

ORCID Member API - Vendor & Open Source System Integration Guide

Introduction

The ORCID API (Application Programming Interface) provides technical infrastructure that can be used to connect the ORCID registry (ORCID iDs and data in individuals' ORCID records) with local organizational systems and applications to help save time and reduce administrative burden for researchers, administrators, and other stakeholders in the research and scholarly communication ecosystem. The ORCID Member API is recommended for use in organizational systems. This guide provides instructions on how to set up an ORCID Member API integration with a vendor or open source software system. For more information about the ORCID API, check out our [ORCID API Basics and Benefits webinar recording](#) and our documentation on [how researchers can connect their ORCID iD with an organization via the API](#).

The ORCID Member API allows for the following functionality, depending on how the integration is configured:

- Users can [log in to an application using ORCID](#)
- The application can [get a user's authenticated ORCID iD](#)
- The application can [read data](#) (set to public and/or trusted parties only visibility) from a user's ORCID record
- The application can [write data](#) to a user's ORCID record
- The application can [receive webhooks notifications](#) to enable syncing data between ORCID records and a local system

An ORCID API “integration” typically consists of 3 main components:

- 1) An end-user facing web page (or “ORCID portal”) where the user is prompted to connect their ORCID iD to the institution/application as a [trusted party](#) via the [ORCID authentication \(OAuth\) process](#) (For details about how the OAuth process works, see our [written documentation](#) and/or [video demonstration](#))
- 2) A secure back-end database where authenticated ORCID iDs and access tokens are stored after the user completes the OAuth process
- 3) [API calls](#) used to read data from and/or write data to a user's ORCID record once the authenticated ORCID iD and access token have been retrieved and stored

These components will already be enabled in vendor software or open source software systems that have ORCID API functionality built in.

Planning

When assessing where and how to use the ORCID API in institutional systems, you should consider the systems and software you are currently using:

- 1) Check our [list of common systems for ORCID integration](#) to see the ORCID functionality status of any systems that you might be using, as well as email templates that can be used for contacting vendors to request ORCID API functionality. Note that some vendor systems are [ORCID Certified Service Providers](#) and have the ORCID API already built-in with varying degrees of functionality. Other vendor systems are [non-certified service providers](#) that may or may not have built-in ORCID API functionalities
- 2) If you are using a vendor system, your approach will be limited to how the vendor has configured their system to use the ORCID API. The availability of ORCID functionality within a software system depends on which [scopes](#) (permissions) the vendor has included in their ORCID API integration. Possible scopes include:
 - a. **/authenticate** - used to collect the user's authenticated ORCID iD and read public data from ORCID record
 - b. **/read-limited** - used to read data from a user's ORCID record that has been set to "trusted parties only" visibility
 - c. **/person/update** - used to update the following information on the user's ORCID record: other names, keywords, countries, researcher URLs, websites, and personal external identifiers
 - d. **/activities/update** - used to update the following information on the user's ORCID record: employment, education, qualifications, invited positions, distinctions, membership, service, funding, works, peer review, and research resources
 - e. **/webhook** - enables your local system to receive a notification when information on a user's ORCID record has been updated
- 3) If you are using custom or open-source systems, you will have more flexibility in what you can do with the ORCID API if you have the staff time and resources to make customizations to the software code. See our [Custom Integration Guide](#) for more details. Some open-source systems already have the ORCID API built-in to varying degrees, and may also be ORCID certified Service Providers.
- 4) Read and learn how other organizations implemented their vendor system integration
 - a) Example: [Pure vendor system at the Research Triangle Institute \(RTI\)](#)
 - b) Example: [ProposalCentral vendor system and Funders](#)
 - c) Example: [Esploro vendor system at Brandeis University](#)

Implementation

Step 1: Determine the status of your software system

Determine whether the software system you are using is an [ORCID Certified Service Provider](#) or not. If it's not listed on ORCID's Certified Service Provider page, it is likely not certified. You can also check our [list of common systems for ORCID integration](#) for more details.

Step 2: Get your ORCID production API key

For an [ORCID Certified Service Provider](#) system, you can get your ORCID production API key right away:

- To get your production API key, please fill out the form: [Register for a client application: Production Member API](#) - Work with your vendor representative on how to fill out the form including what redirect URIs you should use, ORCID functionalities that can be enabled, and the scopes that need to be used
- Decide what ORCID functionalities you want to enable, if applicable. Some functionalities could be enabled at a later time; however it is recommended to ask for all scopes (see scopes above) when your user first connects their ORCID iD
- Test all ORCID functionalities before launching your application

For a [non-certified service provider](#) system, an integration review needs to be conducted by an ORCID US Community staff member prior to getting a production API key, to confirm that your integration meets the [minimum requirements for an ORCID integration](#).

- To get your ORCID sandbox API Client ID and Client Secret, fill out [ORCID's sandbox credential request form](#) - Work with your vendor representative on how to fill out the form including what redirect URIs you should use, ORCID functionalities that can be enabled, and the scopes that need to be used
- Decide what ORCID functionalities you want to enable, if applicable. Some functionalities could be enabled at a later time; however it is recommended to ask for all scopes (see scopes above) when your user first connected their ORCID iD
- Follow the instructions for testing in the ORCID [Sandbox Testing Server](#), and test all ORCID functionalities in the sandbox environment before launching your application
- When you are ready to move to production, or if testing in the sandbox is not possible, contact orcidus@lyrasis.org and we will schedule an integration review (see below for details about the integration review)

Step 3: Document and promote your ORCID integration

Create an informational web page where your researchers can learn about the ORCID integration within your vendor or open-source system, including documentation for how to use the ORCID functionality that is available within the system.

Decide where the ORCID informational page will live, and design the ORCID information page to include what is ORCID and why researchers should connect their ORCID iD

- a. Example: [University of Tennessee at Knoxville](#)
- b. Example: [University of Iowa](#)

Consider offering informational sessions, training, and other ways to promote your ORCID API integration to ensure that your researchers are aware of the integration and encouraged to use it. See our [Outreach Planning Guide](#) for ideas and examples.

Integration Review (for non-certified service providers only)

When you have completed development of your non-certified vendor system integration, please contact orcidus@lyrasis.org to schedule an integration review via Zoom, where we will ask to see a demo of the integration. For the demo, we will ask you to walk us through the ORCID OAuth process that you have set up using the ORCID sandbox environment, where we will be looking for the following:

- **Required:**
 - Confirm use of OAuth to collect authenticated ORCID iDs. Specify scopes used.
 - Do not allow users to edit, search for, type in ORCID iDs.
 - Confirm that ORCID iDs are being publicly displayed. [Check display formats](#).
 - Confirm that at minimum the authenticated ORCID iD and access token are being stored securely.
 - Use HTTPS for your site's redirect URIs and on ORCID API calls.
 - If your integration is set up to write information to ORCID records, we will also need to confirm that put codes are being stored. (Every item that you add to the ORCID Registry will be returned with a put code by the ORCID API, and you will need the put code if you need to [update the item](#) later, for example, updating the end date on an employment affiliation.)
- **Recommended:**
 - Confirm use of Branded buttons and other [UX guidelines](#).
 - Confirm workflow if the user clicks “deny” during the OAuth process (see [sample “Deny” text](#)).
 - Confirm option to allow the user to disconnect their iD from the application.
 - Confirm user-facing text that explains the purpose of the integration, why the user should connect their ORCID iD, and how the ORCID iDs and ORCID data will be used by the organization.
 - See [ORCID's additional best practices](#)

After the integration review, you can get your production API key (Client ID and Client Secret) by filling out [ORCID's production credential request form](#). Work with your vendor representative on how to fill out the form including what redirect URIs you should use.

Assessment & Maintenance

- Make sure you are using the most current ORCID API version. As of Feb. 2022, the most current ORCID API version is [v3.0](#).
- If writing affiliations to ORCID, make sure to update end-dates when someone leaves and is no longer affiliated with your organization. If a user has revoked their access token, you will no longer be able to update their record, but you can still [delete any affiliation entries](#) as needed.

- Periodically check with your vendor to learn more about system developments and updates involving ORCID and/or check the [Common Systems for ORCID Integration](#) for updates
- Consider adding more value by reading and/or writing more fields to ORCID records.
- Make sure your researchers know about your ORCID integration so they can take the necessary steps to connect their ORCID iD. Conduct additional outreach to researchers as needed, using resources available on our [ORCID Outreach Resources](#) page.
- Check your [integration reports](#) in the ORCID Member Portal (log in at <https://member-portal.orcid.org/>) to monitor usage and connections.
- Contact orcidus@lyrasis.org for any questions.