



Setting up teamSOS Enterprise

Configure your users, teams, incident types and templates

This guide walks you through a clean set-up of teamSOS Enterprise — the key configuration steps, how everything fits together, and how to test it before you go live. **Work through it in order: users first, then teams, then the incident types and templates that sit on top of them.**

Before you start: If your organisation has just been created, you will be taken through the **Onboarding Wizard** first. That covers users, response teams and Desktop Alerts deployment. This guide picks up where the wizard leaves off and covers the full set of Configuration in the Admin Portal.

STEP 1 · Add your team members

You must add your users to teamSOS before the system can be used. There are three ways to do it — you can mix and match, but pick one as your main route so your user list stays predictable.

1 Add users manually

Go to **User Management** and click **Invite New User**. Enter each user's first name, surname and email, then click **+Add** for more people and **Add Users** to finish. Best for a small number of users or one-off changes.

2 Import users from a spreadsheet

Go to **User Management > Import Users**, click **+Upload**, download the CSV template, fill it in with your users' names, emails and roles, then upload it and click **Import**. Best when you already have a staff list to work from.

3 Sync users from Active Directory (Entra)

If your organisation uses Microsoft Entra (formerly Azure AD), you can synchronise users automatically from your directory so teamSOS stays in step with your current staff list. You can also enable **Single Sign-On** so users sign in with their existing organisational credentials. Set this up from **Admin > User Management > Manage Users**.

Please note: The Entra option only appears if your email address is associated with an Entra tenant. Email invites are not sent automatically when you import or sync — trigger them from **Manage Users > Email Invites** when you are ready for staff to log in.

User roles

A user's role determines what they can see and do. Set it when you add the user, or change it later from User Management > Manage Users.

Role	What it allows
User	Respond to incidents, raise new incidents, take part in chats, have tasks assigned, and receive announcement alerts.
Admin	Full access to all teamSOS features — create, edit and manage users, Configuration and incidents, configure other users' permissions, and make announcements.
Announce	Make announcements within teamSOS without full admin access. This permission is required for lockdown functionality.

Windows sign-in: On managed Windows devices teamSOS recognises the Windows login and prompts the user to sign in with those credentials, so most staff will not need to enter a password manually.

STEP 2 · Set up Response Teams

Response Teams are the groups of staff assigned to specific incident types — for example "First Aid", "Safeguarding" or "Site Management". They decide who gets notified when an incident is raised.

1

Create the team

Go to **Response Teams** and click **Create**. Give the team a name and click **Save**.

2

Add your people

Click **Edit**, select the users who should belong to the team, then **Save**.

STEP 3 · Create Managed Groups

Managed Groups organise users into membership groups for targeted announcements — for example "Year 6 Staff" or "Incident Management Team". Use them to send the right message to the right people rather than to everyone.

- Go to **Managed Groups** and click **Create**.

- Add a name and, if you want one, an icon.
- Select the users who belong to the group and click **Save**.

Worth knowing: Managed Groups are also used when you target Desktop Alerts, so it is worth setting these up before you configure your announcement templates.

STEP 4 · Set up Incident Types

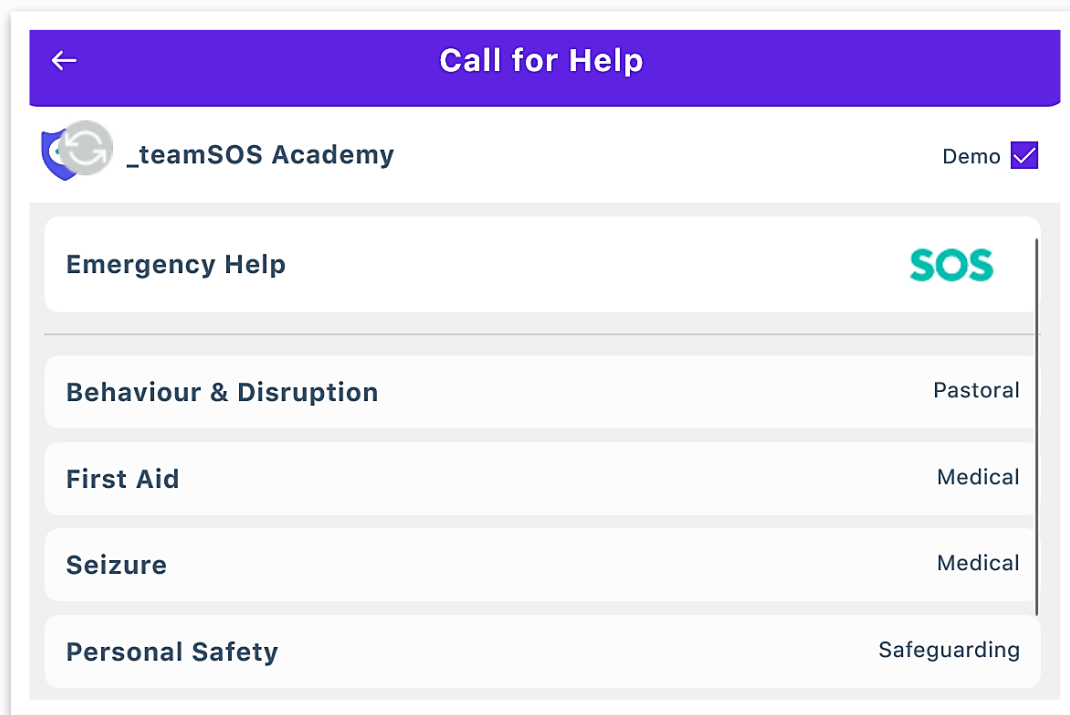
Incident Types are the categories staff choose when they need help. Each type defines the nature of the situation so the right team responds. They appear as menu buttons in the app.

INCIDENTS **Everyday issues**

Situations such as classroom removal or behaviour support. The user sees a detail screen before the incident is raised, so they can add notes and tags.

EMERGENCIES **Urgent, high-risk**

Situations such as Lockdown or Student Violence. These bypass the detail screen and are created instantly after a short countdown.



The Call for Help menu — Incident Types and Emergency Types as staff see them

How to create an Incident Type

- Go to **Admin > Configuration > Incident Management > Incident Types** and click **Create**.
- Enter a name (for example "Classroom Removal") and, optionally, an icon.
- Configure the Configuration below, then save.

Visibility and display

- **Hidden** — hide the type from staff while you finish configuring it.
- **Display Order** — controls how prominently it appears in the app. Put Lockdown at the top.

Assign to a team

- **Response Team** — who is notified when this type is raised.
- **Group Type** — organises types into categories (for example "Medical" or "Behaviour") for easier filtering.

Alerts and escalation

- **Longer Alert Sound** — makes the alert more noticeable.
- **Show First Responder in Timeline** — displays who responded first.
- **First Arrival is First Responder** — automatically assigns the first viewer.
- **Assign Only One Responder** — prevents several people from picking up the same incident.
- **SOS Team if Unresponded** — escalates to a backup team if nobody responds in time.
- **Repeat Alert** — how often the alert repeats, in 30-second intervals.
- **Stop Repeating After** — a time limit for repeated alerts.
- **Start Hunting After** — when escalation to another team begins.

Hunt Group Routing (escalation)

Create a custom escalation path for when a Response Team does not respond.

- Click **Show Custom Routing**.
- Tick **Custom Hunt Path**.
- Add teams in the order they should be notified, then **Save**.

Task Lists (optional)

Task Lists give staff step-by-step guidance during an incident — a lockdown procedure or a medical checklist, for example. Once attached to an Incident Type, the list appears automatically whenever that type is raised.

- Go to the relevant **Incident Type > Edit > Task List**.
- Add the steps in the order they should be followed.

Naming change: Task Lists were previously called **Playbooks**. If you have older documentation or training material that refers to Playbooks, it means the same thing.

STEP 5 · Set up Emergency Types

Emergency Types are critical situations needing an immediate response — "Evacuation", "Lockdown", "Medical Emergency". They bypass the usual incident detail screen and are created instantly after a short countdown.

- Go to **Admin > Incident Management > Emergency Types** and click **Create**.
- Enter a name, an icon and the responding team.
- Configure visibility, display order, alerts, escalation and hunt group exactly as you would for a standard Incident Type.

STEP 6 · Set up Templates

Templates save time and keep your communications consistent. They pre-fill content, structure responses and can include recipient groups automatically.

Heads up: The template creation interface was redesigned in May 2026 with a cleaner layout. The options below are unchanged — but if you are following older screenshots, the arrangement on screen will look different.

Announcement Templates

Pre-written alerts you can send in one tap — "Lockdown in progress", for example. Go to **Admin > Configuration > Templates > Announcement Templates**.

Setting	What it does
Title & Description	Required. The heading and body staff will see.
Type	Confirm you're OK (requires a response) or To be acknowledged (read receipt).
Urgent	Raises the priority of the announcement.
Silent	Sends the announcement without an audible alert — useful when noise would put people at risk. Can be set as the default here so it is always on for this template.
Desktop Alert	Pushes the announcement onto staff desktops. You can target specific groups rather than every device.
Default Group	Who receives the announcement.
Visibility	Show or hide the template from users.
Behaviour	Replace or append the template text when it is used.

Incident Response Templates

Predefined templates linked to specific incident types, so staff can raise an incident with the key detail already filled in. Go to **Admin > Configuration > Templates > Incident Responses**.

- **Title & Notes** — required.

- **Incident Type** — which type the template applies to.
- **[Student] tag** — prompts the user to enter a student name.
- **Visibility & Behaviour** — replace or add to any existing notes.

Quick Message Templates

Predefined replies for use inside an incident — "On my way", "Need backup". Go to **Admin > Configuration > Templates > Quick Messages** and set the message text and visibility.

Location Templates

Define specific areas in and around your site so responders know exactly where to go. Go to **Admin > Configuration > Templates > Locations**.

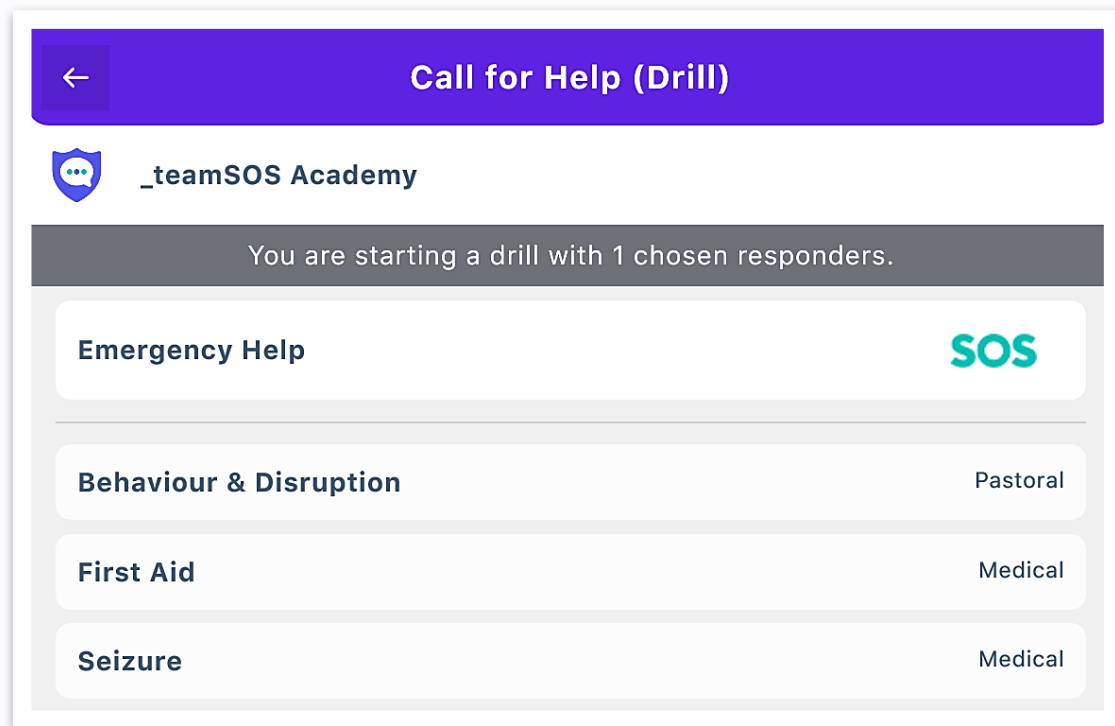
- **Location Name** — required, for example "Science Block".
- **Code** — required, a unique identifier.
- **What3Words** — the three-word address for precise pinpointing. (not fully functional currently)
- **Radius** — the area covered. This becomes mandatory once you enter a What3Words address.
- **Visibility** — show or hide the location.
- Optional advanced settings: elevation in metres, and latitude / longitude.

STEP 7 · Test your set-up

Test before you go live. Drill Mode lets you run the full Call for Help flow with a small group without alerting the whole organisation.

- 1 Run a drill**
Open the menu and tap **Start a Drill**, select the users to include, then click **Start Drill**. This mirrors a live incident from alert through to response, and the drill auto-deletes after one hour.

- 2 Test an announcement**
Inside the drill, tap **+ > Make an Announcement**. Use a template or write a custom alert, and label it clearly with "TEST" so staff know it is a simulation.



A test announcement – Drill mode

Check the escalation too: If you have configured a hunt path or an SOS team, leave the drill incident unanswered long enough to confirm it escalates to the next team as you expect.

STEP 8 · Technical setup checklist

Confirm the technical side is in place before rollout. Each item below has its own How to Guide.

Check	Where to find the detail
Firewall and filtering	How to Guide: Firewall and Filtering Setup — allow the teamSOS endpoints through your web filter and firewall.
Onboarding Wizard	How to Guide: Onboarding Wizard — guide you through the onboarding process.
Windows app deployment	How to Guide: Installing teamSOS — MSI with Group Policy, or Intune.
Desktop Alerts	How to Guide: Installing teamSOS Desktop Alerts — create the API client, deploy the registry Configuration or Intune package, and test.
Mobile devices	teamSOS is available from the Google Play Store and the Apple App Store. iOS users should accept the Critical Alerts prompt so alerts break through silent and Do Not Disturb.
Active Directory sync	How to Guide: Integrating teamSOS with Active Directory — Entra connection, user sync and SSO.

Where to find these: Log in to the teamSOS web app, then open **Help & Support** in the left-hand menu and choose **FAQs**. You can also find them on the **Onboarding space** that was shared in the welcome email.

Need help?

If you encounter any issues, please contact help@teamsos.co.uk