighted with a red box) and 'Snooze'. Below these is the 'Alert Details' section, which includes a red banner stating 'Alarm Triggered : Temperature CH:1 is below 90.0°F' and a blue banner stating 'Returned to Normal : 01/31/2024 3:46:43 pm'. A table below provides details: Triggered (01/31/2024 3:40:04 pm), Promoted to Excursion (01/31/2024 3:40:04 pm), Duration (7 minutes), Alert Type (Excursion), Status (Resolved, Not Acknowledged), and Recent Reading (71.1°F). Below the table are sections for 'Alert Reason' (Reason Code dropdown), 'Corrective Action' (text input), and 'Preventive Action' (text input). A 'Save changes' button is at the bottom left. On the right, the 'Comments and Alert Events' panel shows a list of events: 'Alert triggered' (01/31/2024 3:40:04 pm), 'Alert promoted to excursion' (01/31/2024 3:40:04 pm), 'Alert notification(s) sent to: mfriske@dicksondata.com' (01/31/2024 3:40:20 pm), and 'Alert resolved' (01/31/2024 3:46:43 pm). At the bottom right is an 'Add a comment' button.

On the **Monitoring Points** → **Equipment** or **Data Loggers** overview pages, only excursion alerts are displayed in the **Annotations** table below the graph and can be acknowledged from there.

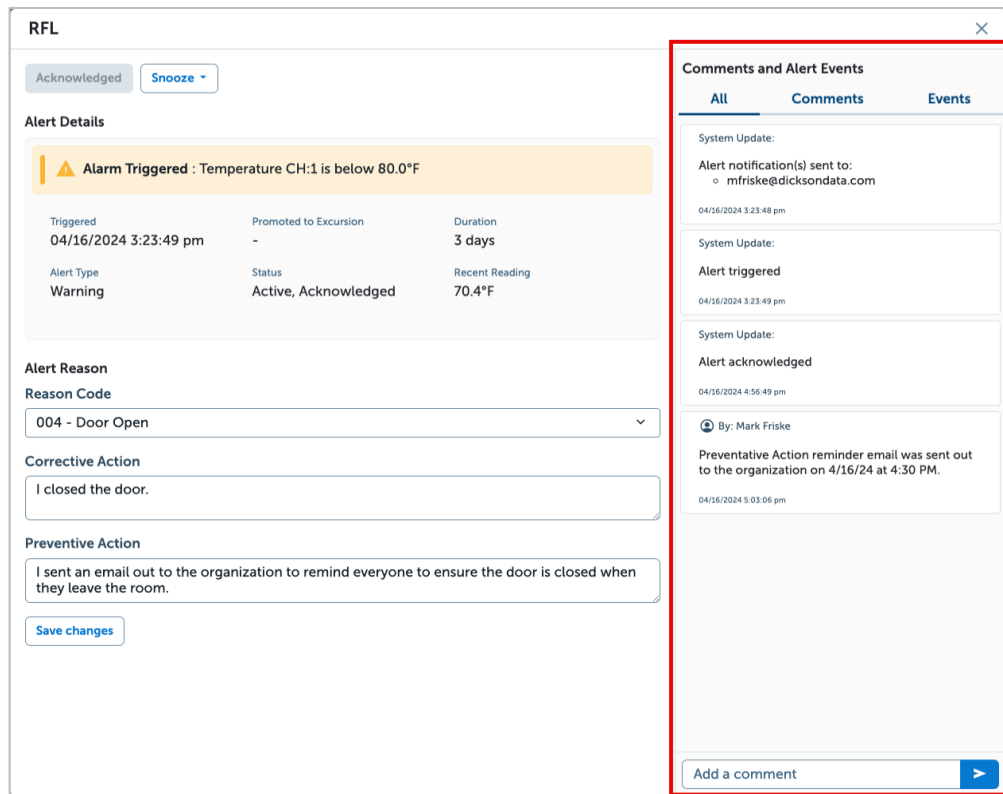
Time	Channel	Type	Annotation	
02/17/2021 4:40:35 pm	Site 1 Lab Temp	Excursion	Is Below 150.0°F Updated 02/17/2021 4:42:13 pm	<button>Acknowledge</button>
02/17/2021 4:29:35 pm	Site 1 Lab Temp	Excursion	Is Below 150.0°F Updated 02/17/2021 4:38:28 pm	<button>Comments (0)</button>

Note Both warnings and excursions are documented in the alerts pages. However, the **Monitoring Points** overview pages only show excursions as flags in the graph area and annotations.

6.4 Commenting on alerts

Comments may be added to the Comments and Alert Events log on the right side of the Alert Details screen at any time.

All users with permission to access the location corresponding to the alert can view the comments left by other users.



The screenshot shows the 'RFL' Alert Details screen. The main area displays alert information for 'Temperature CH:1 is below 80.0°F' triggered on 04/16/2024 at 3:23:49 pm. The status is 'Active, Acknowledged' with a recent reading of 70.4°F. The alert reason is '004 - Door Open'. The corrective action is 'I closed the door.' and the preventative action is 'I sent an email out to the organization to remind everyone to ensure the door is closed when they leave the room.' A 'Save changes' button is at the bottom.

The right-hand pane, titled 'Comments and Alert Events', is highlighted with a red border. It contains a log of events:

- System Update:** Alert notification(s) sent to: mfriske@dicksondata.com (04/16/2024 3:23:48 pm)
- System Update:** Alert triggered (04/16/2024 3:23:49 pm)
- System Update:** Alert acknowledged (04/16/2024 4:56:49 pm)
- By: Mark Friske** (04/16/2024 5:03:06 pm): Preventative Action reminder email was sent out to the organization on 4/16/24 at 4:30 PM.

At the bottom of the pane is an 'Add a comment' input field with a submit button.

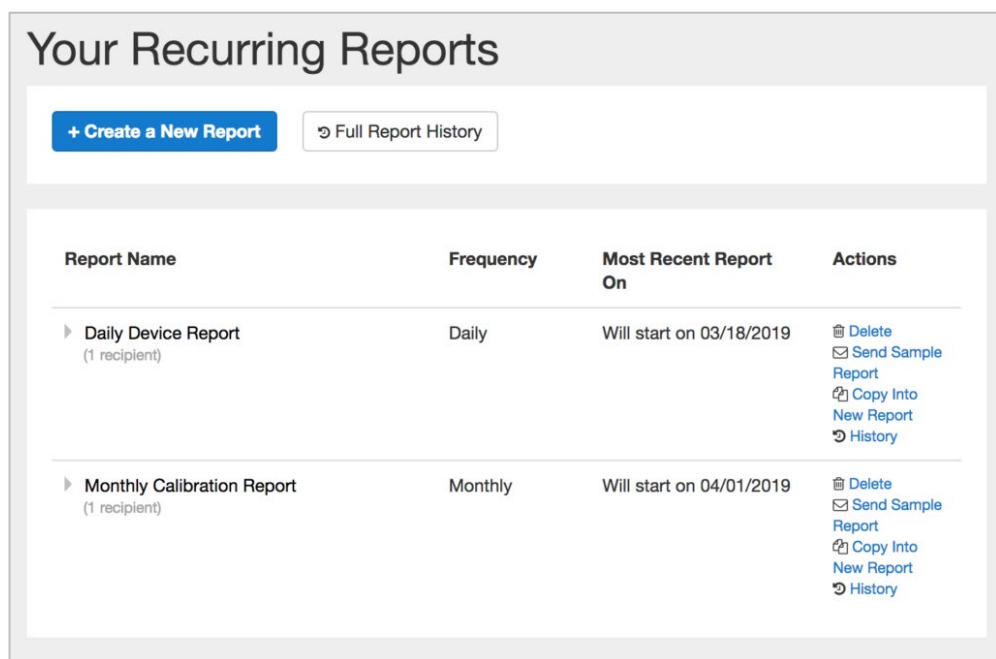
Note: Text entered into the **Corrective Action** and **Preventative Action** fields is not shown in the **Comments and Alert Events** pane on the right-hand side of the screen. These details are visible in the audit trail.

7 Creating reports

- DicksonOne allows you to create various reports for different purposes that can be useful as part of your Standard Operating Procedures (SOP) and audit purposes.
- DicksonOne reports are delivered in PDF format and are 21 CFR compliant.
- Reports can be automated so that they are emailed daily, weekly, and/or monthly.

7.1 How to create a report

1. Login to DicksonOne and select **Reports** in the left-hand menu.
2. Click **+Create a New Report**



Your Recurring Reports			
+ Create a New Report Full Report History			
Report Name	Frequency	Most Recent Report On	Actions
▶ Daily Device Report (1 recipient)	Daily	Will start on 03/18/2019	Delete Send Sample Report Copy Into New Report History
▶ Monthly Calibration Report (1 recipient)	Monthly	Will start on 04/01/2019	Delete Send Sample Report Copy Into New Report History

4. Select a report type from the down-down options.
Depending on the report type, you can use checkboxes to include a daily summary and/or add a signature line.

Build Report

Data Monitoring Points Setup Summary

Select a Report Type

Monitoring Point and Excursions

Monitoring Point and Excursions - A Monitoring Point Report provides an overview snapshot of the selected monitoring points. The report contains Excursion events, Excursion Acknowledgments and Comments, User Annotations, a Monitoring Point Graph, and Summary Data. Users have the option to include a Daily Summary and/or Signature Line on the report. The report is delivered via Email as a PDF and can be viewed on DicksonOne.

☐ Include daily summary

☐ Add signature line

Save and continue

DicksonOne 09/09/2019 - 09/16/2019
Pharma Co. Production Report

Laboratory - Ambient - 16279746

Laboratory - Ambient - 16279746
Showing at 2.0min resolution

Channel	Average	Minimum	Maximum	Mean Kinetic Temp
Ambient Temperature	74.8°F	70.5°F	77.8°F	74.9°F
Ambient Relative Humidity	54.4%RH	42.3%RH	69.5%RH	N/A
Ambient Dew Point	57.1°F	48.4°F	62.0°F	N/A

Excursion: Ambient Relative Humidity Is Below 55.0%RH

Triggered 09/16/2019 01:28:19 PM CDT

Duration 1 min

Comments Matt McNamara Alarm acknowledged 09/16/2019 01:28:59 PM CDT

Example Monitoring Point and Excursions Report

- Click **Save and continue** to select the monitoring point(s) and/or locations covered by the report.

Build Report

Data Monitoring Points Setup Summary

Choose the monitoring points to be included in your report ? Type to search

Type to begin searching for monitoring points

☐ Generate report using only Equipment instead of Data Loggers for selected Locations

Save and continue

Type text in the empty field or click in the field to select from available options.



Difference between selecting a location or a data logger

When one or more data loggers are selected, the report contains only those data loggers. If one or more locations are selected, the report will include any additional devices that are added in the future on future reports.

6. Click on **Save and continue** to continue setting up the report.

Build Report

Data Monitoring Points **Setup** Summary

Name of your report

Frequency [?] **Weekly**

Archived and legacy data loggers are not included in recurring reports. To generate a report for these data loggers, set the frequency to "Once".

Time zone [?] **(GMT+01:00) Paris**

First Report Delivery

Decimal Separator [?] **Period (.)**

Send a copy to:

+ Add Another Recipient

Save and continue

In this section, determine the frequency for how often the report should be delivered

- Provide a name for the report
- Use the pull-down menu to set the frequency
- Choose when to send the first report

7. The current user's email address is automatically selected. You can click on **+Add Another Recipient** if you want to send the report to other people.

8. Click on **Save and continue** to review and/or edit the information you provided for the report.

Build Report

DataMonitoring PointsSetupSummary

Data
Type: Monitoring Point and Excursions
Daily summary: Yes
Include signature: Yes

Edit

Monitoring Points
Reporting on the following 1 location:
MMA Lab

Edit

Setup
Report Name: Weekly
Frequency: Weekly
Time zone: Paris
Decimal Separator: Period (.)
Start date: 22/08/2024
Recipients:
your.name@yourcompany.com

Edit

Save and finish

9. Click **Save and finish** to complete the process.

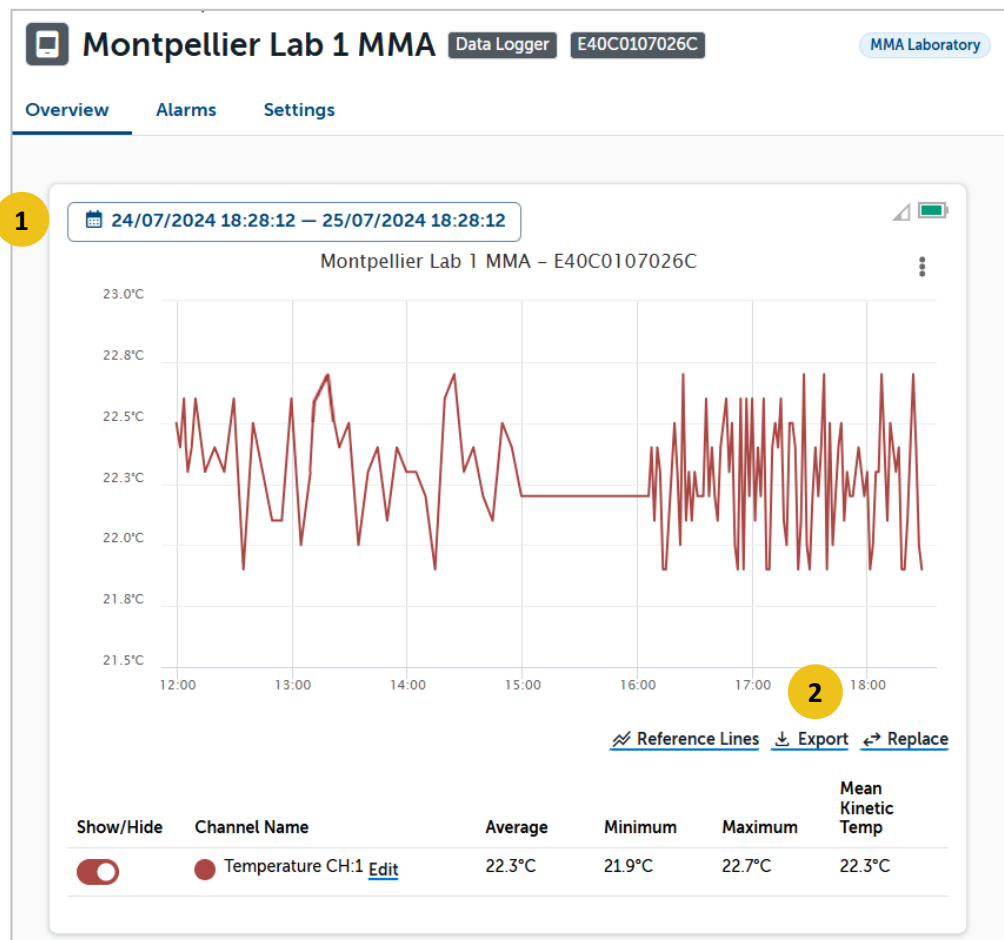
Reports can be edited as needed at any time. To learn more on how to edit a report, please visit the DicksonOne [Knowledge Base](#).

8 Exporting data logger data

- The data that is collected by each individual logger can be exported to a CSV file so you can view it, store it, or distribute it via an Excel file.

8.1 How to export data in MS Excel format

- Filter the data to cover the precise range you want to export.
- You can use the date range selector (1) to choose start/stop dates and times, or do that in the next step.



- Click on **Export** (2). You can adjust the date/time range here if you want.

Export for Montpellier

Lab 1 MMA

Starts at

24/07/2024 18:28:12

Ends at

25/07/2024 18:28:12

Export

- Complete the process by clicking on **Export**.
Within a few moments, you should receive an email message from noreply@dicksonone.com with a .zip file attached. The .zip file contains the data you exported in CSV format, which you can open easily in MS Excel.



If you did not receive the file, please add "noreply@dicksonone.com" to your email servers' approved senders list and export the file again.

- If you want to access the data directly, or at a later time, select **Manage → Exports** in the left-hand menu, where you can see all previous data exports.

Exports					
My Exports		All			
Monitoring Point	Location	Range	Requested		
Lab 1 MMA - E40C0107026C Logger	MMA Lab	24/07/2024 18:28:12 CEST– 25/07/2024 18:28:12 CEST	21/08/2024 18:43:13 CEST	By Fred Nobel	Download

Click on **Download** to access the .zip file with the data directly.

8.2 Using CSV or MS Excel files in highly regulated environments

Data that is exported to Excel is generally not considered auditor-friendly. This is because anybody can effectively alter the data contained in these types of files.

Because of this, your auditor will always consider the digitally-stored data (in this case, the data within DicksonOne) as your “system of record”, as the data stored on DicksonOne servers cannot be altered by anyone.

Nonetheless, CSV/Excel exports are a convenient way to quickly access large amounts of data for analysis and distribution among users, notably those who may not have access to the DicksonOne system.

9 Troubleshooting

9.1 DWE data logger error codes

Though DWE Devices do not offer a touchscreen interface, there are different ways we alert users by using error codes.

9.1.1 Error codes displayed on the data logger

Code	Meaning
001	USB is connected, but the device has disassociated from the PC
002	No AC power detected that is required for attempted feature or function (does not include normal battery operation)
003	Rechargeable battery not charging
004	USB stick connected, but not readable because it isn't formatted properly or otherwise unreadable
005	USB stick connected, but cannot write to the stick
006	Download to the USB stick has failed
007	Firmware update has failed
008	Internal clock battery is dead
009	Multiple firmware files found
010	No firmware found. Will clear upon reboot.
011	Error flashing new firmware during update. Will clear upon reboot.
101	No Wi-Fi settings have been configured on this device
102	The device is configured with Wi-Fi, but is not connecting to the Access Point (AP)
103	The device is connected to an Access Point (AP), but is not connected to the Internet
201	The device is connected to a switch, but is not connected to the Internet
202	The Ethernet cable is connected, but the device is not connected to/seeing the switch

9.1.2 LED Functionality

LED behavior	Function
Off	Normal state/no activity
Blinking green	Successful transmission of packet
Blink green once and blink blue once	Successful transmission of packet with a DicksonOne configuration change
Blink green once and blink red once	Failed transmission of packet
Yellow blinking until cleared	Error state
Solid blue	Updating firmware
Solid red	Loading / reloading initializing or disconnect / reconnect
Solid green	Booting up

10 RFL data logger troubleshooting

Why does the device display a dashed line and won't do anything?

Ensure that your gateway is connected to the Internet, and use the side power button on the logger to reboot it. If the logger is too far away from the gateway, you may need to move closer to the gateway and reboot the device again.

Why won't the RF loggers display a code on the screen?

Ensure that your gateway is connected to the Internet as this is required in order for the devices to get a registration code.

Press the right-side transmit button of the logger and see if the device gets a code within a minute.

If the logger is too far away from the gateway, the logger will not get a registration code if it cannot reach the gateway.

Why won't the RF loggers display in Unassigned Devices on my account?

Ensure that your gateway is registered to your DicksonOne account and connected to the Internet.

If the RF loggers display an "x" on the signal strength, the logger is not able to reach out to the gateway. Moving closer to the gateway pressing the right-side transmission button on the logger.

How far can my RF loggers be from the RF gateway?

Transmission distance is extremely dependent on the environment the loggers are used in. Generally speaking, a few hundred feet shouldn't be an issue and oftentimes devices can communicate well over 1,000 feet. The key is to have adequate coverage of the LoRa network at your facilities.

How many RF gateways do I need for my RF loggers?

At least one RF gateway is required on-site at each site. While the gateways can support more than 100 RF loggers, we recommend limiting the maximum to 100. Furthermore, there are reasons (e.g. redundancy, better coverage, etc.) you may want an additional gateway well below our recommended number.

Do RF loggers require an Internet connection?

RF loggers do not connect to the Internet, and instead reach out to your gateway automatically which the gateway must be connected to the Internet.

What happens when I delete my RF gateway from my DicksonOne account?

If your RF gateway is deleted from your DicksonOne account but remains connected to the Internet, the RF loggers will continue to send data if the loggers are still registered and active.

How do audible alarms work?

When an audible alarm is triggered on the RF logger, an alarm icon will flash on and off till the alarm is cleared.

The audible alarm will sound for an entire minute beeping, and then after a minute it will chirp every 5 minutes until the conditions go back to normal and the alarm has cleared.

How do I recalibrate my RF loggers?

RF loggers use replaceable sensors, so you can simply [purchase newly recalibrated sensors](#) and swap them out with the old ones or you can have your current sensors recalibrate to retain the as-is data. Contact us at support@dicksondata.com.

10.1 RFL data logger error messages

Error Message	Cause	Remedy
EXPORT ERR	The device is failing to export data to the flash drive.	After the flash is removed and message has cleared, attempt again to export your data. If it fails again, confirm that you are using a FAT32 flash USB stick.
BAD FILE	This occurs when the firmware file detected on the USB flash is not the correct format.	Confirm that the file on the USB flash is an .rff file. The firmware file should be downloaded from the DicksonOne change logs and should be an .rff file.
MULT FILE	This occurs when multiple firmware files are found on USB flash drive.	Make sure that the USB flash contains only one single .rff file.
BAD USB	This occurs when the USB flash is not working properly and has failed to mount.	Ensure that you are using a FAT32 USB flash. If that does not work, attempt with a second USB flash.
FLASH FAIL	Caused when an error occurs while the device is programming internal memory.	Unplug your USB from the RF logger and attempt a second time. If it does not work, attempt with a different USB flash, and be sure that it is a FAT32 flash stick.
NO PROGRAM	Occurs on startup if device determines currently loaded firmware is invalid. Clears when new USB flash drive is inserted.	Please contact Dickson at support@dicksonone.com
NO SETTING	Occurs when device has not been programmed with a valid LoRa app key.	Please contact Dickson at support@dicksonone.com



You can download the most recent RF logger firmware file in the [DicksonOne change logs](#).

10.2 Understanding how “Not reporting” alarms work

You can create “Not reporting” alarms so that you can be notified when your RF loggers stop transmitting data to your DicksonOne account.

Here are some reasons why “Not reporting” alarms may be triggered:

- The RF logger is too far away from the RF gateway to send data
- The RF gateway that the RF logger reports through has lost power or an Internet connection (not communicating on a local LAN)
- The RF logger was powered off
- The RF logger has turned off due to the batteries dying
- The sensor pod was removed from the logger
- An intermediary part of the infrastructure is down (Dickson issue)
- The RF logger has malfunctioned

11 Credit card payment failed (Stripe)

This section applies to Basic, Standard, and Compliant plans.

11.1 About credit card payments

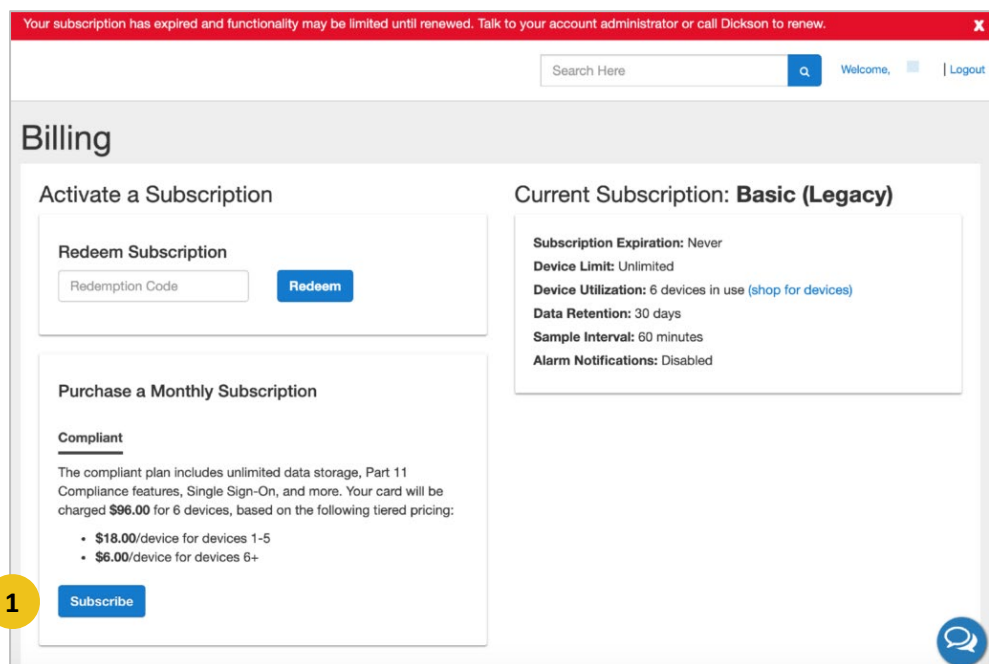
- Your monthly credit card subscription will be cancelled after three consecutive failed payments.
- If you see a failed payment, we recommend contacting your card issuer first to understand why the payment was not processed.
- You can also update your credit card information as needed when a payment fails.

11.2 Subscription is cancelled in case of failed payment

Your monthly subscription paid using a credit card may be cancelled if the system has exhausted all attempts to process a payment.

1. When the first payment attempt fails, the system will try again after 24 hours.
2. If the second payment fails, the system will try again 24 hours after the last attempt.
3. If the **third payment fails, the system automatically cancels your subscription.**

Once the subscription is cancelled, you have the option to click on **Subscribe** (1) to purchase a monthly plan again. Otherwise, please reach out to your sales representative if you are interested in purchasing a Yearly-Compliant plan.

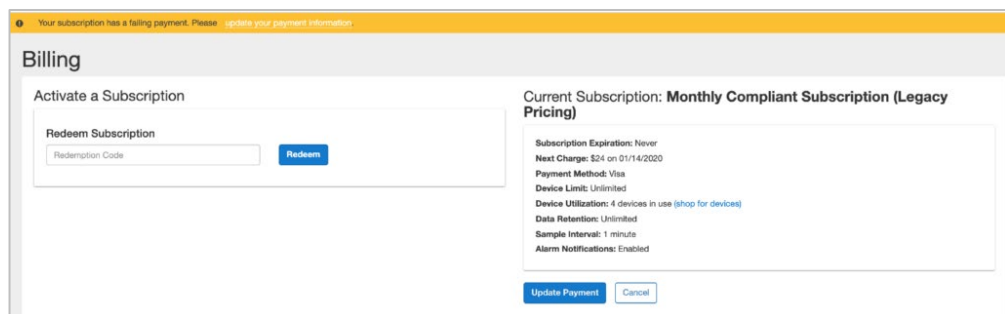


11.3 What to do if credit card payment fails

DicksonOne automatically sends notification to the email address tied to the credit card on DicksonOne when the first attempt fails.

The system also displays a warning banner to inform users that the subscription has a failing payment. Please update your payment information.

1. A failed payment is typically due to the card issuer not honoring the payment.
2. Please contact your card issuer as soon as possible to understand why a payment was failed.
3. You also have the option to update your credit card information to a new card by clicking **Update Payment** (as shown below) so that your payment can be processed.



The screenshot shows a web interface for a billing page. At the top, a yellow banner contains the message: "Your subscription has a failing payment. Please update your payment information." Below this, the page is titled "Billing". On the left, under "Activate a Subscription", there is a "Redeem Subscription" section with a text input for "Redemption Code" and a blue "Redeem" button. On the right, under "Current Subscription: Monthly Compliant Subscription (Legacy Pricing)", there is a list of details: "Subscription Expiration: Never", "Next Charge: \$24 on 01/14/2020", "Payment Method: Visa", "Device Limits: Unlimited", "Device Utilization: 4 devices in use (shop for devices)", "Data Retention: Unlimited", "Sample Interval: 1 minute", and "Alarm Notifications: Enabled". At the bottom right of this section are two buttons: "Update Payment" (blue) and "Cancel" (white).



The warning message may continue to be displayed even when you update your credit card information after a payment failed, as the system attempts to run the transaction at the exact time. Please allow up to 24 hours for the payment status and warning banner to be updated.

12 IT requirements and notes

DicksonOne is a system that combines network-connected data loggers and cloud-based software (i.e. an Internet of Things or IoT platform). Depending on your organization's IT requirements/controls, you may need to collaborate with your IT team to get approval to use the system on your company's network and ensure the system will work once installed.

The IT infrastructure and environment varies drastically from one organization to the next. As such, if you have any additional questions please feel free to reach out to us for more information. Below are some answers to the most common questions and concerns from an IT perspective.

12.1 Data Loggers (DWE2)

- As of Q4 2023, loggers only communicate via port 443 (HTTPS); older versions of firmware were configurable for either port 80 (HTTP) or port 443.
- As a best practice, all communication is generated by the data loggers.
 - For these devices, no ports need to be opened.
 - There are no incoming commands/control/access for these devices.
- The data loggers have a proprietary OS/firmware (i.e. NOT Windows CE, Linux, Android, etc.)
- Devices support both Wi-Fi and Ethernet, but only one at a time.
- Supported network types include 2.4Ghz B/G/N.
- Supported encryption protocols:
 - WEP
 - WPA Personal
 - WPA Enterprise
 - WPA2 Personal
 - WPA2 Enterprise (with some certificates; excludes the DWE2)
- Organizations who use WPA/2 Enterprise protocols may want to consider a dedicated user for authentication which does not require password changes on a regular basis as the need to update the password regularly across many devices might be burdensome for some organizations; consider a VLAN to reduce any associated risks.
- DWE data loggers are not proxy aware.
- Data loggers are not compatible with a captive portal without additional network configuration (e.g. safe-listing MAC addresses, see below)

12.2 DWE2 and MDIX

The DWE2 data logger does not support auto MDIX at this time and may result in your loggers not being able to connect to a network if switches are not configured correctly and/or the correct Ethernet cables are in use.

To avoid MDIX related issues, you can either:

1. Enable Auto MDIX on the network switch.
2. Use a crossover Ethernet cable between the logger and a switch that does not have Auto MDIX enabled.

12.3 RF LoRa data logging system

12.3.1 LoRa System Components

A LoRa network consists of several pieces of hardware:

- End points (e.g. RFL Logger): The endpoints are the data loggers in the LoRa network where readings and data are taken.
- LoRa gateway (e.g. RFG Gateway): The gateway receives communications from the LoRa endpoints and then transfers them to a network server. The gateway is the only device treated as a client on a physical network. Gateways are connected to the network via Wi-Fi, Ethernet, or Cellular.
- LoRa Network Server (e.g. The Things Network): The LoRa network server enables connectivity, management, and monitoring of devices, gateways, and end-user applications. Its main objectives are to ensure the security, scalability, and reliability of data routing throughout the network.
- Remote computer (The user): a remote computer can then control the actions of the endpoints or collect data from them

12.3.2 LoRa System requirements

Dickson has two main LoRa data loggers: RFL and Cobalt X2.

12.3.2.1 For RFL data loggers

- The device is compatible with the RFG and RFG-LTE gateways:
- RFLs utilize the LoRa protocol to communicate information back to a gateway which uses Wi-Fi, Ethernet, or Cellular for a backhaul
- The LoRa Gateways must be able to make an outgoing connection using UDP port 1700 and receive all replies
- The RFL has a proprietary OS/firmware (i.e. NOT Windows CE, Linux, Android, etc.), while the RFG and RFG-LTE run Linux

12.3.2.2 For Cobalt X data loggers

- The device is compatible with the Pro and Advanced gateways
- Cobalt X uses the LoRa protocol to communicate information back to a gateway which uses Wi-Fi, Ethernet, or Cellular for a backhaul.
- LoRa Gateways must be able to make an outgoing connection using UDP port 1700 and receive all replies.
- Cobalt X has a proprietary OS/firmware (i.e. NOT Windows CE, Linux, Android, etc.); compatible gateways run Linux.

12.4 VLANs

It is common for users of the DicksonOne monitoring system to utilize VLANs as part of their deployments. Many organizations have an “IoT” network dedicated to products and services like DicksonOne.

12.5 Local IP Addresses

Devices can be configured in either DHCP or via a static IP address. If using DHCP, ensure the devices are allowed to receive their own IP addresses via your DHCP server.

We recommend DHCP reservations via MAC address instead of static IP addresses but devices can be configured according to your company’s policies.

12.6 Safe-listing application IP addresses/FQDNs for firewalls

DicksonOne utilizes application load balancers as part of its high availability design and cannot currently offer a static IP address for the purpose of safe-listing at this time. As an alternative, we recommend safe-listing the FQDNs which are commonly supported by most firewall/networking equipment these days.

If your organization requires safe-listing applications via IP addresses or FQDNs, please ensure the table below to ensure the domains are on your safe-lists:

FQDN	Port	Protocol	Related Product	Description
dicksonone.com	443	TCP	DWE TWE TWP	Device communication to/from the cloud software and user interface
api.dicksonone.com	443	TCP	DWE/2 TWE TWP RFG	Device communication to/from the cloud software
dicksonone.nam1.cloud.thethings.industries	1700	UDP	RFG	Communication between LoRa devices/gateways and the application
s3.amazonaws.com	443	TCP	DWE/2 TWE TWP RFG	Over the air (OTA) firmware updates for supported devices
time.nist.gov		NTP	DWE/2 TWE TWP	External time server to ensure accurate time tracking on data loggers



If your company uses firewalls, web filtering, or proxies, please ensure they are not blocking packets TO or FROM DicksonOne.

12.7 MAC address filtering

If your organization utilizes MAC address filtering, the MAC address can be found for each device according to the table below.

Device	MAC Available	Address Location
DWE/2	Yes	Network Connection Widget
TWE & TWP	Yes	Information Screen on device
RFL	Not Applicable	Not Applicable
RFG RFG-LTE	Yes	Label on the Device Administrative screen
Cobalt X	Not Applicable	Not Applicable
Pro Gateway / Advanced Gateway	Yes	Label on the Device Administrative screen

12.8 Backup data independently from DicksonOne

While DicksonOne has adequate redundancy built into the system, customers often ask how they can back up their data on their own servers.

This can be accomplished in multiple ways:

- Manually exporting CSV files from the devices on a regular basis that can be stored on an organization's servers
- Automatically configuring PDF reports that can be stored on an organization's servers
- Leverage the available REST API to integrate a backup of your data onto your own servers or with a third-party system such as a Building Management System.

12.9 Integrations & REST APIs

DicksonOne offers a robust REST API for custom integrations. If your organization has access to developers and/or other IT staff who are familiar with and capable of working with REST APIs, you can utilize the APIs to integrate with a variety of systems or use cases including:

- ERP/MRP
- QMS
- Business Intelligence (Tableau, Power BI, etc.)
- Custom dashboarding
- Custom backup solutions

Documentation for the DicksonOne REST APIs can be found here: <https://www.dicksonone.com/developers>.

12.10 Wi-Fi Access Points

If your facility uses multiple access points with the same SSID and security key to cover a large area, ensure the following: the device's encryption type set to Auto Select and the security keys are identical. We highly recommend that any two access points within range of one another are configured to use channels that do not overlap with one another.

Most access points have a limit to how many devices can concurrently be connected. This varies, but is often as few as 25. Consider laptops, cell phones, equipment, loggers, and any other devices that may be connected to an access point.



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