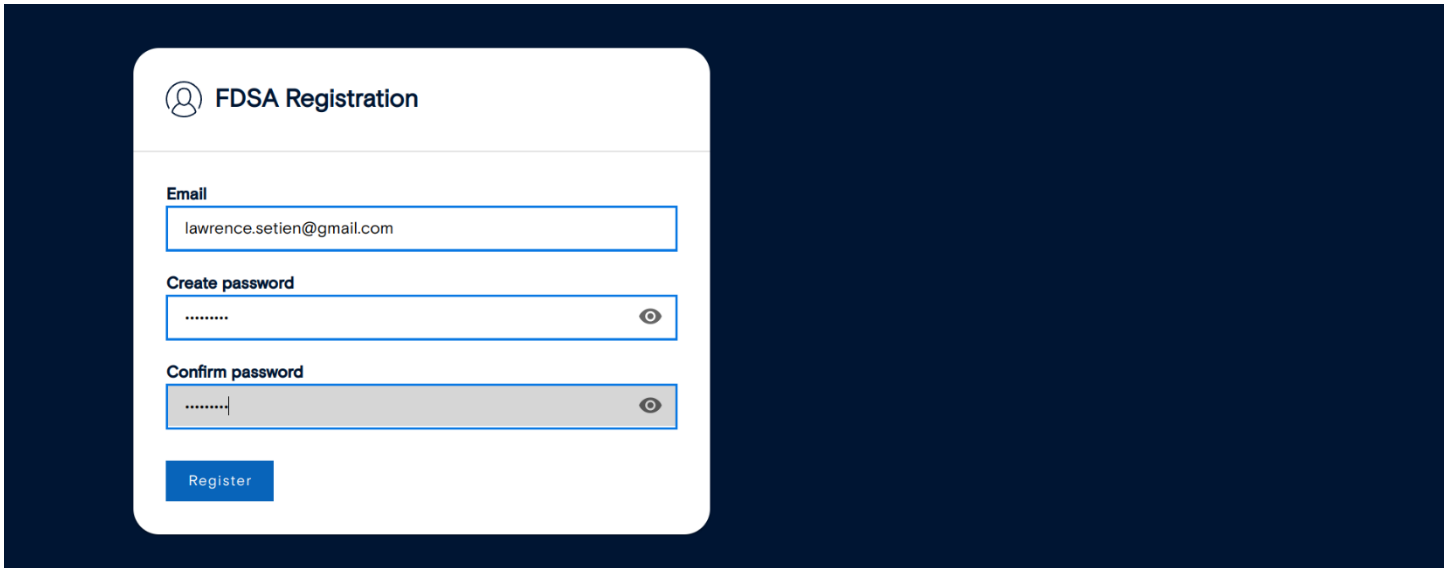
Administrator - First Time Configuration

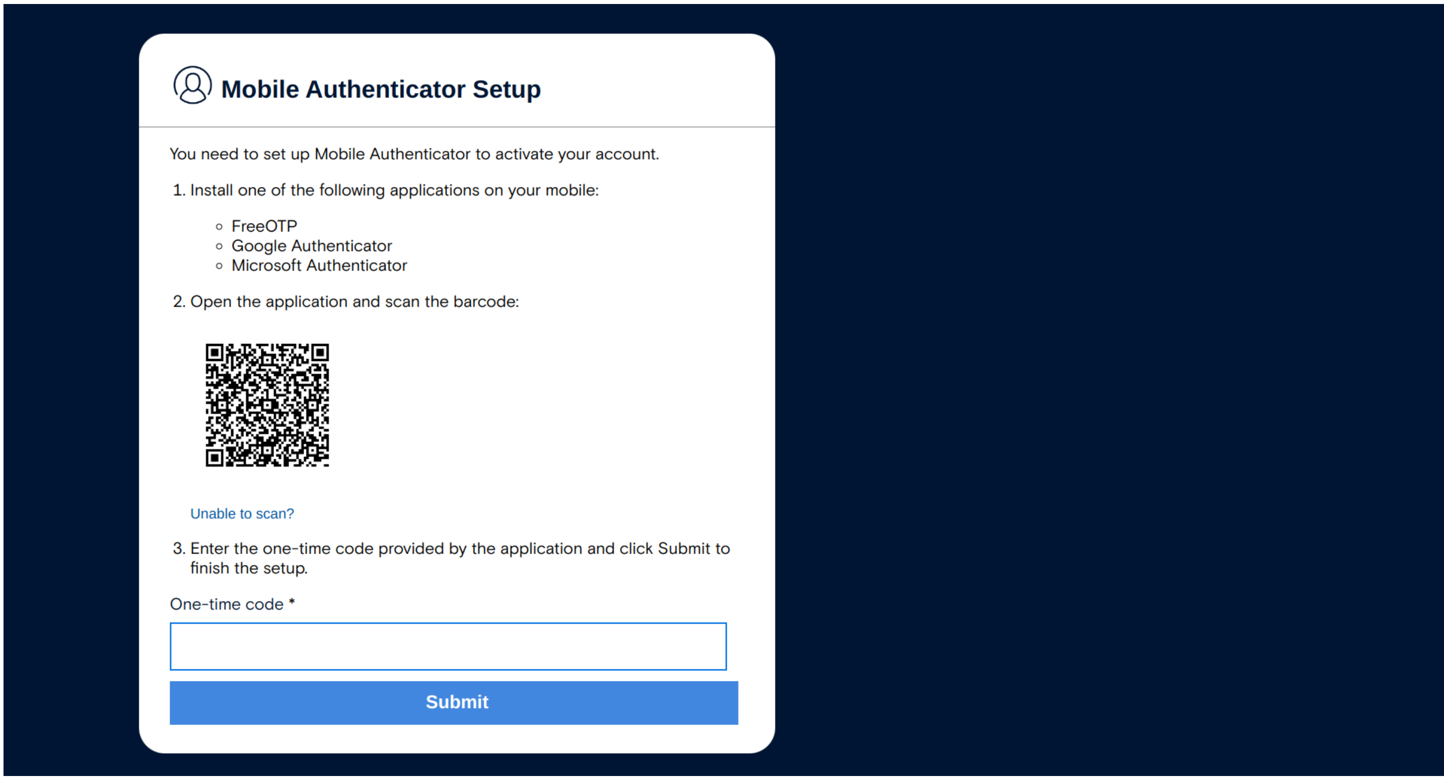
1. Create the first administrator

- Navigate to https://<your_domain>/admin

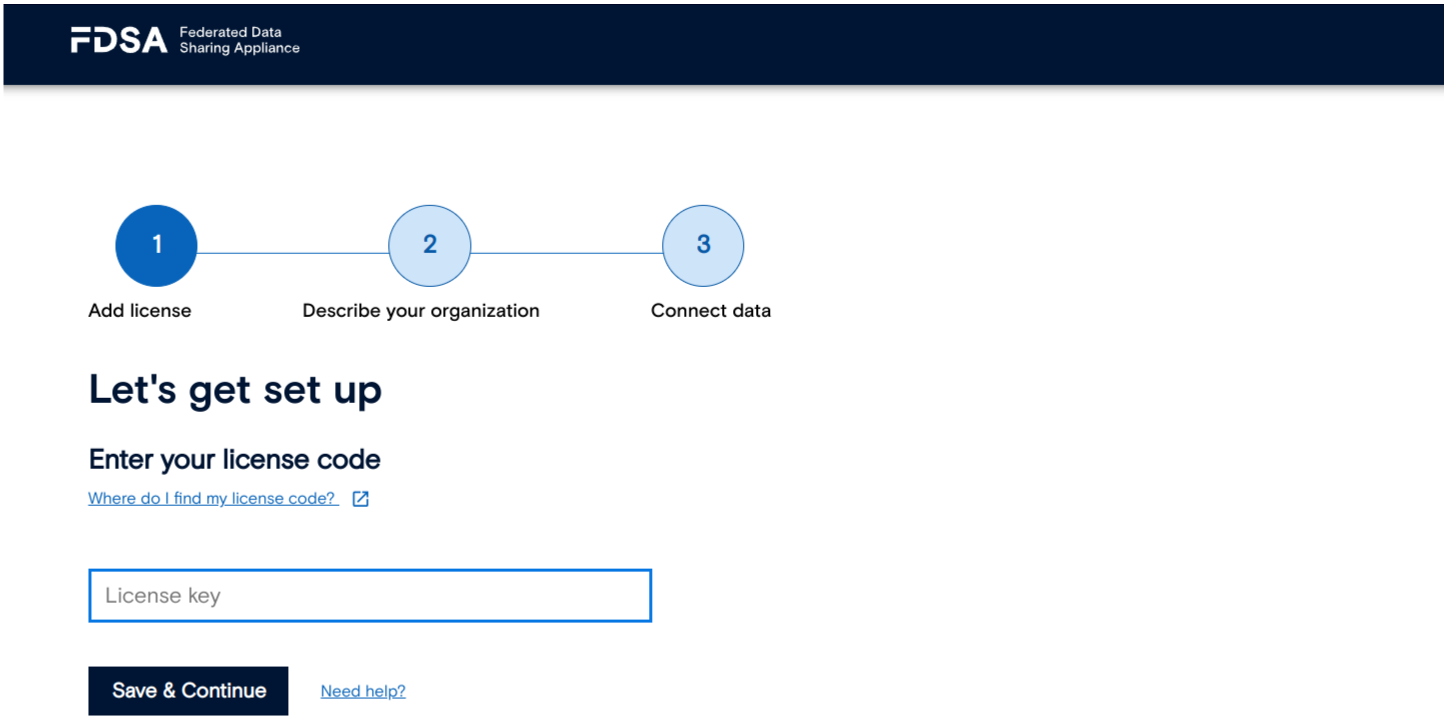


2. Sign in and setup your Multi Factor Authentication app

Note: If after scanning the MFA keeps failing, make sure the time in your phone and in the server are in synch.



3. Follow the first login set up steps



FDSA Federated Data Sharing Appliance

Add license — Describe your organization — Connect data

Let's get set up

Describe your organization

[Learn more](#)

Name of your appliance*

Documentation URL*

Name of your organization*

Contact email address*

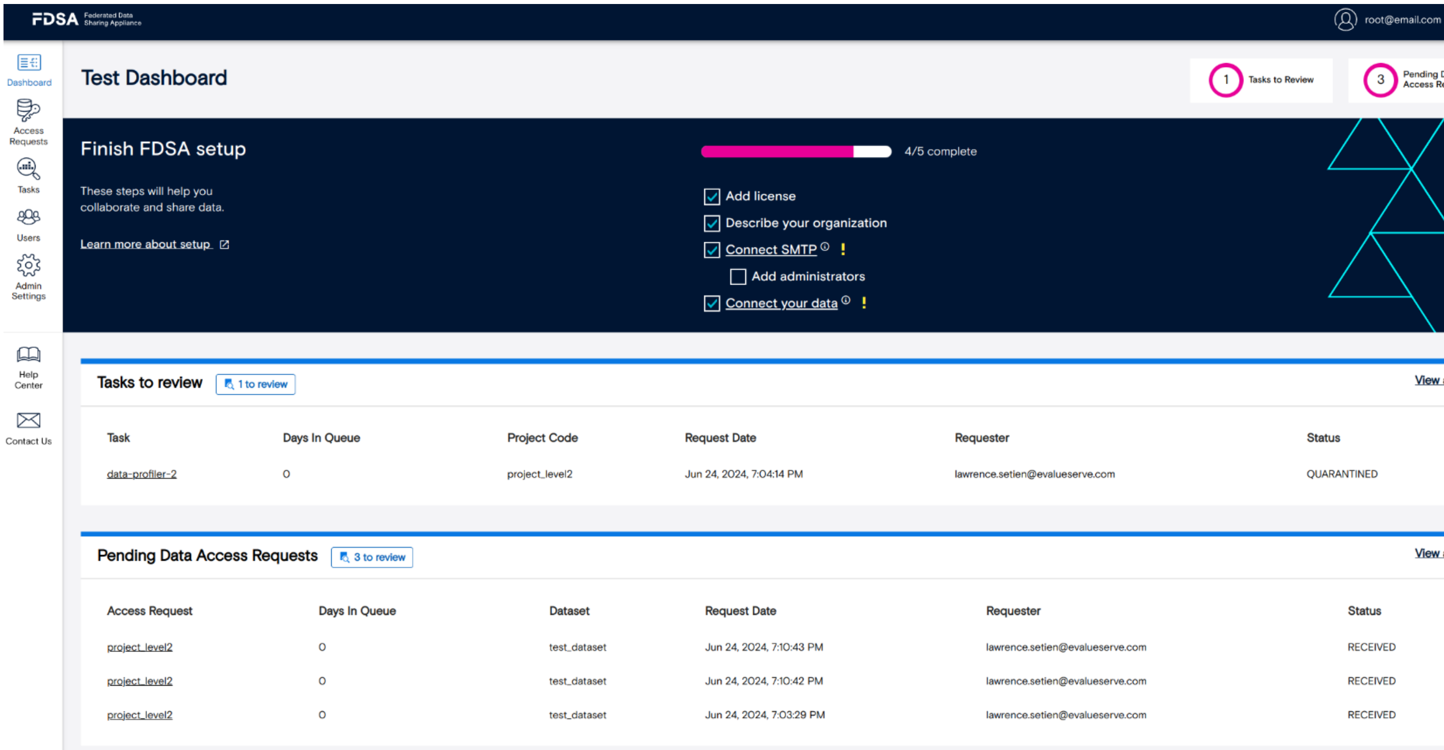
Description*

Save & Continue

[Need help?](#)

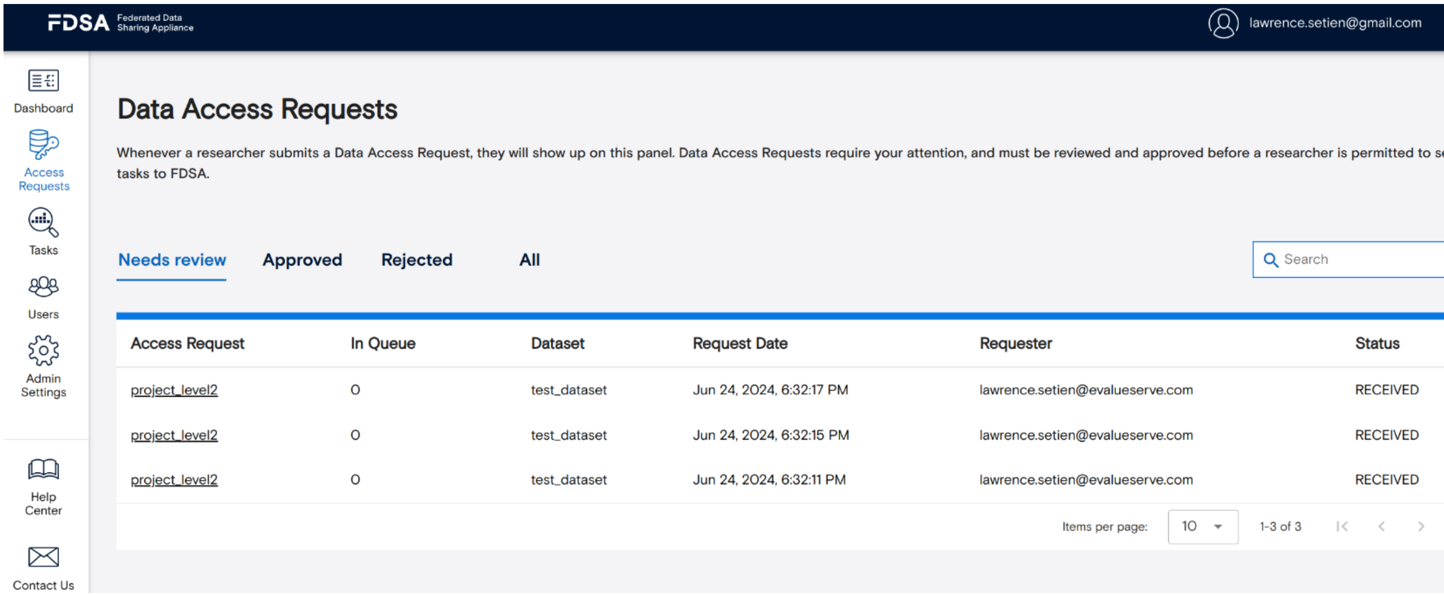
4. The Overview Section

On this section Admins can get a quick view of the FDSA status, including pending DAR and Tasks reviews.

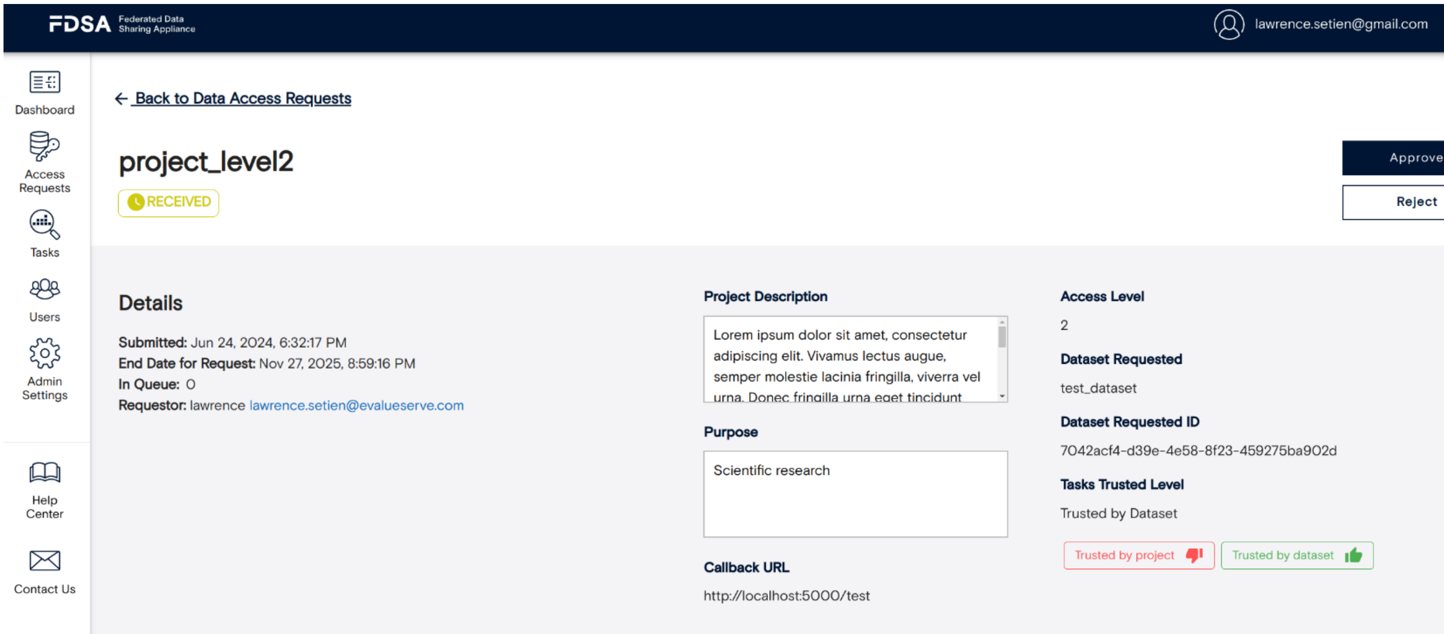


5. The Data Access Requests section

- On the Data Access Requests section, you can find more detailed information about the submitted DARs.



- Click on the Access Request name to view the details of a specific DAR.
- On this window, you can Approve or Reject the DAR.

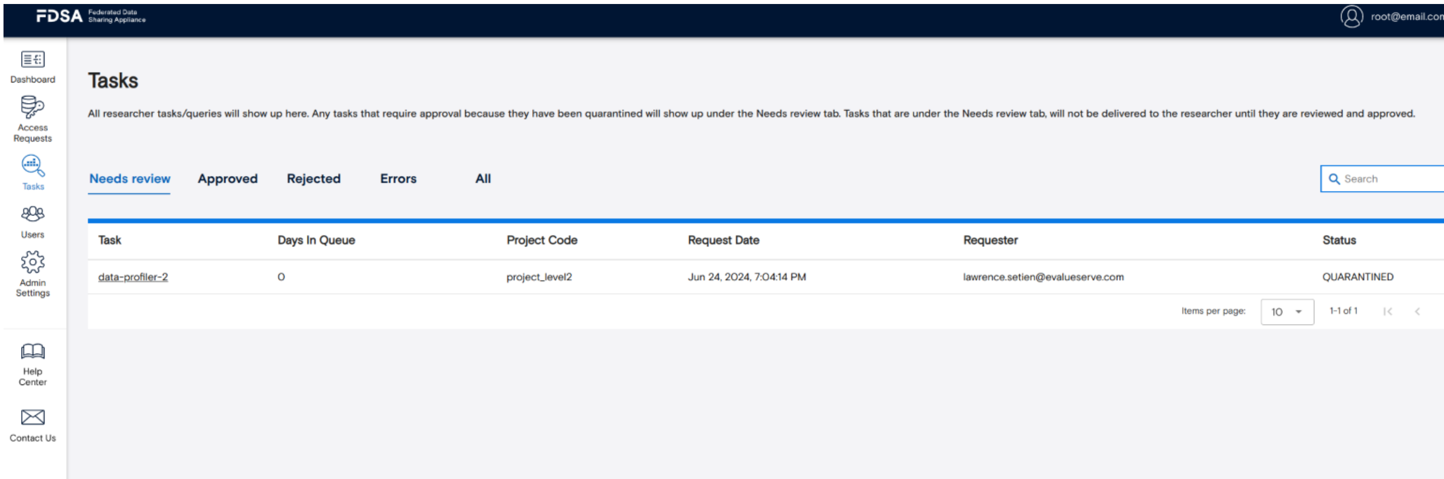


Note: There are two types of 'trust' mechanisms:

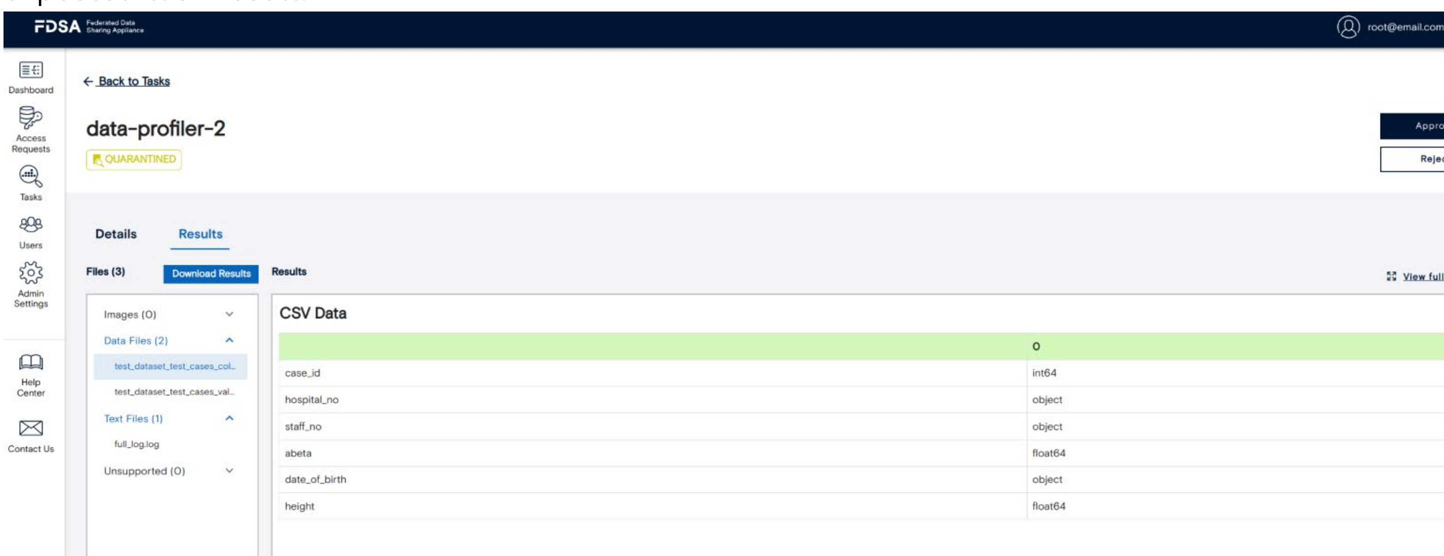
1. By dataset: Every task created under that dataset will go directly to COMPLETE without needing a review.
2. By project: Every task created under that project code will go directly to COMPLETE without needing a review.

6. The Tasks Section

In this section you can review Researcher submitted tasks.



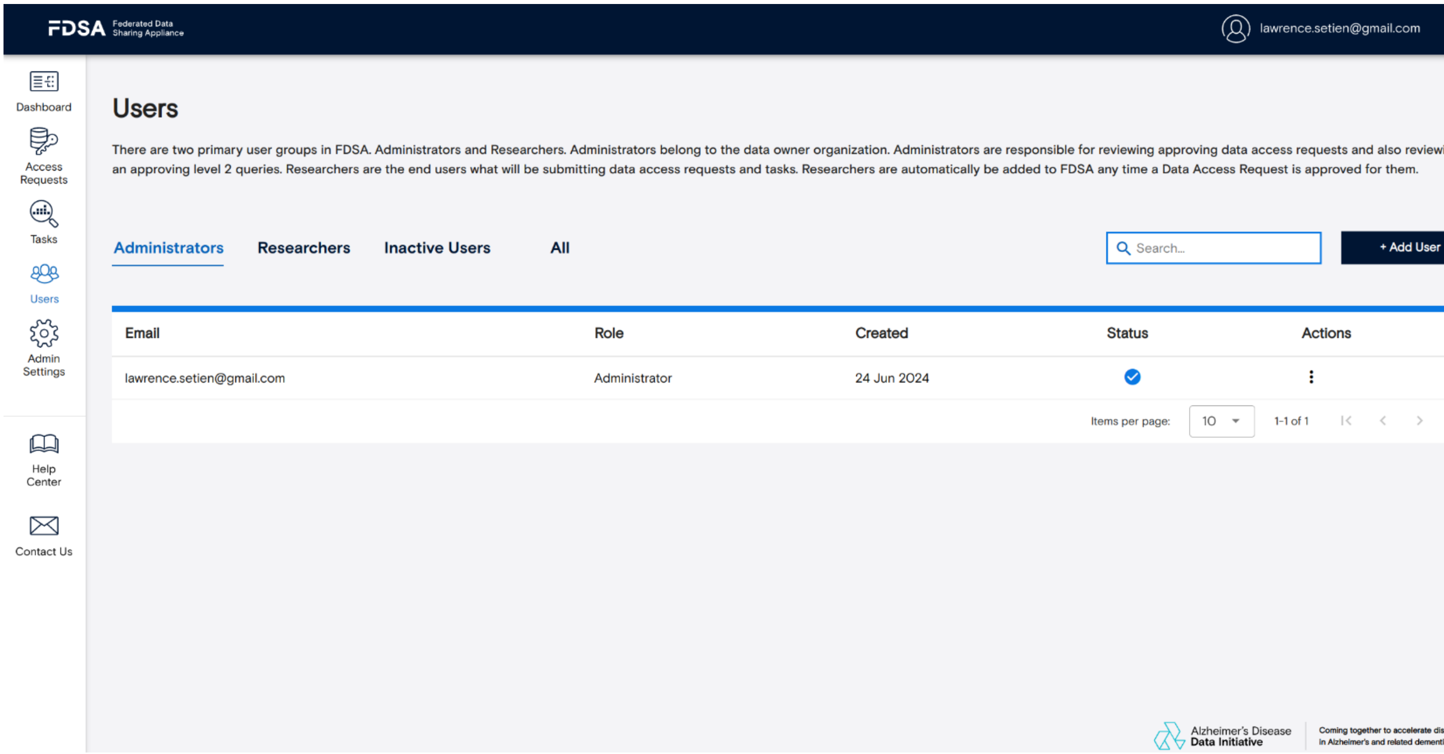
By clicking on the task name, you will see a detailed view. Click on Results to see the expected task result.

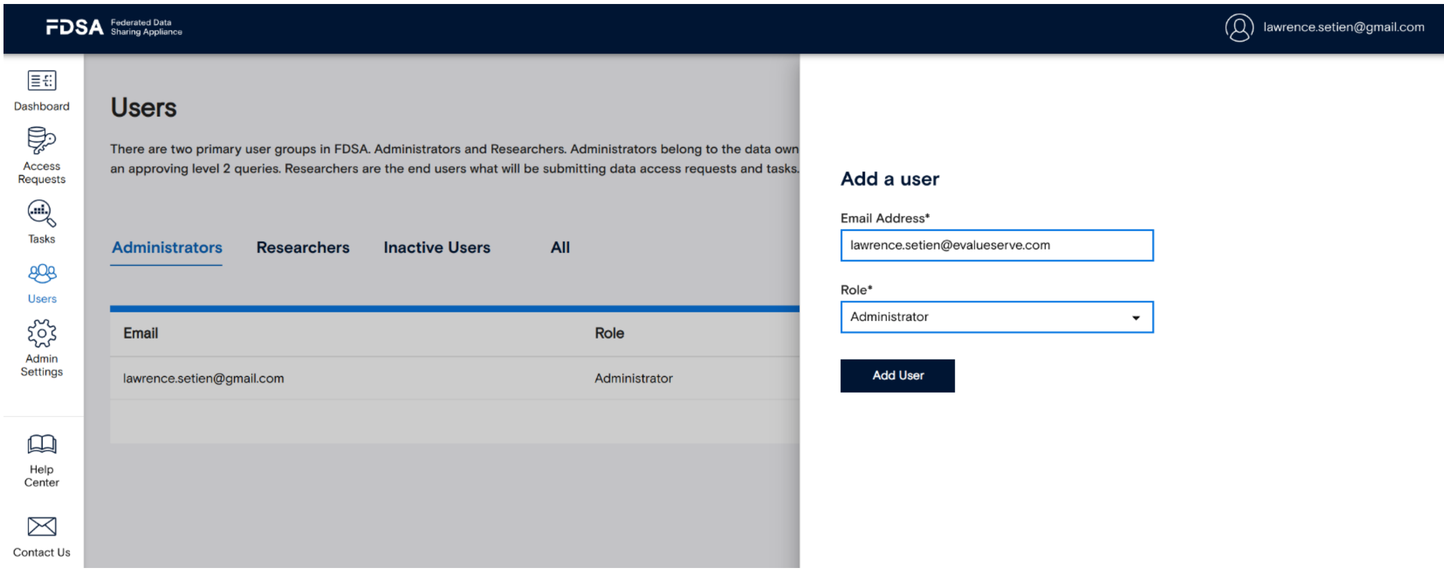


7. The Users Section

How to add a new FDSA user:

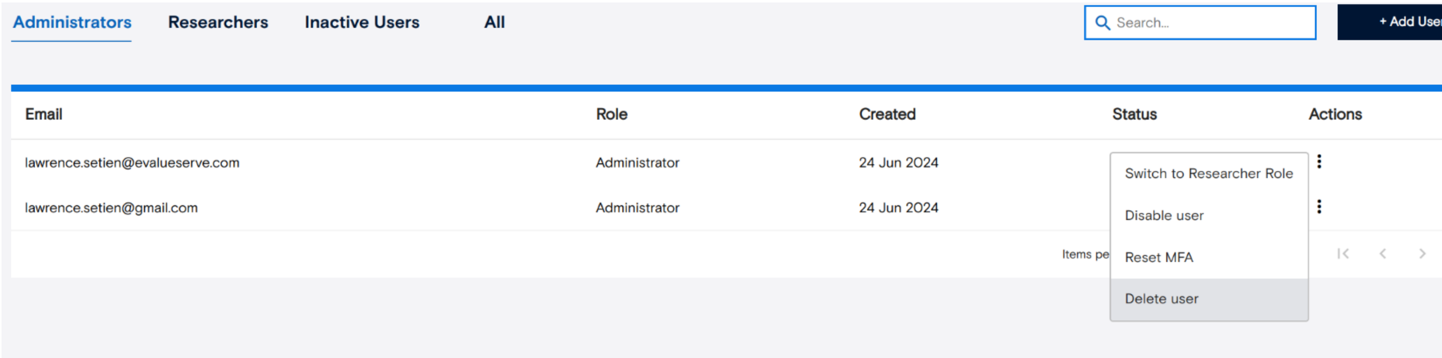
- Go to the Users tab and click on “+ Add User”
- Add the user email, role and click on “Add User”



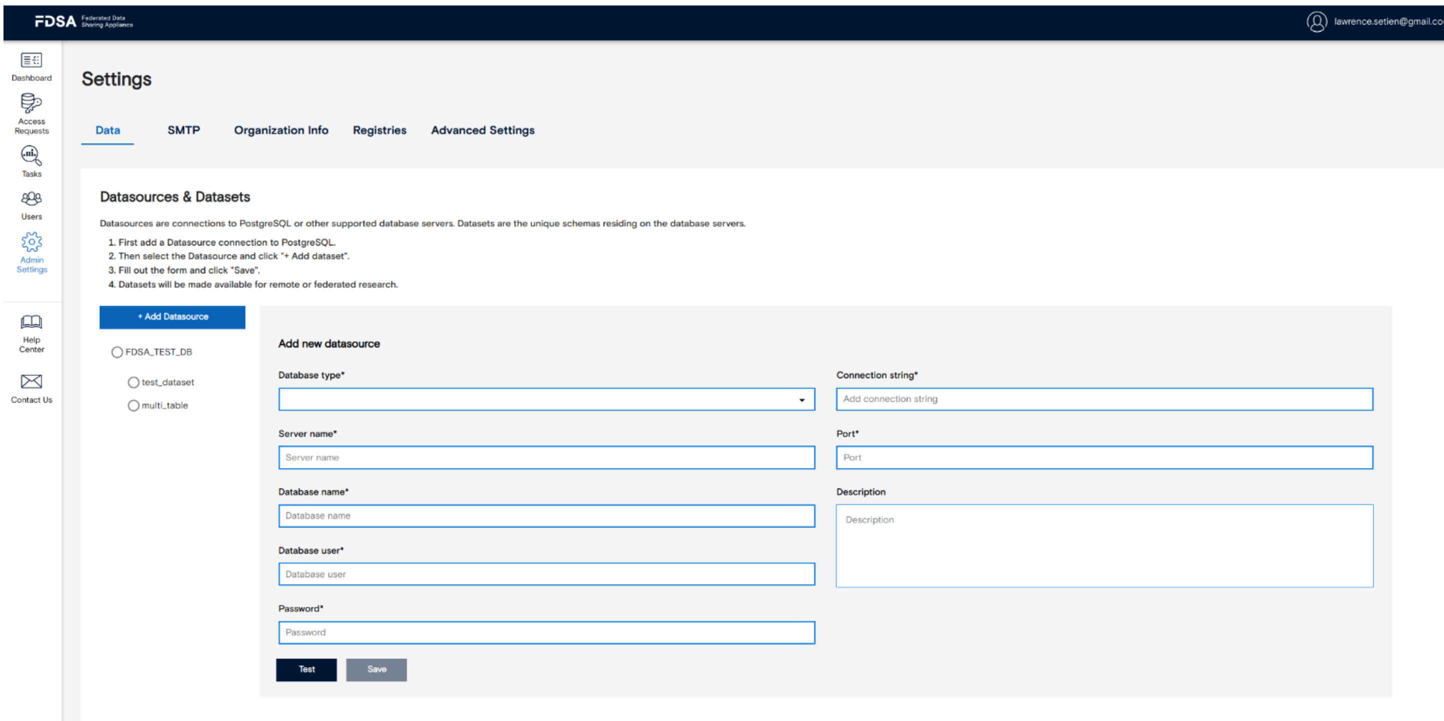


Note: The user will receive an email with the temporary credentials; after logging in, they must set up the MFA and update the password.

Under “Actions” you can change the role, reset the MFA, and disable and/or delete the user.



8. The Admin Settings tab

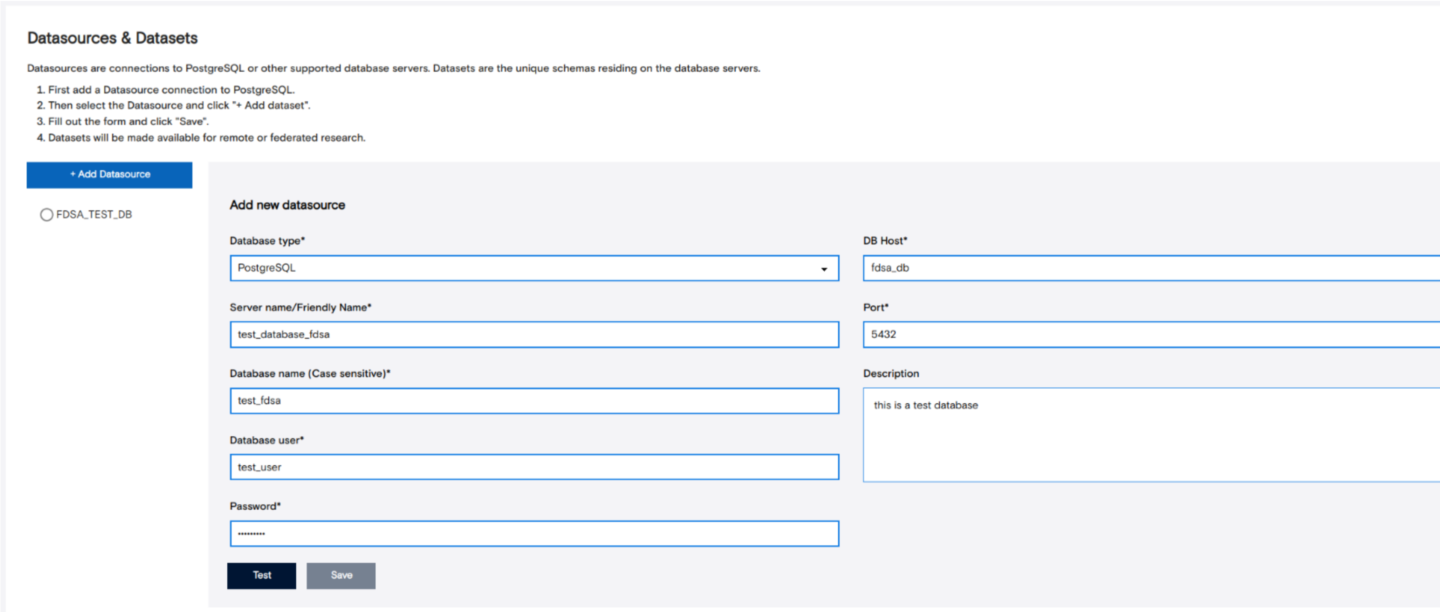


On the **Settings** section you can:

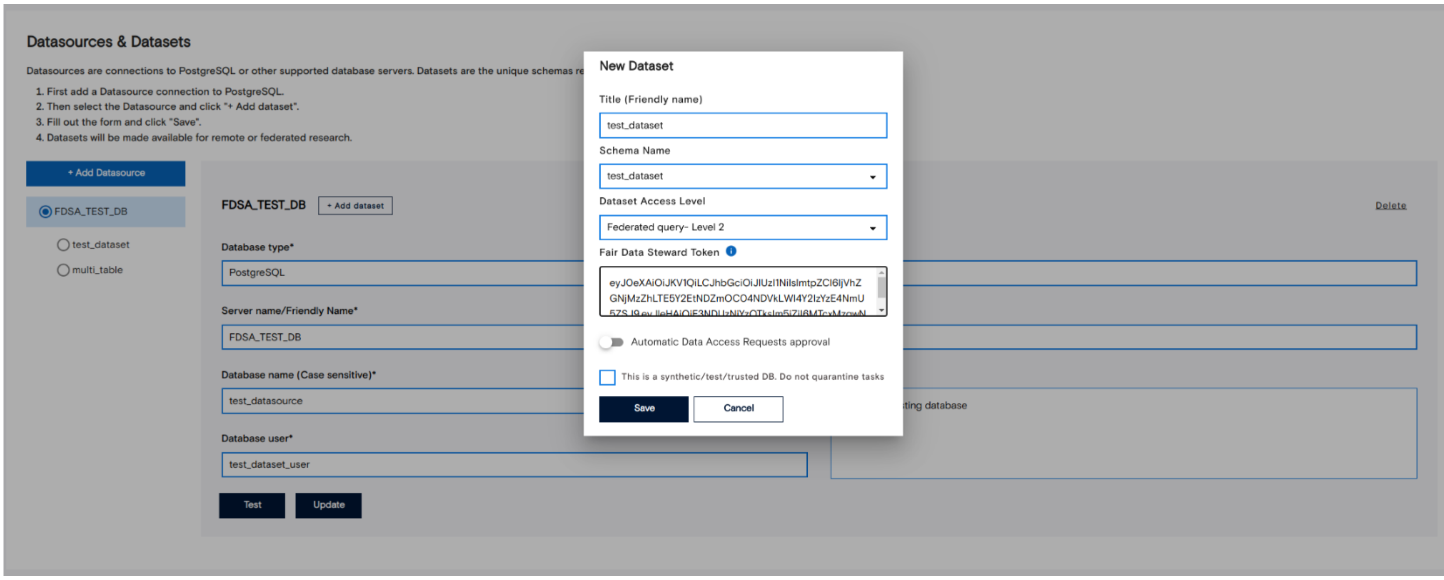
1. Manage Datasource connections and Datasets
2. Manage the SMTP configuration
3. Update the FDSA organization information
4. Add or delete model registries
5. Add a DAR Webhook
6. Update your License
7. Manage token lifetime
8. Whitelist specific IPs to the different part of FDSA

8.1 The Data Tab

- FDSA Comes by default with a test data source already added (FDSA_TEST_DB).
- Read the instructions on how to create a Datasource DB before adding it in FDSA.
- Add the new Datasource in FDSA.



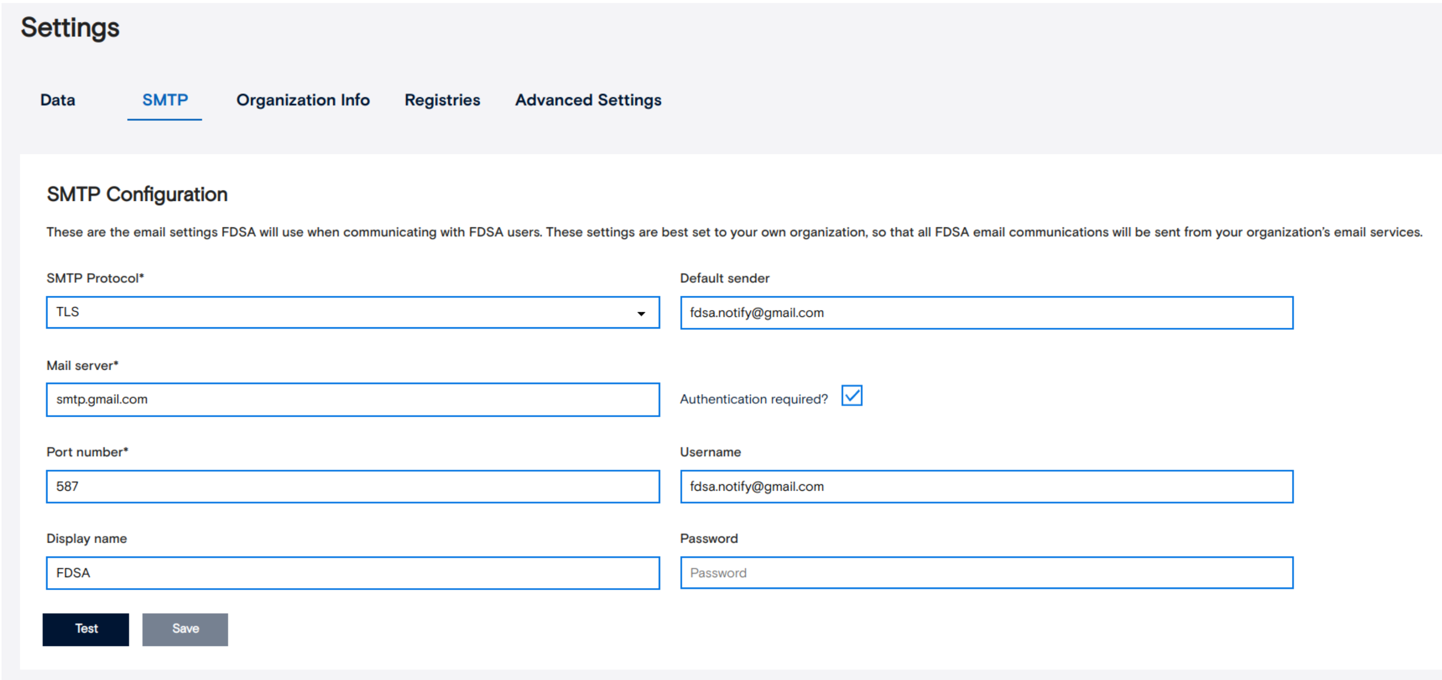
- Select the added Datasource
- Click on “+ Add dataset”
- Read these instructions to understand how to generate the Fair Data Steward Token
- Complete the form and click on "Save”



Note: On this window you can also update and delete Datasources and Datasets.

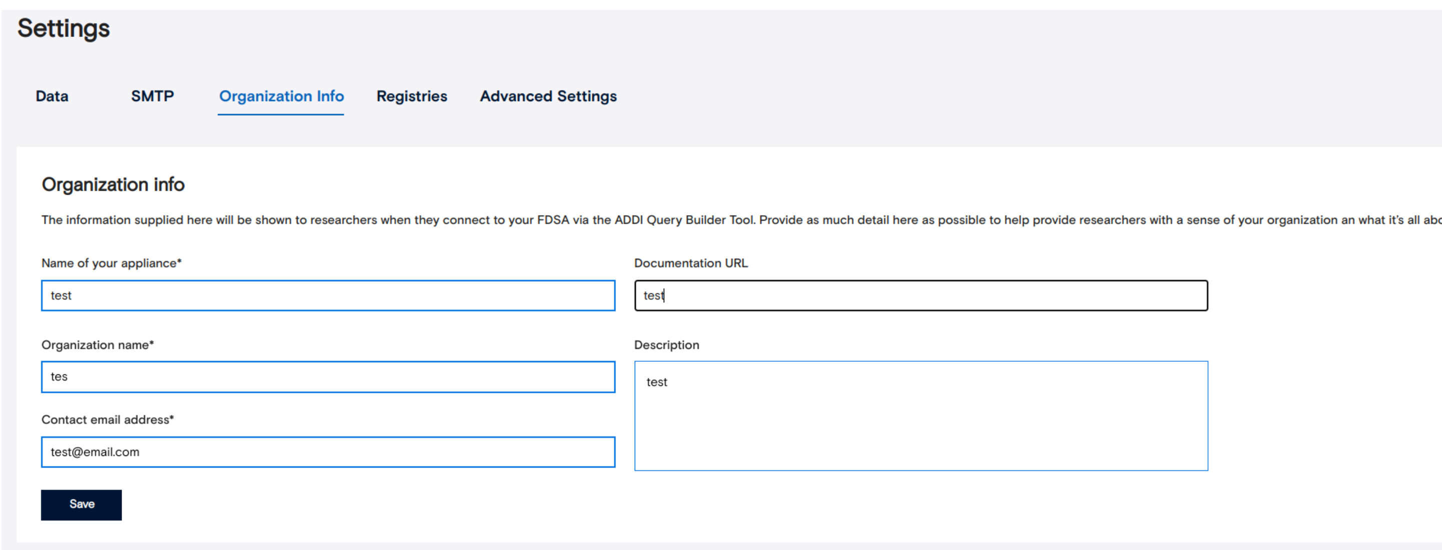
8.2 The SMTP Tab

On this view you can test and update the SMTP configuration.



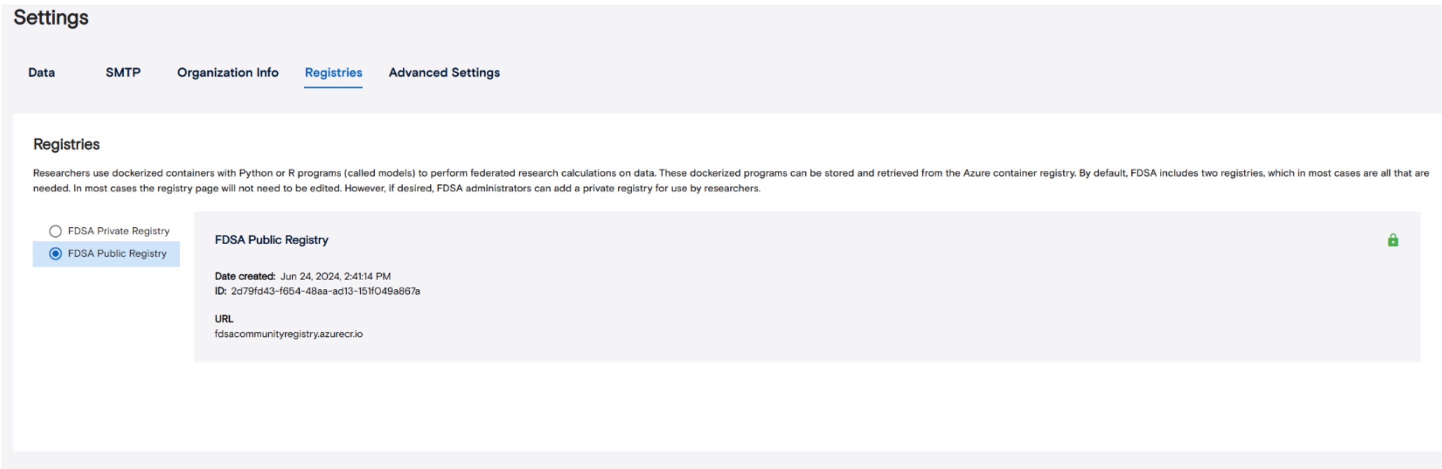
8.3 The Organization Info Tab

On this view you can update the information about your FDSA. This information will be useful to the researcher.



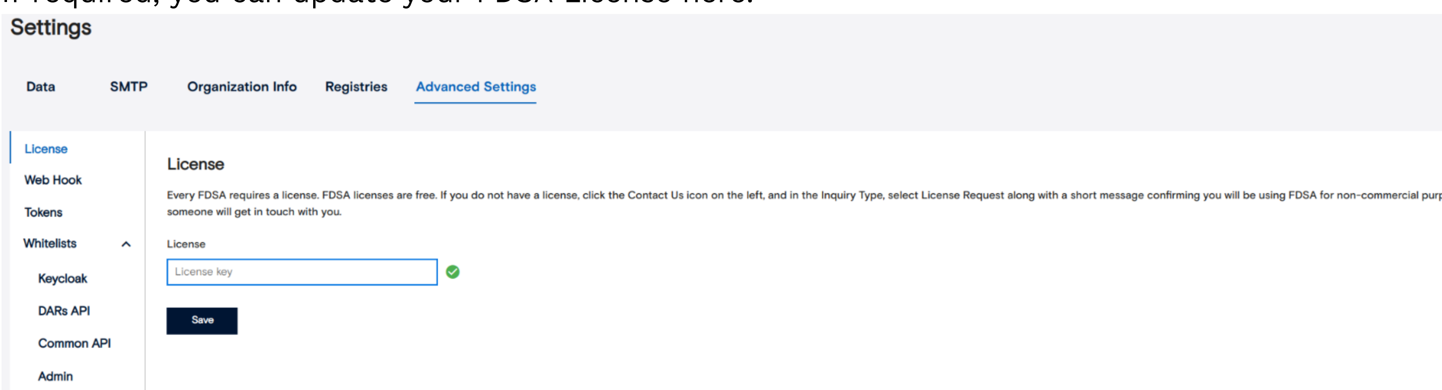
8.4 The Registries Tab

On this tab you can view the existent model registries to which your researchers will have access to.
The FDSA Public Registry and FDSA Private Registry are added by default during the installation.



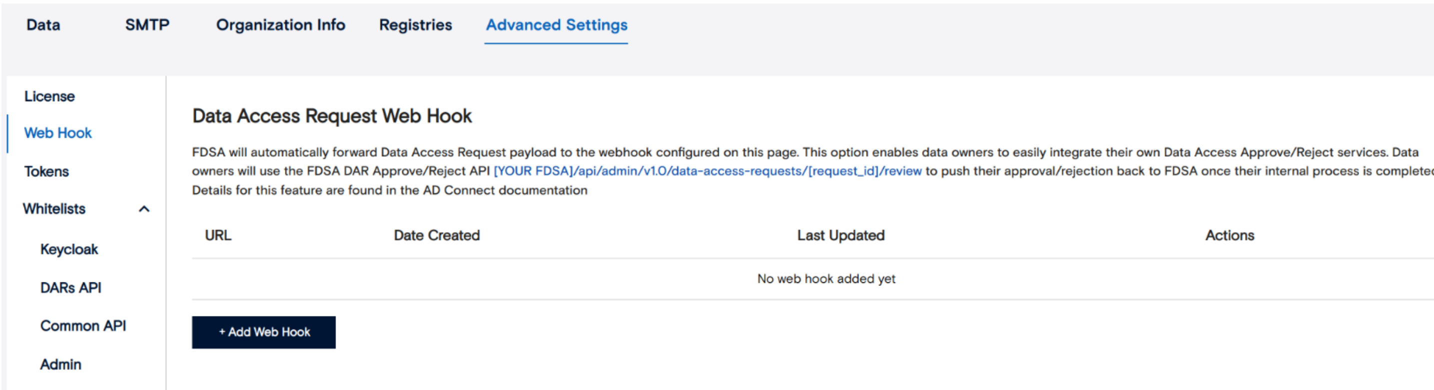
8.5 The Advanced Settings Tab – License

If required, you can update your FDSA License here.



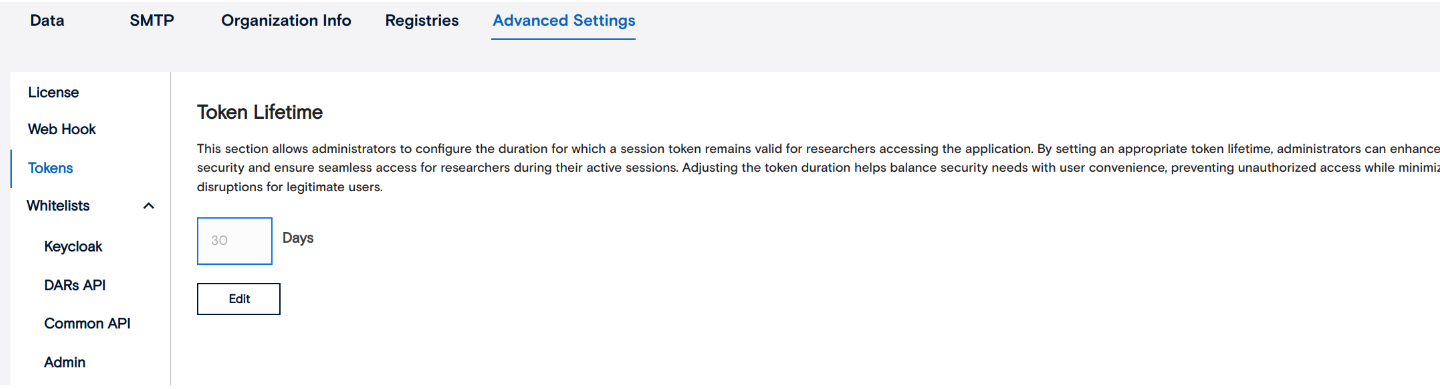
8.6 The Advanced Settings Tab – Web Hook

[Find here more information about the Web Hook feature.]


Data
SMTP
Organization Info
Registries
Advanced Settings
License
Web Hook
Tokens
Whitelists
Keycloak
DARs API
Common API
Admin
Data Access Request Web Hook
FDSA will automatically forward Data Access Request payload to the webhook configured on this page. This option enables data owners to easily integrate their own Data Access Approve/Reject services. Data owners will use the FDSA DAR Approve/Reject API [YOUR FDSA]/api/admin/v1.0/data-access-requests/[request_id]/review to push their approval/rejection back to FDSA once their internal process is completed. Details for this feature are found in the AD Connect documentation
URL
Date Created
Last Updated
Actions
No web hook added yet
+ Add Web Hook

8.7 The Advanced Settings Tab – Tokens

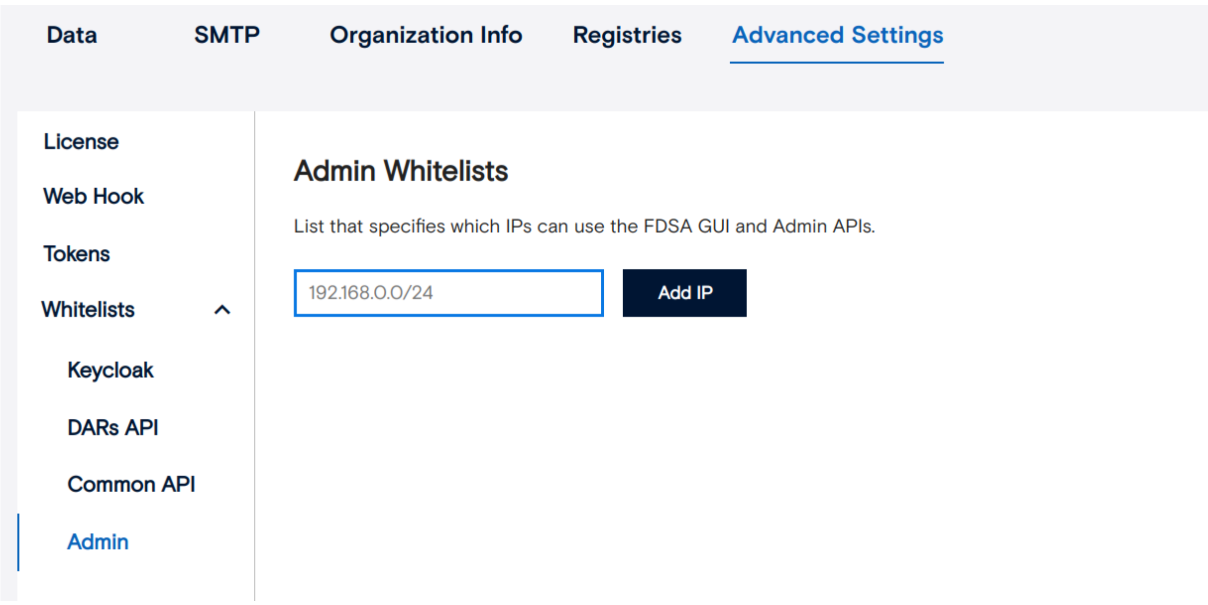
This section allows administrators to configure the duration for which a session token remains valid for researchers accessing the application.



8.8 The Advanced Settings Tab – Whitelists

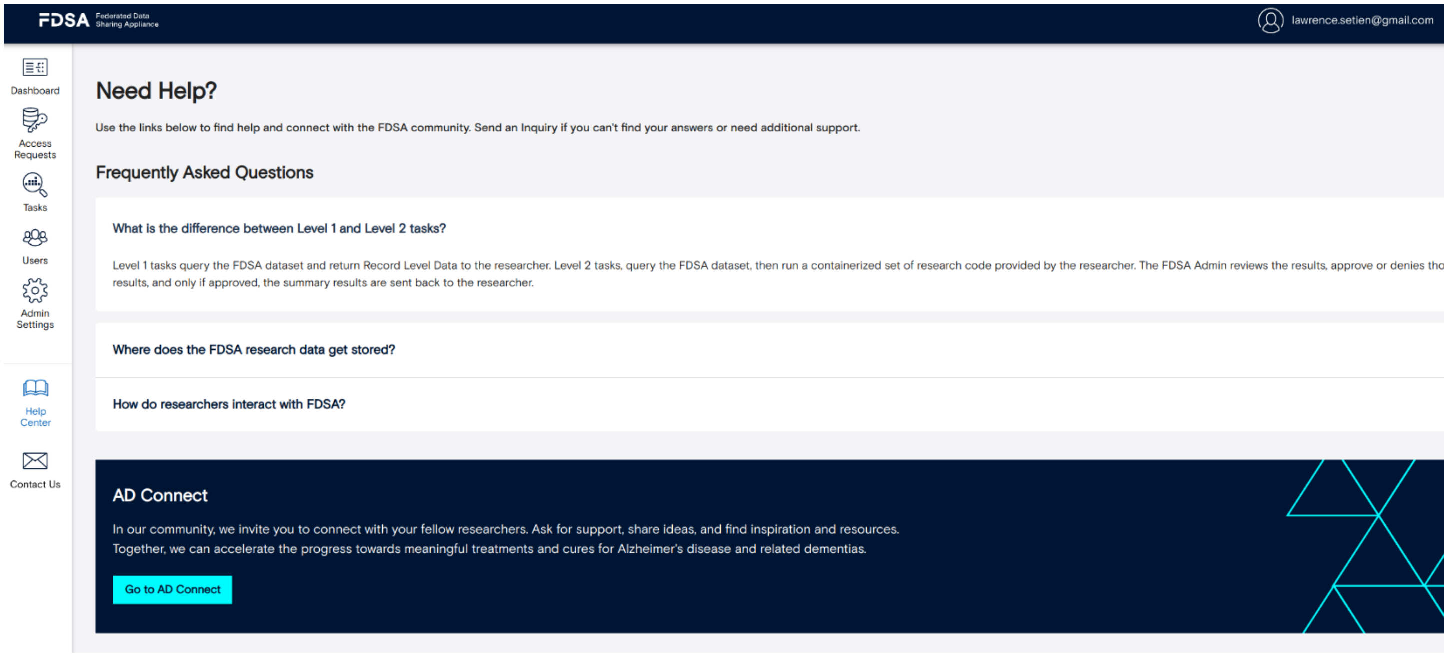
This section allows admins to manage access to the different components of FDSA. By default, all IPs are whitelisted, but once an IP is added, only that IP will be able to use that FDSA component.

Please be aware that wrong IPs may block access to the appliance.



9. Help Center

You can find more information about FDSA in the Help Center section.



10. Contact Us

If you face any problem with your FDSA, please email us using the Contact Us section.