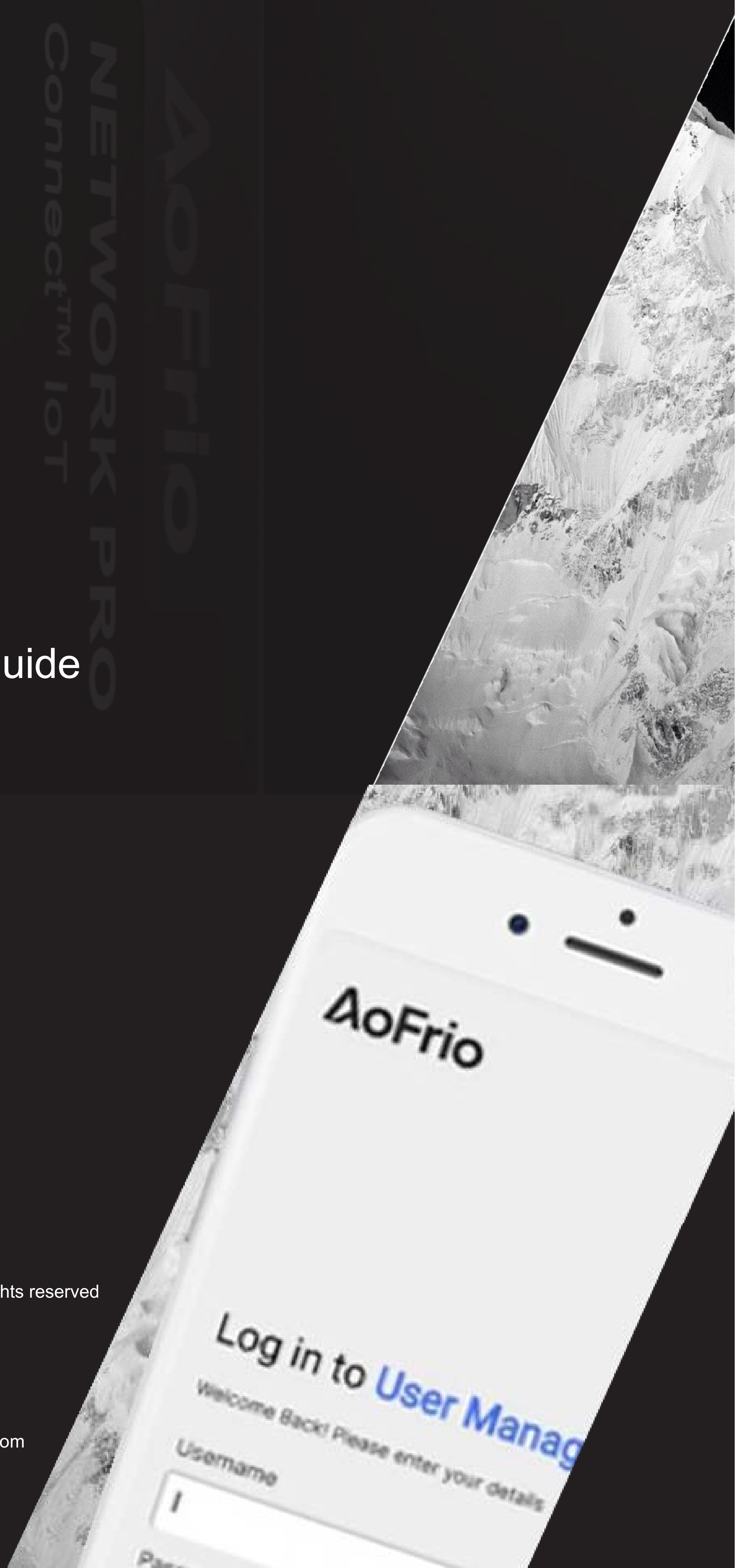
AoFrio

User Manager Guide

Document # WT 9731_i4

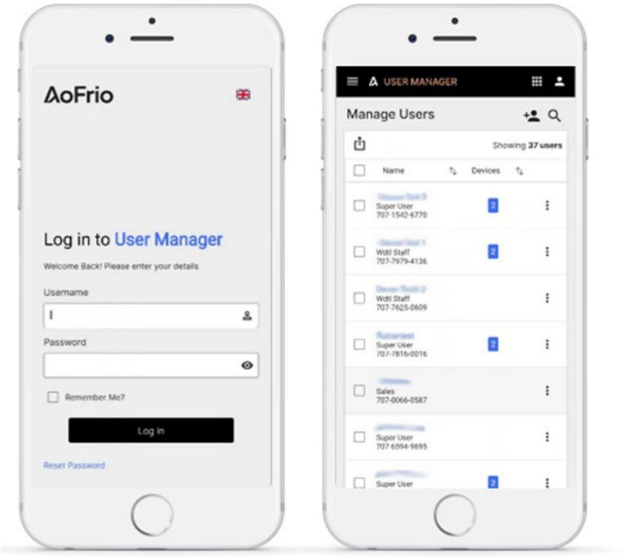
Issue date: November 2024



AoFrio Ltd
P: +64 9 477 4500 E: sales@aofrio.com
www.aofrio.com

Introduction

AoFrio's User Manager application has been designed to manage SCS infrastructure. It allows easy creation of new users, editing existing users, as well as appropriate permissions setup for those users within SCS applications.



Manage users and their roles

The User Manager app lets you manage user and role information for access to a variety of AoFrio's IoT technology. User information includes:

- **Name**: Name of the user
- **Username**: This is the username that will be used to log into the reporting app. This username must be unique (We suggest using the person's email address.)
- **Email**: email address of the person (In most of the cases, the Username & email address columns will have the same information.)
- **Position**: (optional) Position in the company (optional)
- **Payroll**: (optional) Payroll information
- **Role**: This is the person's role and determines their permissions and access to apps
- **Outlet ID**: (optional) This means a user can be assigned access to coolers in a specific location or outlet.
- **Organization Structure**: (optional) You can also choose to have an organization structure defined for the database of your organization such as the hierarchy level of each user and also limit the access of different users to areas which are not relevant to them.

Roles determine the permissions and access each user has on an app by app basis. Each role may have a different permission set, allowing custom app access for different user groups. There are a few underlying rules that apply:

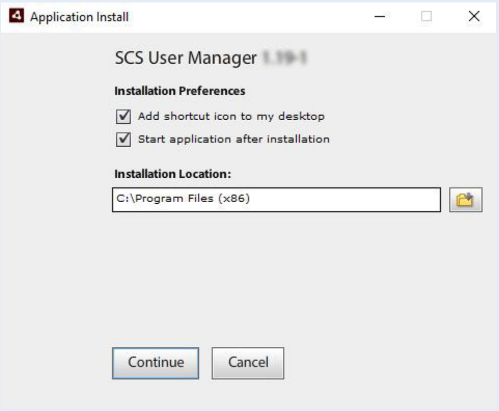
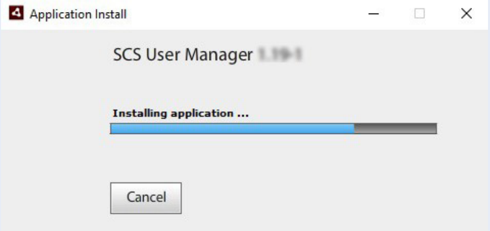
- When permissions are changed for a role, all users assigned to that role will be affected.
- Each new database has the following default roles: Sales, Technical, Evaluation 1, Evaluation 2, User Manager, and Disabled.
- A “Disabled” role removes all permissions from a user. This means that users are not deleted when no longer required. They should simply be set to a "Disabled" status.
- Other role types can be created on request to your AoFrio representative.

Forgotten password?

If you forget your password for the User Manager app at any time, return to the login screen and click **RESET PASSWORD**. This will send an email to your address and provide instructions on what to do to reset it.

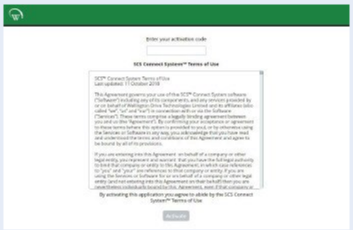
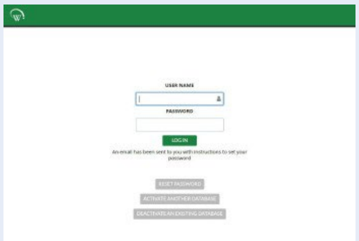
Initial setup

Installation process

	Step
1	Request an installation file for the User Manager app from your AoFrio representative. They will provide it to you in the form of downloadable link along with your Username Activation code.
2	Download the User Manager application by clicking on the provided link. The download will start in your browser.
3	Wait for the download to finish, then locate the install file on your local computer. By default the files are saved to the PC/Downloads folder. Please look for the file prefixed with: **scs-usermanager**.
4	Double click on the **scs-usermanager.exe** file and select **Run** to initiate the install process.
5	When the install process is complete, you will see an **Application Install** screen and application version number. Click to confirm both options for: • **Add shortcut option to my desktop** • **Start application after installation** Choose an **Installation Location** by clicking the folder icon and choosing a folder on your local computer. Click **Continue** and the installation process will begin.  Application Install SCS User Manager [redacted] **Installation Preferences** ☑ Add shortcut icon to my desktop ☑ Start application after installation **Installation Location:** C:\Program Files (x86)
6	The User Manager application will automatically start after the installation process has completed, if the appropriate option has been selected on a previous screen. If it hasn't started automatically, navigate to the saved location of the install application and start it from there.  Application Install SCS User Manager [redacted] **Installing application ...**

Activation & First Login

Once the User Manager app is installed, you will need to activate your account.

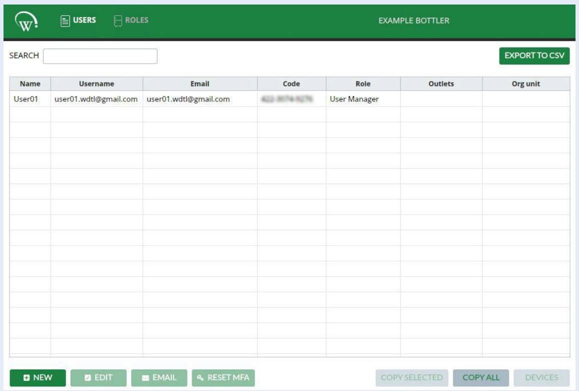
	Step	
1	Enter your unique Activation code and click **Activate** to confirm the Terms of Use.	 Enter your activation code SCS Connect System™ Terms of Use SCS™ Connect System Terms of Use Last updated: 11 October 2018 This Agreement governs your use of the SCS™ Connect System software ("Software") including any of its components, and any services provided by or on behalf of Wellington Drive Technologies Limited and its affiliates (also called "we", "us" and "our") in connection with or via the Software ("Services"). These terms comprise a legally binding agreement between you and us (the "Agreement"). By confirming your acceptance or agreement to these terms (where this option is provided to you), or by otherwise using the Services or Software in any way, you acknowledge that you have read and understood the terms and conditions of this Agreement and agree to be bound by all of its provisions. If you are entering into this Agreement on behalf of a company or other legal entity, you represent and warrant that you have the full legal authority to bind that company or entity to this Agreement, in which case references to "you" and "your" are references to that company or entity. If you are using the Services or Software for or on behalf of a company or other legal entity (and not entering into this Agreement on their behalf) then you are nevertheless individually bound by this Agreement, even if that company or By activating this application you agree to abide by the SCS Connect System™ Terms of Use Activate
2	If this is your first login, enter the **USERNAME** provided by your AoFrio representative. You will receive an automated email asking you to reset your password. Follow the instructions within the email and return to the login screen to enter your password, then click **LOGIN**.	 USER NAME PASSWORD LOG IN An email has been sent to you with instructions to set your password RESET PASSWORD ACTIVATE ANOTHER DATABASE DEACTIVATE AN EXISTING DATABASE

How the Home Screen works

Each time you login, you will go directly to the User Manager Home Screen. Once you have added users, this screen will display details for all the existing users in the database including their Name, Username, Email Id, Activation codes, and Role. If an organization structure has been applied to your database you will also see the place of users in the structure. If you need to edit user information, your AoFrio representative will need to enable this functionality.

? You can also set up the system so that only users in a lower organization node are displayed. This allows for the setting of sub-usermanagers who can still create users in selected roles within their ORG nodes but not outside it. You will see the level the user is assigned to within the organizational structure.

Key functionality



Name	Username	Email	Code	Role	Outlets	Org unit
User01	user01.wdtl@gmail.com	user01.wdtl@gmail.com	[redacted]	User Manager		

- Tab between **Users** and **Roles** screens for detailed information about the existing users, as well as their place within the organization structure (if this detail has been added).
- Make a text search in the **SEARCH** field to find user information from any column and row.
- Click **EXPORT TO CSV** to export the list of users to a .csv format file.
- Add new and edit existing users through the **NEW** and **EDIT** functions (described in more detail elsewhere in this manual).
- Send an automated email to selected users containing their username and activation code for access to the User Manager app using the **EMAIL** function.
- Reset your Multi-Factor Authentication (MFA) settings through the **RESET MFA** function.

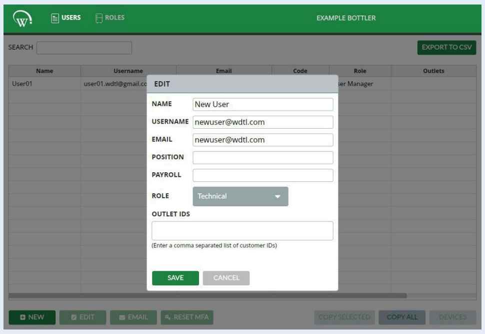
Create a new user & send them their activation code

<table>
<tr><th>Step</th><th>Details</th></tr>
<tr><td>1</td><td>Go to the <b>Home Screen</b>, click <b>+ New</b>.</td></tr>
<tr><td>2</td><td>

Complete the new user fields as follows:

- **NAME**
- **USERNAME** (This must be unique for each user. We suggest using the email address of the person.)
- **EMAIL** (In most cases, the Username and Email fields will have the same information
- **POSITION** (Optional)
- **PAYROLL** (Optional)
- **ROLE**
- **OUTLET IDS** (Optional)
- **ORGANIZATIONAL STRUCTURE** (Optional)

Then click **SAVE** to confirm.



EDIT

NAME: New User

USERNAME: newuser@wdtl.com

EMAIL: newuser@wdtl.com

POSITION:

PAYROLL:

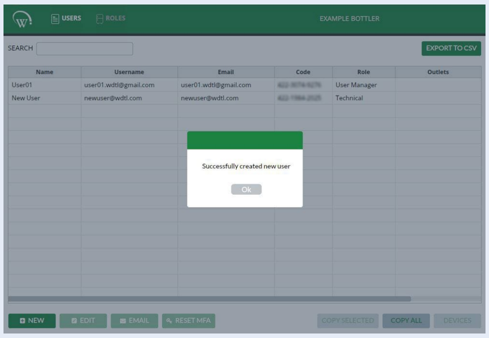
ROLE: Technical

OUTLET IDS:

(Enter a comma separated list of customer IDs)

</td></tr>
<tr><td>3</td><td>

You will now see the new user appear on the Home Screen with a confirmation that you have successfully created a new user. Click **OK** to confirm.



Name	Username	Email	Code	Role	Outlets
User01	user01.wdtl@gmail.com	user01.wdtl@gmail.com	[redacted]	User Manager	
New User	newuser@wdtl.com	newuser@wdtl.com	[redacted]	Technical	

Successfully created new user

</td></tr>
</table>

When a new user is created, they are assigned a unique activation code which displays in the **Code** column on the **Home Screen**. You can send an automated email to individual or multiple users as follows.

<table>
<tr><th></th><th>Send activation codes to individual users</th></tr>
<tr><td>1</td><td>Go to the <b>Home Screen</b> and select a user by clicking on their name in the <b>NAME</b> column.</td></tr>
<tr><td>2</td><td>

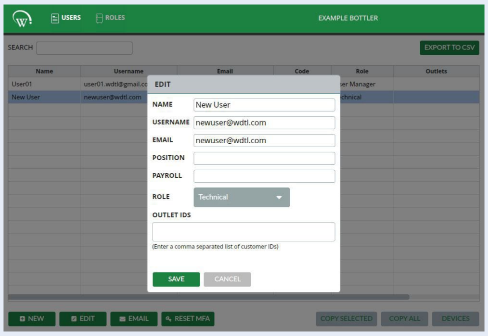
To send an email, you have two options. If you want to:

- Send an automated email to the user with their username and activation code, go to the **Home Screen** and click the **EMAIL** function.
- Send an email from your own email or messaging system, go to the **Home Screen** and click **COPY SELECTED**. This copies the user's information into your clipboard to paste it into another message.

</td></tr>
<tr><th></th><th>Send activation codes to multiple users</th></tr>
<tr><td>1</td><td>Go to the <b>Home Screen</b> and select a user by clicking on their name in the <b>NAME</b> column.</td></tr>
<tr><td>2</td><td>Press down and hold the <b>ctrl</b> key on your keyboard, then select other users by clicking on their name in the <b>NAME</b> column.</td></tr>
<tr><td>3</td><td>Continue holding down the <b>ctrl</b> key and click <b>EMAIL</b> to send separate automated messages to each of the selected users.</td></tr>
</table>

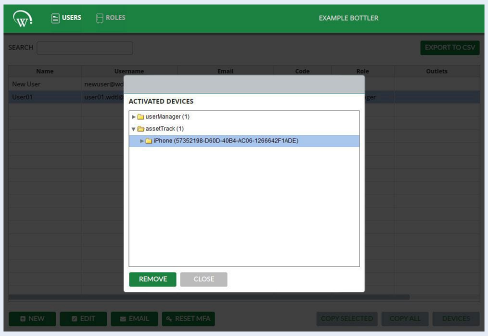
Edit user information

If you have the correct set of permissions in User Manager you can edit one user at a time. Talk to your AoFrio representative if editing permissions have not been set up.

Step	Details
1	Go to the **Home Screen** and select a user by clicking on their name in the **NAME** column.
2	Update the information as needed, then click **SAVE** to confirm.  EXAMPLE BOTTLER Name: User01, Username: user01.wdtl@gmail.co…, Role: …ser Manager Name: New User, Username: newuser@wdtl.com, Role: …chnical EDIT NAME: New User USERNAME: newuser@wdtl.com EMAIL: newuser@wdtl.com POSITION: PAYROLL: ROLE: Technical OUTLET IDS: (Enter a comma separated list of customer IDs) USERS ROLES SEARCH EXPORT TO CSV Name Username Email Code Role Outlets SAVE CANCEL NEW EDIT EMAIL RESET MFA COPY SELECTED COPY ALL DEVICES

View or remove activated devices

User Manager keeps the record of all devices that have been activated in AoFrio's IoT applications, according to each user's permissions. This includes a "Maximum Activated Devices" for each app which means the system will not allow a user to activate more than the predefined number of devices for their role. View or remove devices as follows:

Step	Details
1	Go to the **Home Screen** and select a user by clicking on their name in the **NAME** column.
2	Click **DEVICES** and select each device in the list to: • View devices allocated to that user, including the make, OS type, version, and the date the device was activated for the app. • Remove the device by clicking **REMOVE**. You will be prompted to confirm this step by clicking **YES**.  EXAMPLE BOTTLER ACTIVATED DEVICES userManager (1) assetTrack (1) iPhone (57352198-D60D-40B4-AC06-1266642F1ADE) USERS ROLES SEARCH EXPORT TO CSV Name Username Email Code Role Outlets New User User01 REMOVE CLOSE NEW EDIT EMAIL RESET MFA COPY SELECTED COPY ALL DEVICES
3	Click **CLOSE** when you have finished to return to the **Home Screen**.

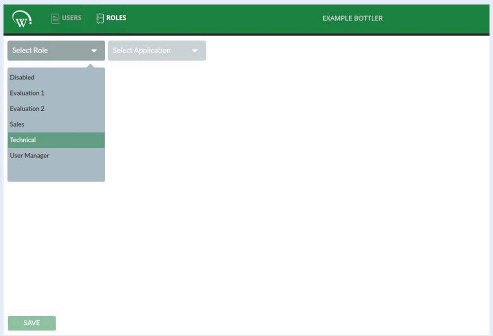
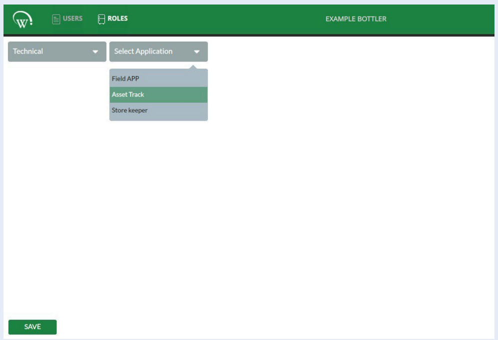
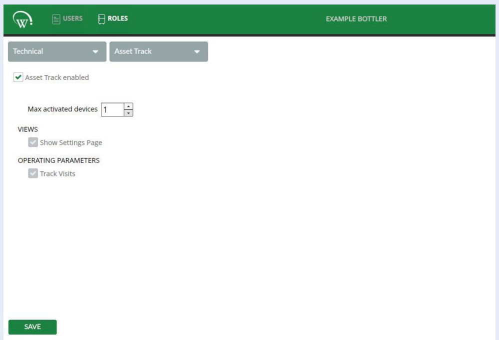
Set up individual role permissions

Set up the permissions for each role type in your organization to enable users to work with the appropriate level of control for each AoFrio software application they use.

You will find the following default roles in each database: Sales, Technical, Evaluation 1, Evaluation 2, User Manager, and Disabled. Talk to your AoFrio representative about adding other role types.

The applications you can assign to each of role varies depending on the database type. For both Bottler and Original Equipment Manufacturer (OEM) databases, lower hierarchy roles are given access AoFrio's Field, Track, and Storekeeper apps by default.

Higher hierarchy roles typically have additional access to AoFrio's User Manager and Report apps while OEM databases also have access to AoFrio's Lab, Dashboard, and Cradle Programmer apps.

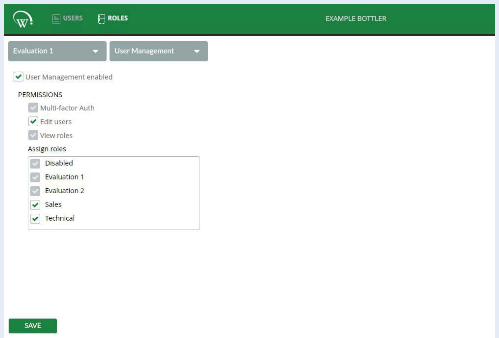
Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Click **Select Role** and choose a role type from the dropdown list.  USERS ROLES EXAMPLE BOTTLER Select Role Select Application Disabled Evaluation 1 Evaluation 2 Sales Technical User Manager SAVE
3	Click **Select Application** and choose an app from the dropdown list.  USERS ROLES EXAMPLE BOTTLER Technical Select Application Field APP Asset Track Store keeper SAVE
4	To enable the role for the app you have selected: • Check the **Asset Track enabled** box • Choose a number of **Max activated devices** for the maximum devices allowed access • (Optional) If other permissions have been enabled in the User Management permission, check the relevant boxes to allow further functionality to that role type. Where the permissions has not been enabled, these checkboxes will appear 'greyed out'.  Technical Asset Track ☑ Asset Track enabled Max activated devices 1 VIEWS ☑ Show Settings Page OPERATING PARAMETERS ☑ Track Visits

Set up User Management permissions

In addition to the basic role permissions you can assign to roles, the primary user of the User Manager app also has the option to permit access to User Management functionality to other roles. Typically, these permissions might be given to subordinate or sub-user manager who has more day-to-day involvement with the app.

User Management permissions include:

- **Multi-factor Authentication** - Add an additional level of login security that requires an additional code from Google Authenticator to verify the user’s identity at the login stage.
- **Edit users** - Update the status of other users.
- **View roles** – Access to the **ROLES** tab for 'view only' insights from the information stored there.

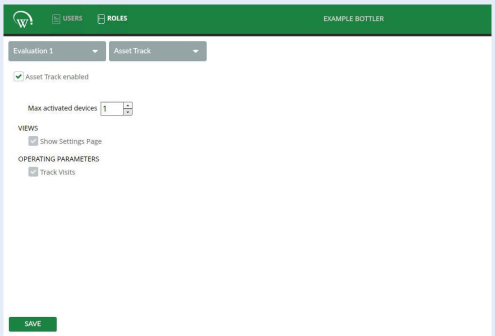
Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role associated with your subordinate or sub-user manager (ie Evaluation 1) and choose **User Management** in the right-hand dropdown menu.  Evaluation 1 · User Management ☑ User Management enabled PERMISSIONS ☑ Multi-factor Auth ☑ Edit users ☑ View roles Assign roles ☑ Disabled ☑ Evaluation 1 ☑ Evaluation 2 ☑ Sales ☑ Technical
3	Check the **User Management enabled** checkbox and any of the **PERMISSIONS** fields that apply to that role: • Multi-factor Auth • Edit users • View roles Under **Assign roles** check the role types that the sub-user manager can assign to other users when editing them. ie. Disabled, Evaluation 1, Evaluation 2, Sales, and Technical.
4	Click **SAVE** to confirm the permissions for the role.

Setting up access to different apps in User Manager

Track

The Track app is designed for use on mobile devices. When an enabled device is near to a cooler with an AoFrio Monitor installed, it collects telemetry data automatically and transfers it directly to the Cloud with no need for further action.

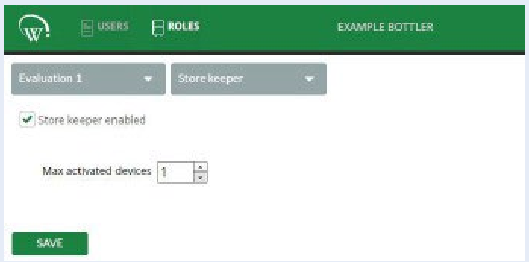
To enable a role in your organization to use the Track app:

Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role from the left-hand dropdown menu and choose **Asset Track** in the right-hand dropdown menu.  USERS ROLES EXAMPLE BOTTLER Evaluation 1 ▾ Asset Track ▾ ☑ Asset Track enabled Max activated devices 1 VIEWS ☑ Show Settings Page OPERATING PARAMETERS ☑ Track Visits SAVE
3	To enable the role for the app you have selected: • Check the **Asset Track enabled** box. • Choose a number of **Max activated devices** for the maximum devices allowed access (We recommend no more than 3 to prevent code sharing between users). • (Optional) If you would like the role to be able to view settings within the Track app check the box **Show Settings page** box. • (Optional) If you would like the role to be able to monitor sales visit data (time at location, GPS) and make use of additional functionality in the Report (SCS Reporting?) app click the **Track Visits** box.
4	Click **SAVE** to confirm the permissions for the role.

Storekeeper

The Storekeeper app enables basic cooler configurations store owners, such as lights and store hours. It also collects telemetry data from the cooler, when near the cooler, and transfers it to the cloud. Internet connection is necessary for the data to be transferred from the app to the cloud.

To enable a role in your organization to use the Storekeeper app:

Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role from the left-hand dropdown menu and choose **Store keeper** in the right-hand dropdown menu.  ☑ Store keeper enabled Max activated devices 1
3	To enable the role for the app you have selected: • Check the **Store keeper enabled** box. • Choose a number of **Max activated devices** for the maximum devices allowed access (We recommend no more than 3 to prevent code sharing between users).
4	Click **SAVE** to confirm the permissions for the role.

Field

The Field app is designed for use by technicians for cooler setup, diagnostics, setting and viewing cooler parameters and data via mobile phone. There are a number of detailed settings that you can enable with User Manager.

These are described below:

Info

- **View SCS Info [Asset No./Model/Firmware Rev.]** - This allows the role to view the SCS INFO screen from the main menu in the SCS Field App.

Provisioning

- **Installation Setup of SCS [Asset No./Model/Install Address]** - This allows the user to view the SCS SETUP screen from the main menu in the Field App. From here they can set up installation data including the Asset Number which are essential to SCS reporting in various applications.
- **Modify Cooler Status [Warehoused/Scrapped]** - The user can view the SET COOLER STATUS screen from the main menu in the Field App. Here they can set the status displayed in the Reporting app for each cooler ie. In service, Warehoused, Maintenance. This function does not require a Bluetooth connection to the controller and can be done by entering or scanning the asset number.

Configuration and diagnostics

- **View Logged Statistics** - The user can view statistics from the past week in the STATISTICS screen on the Field App.
- **View Logged Events** - This enables the YELLOW ALERT SYMBOL in the app banner. When the user selects this symbol they will see the EVENTS screen and the event log will begin to download.
- **Edit Parameters** - The user can access the EDIT PARAMETERS screen in the Field App and can edit parameters for the controller. The permission level for their role does affect which parameters they can edit. For example, the Sales permission level has the lowest access while the Technical permission level provides the greatest access.
- **Edit Existing Asset Number** - If the Installation Setup of SCS screen has been enabled then this function can be selected so that the user can change the cooler Asset# after it has been set the first time.
- **Control SCS Outputs [Technician Use Only]** - The user can see the OUTPUT CONTROL menu item and a graph symbol in the top banner. This function lets the user alter all available outputs connected to the SCS controller which is mostly important for cooler diagnostics and testing.
- **Allow disabling of coolers** – lets the user disable a cooler from the SCS INFO screen in Field app. This will disable components and eventually cause the cooler to shutdown. Parameter editing is also disabled.
- **Allow enabling of coolers** - lets the user enable a disabled cooler from the SCS INFO screen in Field app, reversing the changes made when disabling a cooler.

Beacons

- **iBeacon Config** - The user can access the iBeacon settings of the controller.

Service system

- **Receive Service Requests** - The user can receive and action service requests through the Field app.
- **Create Service Request** - The user can create service requests and indicate faults through the Field app.

Field

To enable a role in your organization to use the **Field** app:

Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role from the left-hand dropdown menu and choose **Field APP** in the right-hand dropdown menu.
3	To enable the role for the app you have selected: • Check the **Field APP enabled** box. • Choose a number of **Max activated devices** for the maximum devices allowed access (We recommend no more than 3 to prevent code sharing between users). • (Optional) Check other boxes as required to provide additional functionality and permissions.
4	Click **SAVE** to confirm the permissions for the role.

Report

The Report app is designed for desktop viewing and visualizing of telemetry data stored within the AoFrio Cloud. There are a number of detailed settings that you can enable with User Manager.

Views

- **Show Sales Visits** - This lets the user to see the sales visit data collected by the Track app. The Sales tab must be enabled in the Report categories panel for this setting to be available.

- **Edit Settings** - This allows the user to edit the Settings page in the Report app. Settings in this area are global and will affect all Report app users on the database. The System tab must be enabled in the Report categories panel for this setting to be available.

- **Edit Service Requests** - This allows the user to edit service requests. The Maintenance tab must be enabled in the Report categories panel for this setting to be available.

- **Edit Cooler Install Notes** - This setting allows the editing of cooler install notes. The Asset tab must be enabled in the Report categories panel for this setting to be available.

- **Delete Cooler Install Notes** - This setting allows cooler install notes removal. The Asset tab must be enabled in the Report categories panel for this setting to be available.

- **Set Cooler tags** - This setting allows the user to set cooler tags from a predefined list. It opens up an option for further customization of cooler groups. The Asset tab must be enabled in the Report categories panel for this setting to be available.

Report categories

Each report category in the following pages matches a main menu item in the Report app. When you enabling an option for a role it will become visible for the end users with that role. At least one of the categories must be enabled to save a permission set for the role you select.

- **Dashboard** - The Main Dashboard in the Report app will be visible for the user.

- **Sales** - This setting allows the viewing of the Sales tab when logged in. The statistics contained here is used by sales staff and relates to sales numbers and cooler performance with respect to product temperature, etc.

- **Maintenance** - Enables Maintenance tab in the main menu. This allows the user to look at cooler statistics and review service requests for coolers.

- **Asset** - This setting allows the viewing of the Asset tab. This section contains all the information about coolers.

- **Capital** - This setting allows the viewing of the Capital tab.

- **System** - This setting allows the viewing of the System tab.

Import Types

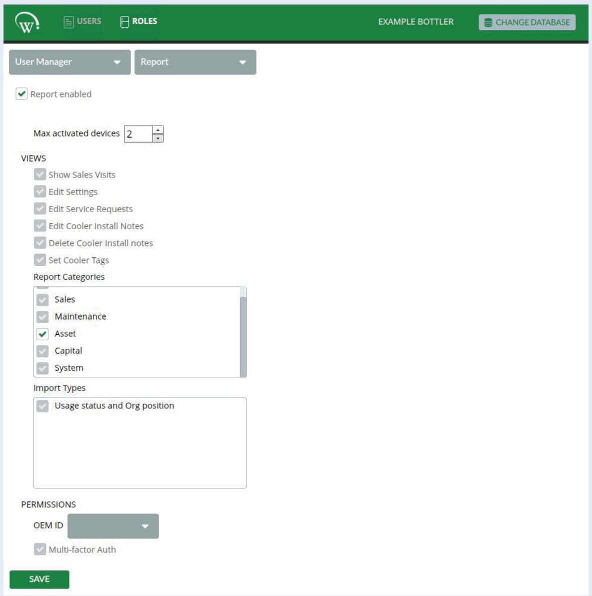
- **Usage status and Org position** - This feature enables bulk update of coolers' usage status and org positions through an import functionality. The System tab must be enabled in the Report categories panel for this setting to be available.

Permissions

- **OEM ID -** This lets the user filter coolers by manufacturer (OEM) on a role basis.
- **Multi-factor Auth** - This lets the user add an additional level of login security that requires an additional code from Google Authenticator to verify the user's identity at the login stage.

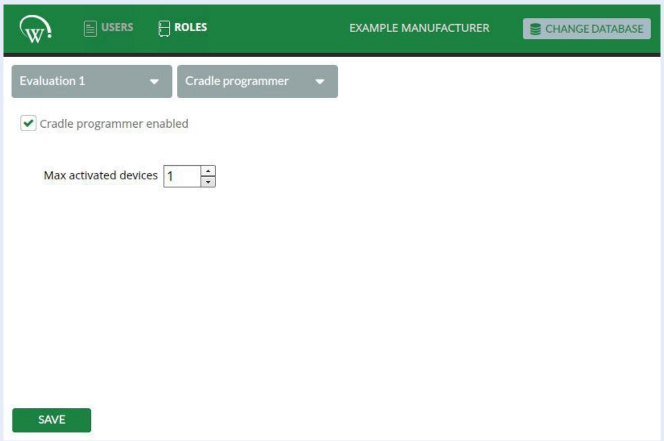
Report

To enable a role in your organization to use the **Report** app:

Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role from the left-hand dropdown menu and choose **Report** in the right-hand dropdown menu.
3	To enable the role for the app you have selected: - Check the **Report enabled** box. - Choose a number of **Max activated devices** for the maximum devices allowed access (We recommend no more than 3 to prevent code sharing between users). - (Optional) Check other boxes as required to provide additional functionality and permissions. ? Please note that some checkboxes require a **Report Category** to be checked before other options become available for selection. Unavailable options appear 'greyed out' in the User Manager app.  USERS ROLES EXAMPLE BOTTLER CHANGE DATABASE User Manager ▾ Report ▾ ☑ Report enabled Max activated devices 2 VIEWS ☑ Show Sales Visits ☑ Edit Settings ☑ Edit Service Requests ☑ Edit Cooler Install Notes ☑ Delete Cooler Install notes ☑ Set Cooler Tags Report Categories ☑ Sales ☑ Maintenance ☑ Asset ☑ Capital ☑ System Import Types ☑ Usage status and Org position PERMISSIONS OEM ID ▾ ☑ Multi-factor Auth SAVE
4	Click **SAVE** to confirm the permissions for the role.

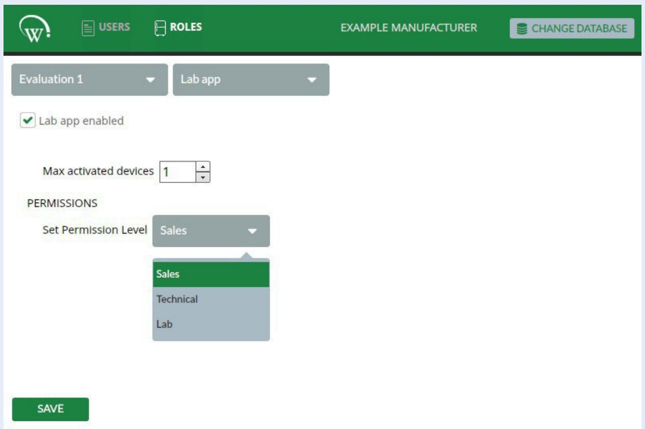
Cradle Programmer

The Cradle Programmer app is designed for programming parameters and asset information into SCS controllers on the cooler assembly line. There are only a few settings that you can enable with User Manager. These are described in the steps below.

Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role from the from the left-hand dropdown menu and choose **Cradle Programmer** in the right-hand dropdown menu.
3	To enable the role for the app you have selected: - Check the **Cradle Programmer enabled** box - Choose a number of **Max activated devices** for the maximum devices allowed access (We recommend no more than 3 to prevent code sharing between users).  USERS ROLES EXAMPLE MANUFACTURER CHANGE DATABASE SAVE Evaluation 1 Cradle programmer ☑ Cradle programmer enabled Max activated devices 1
4	Click **SAVE** to confirm the permissions for the role.

Lab Programmer

The Lab app is designed for cooler diagnostics, setting and viewing cooler parameters. It may also be used for creating and managing new parameter files. There are only a few settings that you can enable with User Manager. These are described in the steps below.

Step	Details
1	Go to the **Home Screen** and select the **ROLES** tab.
2	Select a role from the from the left-hand dropdown menu and choose **Lab app** in the right-hand dropdown menu.
3	To enable the role for the app you have selected: • Check the **Lab app enabled** box • Choose a number of **Max activated devices** for the maximum devices allowed access (We recommend no more than 3 to prevent code sharing between users).  Evaluation 1 Lab app ☑ Lab app enabled Max activated devices 1 PERMISSIONS Set Permission Level Sales
4	Under **PERMISSIONS** select an option for **Set Permission Level**: • **Sales** – This is a restricted access setting that allows read rights only. • **Technical** – This offers partial access with read and limited write permissions. • **Lab** – This provides full access to parameter files, with full read and write permissions.
5	Click **SAVE** to confirm the permissions for the role.

User Manager Guide

WT9731_i4 Issue date: November2024

www.aofrio.com