Task Card

For Authorised Access delegates Managing Access to the Inclusion Support Portal

Who will need this task card?

The Inclusion Support Portal (IS Portal) is a web-based application that manages all early childhood education and care services' (ECEC) interactions with the Inclusion Support Program (ISP).

This task card is intended for service provider Authorised Access Delegates. It contains instructions to assist Authorised Access Delegates to **manage who has access** to the Inclusion Support Portal for the service.

What is this task card for?

This Task Card provides information and a step-by-step guide to support Authorised Access Delegates to manage access to the Inclusion Support Portal.

Contents

About the Role

Authorised Access Delegates are responsible for reviewing and approving new users access requests, updating users access, removing access if a user leaves the service and suspending access if a user goes on long term leave. Authorised Access Delegates can also submit an access request for a new user.

Logging into the IS Portal

Authorised Access Delegates must be logged into the IS Portal in the role of Authorised Access Delegate to manage who has access to the Inclusion Support Portal for the service.

the IS Portal can then be accessed via:

[Login | PRODA](https://proda.humanservices.gov.au/prodalogin/pages/public/login.jsf) - https://proda.humanservices.gov.au/prodalogin/pages/public/login.jsf

Login to your PRODA account and select the Inclusion Support Portal tile:

When your identity is verified, the '*Portal entry point'* page is displayed.

1. **Select** your employer from the **Provider name** dropdown list.

2. Using the **Role dropdown** option, **Select** the role of *Authorised Access Delegate*.

3. At **Role** select *Authorised Access Delegate.*

4. **Click** *Continue.*

The Identity Manager (IDM) 'Access requests' page is displayed.

To return to this page from within IDM, choose **Portal access requests** from the main menu or **Access requests** from the organisation panel.

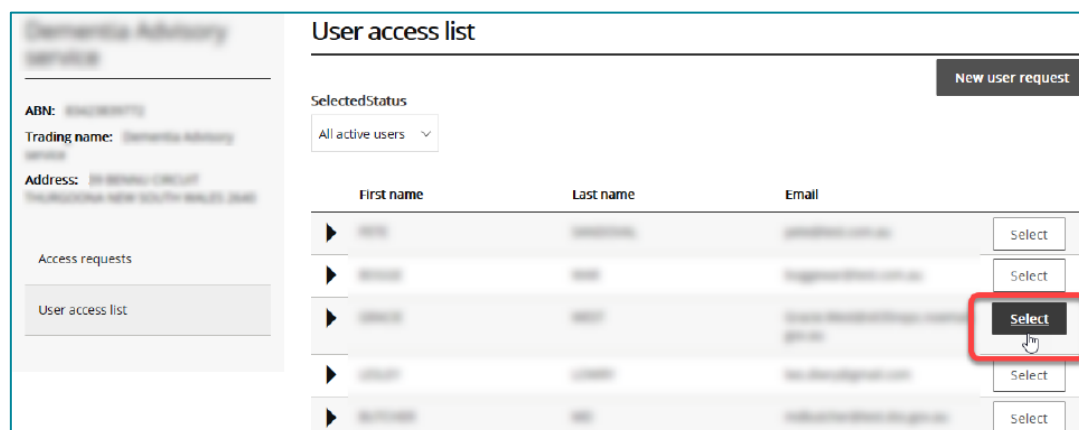# Finding a user who has been granted access

1. When logged in to the IS Portal in the role of Authorised Access Delegate, **Select *User access list***.
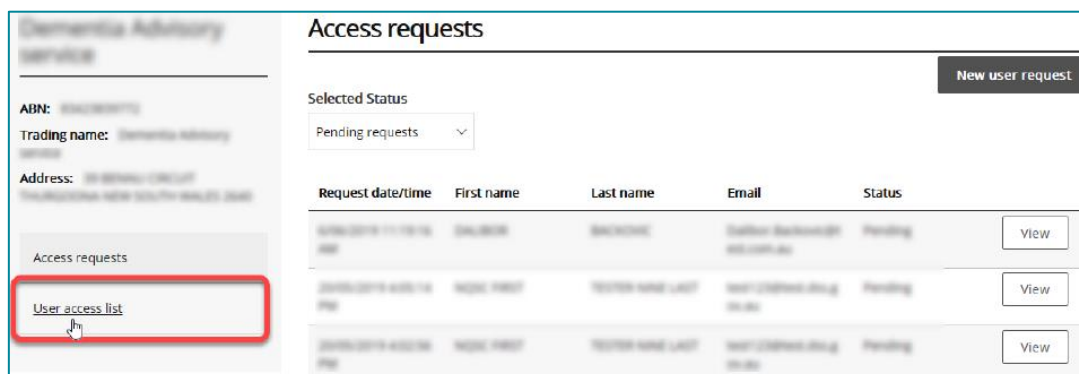
5. On the User Access list page, **Select *All active users*** as the *status* from Selected Status dropdown list.
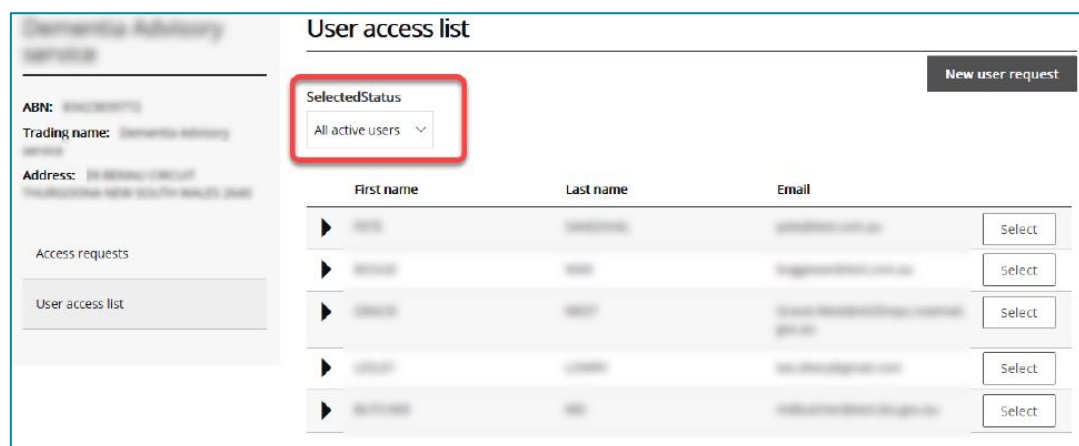
3. Find the relevant user in the list and **click *Select.***

The *View employee details* page for the selected user is displayed. The user roles they have been approved for are identified.

Requesting access for a new user

Authorised Access Delegates can submit an access request for a new user on their behalf.

• To request additional access for an existing user, refer to the

1. When logged in to the IS Portal in the role of Authorised Access Delegate, **click *New user request*** on the Access requests page.

2. **Click *I'm ready to request access*.**

3. On the User details access request page, **enter** the ***users details***. The Provider details will be prepopulated.
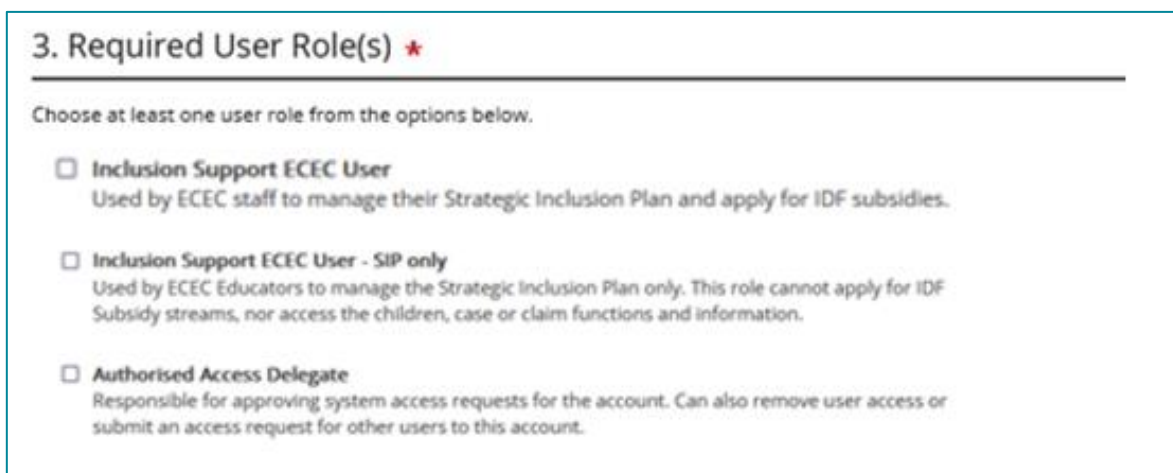

- **First name** — May contain letters, numbers, hyphens, spaces and apostrophes.

- **Last name** — May contain letters, numbers, hyphens, spaces and apostrophes.

- **Email** — Must be a valid email address for the user. A confirmation email will be sent to the user to validate and link it to their PRODA account before the request can be approved.

- **Work phone number** – Must contain numerals only, 10 digits e.g. 0212345678

- **Mobile phone number** – This is optional. Must contain numerals only, 10 digits.

5. **Select** one or more *Required User Roles* for the user.

Note: Users cannot be approved in both the role of Inclusion Support ECEC User and Inclusion Support ECEC user – SIP only. Choose the most appropriate role.

A person in the role of Authorised Access Delegate can also hold the role Inclusion Support ECEC User.
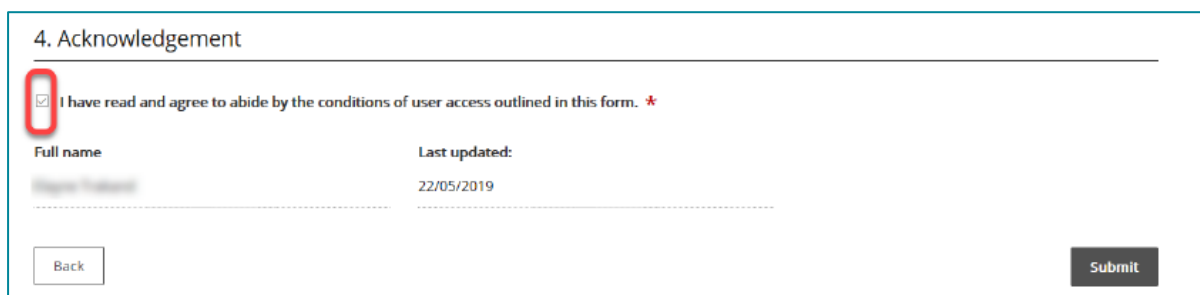

4. **Select** the *I have read and agree to…* checkbox in the Acknowledgement section.
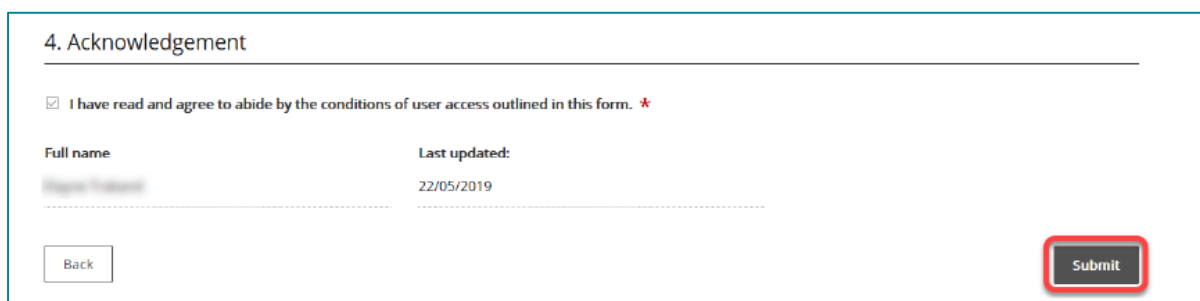   *IMPORTANT: This is your formal approval of the access request*.

5. **Click** *Submit*.

6. **Click** *Finish.* Refer to the image on the next page.

The user will be sent an email to validate their email address. When they click the link in this email and login to PRODA, the request will be linked to their PRODA account, and the request will be automatically approved.

To view this access request prior to the user responding to the validation email

1. **Access** the *Access Requests page*.

2. **Select,** *Requests awaiting user* from the **Selected Status** dropdown list.

3. Locate the relevant user, **select view** to view the user roles request.

Approving access

The Authorised Access Delegate needs to approve each user access request submitted.

The *Selected Status* dropdown, on the *Access Request page*, is automatically set to Pending Requests. A list of pending requests is displayed.

1. Confirm the **Select Status** dropdown is displaying ***Pending requests.*** If it is not, select it from the dropdown menu options.
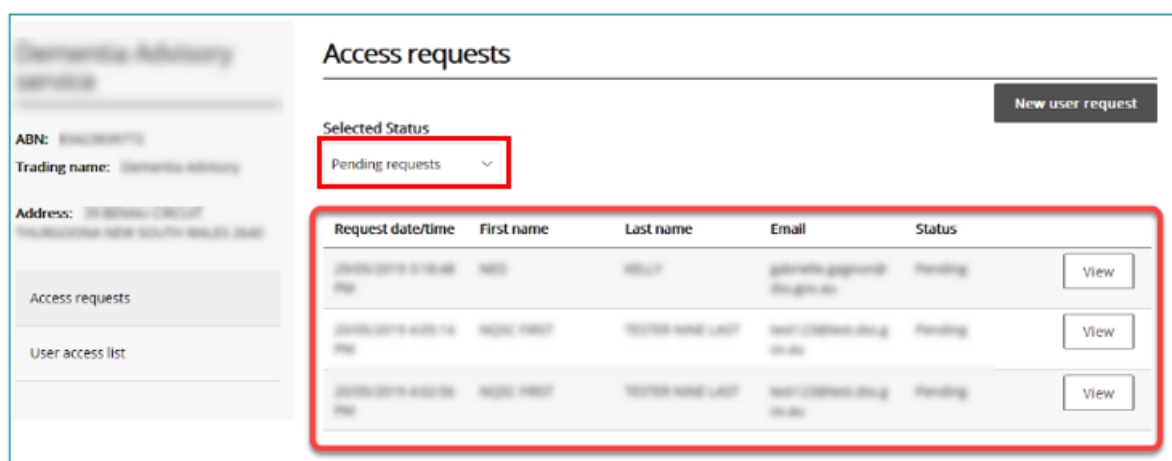
2. **Select *View***, to see the details of a user's request.
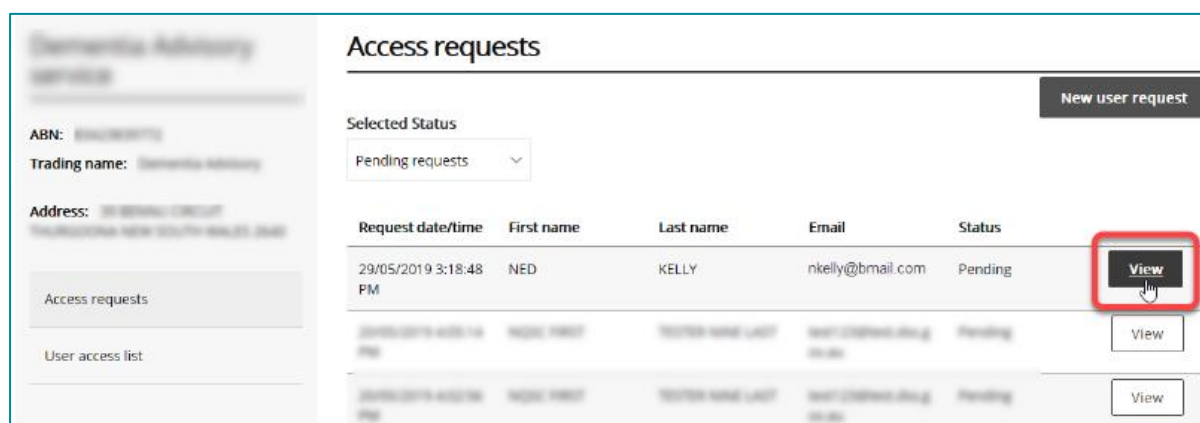
The *View portal access request* page is displayed. Refer to the image on the next page.

3. On the *View portal access request* page, check that the user role requested is correct and appropriate. Make changes, if needed. Then click **Approve** (or **Reject**).

Updating access

An Authorised Delegate can add new access user roles to an existing user, revoke a user's access to all roles or reinstate user access roles that have previously been revoked.

1. When logged in to the IS Portal in the role of Authorised Access Delegate, **Select *User access list***.

4. On the User Access list page, **Select *All active users*** as the *status* from Selected Status dropdown list.

3. Find the relevant user in the list and **click *Select.***

The *View employee details* page for the selected user is displayed.

4. On the 'View employee details' page, individual changes to the user's roles.

5. To add or remove individual roles, select (or deselect) roles and **click *Save***.

6. To revoke all access to the organisation, click **Revoke access**.
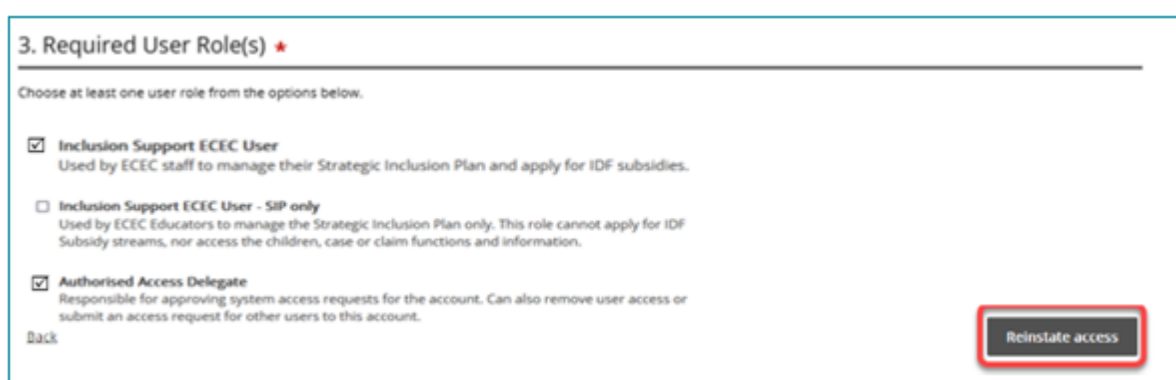
7. To reinstate previously revoked access, click **Reinstate access**.


Changing organisations or roles

The Provider Portal allows you to exercise access privileges for only one provider and one role at a time. These are selected on the 'Portal entry point' page.

If you are a delegate for multiple organisations, or if you serve in different roles, you can return to the Portal entry point and change your provider organisation or role to act in a different capacity.

Access the *Portal entry point* page:

- If you are logged in as an Authorised Access Delegate, **click *Select organisation***, at the top of any IDM screen. Refer to the image on the next page.
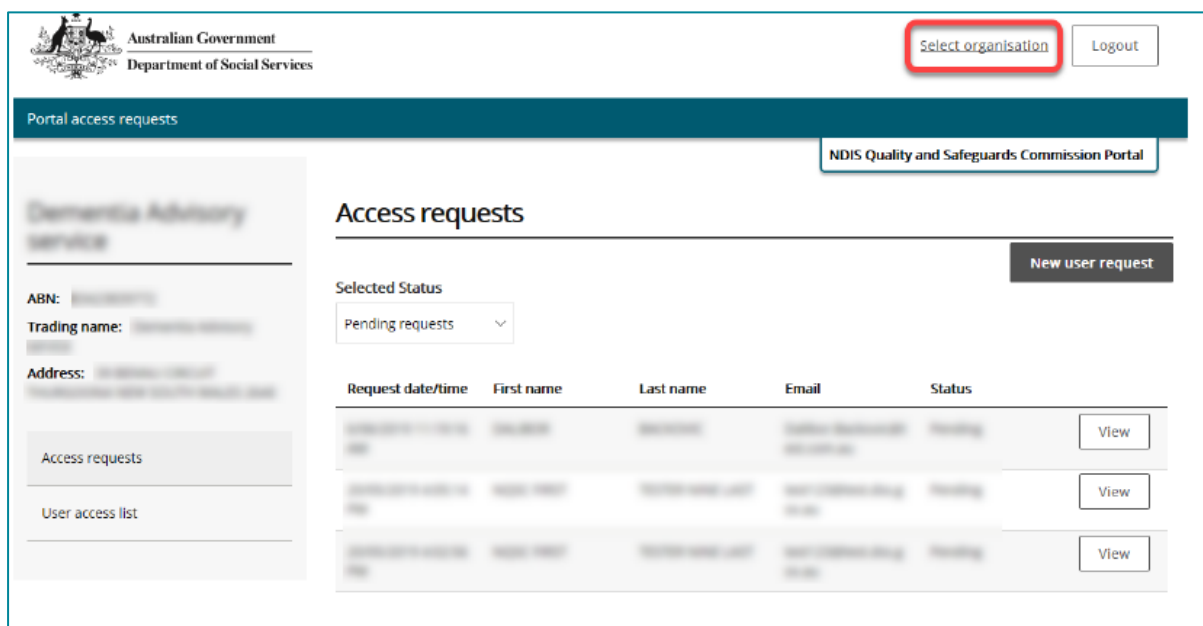
- If you are logged in as another role, **click *Change role/Manage access***, at the top of any IS Portal homepage.
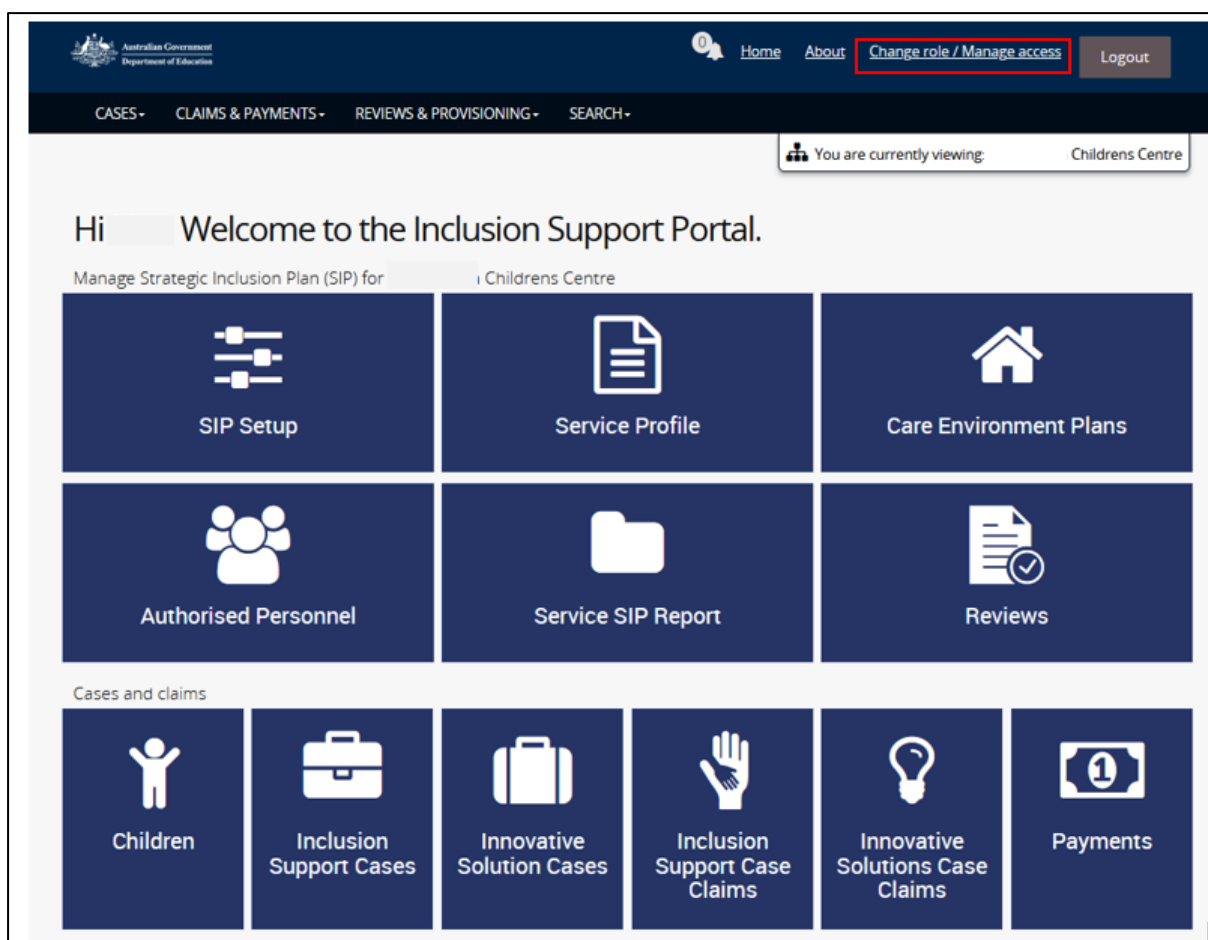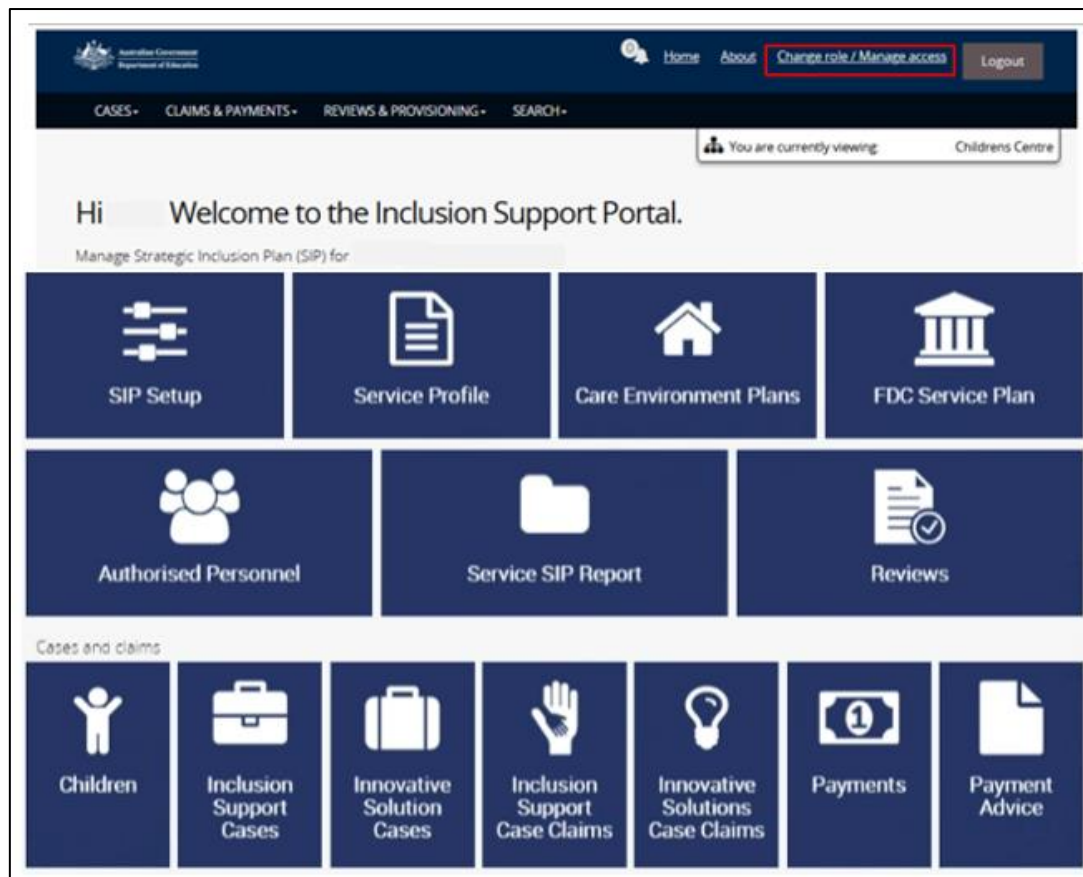
Image of the CBDC and OSHC homepage

Image of the FDC homepage dashboard

Clicking either one of these links returns you to the 'Portal entry point' page.

2. **Select** the ***Provider name and Role*** you want to change to, from the dropdown lists.

3. **Click** *Continue.*

4. If you changed to a non- Authorised Delegate Role, you are taken to the Inclusion Support Portal entry page. Read the conditions of use and **click *I agree*** to proceed to the portal.

Responding to emails

As an Authorised Access Delegate, whenever one of your service provider's employees requests access to the IS Portal, you will receive an email notifying you of the pending request.

You can respond to these requests by logging into the portal and following the steps for Approving access on pages 9-10.
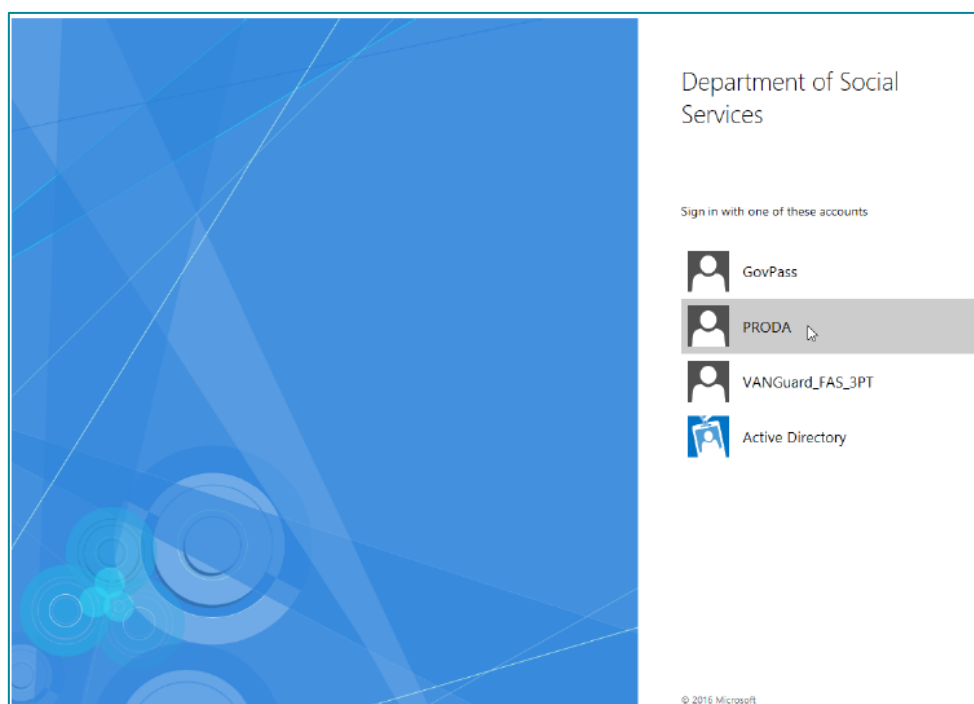
Alternatively, you can take a shortcut to the request, by responding directly from the email:

1. From the opened email, click View Inclusion Support Portal access request.
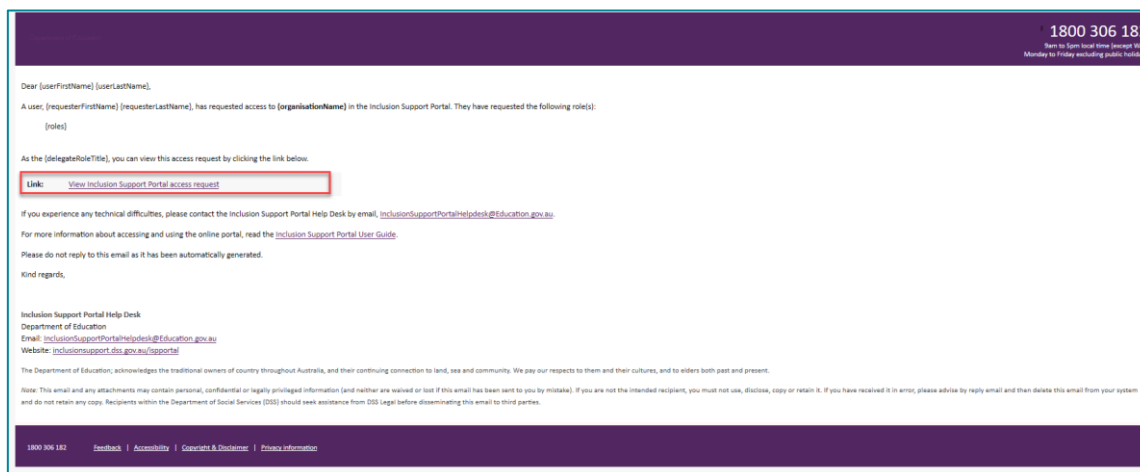
This opens a browser and takes you to Department of Social Services (DSS) account selection page.

2. On the Department of Social Services account selection page, select **PRODA**.

3. *Log into PRODA* as described on pages 1 to 3, Logging in to the IS Portal.

4. Follow the steps outlined on pages 9-10. Approving access.