



Member flow: ORCID to eduGAIN IdP cross-link

In February 2016, ORCID enabled IdP SSO for all eduGAIN member institutions, allowing the first direct connection between the systems by making it possible for researchers to log into the ORCID registry using their university credentials. To complete the circle, universities need to be informed when links are created, and be given the opportunity to request access to researcher ORCID records.

This member workflow initiates an ORCID user-based permission request directly after the association of the two accounts. Through this process, institutions can add ORCID IDs to their user directories so that they can be asserted as attributes via their federated identity provider (IdP). Institutions can also opt to interact with researcher ORCID records directly using the member API to add and update activities, including verified education and employment. Specifically, they may

- obtain and store an authenticated ORCID iD,
- read data in the ORCID record that is only available to trusted parties, and
- assert claims, such as a “verified” affiliation with the institution.

The purpose of this document is to provide details on the user experience of this process, and provide basic information for institutions to implement this solution.

## Institution single sign on

Today a user may sign onto the ORCID site using their institution credentials. The first time this action is attempted, ORCID guides the user through the account linking, having the user sign into both their institution and ORCID accounts to verify the link.

### User signs into their institution account

The user clicks the ‘institutional’ link from the ORCID sign in page

Sign in using your

☐ Personal Account ☒ Institutional Account

Sign in with an institutional account ?

Use a suggested selection:

[unitedID.org](#) [TESTSHIB TWO](#) [ORCID](#)

[United ID](#) [TestShib Test IdP](#) [EHU - Universidad del Pais Vasco](#)

Or enter your organization's name

[Allow me to pick from a list](#)

The user selects his/her institution, and click continue. The institution's sign in page will appear.

PENNSSTATE **WebAccess** [Help](#)

Please enter your Access Account ID or Friends of Penn State ID (e.g. xyz5000).

User ID

Password

[Change Access Account Password](#) [Change FPS Account Password](#)

The Pennsylvania State University ©2015. All rights reserved.  
[Nondiscrimination Policy](#) - [Privacy and Legal Statements](#)

The user authenticates to his/her institution and is asked to sign into his/her ORCID account (if not already signed in.) This action links the accounts:



Member flow: ORCID to eduGAIN IdP cross-link

## Link your United ID account to your ORCID record

**You are signed into United ID as `apcardoso@unitedid.org`**

To finish linking this United ID account to ORCID, sign into your ORCID iD below.

*You will only need to complete this step once. After your account is linked, you will be able to access your ORCID record with your United ID account. Questions? [Visit our knowledgebase](#)*

[Link my existing ORCID iD](#) | [Register for an ORCID iD](#) | [Return to ORCID sign in](#)

Email or ORCID iD

`p.cardoso@orcid.org`

ORCID Password

\*\*\*\*\*

[Forgotten password?](#)

Sign into ORCID

## Obtaining ORCID authenticated iD/permission *new*

Once the two accounts are linked, ORCID will initiate a user-based permission flow using its standard OAuth 2.0 connection. 1-time institution set up is required, with the the following information:

- EntityID of the Federated IdP (*when users sign in using this IdP, the OAuth process will be initiated*)
- Redirect URL - the Institution endpoint (a software component that will receive newly linked ORCID account holders - see below)
- Requested permissions (expressed as scopes)
- ORCID Member client ID that you want the permissions linked to

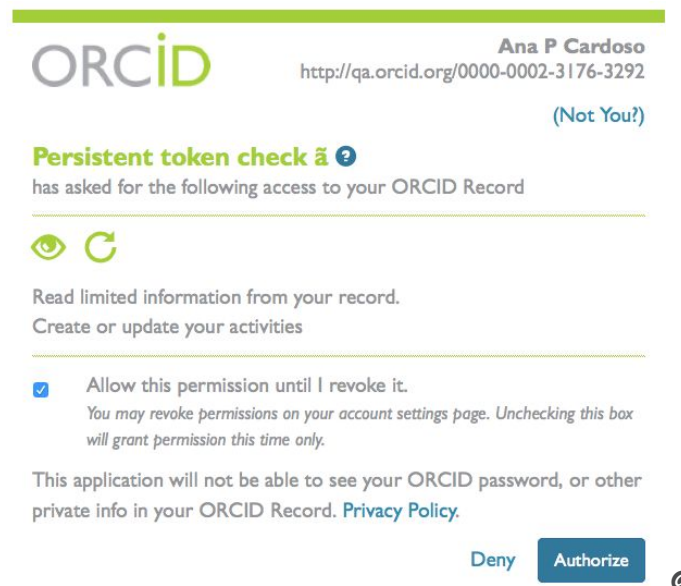
## Connecting your institutional account

You can now sign into ORCID with your Persistent token check ã account. Please complete the process by connecting your institution with your iD.

[Remind me later](#)



[Connect](#)

The user experience: ORCID presents permission screen with the scopes & client ID specified above.



ORCID Ana P Cardoso  
http://qa.orcid.org/0000-0002-3176-3292  
(Not You?)

**Persistent token check ã** ?  
has asked for the following access to your ORCID Record

   
Read limited information from your record.  
Create or update your activities

☒ Allow this permission until I revoke it.  
You may revoke permissions on your account settings page. Unchecking this box will grant permission this time only.

This application will not be able to see your ORCID password, or other private info in your ORCID Record. [Privacy Policy](#).

[Deny](#) [Authorize](#) @

The user clicks the “Authorize” or “Deny” link to confirm (or reject) they will grant the institution the requested permissions. *Note, if user clicks the “close” link instead, (s)he can re-initiate this flow later.*

The user is sent to the institution’s redirect URL that is appended with information about the user’s selection (authorize or deny.) Usually users authorize the permission, causing ORCID to append a 6-character authorization code to the end of the URL. The institution exchanges this code for an access token and ORCID iD, that are stored in the institution’s system with the user’s information.

The institution then presents the user with a screen based on if she/he clicked the “authorize” or “deny” button (which can be determined by the information appended to the URL.) Closing this window will return the user to the ORCID page.

User Authorizes connection


- How the client application knows: a 6-character authorization code is appended to the redirect URL
- What the application should present: institution presents a confirmation



## User Denies connection

- How the client application knows: the following error is appended to the redirect URL, "error=access\_denied&error\_description=User%20denied%20access "

- What the application should present: institution confirms that no connection was made, and provides additional information for the user to consider.

 **PennState**

**ORCID**  
Connecting Research  
and Researchers

Member  
Organization

---

## No connection was made

### Didn't I just do this?

You have enabled single sign on, allowing your Penn State log in credentials to be used when using the ORCID website and services. At the moment this connection is in one direction: the ORCID site understands who you are when you use your Penn sign in, though the university doesn't know your ORCID ID, and can't read or write to your ORCID record.

### Why is Penn State asking for permission to access my ORCID iD & Record?

As you know, ORCID iDs are used by publishers, funders, associations and other organizations to make sure that your work is correctly attributed to you. Connecting your iD and record to the university will provide several other benefits, including:

- \* UNIVERSITY PROFILE UPDATE: Matches publications by your ID eliminating your need to confirm each publication is yours.
- \* REPOSITORY SERVICES: When you deposit datasets and publications in the university repository, we will automatically add them to your ORCID record, making them available to other organizations and services.
- \* AUTOMATED FORMS & REPORTING: If you connect your iD and Record, we will pre-fill <this specific> annual report, eliminating paperwork and reporting burden.

To do this, Penn State needs your permission.

### Can't I just give you my iD?

Yes. We have provided a link below to enable this more-limited access to your ORCID information. Some benefits mentioned above will not be available with this more limited access.

I still don't want  
to grant permission.  
Don't ask again

Only link my  
ORCID iD

I changed my mind.  
Let me try again



Member flow: ORCID to eduGAIN IdP cross-link

## Asserting affiliation

Once permission has been obtained in the previous step, ORCID recommends asserting affiliation information for the user. Doing so will earn your institution “Connect” status in ORCID’s Collect and Connect program, and will benefit the user by providing a “validated” affiliation with your institution that can be used to communicate their connection to your institution via their ORCID records.

All steps in this process can be done at any time with the permission that was obtained without further interaction with the user.

To post an affiliation:

1. Format an ORCID message with data related to the user’s affiliation with the institution. When posting an affiliation, you should include your institution’s Ringgold ID.
2. Post the affiliation to the ORCID record using the ORCID API and the access token obtained during the permission step above.

Affiliation information that you have added can be updated at any time with the same permission authorization as long as the user has not revoked it.