teamSOS

Onboarding Wizard Guide

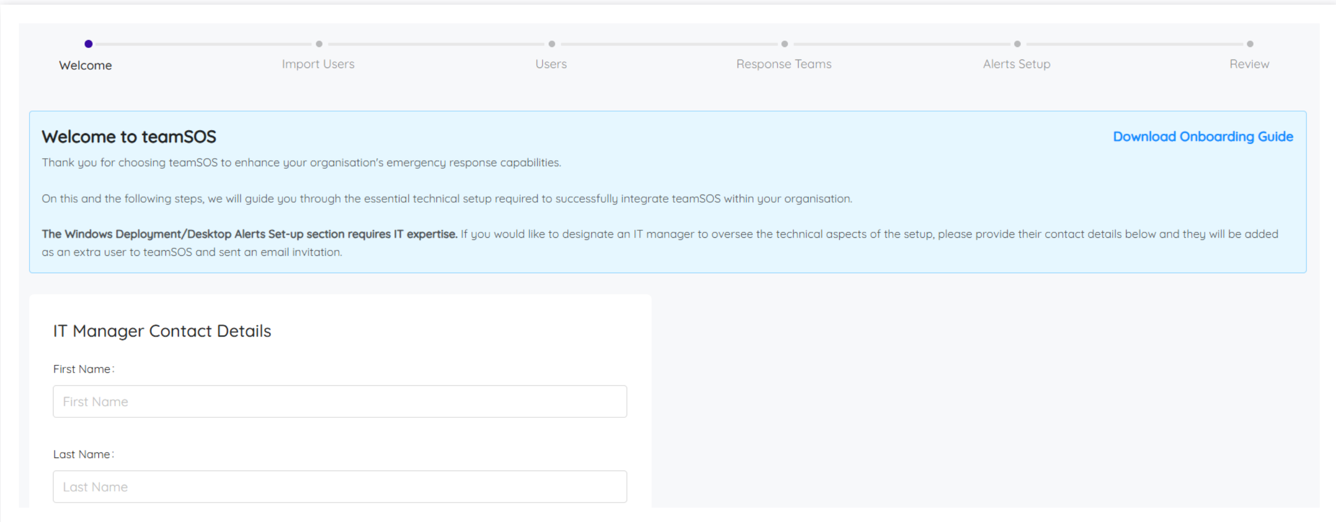
Configure your system before it goes live

The teamSOS Onboarding Wizard guides you through the essential steps required to configure your system. **It makes sure all core settings, users and response teams are set up correctly before the system goes live.**

Enterprise & Lockdown: The wizard is the same for both editions. The one place they differ is the Response Teams step — teamSOS Enterprise supports multiple response teams and escalation pathways, while teamSOS Lockdown uses a single designated response team.

STEP 1 · Welcome

Once we have created your organisation within the system, a welcome email is sent to the primary contact provided at the point of sales approval. Follow the link in that email to create your account — you will then be taken straight to the Onboarding Wizard. The first screen you see is the Welcome Page.



The Welcome Page — add your IT manager's contact details, or skip this step

1 **Review what's on screen**

Read through the information shown on the Welcome Page before you begin.

2

Gather what you'll need

Have your team member information, roles and responders to hand.

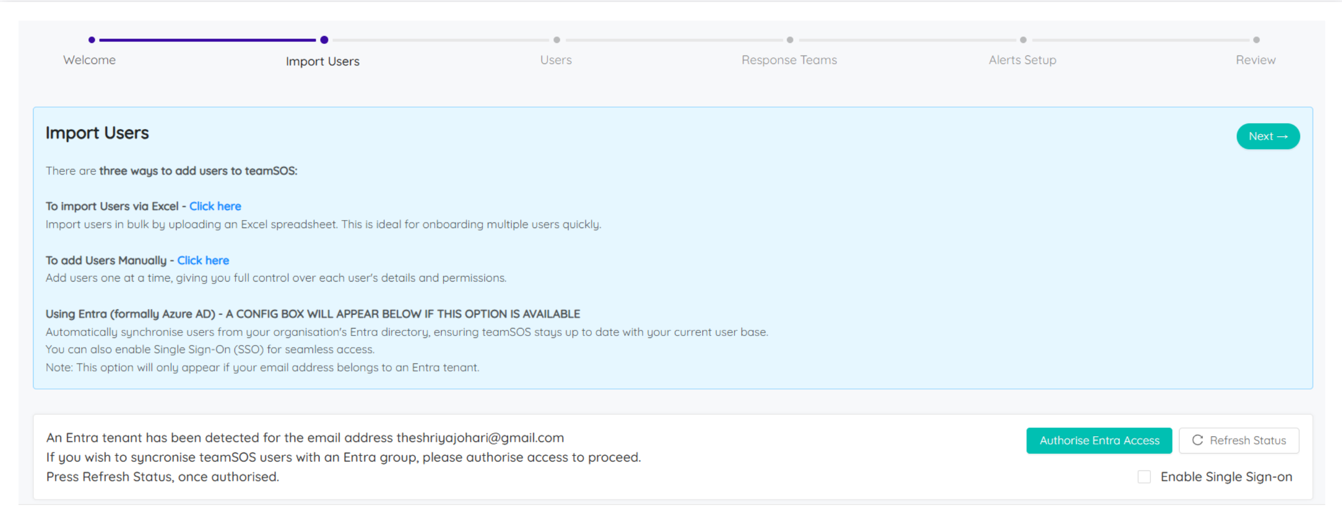
3

Invite your IT manager

If the technical setup needs IT expertise, invite your IT manager to help with the deployment steps.

STEP 2 · Import Users

You must add your users to teamSOS before the system can be used. There are three ways to add users:



The Import Users Page — add your users

1

Import users via Excel

Upload a spreadsheet to add many users at once. Ideal if you're onboarding a large number of users, already have a user list, or don't use Entra. Complete the spreadsheet in the required format before uploading.

2

Add users manually

Add users individually — enter each user's details, assign specific roles and permissions, and keep full control. Best for a small number of users or one-off changes.

3

Use Entra (formerly Azure AD)

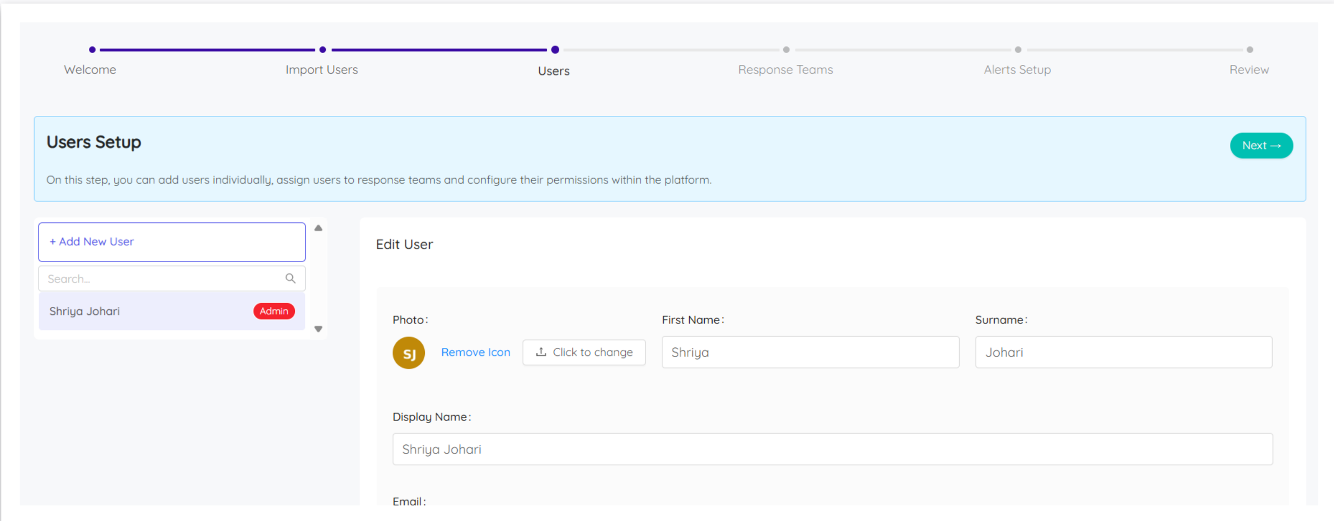
If your organisation uses Microsoft Entra, synchronise users automatically from your directory so teamSOS stays in step with your current user base. You can also enable Single Sign-On (SSO) so users sign in with their existing organisational credentials.

Please note: The Entra option only appears if your email address is associated with an Entra tenant — a configuration box appears below the option when it's available. This method is recommended for organisations already managing users through Microsoft 365 or Entra.

Not sure which to choose? Use Entra if you want automatic sync and SSO; use Excel import for a large existing user list; add users manually for a small number or individual changes.

STEP 3 · Users & Roles

At this stage you can manage individual users — add them, assign them to response teams, and configure their roles and permissions. Getting these right matters, as a user's role determines what they can access and how they respond within the system.



The Users Page — manage individual users

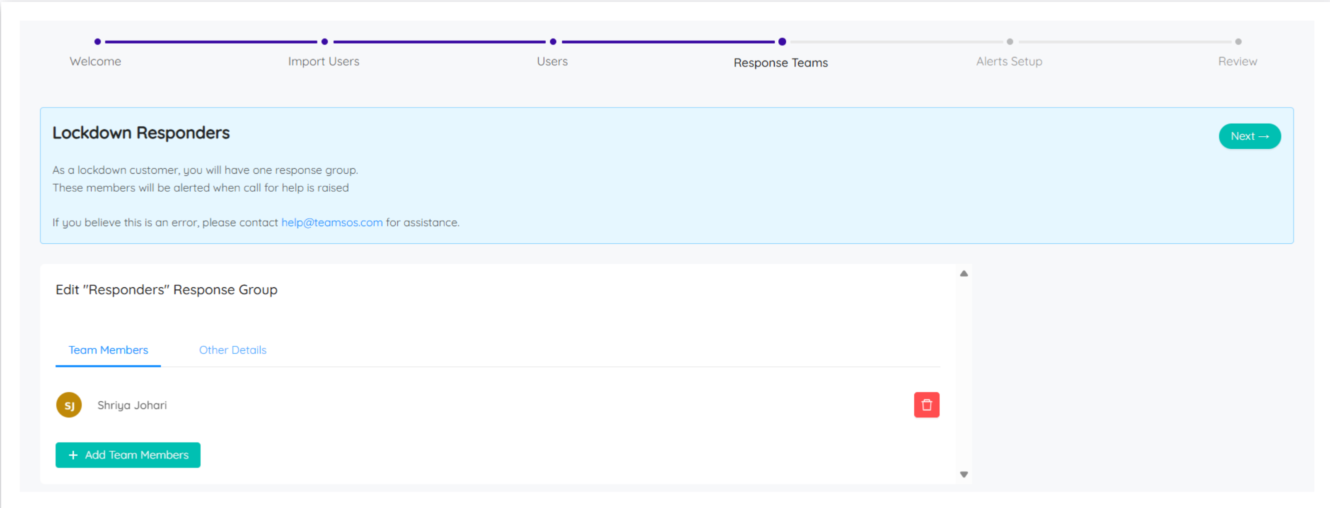
Role	What it allows
User	Respond to incidents, raise new incidents, take part in chats, have tasks assigned, and receive announcement alerts.
Admin	Full access to all teamSOS features — create, edit and manage users, settings and incidents, configure other users' permissions, and make announcements.
Announce	Make announcements within teamSOS. This permission is required for lockdown functionality.

What you should do

- Add anyone who wasn't included during the import stage.
- Confirm the correct role and permissions are applied to each user.
- Assign each user to the appropriate response team(s) — you can also do this in the next step.

STEP 4 · Response Teams

Response Teams are the groups or individuals configured to respond to specific incident types, so the right people are notified quickly and can act. Teams are customisable to your organisation's structure — for example a First Aid Team, Safeguarding Leads, or Site Management.



The Response Teams Page — manage your groups

ENTERPRISE **Multiple teams**

Create as many response teams as you need and map them to incident types, giving you multiple escalation pathways to different teams.

LOCKDOWN **One response team**

Standard response groups don't apply. A Lockdown subscription uses one designated response team only.

What you should do

- Create response teams that reflect your organisation's structure.
- Add the appropriate users to each team.
- Link each team to the relevant incident types (if applicable).

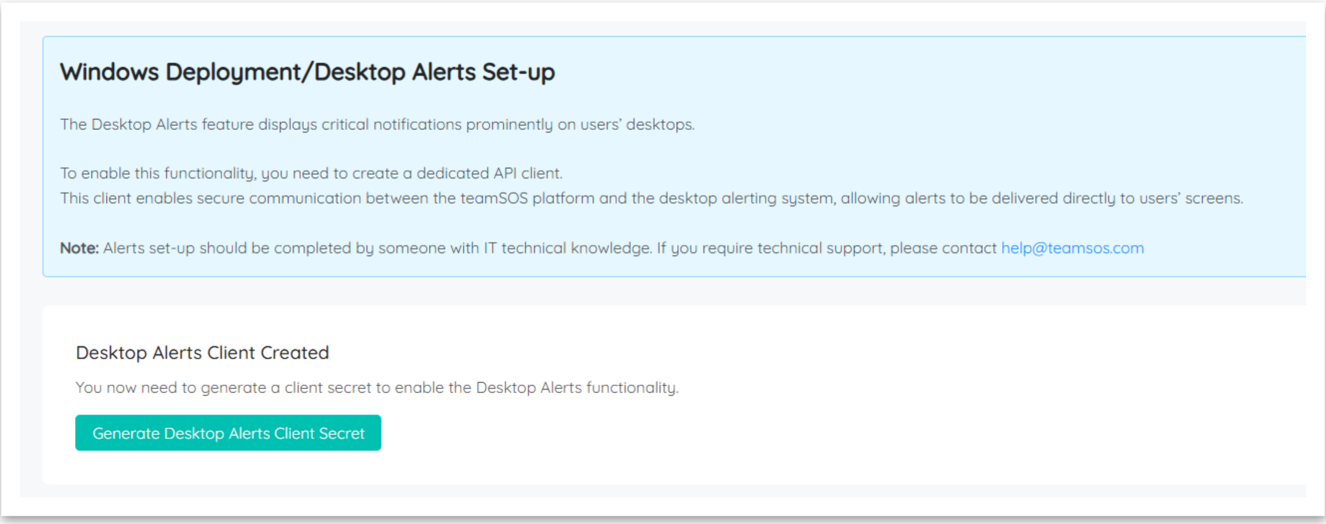
STEP 5 · Alerts Setup — Windows App & Desktop Alerts

This step deploys the Windows app and Desktop Alerts, which display critical notifications directly on users' screens to help make sure important alerts are seen. To enable this, you create a dedicated API client that allows secure communication between teamSOS and the desktop alert system.

1

Create the Desktop Alerts client

Click Create Desktop Alerts Client.



Step 1 — Create Desktop Alerts Client

2

Generate the client secret

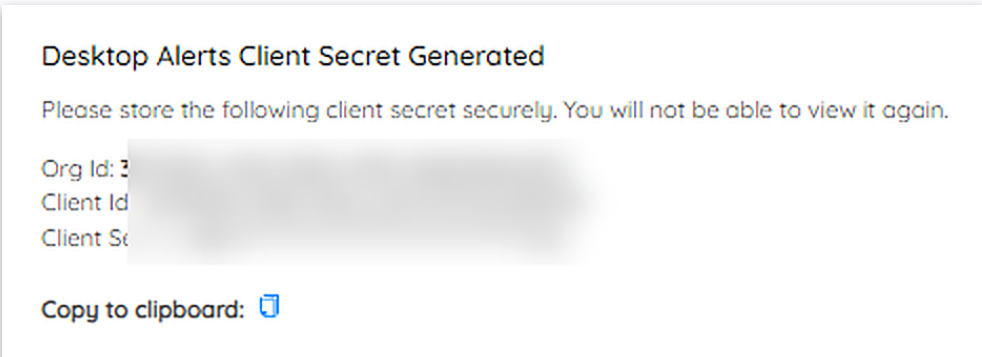
Click Generate Desktop Alerts Client Secret.

Please note: Steps 1 and 2 must be completed by the same person, in the same session, to avoid errors.

3

Copy the client secret

Copy the client secret somewhere safe — you won't be able to view it again.

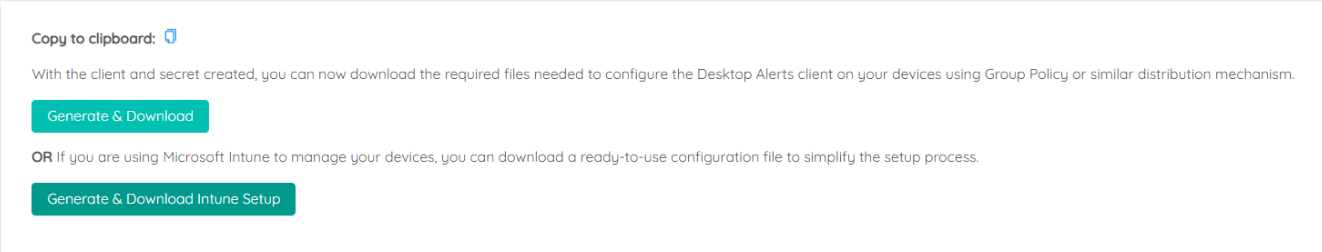


Step 3 — copy the generated client secret before leaving this screen

4

Choose your deployment method

Select either the **GPO** (or similar) registry download or **Intune**, then download the relevant files.

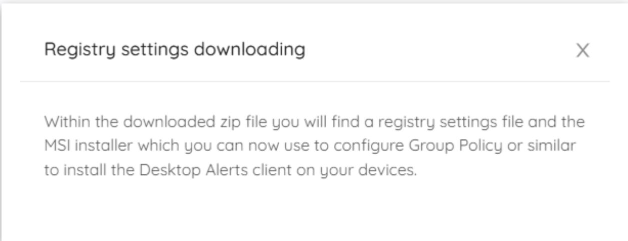


Step 4 — choose Registry (GPO) or Intune, then download

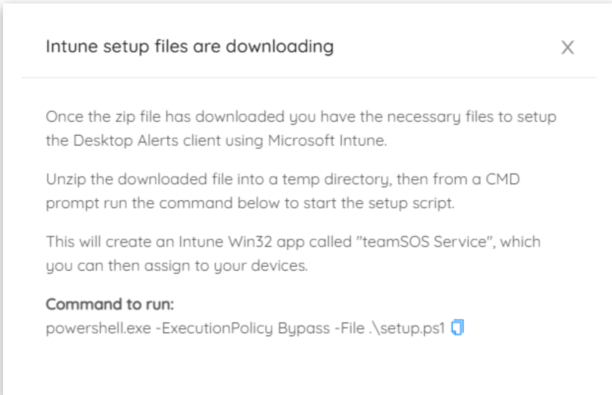
5

Download and set up

Once the zip file has downloaded, you have the files needed to set up the Windows app and Desktop Alerts. Follow the on-screen instructions to finish.



GPO / registry download



Intune setup files download

GPO (or similar): The zip contains a registry settings file and an MSI installer to configure GPO or similar and install the Desktop Alerts client.

Note: teamSOS is a staff app; it is not designed for use by students, and so deployment would be expected only onto managed staff devices. Your existing workstation Group Policy can include enabling “Turn off the Store application”, and the MSI deployment route will still work.
However, teamSOS is a Store app (regardless of the mechanism you use to install it), so you cannot apply Group Policy to “Disable all apps from Microsoft Store” because the teamSOS app, along with Calculator, Camera, etc will be unable to run.

Intune: Unzip the file to a temp directory, then run the command below from a CMD prompt. This creates an Intune Win32 app called “teamSOS Service” that you can assign to your devices.

```
powershell.exe -ExecutionPolicy Bypass -File .\setup.ps1
```

STEP 6 · Review

The Review stage is your final chance to check the system is configured correctly before completing onboarding. Carefully review your Users and permissions, and your Response Teams and members, so the right people will be notified, and permissions are set appropriately before go-live.

Need help?

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