IATI Unified Platform

IATI Secretariat

May 26, 2026

UNIFIED PLATFORM

The IATI Unified Platform is the data platform operated by the IATI Secretariat. It provides tools for registering published IATI data and downloading IATI data in various forms.

CHAPTER

ONE

ACCESSING DATA

IATI provides a number of tools to access IATI data. For more information and to choose the most appropriate one for you, see the Tools & Resources page on the IATI website

CHAPTER

TWO

PLATFORM OVERVIEW

2.1 Register Your Data service

The IATI Registry was replaced in December 2025. We have written a *developers guide* to help adapt tools to work with the new set up.

Information about reporting organisations and their IATI files is now available on the IATI Dashboard.

Reporting organisations can manage their IATI file information in IATI Account.

2.2 Bulk Data Service

The Bulk Data Service runs on a continuous basis to maintain a copy of every file listed in the IATI Registry. Changes to published data can be reflected in as little as an hour, but may take up to 24 hours depending on the reporting organisation's technical configuration. Bulk downloads, debug information and download session listings are available from the Bulk Data Service.

2.3 Validator

All downloaded files are passed to the *Validator*, which assesses them against the IATI Standard. Validation reports are available on the web and via API.

2.4 Data Access Tools

Data access tools import data that has been downloaded by the Bulk Data Service and use information from the Validator to decide which data to use.

Caution

D-portal does not use the Unified Platform. Please refer to the D-portal documentation to understand how it works.

The *Datastore* saves all IATI activities, budgets and transactions from files that do not contain critical errors into a document store database and provides extensive querying and filtering capabilities. The Datastore can be accessed via a website and an API.

2.5 IATI Dashboard

The *Dashboard* provides a range of summaries, statistics and computed metrics of IATI data. In addition to summarising current IATI data, it provides historical data for most of the metrics of which it keeps track.

2.5.1 Developer Guide (IATI Registry replacement)

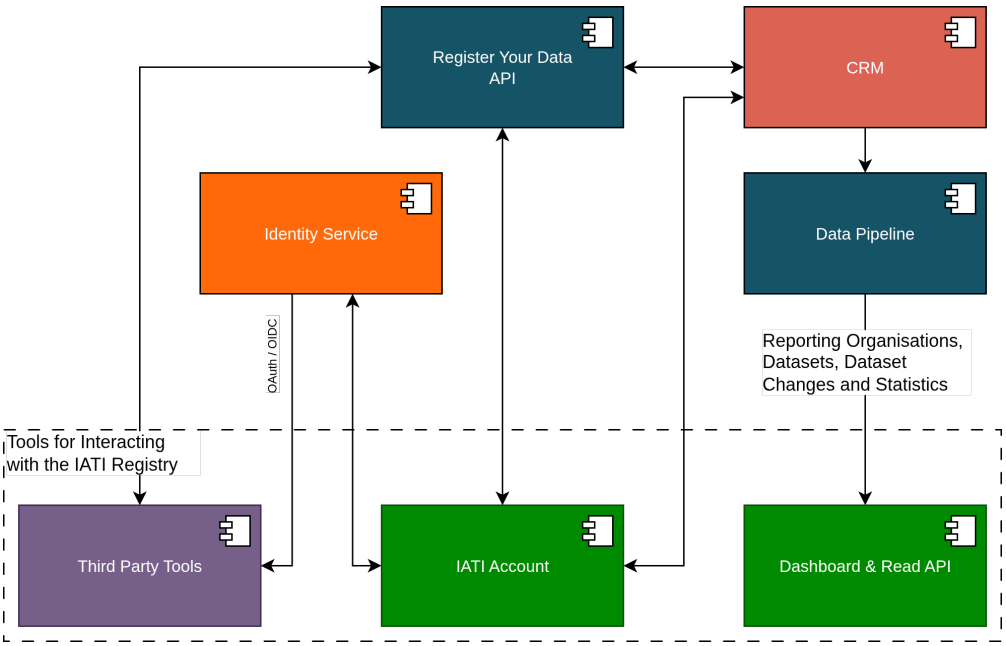
> **Attention**
>
> The IATI Registry was replaced in December 2025. If you believe that you will rely on the contents of these documents, please contact us to discuss your work.

Architecture Overview

The IATI Registry was replaced by IATI Account and changes to the IATI Dashboard in December 2025. There are a number of architectural differences between the new set-up and the previous CKAN-based Registry. To aid in the transition of tools and infrastructure, this document describes some of those architectural differences and how applications should now interact with IATI.

The diagram below shows a simplified architectural view of the new set-up. IATI reporting organisation and dataset metadata is stored in a CRM, and user data is stored in an Identity Service.

Data is changed in the CRM by the *Register Your Data API*. Data enters the IATI data pipeline from the CRM and is fed into the IATI Dashboard, which provides a *new read API and backwards-compatible CKAN read-only API* for downstream users to examine the contents of the CRM. Third party tools connect to the Identity Service and the Register Your Data API to provide services to end users. IATI Account is our new tool for creating and self-servicing user accounts, creating, editing and deleting reporting organisations and datasets, and managing user permissions for different reporting organisations.



Applications and Single Sign-On (SSO)

One of the key differences between the old CKAN-based IATI Registry and the new set-up is the use of Single Sign-On (SSO) as the method of authentication. This has been designed to simplify the user experience and enable a range of third party integrations with IATI infrastructure. However, to enable this enhanced functionality, applications will need to be refactored to facilitate SSO via our Identity Service. Although we emphasise SSO (via OpenID Connect) we will also support some limited OAuth2-based authentication.

OAuth2/OpenID Connect interactions with the Identity Service yield a short-lived access token that will be used to access an API for write access to the CRM. Details of how to use the access token are provided in the *Register Your Data API specification*. We intend to support three modes of connection:

- **Single Sign-On via OpenID Connect**: in this mode clients will log users into their application using OpenID Connect and will obtain an access token that will permit access to the organisation(s) associated with that user. This will be available at launch.
- **Machine-to-machine applications**: we will support connections using a Client Credentials OAuth2 grant. These connections are far more limited in terms of the organisations and calls that can be made to the API. We expect this to be available in Q3/Q4 2026.
- **Account linking**: we eventually expect to support clients that want to retain their own login system but facilitate linking to an existing IATI account. We expect this to be available in Q4 2026.

Third party tool providers that would like to connect to IATI infrastructure cannot do this without being registered in advance with the IATI Secretariat. Through this registration process we will discuss your needs, setup your application in the Identity Service, supply you with credentials to use when making calls to the Identity Service, and provide developer support.

> **Note**
>
> SSO is being rolled out across the IATI ecosystem and provides access for users to a range of services via a single user account. If your application logs in a user, that user will be logged into IATI and will also be able to access other tools. The converse is also true - that a user may arrive at your application having already logged into IATI through SSO in another tool. Applications should be designed to encounter these different scenarios and should support logout from IATI.

Restrictions

The Register Your Data API implements the same functionality as present in the previous CKAN-based Registry, but we have implemented additional per-application controls. As a result, the functionality available to third party tools is less permissive. In particular:

- Third party applications are not able to create new reporting organisations in the CRM.
- Applications using machine-to-machine OAuth2 connections are not be able to modify any user permissions or delete organisations.

Access tokens and API tokens

CKAN moved from API keys to API tokens as a progression from more simplified application-level authentication to more specific user-centric authentication and authorisation. The development of the Registry replacement continues this progression and introduces **individual authentication with short-lived, auto-expiring access tokens**. Any functionality that relies on using an API key or API token generated in CKAN must be refactored to work with the new set-up. An access token contains no information about what organisation(s) a user is attached to. This information is only available via the *Register Your Data API*.

To call the *Register Your Data API* and write any changes to the CRM, a short-lived access token must be obtained from the IATI Identity Service (e.g. through single sign on (SSO)) and passed to the API. This should be passed to the API via the HTTP `Authorization` header with a `Bearer` parameter. It is entirely possible that the token will automatically expire between receiving the token from the identity server and an API call being made, so tools should be prepared to handle error messages from the API and refresh the access token. As explained above, applications that wish to obtain an access token to call the API must be registered in advance with the IATI Secretariat.

User permissions

In CKAN, per organisation user permissions are controlled with the roles *admin*, *editor*, and *member*. In the replacement set-up, we have two levels of user permissions:

- coarse access control that determines which endpoints an access token can reach.
- *fine-grained* authorisation that determines which organisations and datasets can be changed, and what information can be changed via those endpoints.

Access Control: OAuth scopes

Access control to call certain API endpoints are restricted using OAuth2 scopes. An application should request the scopes it requires as part of it's OIDC/OAuth2 flow with the Identity Service. **It is important to recognise that not all these scopes may be granted** and so applications should should check these after the Identity Service flow has completed. If an API endpoint is called with an access token that does not have the required scopes, a 403 Forbidden HTTP response will be returned. The *Register Your Data API specification* lists the required scopes against each API endpoint.

Associated with this, a user with access to the *Register Your Data API* will have `iati_register_your_data` as a `role` in the OAuth2 claims obtained from the Identity Service `userinfo` endpoint.

Fine-grained Authorisation

Per organisation user permissions are controlled with a system of *fine-grained* authorisations that offers similar permission groups to CKAN. These control which organisations and datasets a user is able to access, and what changes they can make. Similar to CKAN, we group these into three roles that are roughly analogous to CKAN's *admin*, *editor* and *member*:

- **admin**: for organisation administrators.
- **editor**: for organisation and dataset editors.
- **contributors**: for data editors.

These can only be assigned to a user for a particular organisation via calls to the Register Your Data API by an organisation admin.

There is a fourth role (**provider admin**) that will be discussed in the provider admin section below.

The table below shows the fine-grained authorisations that these roles have:

Authorisation	Admin	Editor	Contributor	Provider Admin
read-org	x	x	x	x
update-org	x	x		x
delete-org	x			
set-org-user-authz	x			
set-org-tool-authz	x	x		
read-dataset	x	x	x	x
create-dataset	x	x	x	x
update-dataset	x	x	x	x
update-dataset-visibility	x	x		x
delete-dataset	x	x		x

Relative to an admin, an editor cannot:

- Delete an organisation.
- Change the public/private visiblity of a dataset.
- Modify the permissions of users associated with an organisation.

Relative to an editor, a contributor cannot:

- Update an organisation's metadata.
- Authorise a tool to access the records of this reporting organisation (or revoke that access).
- Delete a dataset.

Super-administration

IATI Secretariat staff will have a *superadmin* authorisation where their access tokens afford them full access to any organisation and dataset. Superadmins can be identified by examining the `role` claim in the payload from the Identity Service userinfo endpoint and which should include `iati_superadmin`.

Provider admin

To support third parties in developing tools and supporting the community, we have implemented a system of enhanced permissions that we refer to as *Provider Admin*. Any third party tool can provide assistance to its users through some limited admin access to an organisation's records. Eventually the authorisation for third party tools to access the records of a reporting organisation will be managed in IATI Account.

There are three components to the Provider Admin model:

1. A *tool* is a third party software application that is developed, maintained and offered by a *provider*. Such tools are built to work with Register Your Data. One *provider* may offer a number of tools to suit different business and user needs.
2. Reporting organisations can give provider admin permission for *tool(s)* to access and edit its records.
3. A user with an IATI Account can be attached to a *tool* and they then become an *admin user* of that tool. When logged into IATI infrastructure - **and when the access token is scoped to include that tool**, these *admin users* will have permissions to make changes to any reporting organisation that has given permission to that *tool*. Normally the access token scoping will be achieved by calling RYD with an access token that has been obtained by a call to the identity service from that tool. This means that a tool admin user cannot use provider admin permissions in a different tool.

By way of example:

- A *tool* called "Aid Support Tool" is provided by "Aid Support Company". The IATI Secretariat add this information to Register Your Data.
- A reporting organisation called "Aid Agency" gives permission for "Aid Support Tool" staff to update its dataset records.
- A staff member, "Analyst", at "Aid Support Company" provides support for users of "Aid Support Tool". The IATI Secretariat add this staff member to the "Aid Support Tool" in Register Your Data.
- When "Analyst" logs into "Aid Support Tool" they will be able to read the datasets of "Aid Agency" and update these records via Register Your Data.
- These changes will be recorded as having being performed by "Aid Agency" (as "Aid Support Company" is providing support to "Aid Agency" under contract).
- As "Analyst" has logged in via single-sign on, they could then log into another IATI tool, for example, IATI Account. However, "Analyst" will not have provider admin within IATI Account and so this functionality will not be available in that tool.

To setup a *tool* in Register Your Data and add/remove *admin users* please contact us.

There are some notable restrictions for provider admin:

- An *admin user* for a *tool* cannot have an *admin*, *editor* or *contributor* role to access any reporting organisation. In these cases users should have separate accounts: one for *admin user* work within *tools*, and one for any work that involves being an *admin*, *editor* or *contributor* of reporting orgs.
- A call to the `/reporting-orgs` endpoint in the *Register Your Data API* will not return a list of all the reporting orgs that the user has access to via provider admin. *Tools* can call the `/users/{uid}/roles` endpoint which will provide broad information on the permissions a user has: superadmin status, the tools for which the specified user is an admin user, and the reporting orgs and roles the user has for them. If the specified user is an *admin user* for a *tool* then this will only include *provider_admin* roles, otherwise, it will show regular roles.
- Per-tool permissions are not currently supported but may be implemented in the future.
- Eventually IATI Account will enable users to see which *tools* have been given provider admin permission, and to revoke and grant this permission. It will not enable reporting organisation users to see the names of *admin users* of *tools*.
- Lists of users with reporting organisation roles (*admin*, *editor* or *contributor*) will not include *tools*.

Augmenting SSO user data

There is nothing in the SSO model that prevents third party tools from having additional user data or user permissions to suit the functionality of the tool.

Additional user data

An example of this case might be that a tool wants to record the last dataset that a user was working on so that they can optionally return the user to that dataset upon login.

This functionality can be implemented by having a separate user database in the third party tool and where the user record in that database can be looked up using the `sub` unique identifier (or other unique information, such as a hash of the username) that is received from the Identity Service. It is important to recognise however, that any personal data about that user (for example, their name or working country) could be changed between logins by the user.

Additional permissions

Some example use cases might be:

- A tool that automatically generates XML files may want to add additional permissions such that some users can overwrite an existing XML file, and some cannot.
- A tool that allows some users to edit dataset metadata for records that point to activity files, vs. organisation files.

These must be added on top of user permissions provided by the new Identity Service, and recorded separately in a similar fashion to additional user data. It is important to recognise that there is nothing to stop a user from logging into another tool and modifying data. For example, if you add permissions to restrict users from modifying the metadata for different categories of XML dataset record, a user can still log into other tools and modify the data.

Key architectural changes

Naming and Identifying Resources

CKAN used the naming system of *Publisher*, *Package* (and associated *Resource(s)*) and *User*. Terminology going forward is designed to be more in line with the IATI Standard.

Publisher

A publisher is now described as a "**Reporting Organisation**"", following the IATI Standard `iati-organisation`, `iati-organisations` and `reporting-org` elements. Any reference to a reporting organisation or a reporting org should be read in the same way as a "**publisher**" in CKAN.

Package (and Resource)

In CKAN a dataset was comprised of a package with one (or potentially more) resources attached. This is because CKAN supported a model where a single package could have more than one file. Going forward, a **Dataset** is a combination of Package and Resource.

Primary keys: organisation and dataset shortnames

We are moving away from using organisation and dataset short names as primary keys and towards using UUIDs. For example, rather than calling `GET /reporting-orgs/bopinc`, you must use the UUID `GET /reporting-orgs/08beaaaf-d007-402f-aca6-993a18082071`. The short names still exist in the new CRM, but they will no longer be supported as primary keys.

Metadata

The new CRM and Identity Service supports far fewer metadata fields than the CKAN-based Registry, particularly for users and reporting organisations. For example, the Identity Service no longer stores fields for users to describe themselves (`about`).

The CRM will not support the following Publisher fields:

- `image_url` and `image_display_url`.
- `publisher_agencies`.
- `publisher_constraints`.
- `publisher_data_quality`.
- `publisher_field_exclusions`.
- `publisher_frequency`, `publisher_frequency_select`.

- `publisher_implementation_schedule`.
- `publisher_record_exclusions`.
- `publisher_refs`.
- `publisher_segmentation`.
- `publisher_thresholds`.
- `publisher_timeliness`.
- `publisher_units`.

Unsupported features

CKAN supported the ability to *tag* packages and allowed the ability to *follow* particular publishers. Both of these features are not supported in the new set-up.

Relationships and Record Ownership

Multiple organisations

In the new set-up, as with CKAN, users will have permissions to administrate and manage metadata for more than one organisation. For example, a user could be an admin for "Organisation A", admin for "Organisation B", and editor for "Organisation C". Accordingly, the `/reporting-orgs` endpoints for the *Register Your Data API* can return more than one organisation for a logged in user. All tools that call the API should be able to handle a response that includes multiple organisations, even if they only expect a single organisation.

Dataset Ownership

In CKAN there was a strong relationship between a dataset and the user that created it. As a result, when an organisation was deleted in CKAN, its datasets could still exist in IATI and be visible in the pipeline. The new set-up removes this strong connection. Datasets are owned by reporting organisations. When a reporting organisation is deleted, its datasets will also be deleted.

Links will still exist between datasets and users, but no ownership is implied:

- We store the user that creates a dataset.
- We record lists of actions that are carried out on datasets (e.g. changing a URL) and which user made that change.

For these reasons we do not provide a *Register Your Data API* endpoint to return all the datasets that a user has access to. This could encourage an opportunity for a user to inadvertently modify a dataset. For example, if a user had the permission to update dataset metadata for multiple organisations and was carrying out a task to change the licence for all the datasets published by one organisation, they could easily inadvertently modify the licence for datasets owned by another organisation.

Migration from the CKAN API to the Register Your Data API

These notes are aimed at providing guidance for migrating from the CKAN API to the new *Register Your Data API* by describing how equivalent operations are performed.

Reporting Orgs (Publishers)

List of reporting organisations: /organization_list

You call the GET /organization_list endpoint to obtain a list of publishers in CKAN, which allows you to fetch a list of all organisations. The equivalent in the Register Your Data API is `GET /reporting-orgs`, which will fetch a list of

all reporting organisations **to which the user has access**. The endpoint will not return other reporting organisations. To achieve this you should make separate calls to the Dashboard API.

Showing reporting organisations details: /organization_show

The details of a reporting organisation are available from the `/reporting-orgs` endpoint. If you wish to fetch organisation details, similar to the CKAN GET /organization_show endpoint, then you can call `GET /reporting-orgs/{oid}` where `oid` is the UUID for the organisation you want to fetch.

Creating a new reporting organisation: /organization_create

To create a new reporting organisation in CKAN you call the POST /organization_create endpoint. In the Register Your Data API, you must call `POST /reporting-orgs`. Note that access to this endpoint is more restricted than in the CKAN-based Registry. The access token must have the `ryd:reporting_org:create` OAuth scope, which will only be available to a small number of client applications.

Updating a reporting organisation: /organization_patch and /organization_update

To update a new reporting organisation in CKAN you either call the POST /organization_update or POST /organization_patch endpoints. The difference is that update will remove all fields not in the provided payload, and patch will replace fields that are provided. In the Register Your Data API, we only support updating organisation metadata using `PATCH` via the `/reporting-orgs/{oid}` endpoint, where `oid` is the UUID for the organisation you want to update.

Deleting a reporting organisation: /organization_delete

To delete an organisation in CKAN you call POST /organization_delete. In the Register Your Data API, you must call `DELETE /reporting-orgs/{oid}` where `oid` is the UUID for the organisation you want to delete.

Datasets (Packages)

In CKAN, getting lists of datasets could be achieved with `/package_list`, ``/package_search` and ``/organization_show` with the `include_datasets=true` query string. This is now achieved with `GET` to `/reporting-orgs/{oid}/datasets`.

Creating datasets

In CKAN, calls to POST /package_create will create a package and associated resource. In the Register Your Data API, this is achieved with `POST /datasets/`.

Viewing dataset metadata

To view dataset (and resource) metadata in CKAN, we call the GET /package_show endpoint. This is achieved with `GET /datasets/{did}` where `did` is the UUID of the dataset you want to get.

Updating dataset metadata

To update a dataset in CKAN you either call the POST /package_update or POST /package_patch endpoints. The difference is that update will remove all fields not in the provided payload, and patch will replace fields that are provided. In the Register Your Data API, we only support updating organisation metadata using `PATCH` via the `/datasets/{did}` endpoint where `did` is the UUID for the dataset you want to update.

Deleting a dataset

To delete a dataset in CKAN you call POST /package_delete endpoint. In the Register Your Data API, this is achieved with `DELETE /datasets/{did}`.

Example application flow

Your application wants to show a list of the reporting organisations your user has access to, perhaps with a little bit of metadata associated with them, such as name, number of published datasets, IATI organisation identifier. A call to `GET /reporting-orgs/?include_meta=yes` will fetch a list of reporting organisations with metadata on those organisations.

Then your application wants to allow a user to open a page for an organisation that shows a list of datasets. Calling the `GET /reporting-orgs/{oid}/datasets` endpoint will return a list of datasets for that organisation and all the metadata associated with each dataset.

Perhaps the user wants to update one of those datasets. A call to `PATCH /datasets/{did}` will update the dataset metadata and return the updated dataset metadata.

Perhaps then the user wants to change some user permissions in their organisation (assuming they are an organisation admin). `GET /reporting-orgs/{oid}/users` will get a list of users associated with an organisation and their roles. With a list of users your user might then change the role via an interface and you can make that change with a call to `PUT /users/{uid}/reporting-org/{oid}`.

2.5.2 Bulk Data Service

The Bulk Data Service runs on a continuous basis to maintain a copy of every file listed in the IATI Registry. The Bulk Data Service makes available a cached copy of each IATI file to allow access during temporary server outages, and in addition provides a ZIP file that allows all IATI files to be downloaded.

The Bulk Data Service API specification explains what information about the download status of each IATI file is available.

2.5.3 Validator

Please see https://docs.validator.iatistandard.org

2.5.4 Datastore

Please see https://docs.datastore.iatistandard.org/en/latest/

2.5.5 Dashboard

The *Dashboard* provides a range of summaries, statistics and computed metrics of IATI data. In addition to summarising current IATI data, it provides historical data for most of the metrics of which it keeps track.

The Dashboard provides an API which is the primary location for IATI data users to access IATI data, including accessing and searching the lists of reporting orgs and datasets.

In addition to the API above, which allows for advanced querying, the Dashboard also provides a limited functionality backwards-compatible CKAN API that mirrors some of the functionality of the CKAN-based Registry.

Further information can be found at https://dashboard.iatistandard.org/faq/.

2.5.6 Register Your Data API

The Register Your Data API allows developers to register IATI files automatically; this ensures that they will be included the data pipeline and made available across the range of IATI tools.

The RYD API might be for you if you are: * A tool developer who wants to include IATI file registration as part of the functionality available for your users. For example, if you make a tool that allows a user to create an IATI XML file, using the RYD API means that they can register it with IATI with just an IATI Account * A reporting organisation whose IATI XML URLs change regularly. Although stable URLs are preferable for consuming systems, this isn't always feasible and so the RYD API can help.

If you have only a few URLs, you can register these via your IATI Account. If you have a lot of URLs but they do not change frequently, the IATI Secretariat can help with a one-time bulk import.

To request access to the RYD API, please contact the IATI Secretariat.