NSW Department of Education

User Guide 1.1

This document is a step by step guide to help Registered Training Organisations (RTOs) administrators manage RTO User Roles and Responsibilities in the Smart and Skilled application portal.

Document snapshot

Use for:	Managing RTO users' roles and responsibilities in the portal
When:	When accessing the Smart and Skilled application portal
For:	RTOs

Table of contents

Table of figures

About User Management

The Smart and Skilled application portal allows RTO administrators to define roles and responsibilities of other users in the RTO.

When an RTO administrator is logged in, there are a range of user management functions.

This document outlines the different roles available in the portal. Each role is mapped to a certain set of permissions.

Roles

The portal primarily provides the following user profiles:

1. **Administrator**: An RTO owner responsible for managing user profiles for other users in the RTO and managing activities related to a Smart and Skilled application and contract
2. **Responsible Officer**: An account representative who can perform all activities of an Administrator within the portal, except managing other user roles in the system
3. **Application Editor**: General user responsible for performing duties related to a Smart and Skilled application such as editing the form and providing additional details.

Each role has a level of permissions to perform certain functions in the portal. Visit the Permissions page for more information.

When you login to the portal using a Digital Identity for the first time, you will be automatically assigned a role based on your authorisation type in RAM.

RAM authorisation type	Smart and Skilled Application Portal Role
Principal authority	Administrator
Authorised administrator	Responsible Officer
All other authorisation types	Application Editor (default role)

Permissions

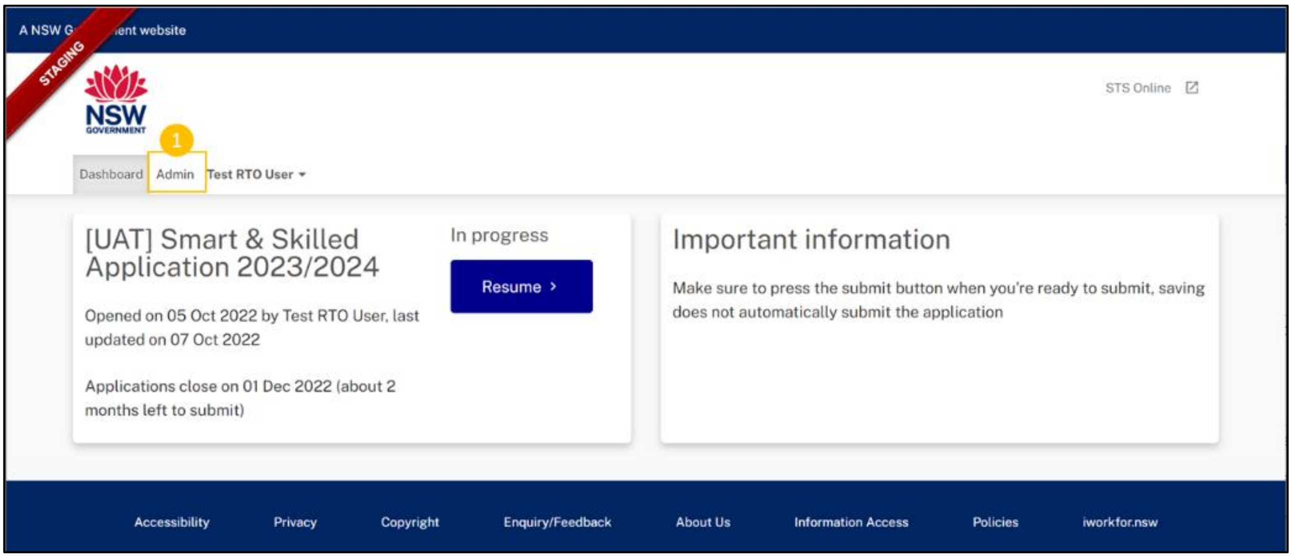
The Smart and Skilled application portal has different access levels that can be assigned to users depending on the functions they need to perform. The table below lists these.

SSAP Role	Permissions
Administrator	• Manage the access of all profiles within the RTO • Manage and update the RTO contracts for government-subsidised Smart and Skilled training • Submit an application • Edit any submitted application if the rules allow.
Responsible Officer	• Manage and update the RTO contracts for government-subsidised Smart and Skilled training • Submit an application • Edit the RTO's open or submitted applications within the specified time period.
Application Editor	• Completing an application form that an Administrator or Responsible Officer has created • Upload any additional documents required during the application process. *Please note that a user with Application Editor role cannot see an application until started by the Administrator or the responsible officer. Application Editor can not submit an application*

Changing User Access

An Administrator will be able to edit the user roles and change the roles' default permissions. Administrators can manage these functions by logging in and following the process below.

Step 1: If you are logged in as an Administrator, go to the Admin menu (see below).



[UAT] Smart & Skilled Application 2023/2024

In progress

Opened on 05 Oct 2022 by Test RTO User, last updated on 07 Oct 2022

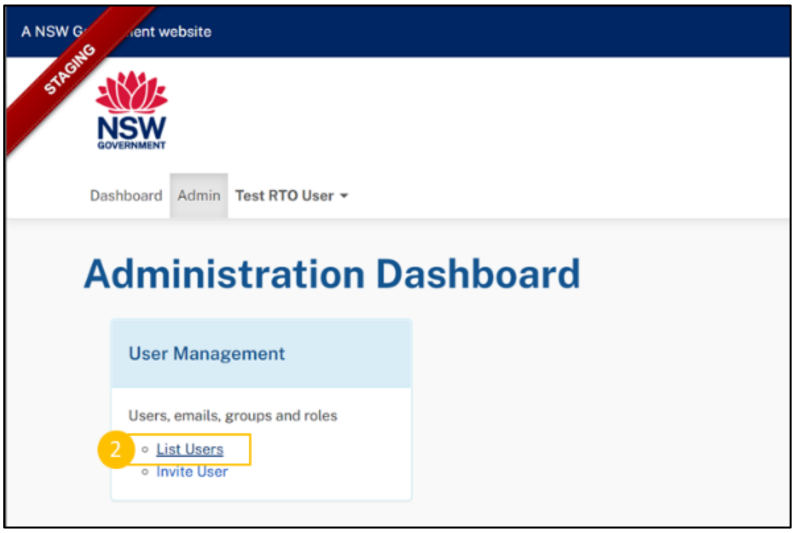
Applications close on 01 Dec 2022 (about 2 months left to submit)

Important information

Make sure to press the submit button when you're ready to submit, saving does not automatically submit the application

Figure 1: Locating the Admin menu in the application portal.

Step 2: To see all the users in your RTO accessing the portal, click on “List Users” in the User Management section.



Administration Dashboard

User Management

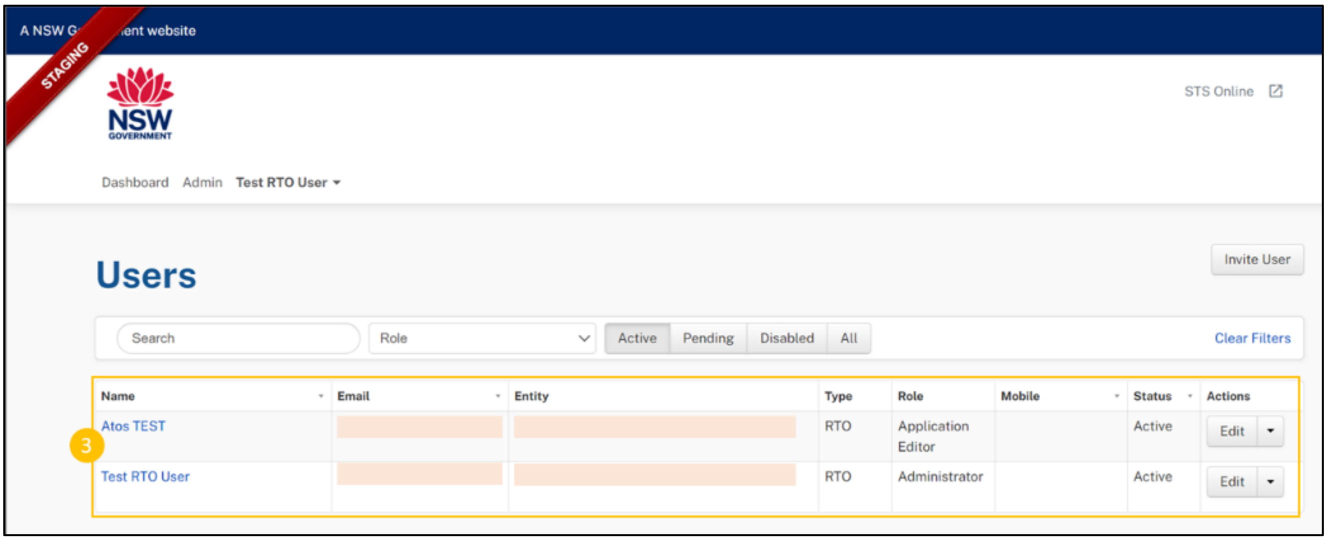
Users, emails, groups and roles

- List Users
- Invite User

Figure 2: Locating the List Users section on the Administration Dashboard

Step 3: On the Administration Dashboard page, the Administrator will be able to see all the users who have logged in the system and filter the list by name, role, and account status.

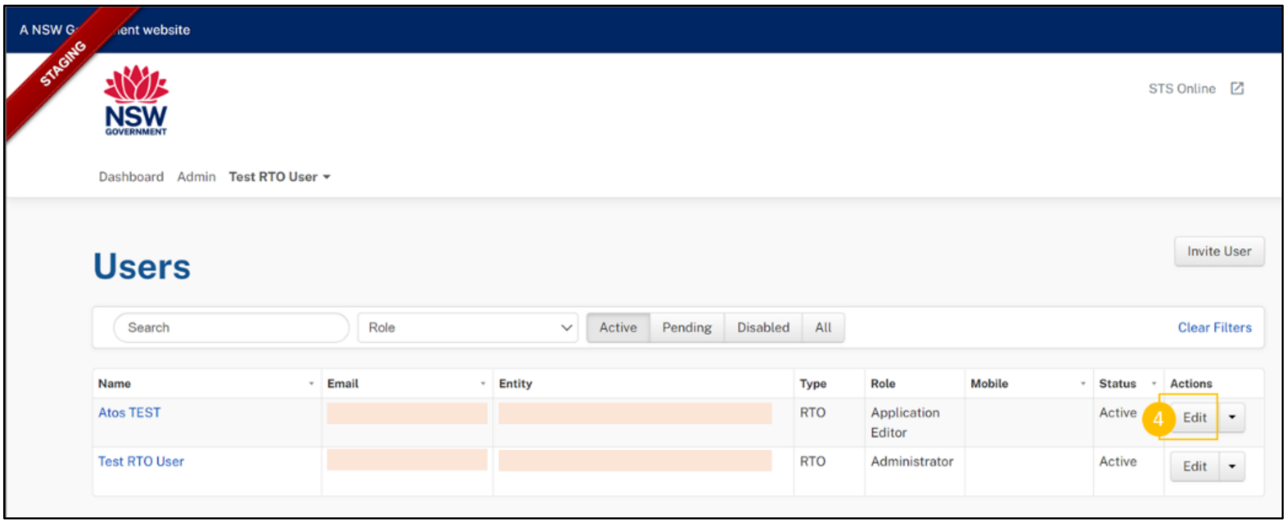
Please note: The user profile in the system is automatically created when a user logs in using a Digital Identity for the first time. After the first login, the Administrator will be able to see the user on the “List Users” page.



Name	Email	Entity	Type	Role	Mobile	Status	Actions
Atos TEST	[redacted]	[redacted]	RTO	Application Editor		Active	Edit
Test RTO User	[redacted]	[redacted]	RTO	Administrator		Active	Edit

Figure 3: List of system users

Step 4: The Administrator can edit the other user's account by clicking on the Edit button under the Actions section. Refer 4 in the below screenshot.

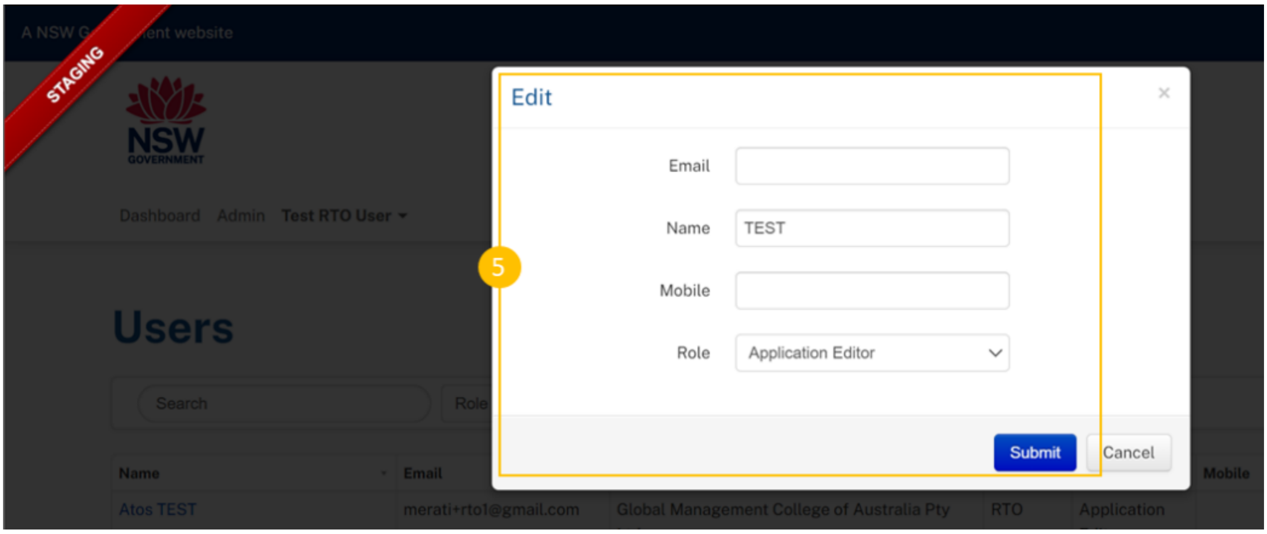


Name	Email	Entity	Type	Role	Mobile	Status	Actions
Atos TEST	[redacted]	[redacted]	RTO	Application Editor		Active	Edit
Test RTO User	[redacted]	[redacted]	RTO	Administrator		Active	Edit

Figure 4: How to edit the list of users

Step 5: In the edit pop-up, the system allows editing of user details such as email, name, mobile number, and user role. Click on the Submit button to save changes.

IMPORTANT: The Portal Administrator is the only role that can edit user roles in the Portal. However, if the Portal Administrator edits their role to other roles e.g. Application Editor, they will lose the user management ability once the change has been submitted.
The current Portal Administrator will need to ensure that there is at least one Portal Administrator in the Portal before allocating their Portal Administrator role to another."



Email

Name: TEST

Mobile

Role: Application Editor

Figure 5: Editing the list of users

Disable users

For security purposes, if you’re a principal authority or authorisation administrator, ensure you regularly maintain authorisations in RAM and remove authorisations immediately when they are no longer valid.