



# New User Profile Setup

TOMORROW BEGINS TODAY



Royal Bank  
of Scotland

# Contents

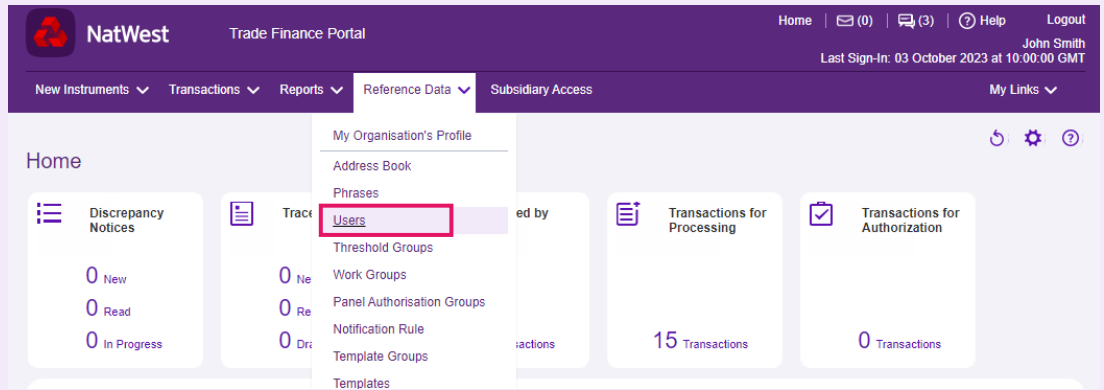
<a href="#">Introduction.....</a>	<a href="#">3</a>
<a href="#">General.....</a>	<a href="#">3</a>
<a href="#">Security .....</a>	<a href="#">4</a>
<a href="#">User Access .....</a>	<a href="#">4</a>
<a href="#">Panel Authority.....</a>	<a href="#">5</a>
<a href="#">Template Groups .....</a>	<a href="#">5</a>
<a href="#">Report Categories .....</a>	<a href="#">5</a>
<a href="#">Subsidiary Access .....</a>	<a href="#">6</a>
<a href="#">Submitting.....</a>	<a href="#">7</a>



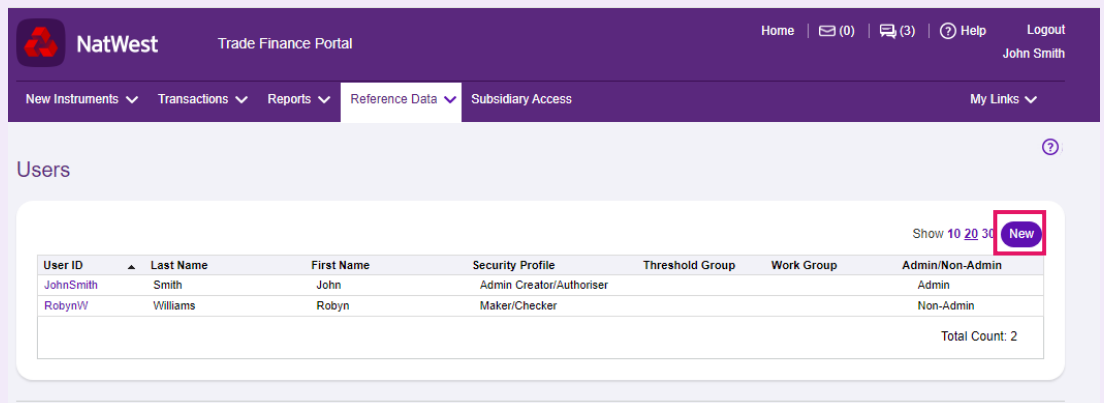
# Introduction

Log into the Trade Finance Portal.

To create a new User Profile, from the home screen select 'Reference Data' then 'Users':



Then select "New":



# General

Complete all the fields below where there is a Red Asterix. For the section "Default Work View" please see below.

\*\* Please ensure you add your email address as this is a mandatory field. \*\*

### 1. General

User ID <input type="text"/>	Email Address <input type="text"/>
First Name * <input type="text"/>	Middle Initial <input type="text"/>
Last Name * <input type="text"/>	<input type="checkbox"/> Receive email notifications for Routed transactions and messages
Phone Number <input type="text"/>	<input type="checkbox"/> Receive email notification for authorized transactions
Fax Number <input type="text"/>	Region Setting * <input type="text"/>
	Time Zone * <input type="text"/>
	Default Work View * <input type="text"/>
	Date Format * <input type="text"/>

### Default Work View \*

- Work for Me
- Work for My Organisation
- Work for Organisation and its Children

- Default Work View:**
1. Work for Me – This option will show only items designated to that user to action.
  2. Work for My Organisation – This option will show all transactions for the organisation.
  3. Work for Organisation and its Children – This option will show all transactions for the organisation and its subsidiaries.

# Security

## 2. Security

Authentication Method  
**2-Factor Authentication**

Login ID \*

Password \*

Retype Password

Security Device Type

**Generic Token**

Security Device ID

Please add a Login ID and Password here. Each must be unique to the User – If a Login ID has been previously taken, an error message will appear.

Once the password has been set, when the User first logs into their account, they should click on their name in the top right corner of the home screen and change the password to their own unique choice.

# User Access

All new users will have a User Role as Non-Admin, however new users can be given Administrator Access by selecting the correct Security Profile, see below options:

### 3. Assigned To

User Role \*  
Non-Admin

Security Profile \*

Threshold Group  
Not selecting a Threshold Group indicates that the user can authorise an unlimited amount of work.

Work Group  
Not selecting a Work Group indicates that the user may not be able to authorise instrument types that require two users from different work groups.

Restricted User Template

Security Profile \*

- Admin Authoriser
- Admin Creator
- Admin Creator/Authoriser
- All Access - Customer
- Checker
- Maker
- Maker/Checker
- Read Only Customer
- View Only

See customer guide entitled 'Security Profiles' to explain the permissions designated to each profile.

# Panel Authority

**4. Panel Authority** ▼

Panel Authority

*This is only applicable if your corporation uses panel authentication for authorising payment instruments.*

Authorise Own Output

*This is only applicable if your corporation uses panel authentication and the user should be allowed to input data and be considered also as an Authoriser for the data input.*

Panel Authority allows you to route transactions to specific levels of authority within your company dependent on transaction value. Please contact the Portal Support Team if you have specific transaction authorisation requirements.

# Template Groups

For this section, if templates have been created then you will be able to restrict which templates the new user will have access to:

**5. Template Groups** ▼

*If a user has associated Template Groups, that user will only be able to create new instruments using these templates and will only be able to create a "blank" transaction using a template.*

	Template Group Name		Template Group Name
1.	<input type="text" value=""/>	2.	<input type="text" value=""/>
3.	<input type="text" value=""/>	4.	<input type="text" value=""/>

[Add 4 More Template Groups](#)

# Report Categories

For the new user, if there are specific reports that they should only have access to, then they can be selected below:

**6. Report Categories** ▼

Select up to 10 Report Categories

<input type="text" value=""/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>

# Subsidiary Access

This section determines whether the new user has access to view or perform actions as a parent on behalf of the subsidiary or not:

You can also select the level of access per subsidiary – They can either have the same access across all parties or separate access levels per entity:

If they are to have separate access, the below is how to designate this access:

Contact the Portal Support Team regarding the below if the new user is to have separate authorisation levels for the subsidiaries to the main Parent entity:

**7. Subsidiary Access Capabilities**

- User is **NOT** able to perform actions on behalf of subsidiaries
- User is **able** to perform actions on behalf of subsidiaries
  - The reference data for the user's organisation is available when the user performs actions on behalf of subsidiaries.

**Subsidiary Access Security Profile**

Determine if the same Subsidiary Access Security Profile can be used by the user when acting on behalf of all users or if a different Subsidiary Access Security Profile can be used for each Subsidiary.

- User can use the same Subsidiary Access Security Profile for each subsidiary
  - Select a Subsidiary Access Security Profile
  -
- User can use different Subsidiary Access Security profiles for subsidiaries
  -

Only display the below subsidiaries when accessing items for subsidiaries in parent Show view. The parent security profile will still be used and not the security profile listed below.

Subsidiary Access Security Profiles

Select each subsidiary to which the user has access and select the Subsidiary Access Security profile that defines the user's security rights when acting on behalf of that subsidiary. If a user cannot access a specific subsidiary, then do not select the subsidiary or assign a profile to it.

	Subsidiary	Subsidiary Access Security Profile
1.	<input type="text"/>	<input type="text"/>
2.	<input type="text"/>	<input type="text"/>
3.	<input type="text"/>	<input type="text"/>
4.	<input type="text"/>	<input type="text"/>

[Add 4 More Subsidiaries/Profiles](#)

- Parent user is able to access subsidiaries' Confidential Payment Instruments/Templates

Only applicable if your corporation/ your subsidiaries use "Payment" instruments. If selected, the parent user will be able to access the subsidiaries "Confidential" payment transactions and templates and also initiate new payment transactions from templates that have been designated as being "Confidential".

Subsidiary Access Threshold Group

Subsidiary Access Work Group

When authorising Subsidiary Transactions:

- Use Product Authorisation Rules defined on Parent Customer Profile
- Use Product Authorisation Rules defined on Subsidiary Customer Profile

Panel Authority

This is only applicable if your corporation uses panel authentication for authorising payment instruments.

- Authorise Own Output

This is only applicable if your corporation uses panel authentication and the user should be allowed to input data and be considered also as an Authoriser for the data input.

# Submitting

Once all the fields are complete, click on “Save”. Once this is done – You will be prompted to have the user be authorised:



The second User will then need go into Reference Data – “Approve Reference Data” and select the new User and then click on Approve:

