3DM.SPACE



Unified Experience
Consistent, intuitive interface across all your devices.

Real-time Control
Monitor and manage operations from anywhere, anytime.

Secure & Reliable
Enterprise-grade security and 99.9% platform uptime.

User Guide

3DM Contents

OVERVIEW & GETTING STARTED

Section	Pages
Platform Overview	6-7
Introduction | What Is 3DM.Space?	8
Who Should Use This Manual?	9
Administrator Responsibilities	10
First Login	11
Site Navigation	12
Account Settings	13
Recommended User Set-Up	14
Home Screen dashboard	15
Basic Admin Checklist	16
Common Mistakes To Avoid	17

ACCOUNT STRUCTURE, ROLES & PERMISSIONS

Section	Pages
Account Structure	18
Tenants	19
Customers	20-21
Users	22
Groups	23-24
User Groups	25
Dashboard Groups	26
Device Groups	27-28
Roles & Permissions	29
Roles & Permissions Overview	30
Setting Up Roles	31
Setting Up Role Details	32
Generic Role Templates	33-35
Group Role Templates	36-38
Editing Role Details	39-40

USER GROUPS

Section	Pages
User Groups	41
Create a User Group	42
Adding Users to a Group	43
Adding a Role to a User Group	44-45
Moving Users Between Groups	46
User Group Property Settings	47-48
User Group Entity Details	49-50

DASHBOARD GROUPS

Section	Pages
Dashboard Groups	51
Creating a Dashboard Group	52-55
Moving a Dashboard into the Group	56-57
Giving Users Access	58-60
Dashboard Group Table Properties	61-62
Dashboard Group Property Settings	63-64
Dashboard Group (Entity) Details	65

 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

3DM Contents

DEVICE GROUPS

Section	Pages
Device Groups	66-67
Creating Device Groups	68
Creating a Device Inside a Group	69-70
Moving a Device into a Group	71
Giving Users Access	72-73
Device Group Table Properties	74-75
Device Group Property Settings	76-77
Device Group Entity Details	78-79

USER SET-UP

Section	Pages
User Set-up	80
Creating a New User in All	81-82
Creating a New User in a Group	83-84
User Management Settings	85
User Details	86-88

CUSTOMERS

Section	Pages
Customers	89
Creating a Customer	90-91
Adding a Customer User	92
Adding Customer Devices	93
Adding Customer Dashboards	94-95
Customer Management Settings	96
Customer Details	97-98

DEVICES & TELEMETRY

Section	Pages
Devices	99-100
Creating a PassPort Gateway (Device)	101-102
Moving Devices into Groups	103
Sending and Receiving Telemetry Data	104
Creating Device Telemetry Variables	105-106
Creating Device Telemetry Attribute Variables	107
Viewing Device Data	108-109
Variable Data Sizes and Transmission Frequency	110
Node-RED Connection	111
Device Management Settings	112
Device Details	113-114

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Contents

ALARMS & NOTIFICATIONS

Section	Pages
Alarms	**115-116**
Where Alarm Rules Can Be Created and Viewed	**117-120**
Creating Your First Alarm Overview	**121-122**
Creating Your First Alarm - Adding an Argument	**123**
Creating Your First Alarm - Adding a Trigger	**124**
Creating Your First Alarm - Adding a Condition	**125**
Creating Your First Alarm - Adding a Clear Condition	**126**
Creating Your First Alarm - Advanced Settings	**127**
Alarms Table Options	**128**
Alarms List	**129-130**
Alarm Notification	**131-133**
Alarm Notification Recipients	**134-135**
Alarm Notification Templates	**136-137**
Alarm Notification Rules	**138-140**
Alarm Notification Send Quick Notification	**141-142**

DASHBOARDS

Section	Pages
Dashboards	**143**
Viewing Dashboards	**144**
Dashboards Non-Edit Mode Navigation	**145-146**
Dashboards Edit Mode Navigation	**147**
Dashboards Time Window Properties	**148-149**
Dashboards Time Window Settings	**150**
Dashboard Settings	**151-152**
Dashboard Layout Settings	**153-154**
Dashboard Layouts and Widget Arrangement	**155-156**
Dashboard Divider Layout	**157**
Dashboard States	**158**
Dashboards - Adding a State to a Widget	**159**
Dashboard Widgets	**160-161**
Dashboard Widget Data Source	**162**
Widget Settings	**163**
Widget Settings - Appearance	**164**
Widget Settings - Widget Card	**165**
Widget Settings - Actions	**166**
How to Add a Widget Action	**167-168**
How to Edit a Widget Action	**169-170**
Types of Actions	**171-172**

 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

3DM Contents

3DM TOOLS & SCADA

Section	Pages
3DM Nodes (Node-RED)	**173-174**
AI Manual Helper	**175**
Smithtek Side Tab	**176**
Scada Canvas Widget	**177-178**
Canvas SCADA Tools and Widgets Explanation	**179**
Canvas SCADA Set-up	**180**
Canvas SCADA Set-up Adding Data	**181**
Canvas SCADA Tips and Tricks	**182**

SUPPORT & INFORMATION

Section	Pages
Warranty	**183**
Contact Us	**184**

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Platform Overview

3DM.Space is a secure **cloud-based SCADA** platform designed for monitoring, control, alarms, event tracking, and data visualisation across connected Smithtek systems. It provides a modern way to view live site data, control equipment, manage users, and respond to alarms from almost anywhere with internet access.

The platform is designed to **work seamlessly** with **Smithtek products** such as the **PassPort Gateway, Mako PLC** and **Solaris PLC.** PassPort Gateways can connect using 3DM nodes, while Mako PLC systems can communicate using the 3DM protocol. This allows field hardware to send data directly into 3DM.Space, where it can be stored, displayed, alarmed, and used for remote control.
3DM.Space allows administrators and approved users to build modern SCADA dashboards using a simplified dashboard builder. Dashboards can be created to show live values, equipment status, process information, trends, alarms, maps, tables, control buttons, and other site-specific information. Multiple dashboards can be created for different sites, systems, users, or operating requirements.

Live device data is captured, stored, and displayed visually through the platform. Depending on the device setup and communication method, refresh times can be as fast as 30 seconds. This gives users a clear and timely view of what is happening across their connected equipment.









 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Platform Overview

The platform includes **user management tools** so administrators can control who has access to specific **dashboards**, **devices**, **alarms**, and **control functions**. Different roles can be created for different users, such as dashboard viewers, operators, field technicians, and operations managers. This helps ensure users only see and control the areas they are responsible for.

3DM.Space also includes **alarm and event management.** Alarms can be configured for conditions such as device disconnection, high or low levels, pump faults, low voltage, equipment status changes, process faults, or other site-specific events. Notifications can be used to alert the right people when an important event occurs.

The system is securely hosted in the cloud and uses modern machine-to-machine security methods to help protect device communication, user access, and stored data. This allows remote sites and equipment to be monitored without requiring users to be physically connected to the system.

3DM.Space is suitable for a wide range of industries, including **mining**, **farming**, **utilities**, **water management, smart factories**, **process automation**, **microbreweries**, **security**, **marine systems**, **irrigation**, and **remote infrastructure**. It is designed to make industrial monitoring and control easier to deploy, easier to manage, and easier to access across desktop, tablet, and mobile devices.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Introduction

This manual is designed to help administrators set up and manage a 3DM.Space account correctly from the beginning. It provides simple guidance for creating users, organising groups, assigning roles, managing dashboards, setting up devices, configuring alarms, and testing user access.

A well-structured account makes 3DM.Space easier to manage as more users, dashboards, devices, and sites are added. The recommended approach is to set up the main groups and roles first, then add users and devices into the correct areas.

This guide is written for administrators who are responsible for controlling access, managing connected devices, and keeping the platform organised.
It is intended to be used as a practical setup reference, not a technical engineering document.
The goal is to help administrators build a clean, secure, and easy-to-use 3DM.Space environment where users only see the dashboards, devices, and functions they need.

What Is 3DM.Space?

3DM.Space is a secure cloud-based SCADA platform used to monitor, control, and manage connected devices from a web browser. It allows users to view live data, create dashboards, manage alarms, control equipment, and access system information from desktop, tablet, or mobile devices.

3DM.Space is designed to work with Smithtek products such as the PassPort Gateway and Mako PLC. These devices send data to the platform, where it can be displayed, stored, alarmed, and used for remote monitoring or control.

The platform is suitable for many industries, including mining, farming, utilities, water management, smart factories, process automation, marine systems, security, irrigation, and remote infrastructure.

In simple terms, 3DM.Space gives users one central place to see what is happening across their connected sites, devices, and systems.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Who Should use this manual?

This manual is intended for 3DM.Space administrators and approved users responsible for setting up, managing, and maintaining the platform. It is most useful for people who need to create users, organise groups, assign roles, manage dashboards, connect devices, set up alarms, and test user access.

This manual is suitable for:

- Administrators who manage the main 3DM.Space account
- Operations managers who oversee users, dashboards, devices, and alarms
- Field technicians who help configure devices and troubleshoot sites
- Support staff who assist users with access or dashboard issues
- Internal team members who need a clear reference for platform setup

This manual is not designed for general dashboard-only users who simply log in to view data. Those users should only need a basic user guide for viewing dashboards, acknowledging alarms, and using approved controls.

How to get access?

To access 3DM.Space, you will need an active 3DM.Space cloud account.

1. **Purchase an account**
   A 3DM.Space cloud account can be purchased from Smithtek through the Smithtek website:
   https://www.smithtek.com.au/telemetry-hardware-software
2. **Reach out if you need us!**
   For sales assistance or account setup, contact: **info@smithtek.com.au**
3. **Wait for account activation**
   Once purchased, the account must be created and activated by Smithtek before it can be used.
4. **Receive your access details**
   Login details will be provided once the account has been successfully activated.
5. **Log in to 3DM.Space**
   New users should only attempt to log in after receiving confirmation that their account is active.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Administrator Responsibilities

Administrators are responsible for setting up and managing the 3DM.Space account correctly. This includes creating users, assigning roles, organising groups, managing dashboards, adding devices, configuring alarms, and checking that users only have access to the areas they need.

Administrators should make sure the platform is structured clearly before adding multiple users or devices. This helps keep the account tidy and reduces the chance of users seeing dashboards, devices, or settings they should not access.

Key administrator responsibilities include:

- Creating and managing user groups
- Setting up dashboard groups and device groups
- Assigning the correct roles and permissions
- Removing users from broad-access groups when required
- Testing user access after setup
- Regularly reviewing alarms, notifications, and device access
- Updating access settings as the account grows or user requirements change

 © 2026 Smithtek Pty Ltd. All rights reserved.

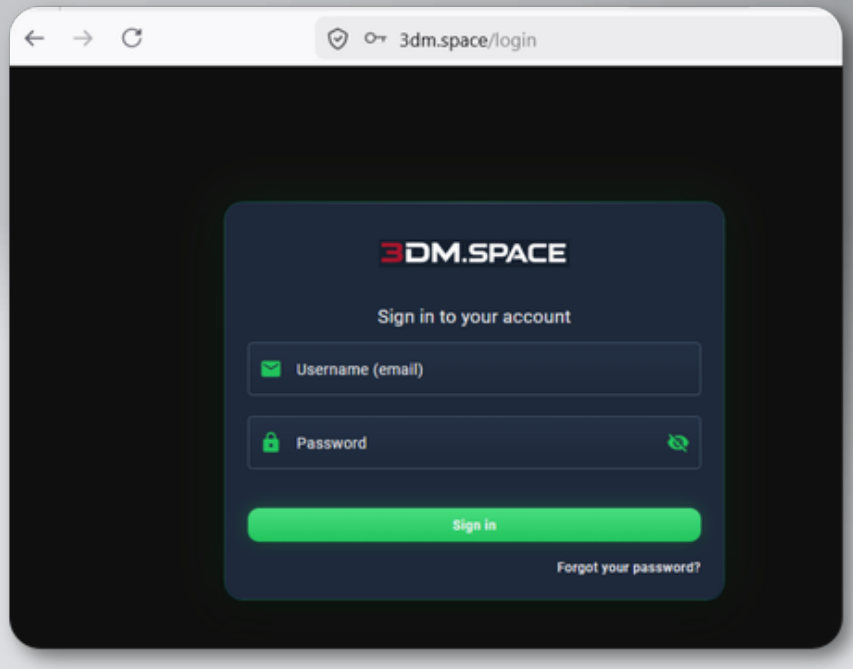
First Login

3DM.Space is accessed through a web browser. For administrator setup, it is recommended to use a desktop or laptop computer with an up-to-date browser such as Chrome, Edge, Firefox, or Safari. The administrator area is best completed on desktop because setup screens, tables, groups, roles, dashboards, and device settings are easier to manage on a larger screen.

To log in, open your 3DM.Space login page in your browser and enter the username and password provided with your account. Your account must be activated before access is available. If you lose or forget your password, click '**Forgot Password'** on the login screen and follow the reset instructions. If your account has not been fully registered or activated, the Forgot Password option may not work. In this case, contact your 3DM.Space administrator for help.

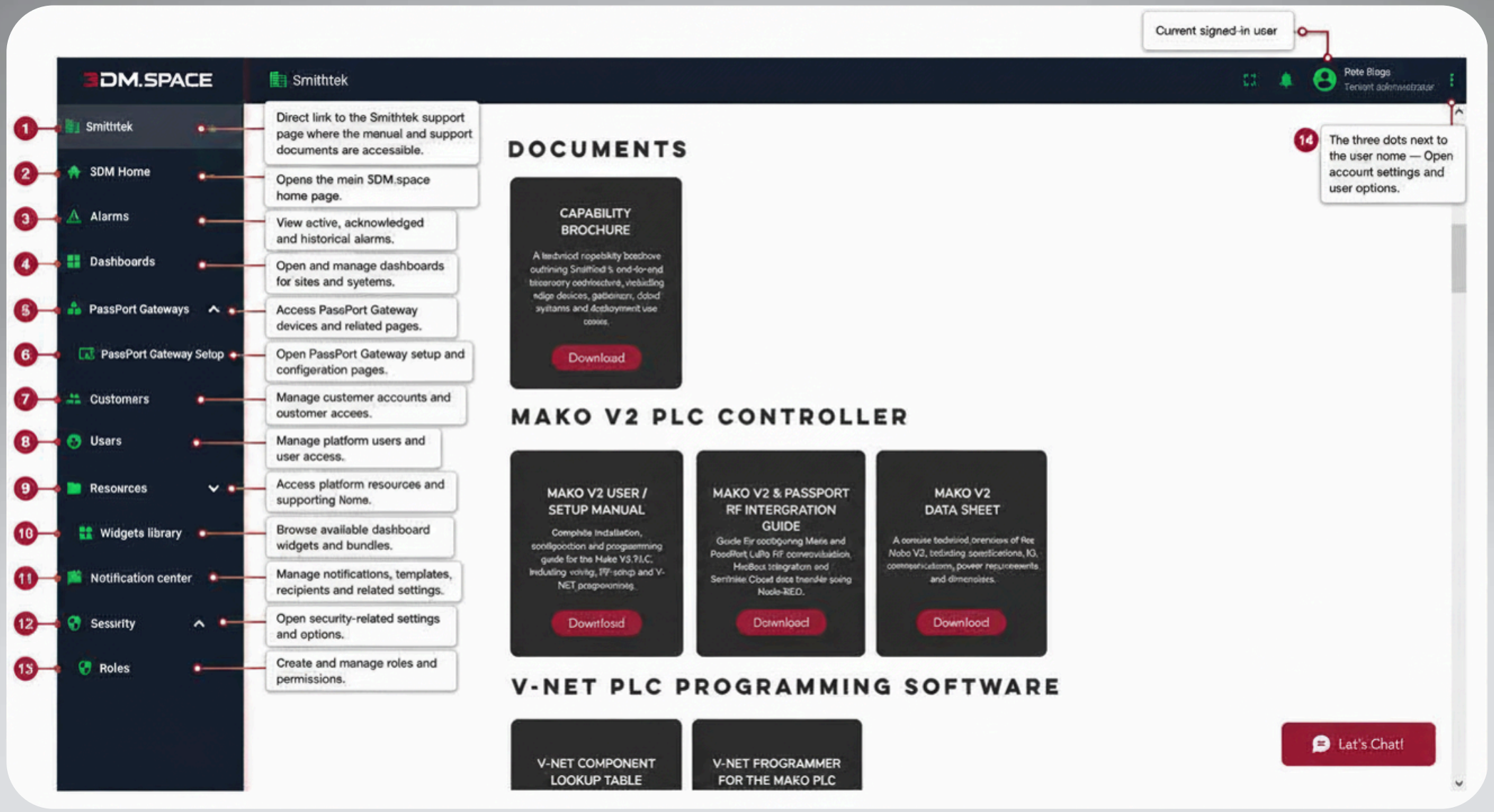
If you are the administrator and cannot access the account, contact Smithtek support.

After logging in for the first time, the administrator should review the account structure before adding users or devices. It is best to set up roles, user groups, dashboard groups, and device groups first, then add users into the correct groups. This manual uses the desktop version of 3DM.Space for all setup instructions. Mobile and tablet access is covered separately near the end of the manual.



 © 2026 Smithtek Pty Ltd. All rights reserved.

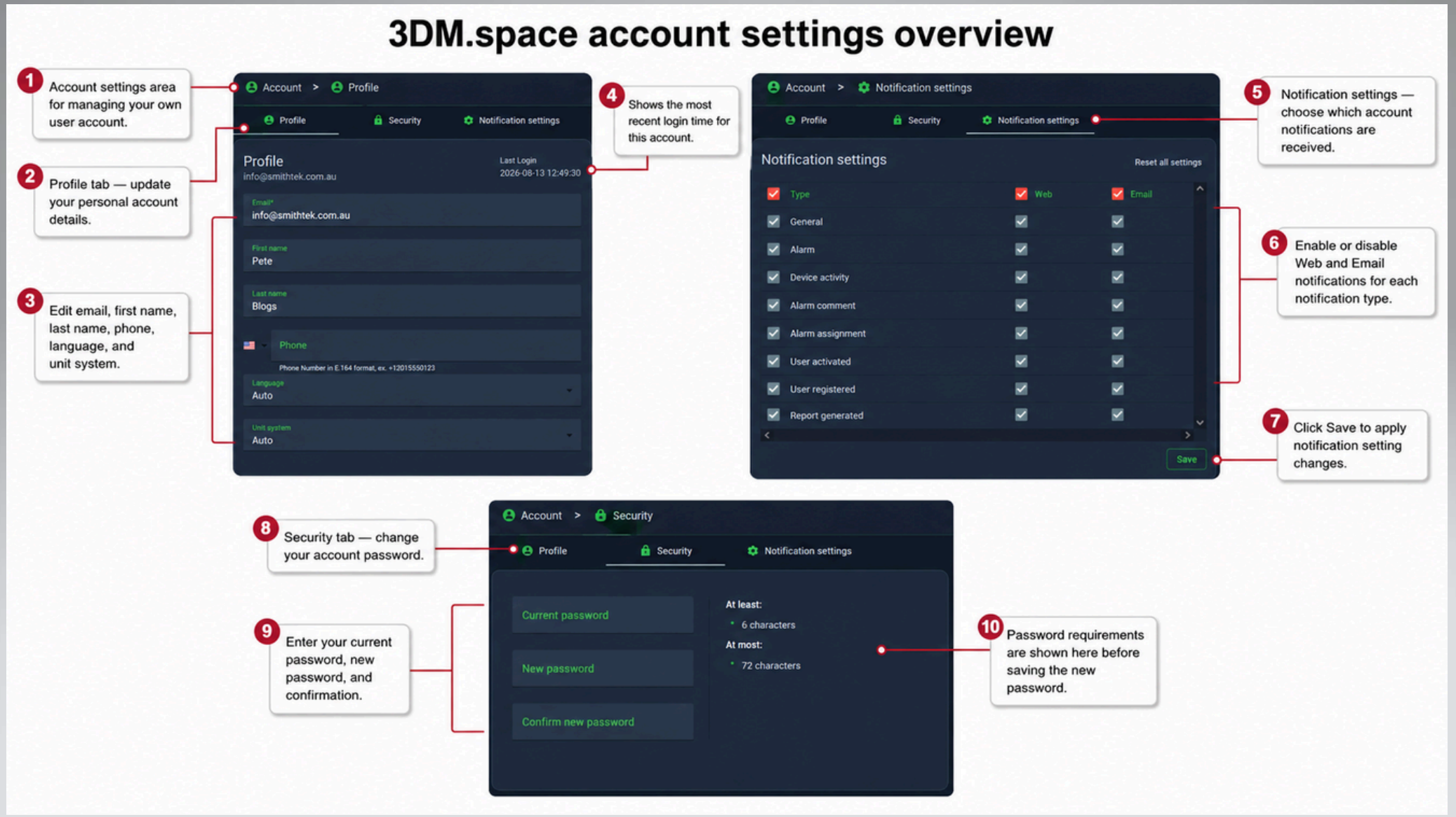
3DM Site Navigation



 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

3DM.space account settings overview



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Recommended User Set-Up

When setting up a new 3DM.Space account, it is best to create the main structure before adding lots of users and devices.
The recommended setup order is:

1. Create the required roles
2. Create user groups
3. Create dashboard groups
4. Create device groups
5. Add or move dashboards into the correct dashboard groups
6. Add or move devices into the correct device groups
7. Add users and place them into the correct user groups
8. Connect user groups to dashboard groups and device groups using roles
9. Set default dashboards for users
10. **Optional:** Test each user account to confirm they only see what they should see

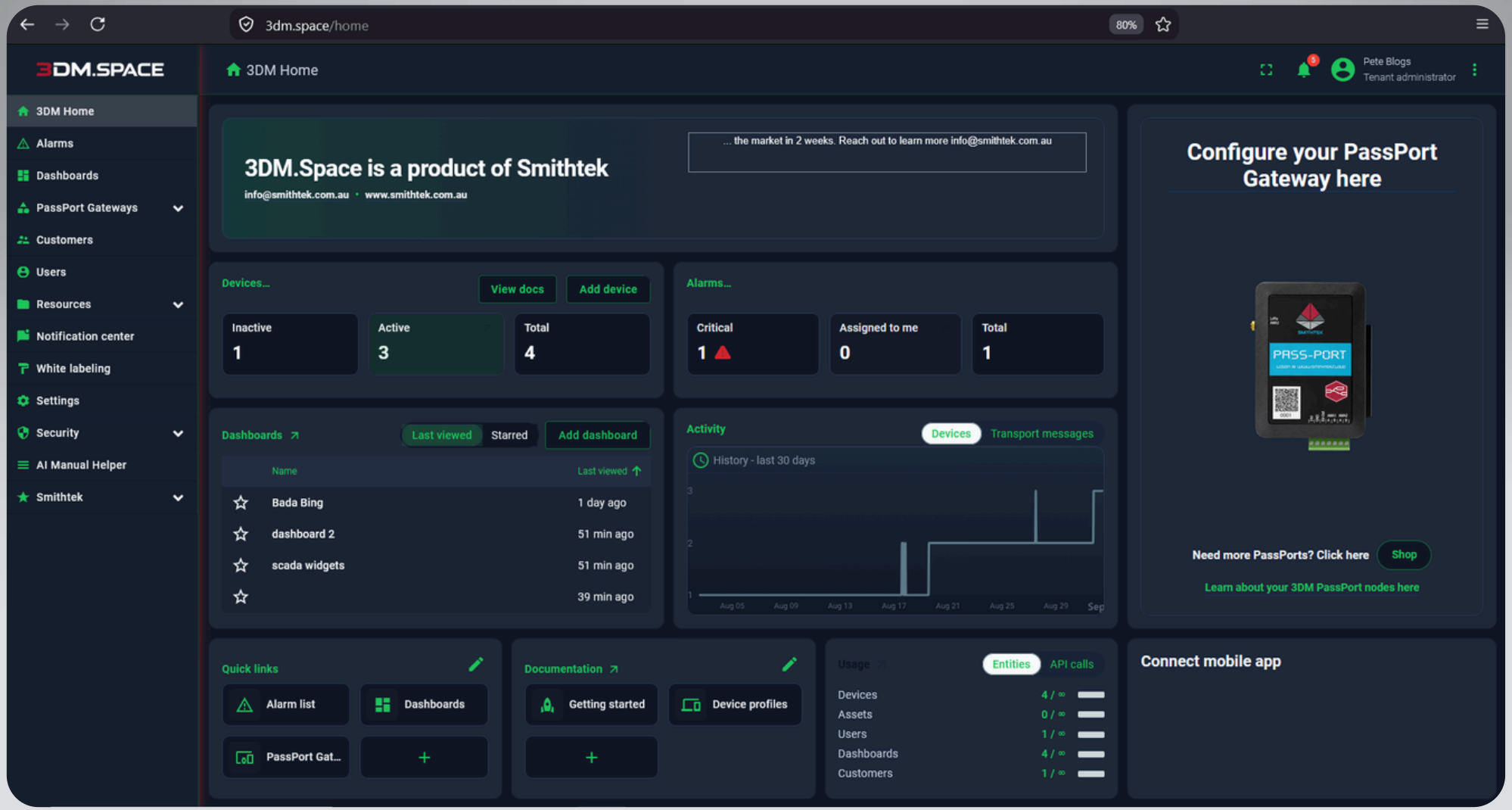
Setting the account up in this order helps keep the platform clean and easier to manage, It also reduces the chance of users being given too much access by mistake.

As a simple rule, build the structure first, then add the people.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Home Screen Dashboard

The **3DM.Space Home screen** gives users a quick overview of their account from one place.
From the Home tab, users can view useful information such as connected **PassPort Gateways**, **dashboards**, **alarms**, **activity**, **documentation links**, **usage metrics**, and other **quick-access tools**.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Basic Admin Checklist

Before adding multiple users and devices, the administrator should complete the basic setup checklist.

1. Confirm the administrator account can log in successfully.
2. Review the main account structure.
3. Create the required roles.
4. Create user groups for each team, site, client, or project.
5. Create dashboard groups for each site, client, or project.
6. Create device groups for each site, client, or project.
7. Add or move dashboards into the correct dashboard groups.
8. Add or move devices into the correct device groups.
9. Add users and place them into the correct user groups.
10. Apply the correct roles to the correct groups.
11. Set default dashboards for users where required.
12. Test each user account.
13. Confirm users can only see the dashboards, devices, alarms, and controls they are allowed to access.
14. Remove users from any broad-access groups if they can see too much.
15. Record the setup so future administrators understand how the account has been organised.

This checklist should be used during the initial account setup and repeated whenever a new user, device, dashboard, group, or site is added. Treat it as an ongoing housekeeping step to keep the system organised, secure, and easy to manage as the account grows.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Common Mistakes To Avoid

When setting up 3DM.Space, the most common mistake is adding users before the roles and groups are ready. It is better to create the structure first, then add users into the correct groups.
Avoid giving users access one by one. This becomes hard to manage as the account grows. Use user groups, dashboard groups, device groups, and roles instead.

Do not leave restricted users inside broad-access groups such as **"All"**, **"Tenant Administrators"**, or any other group that can see everything. If a user can see too much, check their group membership first.
Do not use **Generic** roles for restricted site users unless you fully understand the access being given. **Generic** roles are better suited to core team members who need wider access across the account.

Do not forget to give users access to the devices behind a dashboard. A user may be able to open a dashboard, but the data may not display properly if they do not also have access to the required device group.

Do not skip testing. After setting up a user, always log in or test their access to confirm they can only see the dashboards, devices, alarms, and controls they are meant to use.

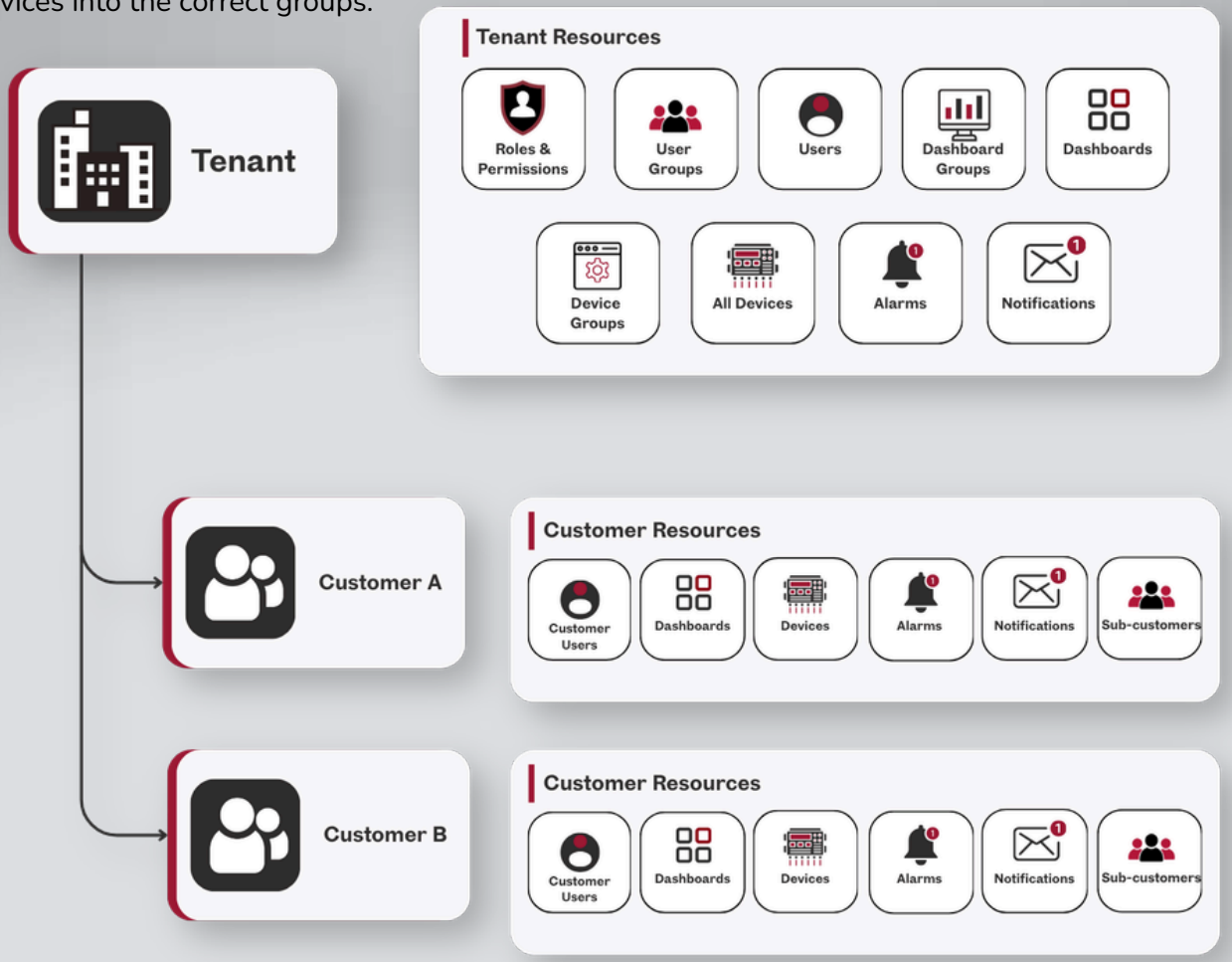
A clean setup at the start prevents permission problems later and keeps the account easier to manage.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Account Structure

A clear account structure makes 3DM.Space easier to manage. The main parts of the account are tenants, users, user groups, dashboard groups, device groups, roles, dashboards, devices, alarms, and notifications.

These parts work together to control who can access the platform, what they can see, and what they are allowed to do.
The best way to manage 3DM.Space is to avoid setting permissions one user at a time. Instead, create groups and roles first, then place users, dashboards, and devices into the correct groups.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Tenants

A tenant is the main account area in 3DM.Space. It is where the account structure, users, dashboards, devices, alarms, notifications, roles, and permissions are managed. The tenant is controlled by one or more tenant administrators.

Administrators can:

- Add and manage users
- Create user groups, dashboard groups, and device groups
- Add and manage dashboards and devices
- Create roles and assign permissions
- Set up alarm rules and notifications
- Control which areas each user can access

A tenant may also include customers. Customers are optional and can be used to separate external organisations, site owners, or clients from the main tenant account. In simple terms, the tenant is the main control area of the 3DM.Space account. All other users, groups, dashboards, and devices are organised underneath it.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Customers

Customers are optional account areas created underneath the main tenant. They are used to separate external organisations, clients, site owners, contractors, or projects from the main tenant account. Each customer can have its own customer users and assigned resources. Customer users should only be able to access the dashboards, devices, alarms, and information made available to their customer area. For example:

Tenant
- **Customer A**
- **Customer B**
- **Customer C**

Using customers helps keep each external group's data and access separate. This prevents one customer from viewing another customer's dashboards, devices, alarms, or account information.

Customer users may be permitted to:
- View assigned dashboards
- View assigned devices and telemetry
- Monitor alarms for assigned devices
- Acknowledge alarms

Customer users cannot:
- Create or manage tenant-level resources
- View another customer's data
- Create or edit device alarm rules
- Configure how alarms are generated

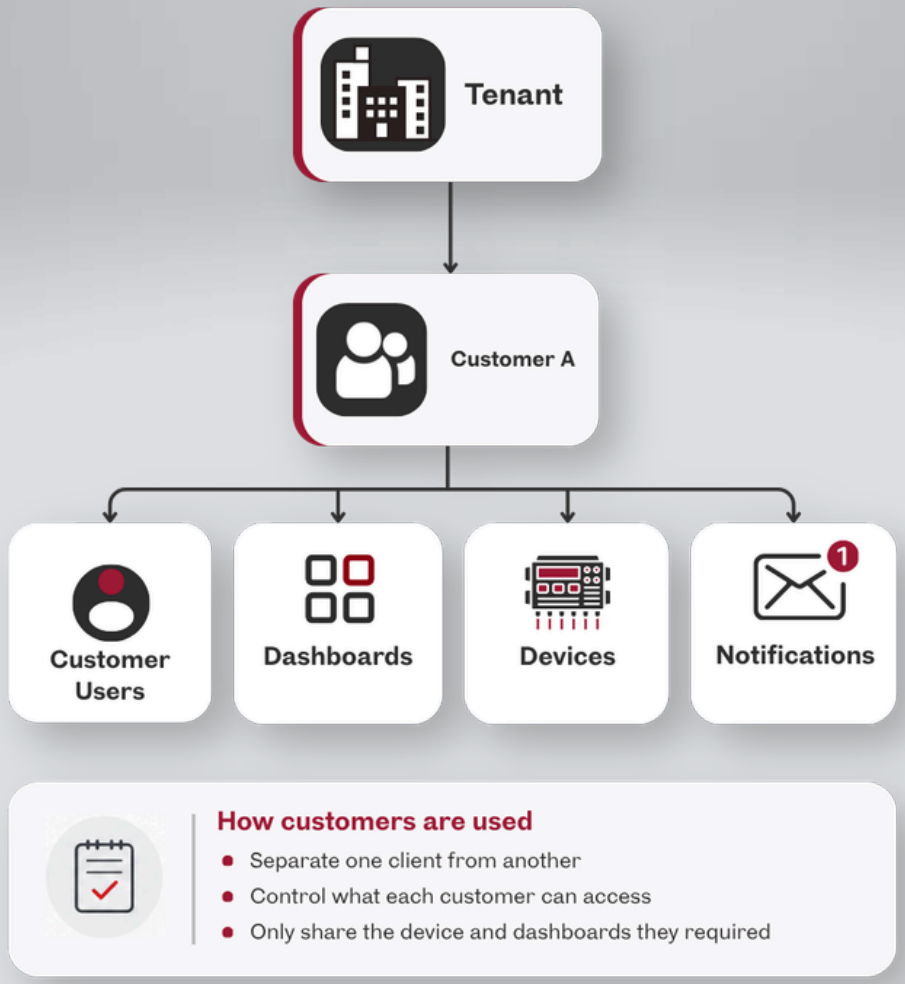
 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Customers

Customer users can view and acknowledge alarms when permitted by their role, but alarm rules must be created and managed by a tenant user.

Customers are best used for external users or organisations. Internal staff, administrators, operators, and support users should normally be managed as tenant users through user groups and roles.

Tenant administrators can create and manage customers within their tenant, but they cannot create another tenant. A separate top-level account must be created by Smithtek or the 3DM.Space system administrator.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Users

Users are the people who log in to 3DM.Space. Each user has their own login details and assigned access permissions.
Users can be created under either the main tenant or a customer:

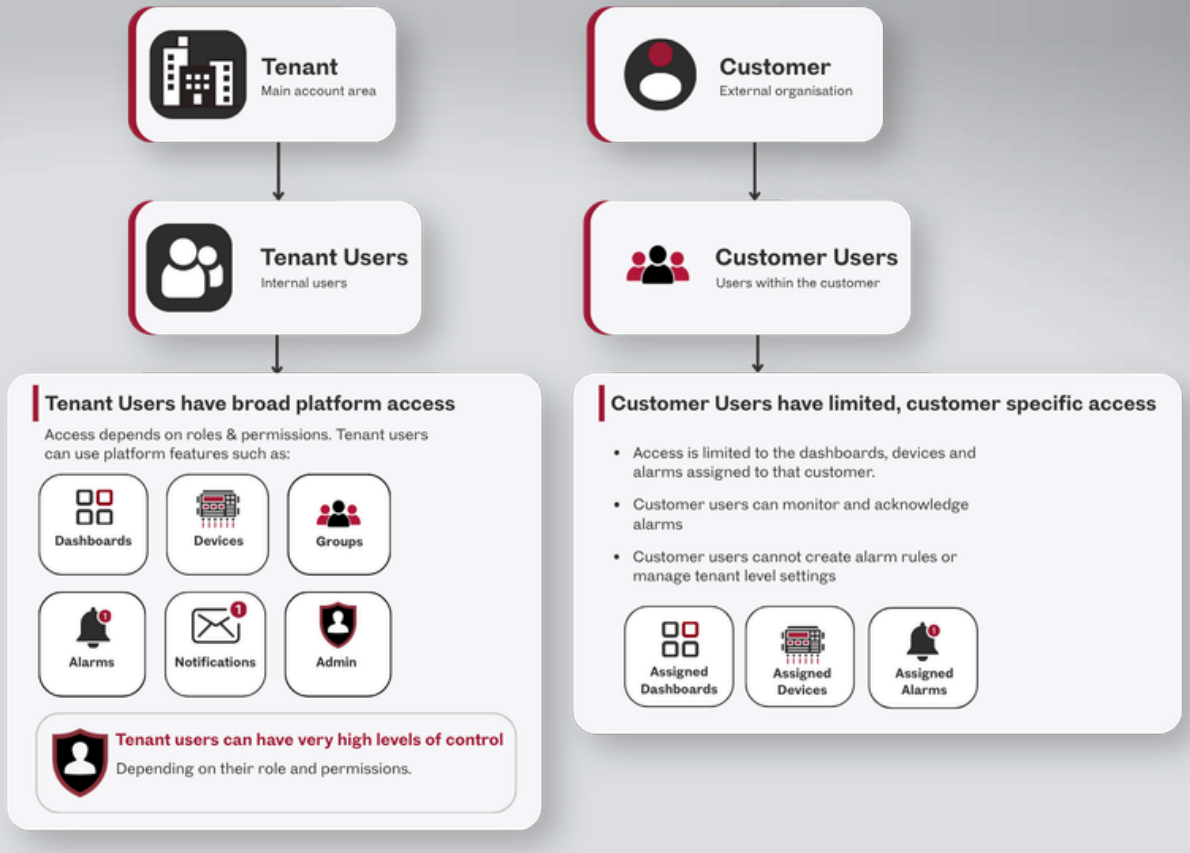
- **Tenant users** are normally used for administrators, internal staff, operators, field technicians, and support users
- **Customer users** are normally used for external clients, site owners, contractors, or organisations with access limited to their customer area

User access should be managed through user groups and roles rather than assigning permissions individually. This keeps the account organised and makes it easier to manage as more users are added.

Depending on their assigned groups and roles, **users may be able to:**

- **View dashboards**
- **View device data**
- **View and acknowledge alarms**
- **Use approved control functions**
- **Manage account settings or resources**

In simple terms, a user is anyone with login access to 3DM.Space. Their assigned groups and roles determine what they can see and do.



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Groups

Groups are used to organise users, dashboards, devices, and other resources within 3DM.Space. They allow administrators to manage access for several items at once instead of assigning permissions individually.

Groups can be created for:

- Companies
- Sites
- Projects
- Departments
- System types
- Access levels

The main group types used in 3DM.Space are:

- User groups organise users
- Dashboard groups organise dashboards
- Device groups organise PassPort Gateways and other devices

Placing a user, dashboard, or device into a group does not automatically provide access.

Access depends on the connection between:

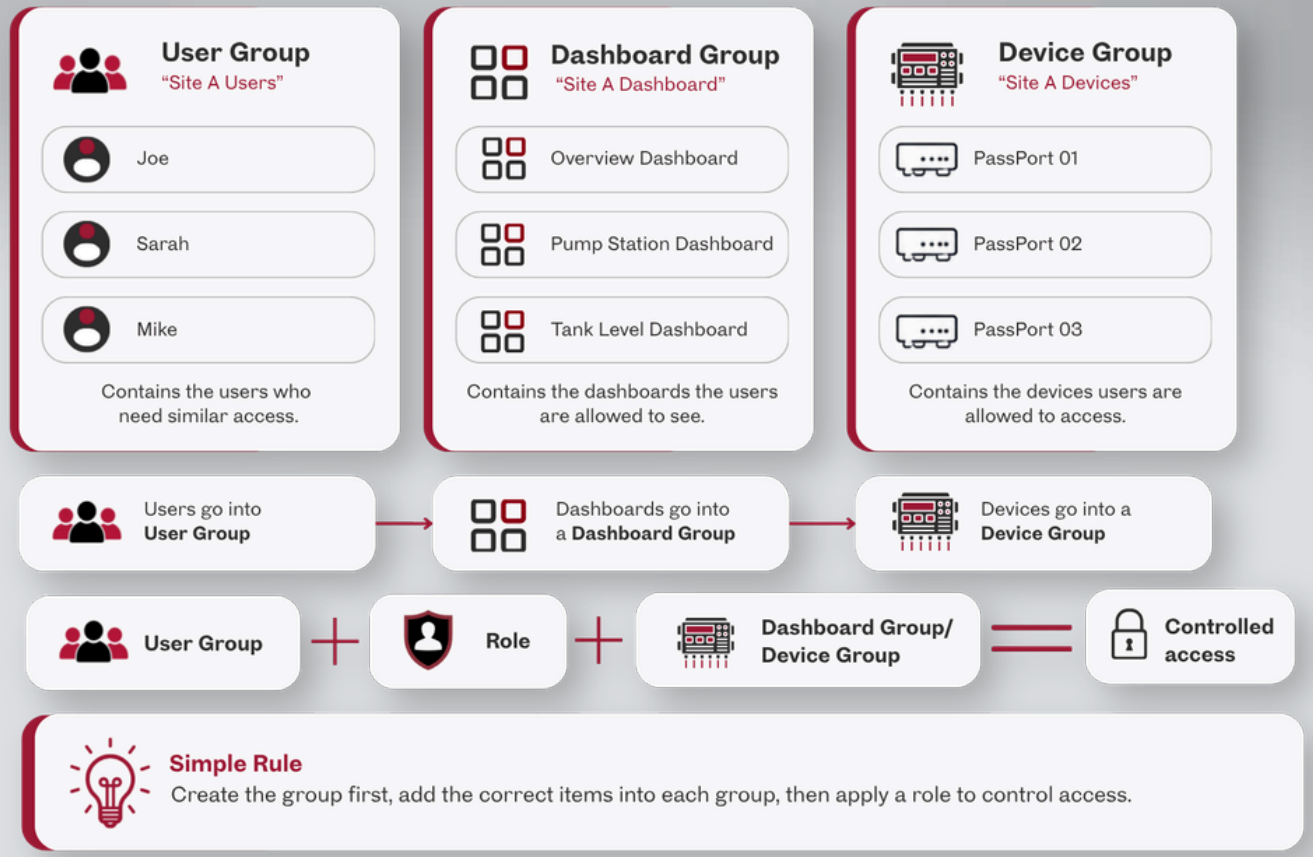
- The user group
- The dashboard or device group
- The assigned role and permissions

 © 2026 Smithtek Pty Ltd. All rights reserved.

For example, a user may have access to a dashboard group but not the related device group. In this case, the dashboard may open, but some widgets may not display live device data.

A simple way to understand the group structure is:
User group: Who receives access
Dashboard group: Which dashboards they can view
Device group: Which devices and data they can access
Role: What they are allowed to see or do

For a clean account setup, create the required groups first, add the correct users and resources, and then connect the groups using the appropriate roles.



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM User Groups

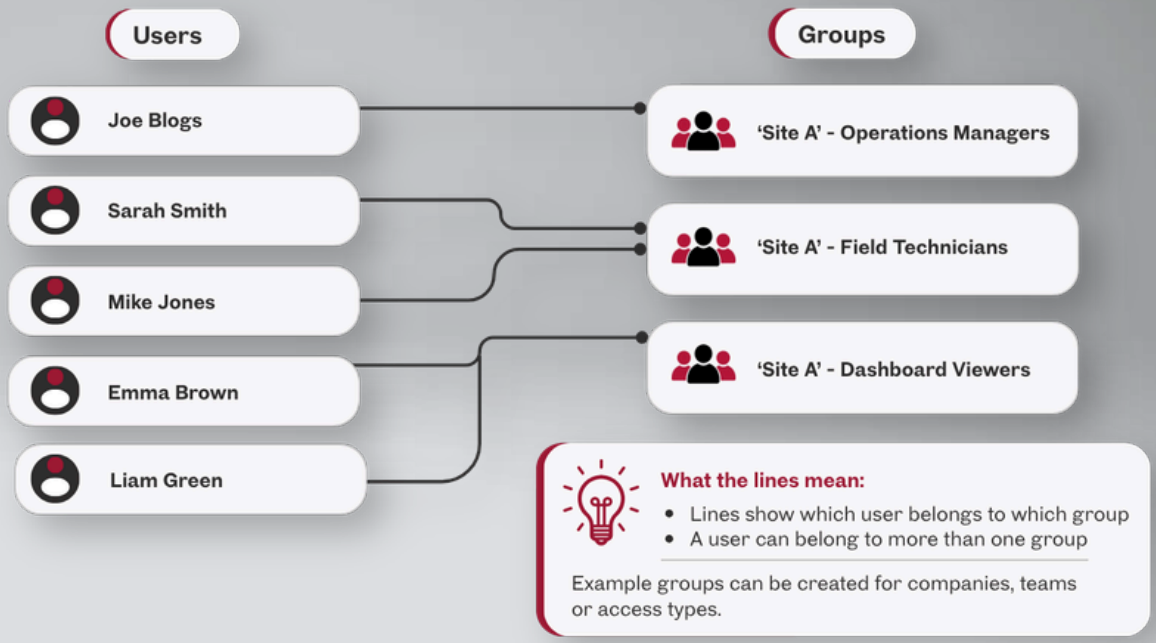
User groups are used to organise users who need the same type of access. Instead of setting permissions for each user one by one, administrators should place users into the correct user group and then assign roles to that group.

A user group may be created for a site, team, client, project, department, or access level. For example, an account may have user groups for dashboard viewers, operators, field technicians, managers, or site-specific users.

User groups help keep permissions clean and easier to manage. When a new user is added to a group, they inherit the access assigned to that group. If a user changes role or moves to a different site, they can be moved into a different user group.

A user can belong to more than one group, so administrators should be careful when assigning users. If a user can see too much, check whether they are still inside a broad-access group such as “All” or another group with wider permissions.

In simple terms, user groups are the people boxes. They decide which set of permissions a user receives.

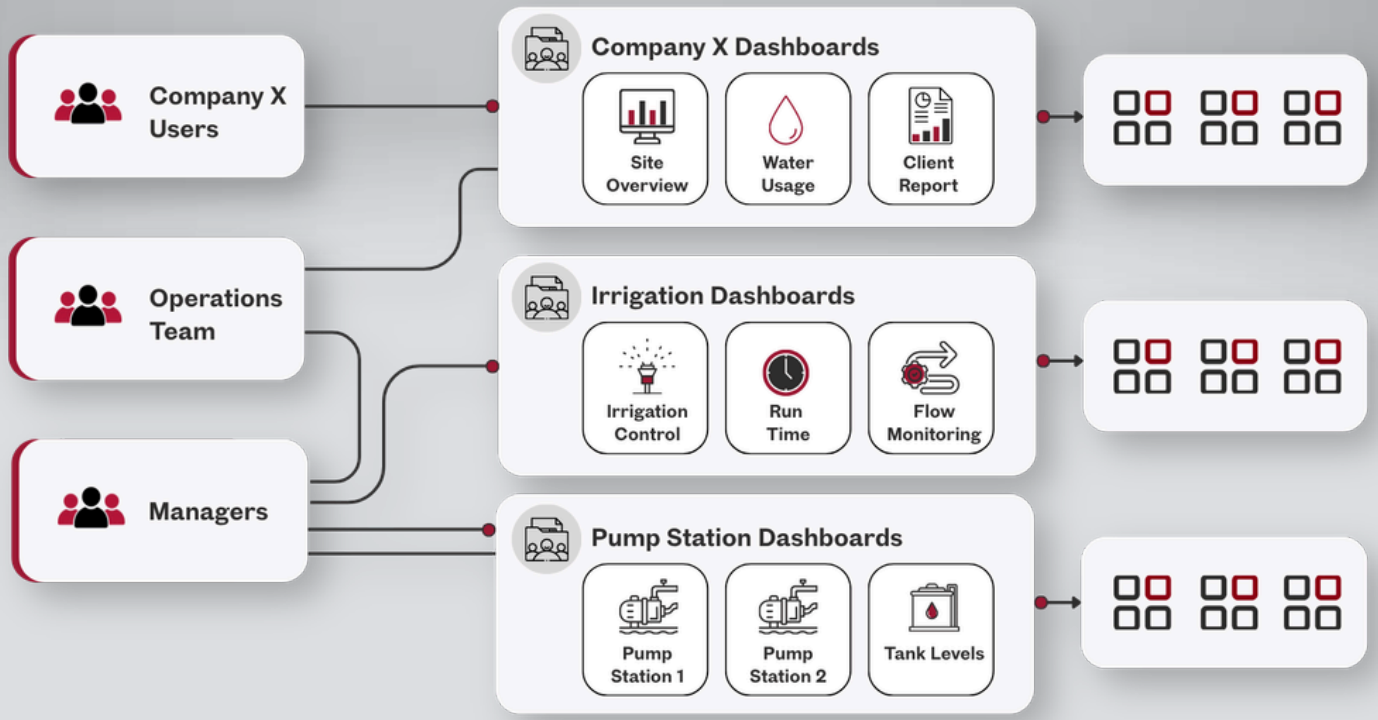


 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Groups

Dashboard groups are used to organise dashboards into clear sections. A dashboard group can be created for a site, client, project, department, or access level. Dashboards can either be created directly inside a dashboard group, or an existing dashboard can be moved into the correct group. This keeps dashboards tidy and makes it easier to manage access as more dashboards are added.
Dashboard groups are also used to control which dashboards users can see. Instead of giving users access to dashboards one by one, administrators should place dashboards into the correct dashboard group, then give the right user group permission to access that dashboard group. For example, an account may have dashboard groups such as:

Company X - Dashboards
Company Y - Dashboards
Irrigation Dashboards
Pump Station Dashboards
Read Only Dashboards



Dashboard groups help keep dashboards organised and limit visability to the authorised users.
Users may also require matching device group access for LIVE dashboard data.

 © 2026 Smithtek Pty Ltd. All rights reserved.

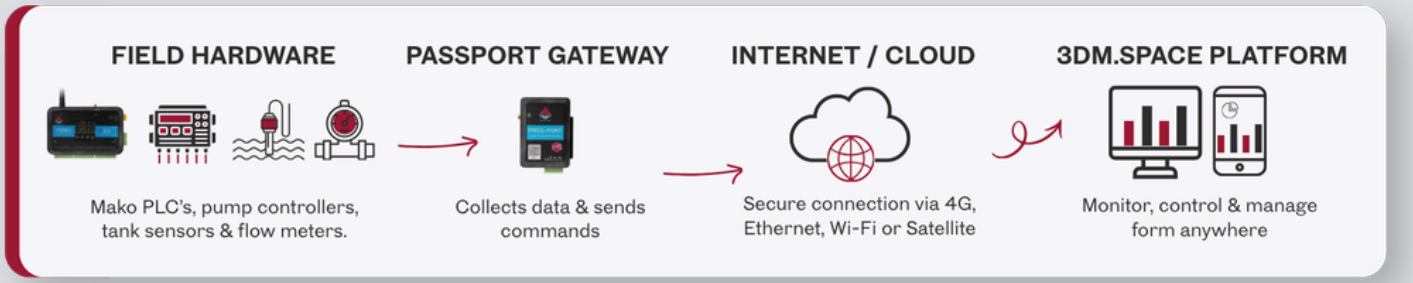
3DM Device Groups

Device groups are used to organise devices into clear sections. A device group can be created for a site, client, project, location, system type, or access level. Devices can either be created directly inside a device group, or an existing device can be moved into the correct group. This keeps devices tidy and makes it easier to manage access as more devices are added. Device groups are also used to control which devices users can access. Instead of giving users access to devices one by one, administrators should place devices into the correct device group, then give the right user group permission to access that device group.

For example, an account may have device groups such as:

Company X - Devices
Company Y - Devices
Irrigation Devices
Pump Station Devices
Tank Monitoring Devices
Remote Site Devices





 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Groups

A user will only access the devices they have permission to use. If a device is placed in the wrong group, the wrong users may be able to see it, or the correct users may not be able to access it.

Device groups are important because dashboards often rely on device data. A user may be able to open a dashboard, but the widgets may not show live values if the user does not also have access to the related device group.

Device groups can include connected equipment such as PassPort Gateways, Mako PLCs, remote sensors, pump controllers, tank monitoring devices, irrigation controllers, and other field devices.

In simple terms, device groups are the device boxes. They help organise equipment and control which users can access device data and control functions.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Roles & Permissions

Roles and permissions control what users are allowed to do inside 3DM.Space. They work together with groups to decide what a user can see, access, edit, control, or manage. A role is a set of permissions. These permissions may allow a user to view dashboards, access devices, control equipment, manage alarms, create dashboards, edit devices, or manage other platform features.

Permissions should not be assigned randomly. The safest way to manage access is to decide what each type of user needs to do, then create a role that matches that responsibility.
For example, a dashboard viewer may only need to see dashboards and live data. A field technician may need to view devices, use controls, and manage alarms. An operations manager may need broader access to manage dashboards, devices, alarms, and day-to-day operations.

3DM.Space uses two main role types: **Generic roles** and **Group roles**.
Generic roles are used when a user needs broader access across the account. These are normally used for internal staff, administrators, operations managers, or trusted users who need access to wider platform features.
Group roles are used when access needs to be limited to specific groups. For example, a user may only be allowed to see one site's dashboards and devices. In this case, a group role can be connected to the correct user group, dashboard group, and device group.
A simple way to understand it is:

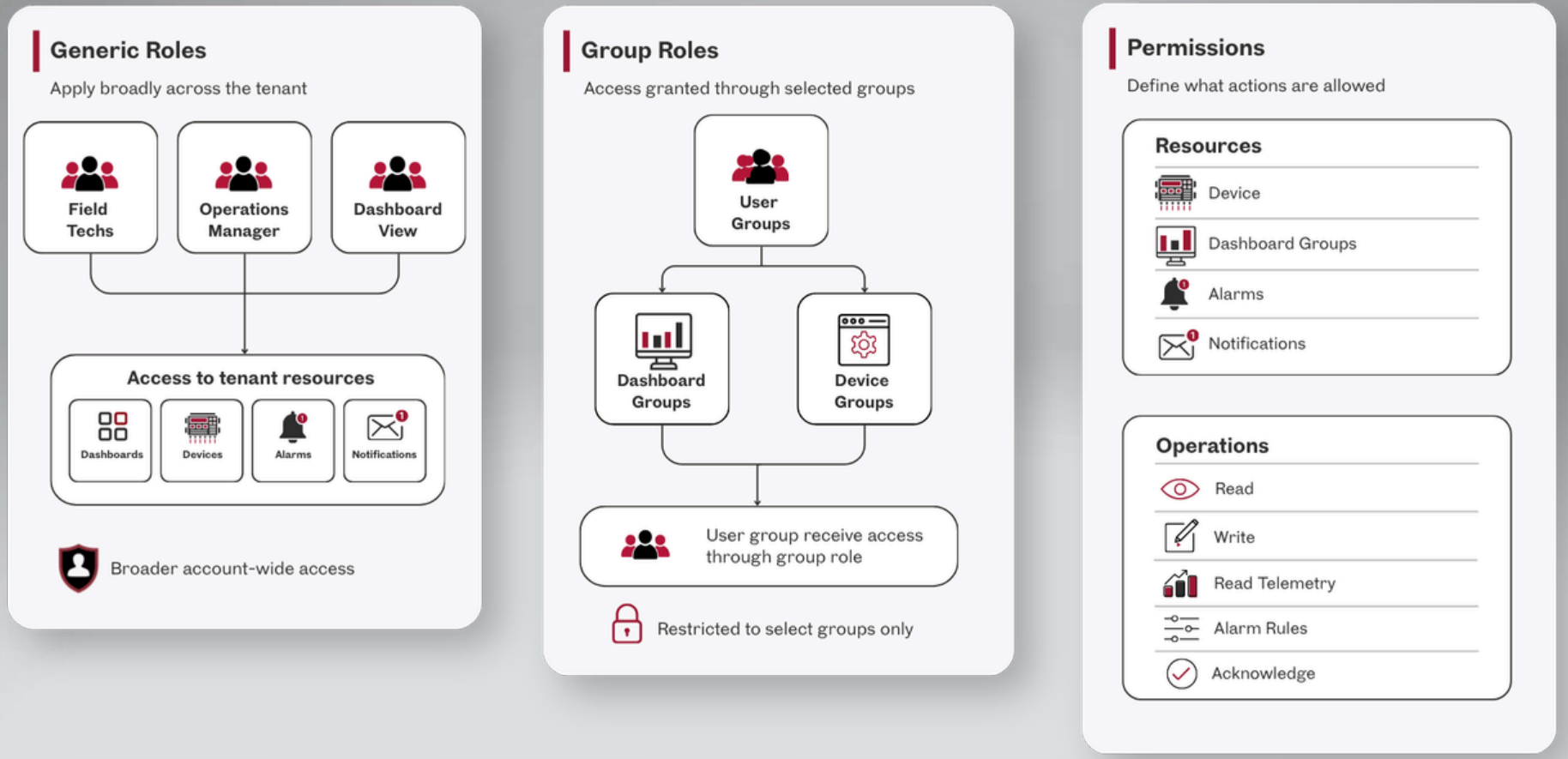
Generic role - broader account access (**Resources and Permissions**)
Group role - restricted access to selected groups (**Permissions only**)

Roles should always match the user's responsibility. Do not give users more access than they need. If a user only needs to view a dashboard, they should not be given permissions to edit dashboards, create devices, or manage alarm rules.
It is also important to remember that permissions can build on each other. If a user belongs to more than one user group, they may inherit access from each group. If a user can see or do more than expected, check all of the groups and roles assigned to that user.

For best results, create the required roles before adding users. This makes setup cleaner and helps avoid permission mistakes later.
In simple terms, roles are the keys. Groups are the boxes. A user only gets access when the correct key is connected to the correct box.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Roles & Permissions Overview





 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Setting Up Roles

How to make a Group Role

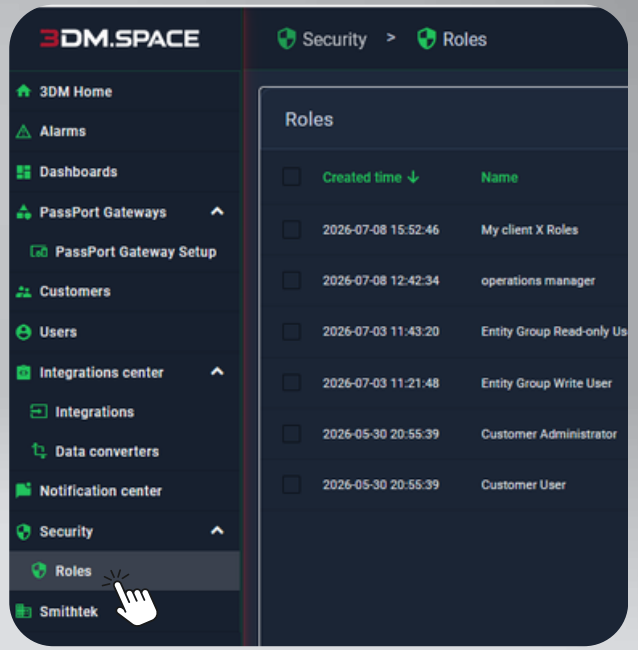
1. Go to **“Security ⟶ Roles”.**
2. Click **“Add role”**.
3. Enter a **“Role name”**. Example: **“Site Operator”** or **“Water Corp Dashboard Read Only”**.
4. Set **“Role Type”** to **“Group”.**
5. Add the required operations.
6. Click **“Save”**.
7. After creating the role, go to the required User Group, Dashboard Group or Device Group to assign the role.

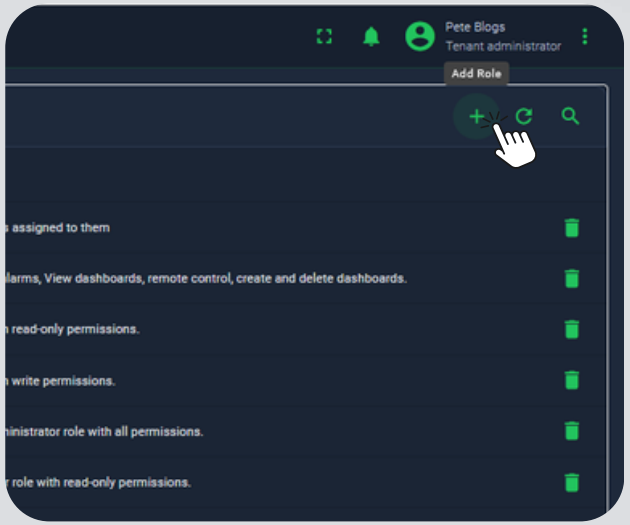
Important: A Group Role does nothing on its own until it is linked to a group.

How to make a Generic Role

1. Go to **“Security ⟶ Roles”.**
2. Click **“Add role”**.
3. Enter a **“Role name”**. Example: **“Field Techs”** or **“Operations Manager”**.
4. Set **“Role Type”** to **“Generic”.**
5. Add the required operations.
6. Click **“Save”**.
7. Assign the role to the relevant user or user group as needed.

Important: Generic Roles are broader and are best for trusted internal users.



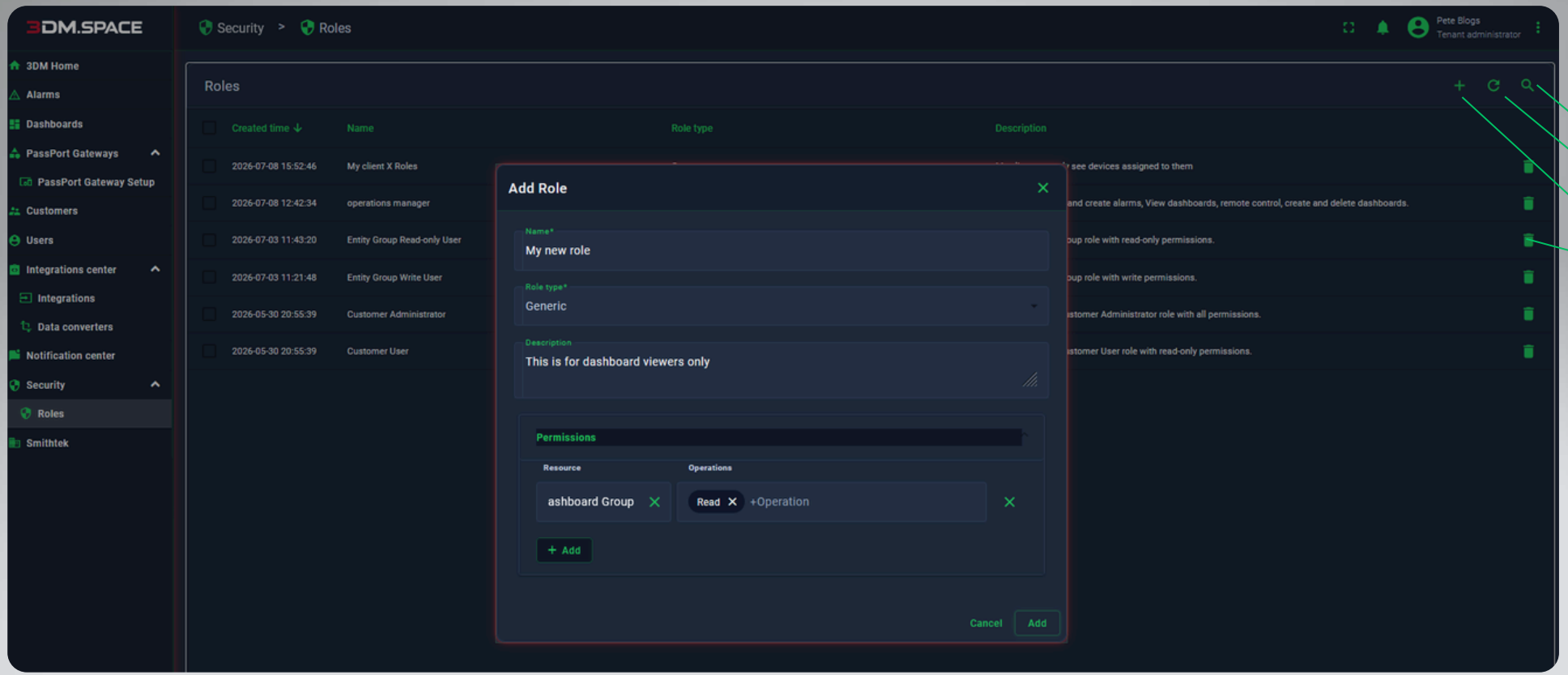


Helpful Tips

- Use clear role names so the purpose is easy to understand.
- Use Group Roles when you want to restrict access to selected groups only.
- Use Generic Roles when users need broader access across the tenant.
- If a user cannot see a dashboard, check their dashboard group, device group and role permissions.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Setting Up Role Details



Generic Role Templates

The following Generic role examples provide a simple starting point for setting up core team access in 3DM.Space. These roles are suitable for many organisations because they cover the most common access levels, from view-only users through to managers and field staff who need broader control.

Generic roles are best used for trusted users who need access across the account, rather than being restricted to one selected site or group. The examples include a Dashboard Viewer role for office staff or supervisors who only need to monitor dashboards, a Dashboard Viewer with Remote Control role for users who also need to operate approved controls, a Field Techs role for technicians who need device and alarm rule access, and an Operations Manager role for users who manage day-to-day platform operations without managing users.
These role names are examples only and can be changed to suit your organisation. The important part is choosing the correct permissions for the level of access required.

Use these roles as a guide when creating your own access structure:

- **Dashboard Viewer** for users who only need to view dashboards and data.
- **Dashboard Viewer with Remote Control** for users who need to view dashboards and operate approved controls.
- **Field Techs** for technicians who need access to devices, alarms, and alarm rule setup.
- **Operations Manager for managers** who need broad operational access, but should not add, edit, or delete users.

As a best practice, only give users the permissions they need for their role. If a user does not need to edit dashboards, create devices, manage alarm rules, or change users, those permissions should not be included.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Generic Role Templates

Operations Manager

Role Summary

Best used for:	Trusted internal managers who run daily operations
Allows:	Manage devices, dashboards, assets, alarms and alarm rules
View only:	Users, user groups and roles
Does not allow:	Add, edit or delete users

Permission Summary

Resource	Operation	Function
Device	All	Can manage devices
Device	Read calculated field & alarm rules	Can view device alarm rules
Device	Write calculated field & alarm rules	Can create or edit device alarm rules
Alarm	All	Can view, acknowledge, clear & manage alarms
Dashboard Group	All	Can manage dashboard groups
Dashboard	All	Can manage dashboards
Asset	All	Can manage assets
Entity View	All	Can manage entity views
Device Profile	Read	Can view device profiles
Rule Chain	Read	Can view rules chains
User	Read	Can view users only
User Group	Read	Can view users groups only
Role	Read	Can view roles only

This role is for broad operational control, but user management remains locked down.

Field Technicians

Role Summary

Best used for:	Technicians who need access across the account
Allows:	View dashboards, view devices, set up and manage alarms
Warning:	This role is broader than a Group Role
Trusted users only:	Only assign this role to trusted users

Permission Summary

Resource	Operation	Function
Device	Read	Can see devices
Device	Read Telemetry	Can view device data
Device	Read calculated field & alarm rules	Can view alarm rules on devices
Device	Write calculated field & alarm rules	Can create or edit alarm rules on devices
Alarm	All	Can view, acknowledge, clear & manage alarms
Dashboard Group	Read	Can see and open dashboard groups
Dashboard Group	Read Telemetry	Can show dashboard data
Dashboard Group	Write Telemetry	Can use dashboard widgets or control actions
Dashboard Group	Write	Can edit dashboards
Dashboard Group	Create	Can create dashboard groups
Dashboard Group	Delete	Can delete dashboard groups

This role gives trusted field technicians broad dashboard & alarm access across the account.

3DM Generic Role Templates

Dashboard View

Role Summary

	Best used for:	Core team members who need to view dashboards across the account
	Allows:	View dashboards & dashboard data only
	View only:	This role is broader than a Group Role
	Trusted users only:	Device control, dashboard editing, creating devices, alarm management or user changes

Permission Summary

Resource	Operation	Function
Dashboard Group	Read	Allows the user to see & open dashboard groups
Dashboard Group	Read Telemetry	Allows dashboard widgets to display live data
Dashboard	Read	Allows the user to view dashboards
Dashboard	Read Telemetry	Allows dashboards to show telemetry data
Device	Read	Allows dashboards to access device information
Device	Read Telemetry	Allows dashboards to show telemetry data
Alarm	Read	Allows dashboard alarm widgets to show alarms

This role is for dashboard viewing only & does not allow control or alarm management actions.

Dashboard Viewer with Remote Control

Role Summary

	Example role name:	Dashboard Viewer with Remote Control
	Role type:	Generic
	Best used for:	Core team members who need to view dashboards & control equipment across the account
	Allows user to:	View dashboards, view device data, use on/off control, view alarms & acknowledgement alarms
	User access rules:	This role cannot edit dashboards, create devices, set up alarms, delete alarms or change users

Permission Summary

Resource	Operation	Function
Dashboard Group	Read	Allows the user to see & open dashboard groups
Dashboard Group	Read Telemetry	Allows dashboard widgets to display live data
Dashboard Group	Write Telemetry	Allows dashboard widgets to send control where telemetry writing is used
Dashboard	Read	Allows the user to view dashboards
Dashboard	Read Telemetry	Allows dashboards to show telemetry data
Dashboard	Write Telemetry	Allows dashboard controls to send commands
Device	Read	Allows dashboards to access device information
Device	Read Telemetry	Allows dashboards to show telemetry data
Device	Write Telemetry	Allows the users to send on/off commands to device
Device	RPC Call	Allows the user to use dashboard controls that send RPC commands
Alarm	Read	Allows the user to view alarms
Alarm	Acknowledgement	Allows the user to acknowledge alarms only

This is role for viewing dashboards & remote controlling equipment. It does not include anyconfiguration or user management permissions.

Group Role Templates

The following Group role examples provide a simple starting point for setting up restricted site, client, or project access in 3DM.Space.
These roles are useful when users should only access selected groups, rather than having access across the whole account. Group roles are best used when access needs to be limited to specific dashboard groups, device groups, asset groups, or other selected areas. Unlike Generic roles, Group roles do not choose the resource inside the role itself. Group roles only define the operations allowed. The actual resource is selected later when the role is assigned to the required group.

These role names are examples only and can be changed to suit your organisation, site, client, or project. The important part is choosing the correct operations for the access level required, then assigning the role to the correct group.

Use these roles as a guide when creating restricted access:

Dashboard Reader for users who only need to view selected dashboards, live data, and related alarm rule information.
Operation Field Staff for users who need to view selected dashboards, view live data, write values, use controls, and work with calculated fields or alarm rules inside selected groups.
Site Dashboard Viewer with Remote Control for users who need to view selected dashboards and operate approved controls, but should not edit dashboards, create devices, manage users, or set up broader account settings.
Site Operations Manager for managers who need to manage selected site groups, devices, alarms, and alarm rules, but should not add, edit, or delete users.

As a best practice, only assign the operations the user actually needs. A Group role will not give access by itself. It must be attached to the correct dashboard group, device group, asset group, or other resource group before the user receives access.
In simple terms, Group roles decide what the user can do, and the assigned group decides where they can do it.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Site Operations Manager

Role Summary

Example role name:	Site Operations Manager
Role type:	Group
Best used for:	Managers who should manage selected site groups only
Allows user to:	Manage selected dashboards, devices, alarms and alarm rules within assigned groups
Important note:	This role does not give access by itself. It must be assigned to the required group. Group roles define operations only

Operations

Operations To Allow	What This Gives The User
All	Gives full available access to the selected group this role is assigned to

This role is for viewing dashboards & remote controlling equipment. It does not include anyconfiguration or user management permissions.

Operational Field Staff

Role Summary

Example role name:	Operation Field Staff
Role type:	Group
Best used for:	Field staff who need to monitor and update selected site dashboards and device data
Allows user to:	View selected dashboards & data, write values, write telemetry & manage calculated fields & alarm rules within assigned groups
User access rule:	This role only applies to the dashboard groups & device groups it is attached to

Operations

Operations To Allow	What This Gives The User
Read	Allows the user to open & view assigned dashboards & related data
Read Telemetry	Allows assigned dashboards to show live telemetry data
Read Calculated Field & Alarm Rules	Allows the user to view calculated fields & alarm rules
Write	Allows the user to update editable items within assigned groups
Write Telemetry	Allows the user to send values & use control actions where telemetry wiring is used
Write Calculated Field & Alarm Rules	Allows the user to create or edit calculated fields & alarm rules

This role is for viewing dashboards & remote controlling equipment. It does not include any configuration or user management permissions.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Group Role Templates

Dashboard Reader

Role Summary

	Role setting:	**Recommended setup**
	Example role name:	Dashboard Reader
	Role type:	Group
	Best used for:	Users who should only read selected dashboards & related data
	Allows user to:	View dashboards, live data & calculated field & alarm rule information
	User access rule:	This role cannot control devices, edit dashboards, create devices, setup alarm rules, manage alarms or change users

Operations

Operations To Allow	What This Gives The User
Read	Allows the user to open selected dashboards & related groups
Read Telemetry	Allows selected dashboards to show live data
Read Calculated Field & Alarm Rules	Allows the user to view calculated field & alarm rule information used by the dashboard

Assign this role to the dashboard groups and device groups the user should access.

Site Dashboard Viewer with Remote Control

Role Summary

	Role setting:	**Recomended setup**
	Example role name:	Site Dashboard Viewer with Remote Control
	Role type:	Group
	Best used for:	Users who should view selected site dashboards and use dashboard controls only
	Allows user to:	View selected dashboards, view selected device data, use on/off controls, and view alarms.
	User access rule:	This role cannot edit dashboards, create devices, set up alarm rules, delete devices, or change users.

Operations

Operations To Allow	What This Gives The User
Read	Allows the user to open selected dashboard groups and selected device groups
Read Telemetry	Allows selected dashboards to show live data
Write Telemetry	Allows dashboard control buttons to send commands where telemetry writing is used
RPC Call	Allows the user to use dashboard controls that send RPC commands
Alarm Read	Allow the user to view alarms
Alarm Write	Allows the user to update alarms where supported, such as acknowledge or clear actions

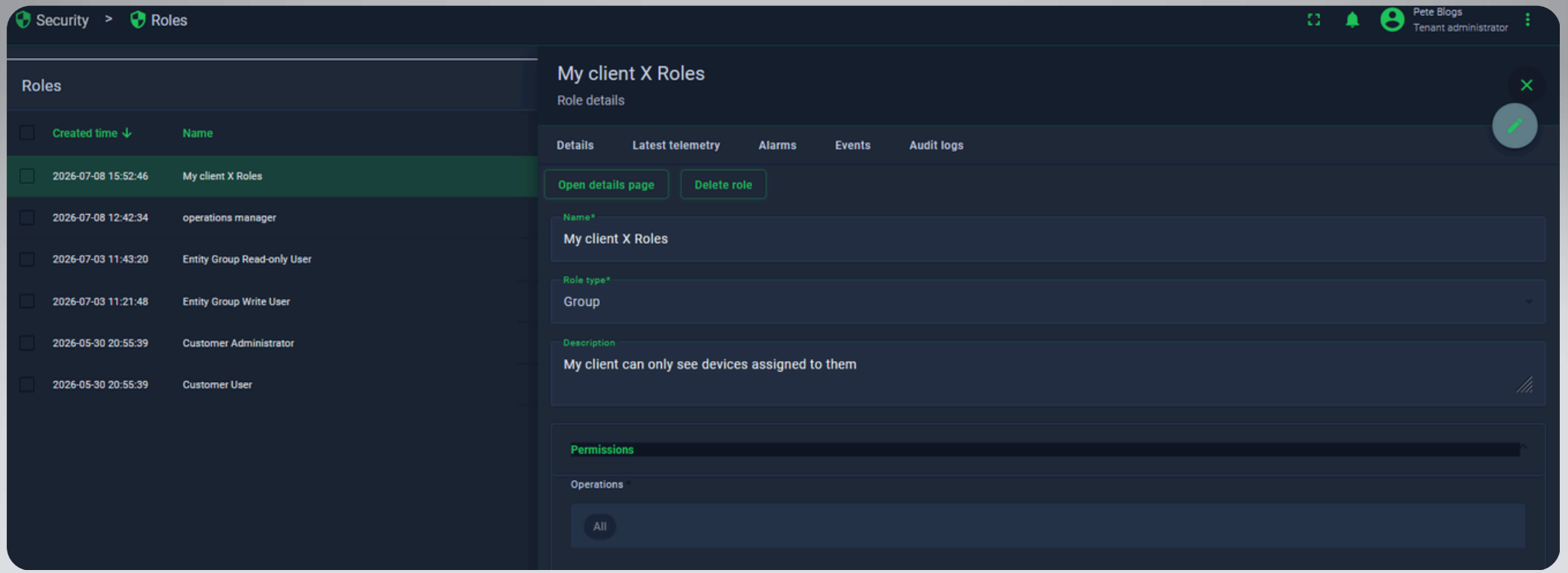
Assign this role to the dashboard groups and device groups the user should access.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Editing an existing role

An existing role can be opened and edited at any time.

Go to **Security → Roles**, then click the role you want to update. A side window will open showing the role details. Click the pen to edit or the cross to exit.



 © 2026 Smithtek Pty Ltd. All rights reserved.

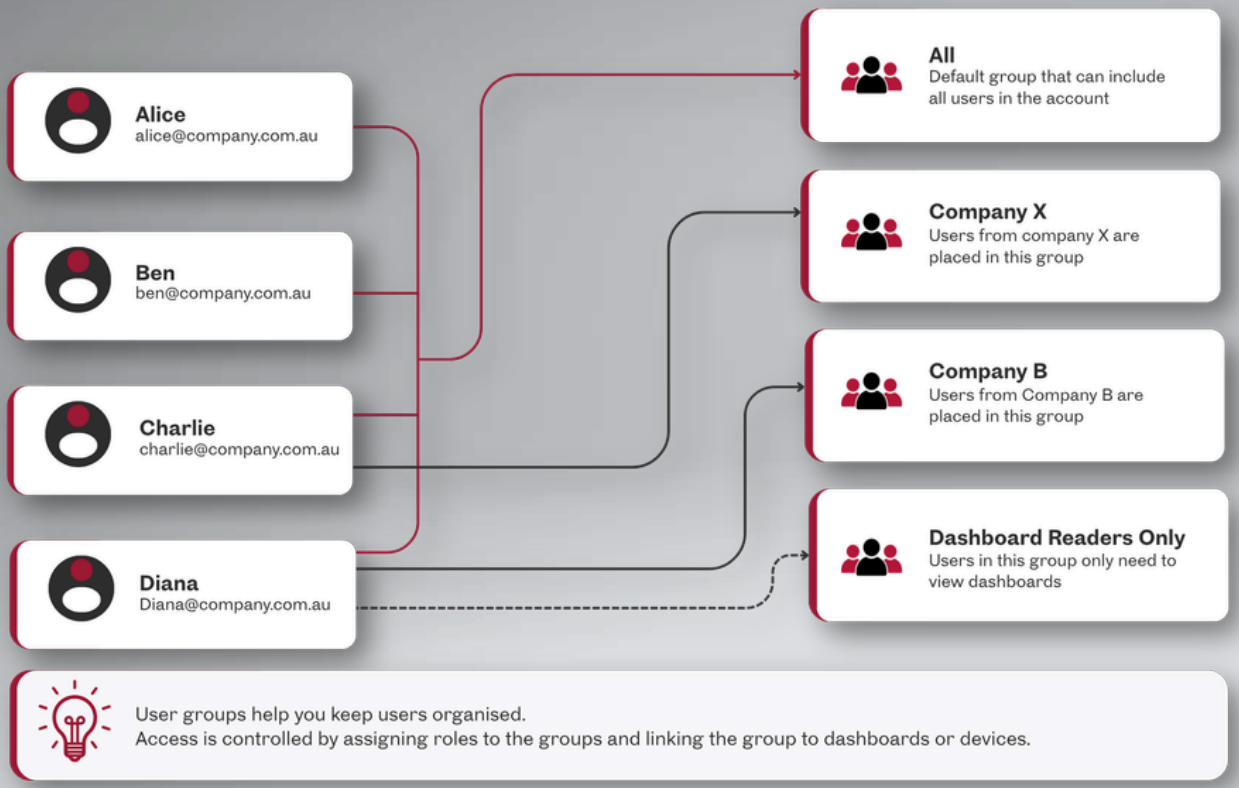
The role details window includes the following areas:

Name
This is the role name. Use a clear name that explains what the role is for, such as “Dashboard Reader”, “Operations Manager”, or “Client X Roles”.
Role type
This shows whether the role is a Generic role or a Group role.
Generic roles are used for broader account access. Group roles are used for access that will be assigned to selected groups.
Description
This is a short note explaining what the role is used for. It is helpful to describe the access level clearly so other administrators understand the purpose of the role later.
Permissions
This is where the allowed operations are set. For Group roles, this section shows the operations only, such as Read, Write, Read Telemetry, Write Telemetry, RPC Call, or All. The actual dashboard group, device group, or other resource group is selected later when the role is assigned.
Details tab
This is the main tab used when setting up or editing a role.
Latest telemetry:
Alarms, Events, and Audit logs tabs
These tabs are not normally used when setting up roles. They can be ignored during normal role setup and may be used for future platform features or system tracking.

After making changes, click the edit button, update the role settings, and save the role.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM User Groups



User groups are used to organise users and make access easier to manage. A new 3DM.Space account may include default user groups that can be used for quick setup, such as:

- **All**
- **Tenant Administrators**
- **Tenant Users**

The default groups should be used carefully. Broad groups such as All or Tenant Administrators may give users more access than expected if roles have been assigned to them. For restricted users, it is best to create specific user groups for each site, company, team, or access level.

User groups organise users who need the same type of access. Instead of setting permissions for each user individually, administrators place users into the appropriate group and apply roles to that group.

A user group can represent a:

- **Company**
- **Site or project**
- **Department or team**
- **Access level**

For example: Dashboard Viewers, Field Staff, Operations Managers, Support Staff or users assigned to a particular site.

Why use user groups?

- **Simpler user management** – new users receive the access assigned to their group.
- **Easier changes** – move a user to another group if their role or site changes.
- **Consistent permissions** – users doing similar work receive the same level of access.
- **Multiple groups** – a user can belong to more than one group when required.

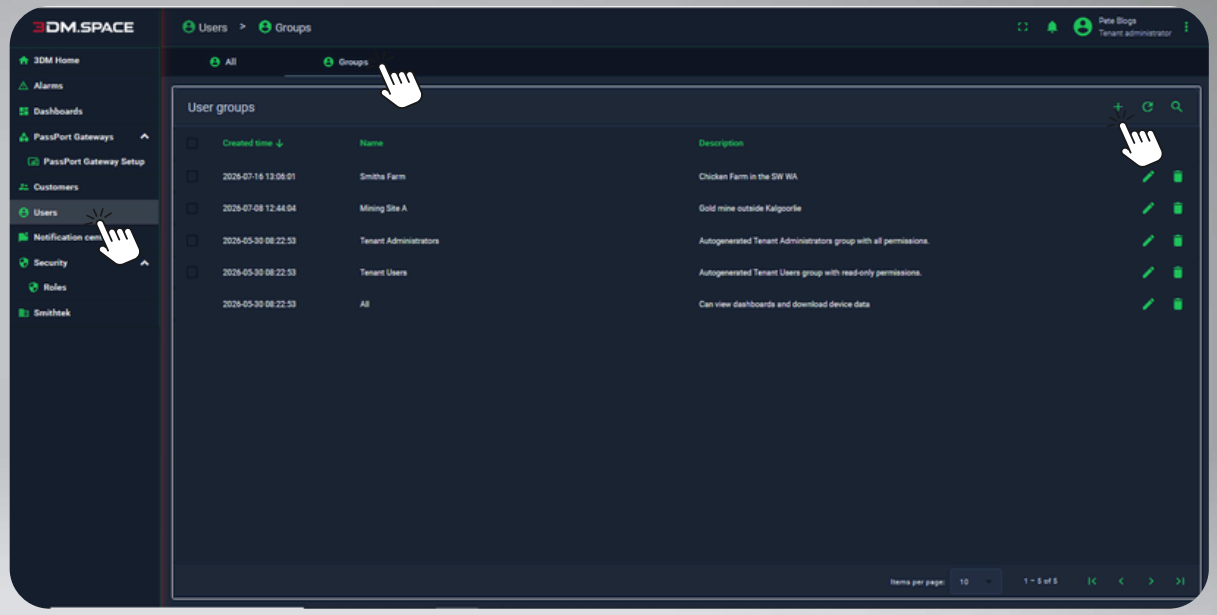
Important: Users may inherit access from every group they belong to. If someone can see or do more than expected, check their user group memberships.
In simple terms: User groups are the people boxes. They organise users and make permissions easier to control.

 © 2026 Smithtek Pty Ltd. All rights reserved.

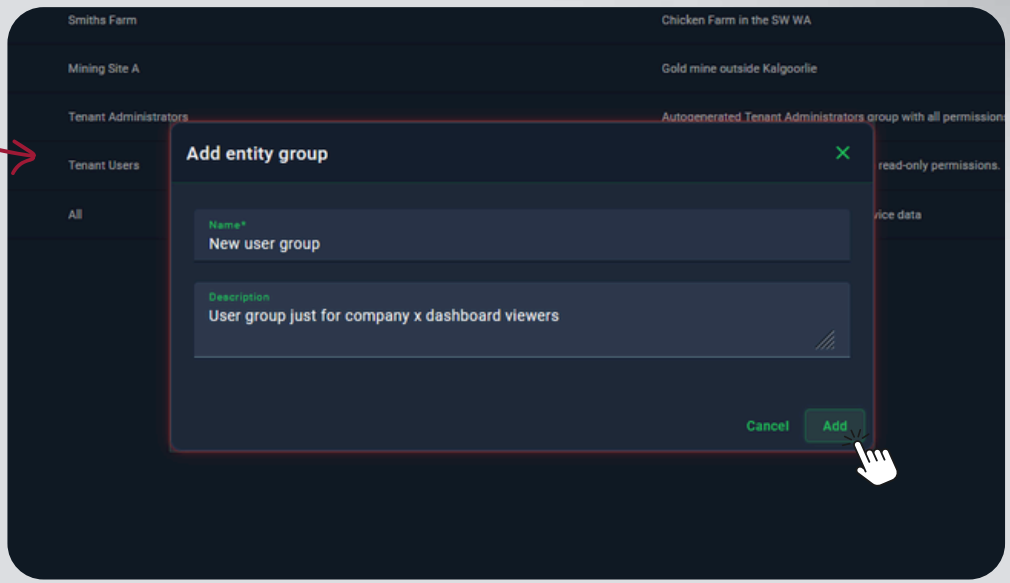
Create a User Group

Setting up a user group:

1. Go to **Users**.
2. Click **Groups.**
3. Click the **+ button** to add a **new user group.**
4. Enter a **clear group name**. **Example:** Company X Users", "Dashboard Readers", or "Field Staff".



5. Add a description if required. **Example:** "Users in this group can access company X dashboards and devices only."
6. Click **Add** or **Save**. **The new user group will now appear in the user group list**



Important:
Creating a user group does not give users access by itself.
A user group is only a container. To provide access, you must:

- **Assign the correct role to the user group.**
- **Link that role to the required dashboard, device, or resource group.**

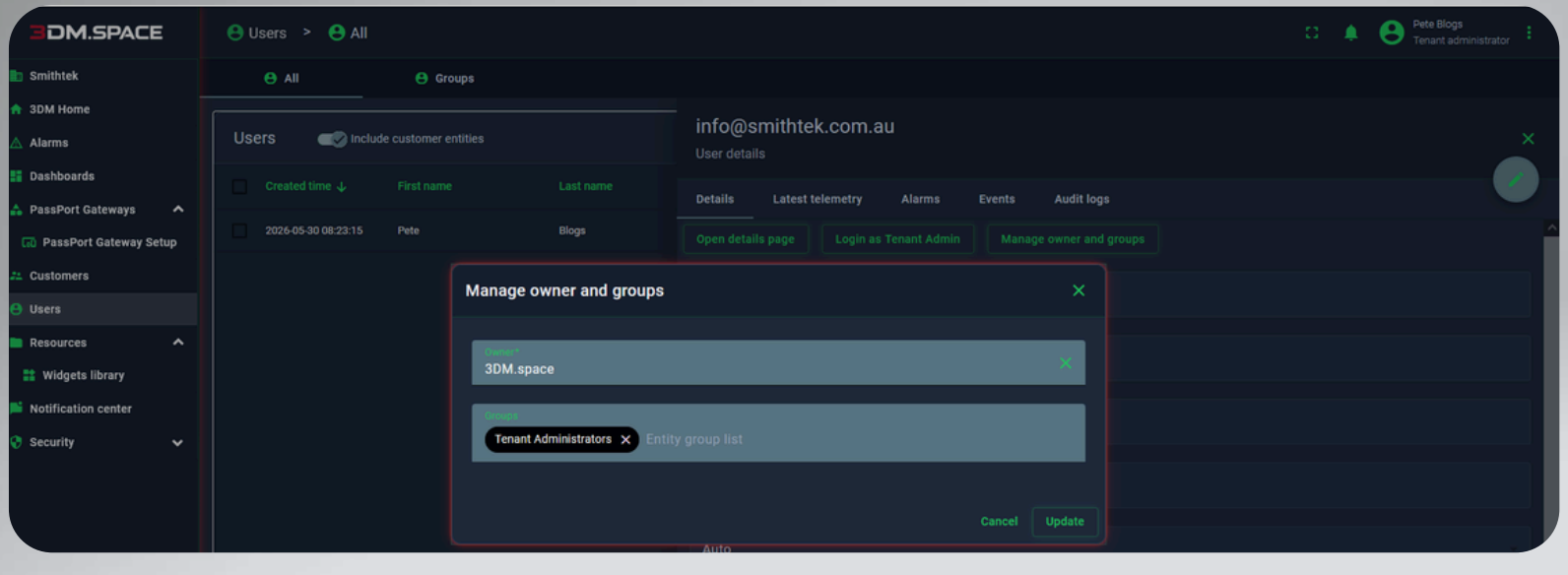
Without a role, users can be added to the group, but they will not receive any useful access.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Adding Users to a Group

Adding users to a group

Users can be added to a user group after the user account has already been created.
This is useful when a user was created from All users first, or when a user needs to be moved into a different access group later.



Steps

1. Click **Users** in the side navigation bar.
2. Click **All**.
3. Find the user you want to add to a group.
4. Click the **user** to open the user details panel.
5. Click **Manage owner and groups.**
6. The Manage owner and groups window will open.
7. Check the **Owner field.** The owner will usually default to the tenant.
8. In the Groups field, **select** the **user group** the user should belong to.
   Example: “Smiths Farm”, “Mining Site A”, or “Tenant Administrators”.
9. Remove any old group if the user should no longer belong there.
10. Click **Update.**

Important:
A user can belong to one group or multiple user groups.
If the user should only have restricted access, check the Groups field carefully and remove any broad access groups they no longer need.

Simple rule:
Users → All = find existing users
Manage owner and groups = choose where the user belongs
User group = controls the access structure for that user

 © 2026 Smithtek Pty Ltd. All rights reserved.

Adding a Role to a User Group

Adding a role to a user group

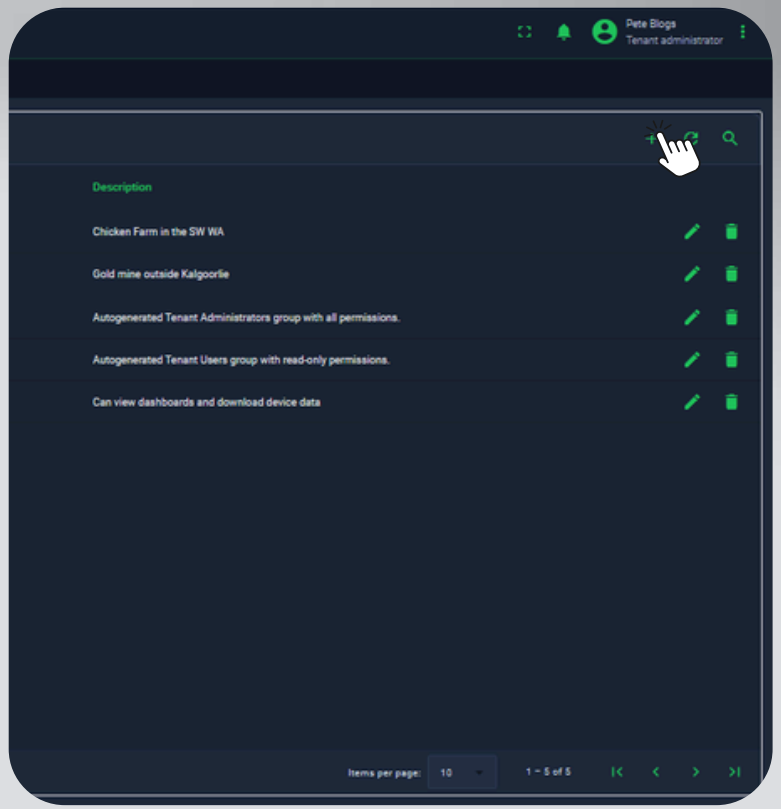
Once a user group has been created, roles can be added to control what the users in that group are allowed to do.
Roles can be added to a user group in two ways:

1. **Directly from the user group using the Roles tab.**
2. **From a dashboard group or device group using the Permissions tab.**

Both methods create the same type of connection. If a dashboard group or device group permission is added and pointed to this user group, it will also appear automatically in the user group's Roles tab. The Roles tab inside a user group shows all access currently assigned to that user group.

Add the Role from the User Group - Method 1:

1. Go to **Users**.
2. Click **Groups**.
3. Click the **user group** you want to edit. **Example:** "Company X Users".
4. Click the **Roles** tab.
5. Click the **+ button** to add a role.
6. Select the **Role type**. **Generic** is used for **broader account roles**, such as internal staff roles. **Example: "Operations Manager"**, **"Field Techs"**, or **"Dashboard Viewer"**. **Group** is used when access should only apply to a selected group, such as one dashboard group or one device group.
7. Select the **Role owner.** This is usually the **Tenant**.
8. Select the role you want to apply.
9. If using a **Generic role**, select the required generic role from the list. **Example:** "Operations Manager" or "Dashboard Viewer".
10. If using a **Group role**, select the **entity group** the role applies to. **Example:** Dashboard Group or Device Group.
11. Select the specific group. **Example:** "Company X Dashboards" or "Company X Devices".
12. Click **Save**. Repeat the process if the user group needs access to more than one group.



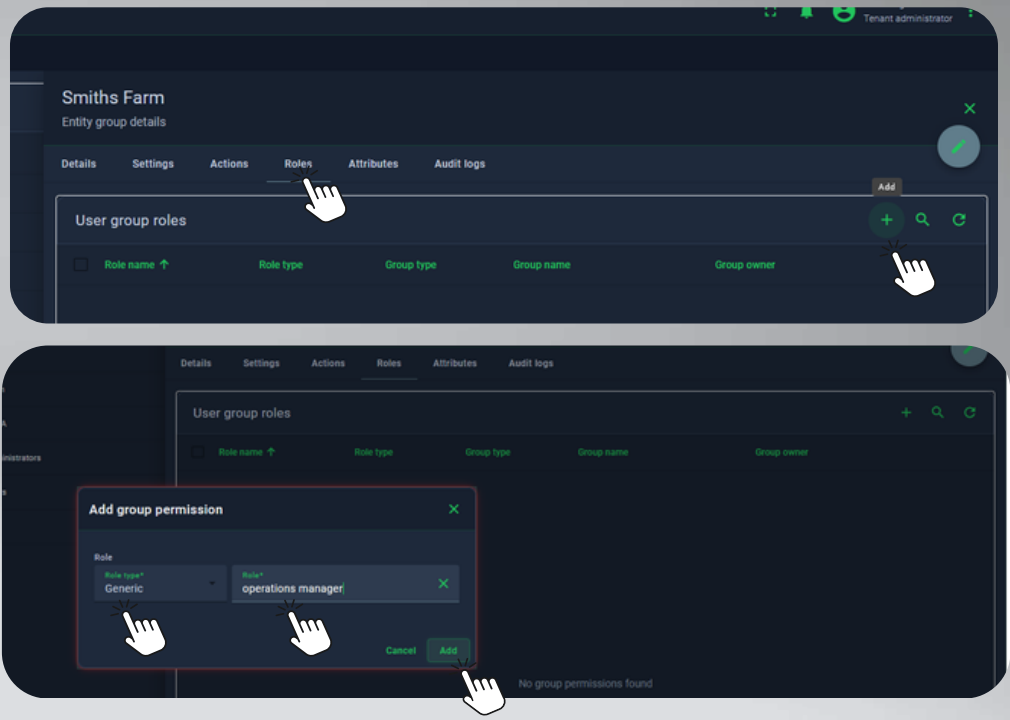
 © 2026 Smithtek Pty Ltd. All rights reserved.

Adding a Role to a User Group

Add the Role from a Dashboard Group or Device Group - Method 2:
You can also add access from the dashboard group or device group itself.
For example:

1. Go to **Dashboards → Groups or PassPort Gateways → Groups.**
2. Open the **required group. Example:** “Company X Dashboards” or “Company X Devices”.
3. Go to the **Permissions tab**.
4. Click **+** to **add a permission.**
5. Select the **role**.
6. Select the **user group** that should receive access. **Example**: “Company X Users”.
7. Click **Add** or **Save**.

This permission will then appear automatically inside the user group’s Roles tab.

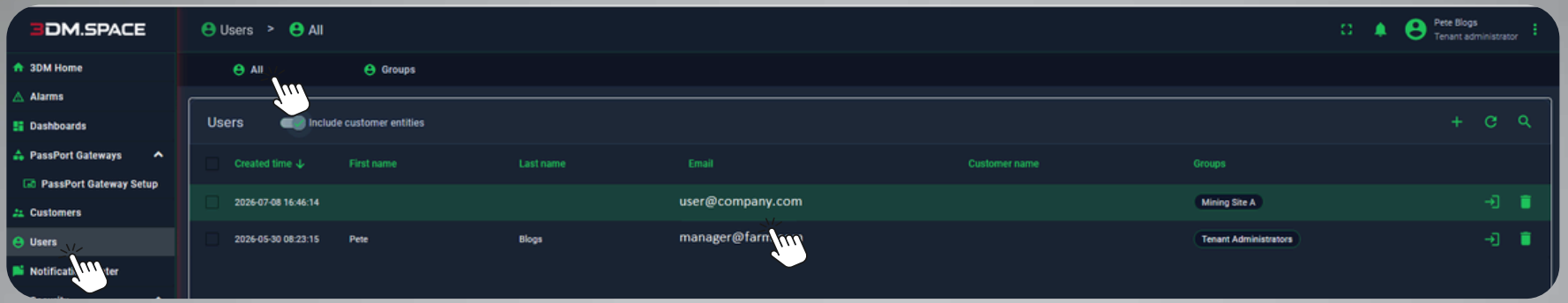


Important:
A Generic role gives broader access across the account. These are normally used for trusted internal users.
A Group role only applies to the selected group it is attached to. This is best for restricted access, such as one client, one site, or one project. When adding a Group role, you may see other entity group types listed. For most standard setups, you will normally use Dashboard Group and Device Group. Other options may be used for advanced setup or future platform features. For dashboards to work properly, users often need both: **Dashboard group access and Device group access.** If a user can open a dashboard but the data does not show, check that the user group also has access to the related device group

Simple rule:
User group = who gets access
Role = what they can do
Dashboard group or device group = where they can do it

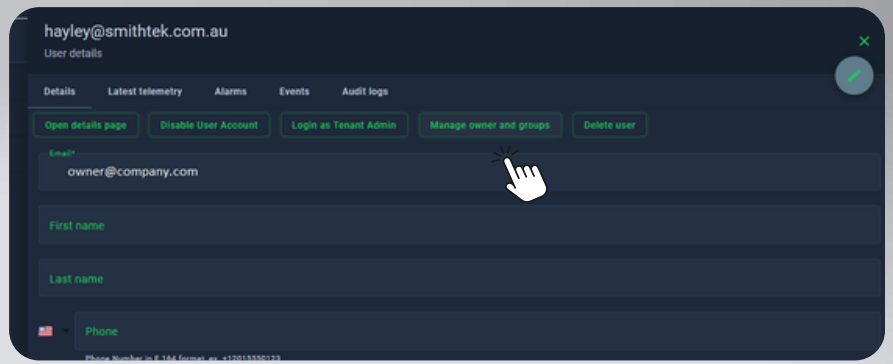
 © 2026 Smithtek Pty Ltd. All rights reserved.

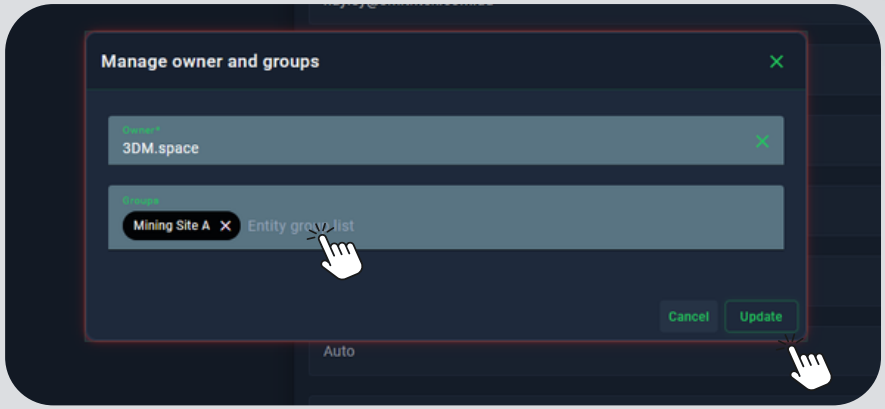
Moving Users Between Groups



Moving Users Between Groups:
Users can be moved from one user group to another when their access needs to change.

1. Go to **Users**.
2. Click **All.**
3. Click the **user** you want to update.
4. Open **Manage owner and groups.**
5. In the **Groups** field, remove the current group if the user should no longer belong to it.
6. Select the **new user group.** **Example:** change from “Dashboard Readers” to “Operation Field Staff”.
7. Click **Update** or **Save**.
8. Test the user account to confirm their access has changed correctly.





Important:
A user can belong to more than one user group. Only remove the old group if the user should no longer receive access from that group. If a user can still see too much after being moved, **check whether they are still inside another broad-access group** such as **“All”**, **“Tenant Administrators”**, or another group with wider permissions.

 © 2026 Smithtek Pty Ltd. All rights reserved.

User Group Property Settings

Details tab

The Details tab shows the basic information for the user group.

Name

This is the name of the user group. Use a clear name that explains who belongs in the group. **Example:** “Smiths Farm”, “Company X Users”, or “Dashboard Readers”.

Description

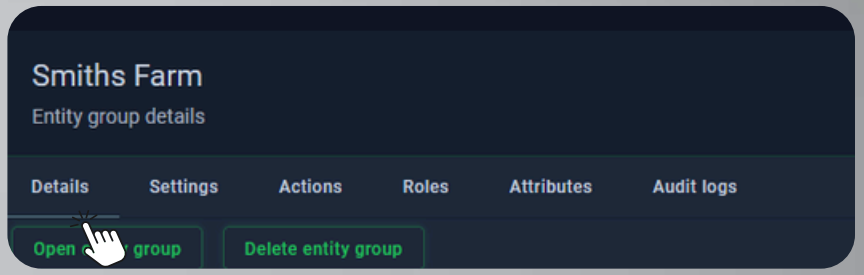
This is an optional note explaining what the group is used for. **Example:** “Chicken Farm in the SW WA” or “Users in this group can access Company X dashboards only.”

Open entity group

This opens the full group page.

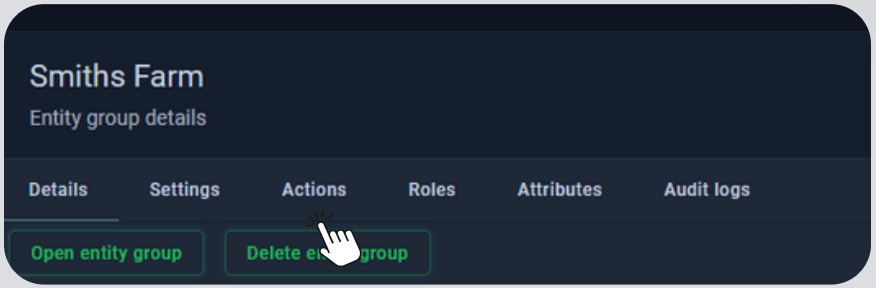
Delete entity group

This deletes the group. Only use this if the group is no longer needed. Deleting a group may affect users or permissions connected to that group.



Actions tab

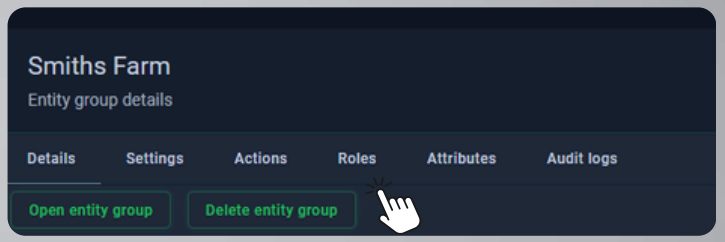
The Actions tab is not normally used during standard user group setup. It may be used for advanced platform actions or future features. Most administrators can leave this section unchanged unless instructed by Smithtek support.



 © 2026 Smithtek Pty Ltd. All rights reserved.

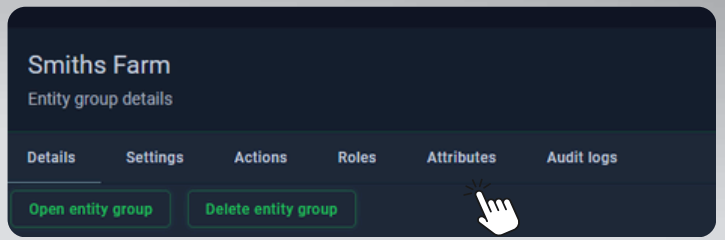
3DM User Group Property Settings

Roles tab
The Roles tab shows which roles are assigned to the user group. This is an important tab because it controls what the users in the group can do. A user group without roles is mostly just a container. Users may be inside the group, but they will not receive useful access until the correct role has been added. Use this tab to check which roles are connected to the group.

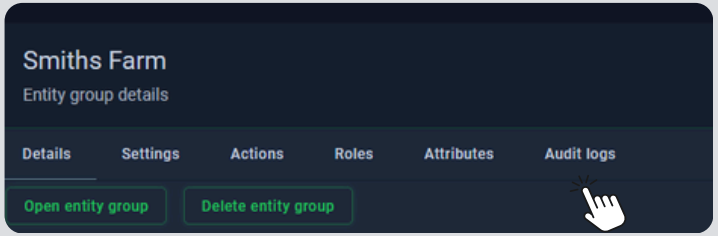


Attributes tab
Client attributes are sent from the device to 3DM.Space.
These may be used when a PassPort Gateway or connected system reports configuration or device-side information.

Server attributes are stored inside 3DM.Space.
These are values kept on the platform side and can be used for internal settings, labels, configuration, or system information.



Shared attributes are stored in 3DM.Space but can be sent down to the device.
These are commonly used when the platform needs to send configuration or control-related values to a PassPort Gateway.



Audit logs tab
The Audit logs tab records changes and activity related to the group. It can be useful for checking who changed something, when a group was edited, or when permissions were updated. Most users will not need this tab during normal setup, but administrators may use it for troubleshooting.

 © 2026 Smithtek Pty Ltd. All rights reserved.

User Group Entity Details

Settings tab
The Settings tab controls how the group list behaves when viewing items inside the group.

Group table title
This allows you to set a custom title for the group table. If left blank, the default group title is used.

Enable entities search
Allows users to search within the group list.

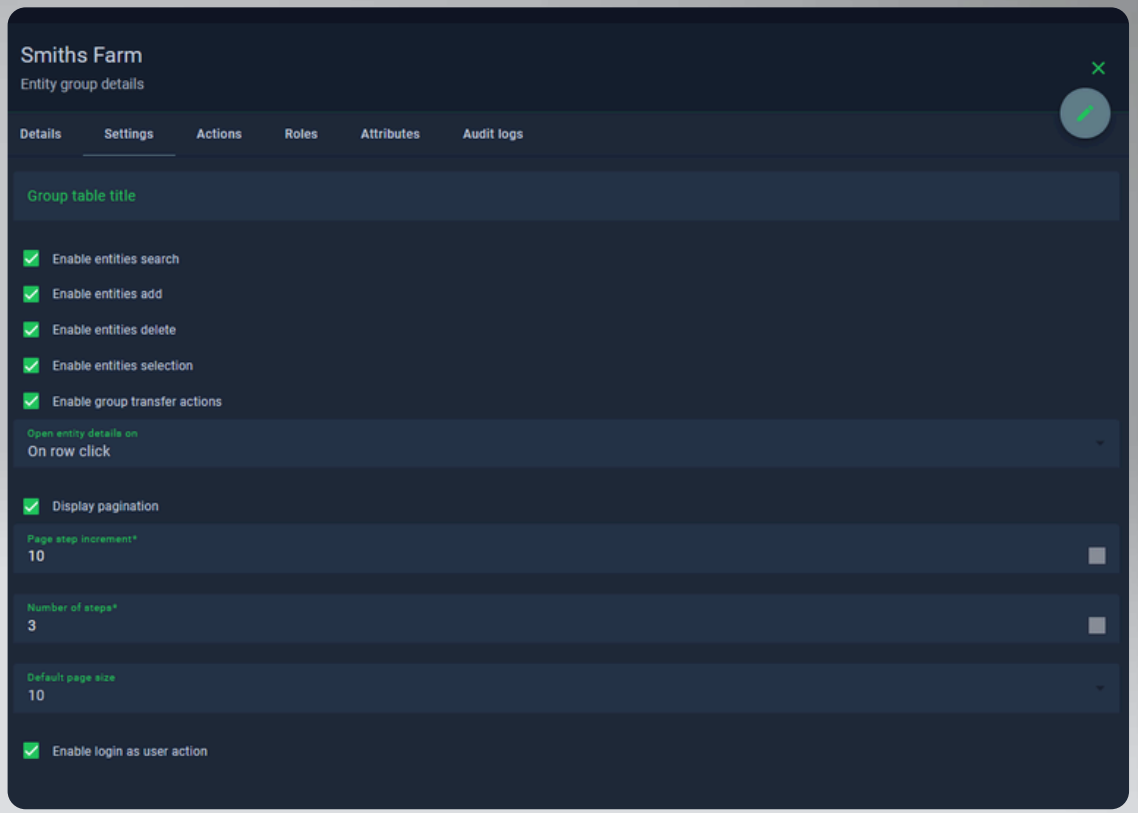
Enable entities add
Allows users with the correct permissions to add items into the group.

Enable entities delete
Allows users with the correct permissions to delete or remove items from the group.

Enable entities selection
Allows users to select items in the group list.

Enable group transfer actions
Allows users with the correct permissions to move or transfer items between groups.

Open entity details on
Controls how item details open. ***Example:*** *"On row click" means the item opens when the user clicks the row.*



 © 2026 Smithtek Pty Ltd. All rights reserved.

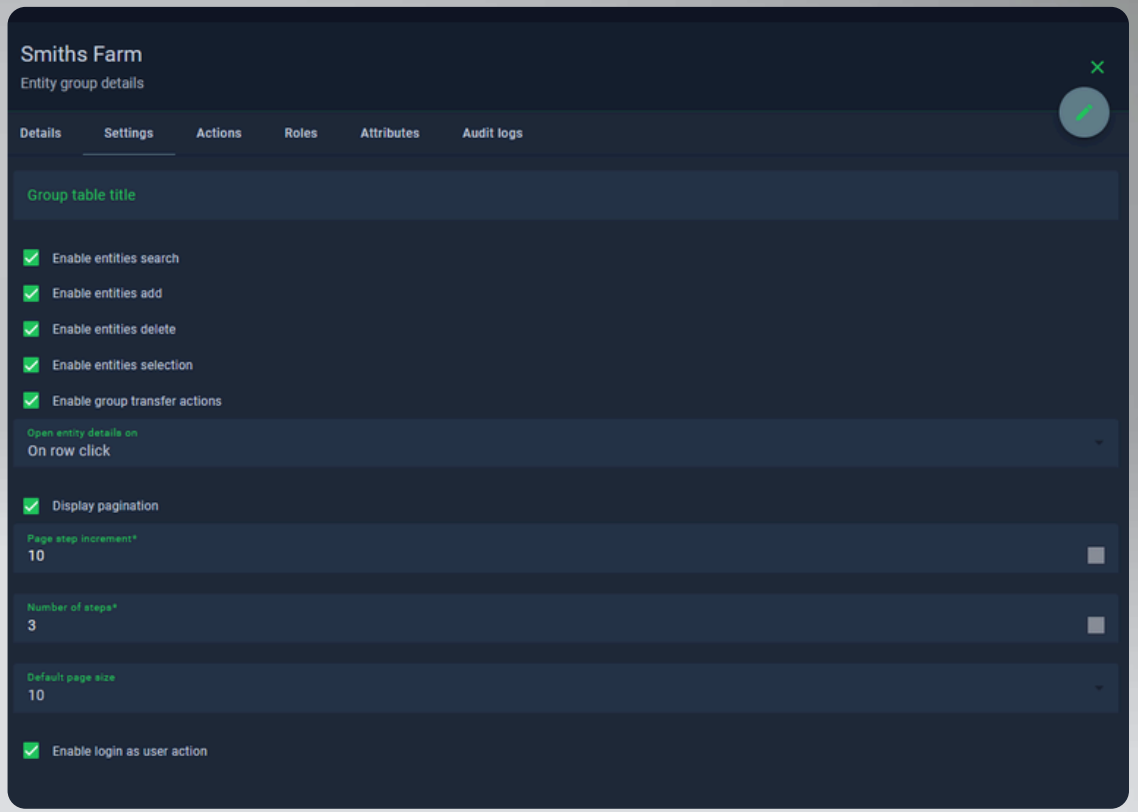
Display pagination
Shows page controls when there are lots of items in the group.

Page step increment
Controls how many extra rows are added when changing page size options.

Number of steps
Controls how many page size options are available.

Default page size
Controls how many items are shown per page. **Example:** 10 means 10 users are shown before pagination is used.

Enable login as user action
Allows an authorised administrator to log in as a user from this group. This is useful for testing user access, but should only be available to trusted administrators.



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Groups

Dashboard groups organise dashboards by **site**, **company**, **project**, **department**, **system type**, or **access level**. They keep accounts tidy and make dashboard access easier to manage.

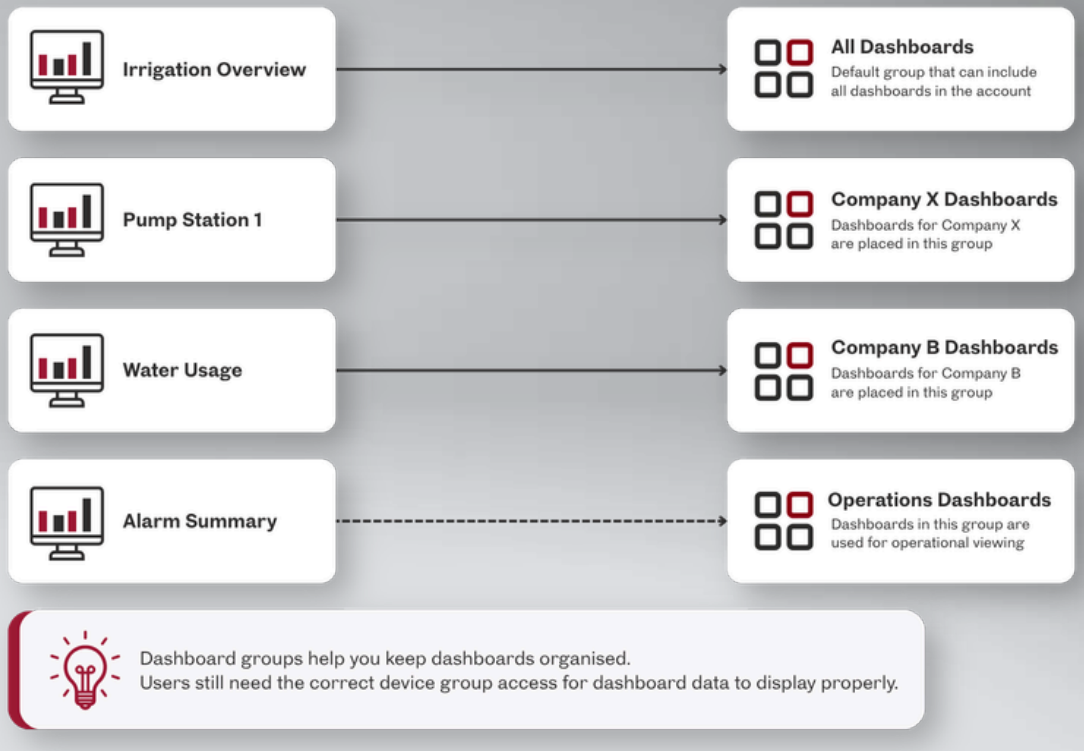
Administrators can:

- **Create new dashboards directly inside a dashboard group.**
- **Move existing dashboards into a group later.**
- **Use groups such as Company X Dashboards, Irrigation Dashboards, Pump Station Dashboards, or Dashboard Readers Only.**

Access control

Instead of assigning dashboards to users individually:

1. Place dashboards into the correct dashboard group.
2. Give the appropriate user group permission to access that dashboard group.

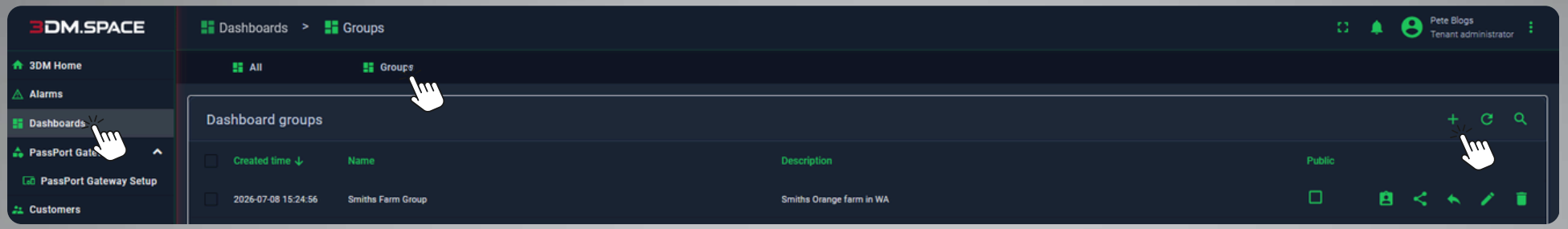


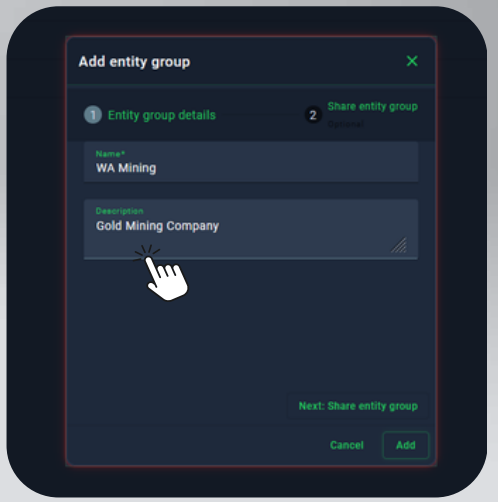
Important:

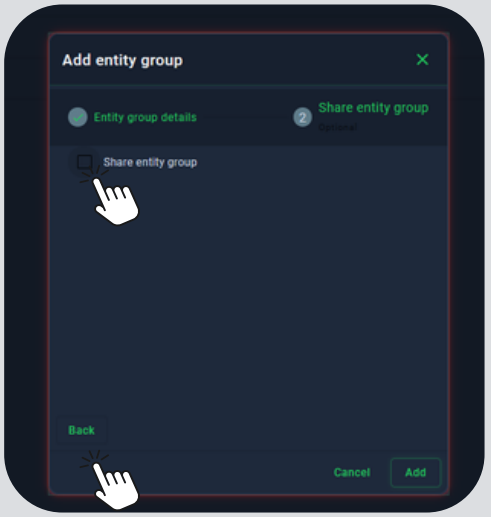
Dashboard access does not automatically provide access to the device data used by the dashboard. If a dashboard uses data from a PassPort Gateway or another device, the user must also have access to the related device group. If device access is missing, the dashboard may open but some widgets may show no data. In simple terms: Dashboard groups are the dashboard boxes. They organise dashboards and help control who can see them.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a Dashboard Group







Steps

1. Go to **Dashboards**.
2. Click **Groups**.
3. Click the **+ button** to add a **new dashboard group**.
4. Enter a **clear group name**. **Example:** “Company X Dashboards”, “Pump Station Dashboards”, or “Irrigation Dashboards”.
5. Add a description if required. **Example:** “Dashboards for Company X site monitoring.”
6. Check the **Share entity group** option.
7. Share entity group can be used to give a user group access to the dashboard group during setup. This can also be done later from the dashboard group **Permissions tab**.
8. For this basic setup, leave Share entity group unticked and add permissions later.
9. To check that **Share entity group** is **unticked**, click the Share entity group tab.
10. **Make sure the Share entity group checkbox is unticked**.
11. Click **Back** to return to the main setup page.
12. Click **Add**. **The new dashboard group will now appear in the dashboard group list.**

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a Dashboard Group

Important:
Creating a dashboard group does not automatically give users access to it. The dashboard group is only a container until dashboards are added and permissions are applied. To let users see dashboards inside this group, you must give the correct user group access to the dashboard group using the correct role.

Permissions can be added in two ways:

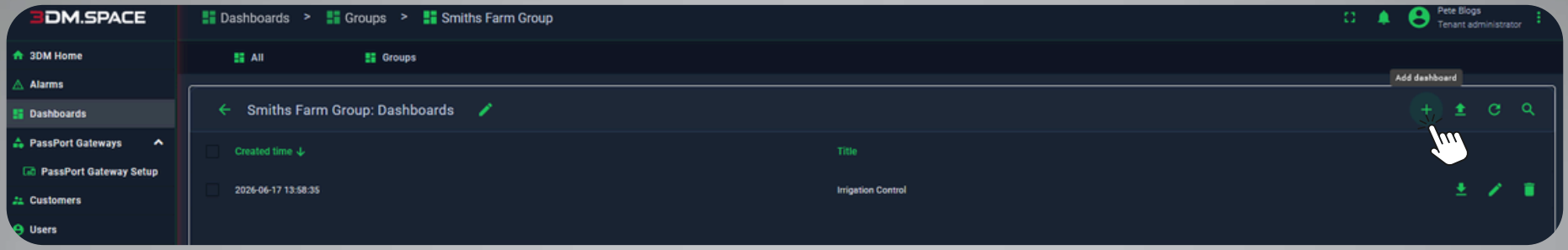
1. During setup using **Share entity group**
2. Later using the **dashboard group Permissions tab.**

Both methods create the same type of access link. Once added, the permission will also appear inside the selected user group under the Roles tab. Also remember that dashboard access does not always mean dashboard data will display. If the dashboard uses live data from a PassPort Gateway, users may also need access to the related device group.

Simple rule:
Dashboard group = where dashboards are stored
User group = who needs access
Role = what they can do
Device group = where the live data comes from

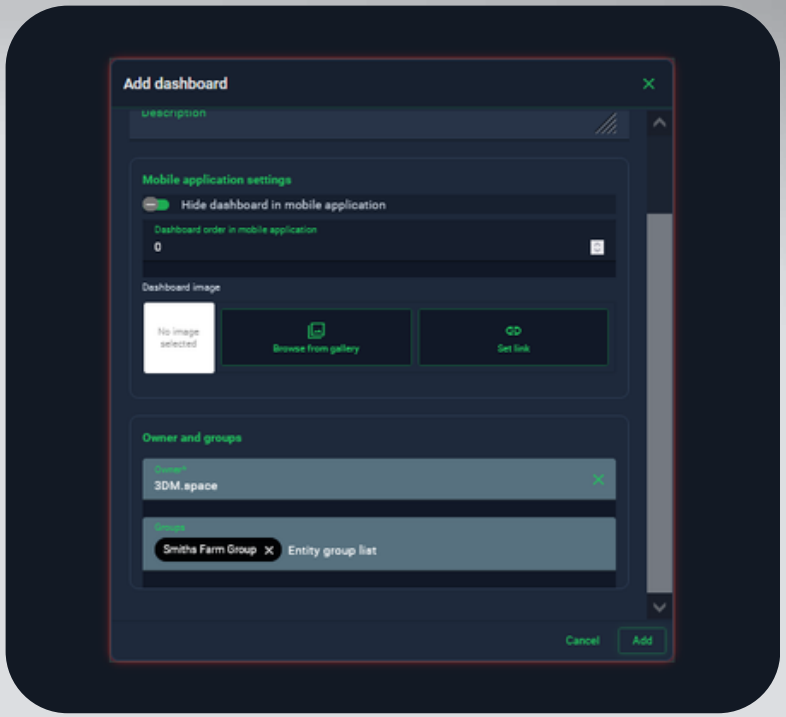
 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a Dashboard Group



Steps

1. Go to **Dashboards**.
2. Click **Groups**.
3. Open the **dashboard group** where the new dashboard should be created. **Example:** “Company X Dashboards” or “Smiths Farm Group”.
4. Click the **+ button** to add a **new dashboard**.
5. Enter a clear **dashboard name**. **Example:** “Smiths Farm Overview”, “Pump Station Dashboard”, or “Irrigation Monitoring”.
6. Add a description if required. **Example:** “Main dashboard for Smiths Farm site monitoring.”
7. **Upload** or **select** a dashboard image if required. This is optional and can be left blank.
8. **Check** the **Owner** and **groups** section. The **Owner** will usually default to the tenant.
9. The **Groups** field should automatically show the dashboard group you created the dashboard from.
10. If required, you can remove the selected dashboard group and choose a different dashboard group instead.
11. Click **Add** or **Save**. **The new dashboard will now be created inside the selected dashboard group.**



 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a Dashboard Group

Important:
When a dashboard is created from inside a dashboard group, the group is normally selected automatically in the Owner and groups section. This can be changed before saving if the dashboard needs to belong to a different group.
Creating a dashboard inside a group keeps the dashboard organised from the start. This is useful when setting up a new site, company, project, or system.

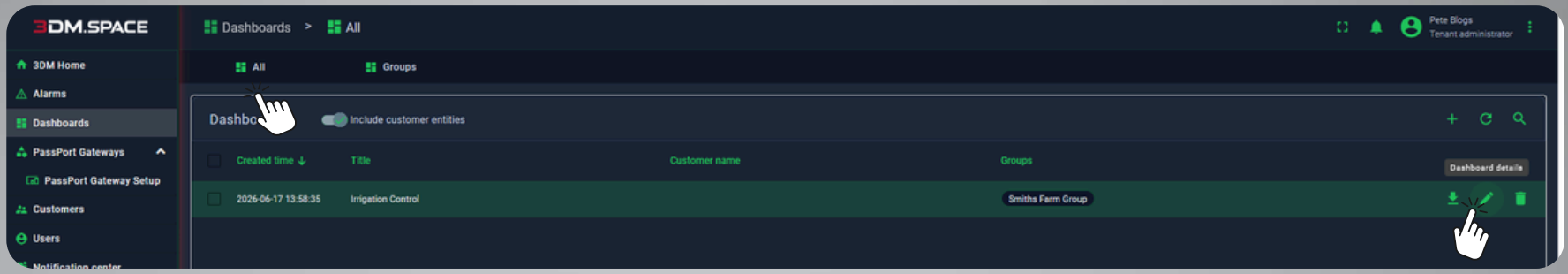
A dashboard created inside a group still needs the correct permissions before users can access it.

If the dashboard uses live data from a PassPort Gateway, users may also need access to the related device group for the data to display correctly.

Simple rule:
Create dashboard inside group = best for new dashboards
Move dashboard into group = best for dashboards that already exist

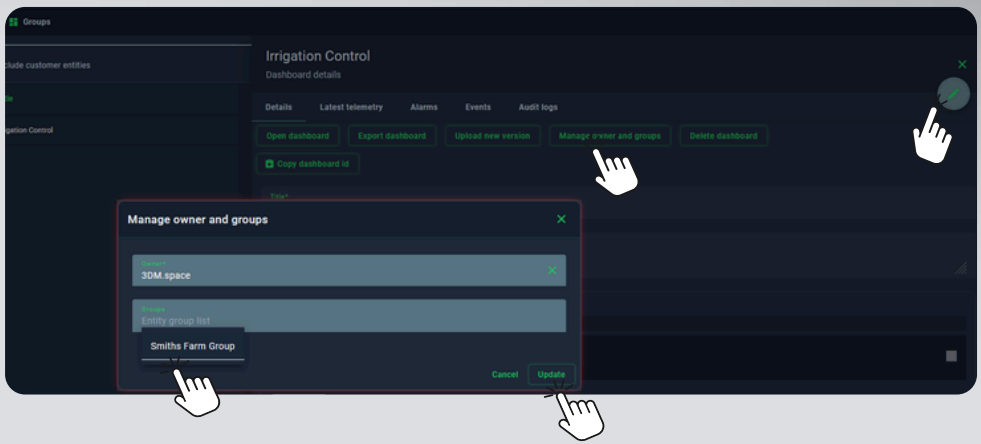
 © 2026 Smithtek Pty Ltd. All rights reserved.

Moving a Dashboard into the Group



Steps

1. Go to **Dashboards** in the side navigation bar.
2. Click **All**.
3. The full dashboard list will open.
4. This table shows all dashboards in the account. It also shows which group or groups each dashboard belongs to.
5. **Find** the **dashboard** you want to move into a group. **Example:** “Irrigation Control”, “Smiths Farm Overview”, or “Pump Station Dashboard”.
6. Click the **dashboard** to open its **details panel**.
7. Click **Manage owner and groups**.
8. Check the **Owner field**. The owner will usually be **3DM.Space** or the **tenant owner**.
9. In the **Groups field**, select the **dashboard group** you want to move the dashboard into. **Example:** “Smiths Farm Group”, “Company X Dashboards”, or “Irrigation Dashboards”.
10. Remove any old group if the dashboard should no longer belong there.
11. Click **Update**. **The dashboard will now appear inside the selected dashboard group.**



 © 2026 Smithtek Pty Ltd. All rights reserved.

Moving a Dashboard into the Group

Important:
A dashboard can belong to one group or multiple dashboard groups. If the dashboard should only be available in one group, check the Groups field carefully and remove any groups it no longer needs to belong to. Use this method when the dashboard already exists and needs to be placed into the correct dashboard group.

Simple rule:
Dashboards → All = find existing dashboards
Manage owner and groups = choose where the dashboard belongs
Dashboard group = where dashboards are organised

A dashboard created inside a group still needs the correct permissions before users can access it.
If the dashboard uses live data from a PassPort Gateway, users may also need access to the related device group for the data to display correctly.

Simple rule:
Create dashboard inside group = best for new dashboards
Move dashboard into group = best for dashboards that already exist

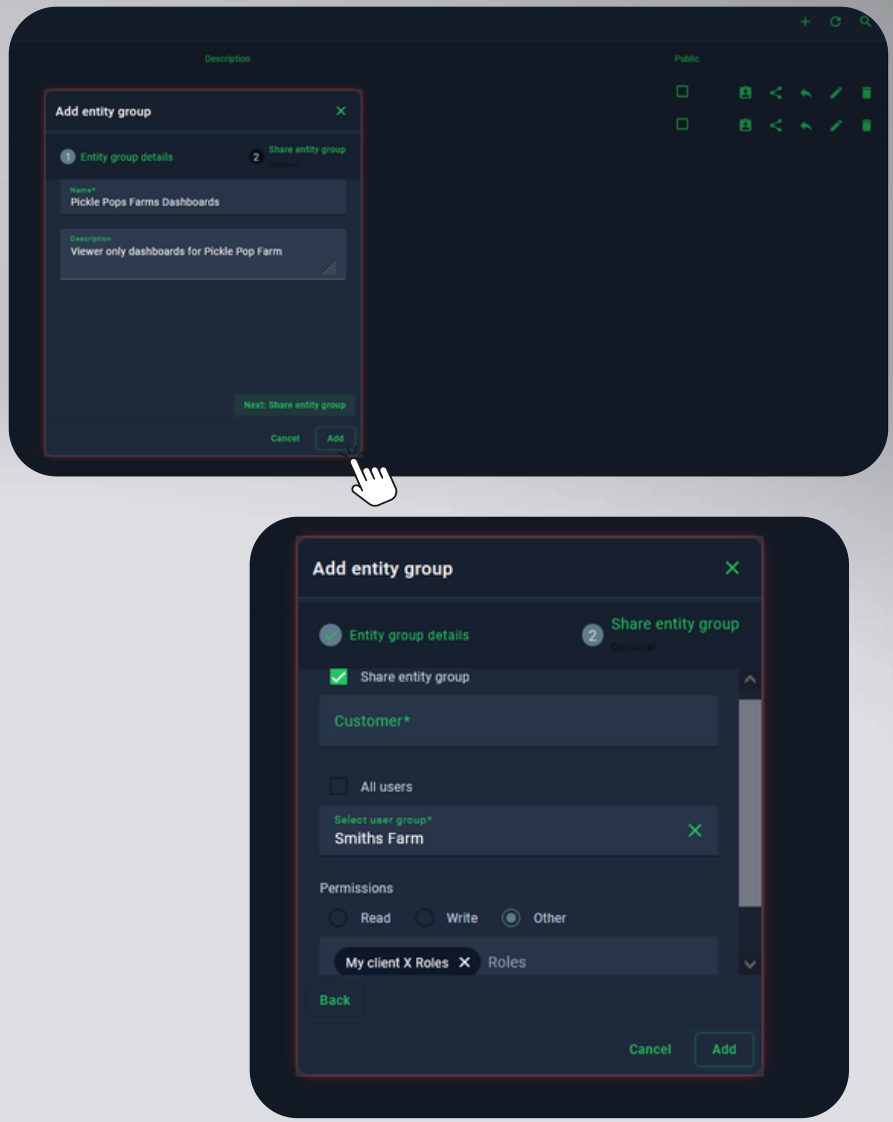
 © 2026 Smithtek Pty Ltd. All rights reserved.

Giving users access to a dashboard group

Dashboard group access controls which user groups can see the dashboards inside a dashboard group. There are two main ways to give users access to a dashboard group:

Option 1: Use Share entity group
Option 2: Use the Permissions tab

Both options create the same type of access link. Once access has been added, it will appear inside the dashboard group Permissions tab.



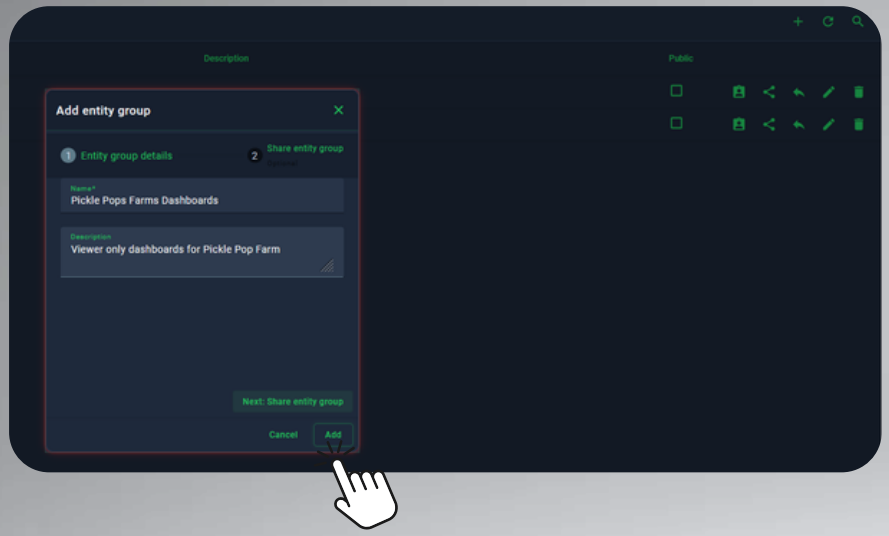
Option 1: Using Share entity group

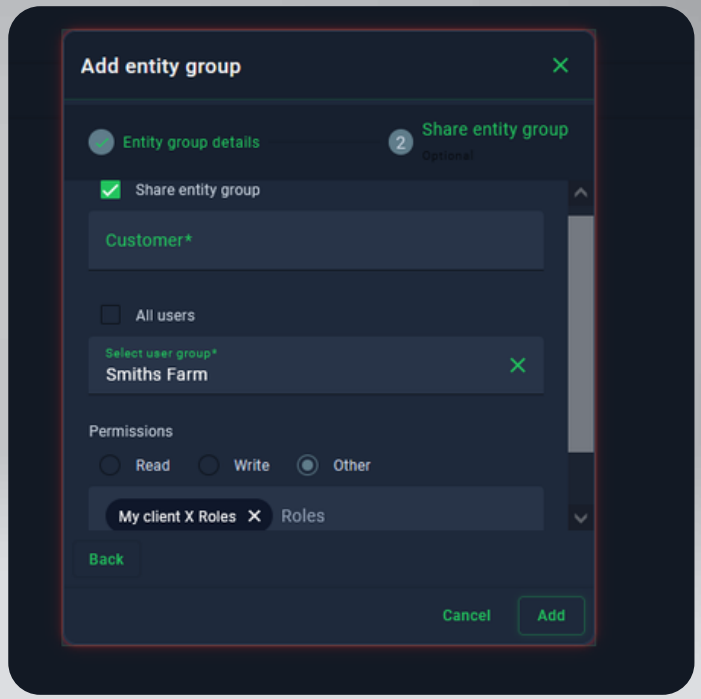
The Share entity group option can be used while creating the dashboard group, or later from the dashboard group list.

During dashboard group creation

1. Go to **Dashboards**.
2. Click **Groups.**
3. Click the **+ button** to add a new dashboard group.
4. Enter the **group name** and **description**.
5. Click Next: **Share entity group**.
6. Tick **Share entity group**.
7. Select the **Customer** or **owner** if required.
8. Select the **user group** that should receive access. **Example:** “Smiths Farm”.
9. Choose the **permission type**:
10. **Read** gives **basic** viewing access.
11. **Write** gives **broader** editing or write access.
12. **Other** allows you to select a **specific role** that was created earlier.
13. If using **Other**, **select the required role**.
14. Click **Add. The dashboard group will be created, and the selected user group will have access to it.**

 © 2026 Smithtek Pty Ltd. All rights reserved.





After the dashboard group has been created:

1. Go to **Dashboards**.
2. Click **Groups**.
3. **Find** the **dashboard group** in the list.
4. Click the **Share entity group** icon.
5. Complete the same sharing details as above.
6. Click **Share**. **The access link will then appear inside the dashboard group Permissions tab.**

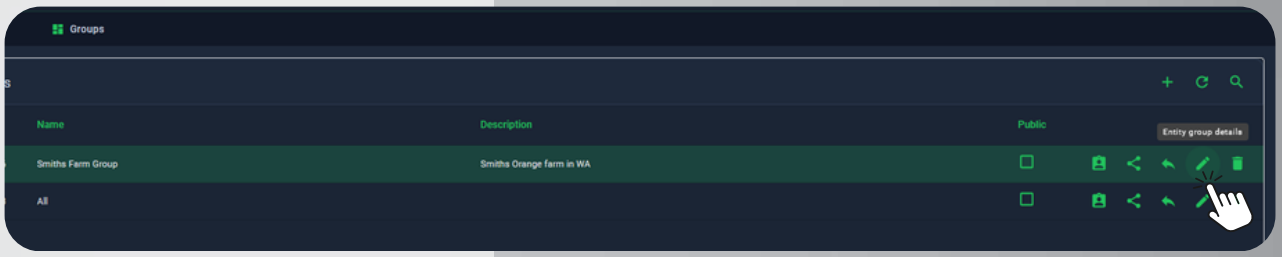
 © 2026 Smithtek Pty Ltd. All rights reserved.

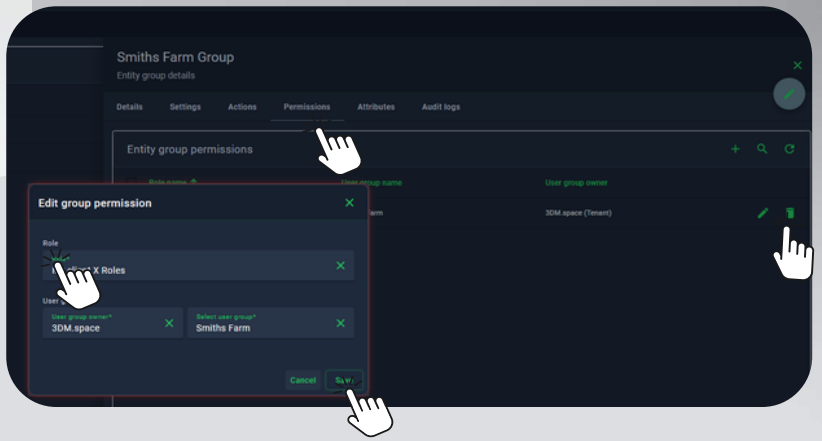
Option 2: Using the Permissions tab

The Permissions tab shows all access that has already been added to the dashboard group. It can also be used to add a new permission, edit an existing permission, or remove access.

Steps

1. Go to **Dashboards**.
2. Click **Groups**.
3. Open the **dashboard group**.
4. Click the **pencil/edit** icon.
5. Click the **Permissions tab**.
6. Click the **+ button** to add a new permission.
7. Select the **Role**.
8. Select the **User group** owner.
9. Select the **user group** that should receive access.
10. Click **Add**.





Important:

Be careful with **All users**. This gives access to every user in the account. For client, site, project, or private dashboards, and select the correct user group instead. Dashboard group access lets the user open the dashboards inside the group. If the dashboard uses live data from a PassPort Gateway, the user may also need access to the related device group.

Simple rule:

Share entity group = quick way to give access
Permissions tab = view, add, edit, or remove access
All users = everyone gets access
Selected user group = only that group gets access

 © 2026 Smithtek Pty Ltd. All rights reserved.

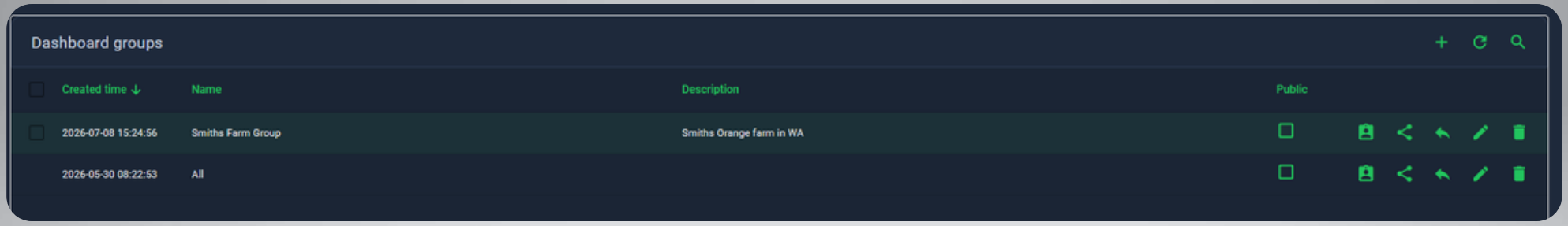
Dashboard Group Table Properties

Dashboard group table property settings

Dashboard group table property settings are managed from the Dashboard Groups list.

To access this area, go to **Dashboards**, then click **Groups**.

This page shows all dashboard groups in the account and provides quick action buttons for **creating groups**, **refreshing the list**, **searching for groups**, **checking public status**, **sharing access**, **opening groups**, **editing groups**, and **deleting groups**.



Dashboard group row options

From left to right, the dashboard group row icons are:

Public status square

Shows whether the dashboard group is public.

If the square is ticked, the dashboard group has been made public.

Share entity group

This is a quick way to set permissions and roles for the dashboard group. Use this to give a user group access to the dashboard group without opening the full group settings. This opens the same type of access setup discussed in the Giving users access section.

Make public

This makes the dashboard group public. Use this carefully, as public access can allow dashboards to be viewed outside normal logged-in access.

Open group

The backward arrow opens the dashboard group and shows the dashboards inside that group in the next table. This does not open the settings page.

Edit group details

The pencil icon opens the Entity group details area.

Use this to edit the dashboard group name, description, and group details.

Delete group

The trash can deletes the dashboard group. Use this carefully, as deleting the group may affect how dashboards are organised and accessed.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Dashboard Group Table Properties

Dashboard group table options

Add group

The + icon is used to add a new dashboard group.

Refresh

The refresh icon reloads the dashboard group list.

Use this if a group has just been added or changed and the list needs to update.

Search

The magnifying glass icon is used to search the dashboard group list.

Use this to quickly find a dashboard group when there are multiple groups in the account.

Important:

Dashboard group access is important because it controls which users can open dashboards inside that group.

If a user cannot see a dashboard, check that the user group has permission to access the related dashboard group.

Be careful with public settings. Making a dashboard group public can allow dashboards to be viewed outside normal logged-in access. If the dashboard uses live data from a PassPort Gateway, the related device group may also need the correct access or public settings for the data to display properly.

 © 2026 Smithtek Pty Ltd. All rights reserved.

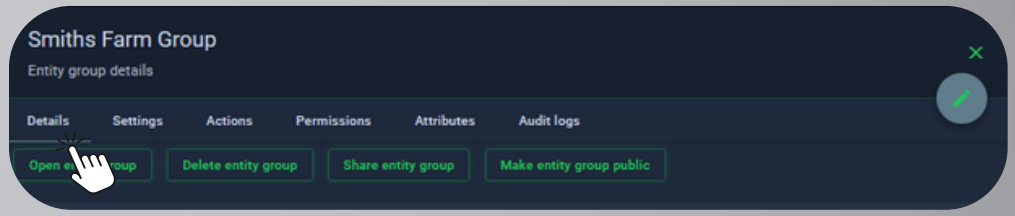
Dashboard group settings

Details tab

The Details tab shows the basic information for the dashboard group.

Name

This is the name of the dashboard group. Use a clear name that explains what dashboards belong in the group. **Example:** “Smiths Farm Group”, “Company X Dashboards”, or “Pump Station Dashboards”.



Description

This is an optional note explaining what the dashboard group is used for. **Example:** “Dashboards for Smiths Farm site monitoring” or “Dashboards for Company X only.”

Open entity group

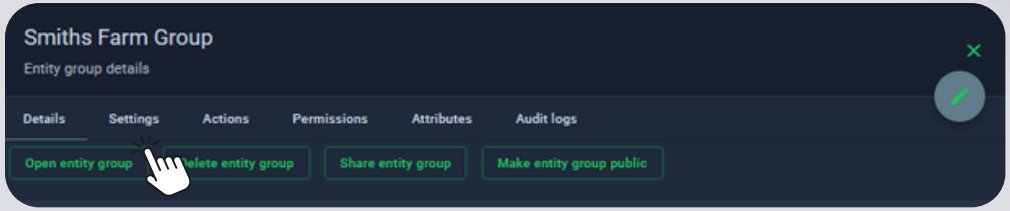
This opens the full dashboard group page.

Delete entity group

This deletes the dashboard group. Only use this if the group is no longer needed. Deleting a group may affect dashboards or permissions connected to that group.

Settings tab

The Settings tab controls how the dashboard group list behaves and displays. In most standard setups, these settings do not need to be changed. The default settings are normally suitable. Administrators may use this section to adjust how dashboards are displayed inside the group, such as list behaviour, searching, selection, pagination, or opening dashboard details. For a basic setup, leave this section unchanged unless there is a specific reason to adjust it.



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Group Property Settings

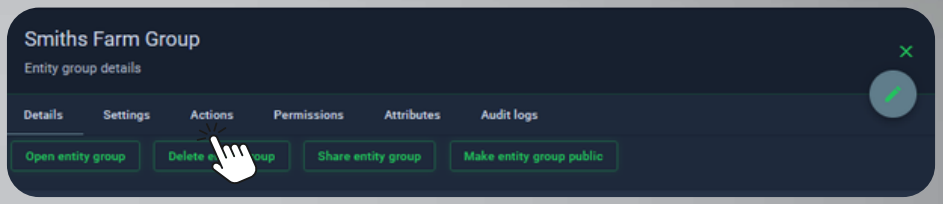
Actions tab

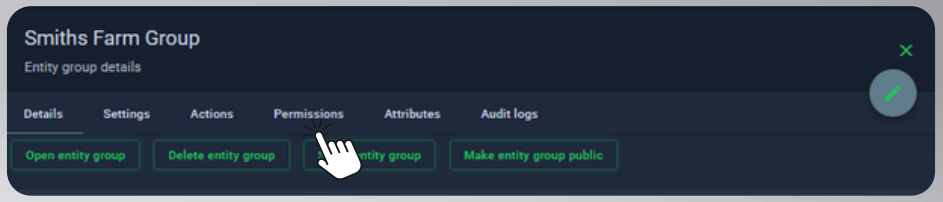
The Actions tab is used for group-related actions and advanced configuration. The Actions tab is not normally used during standard dashboard group setup. It may be used for advanced platform actions or future features. Most administrators can leave this section unchanged unless instructed by Smithtek support.

Permissions tab

The Permissions tab shows which user groups have access to the dashboard group. This is an important tab because it controls who can access dashboards inside the group. A dashboard group without permissions is mostly just a container. Dashboards may be inside the group, but users will not receive access until the correct permission has been added. Use this tab to check which user groups are connected to the dashboard group and which role is being used.

Example: The Smiths Farm user group may be given a dashboard role for the Smiths Farm Group dashboard group.





Attributes tab

Client attributes are sent from the device to 3DM.Space.

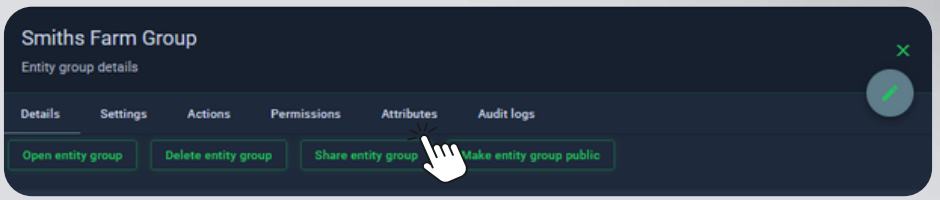
These may be used when a PassPort Gateway or connected system reports configuration or device-side information.

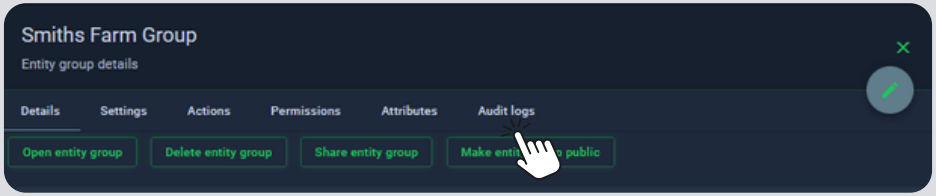
Server attributes are stored inside 3DM.Space.

These are values kept on the platform side and can be used for internal settings, labels, configuration, or system information.

Shared attributes are stored in 3DM.Space but can be sent down to the device.

These are commonly used when the platform needs to send configuration or control-related values to a PassPort Gateway.





Audit logs tab

The Audit logs tab records changes and activity related to the dashboard group. It can be useful for checking who changed something, when a group was edited, or when permissions were updated. Most users will not need this tab during normal setup, but administrators may use it for troubleshooting.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Settings tab

The Settings tab controls how the group list behaves when viewing items inside the group.

Group table title
This allows you to set a custom title for the group table. If left blank, the default group title is used.

Enable entities search
Allows users to search within the group list.

Enable entities add
Allows users with the correct permissions to add items into the group.

Enable entities delete
Allows users with the correct permissions to delete or remove items from the group.

Enable entities selection
Allows users to select items in the group list.

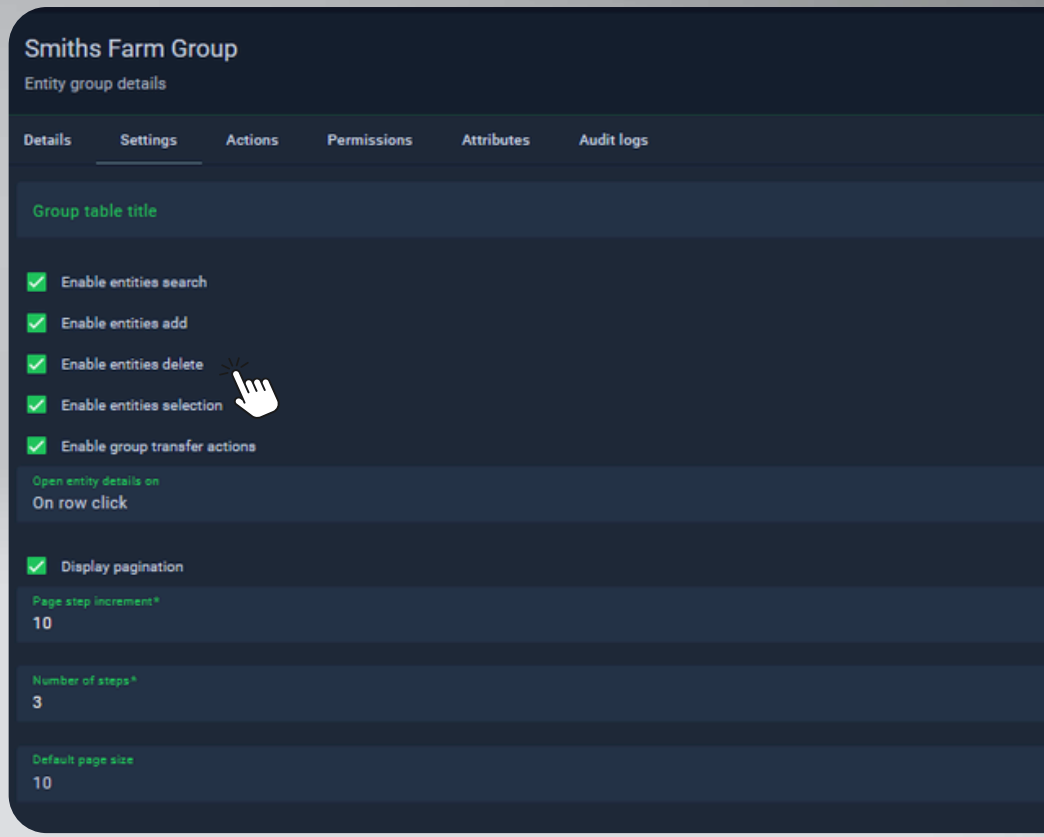
Enable group transfer actions
Allows users with the correct permissions to move or transfer items between groups.

Open entity details on
Controls how item details open. **Example:** “On row click” means the item opens when the user clicks the row.

Display pagination
Shows page controls when there are lots of items in the group.

Page step increment
Controls how many extra rows are added when changing page size options.

Number of steps
Controls how many page size options are available.

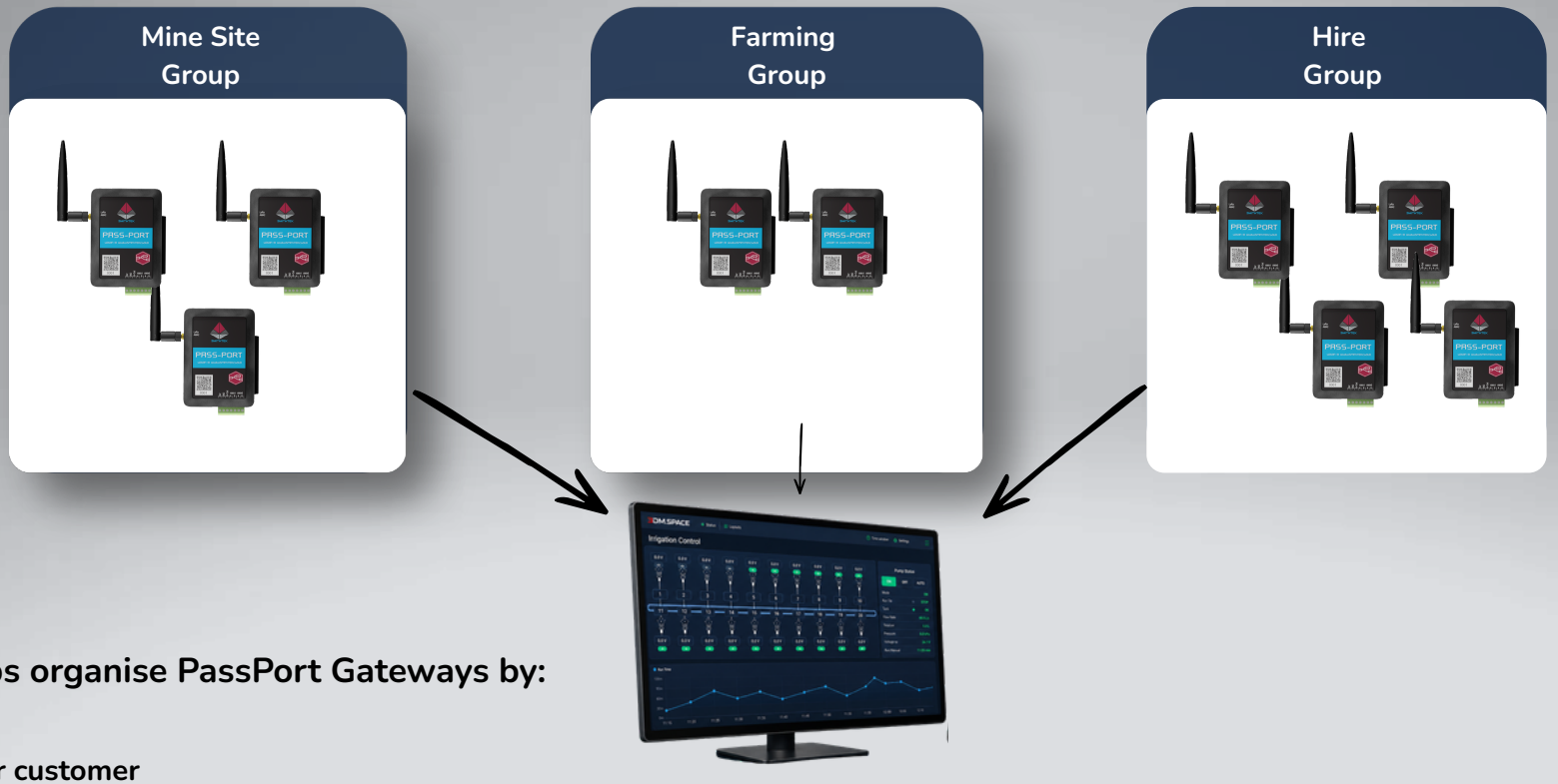


Default page size
Controls how many items are shown per page. **Example:** 10 means 10 users are shown before pagination is used.

Enable login as user action
Allows an authorised administrator to log in as a user from this group. This is useful for testing user access, but should only be available to trusted administrators.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Groups



Device groups organise PassPort Gateways by:

- **Site**
- **Company or customer**
- **Project or department**
- **System type**
- **Access level**

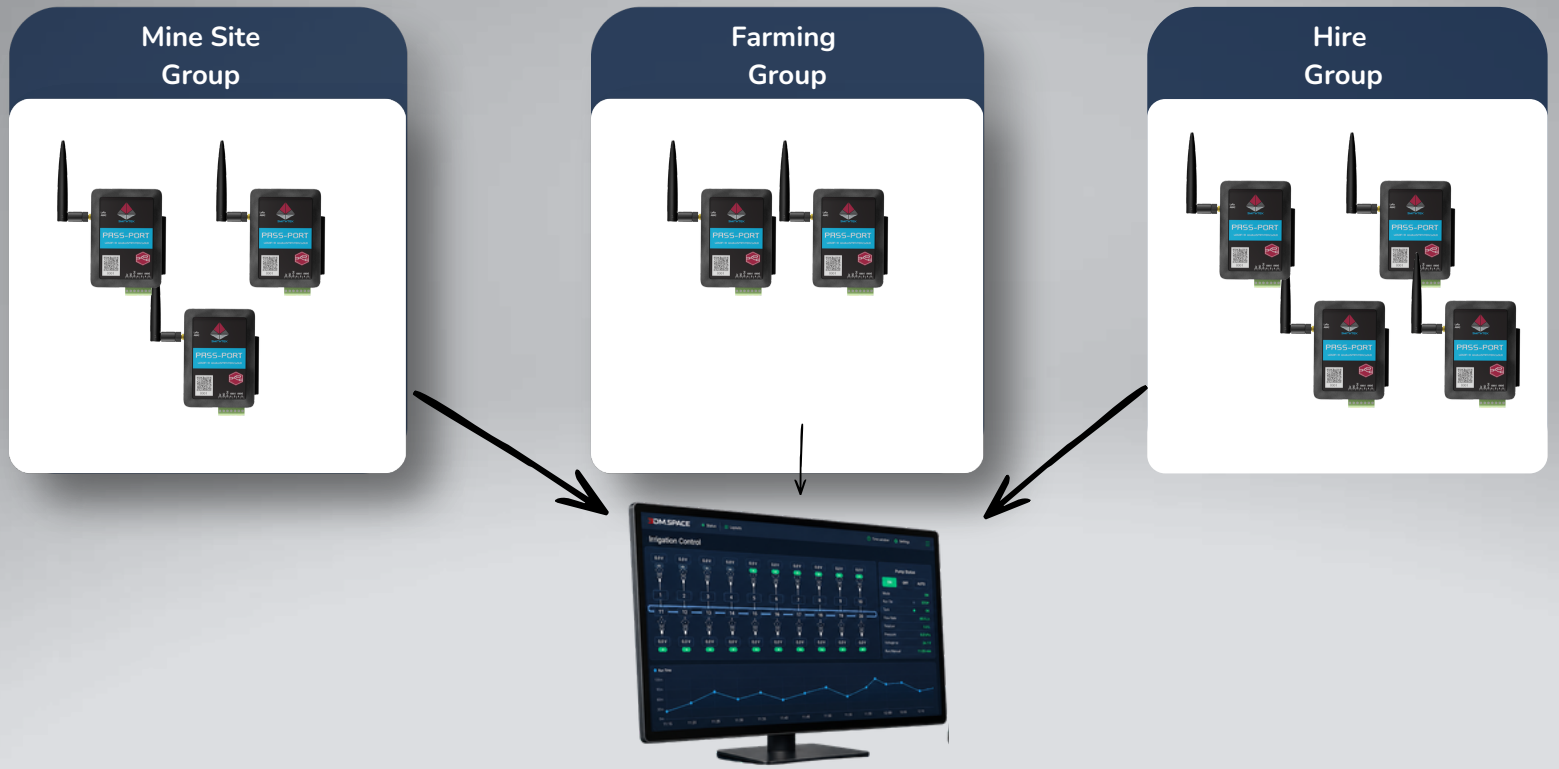
In 3DM.Space, a device normally means a PassPort Gateway. Field equipment such as Mako PLCs, Solaris RTUs, pumps, tanks, valves, sensors and controllers communicates through the PassPort and is not grouped individually.
Managing PassPorts

Administrators can:

- Create new PassPort Gateways directly inside a device group.
- Move existing PassPort Gateways into a group later.
- Use groups such as Smiths Farm Devices, Mining Company, Pump Station Devices or Irrigation PassPorts.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Groups



Access control

Device groups also control who can access the PassPort Gateway and its data.

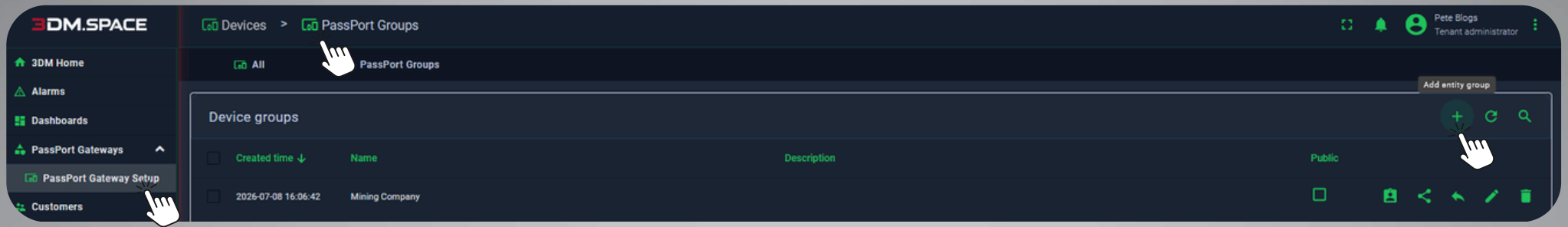
1. **Place PassPort Gateways into the correct device group.**
2. **Give the appropriate user group access to that device group.**

Important:
A user may be able to open a dashboard but still see no live data if they do not have access to the related PassPort Gateway device group.

Simple rule:
Device groups are the PassPort Gateway boxes. They organise PassPorts and control access to their data.

 © 2026 Smithtek Pty Ltd. All rights reserved.

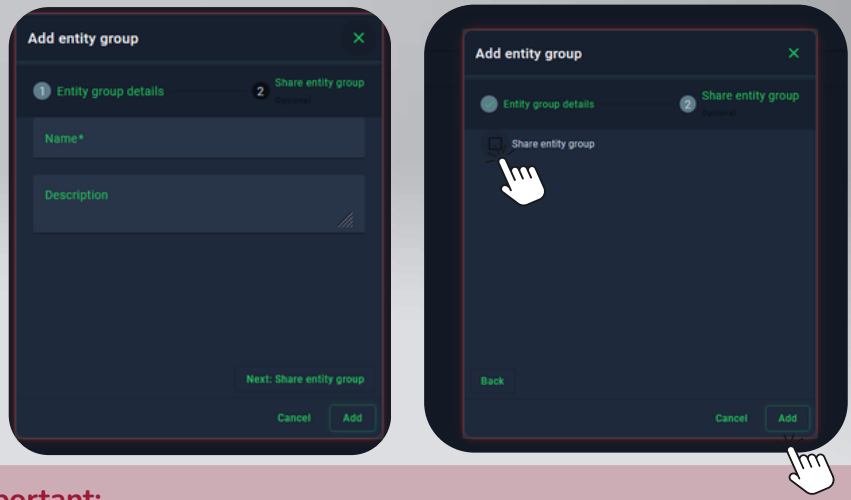
3DM Creating Device Groups



Creating a device group

Steps

1. Go to **PassPort Gateway Setup** in the side navigation bar.
2. Click **PassPort Groups**.
3. Click the **+ button** to add a new device group.
4. The **Add entity group** window will open.
5. Enter a clear group name. **Example:** “Company X Devices”, “Pump Station Devices”, or “Irrigation Devices”.
6. Add a description if required. **Example:** “PassPort Gateways for Company X site monitoring.”
7. Check the **Share entity group** option. Share entity group can be used to give a user group access to the device group during setup. This can also be done later from the device group Permissions tab. For this basic setup, **leave Share entity group unticked** and add permissions later.
8. To check that Share entity group is unticked, click the Share entity group tab.
9. **Make sure the Share entity group checkbox is unticked**.
10. Click **Back** to return to the main setup page.
11. Click **Add**. **The new device group will now appear in the device group list.**



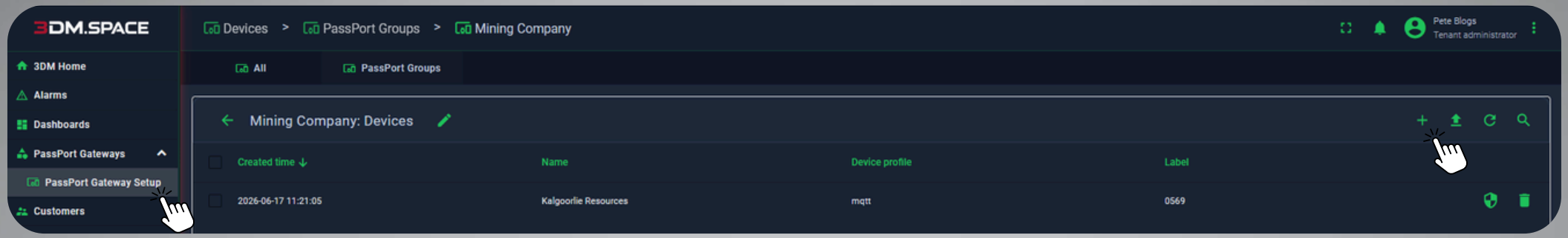
Important:
Creating a device group does not automatically add PassPort Gateways or give users access. To make the group active:

- Add the required PassPort Gateways.
- Give the correct user group access using the appropriate role.

Dashboard access alone may not be enough. If a dashboard uses live PassPort data, users must also have access to the related device group.

Simple rule:
Device group = where PassPort Gateways are stored
User group = who needs access
Role = what they can do
Dashboard group = where the dashboard is stored

Creating a Device Inside a Group



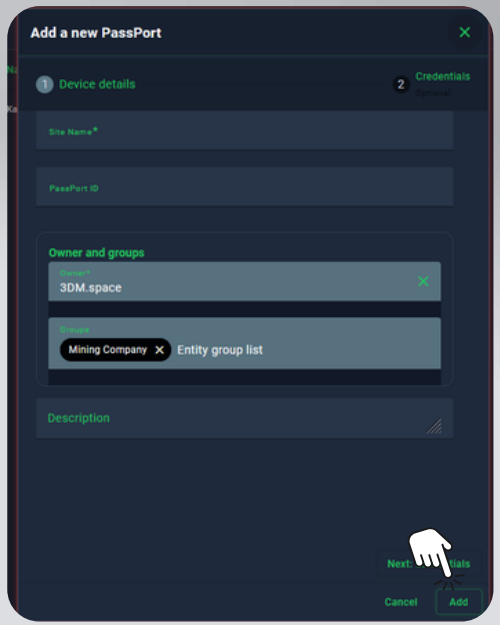
Creating a device inside a device group

Creating a device inside a device group is useful when the device group already exists and the new PassPort Gateway should belong to that group straight away.

This method keeps the PassPort Gateway organised from the start.

Steps

1. Go to **PassPort Gateway Setup** in the side navigation bar.
2. Click **PassPort Groups.**
3. Open the **device group** where the new PassPort Gateway should be created. **Example:** “Mining Company”.
4. Click the **+ button** to add a new device.
5. The **Add a new PassPort** window will open.
6. Enter a clear Site Name. **Example:** “Kalgoorlie Resources”, “Pump Station 1”, or “Smiths Farm Bore”.
7. **Enter a PassPort ID.**
8. This can be used as an internal reference, site number, gateway number, or asset ID.
9. **Check the Owner and groups section.**
10. The **Owner** will usually default to the tenant.
11. The **Groups field** should automatically show the device group you created the device from. **Example:** “Mining Company”.



12. If required, you can remove the selected device group and choose a different device group instead.
13. **Add a description if required. Example:** “PassPort Gateway installed at main pump station.”
14. Click **Next: Credentials.**
15. Add the device credentials if they are ready.
16. Click **Add. The new PassPort Gateway will now be created inside the selected device group.**

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a Device Inside a Group

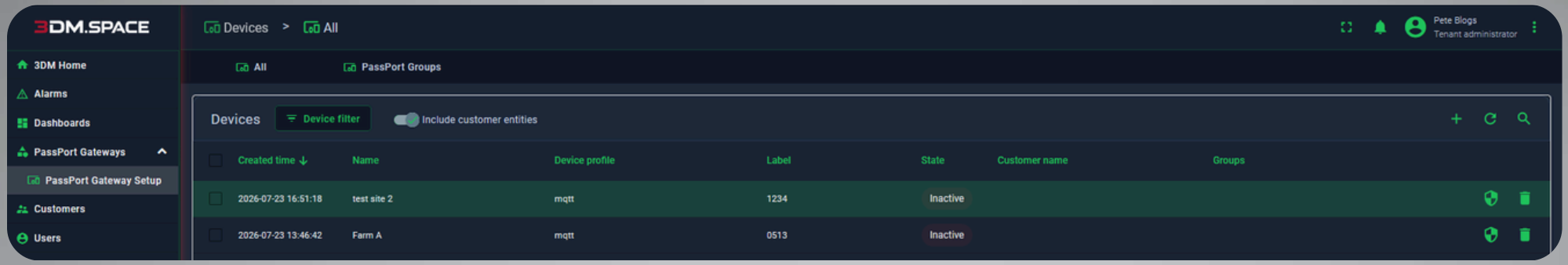
Credentials note
Credentials can be added during device setup or added later from the device list.
To add credentials during setup, **click Next: Credentials**, then **select PassPort secret credentials**. This will show the credential fields for Client ID, username, and password. These credentials can be entered manually or created using the automatic generator. **The same credentials must be entered into the PassPort Gateway Node-RED 3DM node**.

Important:
When a device is created from inside a device group, the group is normally selected automatically in the Owner and groups section. This can be changed before clicking Add if the PassPort Gateway needs to belong to a different group.

Simple rule:
Create device inside group = best for new PassPort Gateways
Move device into group = best for PassPort Gateways that already exist.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Moving a Device into a Group

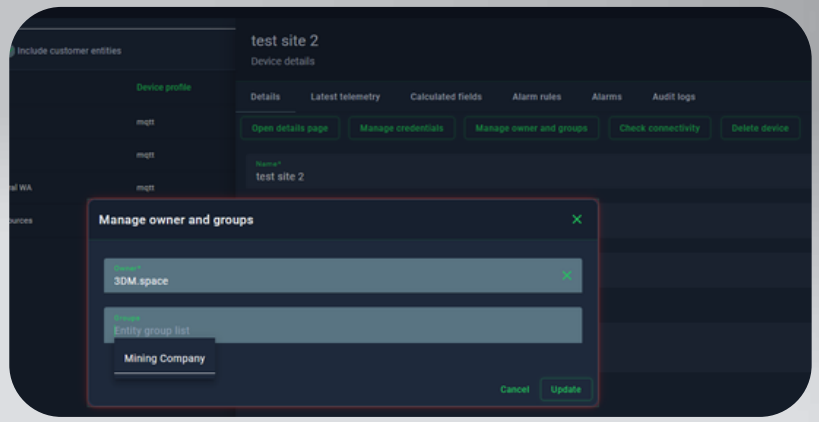


Moving a device into a device group

Use this method when a PassPort Gateway already exists and needs to be placed into the correct device group.

Steps

1. Go to **PassPort Gateway Setup** in the side navigation bar.
2. Click **All**.
3. The full device list will open. This table shows all PassPort Gateways in the account. It also shows which group or groups each device belongs to.
4. **Find** the **device** you want to move into a group**. Example:** “test site 2” or “Kalgoorlie Resources”.
5. **Click** the **device** to open its details panel.
6. Click **Manage** owner and groups.
7. The **Manage owner and groups** window will open.
8. Check the **Owner** field. The owner will usually be 3DM.Space or the tenant owner.
9. In the **Groups field**, select the device group you want to move the device into. Example: “Mining Company”.
10. **Remove** any **old group** if the device should no longer belong there.
11. Click **Update**. **The device will now appear inside the selected device group.**



Important:
A device can belong to one group or multiple device groups. If the device should only be available in one group, check the Groups field carefully and remove any groups it no longer needs to belong to. Use this method when the PassPort Gateway already exists and needs to be placed into the correct device group.

Simple rule:
PassPort Gateway Setup → All = find existing devices
Manage owner and groups = choose where the device belongs
Device group = where PassPort Gateways are organised

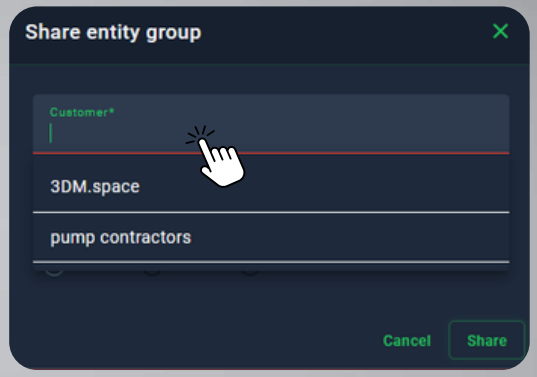
 © 2026 Smithtek Pty Ltd. All rights reserved.

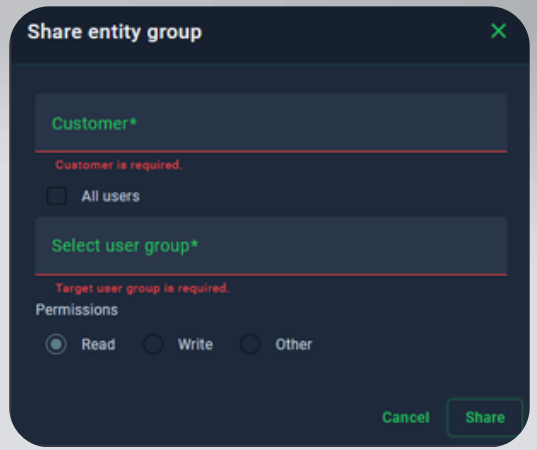
Giving users access to a device group

Device group access controls which user groups can access the PassPort Gateways inside a device group. There are two main ways to give users access to a device group:

Option 1: Use Share entity group
Option 2: Use the Permissions tab

Both options create the same type of access link. Once access has been added, it will appear inside the device group Permissions tab.





Option 1: Using Share entity group

The Share entity group option can be used while creating the device group, or later from the device group list.

During device group creation

1. Go to **PassPort Gateway Setup**.
2. Click **PassPort Groups**.
3. Click the **+ button** to add a **new device group**.
4. Enter the **group name** and description.
5. Click **Next**: **Share entity group**.
6. Tick **Share entity group**.
7. Select the Customer or owner if required.
8. Select the **user group** that should receive access. **Example:** “Smiths Farm” or “Mining Site A”.
9. Choose the **permission type**:
10. **Read** gives **basic viewing access**.
11. **Write** gives **broader editing** or write access.
12. **Other** allows you to select a **specific role** that was created earlier.
13. If using Other, select the required role.
14. Click **Add**. **The device group will be created, and the selected user group will have access to it.**

After the device group has been created

1. Go to **PassPort Gateway Setup**.
2. Click **PassPort Groups**.
3. **Find** the **device group** in the list.
4. Click the **Share entity group** icon.
5. Complete the same sharing details as above.
6. Click **Share**. **The access link will then appear inside the device group Permissions tab.**

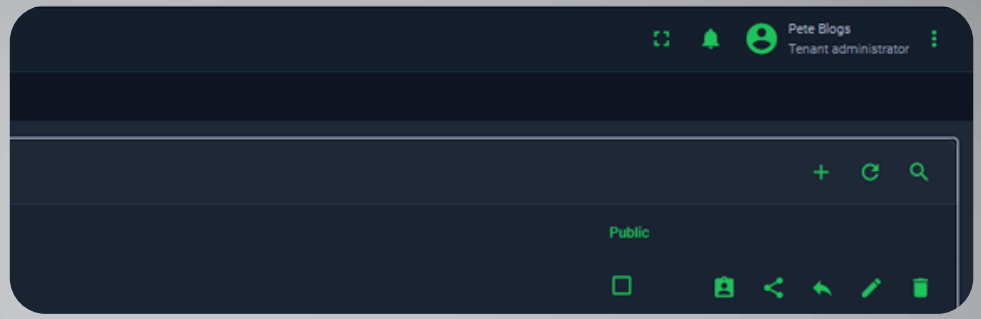
 © 2026 Smithtek Pty Ltd. All rights reserved.

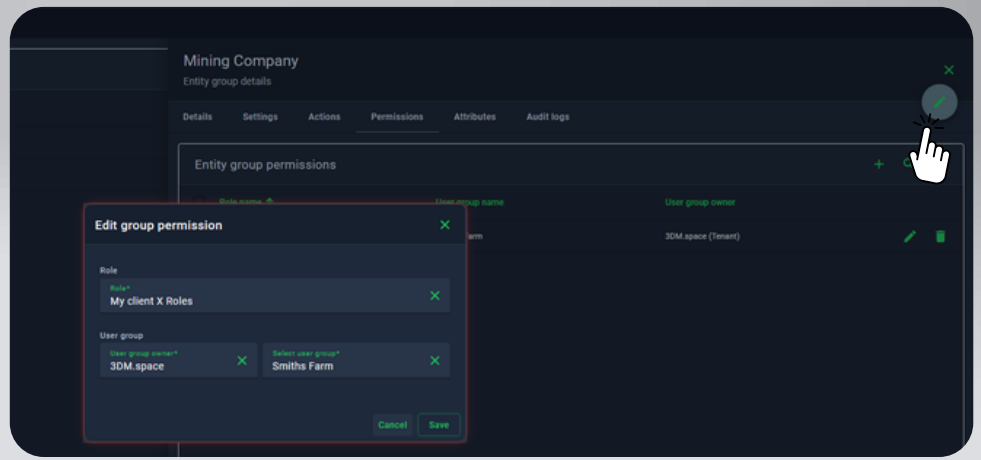
Option 2: Using the Permissions tab

The Permissions tab shows all access that has already been added to the device group. It can also be used to add a new permission, edit an existing permission, or remove access.

Steps

1. Go to **PassPort Gateway Setup**.
2. Click **PassPort Groups**.
3. Open the **device group**.
4. Click the **pencil/edit** icon.
5. Click the **Permissions tab**.
6. Click the **+ button** to add a **new permission**.
7. Select the **Role**.
8. Select the **User group owner**.
9. Select the **user group** that should receive access.
10. Click **Add**.





Important:

Be careful with All users. This gives access to every user in the account. For client, site, project, or private device groups, leave All users unticked and select the correct user group instead. Device group access allows the user group to access the PassPort Gateways inside the group. If a dashboard uses live data from a PassPort Gateway, the user may need access to the related device group for the dashboard data to display correctly.

Simple rule:

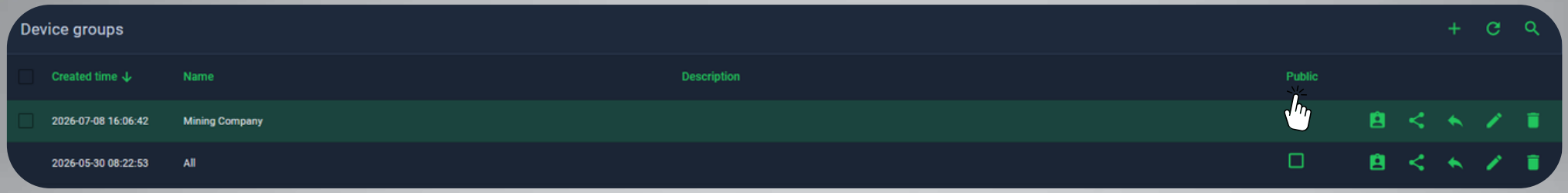
Share entity group = quick way to give access
Permissions tab = view, add, edit, or remove access
All users = everyone gets access
Selected user group = only that group gets access

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Group Table Properties

Device group table property settings

Device group table property settings are managed from the PassPort Groups list.
To access this area, go to PassPort Gateway Setup, then click PassPort Groups.
This page shows all device groups in the account and provides quick action buttons for creating groups, refreshing the list, searching for groups, checking public status, sharing access, opening groups, editing groups, and deleting groups.



Device group row options
From left to right, the device group row icons are:
Public status square
Shows whether the device group is public. If the square is ticked, the device group has been made public.
Share entity group
This is a quick way to set permissions and roles for the device group. Use this to give a user group access to the device group without opening the full group settings.This opens the same type of access setup discussed in the Giving users access section.
Make public
This makes the device group public. Use this carefully, as public access can allow device data to be used outside normal logged-in access.
The backward arrow
This opens the device group and shows the devices inside that group in the next table.
This does not open the settings page.

Edit group details
The pencil icon opens the Entity group details area.
Use this to edit the device group name, description, and group details.
Delete group
The trash can deletes the device group.
Use this carefully, as deleting the group may affect how devices are organised and accessed.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Device Group Table Properties

Device group table options

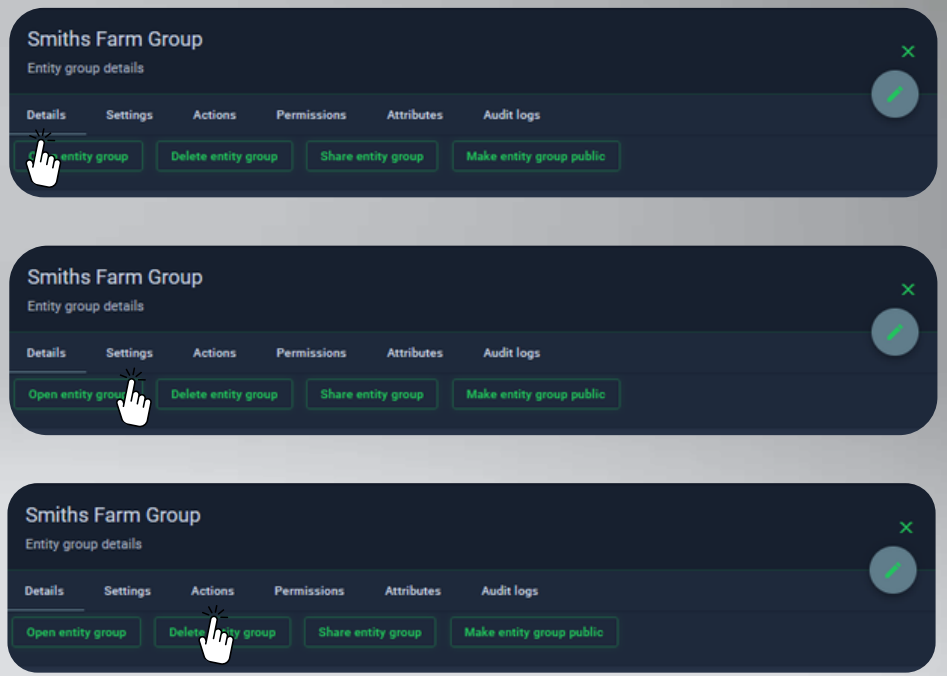
Add group
The **+ icon** is used to add a **new device group**.
Refresh
The refresh icon reloads the device group list.
Use this if a group has just been added or changed and the list needs to update.
Search
The magnifying glass icon is used to search the device group list.
Use this to quickly find a device group when there are multiple groups in the account.

Important:
Device group access is important because dashboards often rely on PassPort Gateway data.
If a user can open a dashboard but live data does not show, check that the user group also has permission to access the related device group. **Be careful with public settings.** Making a device group public does not automatically mean external users can see dashboard data. The related dashboard must also be public.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Group Property Settings

Details tab
The Details tab shows the basic information for the device group.
Name
This is the name of the device group. Use a clear name that explains what devices belong in the group. **Example:** “Smiths Farm Group”, “Company X Devices”, or “Mine Site A Devices”.
Description
This is an optional note explaining what the device group is used for. **Example:** “Devices for Smiths Farm site monitoring” or “Devices for Company X only.”
Open entity group
This opens the full device group page.
Delete entity group
This deletes the device group. Only use this if the group is no longer needed. Deleting a group may affect devices or permissions connected to that group.
Settings tab
The Settings tab controls how the device group list behaves and displays.
In most standard setups, these settings do not need to be changed. The default settings are normally suitable. Administrators may use this section to adjust how devices are displayed inside the group, such as list behaviour, searching, selection, pagination, or opening device details. For a basic setup, leave this section unchanged unless there is a specific reason to adjust it.
Actions tab
The Actions tab is used for group-related actions and advanced configuration.
The Actions tab is not normally used during standard device group setup. It may be used for advanced platform actions or future features. Most administrators can leave this section unchanged unless instructed by Smithtek support. Most users will not need this tab during normal setup, but administrators may use it for troubleshooting.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Permissions tab

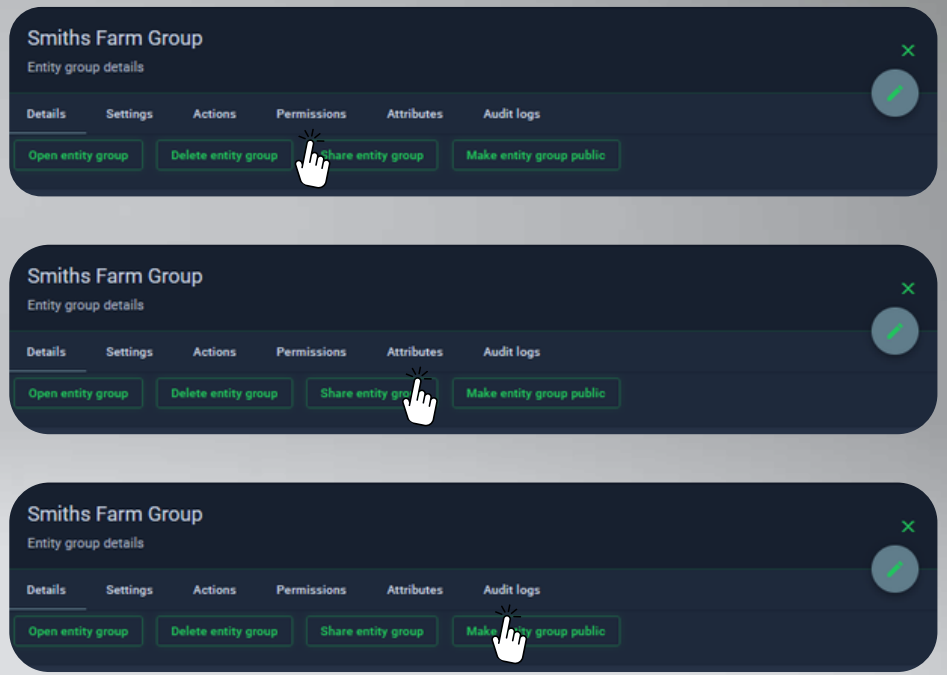
The Permissions tab shows which user groups have access to the device group. This is an important tab because it controls who can access devices inside the group. A device group without permissions is mostly just a container. Devices may be inside the group, but users will not receive access until the correct permission has been added. Use this tab to check which user groups are connected to the device group and which role is being used. **Example:** The Smiths Farm user group may be given a device role for the Smiths Farm Devices device group.

Attributes tab

The Attributes tab is for advanced group attributes. This is not normally required for basic device group setup. The Attributes tab is not used in the standard 3DM.Space setup covered by this manual. Leave this section unchanged unless Smithtek support has advised otherwise.

Audit logs tab

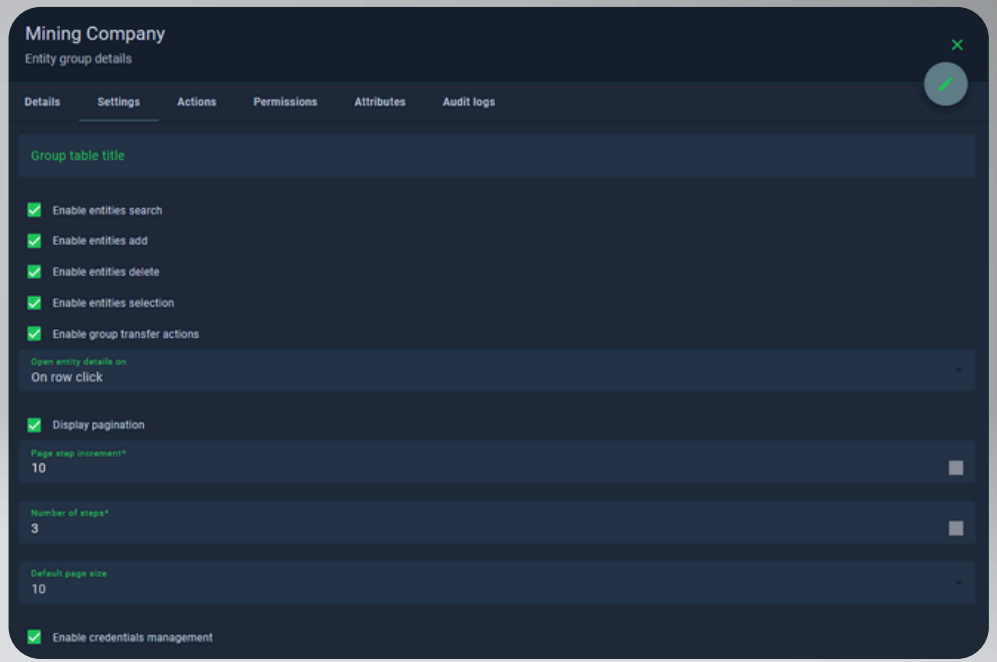
The Audit logs tab records changes and activity related to the device group. It can be useful for checking who changed something, when a group was edited, or when permissions were updated. Most users will not need this tab during normal setup, but administrators may use it for troubleshooting.



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Group Entity Details

Settings tab
The Settings tab controls how the group list behaves when viewing items inside the group.
Group table title
This allows you to set a custom title for the group table. If left blank, the default group title is used.
Enable entities search
Allows users to search within the group list.
Enable entities add
Allows users with the correct permissions to add items into the group.
Enable entities delete
Allows users with the correct permissions to delete or remove items from the group.
Enable entities selection
Allows users to select items in the group list.
Enable group transfer actions
Allows users with the correct permissions to move or transfer items between groups.
Open entity details on
Controls how item details open. Example: “On row click” means the item opens when the user clicks the row.
Display pagination
Shows page controls when there are lots of items in the group.
Page step increment
Controls how many extra rows are added when changing page size options.



Number of steps
Controls how many page size options are available.
Default page size
Controls how many items are shown per page. Example: 10 means 10 users are shown before pagination is used.
Enable login as user action
Allows an authorised administrator to log in as a user from this group. This is useful for testing user access, but should only be available to trusted administrators.

 © 2026 Smithtek Pty Ltd. All rights reserved.

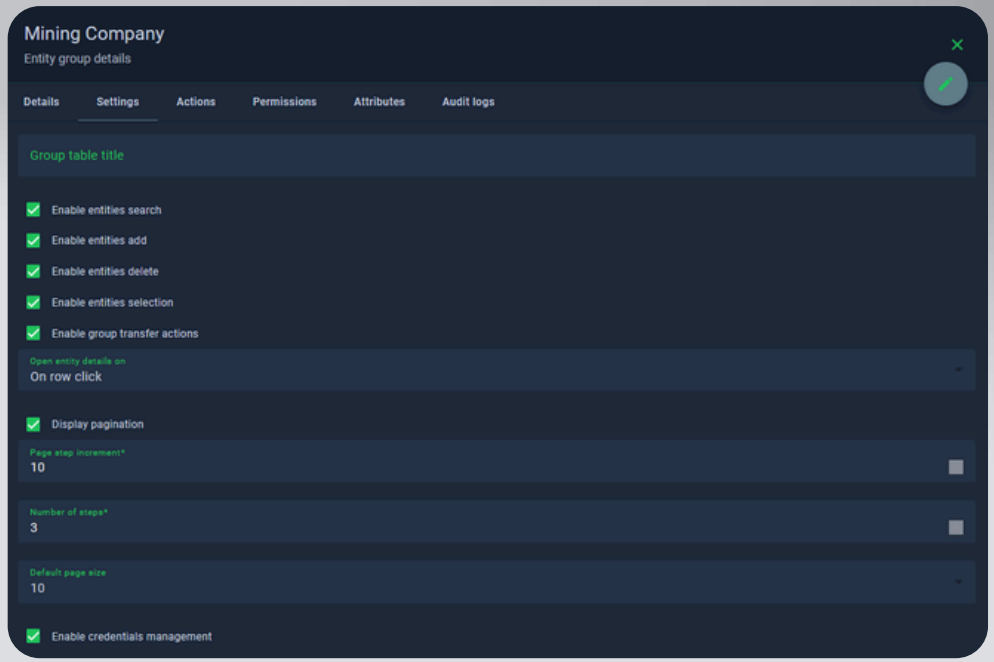
Device Group Entity Details

Enable credentials management

Enable credentials management controls whether device credentials can be managed for devices inside this device group.
Device credentials include the **Client ID**, **username**, and **password** used by the **PassPort Gateway** to **connect to 3DM.Space**.
When this setting is enabled, users with the correct permission level can manage credentials for PassPort Gateways in the group.

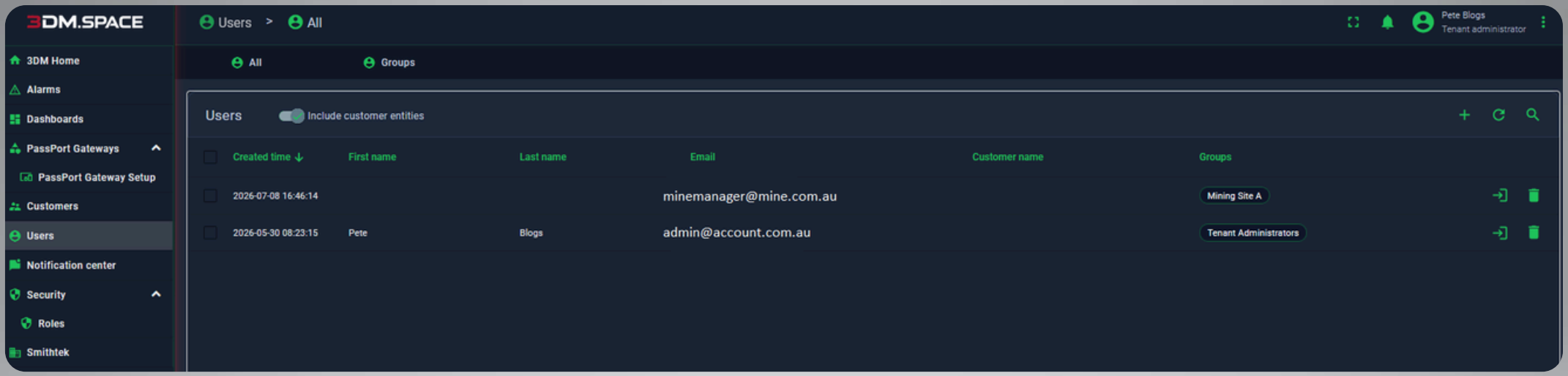
This setting is useful for administrators or trusted technical users who need to create, view, or update device credentials.
Lower level roles should not be able to turn this setting on or off. This helps prevent users with limited access from changing or interfering with PassPort Gateway credentials. For standard setups, leave this setting controlled by administrators only.

Simple rule:
Enable credentials management = allows credential management
Credentials = Client ID, username, and password
Admin users = can manage credentials
Lower level users = should not change credential settings



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM User Set-up



User Setup

User setup is the **final step** in giving someone **access to 3DM.Space**. Before creating or editing users, the main access structure should already be in place. This usually includes the required user groups, dashboard groups, device groups, and roles.

A user account on its own does not decide what the person can see or do. Access is controlled by the groups and roles connected to that user. This means a user must be placed into the correct user group before they receive the correct dashboard, device, alarm, or control access.
For restricted users, it is important to check which groups they belong to. A user may belong to more than one group, and each group may provide extra access. If a user can see more than expected, check whether they are still included in broad groups such as All, Tenant Users, or any internal staff groups.

This section covers **how to create a new user**, **move them into the correct user group**, **set a default dashboard**, **enable full screen dashboard mode**, and **remove broad access** so the user only sees what they need.

Simple rule:
User = the person logging in
User group = what access structure they belong to
Role = what they can do
Dashboard group and device group = what they can access

 © 2026 Smithtek Pty Ltd. All rights reserved.

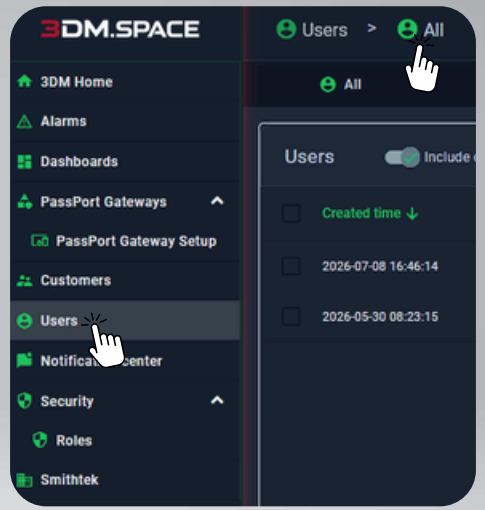
Creating a New User in All

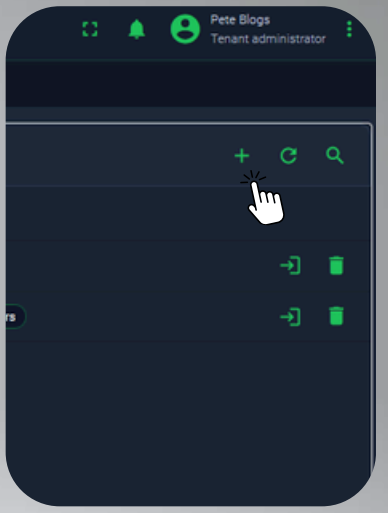
Creating a user from All users

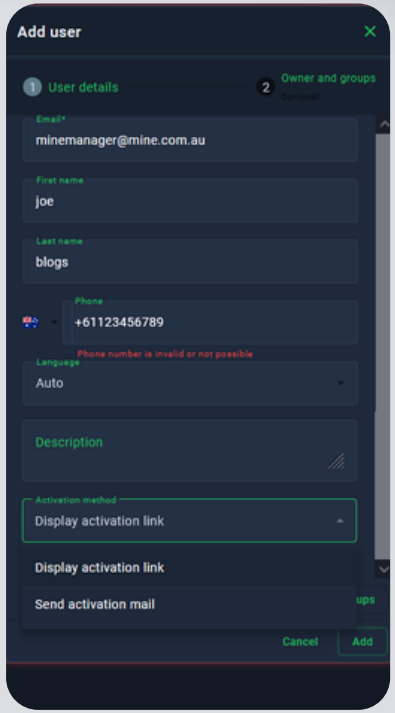
Creating a user from All users is useful when you want to create the user account first, then place the user into the correct user group afterwards.
This method can be used for internal users, general tenant users, or when the correct user group has not been selected yet.

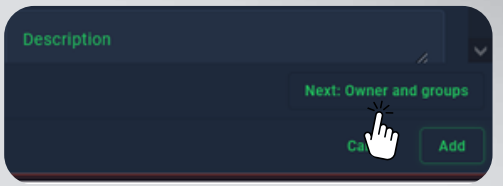
Steps

1. Click **Users** in the side navigation bar.
2. Click **All**.
3. Click the **+ button** to add a new user.
4. Enter the **user's details**.
5. **Email address**
6. Enter the user's email address. This is what the user will use to log in.
7. Enter the user's **first name**.
8. Enter the user's **last name**. (**Scroll down using the side scroll bar**)
9. Add a **description** if required. **Example**: "Smiths Farm dashboard user" or "Internal operations staff."
10. Check the **Owner and groups** section.
11. The **Owner** will usually default to the tenant.
12. The **Groups field** may include a **default group** such as **All** or **Tenant Users**.
13. Choose the **activation method**.
14. **Display activation link**. This shows an activation link on screen after the user is created. The administrator can copy this link and send it to the user manually.
15. **Send activation mail**. This sends the activation email directly to the user's email address.
16. Click **Add**. **The new user will now appear in the All users list.**









 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a New User in All

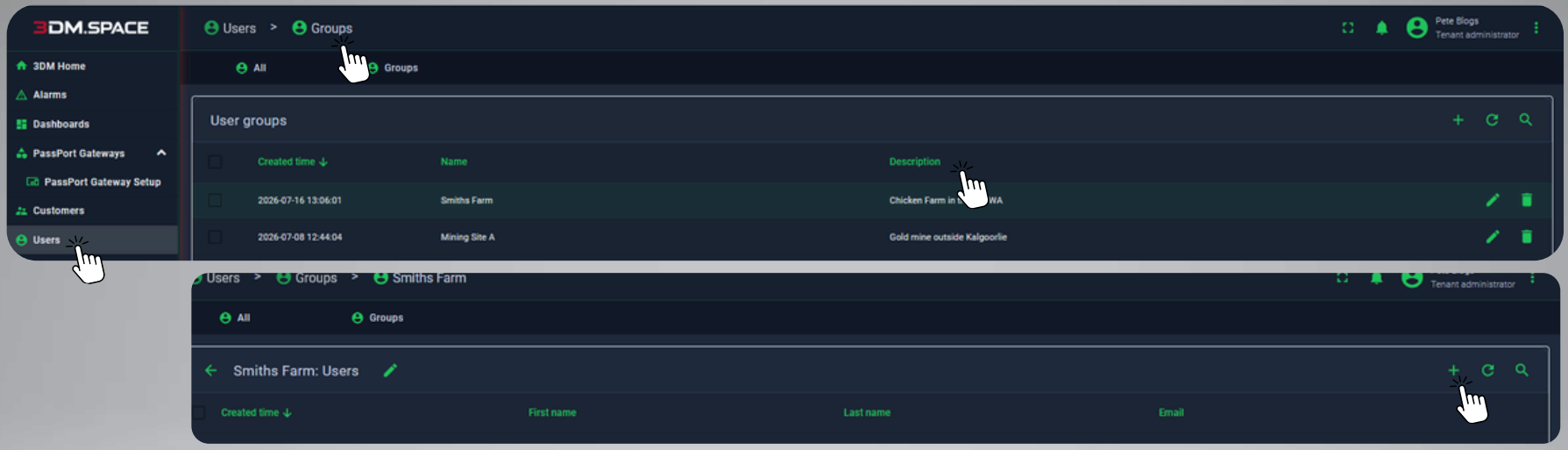
Side note
When creating a user, the Owner and groups section can be used to place the user into an existing user group straight away. You can select the correct group during setup, or leave this until later if you are not sure which group the user should belong to yet.

Important:
Creating a user from All users does not automatically mean the user has the correct access.
After creating the user, check which groups they belong to and move them into the correct user group if required. For restricted users, make sure they are not left in broad access groups that may give them more access than intended. The activation option is important. If Display activation link is selected, the administrator must copy and send the link manually. If Send activation mail is selected, 3DM.Space sends the activation email to the user.

Simple rule:
All users = create the user first
User group = control what access they receive
Display activation link = admin sends link manually
Send activation mail = platform emails the user

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Creating a New User in a Group

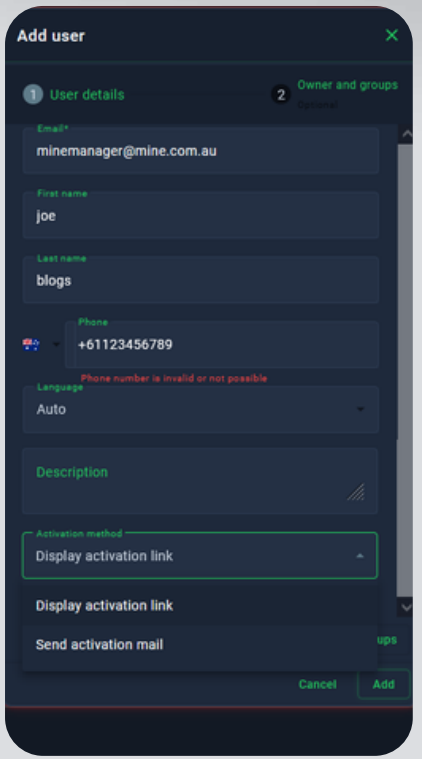


Creating a user inside a user group

Creating a user inside a user group is very similar to creating a user from All users. The user details are the same, but the starting point is different. This method is useful when the user group has already been created and you want the new user to be placed into the correct group straight away.

Steps

1. Click **Users** in the side navigation bar.
2. Click **Groups**.
3. **Find** the **user group** you want to create the user in. **Example:** “Smiths Farm” or “Company X Users”.
4. Click the **name** or **anywhere** in that group row, **DO NOT CLICK THE PEN**
5. If the required user group has not been created yet, see Section: User Groups.
6. Once inside the **user group**, click the **+ button** to **add a new user**.
7. **Email address**, enter the user’s email address. This is what the user will use to log in.
8. Enter the user’s **first name**.
9. Enter the user’s **last name.**
10. Add a **description if required**.
11. Choose **activation** method.



Side note

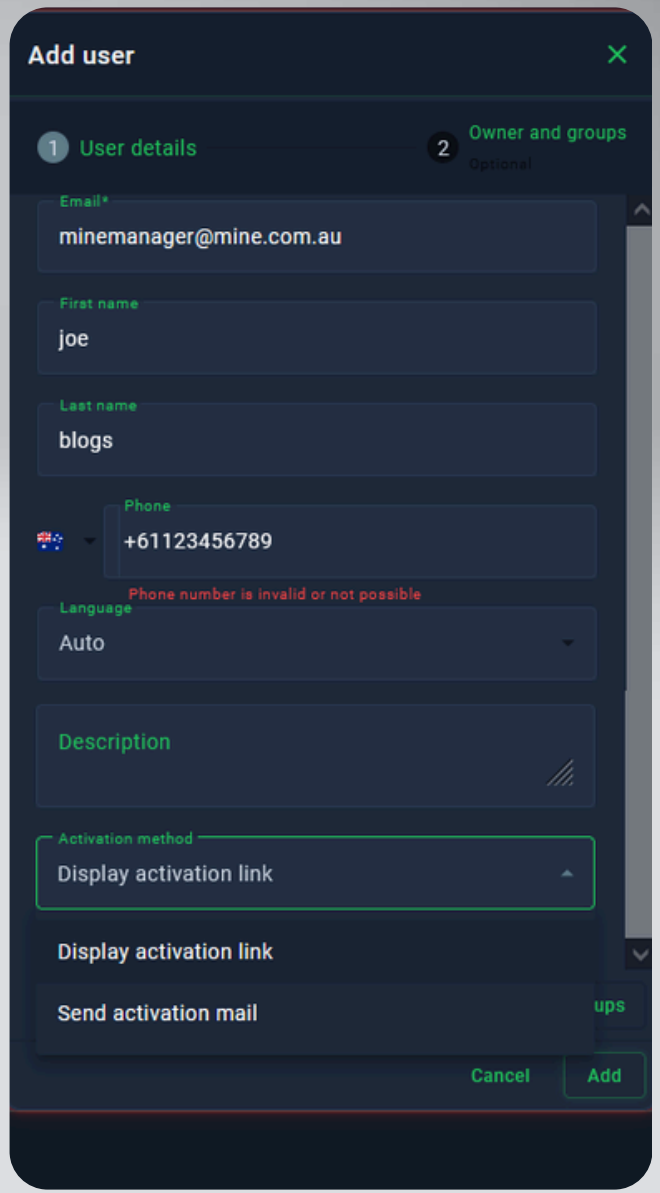
When creating a user, you do not need to change the Owner and groups section if the user is already being created in the correct place. This section can be used later if you need to move the user into a different user group. You can update the selected group here and then click Add when creating the user.

 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

Creating a New User in a Group

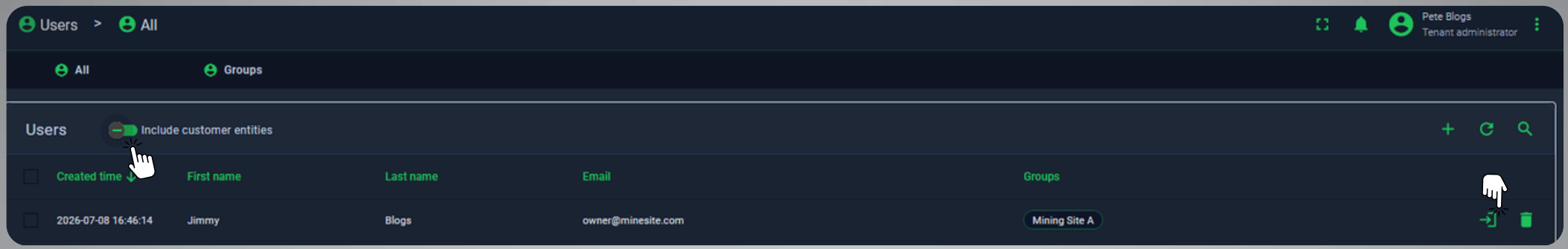
12. Display **activation** link. This shows an activation link on screen after the user is created. The administrator can copy this link and send it to the user manually.
13. **Send activation** mail. This sends the activation email directly to the user's email address.
14. Click **Add. The new user will now be created inside the selected user group.**



Important:
Creating a user inside a user group is usually the cleaner method for restricted users because the user starts in the correct access group. The user will still only receive useful access if that user group has the correct roles and permissions assigned.

 © 2026 Smithtek Pty Ltd. All rights reserved.

User Management Settings



User management settings

User management settings can be accessed from any user list. This may be from Users → All or from inside a specific User Group. These settings allow administrators to manage user accounts, check access, log in as a user for testing, or remove a user if required.

Login as user icon

The doorway icon allows an administrator to log in as that user. This is useful for testing what the user can see after their groups, roles, dashboards, and devices have been set up. This option is only available to account administrators.

Delete user icon

The trash can icon is used to delete a user account. If this icon is clicked, a security prompt will appear asking the administrator to confirm the deletion. Deleting a user is permanent. Once the user has been deleted, their user account and related user data cannot be recovered by Smithtek or 3DM.Space. Only delete a user if you are sure the account is no longer required.

Include customer entities

The Include customer entities toggle changes what is displayed in the user table. When enabled, the table may also show users or details related to customer entities. This can be useful when checking users connected to customer accounts. For standard user management, this can usually be left off unless customer users need to be reviewed.

Important note

Use the Login as user option carefully. It is a helpful testing tool, but it should only be used by authorised administrators. Use the Delete user option with extra care. Deleted users cannot be restored.

Simple rule:
Doorway icon = log in as user
Trash icon = delete user permanently
Include customer entities = show customer-related users/details

 © 2026 Smithtek Pty Ltd. All rights reserved.

User settings

To **view a user's settings**, click on **any user** from the **user lis**t. The user details panel will open and show the current settings for that user. To **edit** the user settings, **click the pencil/edit icon**. To close the user details panel and return to the user list, click the X icon.

User settings tabs

The user settings area is split into several tabs. Each tab shows a different type of information connected to the selected user.

Details

Shows the main user account information, such as email, name, phone number, language, unit system, description, default dashboard, full screen setting, and user group information. This is the main tab used when setting up or editing a user.

Latest telemetry

Shows telemetry information related to the user. This is not normally used during standard user setup.

Alarms

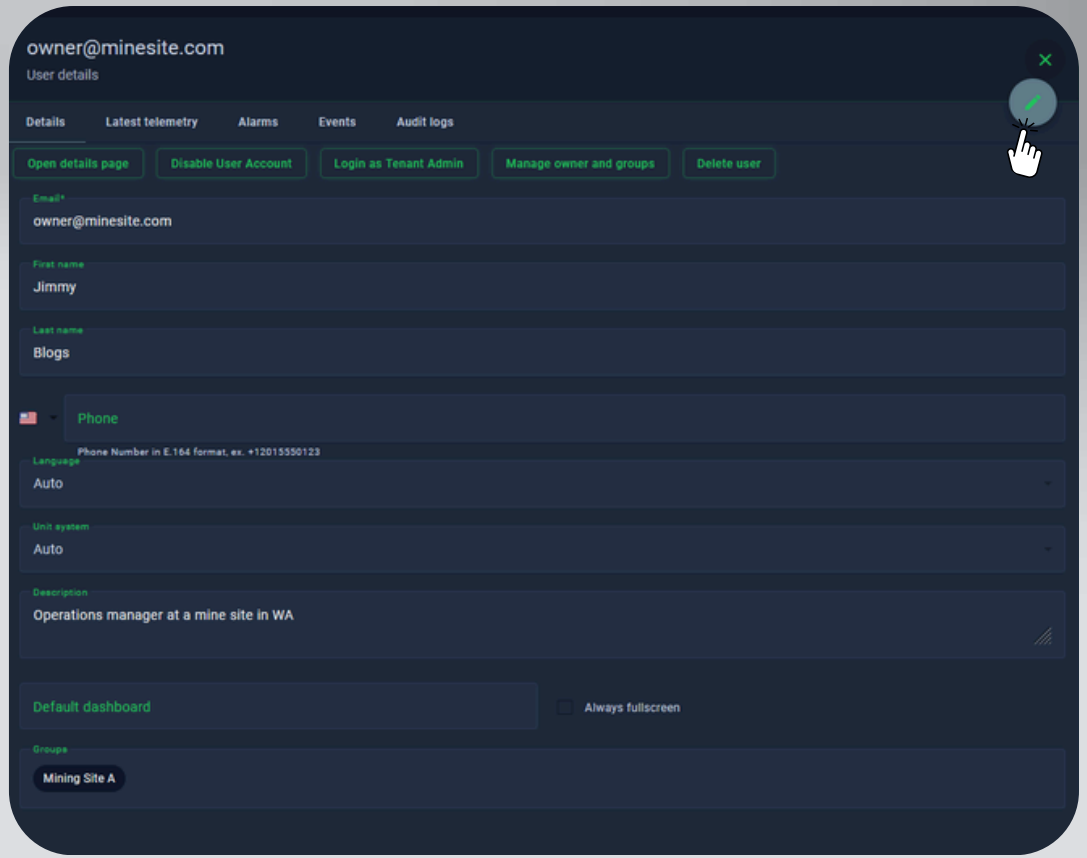
Shows alarms related to the user. This is not normally required for basic user setup.

Events

Shows events related to the user account. This can include platform activity or system events linked to the user.

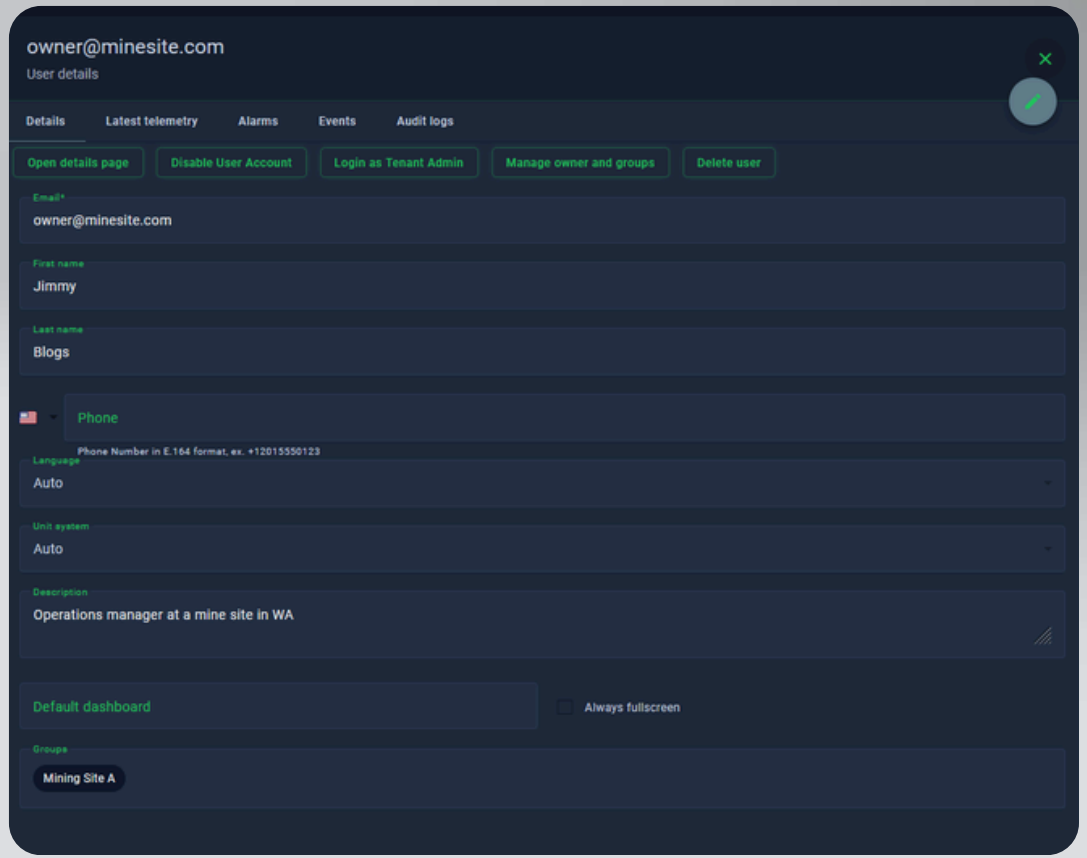
Audit logs

Shows changes and activity related to the user. This can be useful for checking when a user was edited, when settings were changed, or who made a change.



 © 2026 Smithtek Pty Ltd. All rights reserved.

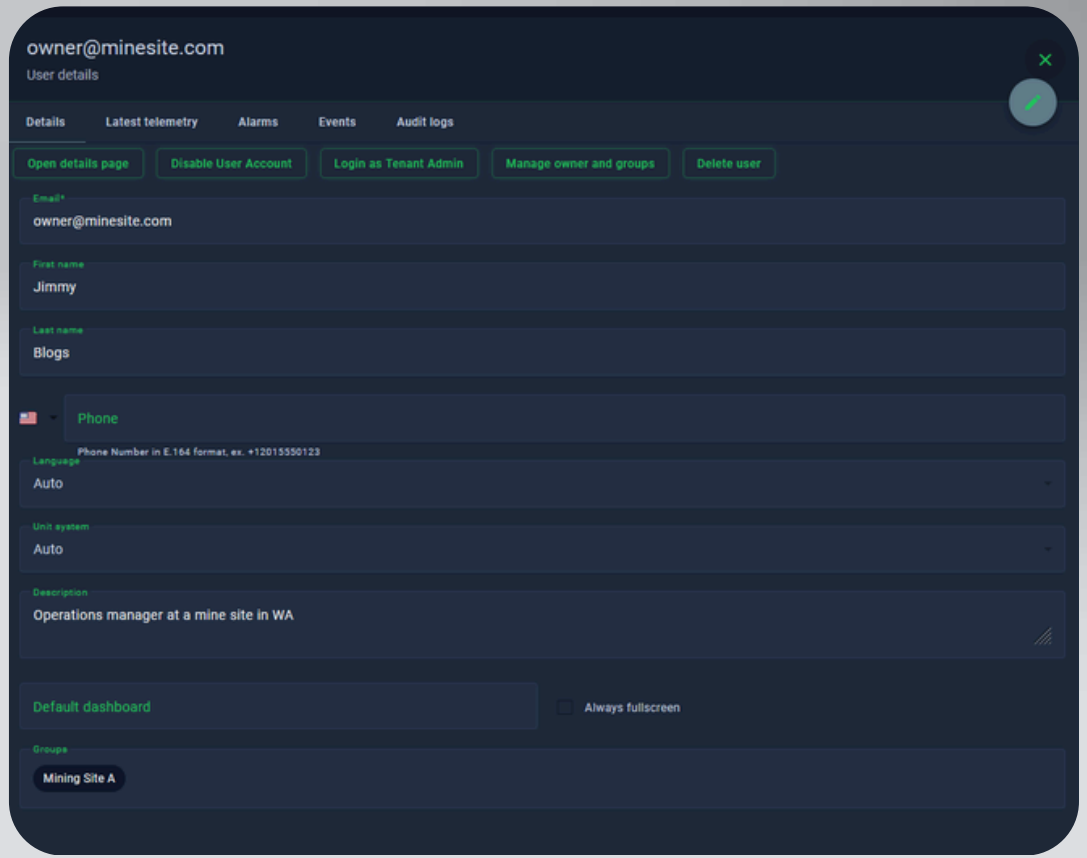
User action buttons
The user details area includes several action buttons. These buttons are used to manage the selected **user account.**
Open details page
Opens the full details page for the selected user.
Disable User Account
Disables the user account without deleting it. This can be used if the user should no longer be able to log in, but the account should not be permanently removed.
Login as Tenant Admin
Allows an administrator to log in as this user for testing or support purposes. This is useful for checking what the user can see after groups, roles, dashboards, and devices have been assigned.
Manage owner and groups
Opens the owner and group settings for the user. This is where the user can be moved into a different user group if required.
Delete user
Deletes the user account. Use this carefully, as deleting a user is permanent.
User details fields
The lower section of the Details tab shows the user information stored against the selected user.
Email
The email address used by the user to log in.
First name / last name
The user's name.
Optional phone number for the user. The phone number should be entered in E.164 format, for example +12015550123.



 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM User Details

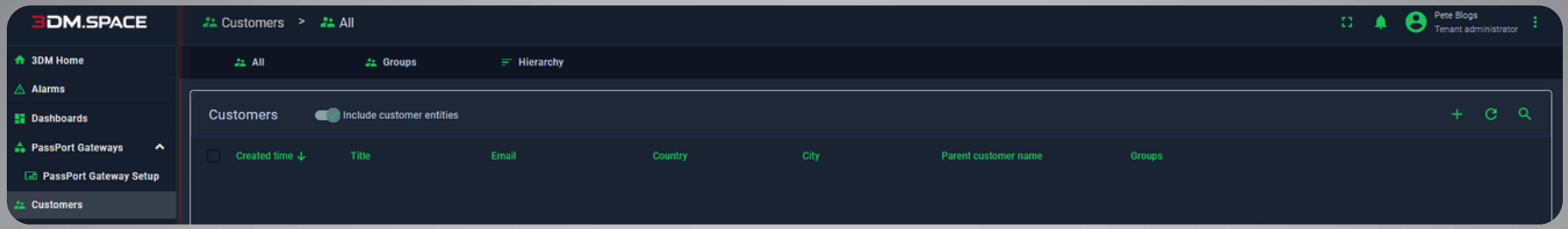
Language
Sets the user's language preference. This may be left as Auto unless a specific language is required.
Unit system
Sets the user's unit preference. This may be left as Auto unless a specific unit system is required.
Description
Optional notes about the user.
Default dashboard
Sets the dashboard that opens by default when the user logs in.
Always fullscreen
When enabled, the selected dashboard opens in full screen mode for that user.
Groups
Shows which user group or groups the user belongs to. **Example:** "Mining Site A".



Important:
For normal user setup, the main areas to check are:
Email
Name
Groups
Default dashboard
Always fullscreen
Disable user account
Manage owner and groups
Use Delete user only when the account is no longer required and you are sure it should be permanently removed.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Customers



Customers are used to separate access for external companies, clients, site owners or contractors who should only see selected information.

A customer sits under the main tenant account. Administrators can:

- **Create the customer.**
- **Add customer users.**
- **Assign selected dashboards and devices.**
- **Control access to alarms and live data through permissions.**

Examples include Smiths Farm, Company X, Mining Site A or Irrigation Client B.

When to use Customers

Use a customer when an external organisation needs access to its own dashboards and devices, but should not have access to the wider tenant account.

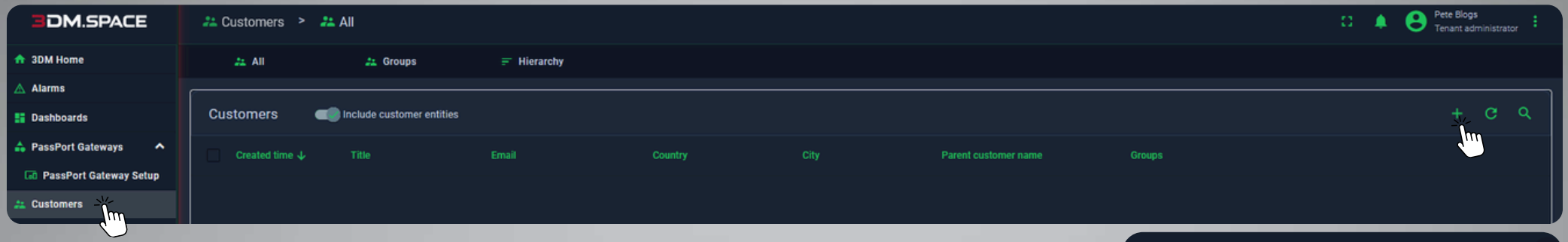
Depending on their permissions, customer users may be able to:

- View dashboards.
- Monitor live data.
- Access assigned devices.
- View or acknowledge alarms.

Simple rule:
Tenant = main 3DM.Space account
Customer = external company, site, or client under the tenant
Customer user = person who logs in under that customer
Assigned dashboards and devices = what the customer can access

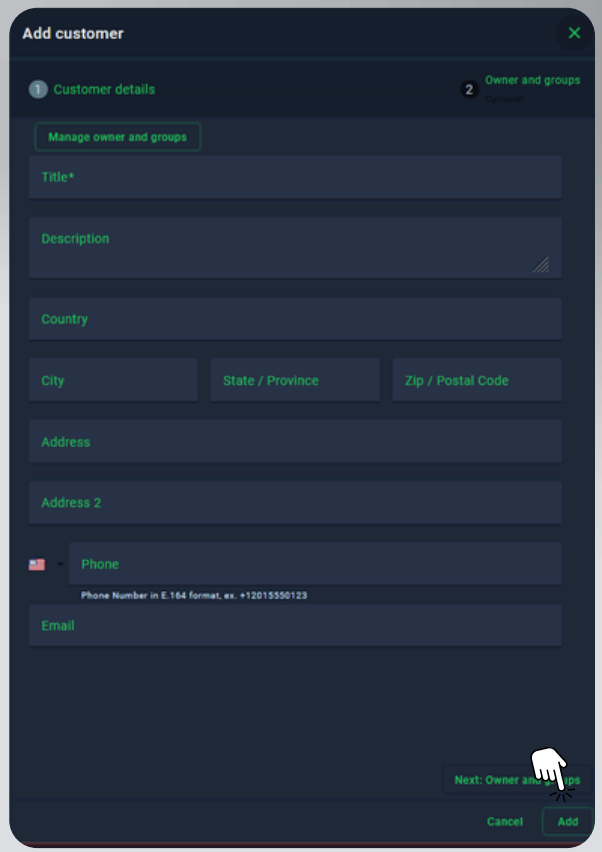
Important:
Customers are generally for external users. Internal staff who need broader account access should normally be managed through Users, User Groups, Roles, Dashboard Groups and Device Groups. **In simple terms:** Customers separate external clients or sites so they only see the information assigned to them.

 © 2026 Smithtek Pty Ltd. All rights reserved.



Creating a customer

Customers can be created from the Customers section in the side navigation bar. A customer can be created on its own first, then added to a customer group later. If the required customer group already exists, the customer can also be added to that group during setup.

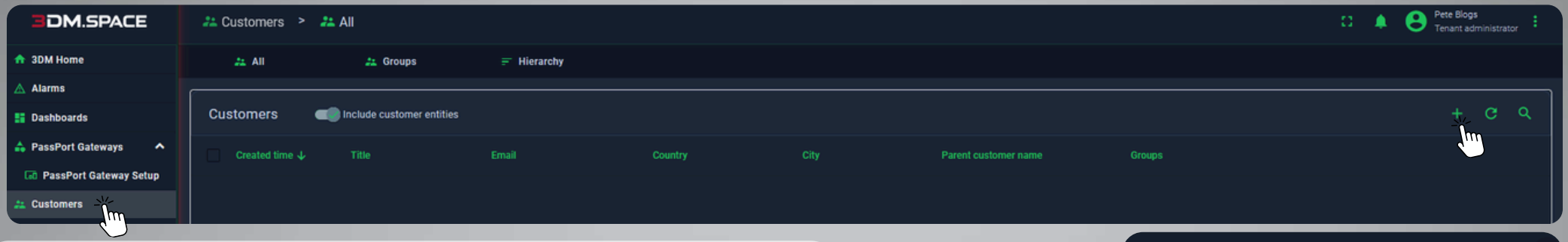


Steps

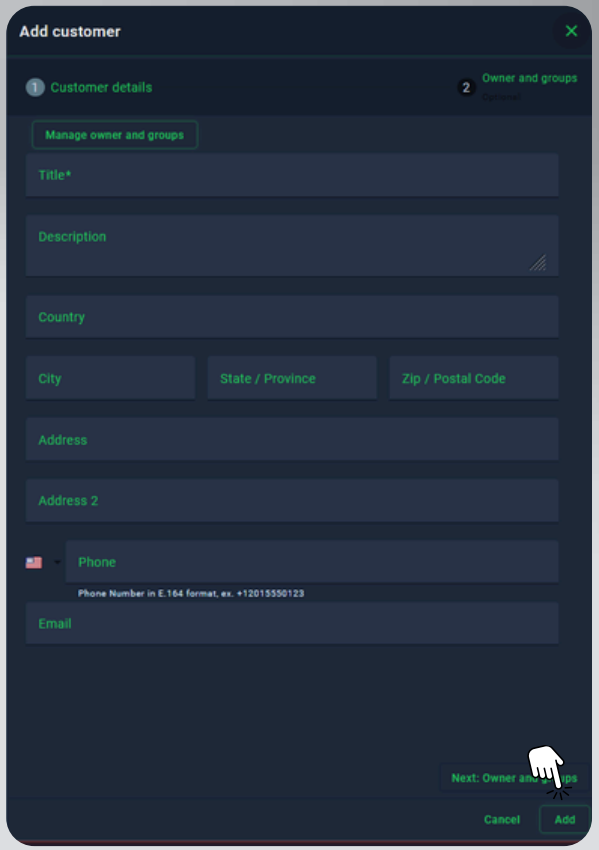
1. Click **Customers** in the side navigation bar.
2. Click **All**.
3. Click the **+ button** to add a new customer.
4. Enter a clear **customer title. Example:** “Smiths Farm”, “Company X”, or “Mining Site A”.
5. Add a description if required. **Example:** “Customer account for Smiths Farm site monitoring.”
6. Complete the **customer details** if required.
7. **Country** - enter the customer’s country.
8. **City** - enter the customer’s city.
9. **State / Province** - enter the customer’s state or province.
10. **Zip / Postal Code** - enter the customer’s postcode.
11. **Address** - enter the customer’s main address.
12. **Address 2** - add extra address details if required.
13. **Phone** - add the customer’s phone number if required.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating a Customer



14. **Email** - add the customer's email address if required.
15. Check the **Owner and groups section**.
16. The **owner** will usually default to the tenant.
17. You can add the customer to an existing customer group during setup, or leave this until later if you are not sure which group the customer should belong to yet.
18. Click **Add**. **The new customer will now appear in the customer list.**

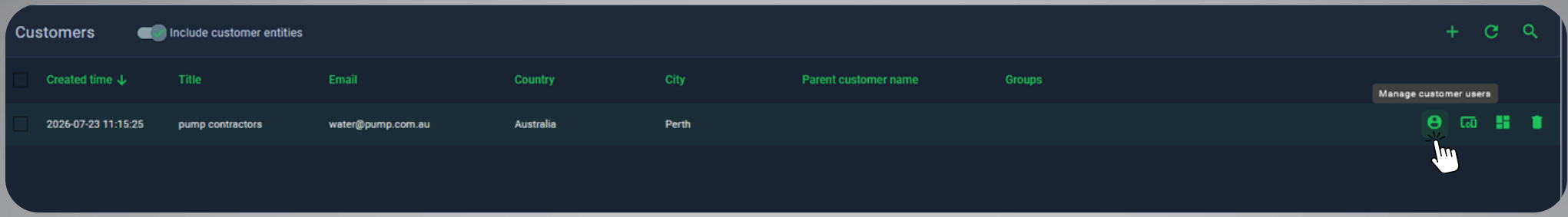


Important:
Creating a customer does not automatically give customer users access to dashboards, devices, or alarms. A customer is the account container. Customer users, dashboards, devices, and permissions still need to be set up correctly. If customer groups are being used, the customer can be added to a group during setup or moved into a group later.

Simple rule:
Customer = external company, site, or client
Customer group = where customers can be organised
Customer users = people who log in under the customer
Add = complete the customer setup

 © 2026 Smithtek Pty Ltd. All rights reserved.

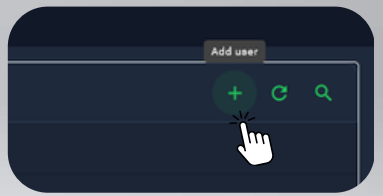
Adding a Customer User

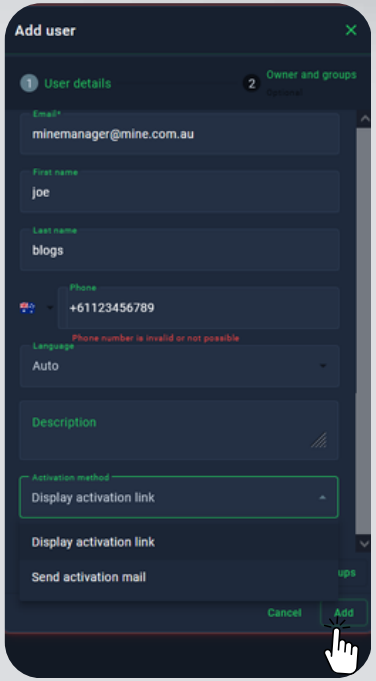


Customer users are managed from the customer list.
On the right side of each customer row, there are four action icons:

- **Customer users**
- **Customer devices**
- **Customer dashboards**
- **Delete customer**

The Customer users icon is used to view or add users under that customer.





Steps

1. Click **Customers** in the side navigation bar.
2. Click **All.**
3. **Find** the **customer** in the list. Example: “Pump Contractors”.
4. Click the **Manage customer users** icon. The customer user list will open.
5. Click the **+ button** to **add a new customer user.**
6. Complete the user setup details.
7. Click **Add**. **The new user will now be created under the selected customer.**

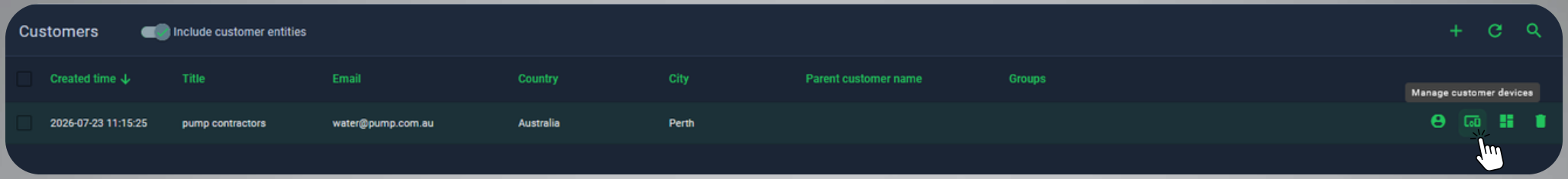
Important:
The process for adding a customer user is the same as adding a standard user.
The new user will now be created under the selected customer. Customer users are linked to the customer they are created under. Customer users should be used for external clients, contractors, site owners, or other people who should only access information assigned to that customer.
Internal staff and administrators should usually be created under the main Users section instead.

Side note
When creating a user, you can leave Owner and groups unchanged if they are already in the correct group.

If you need to move the user to a different user group, update the selected group here and click Add.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Adding Customer Devices



Manage customer devices

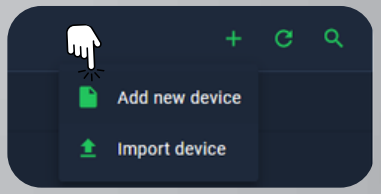
Customer devices are managed from the customer list. On the right side of each customer row, there are four action icons:

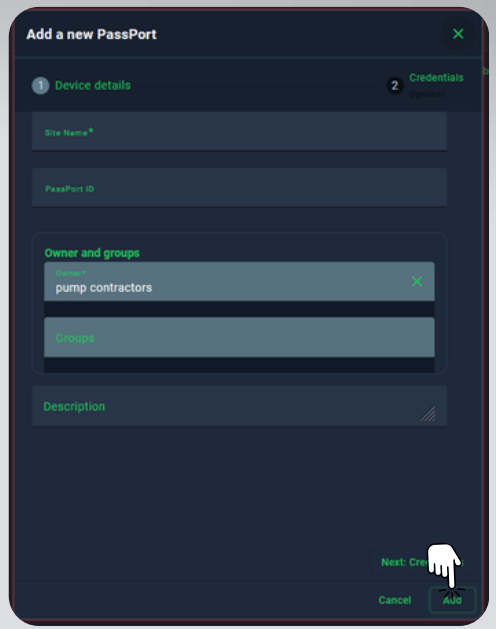
- **Customer users**
- **Customer devices**
- **Customer dashboards**
- **Delete customer**

The Customer devices icon is used to view or add devices under that customer.

Steps

1. Click **Customers** in the side navigation bar.
2. Click **All**.
3. **Find** the **customer** in the list. Example: “Pump Contractors”.
4. Click the **Manage customer devices** icon. The customer device list will open.
5. Click the **+ button** to **add a device**.
6. Complete the device setup details.
7. Click **Add**. **The device will now be created under the selected customer.**





Side note:
Use Import devices to add many devices at once instead of creating them individually.

- *Small setups: Add devices manually.*
- *Large deployments or fleets: Import devices to save time and keep setup consistent.*

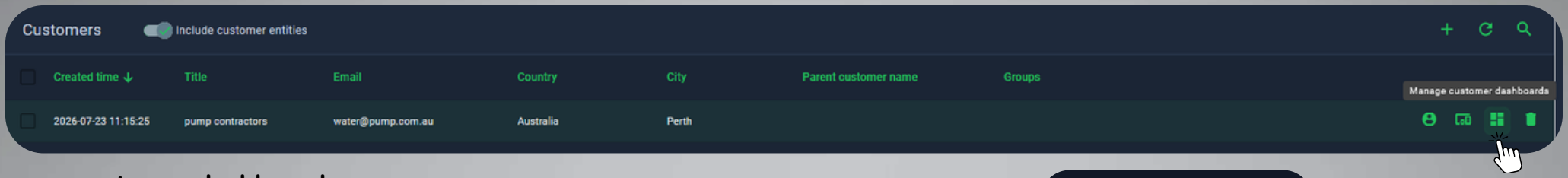
The process for adding a customer device is the same as adding a standard device. Customer devices are linked to the customer they are created under.

Important:
In 3DM.Space, devices are usually PassPort Gateways. The connected hardware, such as Mako PLCs, sensors, pumps, tanks, or controllers, communicates through the PassPort Gateway. Only add devices under a customer when that device should belong to that customer’s access area.

 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

Adding Customer Dashboards

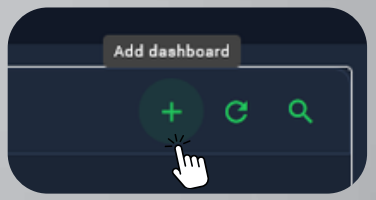


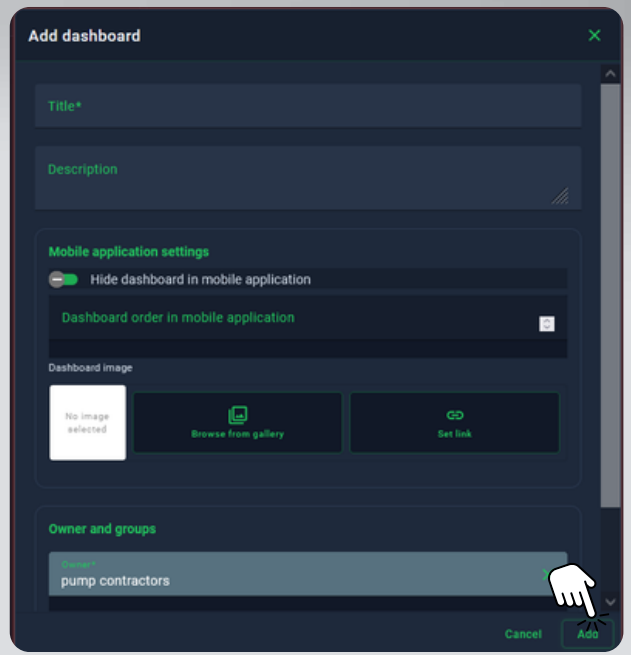
Manage customer dashboards

Customer dashboards are managed from the customer list. On the right side of each customer row, there are four action icons:

- **Customer users**
- **Customer devices**
- **Customer dashboards**
- **Delete customer**

The Customer dashboards icon is used to view or add dashboards under that customer.





Steps

1. Click **Customers** in the side navigation bar.
2. Click **All**.
3. **Find** the **customer** in the list. Example: “Pump Contractors”.
4. Click the **Manage customer dashboards** icon. The customer dashboard list will open.
5. Click the **+ button** to add a dashboard.
6. Complete the dashboard setup details.
7. Click **Add**. **The dashboard will now be created under the selected customer.**

The process for adding a customer dashboard is the same as adding a standard dashboard. When adding a dashboard, you may also see an option to import a dashboard.

 © 2026 Smithtek Pty Ltd. All rights reserved.

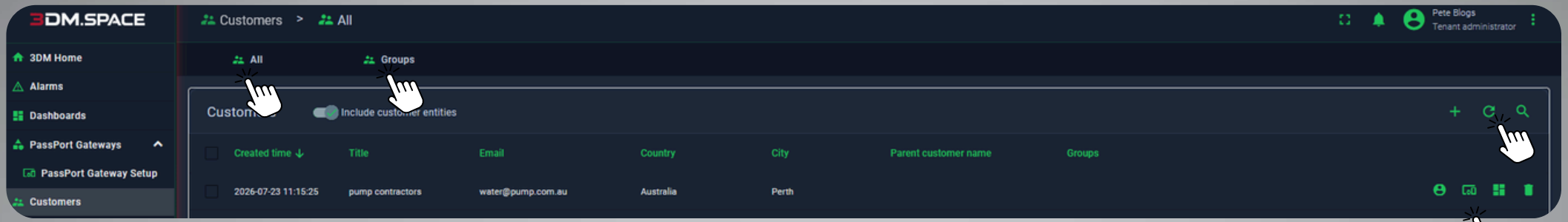
Adding Customer Dashboards

Side note:
Importing dashboards
The Import dashboard option is used when a dashboard has already been created and needs to be added into 3DM.Space. This is useful when reusing dashboard templates, copying dashboards between sites, or setting up similar dashboards for multiple customers or projects. For most small setups, dashboards can be created manually. For larger deployments, importing dashboards can save time and help keep dashboard setup consistent.

Important:
Customer dashboards are linked to the customer they are created under. Only add dashboards under a customer when that dashboard should belong to that customer's access area. Also remember that dashboard access does not always mean live data will display. If the dashboard uses data from a PassPort Gateway, the customer may also need access to the related customer device.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Customer Management Settings



Customer management settings

Customer management settings are available from the main customer list.
To access this page, click **Customers** in the **side navigation bar**, then click **All**. This page shows the customers that have been created in the account and provides quick action buttons for managing customer users, devices, dashboards, and customer records.

Customer list options:

Add customer

The + button is used to add a new customer.
Use this when creating a new customer, client, site, contractor, or external organisation.

Refresh customers

The refresh icon reloads the customer list.
Use this if a customer has just been added or changed and the list needs to be updated.

Simple rule:
+ = add customer
Refresh = reload customer list
Search = find a customer
Customer users = manage people under the customer
Customer devices = manage devices under the customer
Customer dashboards = manage dashboards under the customer
Trash can = delete customer

Search customers

The search icon is used to search the customer list.
This is useful when the account contains many customers and you need to quickly find a specific customer.

Include customer entities

The Include customer entities toggle controls what appears in the customer table. When enabled, it may show additional customer-related information. For normal customer management, this can usually be left off unless you need to review those extra details.

Customer row options

On the right side of each customer row, there are four action icons.

Manage customer users

This opens the user list for the selected customer. Use this to view, add, or manage users under that customer.

Manage customer devices

This opens the device list for the selected customer. Use this to view, add, or manage devices under that customer.

Manage customer dashboards

This opens the dashboard list for the selected customer. Use this to view, add, or manage dashboards under that customer.

Delete customer

The trash can icon is used to delete the customer. Use this carefully.
Deleting a customer may affect customer users, devices, dashboards, and access connected to that customer.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Customer settings

Customer settings tabs
The customer settings area is split into several tabs. Each tab shows a different type of information connected to the selected customer.

Details
Shows the main customer information, such as title, description, contact details, address details, and customer group information. This is the main tab used when setting up or editing a customer.

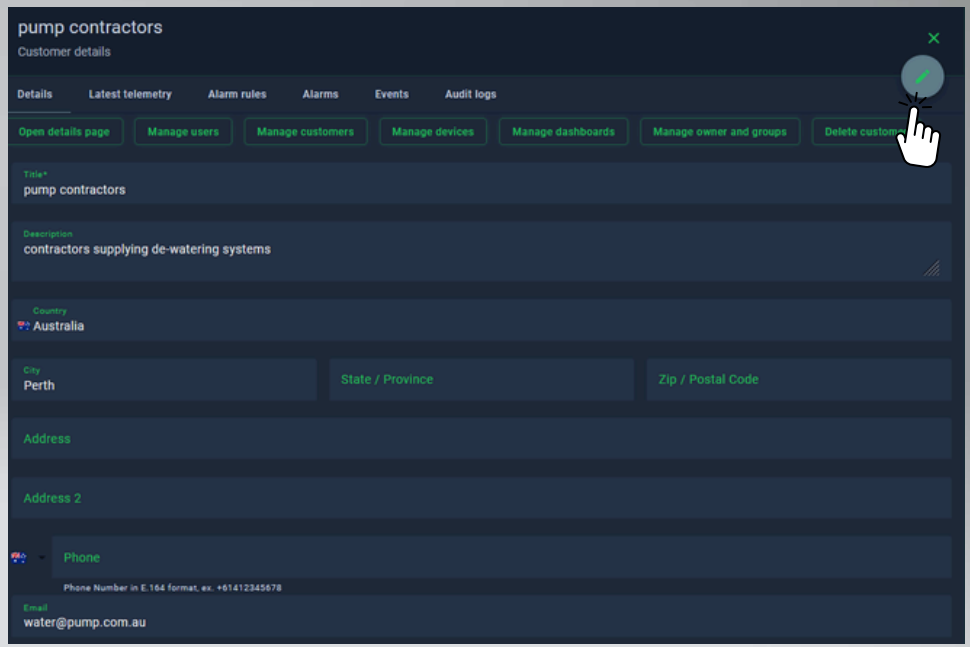
Latest telemetry
Shows the latest telemetry information related to the customer. This is not normally used during standard customer setup.

Alarm rules
Shows alarm rules related to the customer. This may be used for advanced alarm setup, but is not normally required during basic customer setup.

Alarms
Shows alarms related to the customer. This can be useful for checking whether the customer has active or historical alarms.

Events
Shows events related to the customer. This can include platform activity or system events linked to the customer.

Audit logs
Shows changes and activity related to the customer. This can be useful for checking when a customer was edited, when settings were changed, or who made a change.



To edit the customer settings, click the pencil/edit icon.
To close the customer details panel and return to the customer list, click the X icon.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Customer action buttons
The customer details area includes several action buttons. These buttons are used to manage the selected customer and the items connected to that customer.

Open details page
Opens the full details page for the selected customer.

Manage users
Opens the user list for the selected customer. This is used to view, add, or manage users under that customer.

Manage customers
Opens the customer management area for customers linked under the selected customer. This is mainly used for customer hierarchy or advanced customer structures.

Manage devices
Opens the device list for the selected customer. This is used to view, add, or manage devices under that customer.

Manage dashboards
Opens the dashboard list for the selected customer. This is used to view, add, or manage dashboards under that customer.

Manage owner and groups
Opens the owner and group settings for the customer. This is where the customer can be moved into a different customer group if required.

Delete customer
Deletes the selected customer. Use this carefully, as deleting a customer may affect users, devices, dashboards, alarms, and access connected to that customer.

Customer details fields
The lower section of the Details tab shows the customer information stored against the selected customer.

Title
The customer name shown in 3DM.Space. Example: “Pump Contractors”, “Smiths Farm”, or “Mining Site A”.

Description
Optional notes about the customer. Example: “Contractors supplying de-watering systems.”

Email
The customer’s email address. This can be used as a general contact email for the customer.

Address and contact details
This section stores the customer’s location and contact information, including country, city, state or province, postcode, address, phone number, and any extra address details. These fields are mainly used for customer records and identification. They help administrators keep customer information organised inside 3DM.Space.

 © 2026 Smithtek Pty Ltd. All rights reserved.



In **3DM.Space**, **devices** are **PassPort Gateways.**

PassPort Gateways are the **field devices** deployed at site locations. They **connect to the internet** and **communicate** with the **3DM.Space** cloud. This allows site data to be sent from the PassPort Gateway into 3DM.Space, where it can be viewed on dashboards, used for alarms, and stored for monitoring.

PassPort Gateways can also **receive data** and **commands** from **3DM.Space**. This allows approved controls to be sent back to the site, such as turning **pumps**, **valves**, **lights**, or other connected equipment on and off.

A customer, site, or project may have one PassPort Gateway or hundreds of PassPort Gateways in their account. These are all visible and managed from the PassPort Gateways menu in 3DM.Space.

Although the platform may use the word device, in this manual a device usually means a PassPort Gateway. Connected equipment such as Mako PLCs, sensors, pumps, tanks, valves, controllers, and other site hardware communicate through the PassPort Gateway.

 © 2026 Smithtek Pty Ltd. All rights reserved.

The current standard **communication** method for **PassPort Gateways** is **MQTT**. This is selected using the Device profile setting. Other device profiles or communication protocols may become available in the future. When a new PassPort Gateway is created in 3DM.Space, device credentials are also created. These **credentials** may include a **Client ID**, **username**, and **password**. They can be generated automatically or created manually.

The **same credentials** are then entered into the **PassPort Gateway Node-RED 3DM node**. This is what links the physical PassPort Gateway in the field to the correct device record in 3DM.Space.

If the credentials in 3DM.Space and the credentials in the PassPort Gateway Node-RED 3DM node do not match, the PassPort Gateway will not connect correctly.

In simple terms, the **PassPort Gateway is the bridge between the site and 3DM.Space**.



 © 2026 Smithtek Pty Ltd. All rights reserved.

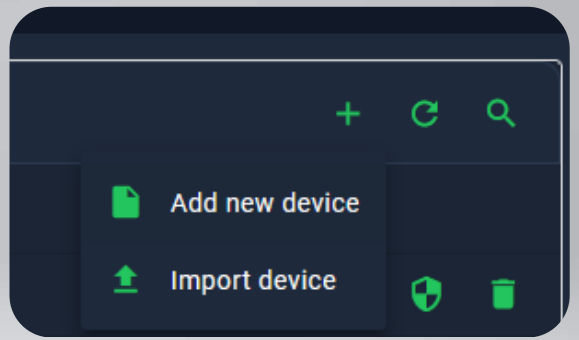
Creating a PassPort Gateway (Device)

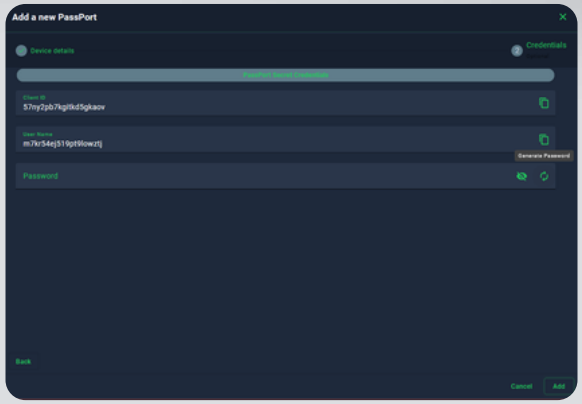
Creating devices

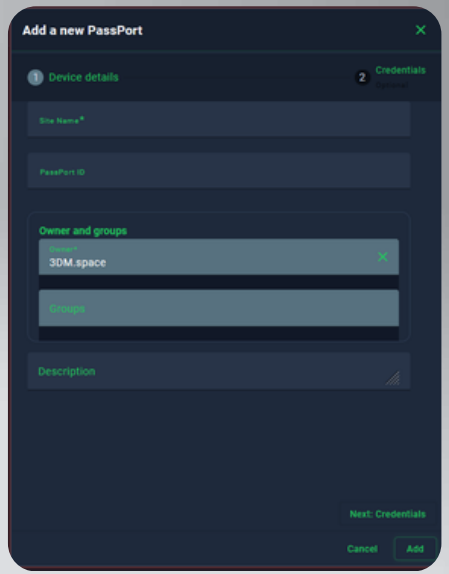
Devices are created from the PassPort Gateway Setup section.
In 3DM.Space, a device usually means a PassPort Gateway. Each PassPort Gateway must be added into 3DM.Space before it can connect, send data to the cloud, and receive commands back from dashboards or controls.

Steps

1. Click **PassPort Gateway Setup** in the side navigation bar.
2. Click **All**.
3. Click the **+ button.**
4. Select **Add new device**. The Add device window will open.
5. Enter a clear **device name**. **Example:** “Smiths Farm PassPort”, “Pump Station 1 PassPort”, or “Mining Site A Gateway”.
6. Add a label or **description** if required. **Example:** “PassPort Gateway installed at main pump station.”
7. Click **Next**: **Credentials.**
8. Click **PassPort secret Credentials**. This will show the credential fields: Client ID, Username, Password
9. **Create** the **credentials**. Click the refresh icon to generate the credential automatically, or enter it manually.
10. **Record** the **credentials**. Enter the same credentials into the **3DM Node-RED node** on the **PassPort Gateway**.
11. Click **Add**. **The new PassPort Gateway will now appear in the device list.**







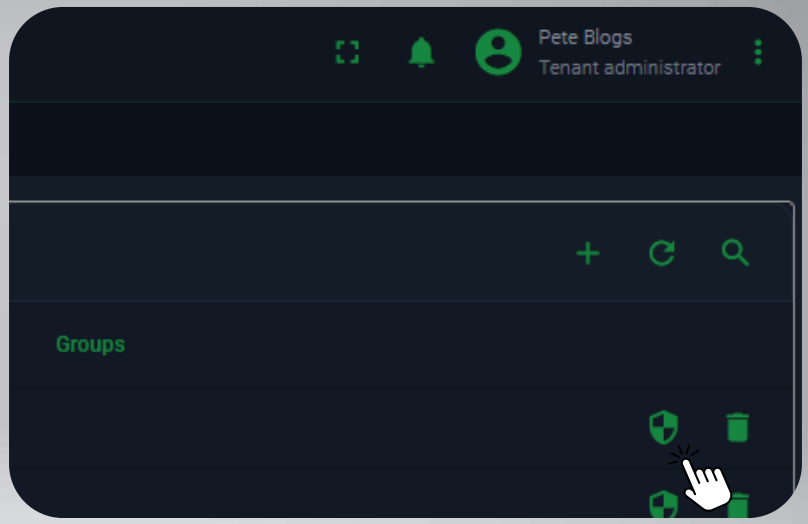
Important:
Credentials can be added during device setup or later.To add them later, click the shield icon beside the device and enter the Client ID, username and password. These credentials must match those entered in the PassPort Gateway 3DM Node-RED node, or the gateway will not connect correctly.

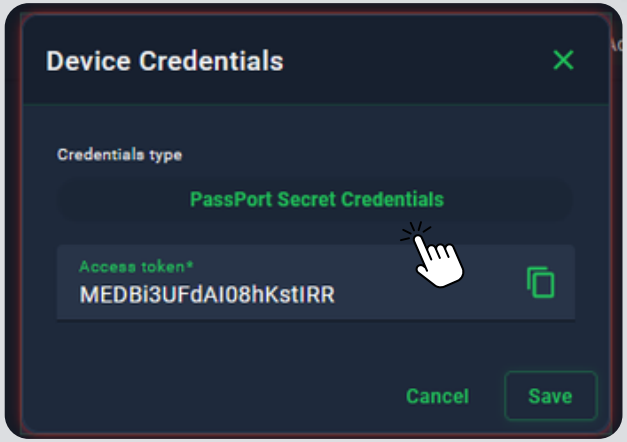
 © 2026 Smithtek Pty Ltd. All rights reserved.

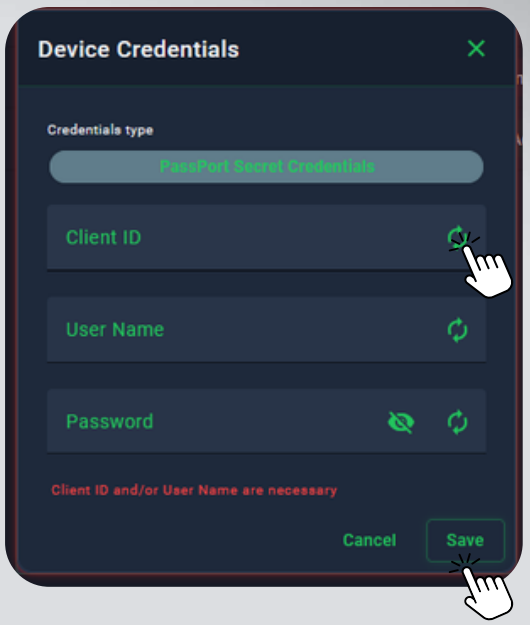
Creating a PassPort Gateway (Device)

How to add Device credentials after a PassPort Gateway has already been created.

1. Go to the **device list.**
2. **Find** the **device** you want to update.
3. Click the **shield icon** beside the device. This is located near the trash can icon.
4. Click **PassPort secret credentials**. Ignore Access token. This is for future API features and is not used for the standard PassPort Gateway setup.
5. In the credentials window, add the device credentials: **Client ID, Username, Password.** These credentials can be entered manually, or created using the automatic generator.
6. Click **Save**.



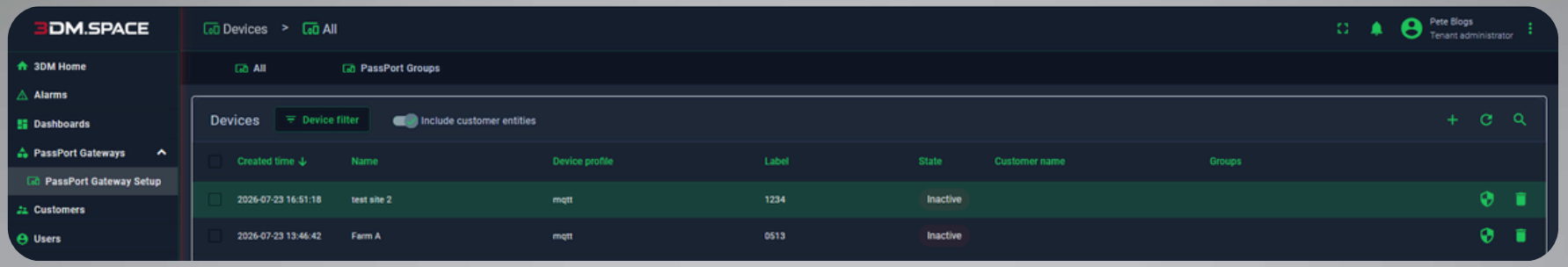




 © 2026 Smithtek Pty Ltd. All rights reserved.

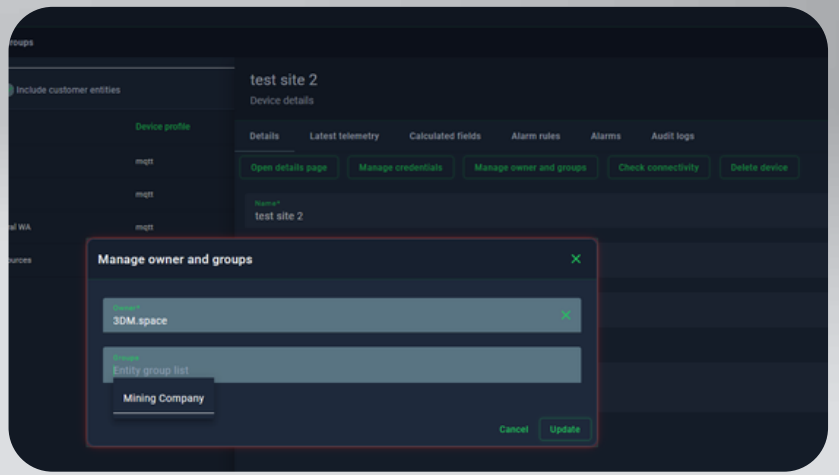
SMITHTEK

3DM Moving Devices into Groups



Moving a device into a device group

Use this method when a PassPort Gateway already exists and needs to be placed into the correct device group.



Steps

1. Go to **PassPort Gateway Setup** in the side navigation bar.
2. Click **All.** The full device list will open. This table shows all PassPort Gateways in the account. It also shows which group or groups each device belongs to.
3. **Find** the **device** you want to move into a group. **Example:** “test site 2” or “Kalgoorlie Resources”.
4. **Click** the **device** to open its details panel.
5. Click **Manage owner and groups**. The Manage owner and groups window will open.
6. Check the **Owner field**. The owner will usually be 3DM.Space or the tenant owner.
7. In the **Groups field**, select the **device group** you want to move the device into. **Example:** “Mining Company”.
8. **Remove** any old group if the device should no longer belong there.
9. Click **Update**. **The device will now appear inside the selected device group.**

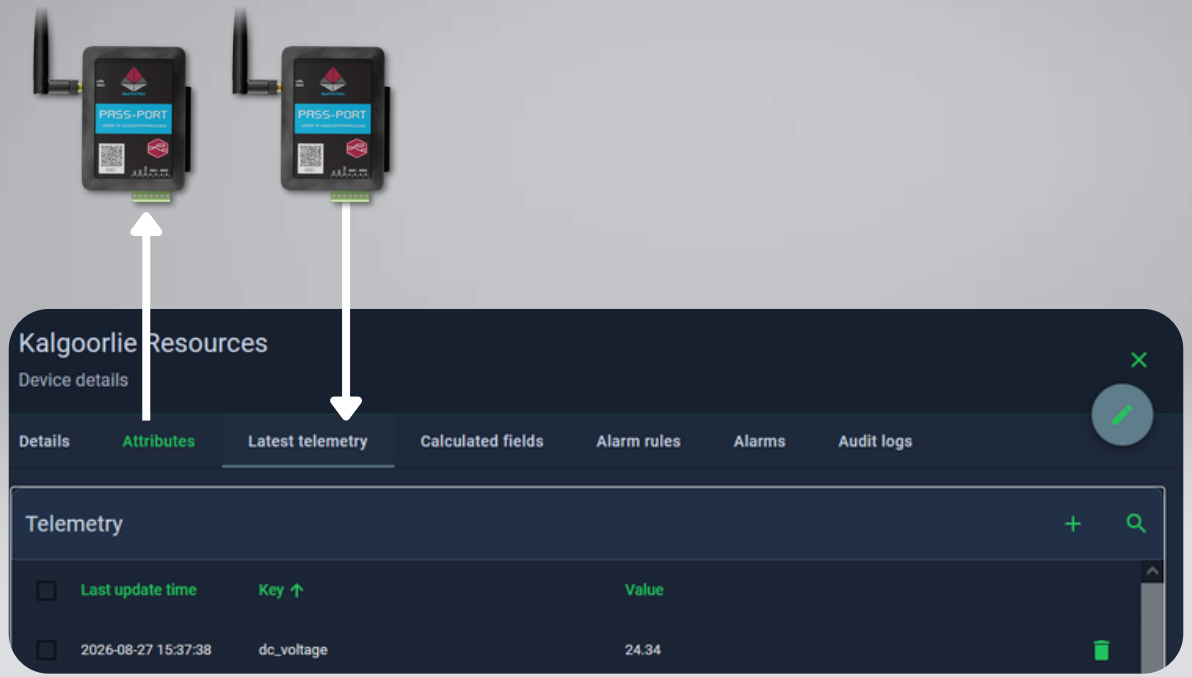
Important:
A device can belong to one or multiple device groups.
If it should only belong to one group, check the Groups field and remove any unnecessary groups. Use this option to move an existing PassPort Gateway into the correct device group.

Simple rule:
PassPort Gateway Setup → All = find existing devices
Manage owner and groups = choose where the device belongs
Device group = where PassPort Gateways are organised

 © 2026 Smithtek Pty Ltd. All rights reserved.

Sending and Receiving Telemetry Data

Sending and receiving data between the PassPort and 3DM is achieved by using **Latest telemetry** and **Attributes.**
Attributes: 3DM sends data to the PassPort. **Latest:** Telemetry PassPort sends data to 3DM.



Latest telemetry
Latest telemetry is live data sent from the PassPort Gateway up to 3DM.Space.
This is the data 3DM.Space reads from the PassPort. Telemetry values are used for dashboards, alarms, trends, status indicators, tables, maps, and live monitoring.

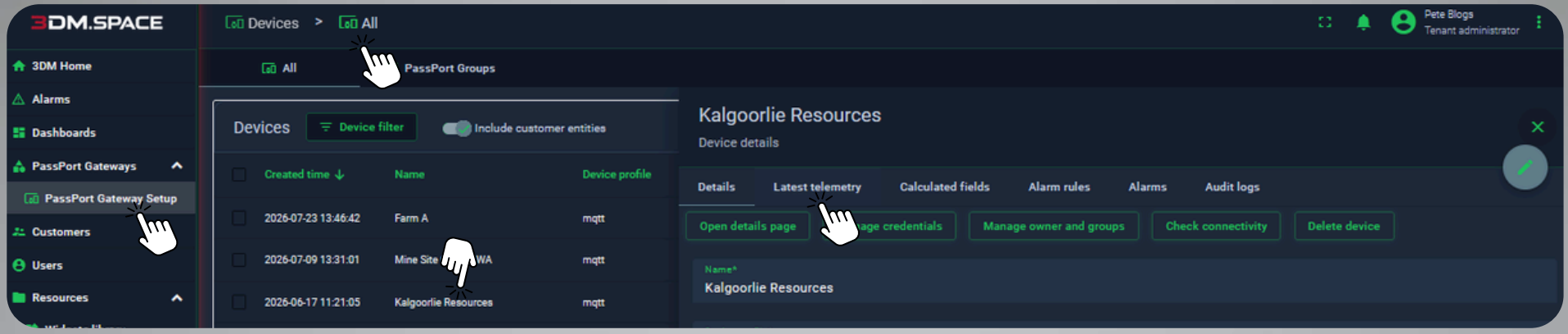
Example:
Tank level, Pump status, Voltage, Flow rate, Pressure, Fault status, Run signal

Attributes
Attributes are stored values that belong to an entity, such as a PassPort Gateway. The most important attribute type for remote control is Shared attributes. Shared attributes are sent from 3DM.Space down to the PassPort Gateway. This is how 3DM.Space sends remote commands to the PassPort,

Example: Start, Stop, On, Off, Setpoint values, Mode changes

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Creating Device Telemetry Variables

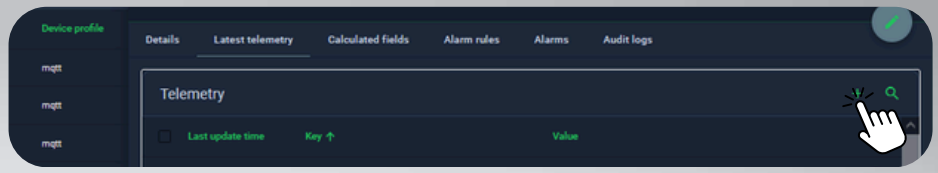


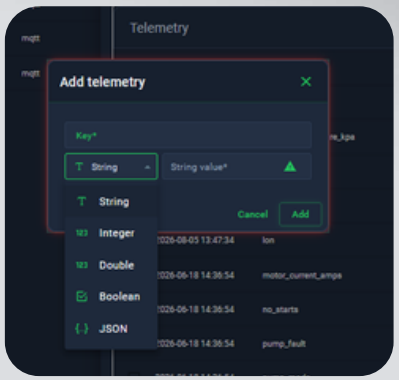
Creating device telemetry variables

Device telemetry variables are the live data values sent from a PassPort Gateway to 3DM.Space. Each value in the JSON telemetry payload becomes a variable that can be:

Viewed under **Latest telemetry.** Displayed on **dashboards.** Used in **alarms.** Used for **control logic**

Examples include tank level, pump status, voltage, flow rate, pressure, fault status and run signals.





Option 1: Creating a telemetry variable manually

Telemetry variables can be created directly from the device Latest telemetry section.

Steps

1. Go to **PassPort Gateway Setup**.
2. Click **All**.
3. **Find** and click the **PassPort Gateway** you want to edit.
4. Click the **Latest telemetry tab**.
5. Click the **+ button** to add a **new telemetry variable**.
6. Enter the **new key name**. The key name is the chosen name for the variable.
   Example: tank_level, pump_status, voltage, or flow_rate.
7. Select the **data type. Example:** String, Integer, Double, Bool, or JSON.
8. **Add a payload value** if required.
9. Click **Add. The new telemetry variable will now appear in the device telemetry list.**

Supported Data Types

String ● Integer ● Double ● Boolean ● JSON

Creating Device Telemetry Variables

Option 2: Creating telemetry variables from Node-RED
The most common way to create telemetry variables is by sending the telemetry payload from the PassPort Gateway Node-RED flow into the 3DM Node-RED node. When the telemetry payload is sent to 3DM.Space, the platform will automatically receive the data and create the telemetry variables. This is usually the quickest method because variables are created as the data is transmitted from the PassPort Gateway.

Important:
Creating variables manually is useful for adding control variables, testing values, or creating ad-hoc variables when required. Sending telemetry through the PassPort Gateway Node-RED 3DM node is the most common method for normal site data because it automatically creates and updates telemetry values in 3DM.Space.

Simple rule:
Telemetry variable = live data value
Key name = variable name
Data type = value format
Manual creation = good for control or ad-hoc variables
Node-RED telemetry = fastest way to create live data variables

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating Device Telemetry Attribute Variables

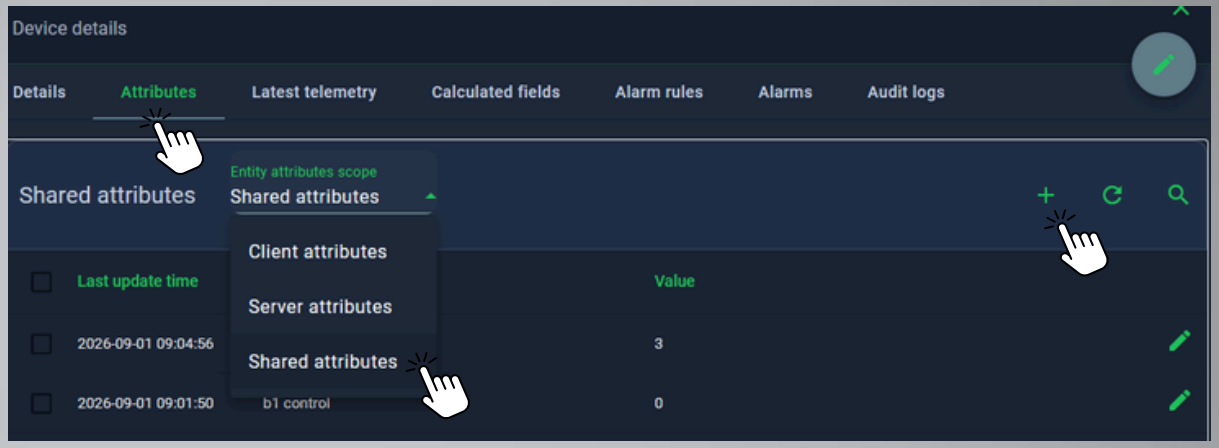
Attributes are stored values that belong to an entity in 3DM.Space, such as a PassPort Gateway, user, customer, asset, or dashboard. Attributes are commonly used for setup values, configuration values, and remote command values.
The main attribute types are:

Shared attributes

Shared attributes are used to send values from 3DM.Space down to the PassPort Gateway.
These are what we use for remote commands, such as sending start, stop, on, off, or setpoint values to the PassPort so it can control connected equipment.

Server attributes

Server attributes are stored inside 3DM.Space.
These are useful for platform-side values such as setup notes, labels, limits, site information, or internal reference values.

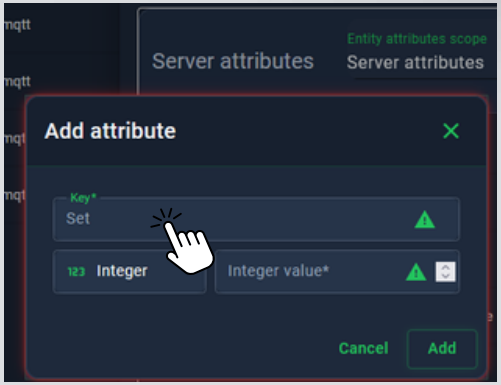


Option 1: Creating a telemetry Attribute manually

Attribute variables can be created directly from the device Attribute section.

Steps

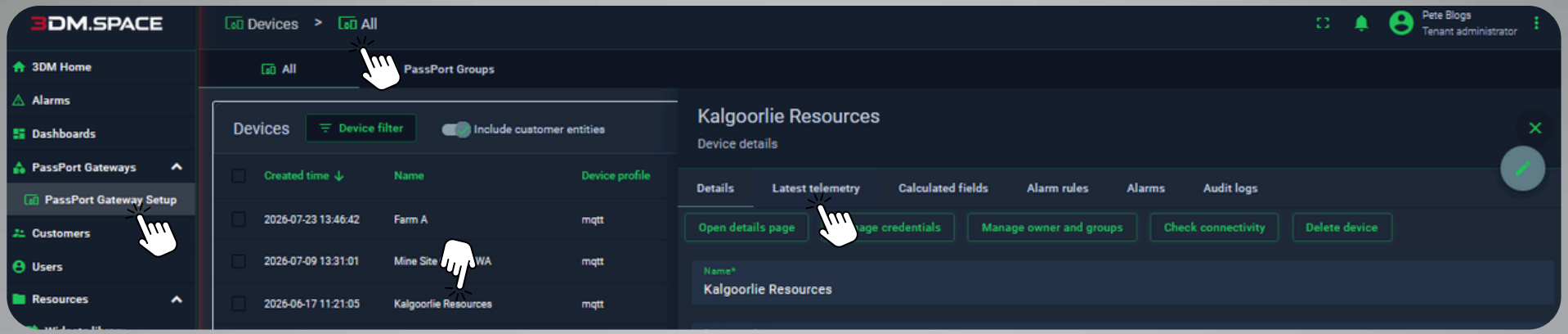
1. Go to **PassPort Gateway Setup**.
2. Click **All**.
3. **Find** and click the **PassPort Gateway** you want to edit.
4. Click the Attributes **tab**.
5. Select the attribute type: *Shared* or *Server*
6. Click the **+ button** to add a **new attribute variable**.
7. Enter the **new key name**. The key name is the chosen name for the variable.
   Example: “pump_control” “setpoint_send”
8. Select the **data type. Example:** String, Integer, Double, Bool, or JSON.
9. **Add a payload value** if required.
10. Click **Add. The new Attribute variable will now appear in the device attribute list.**



Supported Data Types

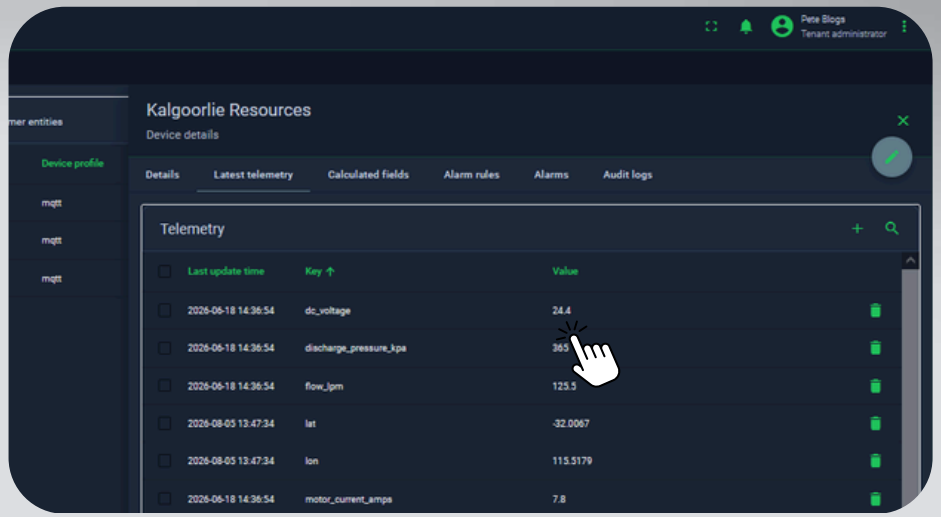
String ● Integer ● Double ● Boolean ● JSON

 © 2026 Smithtek Pty Ltd. All rights reserved.



Viewing device data

Device data can be viewed from the selected PassPort Gateway details panel. This is useful for checking whether the PassPort Gateway is sending data into 3DM.Space and confirming that telemetry values are updating correctly.



Steps

1. Go to **PassPort Gateway Setup** in the side navigation bar.
2. Click **All.** The full device list will open.
3. Find the **PassPort Gateway** you want to check. **Example:** “Smiths Farm PassPort” or “Pump Station 1 PassPort”.
4. Click the **device** to open its details panel.
5. Click the **Latest telemetry tab**. The latest telemetry table will show the most recent data received from the device.
6. Check the **telemetry keys**, **values**, and **timestamps**.

The telemetry values shown here are the latest values received by 3DM.Space from the PassPort Gateway.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Important:

If telemetry is not showing, first check the device State:

Active means the PassPort Gateway is online and communicating with 3DM.Space. Inactive means it is offline or has not communicated recently. Also check the latest telemetry timestamp to see when data was last received, and confirm the device credentials match those entered in the PassPort Gateway 3DM Node-RED node. Old telemetry values may indicate the gateway was previously connected but is no longer sending new data.

Telemetry Table Options

The Latest telemetry tab shows the variables currently being received from the PassPort Gateway.

Add variable

The + icon is used to add a new variable manually if required.

Search variable

The magnifying glass icon is used to search for a variable in the telemetry list. This is useful when the device has many telemetry values.

Delete variable

The trash can icon is used to delete a variable from the telemetry list. Use this carefully, as deleting a variable removes it from the displayed telemetry list.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Variable Data Sizes and Transmission Frequency

Telemetry Data Limits

3DM.space device plans are designed for regular telemetry updates while allowing flexibility for real-world communications, including temporary outages and store-and-forward recovery.

Data Transmission

Each device plan is designed around:

- 1 telemetry transmission per minute
- Approximately 100 telemetry values per transmission
- Continuous operation, 24 hours a day

A telemetry value is an individual piece of data such as tank level, pressure, flow, temperature, pump status or battery voltage.

100 values is an average guide, not a requirement for every message. Some messages may contain fewer values and others may contain more.

Monthly Data Guide

At one transmission every minute, a single device will normally send approximately:

- 1,440 messages per day
- 43,200 messages in a 30-day month
- Around 4.32 million telemetry values per month when averaging 100 values per message

The device plan includes additional capacity above normal operation to accommodate variations in message size and communications.

Store-and-Forward Bursts

PassPort Gateways can store telemetry when the internet connection is unavailable.

When communications are restored, stored data may be transmitted to 3DM in a short burst rather than waiting one minute between each historical message.

This allows the system to catch up quickly while retaining the original telemetry timestamps.

Store-and-forward bursts do not increase the monthly data allowance. They simply allow previously stored data to be delivered faster when the connection returns

Important Note

The one-minute transmission rate is intended for normal site monitoring. Sending data significantly faster, continuously transmitting unusually large messages, or generating unnecessary telemetry can consume the available data allowance more quickly. Only send values that are useful for monitoring, alarms, control or historical records.

Simple Rule

Transmission rate = normally once per minute
Telemetry value = one individual data point
Typical message = approximately 100 telemetry values
Typical monthly usage = approximately 4.32 million values per device
Store-and-forward = stored data can catch up in short bursts
Monthly allowance = bursts do not provide additional monthly data

 © 2026 Smithtek Pty Ltd. All rights reserved.

Node-RED Connection

Node-RED Connection

Your PassPort Gateway uses Node-RED to manage data between field devices, local logic and 3DM.space.

New PassPort Gateways are supplied with the Smithtek 3DM.space Node-RED nodes already installed, so in most cases no additional installation is required.

Older PassPort Gateways may not have the 3DM.space nodes installed. These can be added directly through the Node-RED Palette Manager.

Installing the 3DM.space Nodes

If the Smithtek 3DM.space nodes are not visible in your Node-RED palette:

1. Open the Node-RED Flow Editor.
2. Select the menu in the top-right corner.
3. Select Manage palette.
4. Open the Install tab.
5. Search for:

node-red-contrib-3dm-space

1. Select Install.
2. Allow the installation to complete.
3. Return to the Flow Editor and locate the 3DM.space nodes in the node palette.

Once installed, the 3DM.space nodes can be dragged directly into your Node-RED flows.

Internet Connection

A reliable internet connection is required for the PassPort Gateway to send and receive data between Node-RED and 3DM.space.

The connection does not need to be extremely fast, however it should be stable enough to support regular telemetry transmission and remote commands.

Poor or intermittent internet may result in:

- Delayed telemetry updates
- Delayed commands from 3DM.space
- Temporary connection loss
- Stored telemetry being sent once the connection is restored

Where store-and-forward is configured, telemetry can continue to be stored locally during an internet outage and transmitted once communications return.

Local Node-RED flows can continue operating independently of the cloud, provided the flow itself does not rely on an active internet connection.

Important Note

Most PassPort Gateways will already have the node-red-contrib-3dm-space package installed.

Only use the Palette Manager installation process if the 3DM.space nodes are missing from the Node-RED palette.

After installing or updating the node package, check that the required 3DM.space nodes are visible before building or modifying the flow.

Simple Rule

New PassPort = 3DM.space nodes already installed

Older PassPort = install the package through Palette Manager if required

Package name = node-red-contrib-3dm-space

Internet connection = required for communication with 3DM.space

Local Node-RED logic = can continue running without cloud access

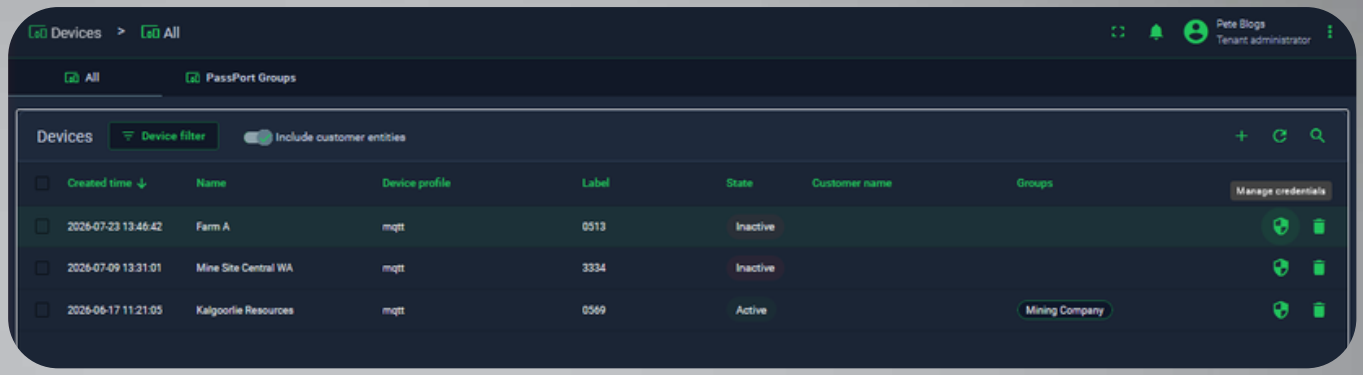
Store-and-forward = holds telemetry during an outage and sends it when the connection returns

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Management Settings

Device management settings

Device management settings are managed from the main Devices list. To access this area, go to PassPort Gateway Setup, then click All. This page shows all PassPort Gateways in the account and provides quick action buttons for adding devices, filtering the device list, refreshing the table, searching for devices, managing credentials, and deleting devices.



Add device

The + icon is used to add a new PassPort Gateway.

Refresh

The refresh icon reloads the device list. Use this if a device has just been added or changed and the list needs to update.

Search

The magnifying glass icon is used to search the device list. Use this to quickly find a PassPort Gateway when there are multiple devices in the account.

Device filter

The Device filter option can be used to filter the device list. This is useful when searching through a large number of PassPort Gateways.

Include customer entities

The Include customer entities toggle changes what is shown in the device table. When enabled, the table may also show devices connected to customer entities.

State

Shows whether the PassPort Gateway is currently active or inactive. Active means the PassPort Gateway is online and communicating with 3DM.Space. Inactive means the PassPort Gateway is offline or has not communicated with 3DM.Space recently.

Customer name

Shows the customer linked to the device, if applicable.

Manage credentials

The shield icon opens the device credentials. This is where the Client ID, username, and password are managed. These credentials are used to link the PassPort Gateway Node-RED 3DM node to the correct device in 3DM.Space.

Delete device

The trash can deletes the device. Use this carefully, as deleting a device may affect telemetry, dashboards, alarms, and any setup connected to the corresponding PassPort .

Simple rule:
+ = add device
Refresh = reload device list
Search = find a device
Device filter = narrow the device list
Shield = manage credentials
Trash can = delete device
State = active or inactive device connection

Important:
The State column is useful for checking whether a PassPort Gateway is online. If dashboard data is not updating, check whether the device is Active or Inactive, then check the latest telemetry timestamp and device credentials.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Device Details

Device settings tabs

Details

Shows the main device information, such as name, device profile, label, description, and device group information. This is the main tab used when checking or editing a device.

Latest telemetry

Shows the latest telemetry values received from the PassPort Gateway. This is useful for checking live data, timestamps, and whether the device is sending data correctly.

Calculated fields

Shows calculated fields connected to the device. These may be used for advanced calculations or derived values.

Alarm rules

Shows alarm rules connected to the device. This is used when alarms are configured from device telemetry.

Alarms

Shows alarms related to the device. This can be useful for checking whether the device has active or historical alarms.

Audit logs

Shows changes and activity related to the device. This can be useful for checking when a device was edited, when settings were changed, or who made a change.

Device action buttons

The device details area includes several action buttons. These buttons are used to manage the selected PassPort Gateway and the items connected to it.

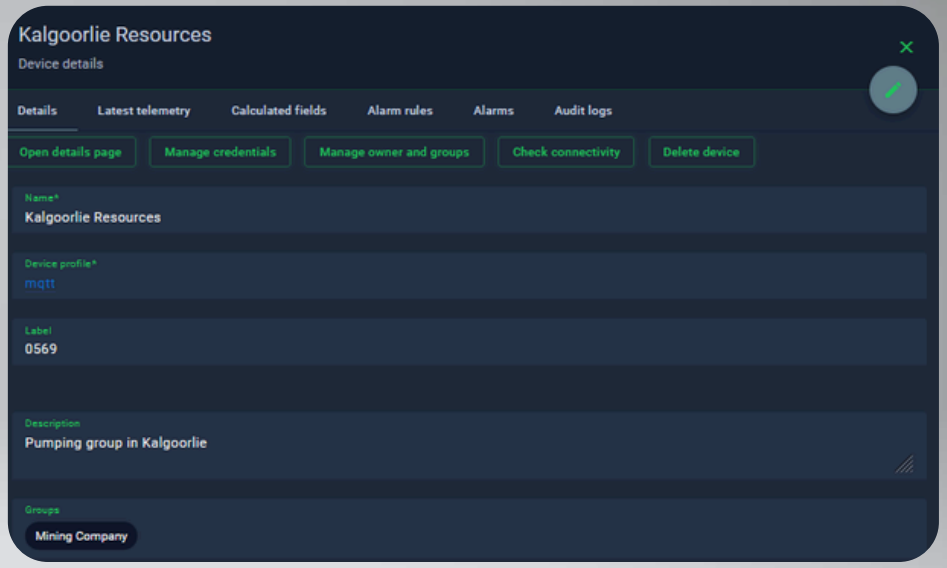
Open details page

Opens the full details page for the selected device.

Manage credentials

Opens the device credentials for the selected PassPort Gateway.

This is where the Client ID, username, and password are managed. These credentials are used to link the PassPort Gateway Node-RED 3DM node to the correct device in 3DM.Space.



Manage owner and groups

Opens the owner and group settings for the device. This is where the device can be moved into a different device group if required.

Check connectivity

Checks whether the device has been configured properly.

Delete device

Deletes the selected device. Use this carefully, as deleting a device may affect telemetry, dashboards, alarms, and any setup connected to that PassPort Gateway.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Device details fields

The lower section of the Details tab shows the device information stored against the selected PassPort Gateway.

Name

The device name shown in 3DM.Space. **Example:** “Kalgoorlie Resources”, “Smiths Farm PassPort”, or “Pump Station 1 PassPort”.

Device profile

Shows the communication profile used by the device. For standard PassPort Gateway setups, this is usually mqtt.

Label

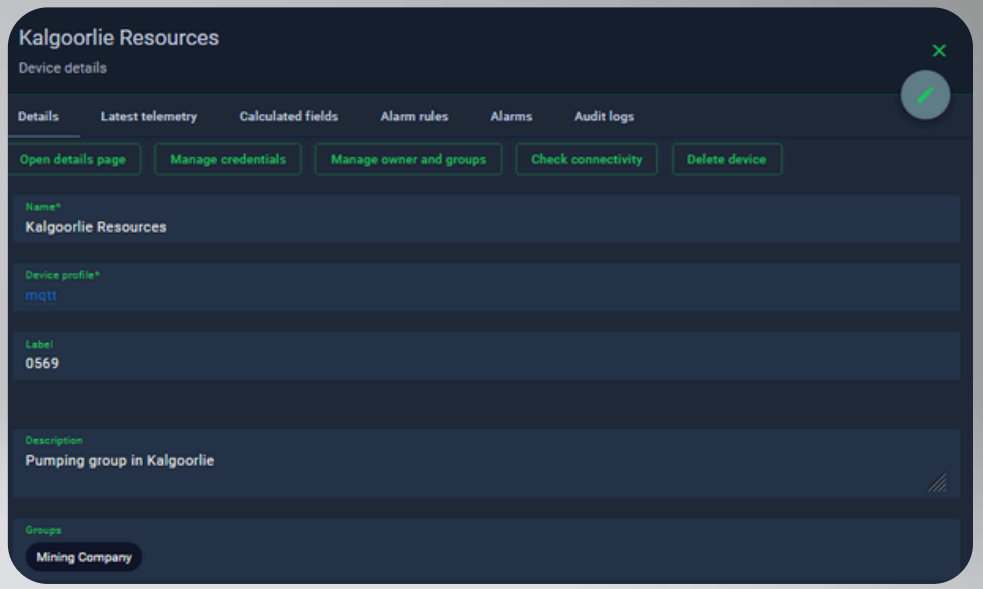
An optional label or ID used to identify the device. **Example:** “0569”.

Description

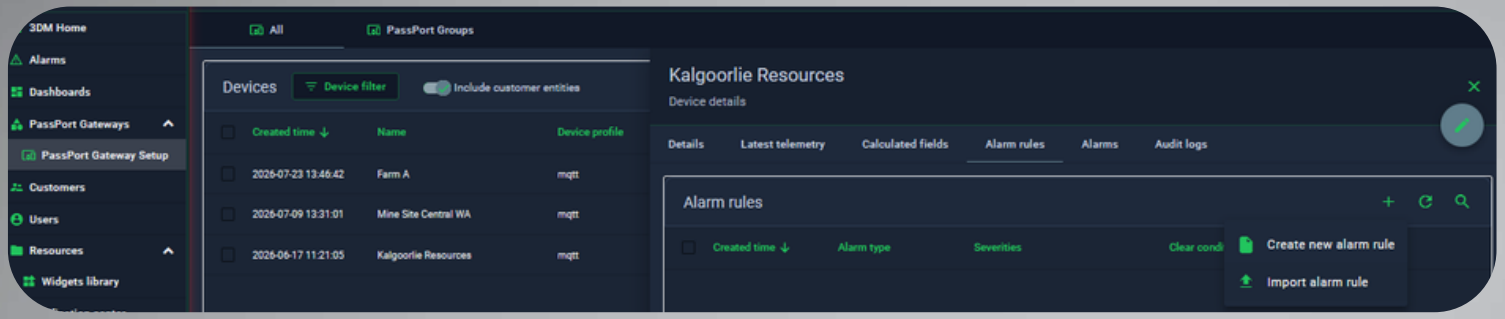
Optional notes about the device. **Example:** “Pumping group in Kalgoorlie.”

Groups

Shows which device group or groups the device belongs to. **Example:** “Mining Company”.



 © 2026 Smithtek Pty Ltd. All rights reserved.



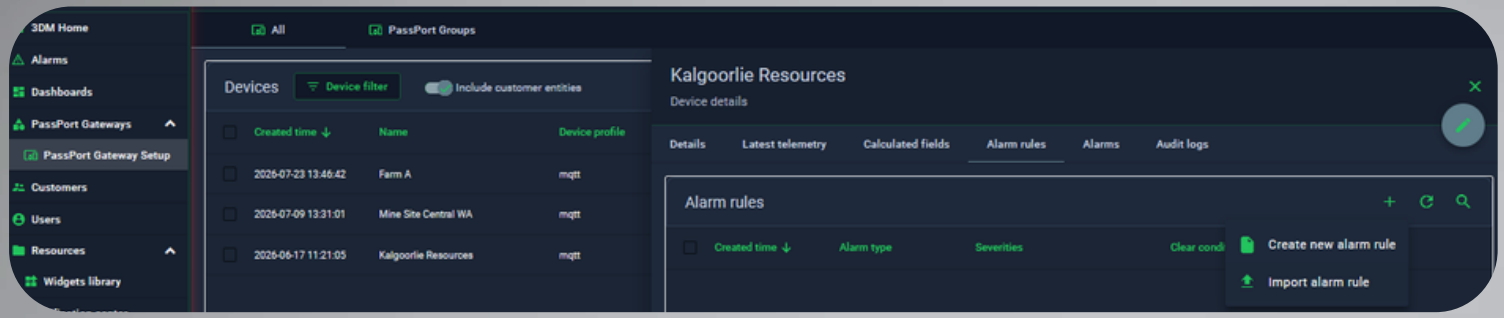
Alarms

Alarms are used to alert users when something on a site needs attention. In 3DM.Space, alarm rules can be created against a PassPort Gateway from the Alarm rules tab inside the selected device. This keeps alarm setup close to the device data being monitored. An alarm rule watches selected data and creates an alarm when the configured condition is met. Alarm rules can also include a clear condition, which decides when the alarm returns to normal.

Alarms can be used for many site conditions, such as:

Low tank level
Used when a tank level drops below a set point.
High tank level
Used when a tank level rises above a set point.
Pump fault
Used when a pump fault signal becomes active.
Low voltage
Used when a PassPort Gateway, battery, or connected system voltage drops too low.
Device offline
Used when a PassPort Gateway stops communicating with 3DM.Space.

 © 2026 Smithtek Pty Ltd. All rights reserved.



Control activity

Alarm rules can use different data sources:

Latest telemetry – live data from the PassPort Gateway, commonly used for tank levels, pump states, pressure, flow, voltage, faults and other site values.
Server attributes – stored device information such as active status, inactivity alarm time, last activity, last connect and last disconnect.
These are commonly used for offline or communication alarms.
Client attributes – not used in the standard setup covered by this manual.
Shared attributes – values sent from 3DM.Space to the device, such as start, stop, reset or other control commands.
Alarm rules can be used when these values change or are activated.

The entity type will normally remain as This entity, meaning the alarm rule applies to the selected PassPort Gateway.
Other options may be available, but standard device alarms should normally use this setting. This section covers common alarms including device disconnection, level thresholds, low voltage, pump faults, viewing and managing alarms, and troubleshooting.

Simple rule:
Alarm rule = watches data
Condition = decides when alarm starts
Clear condition = decides when alarm returns to normal
Latest telemetry = live site data
Server attributes = device activity and connection information
Shared attributes = values that may be sent to the device
Device alarm rules = alarms attached to the selected PassPort Gateway

Important:
The number of alarms you can configure and send and the frequency depends on your account plan. Please discuss your allowance with your Smithtek account Manager.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Where Alarm Rules Can Be Created and Viewed

Alarm rules and alarms can be accessed from two main areas in 3DM.Space.

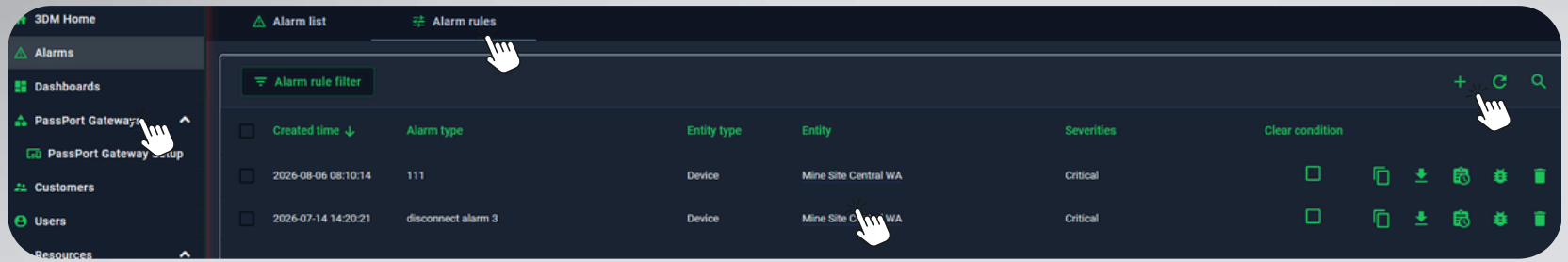
- **Main Alarms menu** - Used to view alarms across the account, including active and historical alarms for devices the user has permission to access.
- **PassPort Gateway Setup** - Used to create and manage alarm rules for a specific PassPort Gateway.

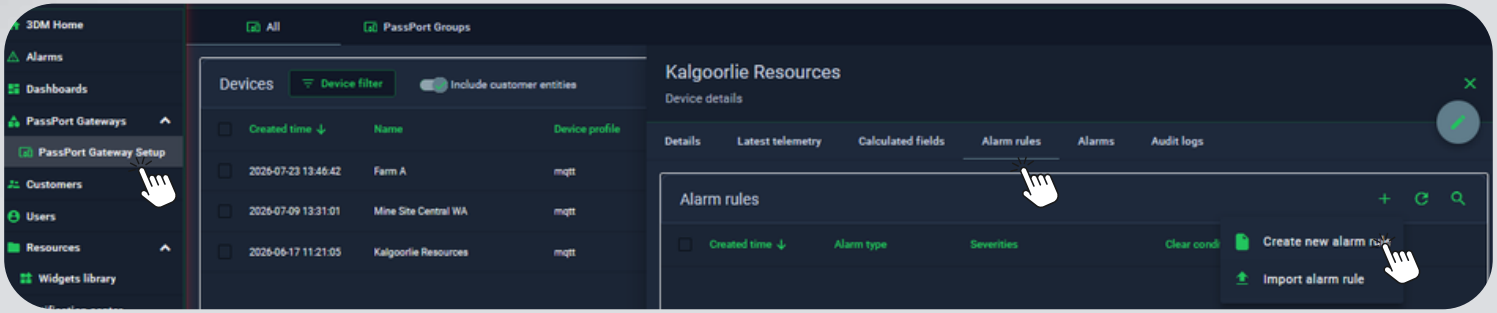
Steps

1. Go to **PassPort Gateway Setup**.
2. Click **All**.
3. Select the required PassPort Gateway.
4. Open the **Alarm rules tab**.

From here, alarm rules can be created, imported, edited or reviewed. The device Alarms tab shows alarms that have been generated for that PassPort Gateway. **In simple terms:** Use the main Alarms menu to view alarms across the platform, and the device Alarm rules tab to create and manage rules for a specific PassPort Gateway.

Simple rule:
Alarms menu = view alarms across the account
PassPort Gateway → Alarm rules = create or edit alarm rules for that device
PassPort Gateway → Alarms = view alarms for that device





 © 2026 Smithtek Pty Ltd. All rights reserved.

Where Alarm Rules Can Be Created and Viewed

Creating an alarm rule from a PassPort Gateway

Alarm rules can be created directly from a selected **PassPort Gateway.** This is the preferred method in this manual because the alarm rule is being created against the device that is sending the data. An alarm rule watches incoming data from the PassPort Gateway and creates an alarm when the selected condition is met.



Incoming message
The incoming message is the telemetry data received by 3DM.Space, usually from the PassPort Gateway.

Example:

flow_rate
tank_level
pump_fault
battery_voltage
pump_running

These values can then be used in an **alarm rule.**

Arguments
An argument is the telemetry value 3DM.Space will monitor in the alarm rule. Arguments use telemetry keys sent from the PassPort Gateway. You can add the required telemetry variables as arguments, then select which ones to use in the trigger condition.

Example:

"flow_rate": 3500
The alarm rule can use flow_rate as the argument.

Common arguments include:
flow_rate – flow alarms
tank_level – low or high level alarms
battery_voltage – low voltage alarms
pump_fault – pump fault alarms

Trigger Condition
The trigger condition tells 3DM.Space when to create the alarm by comparing an argument against a set value.

Example:

flow_rate <= 4000
Creates an alarm when the flow rate is 4000 or below.
tank_level < 2000
Creates an alarm when the tank level drops below 2000 mm.

Trigger conditions can also use **AND** or **OR** logic.

Example:
flow_rate <= 4000 AND pump_running = true
This creates an alarm when the pump is running and the flow rate is too low.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Where Alarm Rules Can Be Created and Viewed



Alarm rule types
When creating an alarm rule, there are three main alarm types that may be used: **Simple**, **Duration**, and **Repeating**.

Simple alarm
A simple alarm is created as soon as the trigger condition is met. **Example:** If tank_level < 20, the alarm is created immediately.*This is useful for direct alarms such as pump fault, low tank level, high pressure, or low voltage.*

Duration alarm
A duration alarm is only created if the trigger condition remains true for a set amount of time. **Example:** If flow_rate <= 4000 for 5 minutes, create the alarm. *This is useful when you do not want short spikes, dips, or temporary signal changes to create alarms.*

Repeating alarm
A repeating alarm continues to trigger or update while the alarm condition remains active. **Example:** If a device remains offline, the alarm can keep repeating at a set interval until the condition clears. *This is useful for important alarms that should keep reminding users until the issue is fixed.*

Clear Condition
The clear condition tells 3DM.Space when to clear the alarm after the value returns to a safe range. This is optional.

Example:

tank_level < 2000
Creates the alarm.
tank_level > 3000
Clears the alarm.

Using a different clear value helps prevent the alarm from repeatedly switching on and off when the value is close to the alarm limit.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Where Alarm Rules Can Be Created and Viewed

Alarm rule schedule
The alarm rule schedule controls when the alarm rule is active.
By default, the schedule is usually set to Static and Active all the time. This means the alarm rule is always running and will check the alarm condition whenever data is received.

Static schedule
A Static schedule uses fixed time settings.

Active all the time
The alarm rule is always active. This is the most common setting for important alarms such as device offline, pump fault, low voltage, or critical tank level alarms.

Active at specific times
The alarm rule is only active during selected times. This is useful when an alarm should only apply during operating hours, irrigation windows, shift times, or site operating periods.

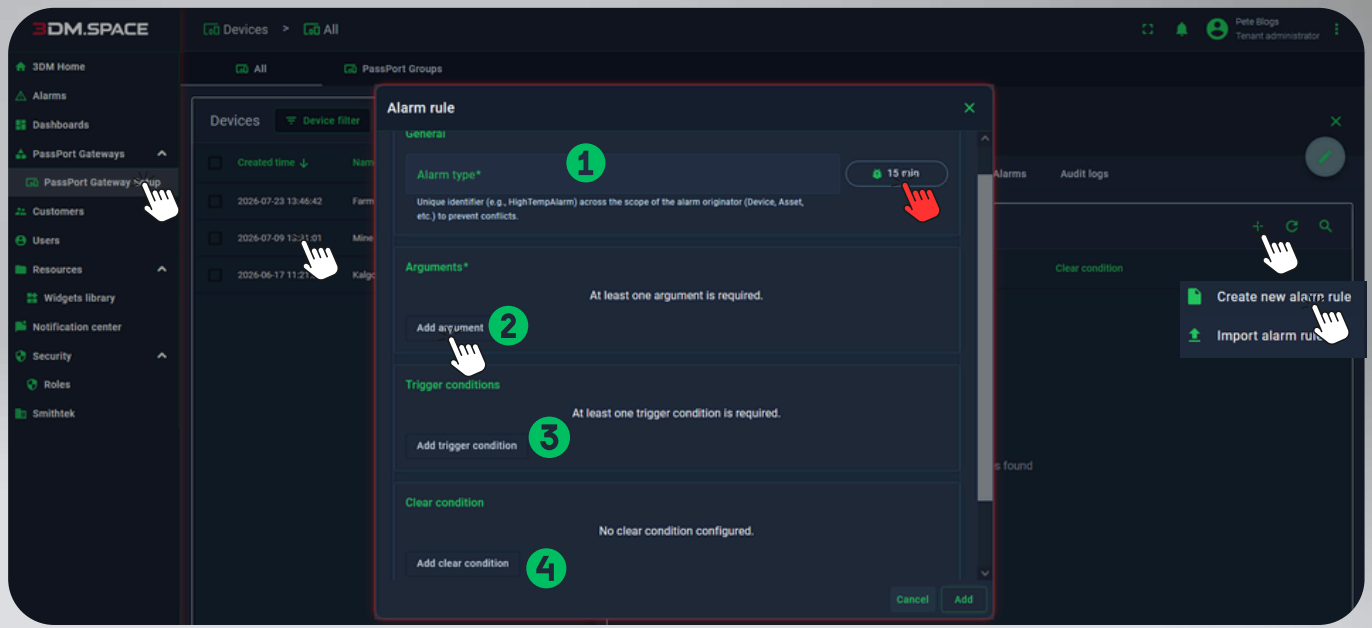
Custom
The custom option allows specific dates and times to be selected. This is useful when an alarm rule should only run during a planned period, temporary project, trial, shutdown, or special operating window.

Dynamic schedule
A Dynamic schedule uses another telemetry variable to turn the alarm rule on or off.
Instead of using fixed times, the alarm rule looks at another value from the device data.
For example, a telemetry variable could be used to enable alarms only when a system is in operation, maintenance mode is off, or a pump station is active.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating your first alarm rule

Alarm rules are created from the selected PassPort Gateway. For this manual, alarm rules will be created from the Alarm rules tab inside a device. This keeps the alarm rule connected to the PassPort Gateway that is sending the telemetry data. This first alarm setup will use Latest telemetry values as the alarm arguments. **These next few pages will teach you how to configure each part of the alarm rule building process and save an alarm.**



Steps

1. Go to **PassPort Gateway Setup** in the side navigation bar.
2. Click **All**.
3. **Find** the **PassPort Gateway y**ou want to create the alarm rule for.
4. Click the **device** to open the device details panel.
5. Click the **Alarm rules tab.**
6. Click the **+ button** to create a **new alarm rule**. Alarm type = Enter a clear alarm rule name. **Example:** “Low Tank Level”, “Low Flow Alarm”, or “Pump Fault Alarm”.
7. Add the **alarm arguments**.
8. Build the **trigger condition**. **Example** combined trigger: low_rate <= 4000 AND pump_running = true
9. Add a **clear condition** if required. **Example:** tank_level > 30
10. Click **Add**. **The alarm rule will now be created against the selected PassPort Gateway.**

DEBUG

Next to the **general Alarm Type** setting, debug mode is enabled by default for 15 minutes. Debug mode tracks events, states and errors while the alarm rule is running, which is useful during setup and testing. Because debug mode can use significant database space, turn it off once the alarm rule has been tested and is working correctly.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Argument source options

When adding an argument, the Entity type decides where the alarm rule gets the value from.

Current entity

Uses data from the current PassPort Gateway the alarm rule is being created on. This is the normal option for device alarms.

Device or Asset

Uses telemetry or attributes from a different device or asset.

Customer

Uses data from the customer entity connected to the device or setup.

Current tenant

Uses data from the main tenant account.

Current owner

Uses data from the owner of the current entity.

For standard PassPort Gateway alarm rules, use Current entity. This means the alarm rule is looking at data from the selected PassPort Gateway.

Alarm severity

Alarm severity shows how serious the alarm is.

This helps operators decide which alarms need urgent attention and which alarms can be reviewed later.

Critical

Used for serious alarms that need immediate action. **Example:** equipment failure, safety risk, shutdown condition, or major system fault.

Major

Used for important issues that affect normal operation, but may not require an immediate shutdown response. **Example:** pump fault, high pressure, or major communication issue.

Minor

Used for lower priority alarms that should be checked, but are not immediately critical. **Example:** early warning level, minor sensor issue, or non-critical fault.

Warning

Used when something may become a problem if it continues. **Example:** tank level getting low, voltage starting to drop, or flow rate moving outside the preferred range.

Indeterminate

Used when the alarm severity cannot be clearly determined.

This may happen if the data is missing, unclear, or does not fit a known alarm level.

Severity is selected inside the alarm rule trigger condition. If an alarm is already active and a new trigger condition fires with a higher severity, the existing alarm severity can be upgraded instead of creating a separate new alarm.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating Your First Alarm - Adding an Argument

Adding an argument settings

Before an alarm rule can check a condition, it needs at least one argument. An argument is the data source the alarm will monitor. For example, if a PassPort Gateway is sending a telemetry key called tank_level, the alarm rule needs that value added as an argument before it can trigger on low or high level conditions.

Fields in the Add argument window

Entity type

This defines where the data is coming from. In most standard PassPort Gateway alarm setups, leave this as Current entity. This means the alarm will use data from the device you are currently setting the alarm rule on.

Argument type

This defines what kind of data the alarm will use. For most live device alarms, choose Latest telemetry. This is used for values such as tank levels, flow rates, pressures, voltages, run signals, fault signals, and other live telemetry variables.

Time series key

This is the exact telemetry variable name being received by 3DM.Space. **Example:** tank_level, flow_rate, pump_fault, or active. This name must match the telemetry key exactly as it appears in the device telemetry list.

Argument name

This is the name used inside the alarm rule. It can be the same as the telemetry key, or it can be a simpler name used for easier reading in the trigger condition.

Example: Time series key = tank_level / **Argument name** = tank_level
or: **Time series key** = train1_ro_status / **Argument name** = ro_status

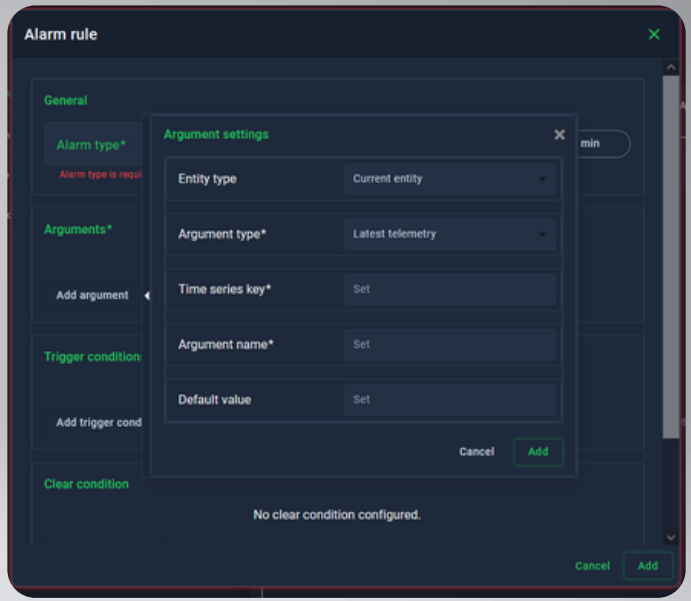
Default value

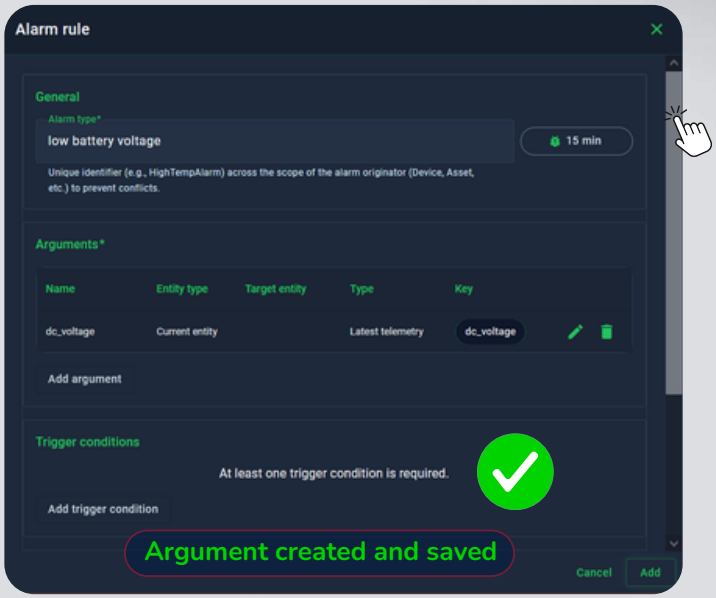
This is optional. It is used if no value is currently available for that argument.
In most basic alarm setups, this can usually be left blank unless a specific fallback value is needed.

Example

If you want to alarm on a low tank level:

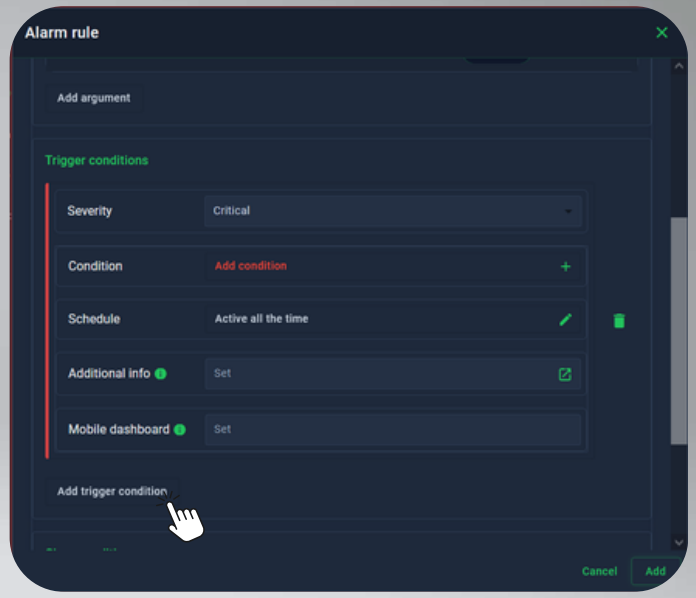
- Entity type: Current entity
- Argument type: Latest telemetry
- Time series key: tank_level
- Argument name: tank_level
- Default value: leave blank or enter a value if required. Click **Add** to **save the argument**.





Trigger condition settings

The Trigger conditions section is where the alarm rule is built. This section decides when the alarm should activate. Before a trigger condition can work, at least one argument must already be added. The trigger condition then uses that argument to check whether the alarm limit has been reached. For example, if the argument is tank_level, the trigger condition may be: tank_level < 20 This means the alarm will activate when the tank level drops below 20.



Trigger condition fields

Severity

Selects how serious the alarm is. **Example:** *Critical - Major - Minor - Warning - Indeterminate*. Choose the severity based on how important the alarm is and how quickly someone needs to respond.

Condition

This is where the alarm rule logic is created. Click the + button beside Add condition to open the condition builder window.This is where you program the actual trigger rule. **Example:** *dc_voltage < 12 or flow_rate <= 4000 or pump_fault = true*

Schedule

Controls when this trigger condition is active. By default, this is usually set to Active all the time. This means the alarm condition is always being checked when data is received.

Additional info

Optional extra information that can be attached to the alarm. This may be used for extra alarm details, notes, or information that may help operators understand the alarm.

Mobile dashboard

Optional setting used if the alarm should link to a specific mobile dashboard. This is not normally required for basic alarm setup.

Adding the trigger rule

To add the trigger rule, click the + button in the Condition row. A new window will open where the trigger logic can be created. This is where you select the argument, choose the comparison, and enter the value. **Example:** *Argument: tank_level - Condition: < - Value: 20 This means: Create an alarm when tank_level is less than 20.*

Add another trigger condition block

You can also click Add trigger condition to create another trigger condition section. This can be used when the same alarm rule needs more than one trigger setup, often with a different severity, schedule, or condition.

Example: Warning trigger: tank_level < 30
Critical trigger: tank_level < 15

An alarm rule can have more than one trigger condition. Use the + button inside the Condition row to build multiple rules inside the same trigger condition, such as using AND or OR logic. Use Add trigger condition to create another trigger condition block inside the same alarm rule.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Add condition settings

To build the alarm rule, click the + button in the Condition row. This opens the Alarm condition window. This is where the trigger rule is created.

Mode

The condition can be built in two ways:

Simple

Used for building the condition manually. This is the normal option for most alarm rules.
Simple mode lets you add argument filters and combine them using AND or OR logic.

Script

Used for writing the condition in script format. This is useful for advanced alarm rules, saved templates, or faster deployment when the same logic is reused across multiple devices.

Argument filters

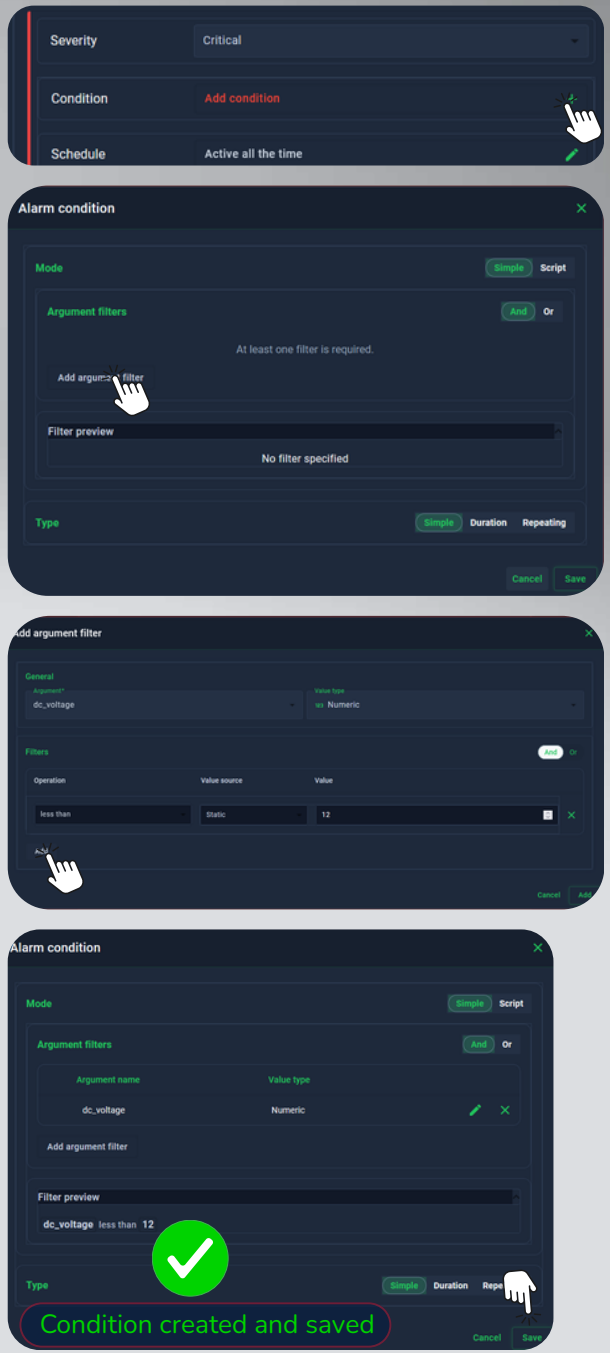
Click Add argument filter to select one of the arguments that was added earlier in the alarm rule.
The argument filter uses that argument to build the trigger condition.
Example: ***Argument:*** *dc_voltage* ***Rule:*** *less than* ***Value:*** *12 This means the alarm condition will become true when dc_voltage is less than 12.*
AND / OR: Use AND or OR when more than one filter is required. AND means all filter conditions must be true. OR means any one of the filter conditions can be true. **Example:** *flow_rate < 5000 lph AND pump_running = true This could indicate the flow rate is low when the pump is running, it could be a burst pipe.*

Filter preview

The Filter preview section shows the condition that has been built. Use this to check the rule before saving.

Type

Select the alarm condition type: Simple - Duration - Repeating
These control how the alarm behaves once the condition is true.
Click Save once the condition has been built.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Creating Your First Alarm - Adding a Clear Condition

Clear condition settings

The Clear condition section is optional. A clear condition is used when the alarm should automatically return to normal after the value goes back into a safe range. The setup process is similar to the trigger condition.

Click the + button in the Condition row to open the Alarm condition window.
Then click Add argument filter to build the clear rule.

Add argument
Select the argument you want to use for the clear condition. **Example:** dc_voltage

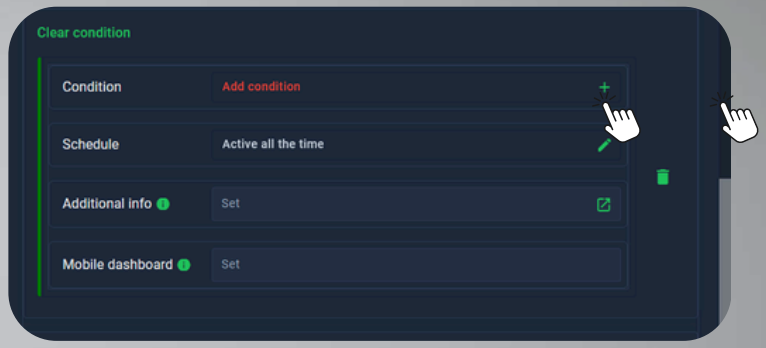
Value type
Select the type of value being checked. **Example:** Numeric

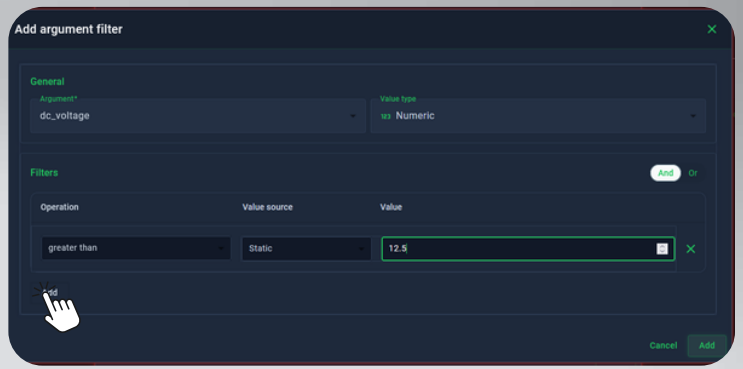
Operation
Select how the value should be compared. **Example:** greater than, less than, equal to, or other available options.

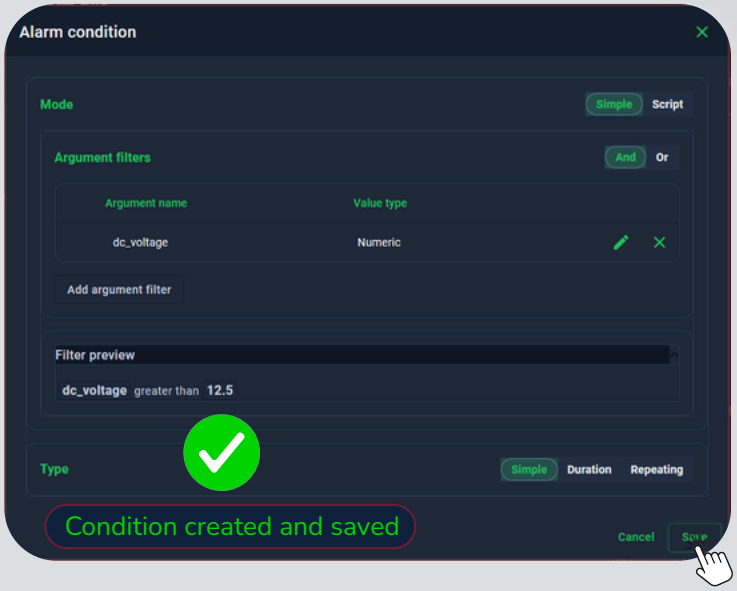
Value source
Select where the comparison value comes from. For basic alarms, this is usually Static.

Value
Enter the value that should clear the alarm. **Example:** 12.5 i.e. If the trigger condition creates a low voltage alarm when: dc_voltage < 11.5. The **clear condition** could be: dc_voltage > 12.5. This means the alarm starts when the voltage drops below 11.5, then clears when the voltage rises back above 12.5.

Important:
The clear condition should normally be set slightly away from the trigger value. This helps stop the alarm from turning on and off repeatedly when the value is sitting close to the alarm.

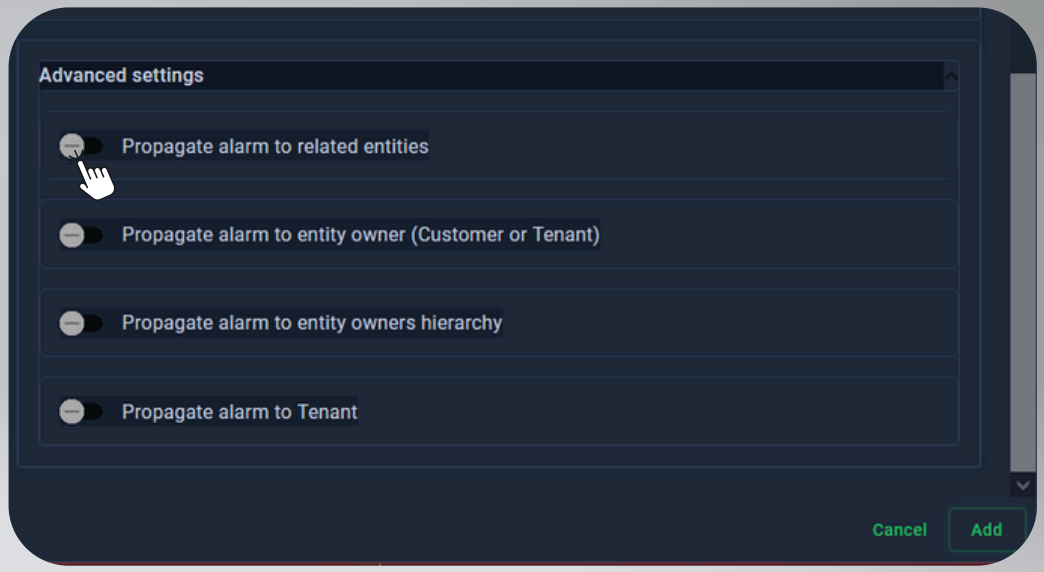






Advanced settings

The Advanced settings section controls where the alarm is visible after it has been created. By default, these options are normally turned off. This means the alarm stays attached to the device that created it. Alarm notifications are still controlled separately through the Notification centre.



Propagate alarm to related entities
Makes the alarm visible to related entities. Use this when the device is linked to another entity, such as an asset, site, system, or parent item, and the alarm should also be visible there. **Example:** A pump fault alarm from a PassPort Gateway may also need to appear against the related pump station asset.

Propagate alarm to entity owner Customer or Tenant
Makes the alarm visible to the direct owner of the device.
Use this when the customer or tenant that owns the PassPort Gateway should also be able to see the alarm. **Example:** A customer-owned PassPort Gateway creates a low tank level alarm, and the alarm should be visible to that customer.

Propagate alarm to entity owners hierarchy
Makes the alarm visible up the ownership chain.
Use this when alarms need to be visible through multiple ownership levels, such as asset, customer, and tenant. **Example:** A device alarm may need to be visible to the site owner, the customer, and the main tenant administrator.

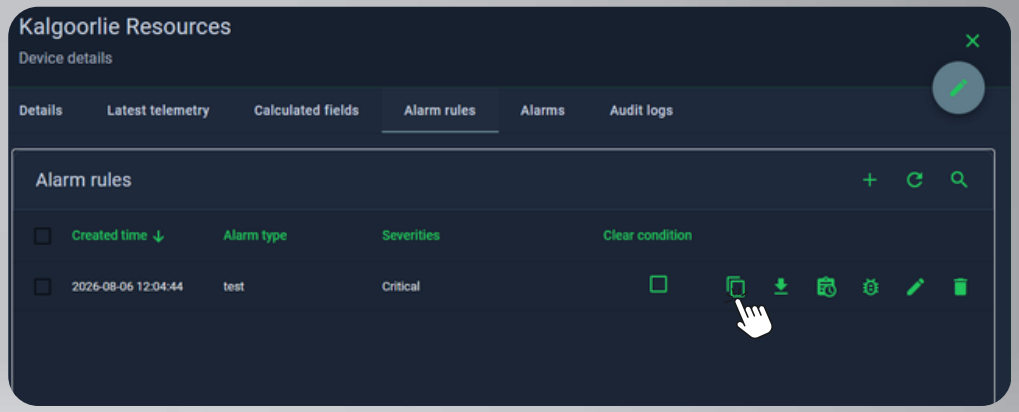
Propagate alarm to Tenant
Makes the alarm visible to the main tenant. Use this when the alarm should always be visible at the tenant level, even if the device belongs to a customer or another owner. **Example:** A critical device offline alarm may need to be visible to the tenant administrator for support or monitoring.

Important:
Propagation controls where the alarm is visible. It does not replace notification rules. To send emails or other alerts, the alarm still needs to be connected to the correct notification setup. Alarm propagation extends alarm visibility beyond the device that triggered it, such as to related entities, owners, owner hierarchy, or tenant level.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Alarms Table Options

Alarm rule table options
The Alarm rules tab shows the alarm rules that have been created for the selected PassPort Gateway. Each alarm rule row includes quick action icons for checking, copying, exporting, testing, editing, or deleting the alarm rule.



Clear condition checkbox
Shows whether a clear condition has been added to the alarm rule.
If the box is ticked, the alarm rule has a clear condition configured.
If the box is not ticked, the alarm may need to be cleared manually or by another rule setup.

Copy alarm rule configuration
Copies the alarm rule configuration. This is useful when you want to duplicate a similar alarm rule and adjust it, instead of building the full alarm again from scratch.

Export alarm rule
Exports the alarm rule configuration. This is useful for backing up an alarm rule, sharing it, or moving alarm rule setup between devices or projects. It exports the rule in JSON format, you can use the Alarm import feature when creating an alarm rule to import it back in. This is ideal for sharing alarms, saving templates for quick deployments.

Events log
Opens the event log for the alarm rule. This can be useful for checking when the alarm rule has triggered, cleared, updated, or changed state.

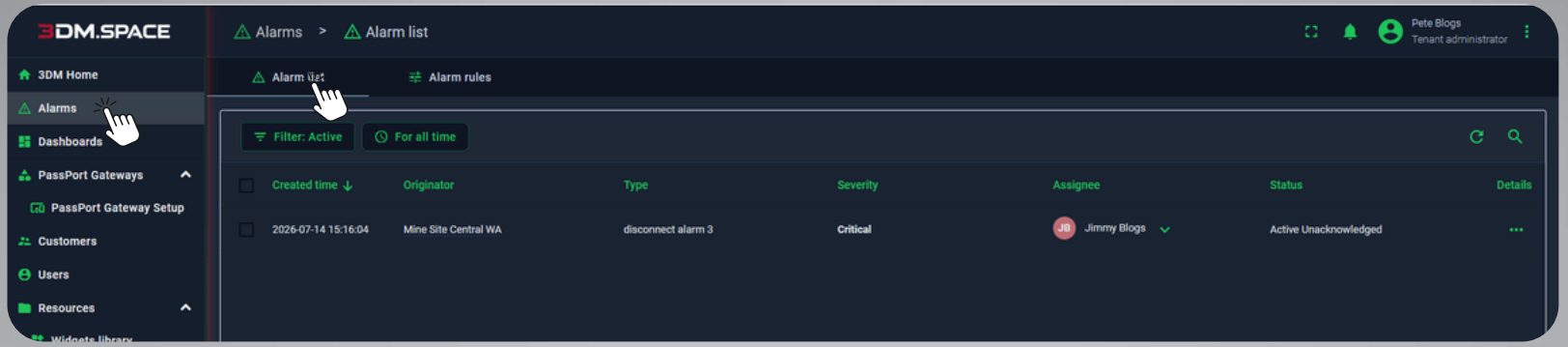
Debug
Opens the debug area for the alarm rule. This is useful for troubleshooting alarm rule behaviour, especially if the alarm is not triggering or clearing as expected.

Edit alarm rule
The pencil icon opens the alarm rule for editing. Use this to change the alarm name, arguments, trigger condition, clear condition, schedule, severity, or advanced settings.

Delete alarm rule
The trash can deletes the alarm rule. Use this carefully. Deleting an alarm rule will stop that alarm rule from running for the selected PassPort Gateway.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Alarms List



Alarm list

The Alarm list is accessed from the side navigation bar.
Go to Alarms, then click Alarm list. This page shows alarms that have been created in the account. It is used to view active alarms, check alarm status, assign alarms to users, and review alarm details.

Alarm list table options

Filter
The filter button is used to narrow the alarm list. **Example:** the list may be filtered to show Active alarms only.

Time range
The time range button controls which alarm period is shown.
Example: For all time shows alarms across the full available history.

Refresh
The refresh icon reloads the alarm list.
Use this if a new alarm has triggered or an alarm status has changed.

Search
The magnifying glass icon is used to search the alarm list.
Use this to quickly find a specific alarm when there are multiple alarms in the account.

Alarm list columns

Created time
Shows when the alarm was created.

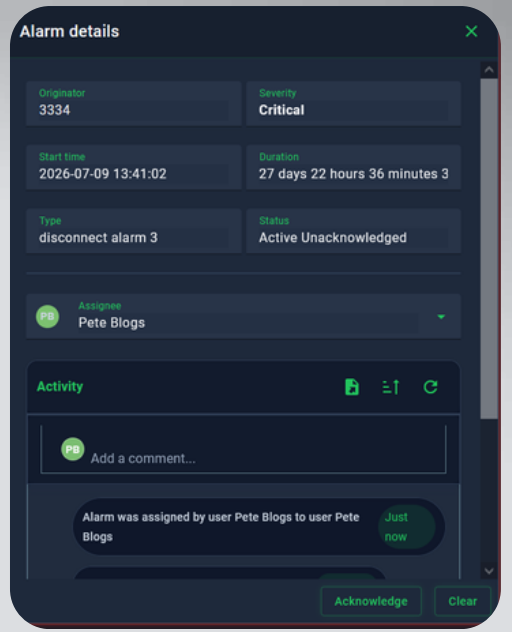
Originator
Shows which device, PassPort Gateway, or entity created the alarm.

Type
Shows the alarm name or alarm type. **Example:** disconnect alarm 3.

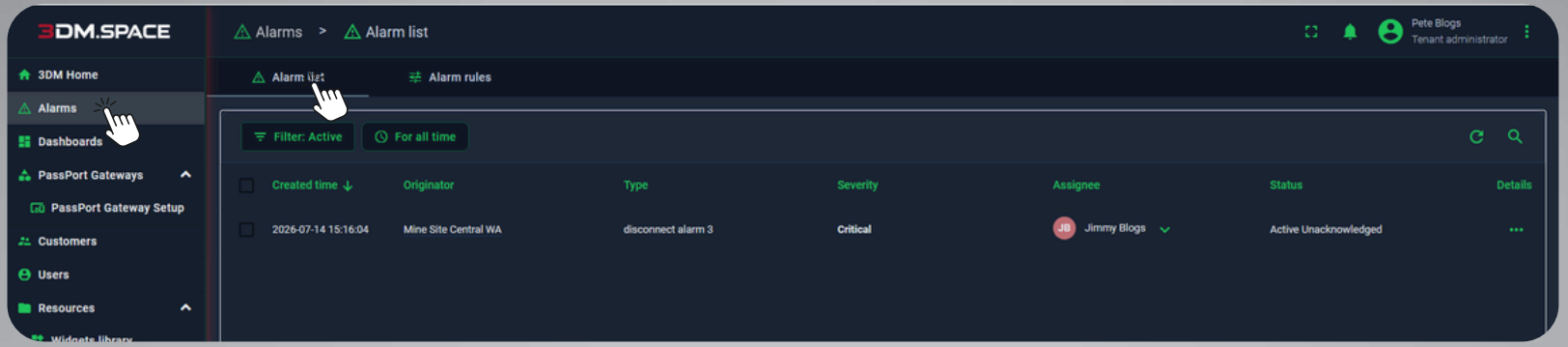
Severity
Shows how serious the alarm is. **Example:** Critical, Major, Minor, or Warning.

Assignee
Shows who the alarm has been assigned to. An alarm can be assigned to a supervisor, technician, operator, or another person responsible for reviewing or actioning the alarm.

Status
Shows the current alarm state. **Example:** Active Unacknowledged. This means the alarm is still active and has not yet been acknowledged.

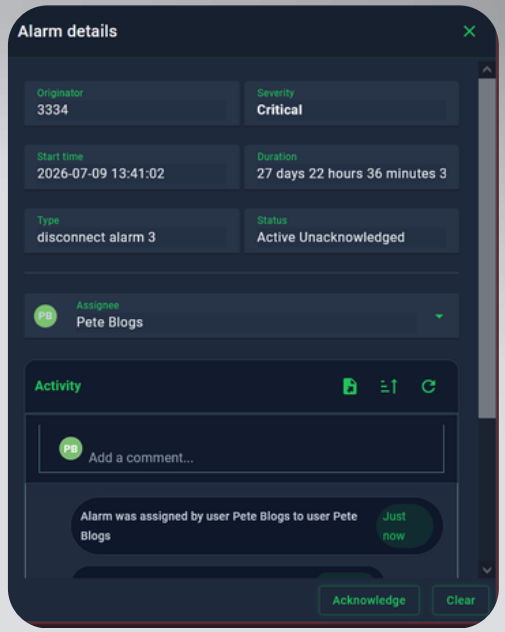


 © 2026 Smithtek Pty Ltd. All rights reserved.



Alarm list actions

The Details three-dot menu opens extra actions for the selected alarm.



Acknowledge alarm

Marks the alarm as acknowledged.

This means someone has seen the alarm and is aware of it. The alarm may still be active, but it is no longer unacknowledged.

Clear alarm

Clears the alarm.

Use this when the alarm condition has been resolved or when the alarm no longer needs to remain active.

Assign alarm

Allows the alarm to be assigned to a user.

This is useful when a supervisor, technician, operator, or responsible person needs to follow up on the alarm.

Export alarms list

Exports the alarm list. This can be useful for reporting, record keeping, troubleshooting, or sharing alarm history.

Refresh list

Reloads the alarm list.

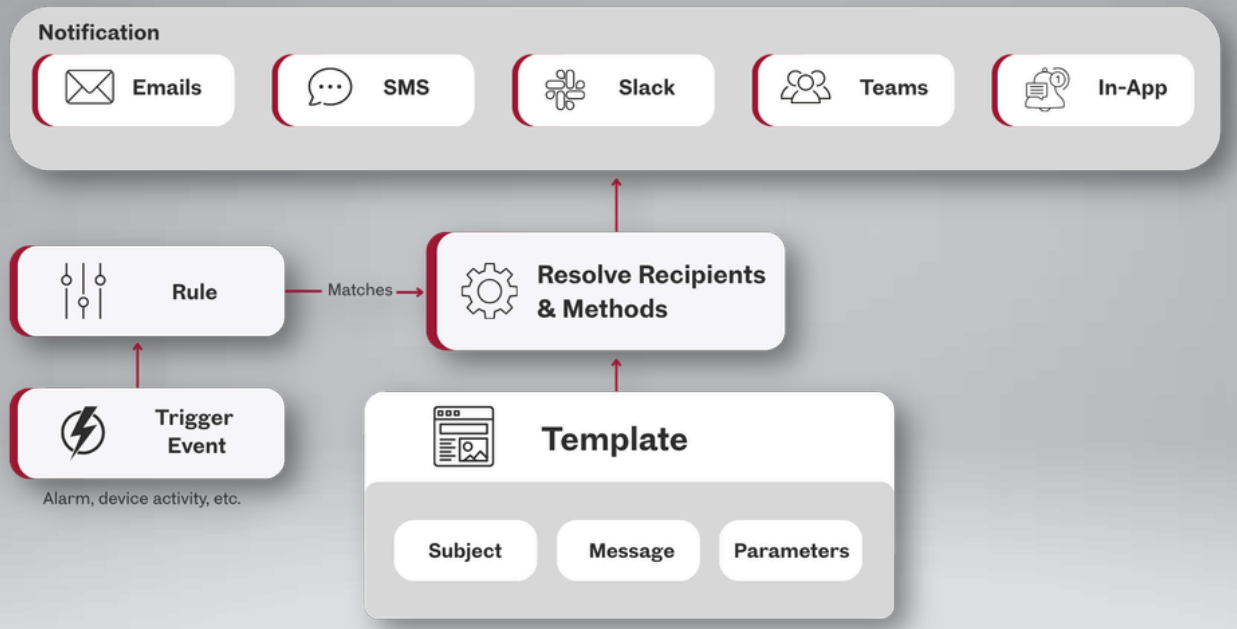
Use this to update the table after an alarm has changed status, been **acknowledged, cleared, or assigned.**

Change table order

The table order can be changed by using the column headings.

This can be used to sort alarms by created time, originator, type, severity, assignee, or status.

 © 2026 Smithtek Pty Ltd. All rights reserved.



Notifications

Notifications alert users when remote equipment needs attention, removing the need to constantly monitor dashboards. They can be used for conditions such as low tank levels, low battery voltage, pump faults, device offline events, abnormal flow, high pressure, shutdowns and other equipment warnings. Notifications help ensure the right person is alerted quickly when an alarm becomes active or communication is lost.

Automated notifications are built from three main parts:
Recipients - Who receives the notification.
Templates - What message is sent and which delivery method is used.
Rules - When the notification is sent.

Important:
Alarm rules must be created first. Alarm rules decide when an alarm is triggered. The Notification Centre controls who is notified, what message is sent, and how it is delivered.

Simple rule:
Alarm rules = create the alarm
Notification centre = sends the message
Recipients = who gets notified
Templates = what they receive
Rules = when it gets sent

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Alarm Notification



Automated notifications are built from three main parts:

Recipients

Recipients decide who receives the notification. A recipient may be a platform user, user group, email recipient, or another supported delivery target.

Example:
Operations Manager
Site Supervisor
Field Technician
Customer contact

Templates

Templates decide what message is sent. A template controls the message content and the delivery method, such as web notification or email notification.

Example:
Alarm email template
Device offline message
Low tank level notification

Rules

Rules decide when the notification is sent. A rule uses a trigger event and filter conditions to decide when the notification should be sent.

Example:
Send an email when a critical alarm is created. Send a notification when a PassPort Gateway goes offline. Send a message when an alarm is cleared.

Important:
Notifications do not create alarms by themselves.
The alarm rule creates the alarm. The notification rule decides who gets told about it

 © 2026 Smithtek Pty Ltd. All rights reserved.

Notification delivery methods

Notification templates can use different delivery methods depending on how the message needs to be sent. At least one delivery method must be selected.
For the standard 3DM.Space setup, Web and Email are available now. Other delivery methods may be available upon request through Smithtek.

Web
Sends the notification inside the 3DM.Space web interface. This is useful for users who are logged in and actively using the platform.

Email
Sends the notification to the recipient's email inbox. This is useful for alarm alerts, device offline messages, and site notifications that need to be sent outside the platform.

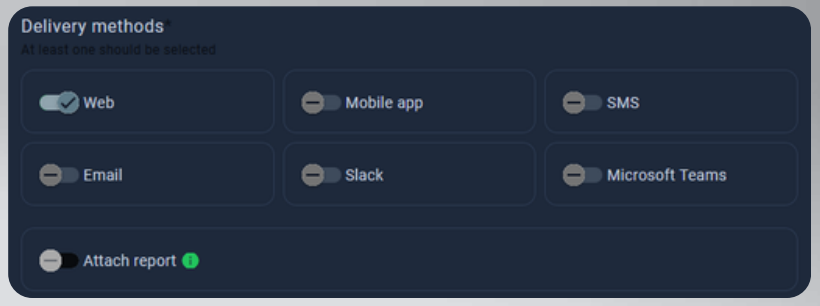
Mobile app
Sends a push notification through the mobile app. This requires mobile app setup and mobile settings to be enabled. Available upon request through Smithtek.

SMS
Sends the notification by SMS. This requires SMS provider setup and may need to be configured by Smithtek or the system administrator.
Available upon request through Smithtek.

Slack
Sends the notification to Slack users or channels. This requires Slack setup.
Available upon request through Smithtek.

Microsoft Teams
Sends the notification to a Microsoft Teams channel. This requires Microsoft Teams webhook setup. Available upon request through Smithtek.

Attach report
Allows a report to be attached to the notification if reporting has been configured.
This is an advanced option and is not normally required for basic alarm notifications.



Slide a delivery method switch to the right to enable it for the notification template. Any enabled method will be used when the notification is sent. **Example: I**f Web and Email are enabled, the notification can appear in 3DM.Space and also be sent by email.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Alarm Notification Recipients

Notification recipients are managed from the Notification centre

Recipients decide who receives notifications when a notification rule is triggered. To access recipients, click Notification centre in the side navigation bar, then click Recipients. 3DM.Space includes default recipient templates. These default recipients can be used if the notification should be sent broadly. They can also be deleted if they are not required.
New recipients can also be created for more specific notification setups.

Recipients can be created for:

Individual users

Used when one specific person should receive the notification.

User groups

Used when a team or group of users should receive the notification.

Customer users

Used when users under a customer should receive the notification.

Entities or whole companies

Used when notifications need to be sent to a wider customer, company, or entity group.
For most setups, it is better to create clear recipient groups so notifications go to the correct people, rather than sending every notification to all users.

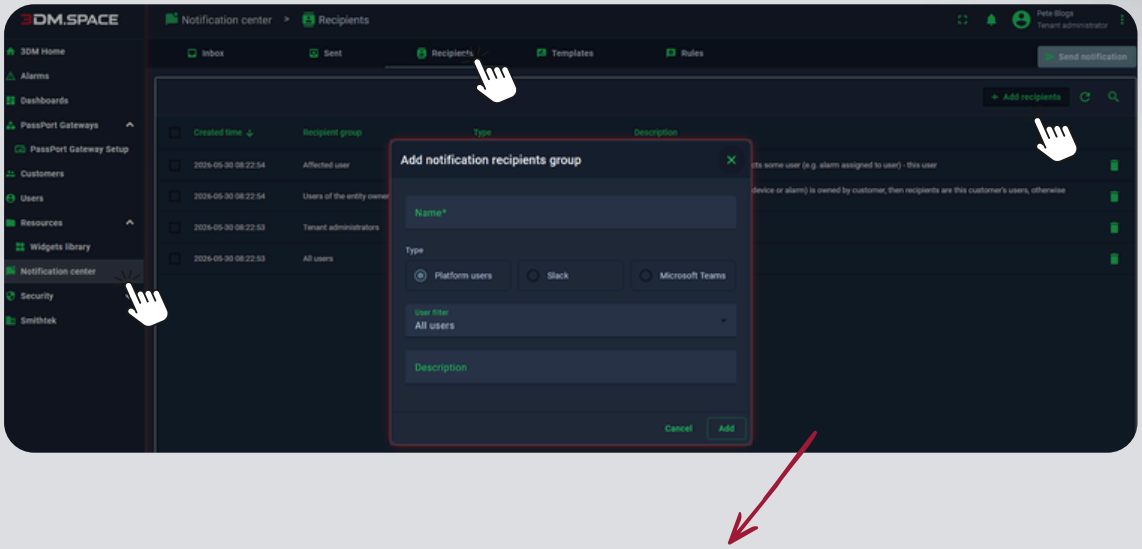
Adding a new notification recipient

To add a new notification recipient:

Steps

1. Click **Notification centre** in the side navigation bar.
2. Click **Recipients.**
3. Click **+ Add** recipient. The recipient setup window will open.

A recipient decides who will receive the notification when a notification rule is triggered. Recipients can be created for individual users, user groups, customer users, or wider entity groups, depending on who needs to receive the alarm notification.



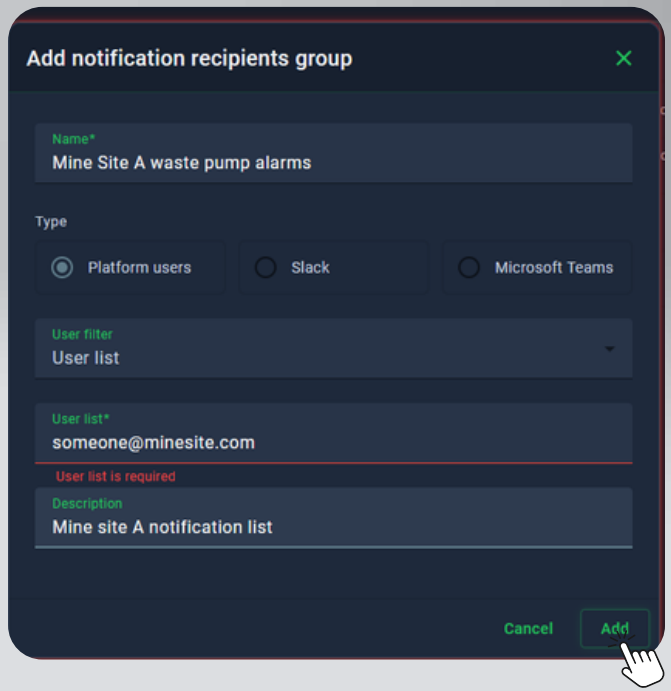
 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Alarm Notification Recipients

Recipient setup
After clicking + Add recipient, the recipient setup window will open.

Steps

1. Enter a clear **recipient name. Example:** “Smiths Farm Alarm Recipients”, “Operations Team”, or “Pump Station Supervisors”.
2. **Type:** Leave this to **platform users** unless you are using external services like Slack or MS Teams
3. Select the **user filter**. The user filter decides which users will be included in the recipient group.
4. Choose the required **filter option** from the list. Some filter options will open a second selection area. **Example:** if **User list** is selected, a second list will appear where individual users can be added.
5. Add the **users**, **groups, customers**, or **roles** required for the recipient setup.
6. Add a description if required. **Example:** “Receives alarm notifications for Smiths Farm devices.”
7. Click **Add**.



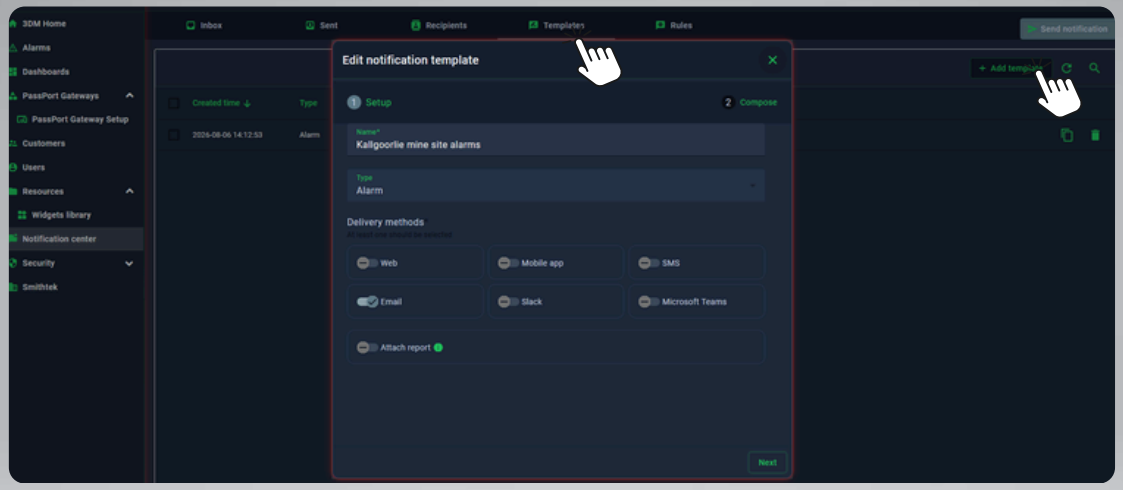
Important:
Some user filter options need an extra selection step.
Example:
User list - allows individual users to be selected.
User group list - allows one or more user groups to be selected.
Customer users- allows users connected to a customer to be selected.
User role - allows users with a selected role to be included.

The selected users will be the people included in the notification recipient group.

Simple rule:
Recipient name = what this recipient group is called
User filter = who should be included
Second selection list = choose the exact users, groups, customers, or roles
Description = optional note explaining what the recipient is used for

 © 2026 Smithtek Pty Ltd. All rights reserved.

Alarm Notification Templates



Notification templates are managed from the Notification Centre

Templates decide what message is sent when a notification rule is triggered. To access templates, click **Notification centre** in the side navigation bar, then click **Templates.** Templates can be created for specific notification setups. Templates are used to build the message content that will be sent to recipients. This may include the notification title, message body, delivery method, and any alarm or device information that should appear in the notification. The most common supported notification methods are **Web** and **Email**. If Web or Email is selected in the delivery method, the compose section will ask for a title and a message.

Title for each delivery method.
The title
is like the subject line of an email or the heading of a web notification. **Example:** “Mine Site A Faults”
Message
The message is the main content of the notification. This should explain what has happened and what the user needs to know. **Example:** “Warning, there is a fault with Pump No. 3.”

Other delivery methods may be available, such as **mobile app**, **SMS**, **Slack**, or **Microsoft Teams**. If additional delivery options are required, **contact Smithtek to have them activated.** For most setups, it is better to create clear templates for each notification type. This makes it easier to understand what message will be sent, who it relates to, and what action may be required.

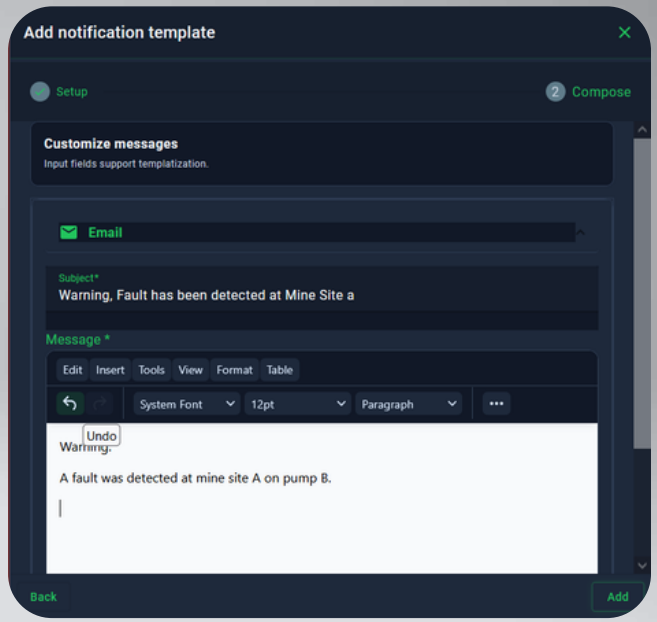
 © 2026 Smithtek Pty Ltd. All rights reserved.

Adding a new notification template

Steps

To add a new notification template:

1. Click **Notification centre** in the side navigation bar.
2. Click **Templates**.
3. Click **+ Add** template.
4. Enter a **clear template name**. **Example:** “Pump Fault Email Template”, “Device Offline Notification”, or “Critical Alarm Message”.
5. Select the **template type**.



General

Used for general notification messages. This can be used for broad messages that are not limited to one specific alarm or device activity event.

Alarm

Used for alarm notification events.

New alarm

Alarm update

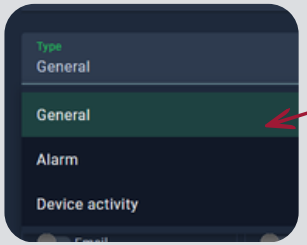
Device activity

Used for PassPort Gateway activity events.

This can include:

Device becomes active

Device becomes inactive



Template type	Used for	Common trigger events	Example use
General	General notification messages that are not tied to one specific alarm or device activity event.	General platform message or broad notification.	Sending a general notice to users.
Alarm	Alarm notification messages.	Alarm created, acknowledged, cleared, severity changed, or deleted.	Sending an email when a pump fault alarm is created.
Device activity	PassPort Gateway online or offline messages.	Device becomes active or inactive.	Sending a notification when a PassPort Gateway goes offline.

Select the delivery method.

The most common delivery methods are Web and Email.

Click Next to compose the message

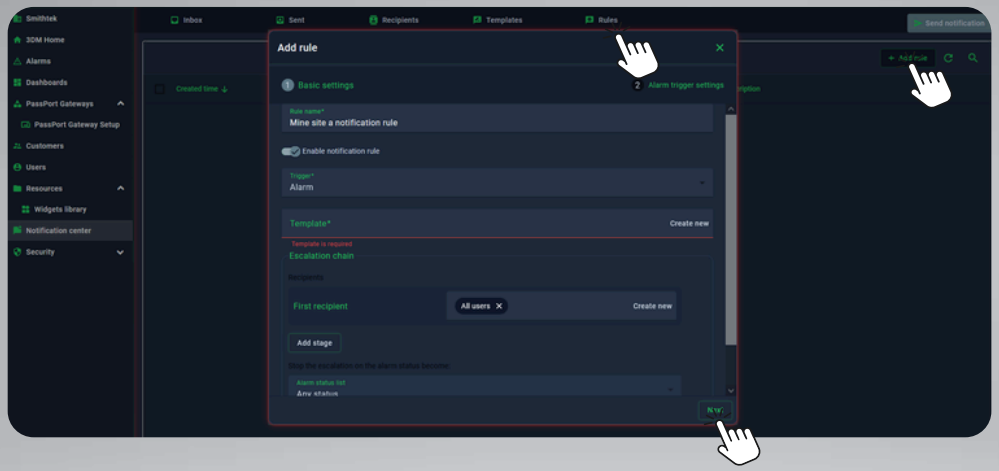
Complete the message for each delivery method you selected. Syntax templates can be copied into the message to dynamically display details such as the alarm name. This avoids creating multiple custom alarm notifications for the same site; one template can often be used across the whole site.

Click Add

The new template will now be available when creating notification rules.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Alarm Notification Rules



Notification rules are managed from the Notification centre.

Rules decide when a notification is sent.

To access rules, click **Notification centre** in the side navigation bar, then click **Rules**.

A notification rule connects the notification setup together. It uses the selected trigger event, recipient, and template to decide when a message should be sent and who should receive it. Before creating a rule, the following should already be set up:

Recipients

Who will receive the notification.

Templates

What message will be sent.

Alarm rules or device activity events

What event will trigger the notification.

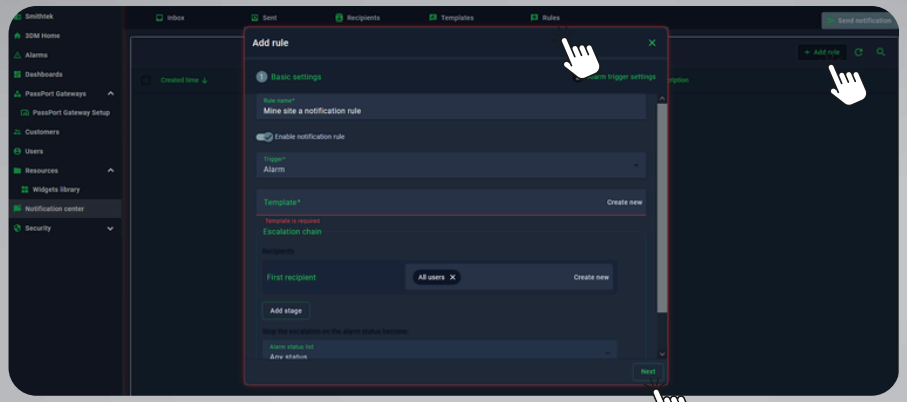
Notification rules can be created for different trigger types, such as:

Alarm events - Used when a notification should be sent for alarm activity, such as a new alarm, alarm update, alarm cleared, or alarm severity change.

Device activity events - Used when a notification should be sent when a PassPort Gateway becomes active or inactive. For most alarm notification setups, the alarm rule should be created first from the PassPort Gateway alarm rule section. The notification rule then decides when the message is sent.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Alarm Notification Rules



To add a **new notification rule,** go to **Notification centre**, click **Rules**, then click **+ Add rule.** A rule decides when a notification is sent. It connects the trigger event, message template, and recipients together.

Basic settings

Rule name

Enter a clear rule name. **Example:** “Mine site notification rule”, “Critical alarm email rule”, or “Device offline notification rule”.

Enable notification rule

Leave this switched on if the rule should start working once it has been added. If this is switched off, the rule will be saved but will not send notifications.

Trigger

Select what type of event will trigger the notification. Common options include:

Alarm - Used when notifications should be sent for alarm events.

Device activity - Used when notifications should be sent when a PassPort Gateway becomes active or inactive.

Template

Select the notification template that should be sent. Templates can be selected from templates that have already been created in the Templates section. A new template can also be created from this page by clicking **Create new**.

Recipients

Select who should receive the notification. Recipients can be selected from recipients that have already been created in the Recipients section. A new recipient can also be created from this page by clicking Create new.

Escalation chain

The escalation chain controls who receives the notification first and whether more people should be notified later. First recipient is the first person or group that receives the notification. Additional stages can be added if the notification needs to escalate to other users or groups.

Stop escalation

The rule can stop escalation when the alarm reaches a selected status. Example: the notification escalation may stop once the alarm has been acknowledged or cleared. Click Next to continue to the trigger settings.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Alarm trigger settings

Filter

Alarm type list

Select which alarm types should trigger this notification. Use Any type if the notification should apply to all alarm types. Select specific alarm types if the notification should only apply to certain alarms, such as pump fault, low voltage, or device offline alarms.

Alarm severity list

Select which alarm severities should trigger this notification.
Use Any severity if the notification should apply to all severities.
Select specific severities if the notification should only apply to certain alarm levels, such as Critical or Major.

Notify on

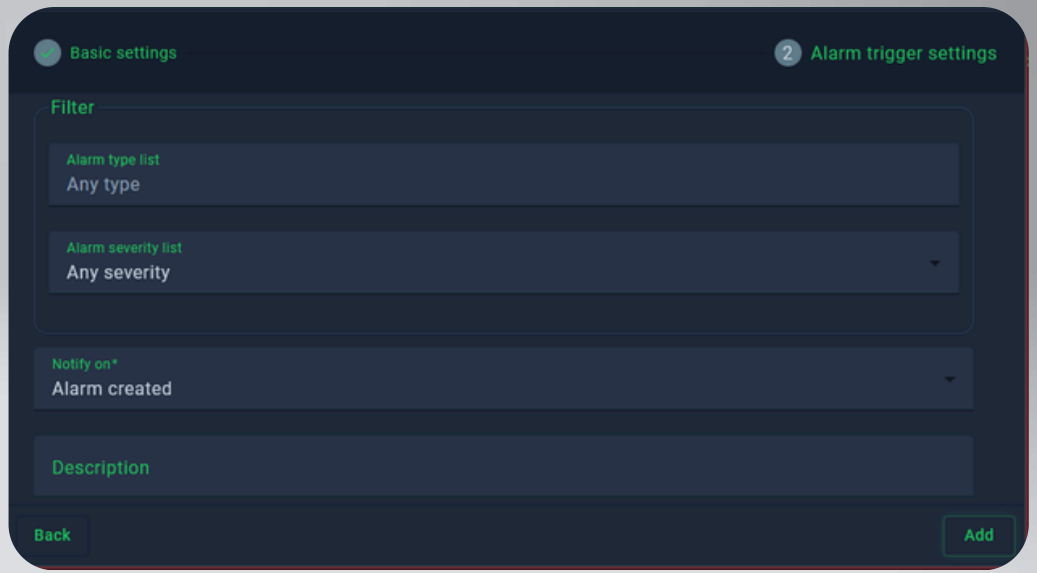
Notify on decides which alarm event will send the notification. **Example:**

Alarm created - Sends the notification when a new alarm is created.
Alarm acknowledged - Sends the notification when someone acknowledges the alarm.
Alarm cleared - Sends the notification when the alarm is cleared.
Alarm severity changed - Sends the notification when the alarm changes severity.

For most basic alarm notification setups, Alarm created is the most common option.

Description

The Description field is optional.



 © 2026 Smithtek Pty Ltd. All rights reserved.

Send notification

The Send notification button is used to send a notification manually from 3DM.Space. This is different from an automated notification rule. Automated notification rules send messages when a trigger event occurs, such as an alarm being created or a PassPort Gateway going offline. The Send notification option is for sending an instant notification from the app.

Start from scratch
Used to create a new manual notification without using an existing template.

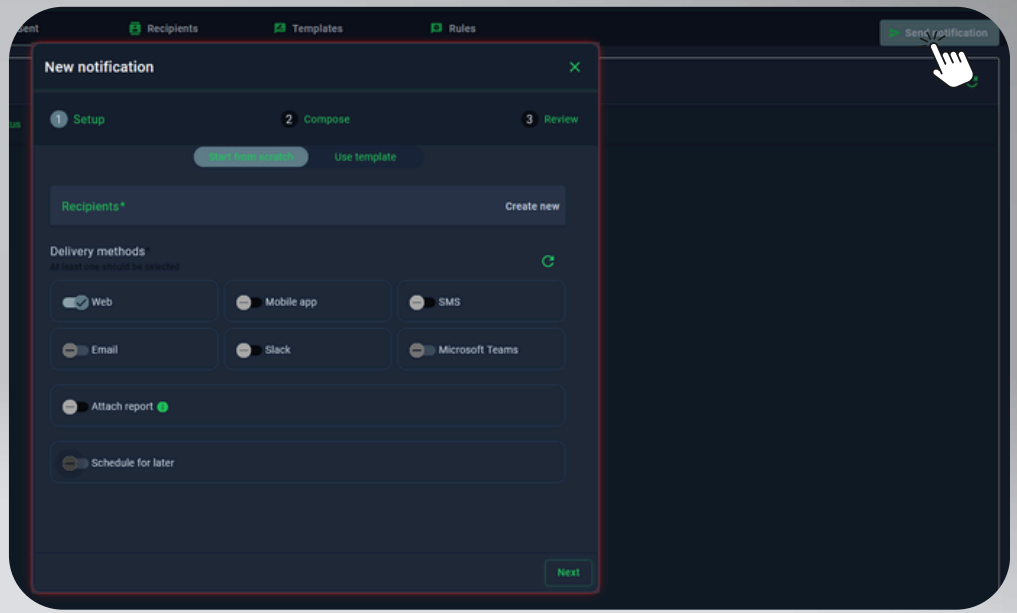
Use template
Used to send a notification using an existing notification template.

Recipients
Select who should receive the notification. Recipients can be selected from recipient groups that have already been created, or a new recipient can be created from this window.

Delivery methods
Select how the notification should be sent. Common options include:
Web - Sends the notification inside 3DM.Space.
Email - Sends the notification to the recipient's email inbox.
Other delivery methods may be available upon request through Smithtek.

Attach report
Used if a report needs to be attached to the notification.
This is not normally required for basic manual notifications.

Schedule for later
Used if the notification should be sent at a later time instead of immediately.



Compose
After the setup step, click Next to compose the notification message. The compose section is where the notification title and message are entered.

Review
The review step allows the notification to be checked before it is sent.

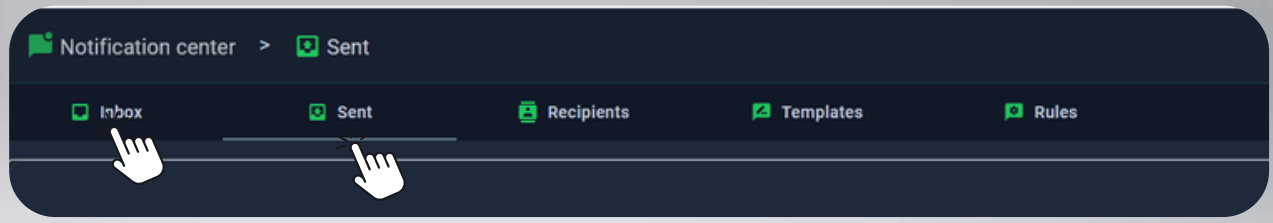
Important note
Use Send notification for manual messages only.
For automatic alarm or device activity messages, use notification Rules.

 © 2026 Smithtek Pty Ltd. All rights reserved.

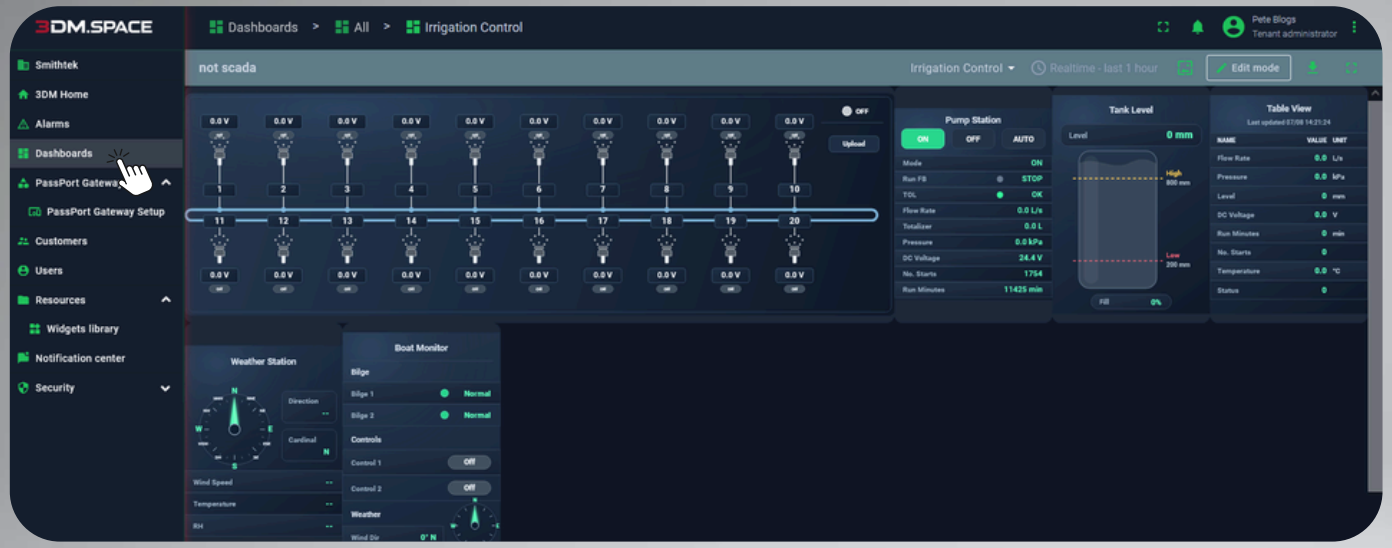
Alarm Notification Send Quick Notification

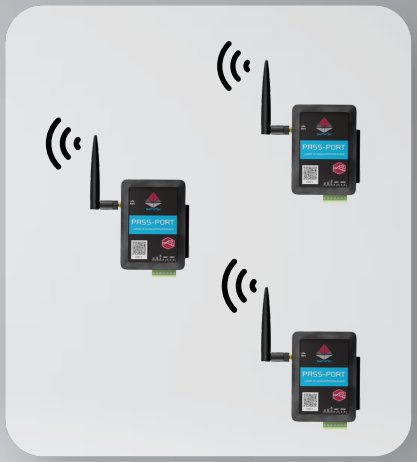
Inbox
The Inbox shows notifications received inside 3DM.Space. This is where users can view web notifications that have been sent to them by the platform, such as alarm notifications, device activity messages, or manual notifications. Use the inbox to check notifications that have been received inside the app.
Sent
The Sent tab shows notifications that have been sent from 3DM.Space. This can be useful for checking whether a notification was sent, reviewing past notification activity, or confirming that a manual notification has gone out.

Simple rule:
Inbox = notifications received
Sent = notifications sent from the platform



 © 2026 Smithtek Pty Ltd. All rights reserved.





Dashboards

Dashboards are the visual part of 3DM.Space, used to display live data, controls, alarms, trends, maps and site information. They can be created for almost any application, including farming, utilities, mining, water treatment, fleet tracking, pump stations, generators and remote monitoring.

3DM.Space includes a wide range of ready-to-use widgets, such as:

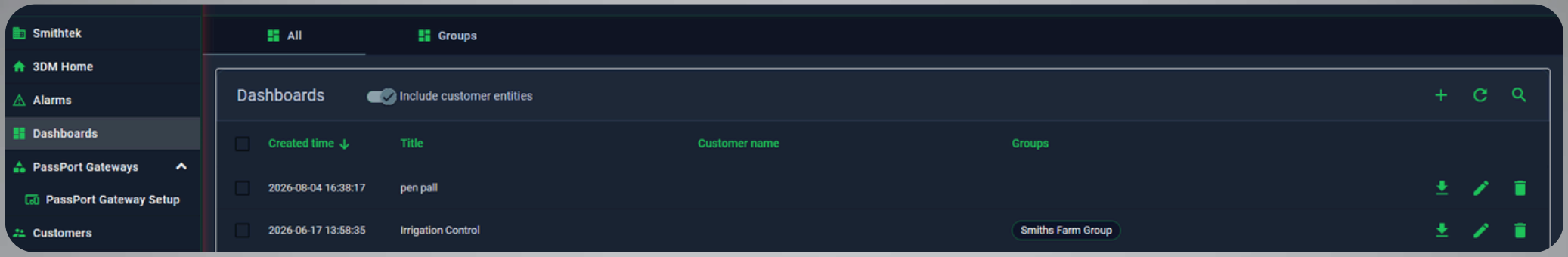
- **Charts and gauges**
- **Indicators and data cards**
- **Buttons, sliders and controls**
- **Maps and alarm tables**
- **Weather displays**
- **SCADA-style widgets**

Dashboards are built using a drag-and-drop editor. Widgets are added, connected to telemetry from a PassPort Gateway, configured and saved. Depending on permissions, users may be able to view live data, control equipment, acknowledge alarms, adjust setpoints or download chart data. Different layout options are available to suit control-room screens, tablets, phones and other displays. A well-designed dashboard should make it easy to see what is running, stopped, in alarm, needs attention and how site data is changing over time.

Simple rule:
Dashboards turn PassPort Gateway data into a visual control and monitoring screen.
Dashboard = visual screen
Widget = display or control item
Telemetry variable = live data value
PassPort Gateway = sends and receives site data
Dashboard group = where dashboards are organised
Device group = allows dashboard data to display correctly
User role = controls whether users can view, control, edit, or download data

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Viewing Dashboards



Viewing dashboards from the main menu

Dashboards can be viewed from the Dashboards section in the side navigation bar. This is the main area used to open dashboards, search for dashboards, and view dashboards that have been created in the account.

Steps

1. Click **Dashboards** in the side navigation bar.
2. Click **All**. The full dashboard list will open.
3. Find the dashboard you want to view. **Example:** “Smiths Farm Overview”, “Pump Station Dashboard”, or “Irrigation Control”.
4. Click the **dashboard name** or **dashboard row**.
5. The **dashboard** will **open**. The dashboard will show the widgets, live data, alarms, controls, charts, maps, or other information that has been configured.

Dashboard list options

Search

Use the search icon to quickly find a dashboard by name.

Refresh

Use the refresh icon to reload the dashboard list.

Add dashboard

Use the + icon to create a new dashboard.

Include customer entities

This toggle can be used to show dashboards linked to customer entities, if required.

Important:

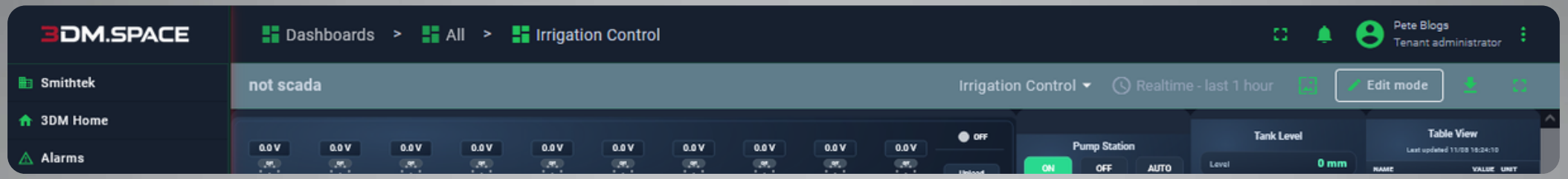
If a user cannot see a dashboard, check that the user has access to the correct dashboard group. If the dashboard opens but live data does not display, check that the user also has access to the related device group.

Simple rule:

Dashboards → All = view the full dashboard list
Click dashboard = open dashboard
Dashboard group access = lets users see dashboards
Device group access = lets dashboard data display properly

 © 2026 Smithtek Pty Ltd. All rights reserved.

Dashboards Non-Edit Mode Navigation



Dashboard navigation bar — non-edit mode

When a dashboard is open, the top navigation bar shows the main dashboard viewing options. From left to right, the options are:

Current dashboard name

This shows the name of the dashboard currently open. **Example**: not SCADA. This helps the user confirm they are viewing the correct dashboard.

Dashboard selector

The dashboard selector shows the currently selected dashboard and includes a drop-down arrow. Use this to switch between dashboards without going back to the main dashboard list.

Example: Irrigation Control. Clicking the drop-down allows the user to select another available dashboard.

Time and date picker

The time and date picker controls the time range used by dashboard widgets. **Example: Realtime** - last 1 hour. This is useful for charts, trends, historical values, alarms, or telemetry widgets that need to display data over a selected time period. Depending on the dashboard setup, users may be able to view live data, recent data, or a custom date/time range.

Upload dashboard image

The upload image icon is used to add or change the dashboard image. This can be useful for organising dashboards, branding dashboards, or making dashboard lists easier to recognise.

Example: a dashboard image may show a site photo, company logo, pump station image, tank farm image, or project graphic.

Edit mode

The Edit mode button opens the dashboard editor.

This is used when the dashboard needs to be changed, such as adding widgets, moving widgets, editing layout, changing settings, or updating controls. Only users with the correct permissions should be able to edit dashboards.

Simple rule:
Dashboard name = what dashboard is open
Dashboard selector = switch dashboards
Time and date picker = select Live or Historical Data
Upload image = organise or brand the dashboard
Edit mode = change the dashboard
Export = save or copy dashboard setup
Full screen = larger operator view

 © 2026 Smithtek Pty Ltd. All rights reserved.

Dashboards Non-Edit Mode Navigation



Edit mode

The Edit mode button opens the dashboard editor. This is used when the dashboard needs to be changed, such as adding widgets, moving widgets, editing layout, changing settings, or updating controls. Only users with the correct permissions should be able to edit dashboards.

Export dashboard

The export icon is used to export the dashboard configuration. This is useful for backing up dashboards, copying dashboard layouts, sharing dashboard templates, or moving a dashboard setup between projects. Exporting a dashboard does not export live telemetry data. It exports the dashboard setup/configuration.

Full screen mode

The full screen icon opens the dashboard in full screen view. This is useful for control room screens, wall-mounted displays, tablets, or operators who want a cleaner view without extra menus. Full screen mode helps focus on the dashboard itself by reducing navigation and surrounding screen clutter.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboards Edit Mode Navigation



States
The States section is used to manage dashboard states.
A state can be thought of as a different dashboard view, page, or screen inside the same dashboard.
Example: Default. If multiple states are used, the drop-down allows the user to switch between them.

Layouts
The Layouts section is used to manage the dashboard layout. This controls how widgets are arranged on the page. Layouts are useful when building dashboards for different screen styles, screen sizes, or dashboard structures. Layouts include, SCADA, Divider, and default for general use.

Add widget
The Add widget button is used to place a new widget onto the dashboard. This is one of the main dashboard building tools.
Widgets can include items such as: **charts - gauges - indicators - control buttons.**

Time window
The Time window option controls the dashboard time range used by time-based widgets. This is useful for charts, trend graphs, telemetry history, and other widgets that use live or historical data.

Settings
The Settings option opens the dashboard settings. This is where general dashboard setup options can be adjusted.

Filters
The Filters option is used to apply or manage dashboard filters. Filters help control what data or entities are shown on the dashboard. This can be useful when a dashboard needs to display selected devices, assets, customers, or other filtered content.

Cancel
The Cancel button exits edit mode without saving the latest changes. Use this if changes were made by mistake or should not be kept.

Save
The Save button saves the current dashboard changes. This should be clicked after editing widgets, layouts, settings, or dashboard content. If Save is not clicked, recent changes may be lost.

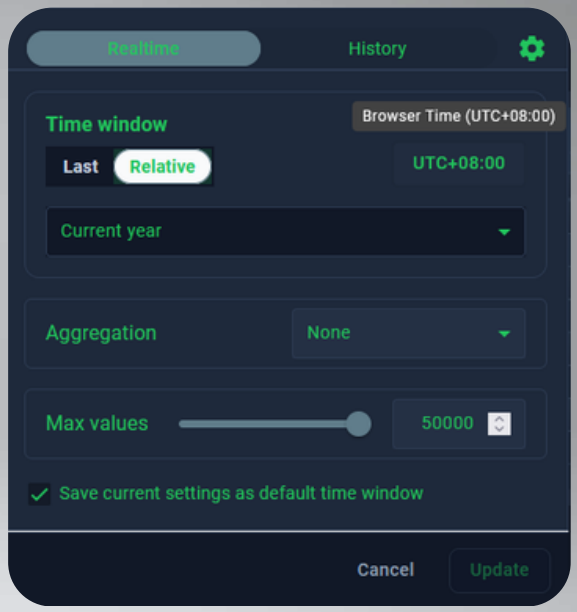
Full screen / expand view
The expand icon at the far right opens the dashboard in a larger or full screen style view. This can be useful while editing if more screen space is needed.

Simple rule:
States = different dashboard views
Layouts = how widgets are arranged
Add widget = place a new widget on the dashboard
Time window = set the dashboard time range
Settings = dashboard setup options
Filters = control what data is shown
Cancel = leave without saving
Save = keep your changes

 © 2026 Smithtek Pty Ltd. All rights reserved.

Dashboards Time Window Properties

The Time window properties control what time period the dashboard uses when displaying time-based data. This is mainly used by charts, trends, telemetry history, alarm widgets, and other widgets that show data over time. For example, a dashboard may show live data from the last hour, historical data from yesterday, or a selected period such as the current year.



Realtime

Realtime mode is used for live dashboards. In this mode, the dashboard continues to update as new data is received. This is normally used for operator dashboards, live monitoring screens, pump stations, tanks, process dashboards, and control room displays. **Example: Realtime** - last 1 hour. This means the dashboard will show the most recent hour of data and continue moving forward as time passes.

History

History mode is used to view a fixed time period. This is useful when checking past site activity, reviewing trends, investigating alarms, or comparing performance over a selected period. **Example:** Yesterday, Last week, Current month, or a custom date range. History mode is useful when the user needs to look back at what happened, rather than watch what is happening now.

Time window options:

Browser time

This shows the time zone being used by the dashboard. **Example:** Browser Time (UTC+08:00)
This means the dashboard is using the time zone from the user's browser. This is important when checking historical data, especially if users are in different time zones or the site is in a different location.

Last / Relative

The Last or Relative setting controls how the time period is selected. A relative time window moves with the current time. **Example**: Last 1 hour means the dashboard always shows the most recent 1 hour.
Current year means the dashboard shows data from the current year.

Aggregation

Aggregation controls how data is grouped or summarised over the selected time period. **Example:** None - Average - Min - Max - Sum - Count. For simple live values, aggregation may be left as None. For longer time periods, aggregation can help make charts easier to read by grouping many data points together.

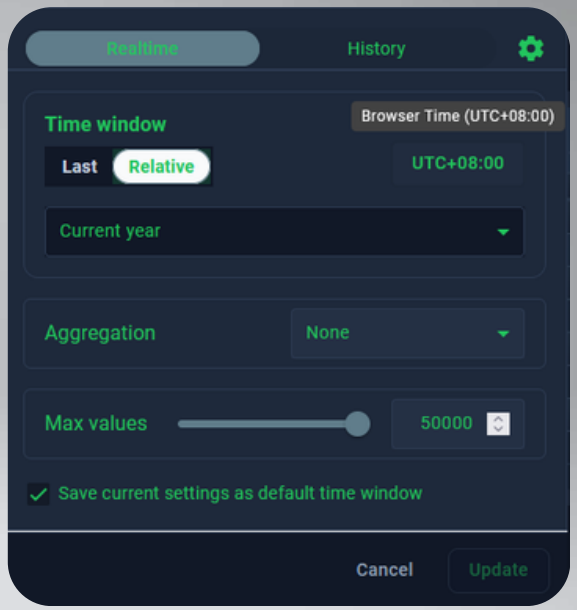
Max values

Max values limit how many data points are loaded or displayed in a time period. This helps stop large time ranges from loading too much data at once. **Example:** 50000. A higher value can show more detail but may take longer to load. A lower value may load faster but may show less detail.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboards Time Window Properties

Realtime
Realtime mode is used for live dashboards. In this mode, the dashboard continues to update as new data is received. This is normally used for operator dashboards, live monitoring screens, pump stations, tanks, process dashboards, and control room displays.
Save current settings as default time window
This option saves the current time window settings as the default for the dashboard.
When enabled, the dashboard will open using these time window settings in the future.
This is useful when a dashboard should always open with a preferred view, such as:
Realtime - last 1 hour, Current day, Current year, Last 7 days
Cancel
Cancel closes the time window settings without applying the latest changes.
Update
Update applies the selected time window settings to the dashboard.
Use this after changing the time range, aggregation, max values, or default time window option.



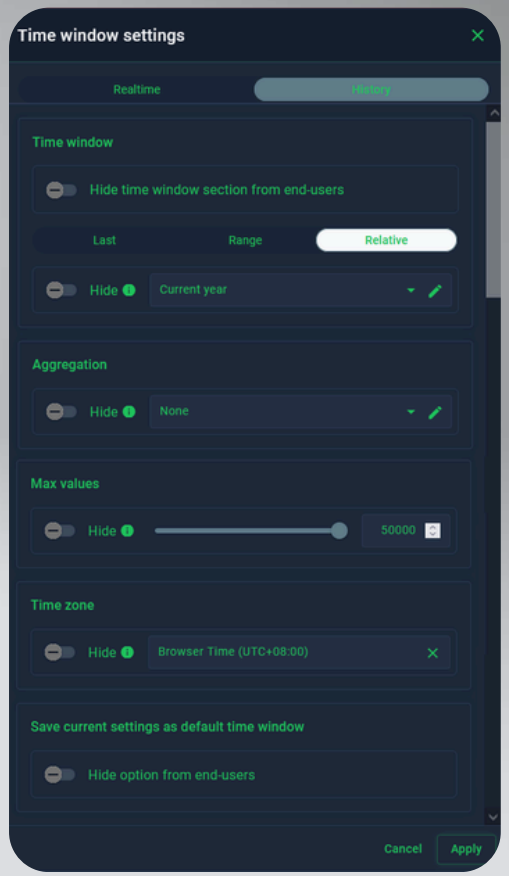
Simple rule
Realtime = live moving time window
History = fixed past time period
Relative = time range that moves with now
Aggregation = how data is grouped
Max values = how much data can be loaded
Save as default = dashboard opens with these settings
Update = apply the time window changes

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboards Time Window Settings

The **Time window setting controls** what time period the dashboard uses when displaying **time-based data**. This is mainly used by **charts, trends, telemetry history, alarm widgets**, and other widgets that show data over time. **Example:** a dashboard may show live data from the last hour, historical data from yesterday, or a selected period such as the current year.

The Time window settings window also allows **administrators to control** which time window **options end-users** can **see** or **change**. This is useful when a dashboard should have a fixed time setup, or when users should only be allowed to adjust certain parts of the time window. The options shown here are mostly the same as the Dashboard time window properties page, but with extra Hide controls.



Realtime and History
The top tabs allow the administrator to configure time window options for Realtime and History mode. Realtime is used for live dashboards. History is used for viewing past data over a selected time period.

Hide options
The Hide switches control whether each section is visible to end-users. If a section is hidden, the end-user will not be able to see or change that option from the dashboard time window menu.

Hide options may be available for:

Time window
Controls whether users can change the selected time period.

Aggregation
Controls whether users can change how data is grouped or summarised.

Max values
Controls whether users can change the maximum number of data points loaded.

Time zone
Controls whether users can change the time zone used by the dashboard. Save current settings as default time window Controls whether users can save their selected time window as the default.

Buttons: Cancel - Closes the window without applying changes.
Apply - Applies the selected time window user settings.

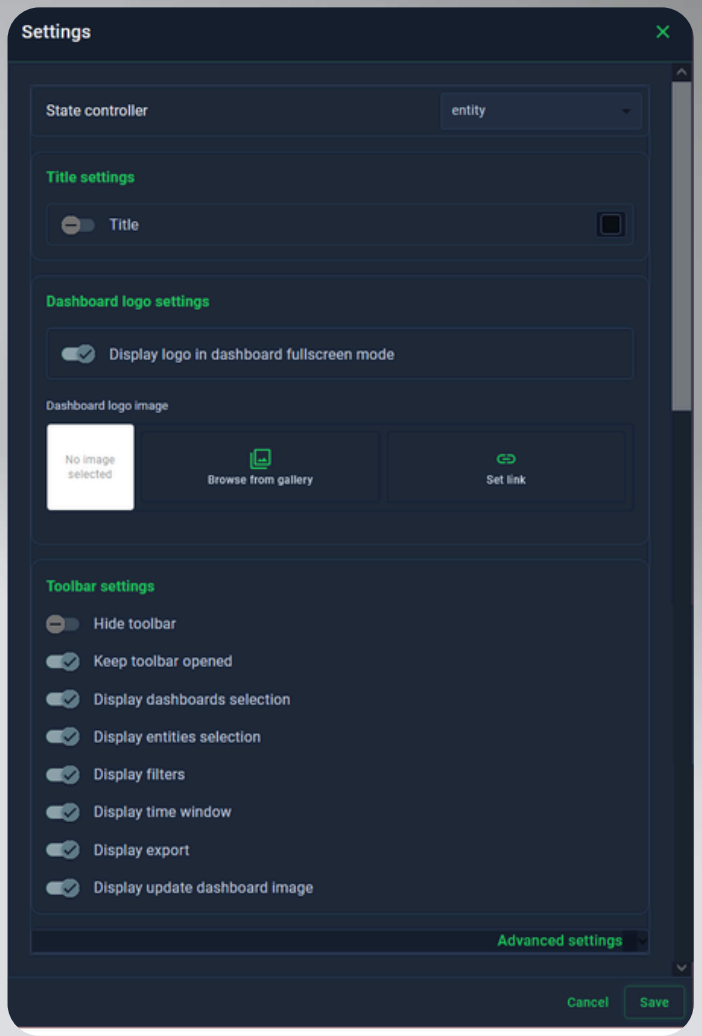
Important:
Only hide options when the dashboard should stay locked to a specific setup. For operator dashboards, it may be better to keep the time window simple and consistent so users do not accidentally change the dashboard view. For investigation or reporting dashboards, it may be useful to allow users to change time range, aggregation, or time zone.

Simple rule:
Hide off = users can see or change the option
Hide on = users cannot see or change the option
Realtime = live data settings
History = past data settings
Apply = keep the changes

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Settings

The Settings window is used to control the main dashboard display options. These settings affect how the dashboard looks and what options are shown to users when the dashboard is opened.



State controller

The State controller setting controls how dashboard states are managed. In most standard dashboard setups, this can be left as the default option.

Title settings

The Title option controls whether the dashboard title is shown. If enabled, the dashboard title will be displayed. If disabled, the dashboard title can be hidden for a cleaner dashboard view. This can be useful when the dashboard already has a custom title built into the layout.

Dashboard logo settings

Dashboard logo settings control whether a logo is displayed when the dashboard is opened in full-screen mode.

Display logo in dashboard full-screen mode

Displays the selected logo when the dashboard is viewed in full-screen mode.

Dashboard logo image

Allows a logo image to be selected. The maximum size logo is 200kb. **Browse from gallery:** Used to choose a logo image from the available image gallery.

Set link: Used to link to an image instead of selecting one from the gallery. This is useful for branding customer dashboards, site dashboards, or control room displays.

Toolbar settings

Toolbar settings control which toolbar options are shown to users.

Hide toolbar: Hides the dashboard toolbar. This can be useful for clean operator screens, wall displays, or dashboards where users should not change settings.

Keep toolbar opened: Keeps the toolbar visible when the dashboard opens.

Display dashboards selection: Allows users to select or switch dashboards from the dashboard toolbar.

Display entities selection: Allows users to select entities from the toolbar, if the dashboard uses entity selection.

Display filters: Shows dashboard filters to the user.

Display time window: Shows the time window option so users can change the dashboard time range.

Display export: Shows the export option for the dashboard.

Display update dashboard image: Allows users to update the dashboard image.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Settings

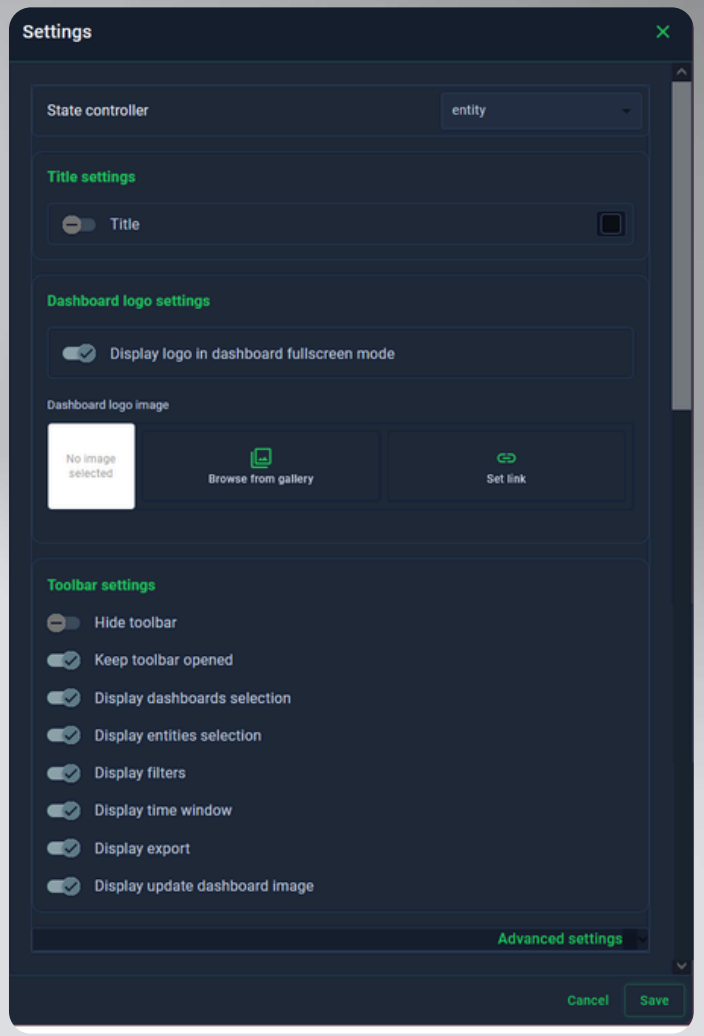
Advanced settings: The Advanced settings section is used for dashboard CSS editing. This is normally only used for advanced dashboard styling or custom visual changes. For standard dashboard setup, leave this section unchanged unless custom CSS styling is required.

Cancel

Closes the settings window without saving changes.

Save

Saves the dashboard settings.



Important:

Only show toolbar options that users actually need. For simple operator dashboards, it may be better to hide unnecessary options so users cannot accidentally change the dashboard view, time window, filters, or dashboard image.

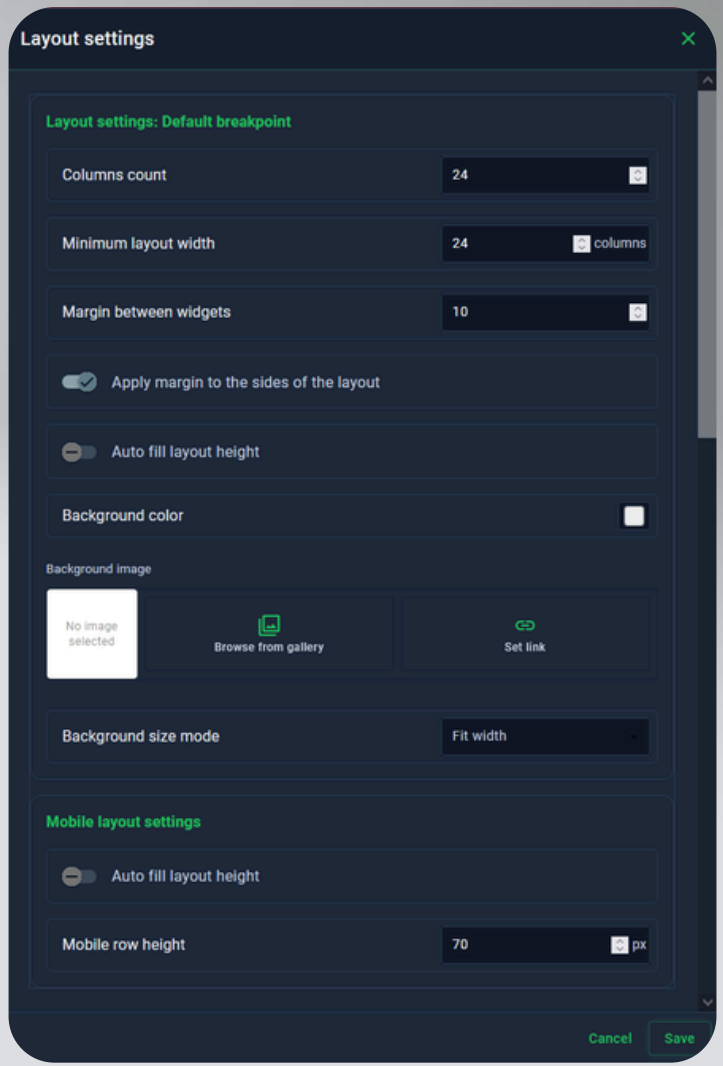
Simple rule:

Title settings = show or hide dashboard title
Logo settings = dashboard branding
Toolbar settings = what users can see or change
Advanced settings = CSS styling
Save = keep changes

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Layout Settings

The Layout settings window controls how widgets are arranged on the dashboard. These settings affect the dashboard grid, widget spacing, background style, and mobile layout behaviour. The layout settings are normally adjusted when building or refining a dashboard layout.



Columns count: Columns count controls how many columns are available across the dashboard grid. **Example:** 24 columns. A higher column count gives more layout flexibility because widgets can be resized and positioned more precisely. For most dashboards, 24 columns is a practical default.

Minimum layout width

Minimum layout width controls the minimum width of the layout before the dashboard changes or uses another breakpoint. **Example:** 24 columns. This helps control when the dashboard should keep its current layout and when another layout may be needed for smaller screens.

Margin between widgets

Margin between widgets controls the spacing between widgets on the dashboard. **Example:** 10. A higher value creates more space between widgets. A lower value makes widgets sit closer together. This is useful for controlling how clean or compact the dashboard looks.

Apply margin to the sides of the layout

This controls whether the widget margin is also applied to the outside edges of the dashboard layout. When enabled, the dashboard will have spacing around the outside edges as well as between widgets. When disabled, widgets may sit closer to the edge of the dashboard.

Auto fill layout height

Auto fill layout height controls whether the layout automatically fills the available screen height. This can be useful for full-screen dashboards or dashboards designed for control room displays. For standard dashboards, this can normally be left off unless the dashboard needs to stretch to fill the screen.

Background colour: Background colour sets the background colour for the dashboard layout. This can be used to match company branding, improve readability, or create a cleaner visual style.

Background image

A background image can be added to the dashboard layout.

This can be useful for SCADA-style dashboards, site layouts, process diagrams, maps, or branded dashboard backgrounds. **Browse from gallery:** Select an image from the image gallery.

Set link: Use an image link instead of selecting from the gallery.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Background size mode: Background size mode controls how the background image is displayed.
Example: Fit width. This can be used to make the image fit the dashboard width, depending on the image and dashboard design.

Auto fill layout height

This controls whether the mobile layout automatically fills the available screen height. For mobile dashboards, this may be useful when creating a cleaner full-screen style layout.

Mobile row height

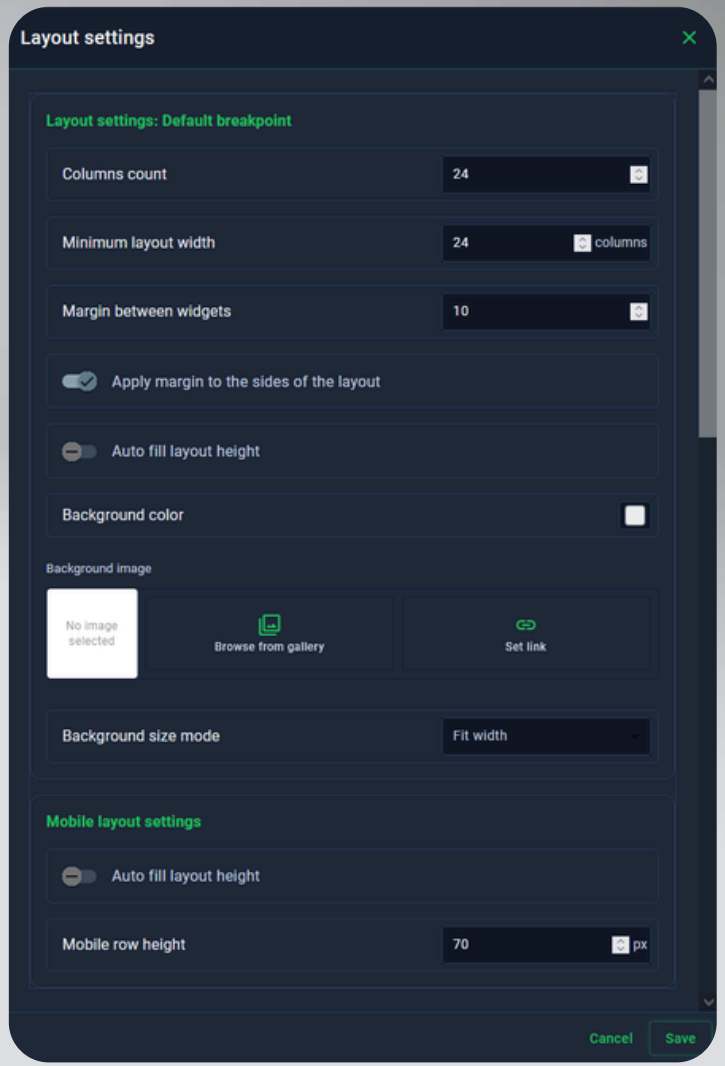
Mobile row height controls the height of each row in the mobile layout.
Example: 70 px. A larger row height gives widgets more vertical space. A smaller row height makes the dashboard more compact. This setting helps make widgets easier to read and use on smaller screens.

Cancel

Closes the layout settings window without saving changes.

Save

Saves the layout settings.



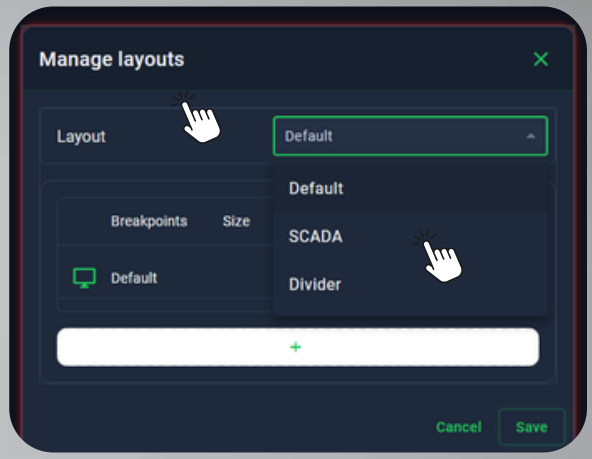
Important:
Changing layout settings can affect how the dashboard appears across different screen sizes. After changing columns, margins, background settings, or mobile layout settings, always check the dashboard in normal view and full screen view. If breakpoints are being used, check each breakpoint separately because widgets may need to be rearranged for each screen size.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Layouts and Widget Arrangement

Dashboard layouts control how widgets are arranged on the dashboard. Layouts are useful when the same dashboard needs to work across different use cases, such as normal monitoring screens, SCADA-style process screens, or split-screen dashboards.

The main layout types are:



Default layout

The Default layout is the standard dashboard layout. This layout is used for most dashboards, including **monitoring dashboards, charts, gauges, alarm tables, maps, status cards, buttons,** and **general telemetry screens.**

Widgets are placed onto the dashboard grid and can be resized or moved to suit the dashboard design. The Default layout is normally best for dashboards that need to work across different screen sizes, such as desktop monitors, tablets, and phones.

Use **Default layout** for:

- **general monitoring dashboards**
- **charts and trend screens**
- **pump station dashboards**
- **tank level dashboards**
- **fleet or map dashboards**
- **operator dashboards with standard widgets**

SCADA layout

The SCADA layout is designed for more fixed-position visual screens. This layout is useful when building **SCADA-style dashboards** where **widgets, symbols, pipework, tanks, pumps, valves,** or **background images** need to stay in a specific position.

Unlike the Default layout, the SCADA layout is intended to keep widgets fixed in their designed positions rather than automatically reflowing in the same way as a normal responsive dashboard. This makes it better for process diagrams, plant layouts, equipment screens, and HMI-style views.

Use **SCADA layout** for:

- **process diagrams**
- **pump station mimic screens**
- **water treatment layouts**
- **mining process screens**
- **tank farm layouts**
- **HMI-style dashboards**
- **dashboards with fixed symbols and background images**

Divider layout

The Divider layout splits the dashboard into separate left and right areas. This is useful when one side of the dashboard is used for navigation, lists, entity selection, or summary information, while the other side shows details, charts, maps, or controls.

The Divider layout is often useful for master-detail style dashboards, where the user selects something on one side and views the detail on the other side.

Use **Divider layout** for:

- **list on the left, details on the right**
- **site selection and site details**
- **asset list and asset information**
- **alarm list and alarm details**
- **map or chart on one side, controls on the other**

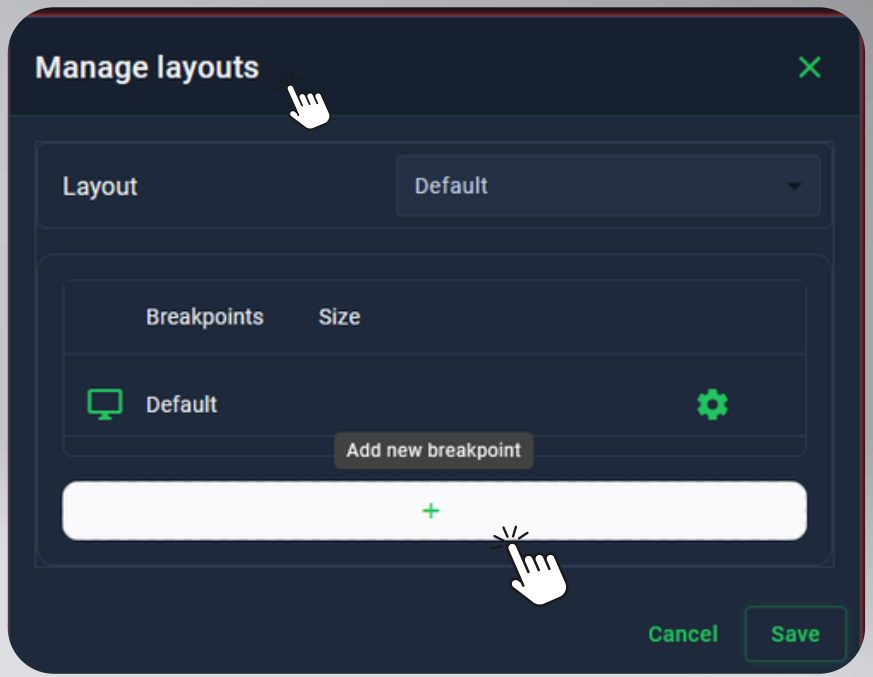
 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Layouts and Widget Arrangement

Breakpoints
Breakpoints allow the same dashboard to have different layouts for different screen sizes. This is useful when a dashboard needs to work on large monitors, laptops, tablets, and phones. Example: a dashboard may have:

Desktop breakpoint - Used for large screens with more space.
Tablet breakpoint - Used when the dashboard needs a tighter layout.
Mobile breakpoint - Used for phones where widgets may need to be stacked vertically.

When the screen size changes, 3DM.Space can look for a matching breakpoint and use the layout designed for that screen size. Breakpoints do not automatically make every dashboard perfect on every screen. After creating a breakpoint, the widgets still need to be moved, resized, and arranged so the dashboard looks correct on that screen size.



Important:
Breakpoints should be tested properly. A dashboard that looks good on a desktop screen may not work well on a phone unless the mobile breakpoint has been arranged correctly. When creating mobile or tablet breakpoints, check that important widgets are still easy to read and controls are still easy to use.

Simple rule:
Default = normal responsive dashboard layout
SCADA = fixed-position process or HMI-style layout
Divider = split dashboard into left and right areas
Breakpoint = different layout for different screen sizes
Widgets still need arranging for each breakpoint

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Divider Layout

The Divider layout splits the dashboard into two separate sections. This is useful when the dashboard needs one area for summary, navigation, maps, lists, or controls, and another area for charts, details, alarms, or live data. Instead of building one large dashboard area, the Divider layout creates a clear left side and right side.

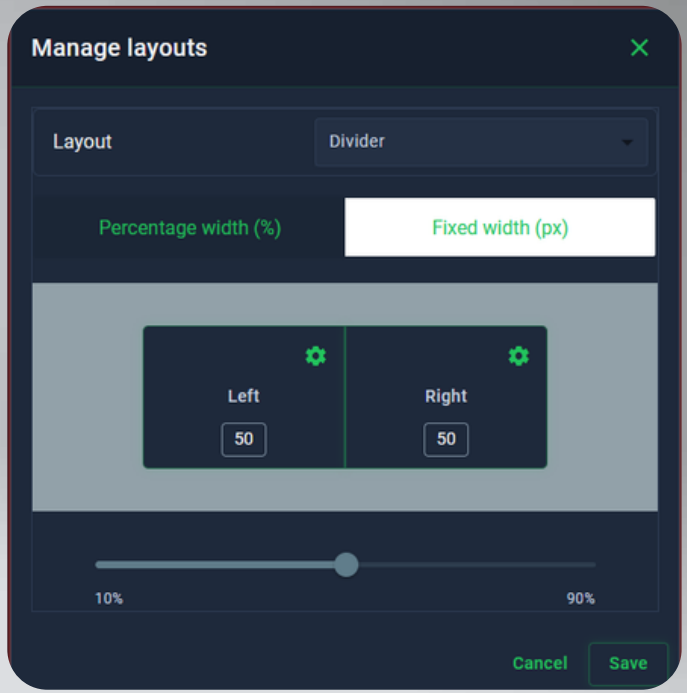
A Divider layout can be useful for dashboards such as:

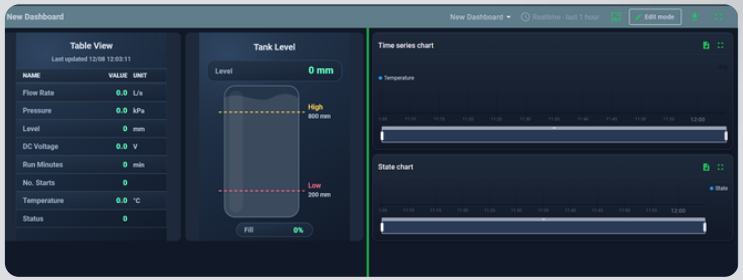
Map and site data
Map widget on one side, live tank levels, pump status, alarms, or controls on the other side.
Line charts and map
Line charts on the left showing flow, pressure, or tank level trends, with a map widget on the right showing the site or asset location.
Alarm list and alarm details
Alarm table on one side, selected alarm details or related device data on the other side.
Control panel and process view
Pump controls, setpoints, and status indicators on one side, with a SCADA-style process view on the other.
Fleet or remote asset overview
Asset list on the left, map or selected asset details on the right.
Percentage width
Percentage width allows the divider sections to be sized using a percentage of the dashboard width or fixed pixels (PX). **Example:** Left 50% / Right 50%. This means both sides take up equal space.

The divider preview shows two sections:
Left: The left side of the dashboard.
Right: The right side of the dashboard.

Each side can have its own layout settings. Use the settings icon on each section to adjust that side.
Divider slider
The slider controls how much space is given to each side. Moving the slider changes the split between the left and right sections. **Example:** 50 / 50 gives both sides equal space. The slider range allows the divider to be adjusted between smaller and larger section widths.

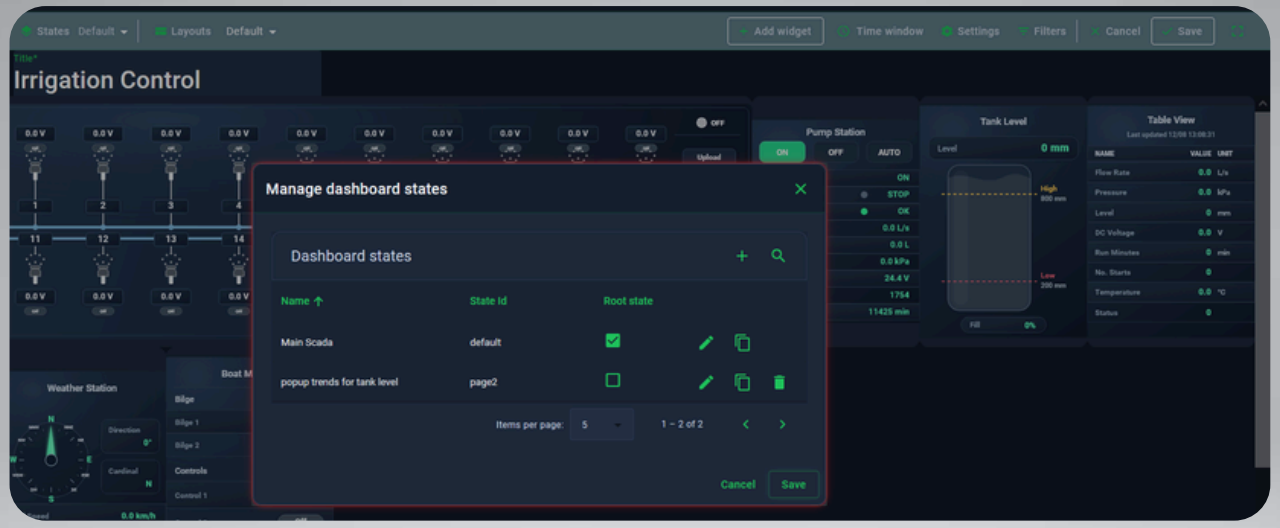
Buttons: Cancel - Closes the layout window without saving changes.
Save - Saves the divider layout settings.





Important:
After changing the Divider layout, check the dashboard in normal view and full screen view. Widgets may need to be moved or resized inside each side so the dashboard still looks clean and is easy to use. If the dashboard is used on tablets or phones, also check the breakpoint layout because the divider may need adjusting for smaller screens.

3DM Dashboard States



Dashboard states are used to create **sub-pages** inside a selected dashboard. A state can be thought of as an additional dashboard page that belongs to the main dashboard. Each state can have its own widgets, layout, controls, charts, maps, tables, or SCADA display.

This is useful when one dashboard needs **more than one screen**, but you still want everything to stay inside the same dashboard. **Example:** A main SCADA dashboard may show a full site overview, while another state may show detailed trend data for one tank, pump, valve, or flow meter.

How states work

Each state works like a separate dashboard page.
Widgets can be dragged and dropped onto each state, just like a normal dashboard. A dashboard may have:

Main SCADA - Used as the main dashboard overview.
Pump details - Used to show pump trends, runtime, alarms, and controls.
Tank level trends - Used to show tank level history and related data.
Flow meter details - Used to show flow rate trends, totaliser data, asset information, or map location.

Root state

The Root state is the main starting page for the dashboard.
This is the first state that opens when the dashboard is loaded.
In the example shown, **Main SCADA** is the root state.

State ID

The State ID is the internal reference used by the dashboard.
Example: default page2. This ID is used by the system to identify which state should be opened.

State actions - Widget setting

States can be linked to widget actions. This allows a button, symbol, image, label, or other widget action to open another dashboard state. **Example:** a SCADA dashboard may show a water flow meter as a visual widget. A button or clickable area can be added to that widget. When the user clicks it, the dashboard can open a second state showing detailed trend data, asset data, alarms, or a map location for that flow meter.

 © 2026 Smithtek Pty Ltd. All rights reserved.

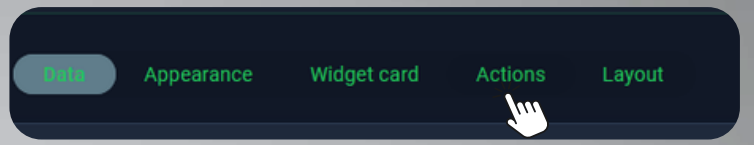
3DM Dashboards - Adding a State to a Widget

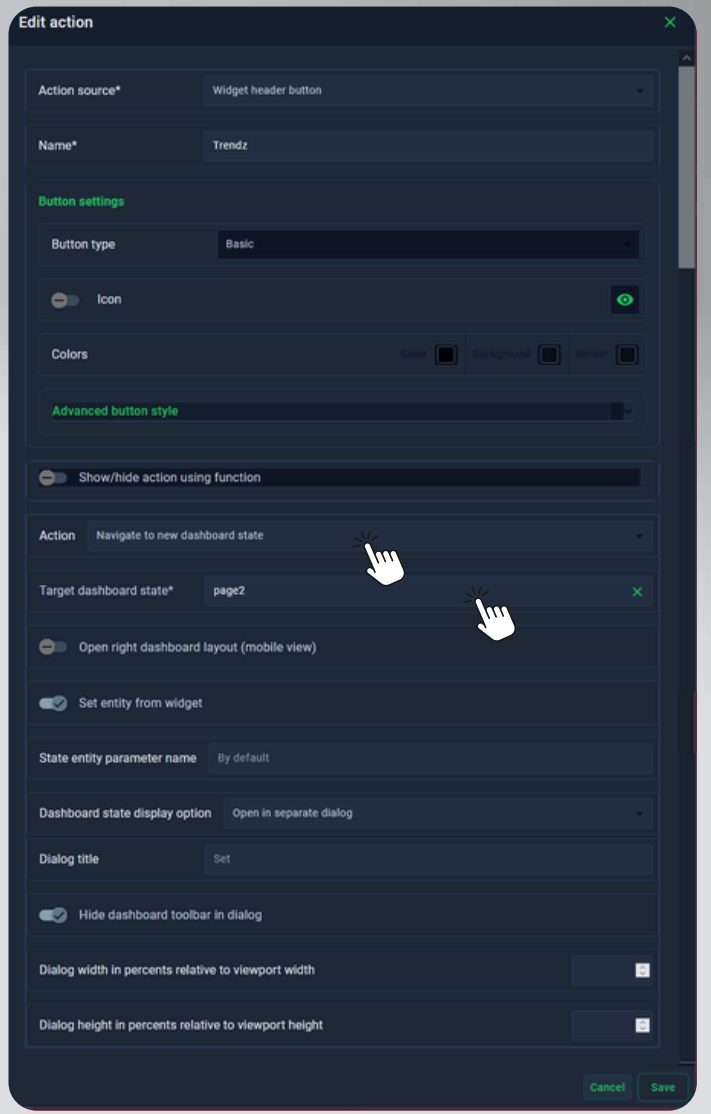
Creating a widget state
A widget can be configured to open a dashboard state.

Steps:

1. Set the dashboard into **Edit mode**.
2. Click and **edit a widget** - This opens widget settings.
3. Go to the **Actions tab**.
4. Click on **Action**
5. Select **Navigate to dashboard state**.
6. Search for the dashboard state that has already been created.
7. Select the required state in “Target dashboard state”
8. Configure the **widget button** or action label.
9. **Save** the widget. **The widget can now act like a link to another dashboard state.**







Important:
Dashboard states are very useful for SCADA dashboards because they allow detailed screens to be opened only when required. Instead of crowding the main dashboard with every chart, map, alarm, and asset detail, states allow extra information to be placed on separate sub-pages

Simple rule:
State = sub-page inside a dashboard
Root state = main starting page
State ID = internal state reference
Widget action = button or click action
Navigate to dashboard state = opens another dashboard sub-page
States keep SCADA dashboards cleaner

 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

3DM Dashboard Widgets

The Dashboard widgets page is where you choose the visual blocks, controls, charts, maps, gauges, alarms, and other components used to build a dashboard. 3DM.Space includes 14 default widget bundles and over 500 available widgets, giving you the main tools needed for remote monitoring, control, alarming, and data visualisation.

Widgets can be used for many different applications, including pump stations, tanks, irrigation systems, generators, environmental monitoring, process equipment, remote sites, and industrial control systems.

Widget bundles include:

Traditional SCADA fluid system: Pipework, tanks, pumps, valves, and process-style layouts.
General high-performance SCADA: Advanced SCADA-style process graphics.
Charts: Trend charts, line charts, bar charts, and data visualisation.
Cards: Simple value cards, QR/code cards, and status display widgets.
Alarm widgets: Alarm lists, alarm counters, and alarm status displays.
Maps: Location maps, site markers, and GPS-based monitoring.
Analogue gauges: Dial gauges and analogue-style value indicators.
Digital gauges: Digital displays for live values.
Industrial widgets: Efficiency, vibration, and equipment display widgets.
Indoor Environment: Temperature, humidity, VOC, and indoor monitoring widgets.
Outdoor Environment: Outdoor weather and environmental widgets.
Air quality: CO_2, PM2.5, and air quality display widgets.
Video Streaming: Camera and video display widgets.
3DM Essentials: Common 3DM.Space widgets and dashboard building blocks.

There are also specialised widgets available for more specific use cases, such as boat monitoring, combined weather station displays, and duty pump controller widgets.



 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

Widgets can be added in two main ways:

1. **Widget bundles** - Browse widgets by category. This is the easiest way to find groups of related widgets.
2. **All widgets** - Browse and select individual widgets directly. Click the widget and the properties will open. Once the properties are correct, save the widget and it will be added to the dashboard.

You can also use Import widget to bring in widgets from another dashboard or system. Imported widgets are handled in JSON format, allowing widgets to be copied, backed up, edited, or transferred between dashboards.

To add a widget, select the required widget from the list. 3DM.Space will then open the widget properties window. From there, you can configure the widget title, data source, telemetry keys, appearance, layout, units, actions, and other available settings.

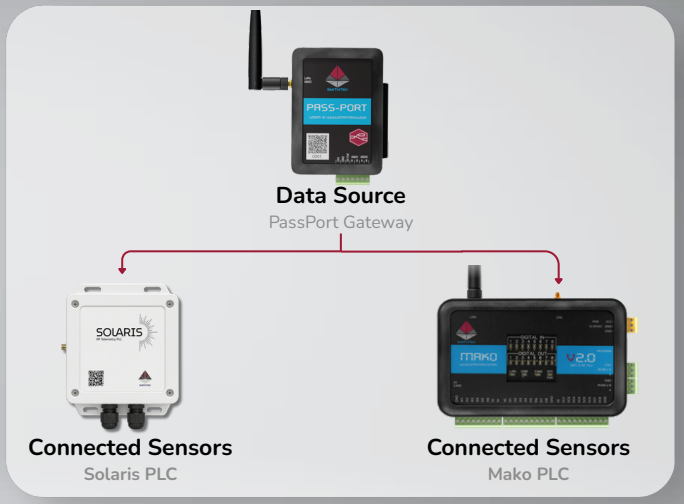
Example: Widget properties vary depending on the widget type.
A chart widget will have different settings to a button, map, alarm table, gauge, or SCADA symbol. Detailed information about common widget properties is explained at the end of this manual.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Dashboard Widget Data Source

After selecting a widget, you need to tell 3DM.Space where the widget gets its data from. This is called the data source. A Data source is a PassPort gateway deployed in the field capturing data from connected sensors

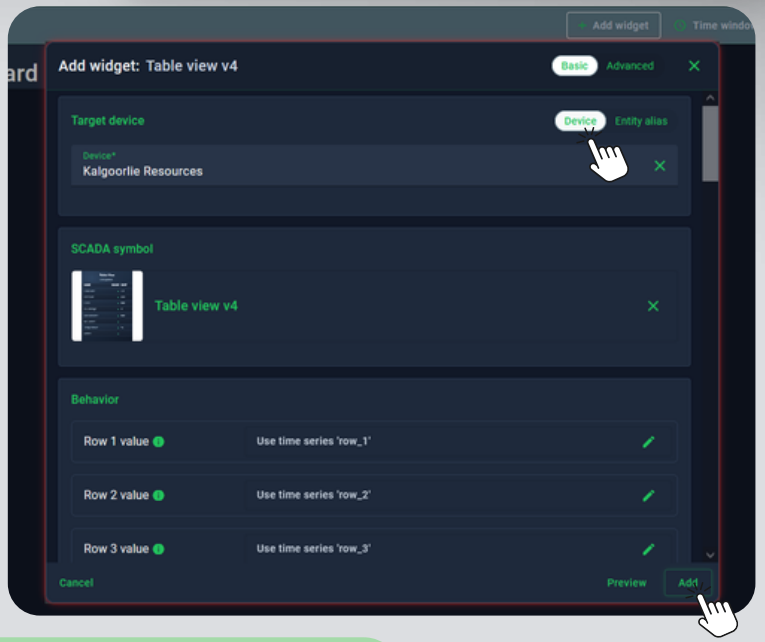
For most dashboards, the data source will be a device. Once the device is selected, you then choose the correct telemetry keys for the widget to display. These keys come from the live data being sent by the device, such as flow, pressure, tank level, voltage, pump status, alarm status, or other JSON variable keys. More detailed information about widget properties, data sources, and keys is explained later in this manual.



Basic example: adding a table widget

Steps:

1. First, create a **new dashboard** or open an existing dashboard.
2. **Click** + Add widget.
3. Select a **widget bundle**. Example: we selected **3DM Essentials**.
4. Select the required widget. Example: we selected **Table View V4**.
5. The **widget setup** window will open.
6. Under **Target device**, choose the device you want the widget to display data from.
7. In the Behaviour section, click the **pencil icon** next to the row you want to configure. A second settings window will open.
8. Set the action to Use time series.
9. Select the required key from the list of available variables.
10. These are the telemetry keys being sent by the device.
11. **Click Apply.** *Repeat this for any other rows or values the widget needs to display. You can click Preview to view the widget with live data before adding it to the dashboard.*
12. When you are happy with the setup, **click Add**.



Important:
A widget will only display data if the selected device is sending the matching telemetry key. If the wrong key is selected, or the device has not sent that key yet, the widget may appear blank or behaviour.

Simple rule:
Select the device first, then select the correct telemetry keys for the widget to display.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Widget Settings



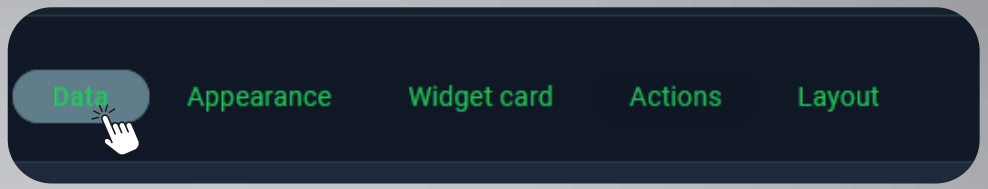
Widget settings
Widget settings are used to configure how a widget looks, what data it uses, and how users interact with it. To open widget settings, first **open the dashboard** in **Edit mode**, then click the **pencil/edit icon** on the widget you want to update.
This opens the widget settings window.

Widget settings can be shown in two main ways:

> **Basic settings** - Basic settings show the main widget configuration in a simpler layout. This usually covers the common setup options such as target device, data source, displayed values, units of measurement, decimal places, labels, colours, and general widget appearance.
> **Advanced settings -** Advanced settings break the widget setup into separate tabs or groups.

These tabs may include options such as:

Data
Controls the target device, telemetry variables, data keys, units, decimals, labels, and data formatting.
Appearance
Controls how the widget looks.
Widget card
Controls the card or container around the widget.
Actions
Controls what happens when a user clicks or interacts with the widget.
Layout
Controls widget layout and sizing behaviour.



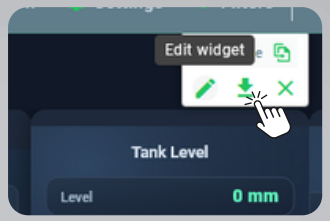
Data tab
The Data tab is where the widget is connected to a device or entity. In most 3DM.Space dashboards, this will be a PassPort Gateway. The data tab allows the widget to be linked to the correct telemetry values, such as tank level, pump status, voltage, pressure, flow rate, fault state, or any other data being sent into 3DM.Space.
The widget can be connected directly to a selected Device, or in some cases through an Entity alias. For standard PassPort Gateway dashboards, selecting the device directly is normally the simplest method.

Important:
Widget settings control how the dashboard behaves at the widget level. The dashboard may have its own time window, layout, and settings, but each widget may also have individual settings that control how it displays data. If a widget is not showing the expected value, check the widget Data settings first.

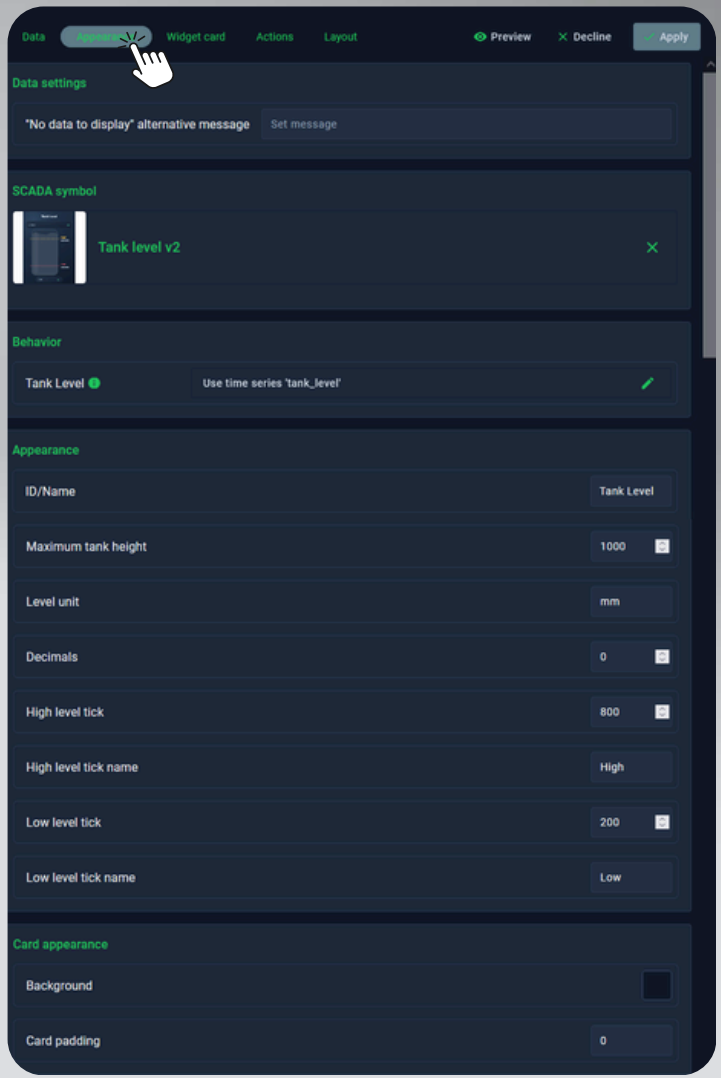
Simple rule:
Widget settings = configure one widget
Basic settings = common setup options
Advanced settings = detailed tabs and actions
Data = device and telemetry values
Appearance = how the widget looks
Actions = what happens when clicked
Apply = keep widget changes

Widget Settings - Appearance

Widget appearance settings



The Appearance tab controls the visual setup of the selected widget.
Appearance settings will be different depending on the widget type. A tank widget, chart widget, button widget, gauge widget, map widget, or SCADA symbol may all show different appearance options. Most appearance settings are designed to be intuitive. The options usually control how the widget looks, what labels are displayed, what units are shown, and how the widget should be presented on the dashboard.



Data settings

Data settings control what the widget should display when data is missing or unavailable.
For example, an alternative message can be shown if there is no data to display. This helps make dashboards cleaner and easier to understand when a telemetry value is missing, offline, or not yet received.

SCADA symbol

The SCADA symbol area controls the selected visual symbol or graphic used by the widget.
This is common for SCADA-style widgets where the widget uses a visual object such as a tank, pump, valve, motor, pipe, level indicator, or other process symbol. The selected symbol gives the widget its visual style.

behaviour

Behaviour controls how the widget uses the selected telemetry value.
This may include which telemetry variable is connected to the widget, how the value is used, or which data key drives the display. For example, a tank widget may use a tank level telemetry value to control the displayed tank level.

Appearance

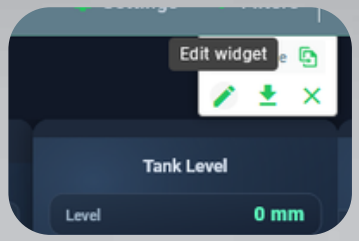
The Appearance section controls the main visual settings of the widget.
Depending on the widget, this may include:

- widget title or ID/name
- units of measurement
- decimal places
- minimum and maximum values
- high and low tick markers
- threshold labels
- special level markers
- colours
- text labels
- gauge ranges
- chart display options
- icon or symbol labels

These settings are normally used to make the widget match the real site value and display correctly for operators.

Important:
Appearance settings vary by widget, so not every widget will have the same options. Open the Appearance tab and work through the available settings from top to bottom. Use Preview to check changes before applying them.

Widget Settings - Widget Card



Widget card settings

The Widget card tab controls the outer card or container around the selected widget. These settings affect how the widget is displayed on the dashboard, including the widget title area, background, spacing, border style, shadow, and card buttons. Widget card settings may change depending on the widget type. Some widgets may show more options than others. Most settings are intuitive and control the visual presentation of the widget card.

Common widget card areas:

Card title

The Card title section controls the title area of the widget. This may include options such as displaying the widget title, changing the title text, adding a title tooltip, showing an icon, or adjusting advanced title styling. This is useful when the widget needs a clear label, such as Tank Level, Pump Status, Flow Rate, or Voltage.

Card style

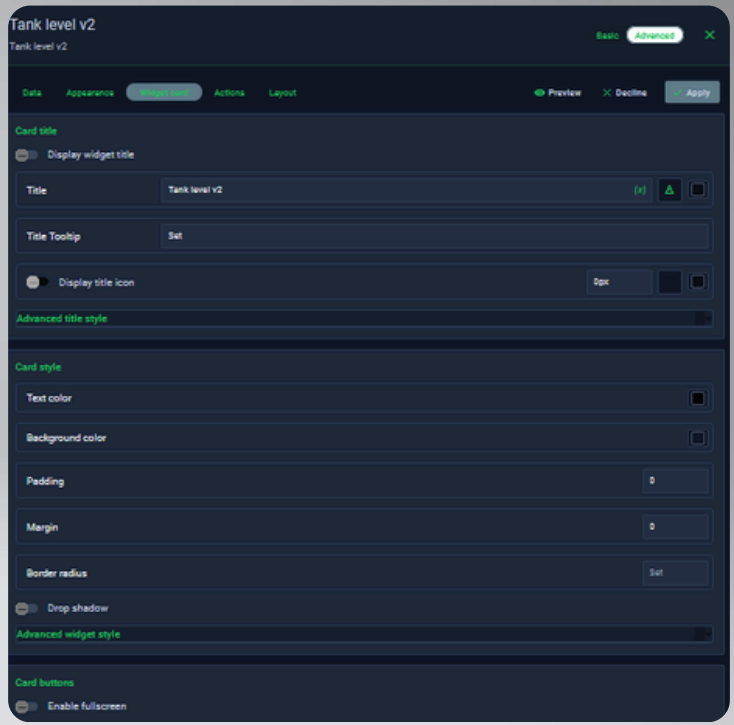
The Card style section controls the main visual style of the widget card.
This may include options such as:

- text colour
- background colour
- padding
- margin
- border radius
- drop shadow
- advanced widget styling

These settings are useful for making widgets match the dashboard design, creating cleaner layouts, or giving the dashboard a more polished SCADA-style appearance.

Card buttons

The Card buttons section controls buttons or extra actions available on the widget card. For example, this may include an option to enable full-screen mode for the widget. Card buttons can be useful when users need to expand a widget, view more detail, or interact with the widget in a specific way.



Important:
Widget card settings control the widget container, such as its background and padding. The telemetry value, unit, and behaviour are usually configured under the Data or Appearance tabs.

Simple rule:
Card title = widget heading and title display
Card style = background, spacing, border, shadow, and visual styling
Card buttons = extra widget actions
Widget card = the outer container around the widget

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Widget Settings - Actions

Widget actions

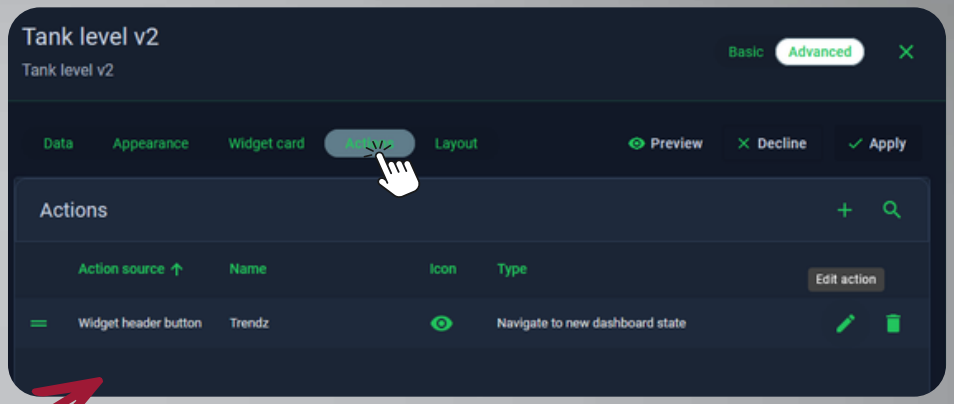


The Actions tab is used to add interactive actions to a widget. Actions allow a widget to do something when a user clicks a button, icon, row, symbol, or other interactive part of the widget. This is useful when building dashboards that need navigation, extra detail screens, popup views, or SCADA-style interaction.

Common action uses

Widget actions can be used for things such as:

- opening another dashboard state
- opening a detailed trend page
- linking to another dashboard
- opening a popup
- viewing Device or Asset Details
- adding a clickable button to a widget
- creating navigation from a SCADA symbol



Action table

The action table shows the actions currently configured for the widget.

Common columns include:

Action source

Shows where the action appears or what part of the widget triggers it. **Example:** Widget header button, this is the most common source and available on almost all widgets.

Name

Shows the name of the action. **Example:** Trends

Icon

Shows the icon used for the action button.

Type

Shows what the action will do. **Example:** Navigate to new dashboard state - click the tab on the widget and it will navigate to or open a new window.

Action options:

Add action

The + icon is used to add a new widget action.

Search

The search icon is used to find an existing action in the list.

Edit action

The pencil icon is used to edit an existing action.

Delete action

The trash icon deletes the action.

Important:

Widget actions can be very powerful and should be set up carefully. For simple dashboards, actions may not be needed. For SCADA dashboards, actions are useful for opening more detailed pages without crowding the main dashboard. A dedicated action setup section can explain the different action types in more detail.

Simple rule:

Actions = make widgets interactive
Action source = where the action appears
Name = action label
Icon = action button symbol
Type = what the action does
Add action = create new interaction

 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

How to add a widget action

Widget actions are added from the Actions tab inside widget settings.
An action allows the widget to do something when a user clicks or interacts with it. This may include opening another dashboard state, updating the current dashboard state, opening a popup, linking to another dashboard, or other configured actions. This page explains the basic action setup window. The different action types can be covered separately.

Action source

Action source controls where the action will appear or what part of the widget will trigger the action. **Example** sources may include a widget header button, widget click, row click, marker click, or another available interaction point depending on the widget type. The available action sources may change depending on the widget being edited.

Name

Name is the label used for the action. Use a clear name that explains what the action does. Example: View trends. Open details, Pump data, Tank history, Map view.

Icon

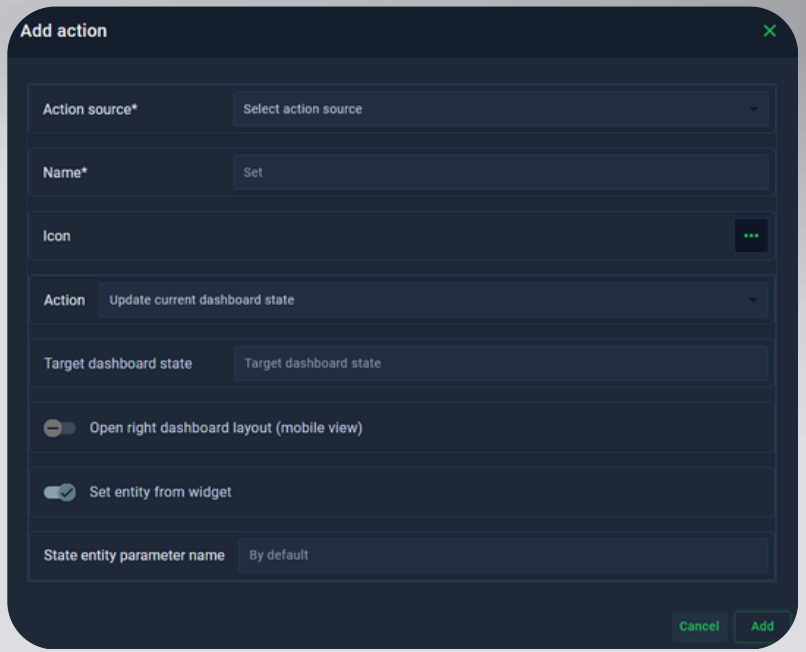
Icon controls the icon shown for the action. This is useful when the action appears as a button or shortcut on the widget. Choose an icon that makes sense for the action, such as a chart icon for trends, a map icon for locations.

Action

Action controls what the action will do. In the example shown, the selected action is: **Update current dashboard state** This type of action is used when the widget should change the currently displayed dashboard state, AKA change page or load a page like SCADA. Other action types may be available depending on the dashboard setup and widget type.

Target dashboard state

Target dashboard state is used to select which dashboard state should open or be used by the action. You create dashboard states in the dashboard settings.
Example: A main SCADA page may have a tank widget. The widget action can open a dashboard state showing tank trends, alarms, asset information, or map location.



 © 2026 Smithtek Pty Ltd. All rights reserved.

How to Add a Widget Action

Open right dashboard layout

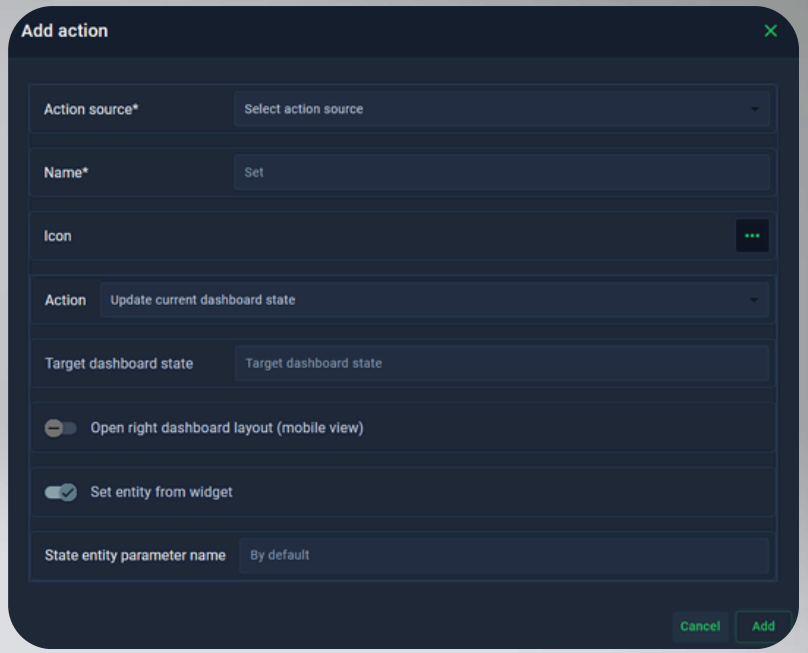
Open right dashboard layout is used for layouts that support a right-side dashboard area, such as divider or mobile-style layouts. This can be useful when the action should open information in the right side of the dashboard instead of replacing the current view.

Set entity from widget

Set entity from widget allows the selected widget entity to be passed into the action. This is useful when the same action should work dynamically depending on which device, asset, or entity the user clicked. **Example:** if a user clicks a specific tank, pump, or PassPort Gateway, the next dashboard state can use that selected entity.

State entity parameter name

State entity parameter name controls the parameter name used when passing the selected entity into the dashboard state. For most standard setups, this can usually be left as the default unless a custom dashboard state or widget configuration requires a specific parameter name.



Important:

Widget actions can make dashboards much more powerful, but they should be kept simple for operators. Use clear action names and only add actions that help the user navigate, view more detail, or complete an approved task.

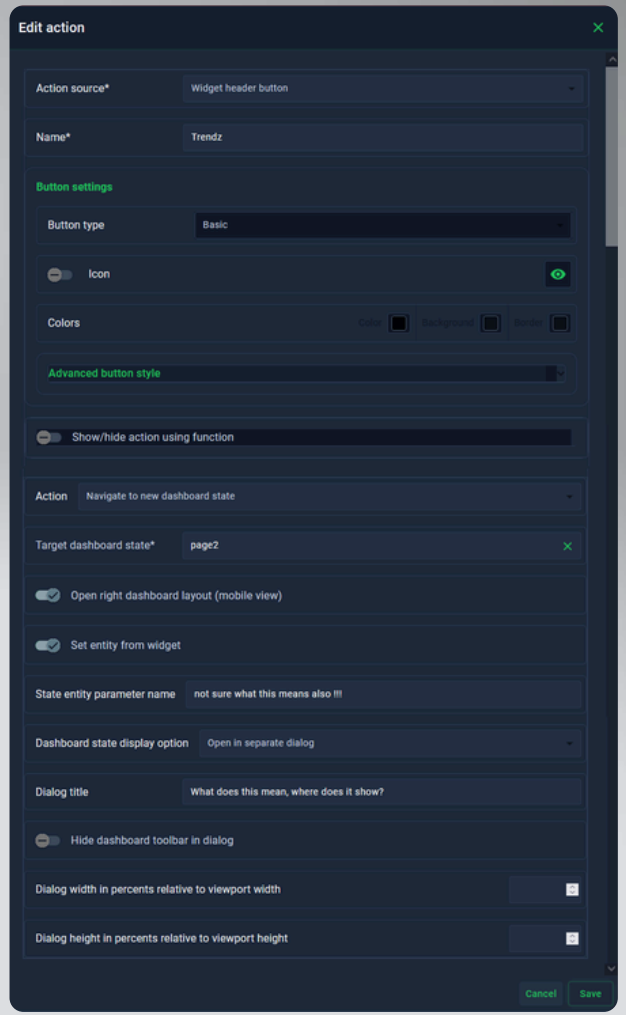
Simple rule:

Action source = where the action is triggered
Name = what the action is called
Icon = action button symbol
Action = what the action does
Target dashboard state = where the action opens
Set entity from widget = pass selected device or asset into the action
Add = create the action

 © 2026 Smithtek Pty Ltd. All rights reserved.

Editing a widget action

Widget actions can be edited after they have been created. This is useful when the action name, icon, button style, target dashboard state, dialog display, or action behaviour needs to be changed. To **edit an existing action**, open the **widget settings**, go to the **Actions tab**, then click the **pencil/edit** icon beside the action. For the basic fields such as Action source, Name, Icon, Action, and Target dashboard state, refer to the previous page: *How to add a widget action*.



Button settings

The Button settings section controls how the action button appears on the widget. This may include options such as button type, icon display, button colours, and advanced button styling. These settings are useful when the action appears as a widget header button or visible shortcut button. **Example:** A trend button may use an eye icon, chart icon, or information icon so the operator understands what the button does.

Show/hide action using function

This option can be used to show or hide the action based on custom logic. This is an advanced option and is normally only used when an action should appear under certain conditions, like faults or schedules. For standard dashboards, this can usually be left disabled.

Dashboard state display option

The Dashboard state display option controls how the selected dashboard state opens. Depending on the selected option, the state may open in the same dashboard area, the right dashboard layout, or in a separate dialog window. In the example shown, the selected option is: **Open in separate dialog**
This means the target dashboard state can open as a popup-style window instead of replacing the main dashboard view. This is useful when the user needs to quickly view extra information without leaving the main SCADA screen. **Example:** A tank widget opens a popup showing tank trend data, alarm history, and site details.

Dialog title

The Dialog title is the title shown at the top of the popup dialog when the dashboard state opens in a separate dialog. Use a clear title so the user understands what has opened. **Examples:** Tank Level Trends, Pump Details, Flow Meter History, Site Location, Alarm Details.

 © 2026 Smithtek Pty Ltd. All rights reserved.

How to Edit a Widget Action

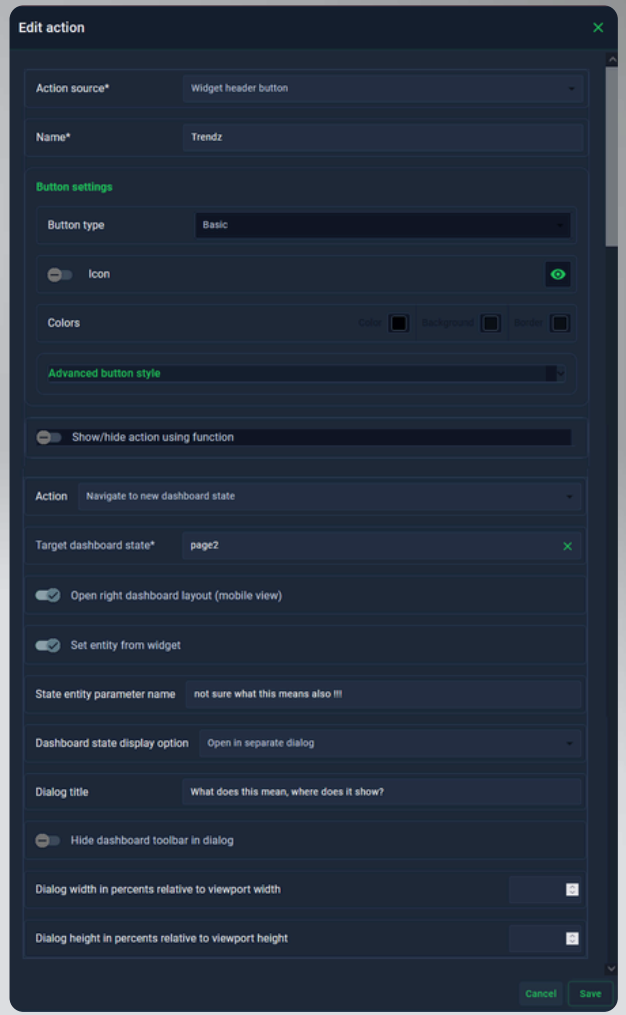
Hide dashboard toolbar in dialog
This option hides the dashboard toolbar inside the dialog window. This is useful when the popup should look clean and only show the information the user needs. For operator dashboards, hiding the toolbar can help prevent users from changing the time window, filters, or other dashboard options inside the popup.

Dialog width
Dialog width in percents relative to viewport width controls how wide the popup dialog appears compared to the screen width. **Example:** 80% means the dialog uses 80% of the screen width. A wider dialog is useful for charts, maps, and detailed information. A smaller dialog may be better for simple status details or quick control panels.

Dialog height
Dialog height in percents relative to viewport height controls how tall the popup dialog appears compared to the screen height. **Example:** 70% means the dialog uses 70% of the screen height. This is useful when the popup needs enough space for charts, tables, or multiple widgets

Important:
When editing an action, keep the user experience simple. The action should clearly tell the user what it does. Use clear names, suitable icons, and popup titles that match the information being opened.

Simple rule:
Edit action = change an existing widget action
Button settings = how the action button looks
Display option = how the target state opens
Dialog title = popup window heading
Dialog width/height = popup size
Save = keep the action changes

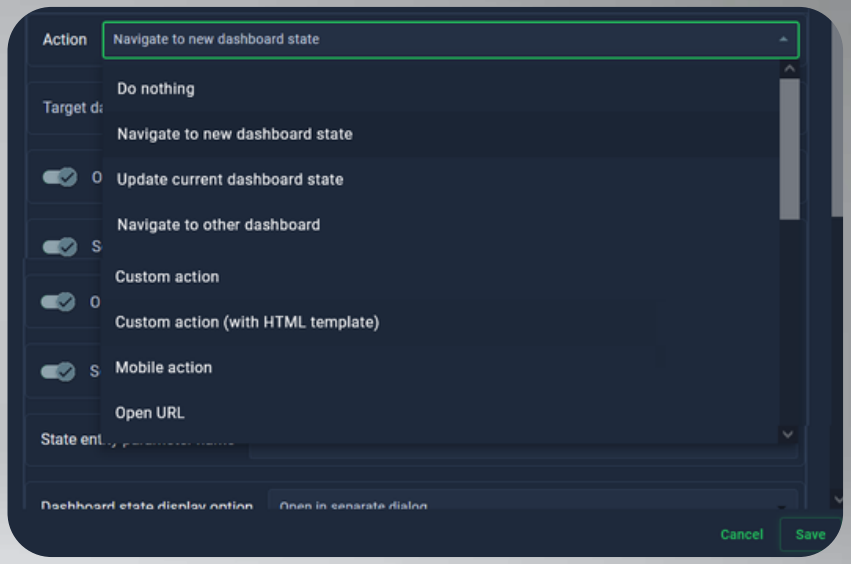


 © 2026 Smithtek Pty Ltd. All rights reserved.

Widget action types

Widget actions control what happens when a user clicks or interacts with a widget.
The action type decides what the widget will do.

Do nothing:
Do nothing means the action is disabled or does not perform any operation. Use this when an action source exists, but no action should happen yet.
Use case:
A widget has a clickable area, but the action is temporarily disabled while the dashboard is still being built.
Navigate to new dashboard state
Navigate to new dashboard state opens another dashboard state as a new view. This is useful when the user should move from the current dashboard state to a different dashboard state.
Use case:
Click a pump symbol on the main SCADA page to open a dedicated pump details page with trends, runtime, alarms, and controls.
Update current dashboard state
Update current dashboard state changes the current dashboard state without opening a separate new state view. This can be used when the existing dashboard view should update based on the selected widget or entity.
Use case:
Click a tank in a site overview and update the current dashboard state to show that tank's telemetry, trends, or details.
Navigate to other dashboard
Navigate to other dashboard opens a different dashboard. This is useful when the user needs to move from one dashboard to another.

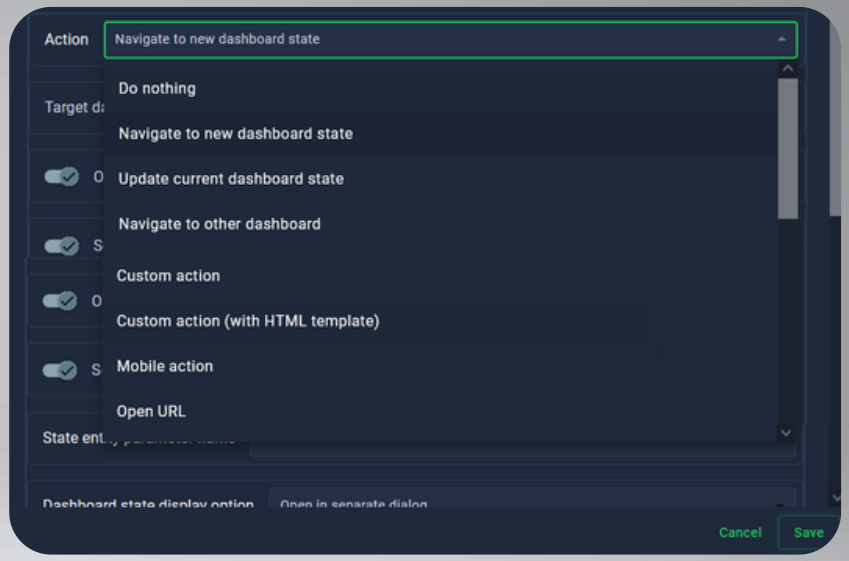


Use case:
Click a tank in a site overview and update the current dashboard state to show that tank's telemetry, trends, or details.
Navigate to other dashboard
Navigate to other dashboard opens a different dashboard. This is useful when the user needs to move from one dashboard to another.
Use case:
Click a button on a customer overview dashboard to open that customer's detailed irrigation dashboard.
Custom action
Custom action allows a custom function or script-based action to be configured. This is an advanced option and is normally used when the dashboard needs behaviour outside the standard action list.

 © 2026 Smithtek Pty Ltd. All rights reserved.

Types of Actions

Custom action
Custom action allows a custom function or script-based action to be configured. This is an advanced option and is normally used when the dashboard needs behaviour outside the standard action list.
Use case:
Run custom logic when a widget is clicked, such as preparing selected data before opening another dashboard view.
Custom action with HTML template
Custom action with HTML template allows a custom action to be displayed using an HTML template. This is useful for advanced popup-style content, custom messages, or custom formatted information.
Use case:
Click a device card and open a custom HTML popup showing formatted site notes, maintenance information, or equipment details.
Mobile action
Mobile action is used for actions designed for mobile dashboard behaviour. This can be useful when the dashboard is viewed from a phone or tablet and needs mobile-specific interaction.
Use case:
Tap a site card on a mobile dashboard to open a mobile-friendly detail screen or action panel.
Open URL
Open URL opens a web link. This can be used to send users to an external page, document, camera feed, map link, support page, or related system.
Use case:
Click a camera icon on a dashboard to open an external CCTV web page or site documentation link.



Simple rule:
Do nothing = no action
Navigate to new dashboard state = open another state
Update current dashboard state = change current view
Navigate to other dashboard = open another dashboard
Custom action = advanced custom behaviour
Custom action with HTML template = custom formatted popup/content
Mobile action = mobile-specific behaviour
Open URL = open an external link

 © 2026 Smithtek Pty Ltd. All rights reserved.



3DM.Space Node-RED nodes

The 3DM.Space Node-RED nodes are installed on the PassPort Gateway and are used to connect the PassPort to 3DM.Space.
These nodes allow the PassPort to send live telemetry up to 3DM.Space, receive remote commands back from dashboards, store control settings locally, and prepare data before it is sent to the cloud.

The nodes are designed to make the connection between Node-RED, the PassPort Gateway, and 3DM.Space simple to configure. Instead of building the full cloud connection manually, the user copies the PassPort device credentials from 3DM.Space into Node-RED, then selects the correct 3DM nodes inside their flow.

The main 3DM.Space Node-RED nodes are:

3DM Cloud Login

Stores the PassPort device credentials copied from 3DM.Space.
This login is used by the other 3DM nodes to connect to the correct PassPort Gateway in the cloud.

3DM Out

Sends telemetry from the PassPort Gateway up to 3DM.Space.
This is used for live values such as tank level, pump status, voltage, pressure, flow rate, fault status, and other site data.

3DM In

Receives values sent from 3DM.Space down to the PassPort Gateway.
This is used for remote commands, setpoints, mode changes, reset commands, scheduler updates, and SCADA button commands.

3DM Config Store

Stores settings received from 3DM.Space and allows the PassPort to keep using those settings locally.
This is useful for schedules, setpoints, control limits, and smart local control logic.

3DM Join

Combines multiple JSON payloads into one clean payload before sending it to 3DM.Space.
This is useful when data comes from multiple PLCs, Mako RF nodes, sensors, or field devices.

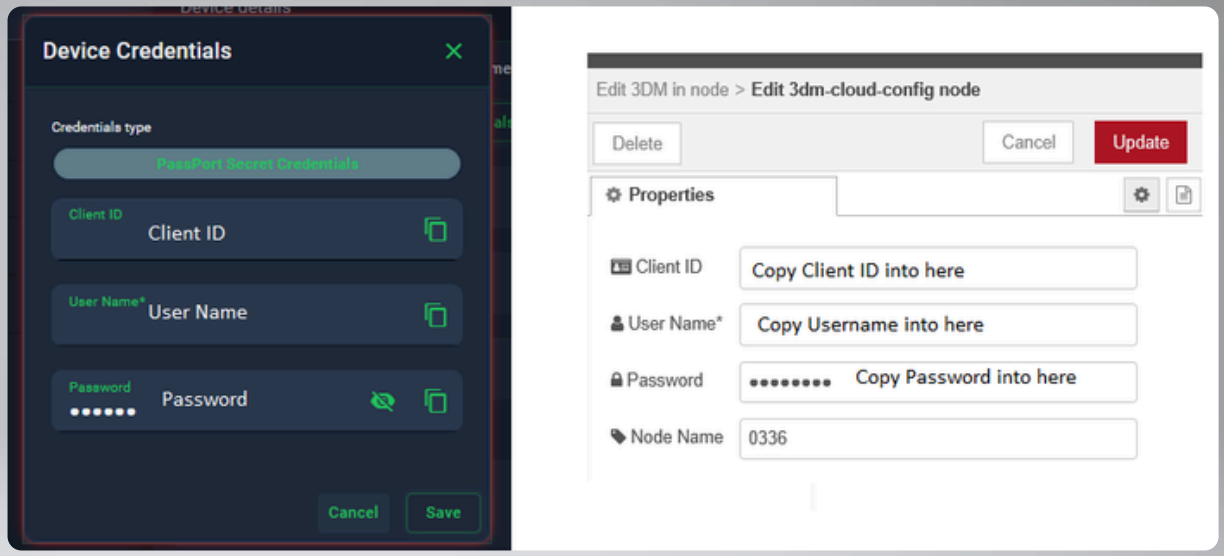
 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Nodes (Node-RED)

Basic methodology:

Steps

1. Create or **open** the **PassPort Gateway** device in **3DM.Space**.
2. Open the **PassPort** device credentials.
3. **Copy** the Client ID, User Name, and Password.
4. **Open Node-RED** on the PassPort Gateway.
5. Add or open the 3DM Cloud Login node.
6. Paste the copied credentials into the matching fields.
7. **Add** the **required 3DM nodes** to the flow.
8. **Deploy** the Node-RED flow.
9. Confirm the **PassPort** is sending data to **3DM.Space** and receiving commands correctly.



How the data flow works

Live site data is normally collected by Node-RED from local equipment, sensors, PLCs, RF nodes, Modbus devices, or function logic. That data is sent through the 3DM Out node to 3DM.Space as telemetry.

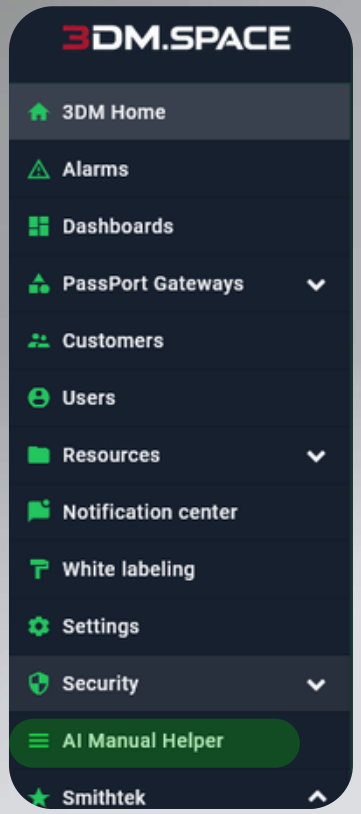
Remote commands work in the opposite direction. A dashboard button, setpoint, scheduler, or SCADA control sends a shared attribute from 3DM.Space down to the PassPort. The 3DM In node receives that value inside Node-RED, where it can then be passed to a PLC, relay, Mako RF node, function node, or local control flow. from the Smithtek side menu.

Important:
The credentials in 3DM.Space must match the credentials entered into the 3DM Cloud Login node. If the credentials are wrong, the PassPort will not sync correctly with 3DM.Space. The 3DM Out node is used for telemetry going up to the cloud. The 3DM In node is used for commands and settings coming back down to the PassPort.

Full Node-RED node guide

For the full Node-RED setup guide, examples, payload formats, node settings, and troubleshooting information, open 3DM.Space, the Node-RED Nodes link from the Smithtek side menu.

 © 2026 Smithtek Pty Ltd. All rights reserved.



AI Manual Helper
The AI Manual Helper tab opens an AI assistant that has been trained on 3DM.Space information.
It can be used to ask questions about how to complete tasks inside 3DM.Space, such as setting up users, creating groups, configuring dashboards, managing PassPort Gateways, setting alarms, or finding the correct setup method.

Users can type a question in plain English, and the AI Manual Helper will provide guidance based on the 3DM.Space manual and platform setup process.

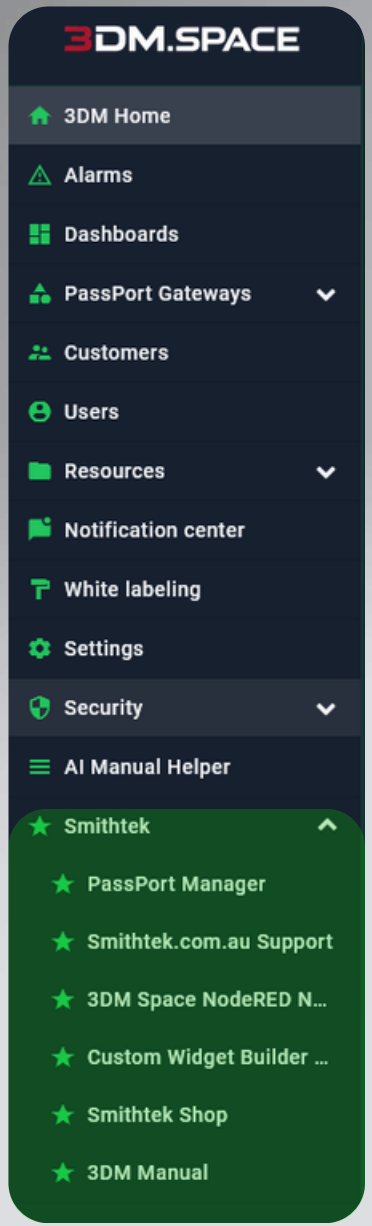
Example questions
How do I add a new user?
How do I give someone access to a dashboard?
Why is my dashboard not showing data?
How do I create an alarm rule?
How do I add a PassPort Gateway?
What is the difference between telemetry and attributes?

Important:
The AI Manual Helper is designed to support users with setup steps and general guidance.
For hardware faults, account access issues, or advanced technical support, users should still contact Smithtek support.

Simple rule:
AI Manual Helper = ask questions about how to use 3DM.Space

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM Smithtek Side Tab



Smithtek side menu

The Smithtek side menu provides quick access to Smithtek tools, support links, product information, and 3DM.Space resources. These links are added to help users find the correct support pages, documentation, hardware shop, and connected Smithtek services without needing to search for them manually.

Smithtek menu options:

PassPort Manager

Opens the PassPort Manager portal directly inside 3DM.Space. This allows users to access gateway management without opening a separate browser window.

Smithtek.com.au Support

Opens the Smithtek support page. Use this link when help, service information, product support, or technical assistance is required.

3DM Space Node-RED Nodes

Opens the information page for the 3DM.Space Node-RED nodes used on the PassPort Gateway. This page includes the full Node-RED node user manual in Markdown format.

Custom Widget Builder

Opens the custom widget builder instructions. This page explains how to build custom 3DM.Space widgets and includes the AI prompt used to help generate widget code.

Smithtek Shop

Opens the Smithtek hardware shop. This can be used to view or purchase compatible Smithtek products and hardware.

3DM Manual

Opens the 3DM.Space user manual for platform setup, dashboards, users, roles, PassPort Gateways, alarms, notifications, and general guidance.

Important:
The Smithtek side menu is designed as a shortcut area. It does not replace the main 3DM.Space setup menus, but it gives users faster access to common support and documentation links.

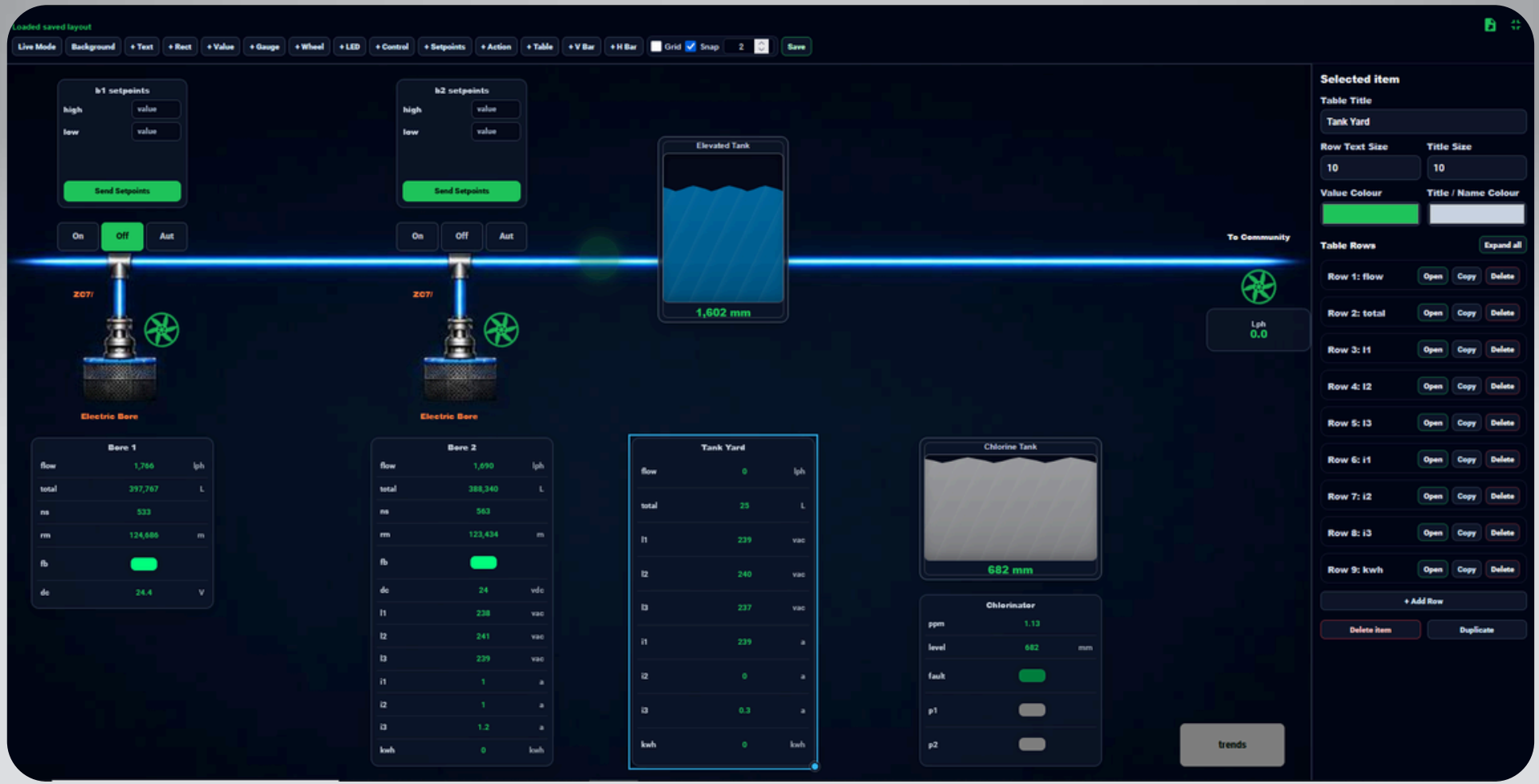
Simple rule:
Smithtek menu = quick access to Smithtek tools, support, manuals, and hardware links

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM SCADA Canvas Widget

The **3DM SCADA** Canvas is the main **dashboard-building widget** used to create SCADA-style screens in 3DM.Space.
It gives users one flexible widget that can display **live values, equipment status, gauges, level bars, indicators, buttons, setpoints, background images,** and **simple process layouts** from one canvas area. This makes it useful for pumps, tanks, bores, irrigation systems, treatment plants, generators, remote sites, and general telemetry projects.

The canvas is designed so dashboards can be built visually. Items can be added, moved, resized, and configured directly on the screen, making it suitable for both simple monitoring dashboards and more detailed SCADA-style views.



 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

SCADA Canvas Widget

What the SCADA Canvas can do

The SCADA Canvas can be used to:

- display live telemetry values
- show pump, tank, valve, motor, or equipment status
- create visual site layouts using background images
- add gauges, bars, tables, LEDs, and run indicators
- send remote start, stop, on, off, mode, or reset commands
- update setpoints from the dashboard
- open detail pages, popups, trends, or dashboard states
- work with 3DM Node-RED nodes running on the PassPort Gateway

How it works

The SCADA Canvas works with the data being sent between the PassPort Gateway and 3DM.Space. Live field data is sent from the PassPort to 3DM.Space using telemetry. The canvas then displays those values using items such as gauges, values, bars, LEDs, tables, and indicators.

Remote commands work in the opposite direction. When a user presses a button or changes a setpoint on the canvas, the command is sent from 3DM.Space down to the PassPort Gateway using shared attributes. The PassPort can then use Node-RED logic to control connected equipment.

Typical data flow

Live data

Field equipment → PassPort Gateway → 3DM.Space telemetry → SCADA Canvas display

Remote command

SCADA Canvas button → 3DM.Space shared attribute → PassPort Gateway → Node-RED / PLC / relay / RF command

Smart local control

SCADA Canvas setting → shared attribute → PassPort Gateway → 3DM Config Store → local control logic

Important:
When adding the SCADA Canvas to a dashboard, only the live telemetry variables that need to be displayed should be added to the widget data source. Command keys, setpoints, and smart control settings are handled internally by the widget using attributes and do not normally need to be added as displayed telemetry variables.

Simple rule:
Telemetry = live data shown on the canvas
Shared attributes = commands sent from the canvas to the PassPort
SCADA Canvas = one visual widget for building complete dashboard screens

 © 2026 Smithtek Pty Ltd. All rights reserved.

SCADA Canvas Tools and Widgets Explanation

Live mode
Switches the canvas from editing mode into live operating mode. Use this when the SCADA screen is ready to view or operate.

Save
Saves the current SCADA canvas layout and changes.

Snap to grid
Locks item movement to the grid, making it easier to line objects up neatly

Show grid
Shows or hides the grid behind the canvas to help align objects.

Grid size %
Controls the grid spacing size. A smaller value gives finer positioning, while a larger value gives wider grid spacing.

Background
Adds or changes the background image behind the SCADA canvas. This may be a site layout, process diagram, pump station image, map, or custom SCADA graphic.

+ **Panel**
Adds a panel or rectangle. This is useful for grouping values, buttons, or equipment sections.

+ Line
Adds a line to the canvas. This can be used for pipework, flow paths, separators, or simple process diagrams.

+ Action
Adds a dashboard action button. This can be used to open popups, trend views, detail pages, or other dashboard states

+ Text
Adds a text label to the canvas.

+ Control
Adds a control button for commands such as start, stop, on, off, auto, reset, or mode selection

+ Setpoints
Adds a setpoint table or setpoint entry area for values such as start level, stop level, pressure limits, or control settings.

+ Value
Adds a live telemetry value display.

+ Gauge
Adds a gauge for values such as pressure, flow, level, voltage, or speed.

+ Wheel
Adds a spinning run indicator, commonly used for pumps, motors, fans, or rotating equipment.

+ LED
Adds an LED status indicator for run, fault, alarm, valve, relay, or communication states.

+ Table
Adds a table for showing multiple telemetry values in one area.

+ H Bar
Adds a horizontal bar display, useful for progress-style values, pump speed, percentage, or load.

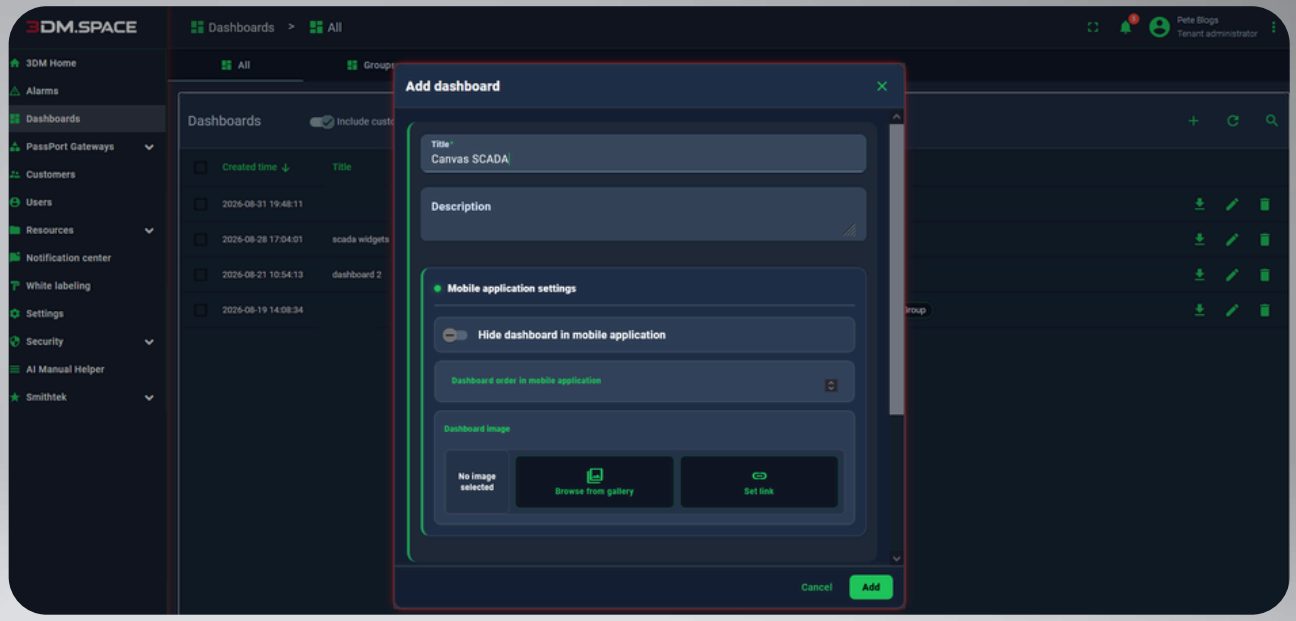
+ V Bar
Adds a vertical bar display, commonly used for tanks, levels, storage, battery level, or chemical level.

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM SCADA Canvas Set-up

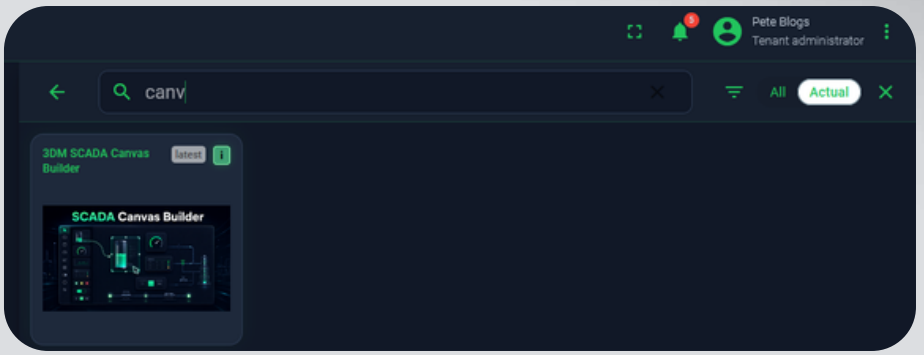
Adding the SCADA Canvas widget

The 3DM SCADA Canvas Builder is added to a dashboard like any other widget. Before adding the canvas, make sure the required PassPort Gateway has already been created in 3DM.Space and is sending telemetry data. The available telemetry keys from the PassPort can then be selected and imported into the widget.



Steps

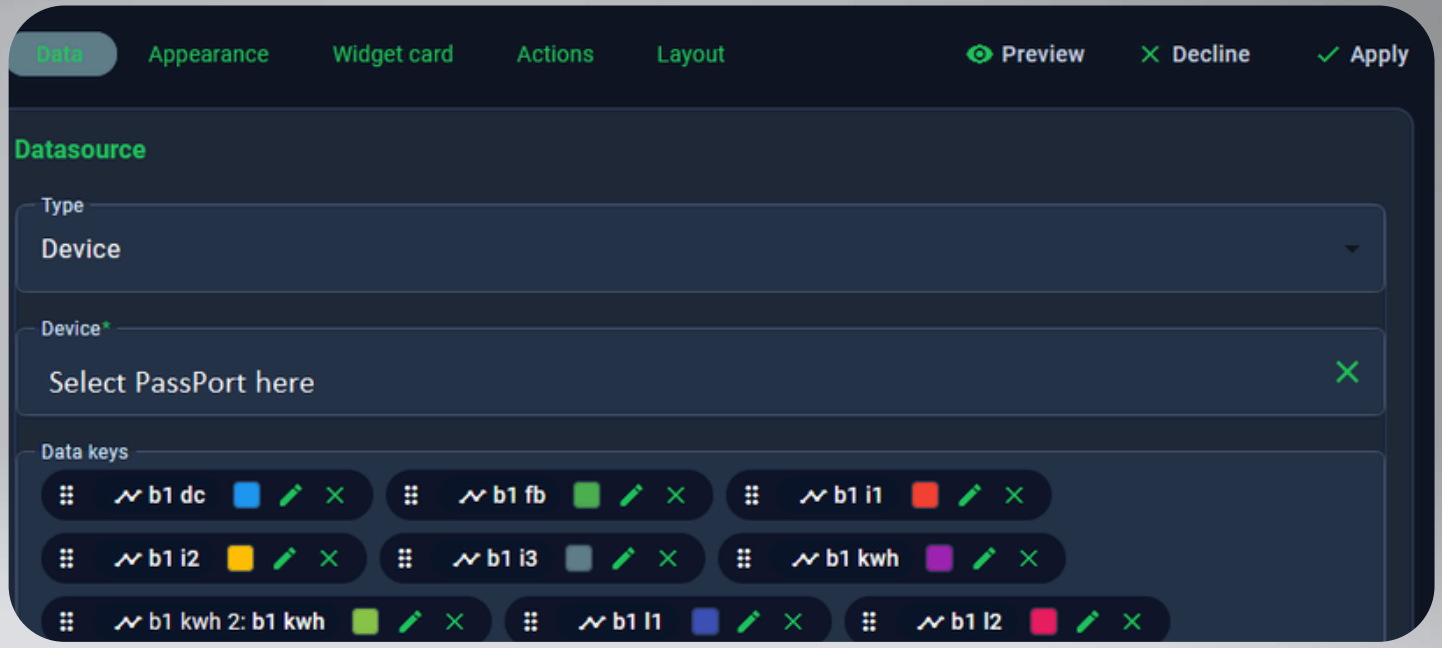
1. Go to **Dashboards.**
2. Create a **new dashboard** or open an existing dashboard.
3. Click **Edit mode**.
4. Click **Add widget**.
5. In the widget search, search for: **3DM SCADA Canvas Builder**



 © 2026 Smithtek Pty Ltd. All rights reserved.

SMITHTEK

6. **Select** the **3DM SCADA Canvas Builder** widget.
7. Set the **data source type** to Device.
8. Select the required **PassPort Gateway.**
9. Select the **available telemetry data** keys you want to use on the canvas. These keys are the live values being sent from the PassPort Gateway, such as tank level, pump status, voltage, flow rate, pressure, run feedback, or fault status.
10. **Add the widget** to the dashboard.
11. Stretch or resize the widget to the required screen size.
12. **Click Save** on the dashboard. Once the widget has been added and saved, the SCADA screen can be edited from inside the widget's own canvas editor.



Important
Only select the telemetry keys that need to be displayed or used visually on the canvas. Remote command keys and setpoints are normally handled through shared attributes inside the widget controls and do not need to be added as telemetry display keys.

Simple rule:
Add widget = place the SCADA Canvas on the dashboard
Device = select the PassPort Gateway
Data keys = live telemetry values available to the canvas
Resize = set the canvas screen size
Save = keep the dashboard changes

 © 2026 Smithtek Pty Ltd. All rights reserved.

3DM SCADA Canvas Tips and Tricks

The SCADA Canvas has its own editing and live operating modes.

Use **Edit mode** when building or changing the SCADA screen. In Edit mode, users can add new items, move objects, change settings, update setpoints, adjust controls, and change the background image.

Use **Live Mode** when the SCADA screen is ready to run. In Live Mode, the dashboard becomes the operating screen and the configured buttons, controls, indicators, values, and actions can be used.

Saving changes
Always press Save after making changes to the SCADA Canvas.
Saving keeps the canvas layout, item settings, and control settings.
If the canvas includes a control item, setpoint table, or smart control setup, pressing Save can also send the updated configuration to the remote PassPort Gateway.
This is important because the PassPort uses these settings for local control logic.

Smart control behaviour
The Control item can do more than send a simple button command.
It can send commands, setpoints, modes, and smart control settings down to the PassPort Gateway. These settings are received by Node-RED and can be stored locally using the 3DM Config Store node. This allows the PassPort to remember the latest settings and keep running local control logic even during a temporary communications outage.

Example:
AUTO mode
Low start setpoint
High stop setpoint
Pump in / pump out direction
Remote key to watch

For the full Node-RED node manual, open Smithtek > 3DM Space Node-RED Nodes from the side menu.

Background images
A background image can be added or changed at any time.
This may be a site layout, pump station drawing, process diagram, map, equipment image, or custom SCADA background.
Keep background images under 1 MB where possible. If the image is too large, the app will prompt the user before it is accepted.

Useful setup tips
Only add telemetry data keys that need to be displayed or used visually on the canvas.
Command keys, setpoints, and smart control settings are handled through attributes and do not normally need to be added as displayed telemetry variables.
Use separate feedback indicators for real equipment status.
For example, a control button may send Pump ON, but an LED or run indicator should use live telemetry feedback from the PassPort to show whether the pump is actually running.

Simple rule:
Edit mode = build and change the SCADA screen
Live mode = run and operate the SCADA screen
Save = keep changes and upload control settings
Telemetry = live values displayed on the canvas
Shared attributes = commands and settings sent to the PassPort
Config Store = remembers smart control settings locally

 © 2026 Smithtek Pty Ltd. All rights reserved.

Software Support and Warranty
Smithtek Pty Ltd provides reasonable support for supplied Smithtek software, platform configuration, and related software tools where they are used under normal conditions and in accordance with Smithtek guidance.
Where a confirmed software issue is identified, Smithtek Pty Ltd may, at its discretion, investigate the issue, provide support, apply updates, issue fixes, or provide a reasonable workaround.

Software is dependent on configuration, internet connectivity, cloud services, user access, browser compatibility, third-party systems, and the customer's operating environment. For this reason, Smithtek does not guarantee uninterrupted access, continuous operation, or compatibility with every external system, device, browser, network, plugin, API, or customer configuration.

This software support does not cover:

- **Issues caused by incorrect setup, misuse, unauthorised changes, or unsupported configuration**
- **Problems caused by internet outages, network faults, SIM card issues, power issues, cloud interruptions, or third-party service providers**
- **Issues caused by changes to third-party software, browsers, operating systems, APIs, plugins, or external platforms**
- **Loss of data caused by user error, deleted devices, deleted dashboards, incorrect retention settings, or unauthorised access**
- **Custom scripts, flows, dashboards, widgets, or integrations not approved or supplied by Smithtek**
- **Problems caused by hardware faults, field wiring, installation issues, power supply faults, or environmental conditions**
- **Dissatisfaction due to buyer's remorse or a change in customer requirements after delivery**
- **Any condition resulting from unsupported edits, incorrect maintenance, or failure to follow Smithtek guidance**

Smithtek Pty Ltd will make reasonable efforts to maintain and support the software; however, software systems may require updates, maintenance, configuration changes, and occasional troubleshooting.
To request support or report a software issue, please contact our support team at:
www.smithtek.com.au/support

You may be asked to provide account details, screenshots, error messages, device information, or steps to reproduce the issue. This statement does not limit any rights you may have under applicable Australian consumer law.



 © 2026 Smithtek Pty Ltd. All rights reserved.



Our Mission

At Smithtek, we are a proud family-run business dedicated to empowering industries, communities, and remote operators across Australia. Our mission is to deliver reliable, locally built telemetry and automation solutions that simplify how people monitor, control, and manage their assets, from water and energy to environmental systems.

Built on the values of trust, integrity, and innovation, we believe technology should be practical, transparent, and designed to last. Every product we create represents our family's commitment to quality, honesty, and hands-on support. By combining robust Australian hardware with intuitive cloud platforms, we help our clients gain Realtime visibility, improve efficiency, and make confident decisions, wherever they are.

CONTACT US

Unit 2/13 Mackinnon Street,
Rockingham, WA 6168.
(08) 61189176
Info@smithtek.com.au
www.smithtek.com.au
www.3dm.space
https://www.linkedin.com/company/smithtek-pty-ltd/

 © 2026 Smithtek Pty Ltd. All rights reserved.