



Module 13

Permission System



CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

mnch
museonacionaldecienciasnaturales



Terminology



Policies

- **Policies** are individual permissions to perform a particular action.
- **Institutional Policies** can be applied directly to a user and impact all collections they have access to.

Role Permission Policies

Querybuilder All Execute Export Csv Export Kml Create Recordset

Table All tables Read Create Update Delete

(Some policies that apply only at the institution-level are not present here at the collection-level.)

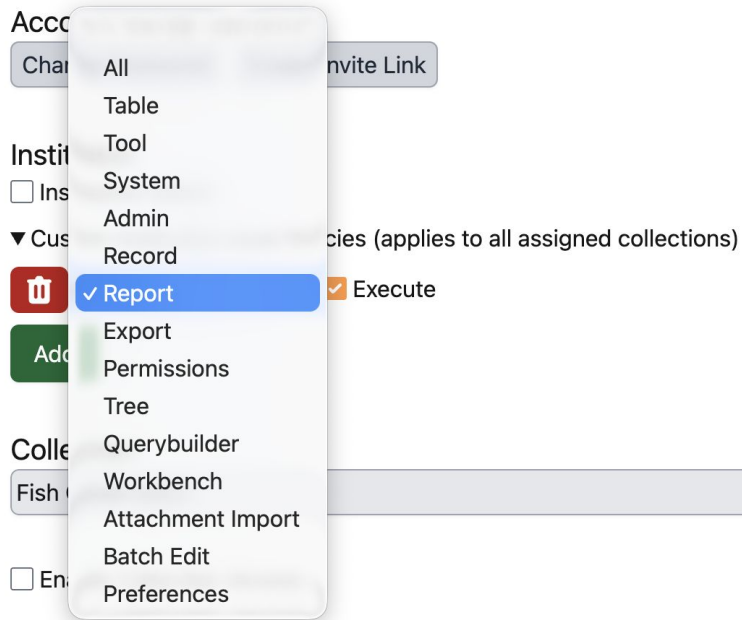
Add

Table All tables Read Create Update Delete

All tables
Accession
Accession Agent
Accession Authorization
Accession Citations
Address
Address Of Record
Agent
Agent Geography
Agent Specialty
Agent Variant
Appraisal
Author
Borrow
Borrow Agent
Borrow Material
Borrow Return Material
Collecting Event
Collecting Event Attribute

Policy Permission Categories

There are a number of categories of policies that can be applied to a user or role.



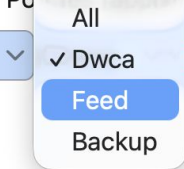
Institution

☐ Institution Admin

▼ Custom Institution-level Policies (applies to all assigned collections)



Export



☒ Execute

Add

Some *even have subcategories*,
and some are restricted to the
institution level.

Policy Permission Categories

- **All** – All permissions
- **Table** – Access to data tables
- **Tool** – Access to Schema Config, Query Builder, Record Sets, App Resources, Pick Lists, and Audit Log
- **System** – Access to collection
- **Admin** – Access to editing passwords, agents, Sp6 permissions, SSO options, *institution-wide only*
- **Record** – Permission to update or delete records when merging.
- **Report** – Permission to run a report/label
- **Export** – Permission to create a DwCA, update the RSS feed
- **Permissions** – Edit permissions for other users
- **Tree** – Access to tree tools (merge, move, synonymize, repair, bulk move) per tree
- **QueryBuilder** – Access to running and exporting queries
- **Workbench** – Access to WorkBench tools (upload, delete, validate, rollback, transfer)
- **Attachment Import** – Access to Bulk Attachment Importer
- **Batch Edit** – Access to Batch Edit tools (commit, delete, validate, rollback, delete dependents, edit multiple tables)
- **Preferences** – Shared statistics

Roles

- **Roles** are groups of **policies**.
- Controls access to specific tables, forms, and tools.
 - Roles are created *once per collection* and can be assigned to multiple users.

Add Role

From library:

Assign Roles
Collection Admin
Create Data Sets
Edit Forms and Global Preferences
Edit Pick lists
Edit Taxon Tree
Export Data
Full Access - Legacy
Full Data Access
Full WorkBench access
Inspect Audit Log
Manage Interactions
Print Reports
Read Only - Legacy
Read-Only Access
Run Queries
Security Admin

Role: Full Access

← KU Fish Observation Collection

Name

Full Access

Description

User Accounts

Add

Role Permission Policies



	Table	All tables	☒ Read ☐ Create ☐ Update ☐ Delete
	Table	Accession	☒ Read ☒ Create ☒ Update ☒ Delete
	Table	Accession Agent	☒ Read ☒ Create ☒ Update ☒ Delete
	Table	Accession Attachment	☒ Read ☒ Create ☒ Update ☒ Delete
	Table	Accession Authorization	☒ Read ☒ Create ☒ Update ☒ Delete
	Table	Accession Citations	☒ Read ☒ Create ☒ Update ☒ Delete
	Table	Address	☒ Read ☒ Create ☒ Update ☒ Delete

Remove

Close

Export

Save

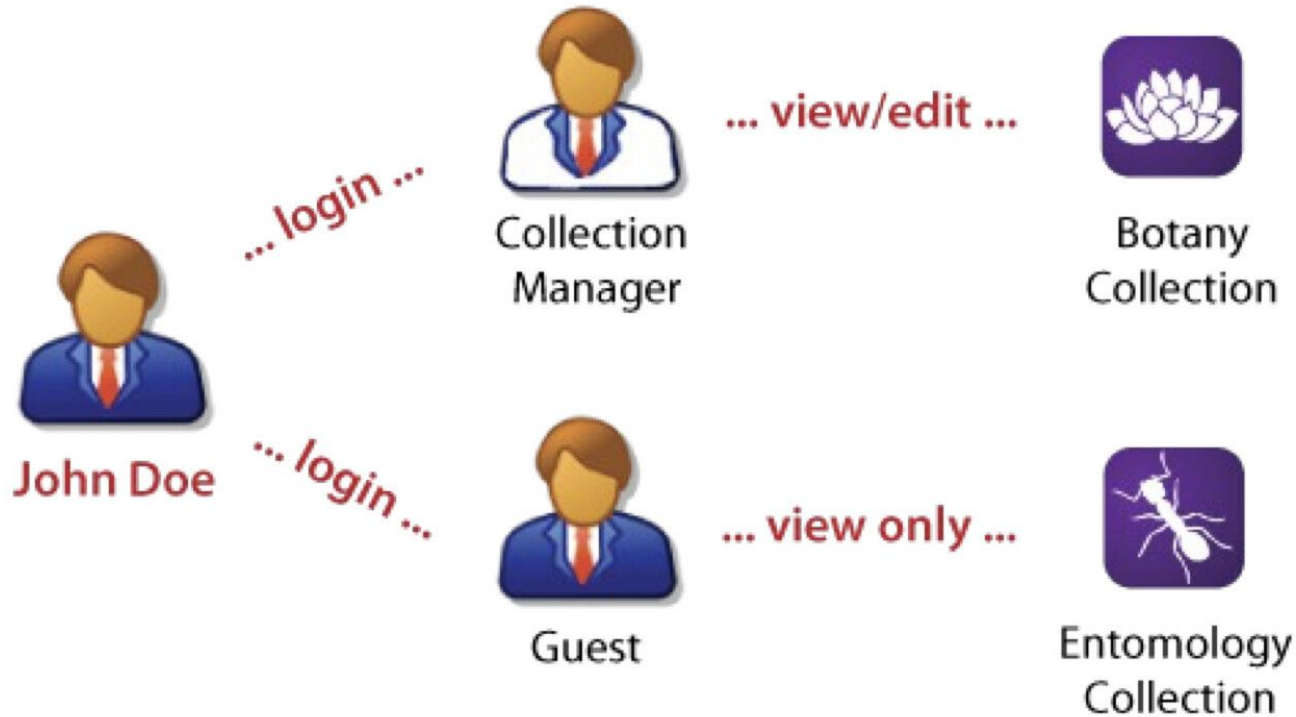


Security and Accounts



Security & Accounts

- The Security and Accounts system in Specify is a comprehensive **Role-Based Access Control (RBAC)** framework.
 - Allows you to align software permissions with your real-world workflows, accommodating everyone from Collection Managers with full access to visiting researchers or students with limited views.



One user can have different permissions **per collection**.

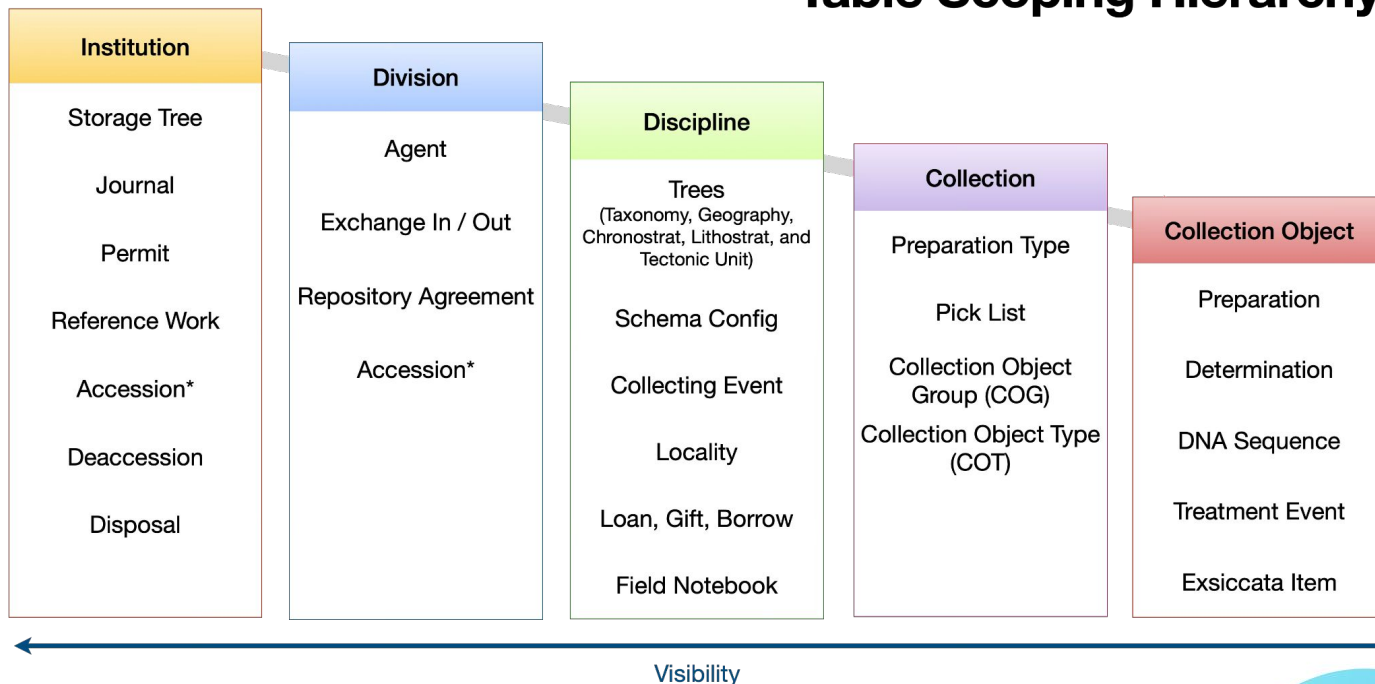
Who Can See My Data?

- 
- When a user logs in to Specify 7, they select a single 'Collection' to work in. This sets the "context" or "scope" for their session.
 - A user's ability to see or interact with any data is determined by the permissions granted to their **Role** for that specific collection, plus any custom **Policies**.
- 

Permissions are impacted by institutional scoping

**Accession can be either at the Institution or Division level*

Table Scoping Hierarchy



Specify Table Scoping Hierarchy. <https://discourse.specifysoftware.org/t/specify-institutional-scopings/1046>

How are permissions applied?

- 
- Security in Specify 7 is **additive**. Users start with zero access.
 - Assigning a **Role** or **Policy** adds permissions to their account. There is no “deny” setting—to restrict access to a function or table, simply ensure the user is not assigned a Role or Policy that grants it.
- 

Record access is handled at the **table level**.

- A policy can be made allowing access to any data in the 'Locality' table, but you **cannot** use it to hide specific 'Locality' records while showing others.
- You can add a custom "flag" field so records can be hidden when exporting.

Loc

Locality: USA, Kansas, Wyandotte: Kansas River, 39.065700531, -94.7512969971

Locality Name

Kansas River

Geography

USA, Kansas, Wyandotte

+

Point

Latitude

Longitude

Parsed

Coordinates

39.0657 N

94.7513 W

39.0657° N, 94.7513° W

Lat/Long Method

Water Type

Freshwater

Remarks

Geo Coord Details

+

-

No Data.

Locality Details

+

-

Section

28

Township

11S

Range

24E

Section Part

Island

Island Group

Water Body

Drainage

Plugins

GeOLocate

Plugin N/A

Show Map

Attachments

Loc

0

Delete

20

Clone

Add

Save

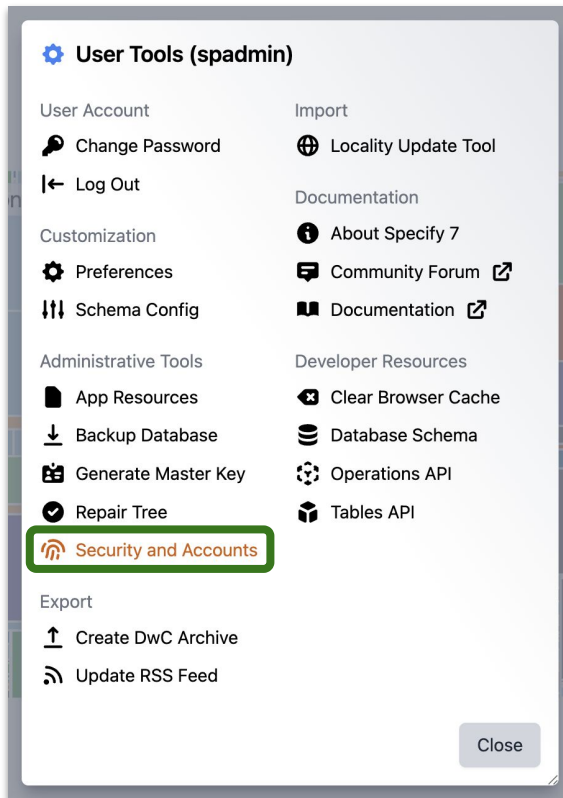


Customizing Permissions



How do I customize permissions?

Click on your **username**, and then click on **Security and Accounts** in the User Tools menu.





Left Side: List of collections within the institution

Right Side: Collection view for all roles and accounts with **access** to that collection

Security and Accounts

Institution

University of Kansas Biodiversity Institute

Collections

Fish Observation

Fish Teaching

Fish Tissue

Fish Voucher

Geology

Herbarium

Insects

Invert Paleo

Collection: Fish Tissue

Collection User Roles

Collection Admin

Read Only - Legacy

Add Role

Import

Export

User Accounts Assigned to this Collection

abentley (Collection Admin)

guest (Read Only - Legacy)

rmartin (Collection Admin)

spadmin (Collection Admin)

Add User

Institution

University of Kansas Biodiversity Institute

Collection(s)

KU Fish Observation Collection

KU Fish Teaching Collection

KU Fish Tissue Collection

KU Fish Voucher Collection

This is your institution

Here are all of the collections contained in the database

Institution

Select the **Institution** name and see:

- Institution Library of Role Templates
- User Accounts Defined in this Institution

Security and Accounts

Institution

University of Kansas Biodiversity Institute

Collections

Fish Observation

Fish Teaching

Fish Tissue

Fish Voucher

Geology

Herbarium

Insects

Invert Paleo

Institution: University of Kansas Biodiversity Institute ✎

Institution Library of Role Templates

Assign Roles

Bulk Attachment Import

Bulk Attachment Import

Collection Admin

Create Data Sets

Edit Forms and Global Preferences

Edit Pick lists

Edit Taxon Tree

Export Data

Full Access - Legacy

Full Data Access

Full WorkBench access

Inspect Audit Log

Manage Interactions

Print Reports

Read Only - Legacy

Read-Only Access

Run Queries

Security Admin

Create

Import

Export

User Accounts Defined in this Institution

abentley (Specify 7 Admin) (Specify 6 Admin)

guest

rmartin

spadmin (Specify 7 Admin) (Specify 6 Admin)

specifyworkshop (Specify 7 Admin)

Create

Institution Library of Role Templates

At the **institution** level:

- Define a role that can be used as a template for *any collection*
- Build on one of our defaults
- Turn a custom role into a template

The screenshot displays the 'Add Role' dialog box, which is used to create or modify roles in a system. The dialog is divided into two main sections: 'From library:' and 'From an existing role:'. The 'From library:' section lists various default roles, including 'Assign Roles', 'Bulk Attachment Import', 'Collection Admin', 'Create Data Sets', 'Edit Forms and Global Preferences', 'Edit Pick lists', 'Edit Taxon Tree', 'Export Data', 'Full Access - Legacy', 'Full Data Access', 'Full WorkBench access', 'Inspect Audit Log', 'Manage Interactions', 'Print Reports', 'Read Only - Legacy', 'Read-Only Access', 'Run Queries', and 'Security Admin'. The 'From an existing role:' section lists roles from existing collections, including 'Fish Observation: Collection Admin', 'Fish Teaching: Collection Admin', 'Fish Tissue: Collection Admin', and 'Read Only - Legacy'. The 'Add Role' button is highlighted in blue. The right side of the dialog shows the 'Role: Export Data' configuration. It includes a 'Name' field with the value 'Export Data', a 'Description' field with the text 'Gives ability to export DwC Archive from any table.', and a 'Role Permission Policies' section. The 'Role Permission Policies' section shows a table with columns for 'Policy', 'Table', and 'Action'. The 'Policy' column has a dropdown menu with 'Export' selected. The 'Table' column has a dropdown menu with 'All tables' selected. The 'Action' column has checkboxes for 'Read', 'Create', 'Update', and 'Delete'. The 'Read' checkbox is checked. Below the table, there is a note: '(Some policies that apply only at the institution-level are not present here at the collection-level.)'. The 'Add' button is highlighted in green. The bottom of the dialog shows a 'Collection: Geology' dropdown and a 'Collection User Roles' section with buttons for 'Add Role', 'Import', and 'Export'. The 'User Accounts Assigned to this Role' section shows a list of users, including 'spadmin (Collection Admin)', and an 'Add User' button.

Add Role

From library:

- Assign Roles
- Bulk Attachment Import
- Bulk Attachment Import
- Collection Admin
- Create Data Sets
- Edit Forms and Global Preferences
- Edit Pick lists
- Edit Taxon Tree
- Export Data
- Full Access - Legacy
- Full Data Access
- Full WorkBench access
- Inspect Audit Log
- Manage Interactions
- Print Reports
- Read Only - Legacy
- Read-Only Access
- Run Queries
- Security Admin

From an existing role:

- Fish Observation: Collection Admin
- Fish Teaching: Collection Admin
- Fish Tissue: Collection Admin
- Read Only - Legacy

Add Role

Role: Export Data

← University of Kansas Biodiversity Institute

Name
Export Data

Description
Gives ability to export DwC Archive from any table.

Role Permission Policies

	Export	Dwca	☒ Execute
	Table	All tables	☒ Read ☐ Create ☐ Update ☐ Delete

(Some policies that apply only at the institution-level are not present here at the collection-level.)

Add

Collection: Geology

Add Role

Collection User Roles

- Collection Admin
- Read Only - Legacy

Add Role **Import** **Export**

User Accounts Assigned to this Role

- spadmin (Collection Admin)

Add User

From library:

- Assign Roles
- Bulk Attachment Import
- Bulk Attachment Import
- Collection Admin
- Create Data Sets
- Edit Forms and Global Preferences
- Edit Pick lists
- Edit Taxon Tree
- Export Data
- Full Access - Legacy
- Full Data Access
- Full WorkBench access

User Accounts Defined in this Institution

This shows a complete list of all users in the **database**.

- You can click on a username to see if a user has **Collection Access**, assigned roles, or institution-level policies.
- Create new users with **Create**.

User Accounts Defined in this Institution

abentley (Specify 7 Admin) (Specify 6 Admin)
guest
rmartin
spadmin (Specify 7 Admin) (Specify 6 Admin)
specifyworkshop (Specify 7 Admin)

Create

Specify User: abentley

Name

abentley

Account Setup Options

Change Password

Create Invite Link

Institution

☐ Institution Admin

▼ Custom Institution-level Policies (applies to all assigned collections)

Add

Collection

Fish Observation

☒ Enable Collection Access

Agent

Bentley, Andrew C

Assigned User Roles

☒ Collection Admin

☐ Read Only - Legacy

Custom Collection-level Policies (applies to this collection only)



System

Sp7

Collection

☒ Access

Single Sign On (SSO)

- If your institution supports **Single Sign On (SSO)** via OpenID endpoints, you can use your institution's identity provider to log into Specify.
 - When creating or editing a user, click **Create Invite Link** and share the URL to start.
- Users can choose between **traditional** and **SSO** login

Account Setup Options

Set Password

Create Invite Link

Actions:

Set Password Create Invite Link ☐ Institution Admin

User Invite Link

Send the following link to joe to allow them to log in for the first time.

`http://a11y.test.specifysystems.org/accounts/use`

Copy To Clipboard

Close



English (en-us)

English (en-us)

Phantauth

Sign In With Specify Account



English (en-us)

Hello, HappyTestUser!

You've been invited to associate an external login to your Specify user account. This will enable you to log in to Specify with your chosen provider going forward.

Phantauth

Creating a New User

- Once you click the **Create** button from the list of users in the database, you need to fill out:
 - **Name** (username)
 - Click **Set Password** and enter a new password
- For each *Collection*, assign an **Agent** and the appropriate roles.
- Optionally, assign any Institution-level policies if needed or use “*Create Invite Link*” if you are using SSO.

Specify User: abentley

Name
abentley

Account Setup Options
[Change Password](#) [Create Invite Link](#)

Institution
☐ Institution Admin
▼ Custom Institution-level Policies (applies to all assigned collections)
[Add](#)

Collection
Fish Observation ▼

☒ Enable Collection Access

Agent
Bentley, Andrew C ✎ + 🔍

Assigned User Roles
☒ Collection Admin ✎
☐ Read Only - Legacy ✎

Custom Collection-level Policies (applies to this collection only) [↻](#)
 System ▼ Sp7 ▼ Collection ▼ ☒ Access

Collection

Select a **Collection** name and see:

- Collection User Roles
- User Accounts Assigned to this Collection

Security and Accounts

Institution

University of Kansas Biodiversity Institute

Collections

Fish Observation

Fish Teaching

Fish Tissue

Fish Voucher

Geology

Herbarium

Insects

Invert Paleo

Collection: Fish Voucher

Collection User Roles

Assign Roles

Collection Admin

Export Data

Read Only - Legacy

Add Role

Import

Export

User Accounts Assigned to this Collection

abentley (Collection Admin)

guest (Read Only - Legacy)

rmartin (Collection Admin)

spadmin (Collection Admin)

Add User

Collection User Roles

Changes to roles in a Collection do not impact others in the database.

- **Add Role** opens a dialog to select a template role or a role from another collection.
- **Import** and **Export** allow you to export all of the roles as a JSON file and import them in any other collection.
 - If two roles have a matching name, the imported one will overwrite the existing one.

Collection User Roles

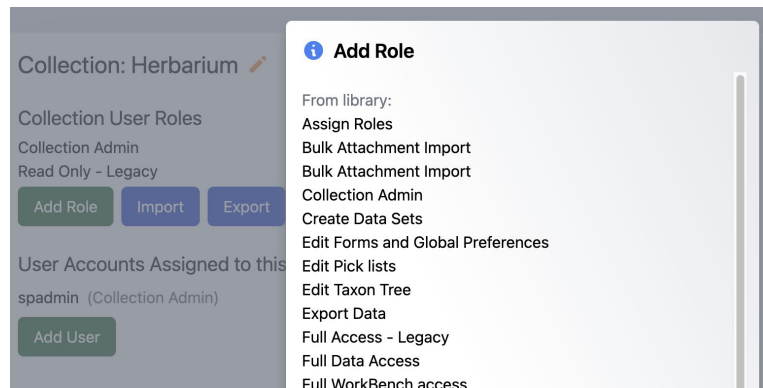
Collection Admin

Read Only - Legacy

Add Role

Import

Export



User Accounts Assigned to this Collection

This shows a complete list of all users in the **database**.

- All users listed here have **Collection Access**.
- This list *does not show* Institution Admin users, who *may* have access.
- Create new users with **Add User**.

User Accounts Assigned to this Collection

abentley (Collection Admin)

guest (Read Only - Legacy)

rmartin (Collection Admin)

spadmin (Collection Admin)

Add User

Specify User: abentley

Name

abentley

Account Setup Options

Change Password

Create Invite Link

Institution

☐ Institution Admin

▼ Custom Institution-level Policies (applies to all assigned collections)

Add

Collection

Fish Observation

☒ Enable Collection Access

Agent

Bentley, Andrew C

Assigned User Roles

☒ Collection Admin

☐ Read Only - Legacy

Custom Collection-level Policies (applies to this collection only)



System

Sp7

Collection

☒ Access

(Some policies that apply only at the institution-level are not present here at the collection-level.)

Add

▼ User's Permission Profile (read-only)

Note: preview may be out of date. Save changes to update the preview

User's Permission Profile

- **Read-only** preview of permissions assigned to a particular user
 - Click on 'Read', 'Create', 'Update', or 'Delete' to see which **role or policy** granted access
- See tool acces on the right side

▼ User's Permission Profile (read-only)

Note: preview may be out of date. Save changes to update the preview

Read Create Update Delete Table

☒ ☐ ☐ ☐ ☒ Accession

Collection User Roles	Action	Resource
Read Only - Legacy	Read	All tables

User Permission Policies Collection Action Resource

None

☒	☐	☐	☐	☒ Agt Accession Agent
☒	☐	☐	☐	☒ AcA Accession Authorization
☒	☐	☐	☐	☒ Cit Accession Citations
☒	☐	☐	☐	☒ Adr Address
☒	☐	☐	☐	☒ Adr Address Of Record
☒	☐	☐	☐	☒ Agt Agent
☒	☐	☐	☐	☒ AG Agent Geography
☒	☐	☐	☐	☒ Agt Agent Identifier
☒	☐	☐	☐	☒ AS Agent Specialty
☒	☐	☐	☐	☒ App Appraisal
☒	☐	☐	☐	☒ Aut Author
☒	☐	☐	☐	☒ Bor Borrow

• Admin

• User

- Agents
 - ▶ ☐ Update
- Invite Link
 - ▶ ☐ Create
- Oic Providers
 - ▶ ☐ Read
- Password
 - ▶ ☐ Update
- Sp6
 - Collection Access
 - ▶ ☐ Read
 - ▶ ☐ Update
 - Is Admin
 - ▶ ☐ Update

• Attachment Import

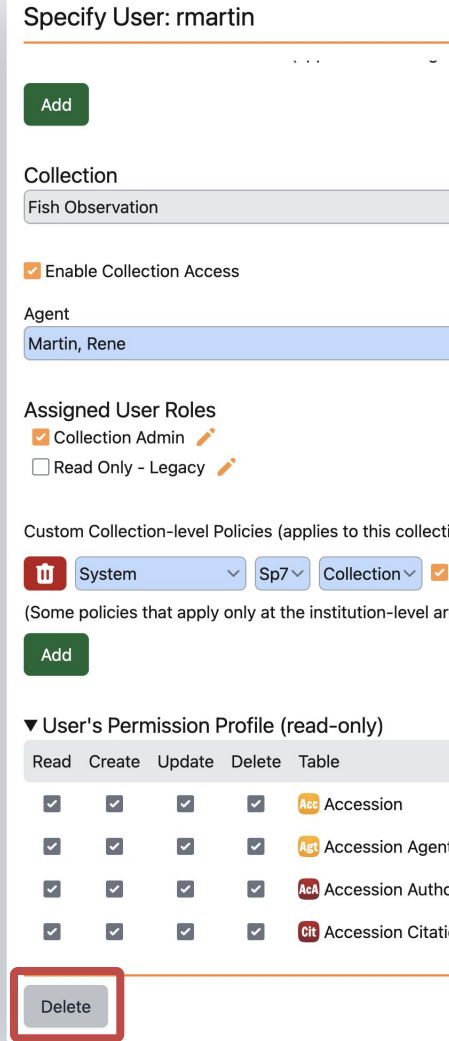
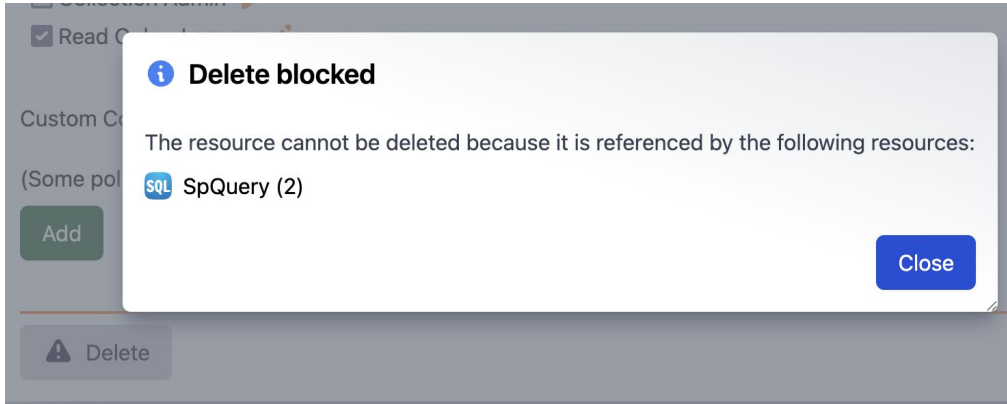
- Dataset
 - ▶ ☐ Create
 - ▶ ☐ Update
 - ▶ ☐ Delete
 - ▶ ☐ Upload
 - ▶ ☐ Rollback

• Batch Edit

- Dataset
 - ▶ ☐ Create
 - ▶ ☐ Update
 - ▶ ☐ Delete
 - ▶ ☐ Commit
 - ▶ ☐ Rollback

Deleting a User

- You can **delete** a user by viewing their profile and clicking **Delete**.
 - If that user has linked resources, those can block deletion (e.g., queries, export mappings, app resources).



Security and Accounts

Documentation • Configuration & Installation Specify-7 , Members-only



Grant Staff

17  Jul 2022

Before proceeding, make sure that you [understand the institutional structure of Specify](#) ⁴ and have the proper permissions to make changes.

Institution	Natural History Museum							
Division	Vertebrate Zoology				Botany			
Discipline	Ichthyology		Herpetology		Non-Vascular Plants		Vascular Plants	
Collection	Wet	Dry	Amphibians	Reptiles	Mosses	Lichens	Herbarium	Pollen

Please read [Introducing the new Role-Based Access System in Specify 7](#) before configuring your institution's policies and user accounts.

To access the **Security and Accounts** panel, you must first navigate to the [User Tools](#) menu. You access this menu by clicking on your username in the navigation menu.

 Search

 Notifications: 0

 sp7demofish

 KUFishvoucher

 Collapse

Now click on  **Security and Accounts**.

 **User Tools** (spfshadmin)

User Account

 Change Password

 Log Out

Export

 Create DwC Archive

 Update RSS Feed

Customization

Documentation

- User Roles
- Role Permission Policies (Policy Builder)

All

Table

Tool

System

Report

Export

Permissions

Tree

Querybuilder

Workbench

Preferences
- User Permissions
- Institution

Collection(s)
- [Jump to end](#)

Learn More



<https://discourse.specifysoftware.org/t/security-and-accounts/539>

