Account roles in the Data Delivery System

Your account in the Data Delivery System (DDS) can have one of four possible roles: Researcher, Unit Personnel, Unit Admin and Super Admin. The Super Admin role is purely for a few members of the SciLifeLab Data Centre. This document gives a brief description of the differences between the three other roles and when to assign a specific user to them. It also defines the differences in administrative permissions, mainly focused on account management. For a detailed, full description of the roles and their different permissions, please read the Technical Overview[1], Appendix A. User roles.

Who should have which role?

Role	***Who?***	***Additional notes***
Researcher	The data recipients; Users wanting to download the data produced and uploaded by a SciLifeLab unit.	This role includes the sub-role Project Owner, which has additional administrative permissions within certain projects. This sub-role should be a Researcher with access to the project, who should also be allowed to invite new users to that project. This could be the PI, but it is not required. You can set multiple users as Project Owners in a project.
Unit Personnel	The members of the SciLifeLab unit which are responsible for uploading the data.	
Unit Admin	A few selected members of the SciLifeLab unit, who should also have some administrative permissions.	These users could also be the ones uploading the data, but they don't have to be.

Recommendations for yearly review of Unit Admins- and Personnel

In the event that a team member resigns, their DDS account should be deleted immediately. If a team member goes on leave for an extended period of time, their account should be deactivated. Due to the risk of this being potentially missed or forgotten, each unit should review their Unit Admins and Unit Personnel at least once a year.

[1] https://delivery.scilifelab.se/technical

Which administrative permissions do the roles have?

In this section we have included the users permissions when it comes to invitations, activation- and deactivation of accounts, deleting accounts, and revoking- and renewing access to projects.

Invitations

Super Admins can invite any role to the DDS: Unit Admins, Unit Personnel and Researchers. They cannot invite the sub-role Project Owner, since this requires access to the projects; Super Admins do not have access to any of the projects within the DDS.

Unit Admins can invite Unit Admins, Unit Personnel, Researchers (incl. Project Owners). Unit Admins and Unit Personnel will automatically be assigned to the same unit as the inviting Unit Admin – this cannot be changed. Researchers can either be invited to the DDS in general, or to specific projects created by the unit. They can also be set as Project Owners in those projects.

Unit Personnel can invite Unit Personnel and Researchers (incl. Project Owners). Unit Personnel will automatically be assigned to the same unit as the inviting Unit Personnel – this cannot be changed. Researchers can either be invited to the DDS in general, or to specific projects created by the unit. They can also be set as Project Owners in those projects.

Project Owners (sub-role of Researcher) can invite Researchers (incl. Project Owners) to the projects where they are set as Project Owners.

Researchers do not have any invitation permissions.

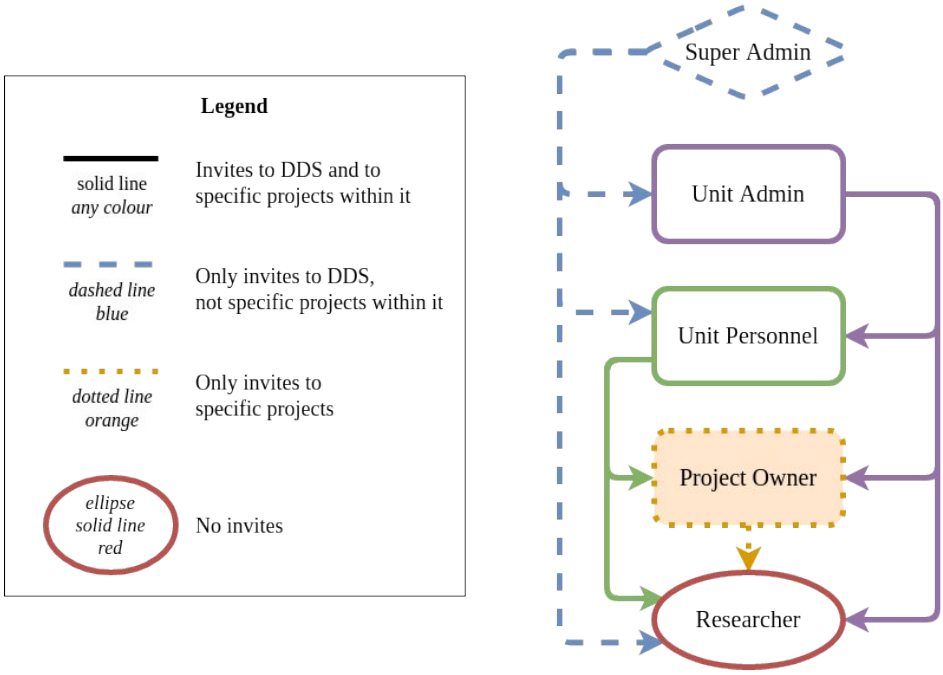

Figure 1. The invitation privileges for each account role.
Project Owners are included here as a sub-role of the role Researcher.

Activating/Deactivating *and* Deleting accounts

Super Admins can activate, deactivate and delete any account.

Unit Admins can activate, deactivate and delete Unit Admins and Unit Personnel within their unit.

Unit Personnel and **Researchers** (incl. Project Owners) do not have any activation, deactivation or deletion permissions.

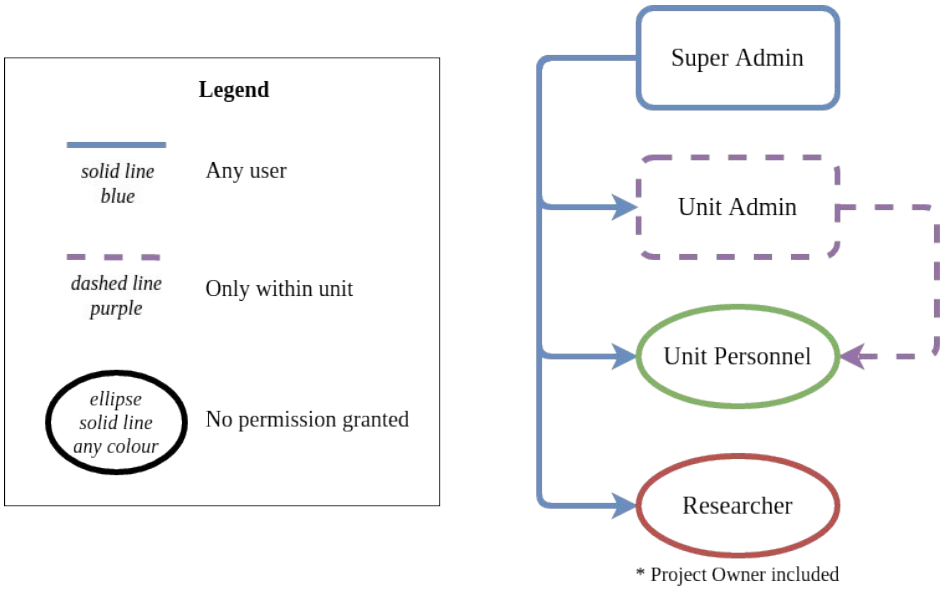

Figure 2. The activation, deactivation and deletion privileges for each account role. Project Owners are included in the Researcher role here.

Revoking project access

Super Admins do not have any permissions related to project access.

Unit Admins *and* **Unit Personnel** can revoke project access for Researchers (incl. Project Owners). They cannot revoke project access for Unit Admins or Unit Personnel.

Researchers (incl. Project Owners) can revoke project access for Researchers with access to the same projects.

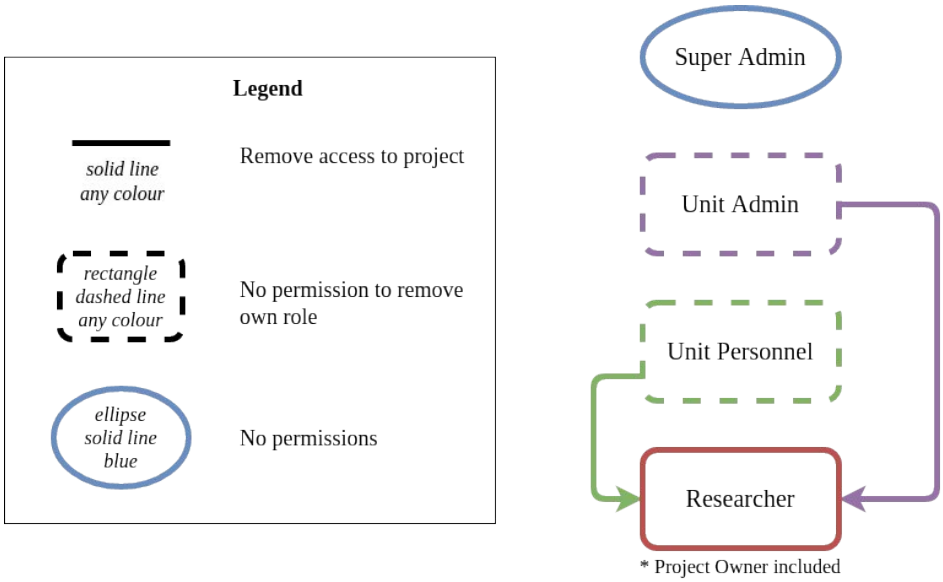

Figure 3. Permissions to revoke project access for users.
The Project Owner sub-role is included in the Researcher role.

Renewing project access

With *renewing* project access we mean that an account has lost access to the data within the project, for example as a result of a password reset.

Super Admins do not have any permissions related to project access.

Unit Admins can renew the project access for Unit Admins, Unit Personnel and Researchers (incl. Project Owners).

Unit Personnel can renew the project access for Unit Personnel and Researchers (incl. Project Owners).

Project Owners (sub-role of Researcher) can renew the project access for Researchers (incl. Project Owners) in the projects where they are Project Owners.

Researchers do not have any permissions regarding renewal of project access.

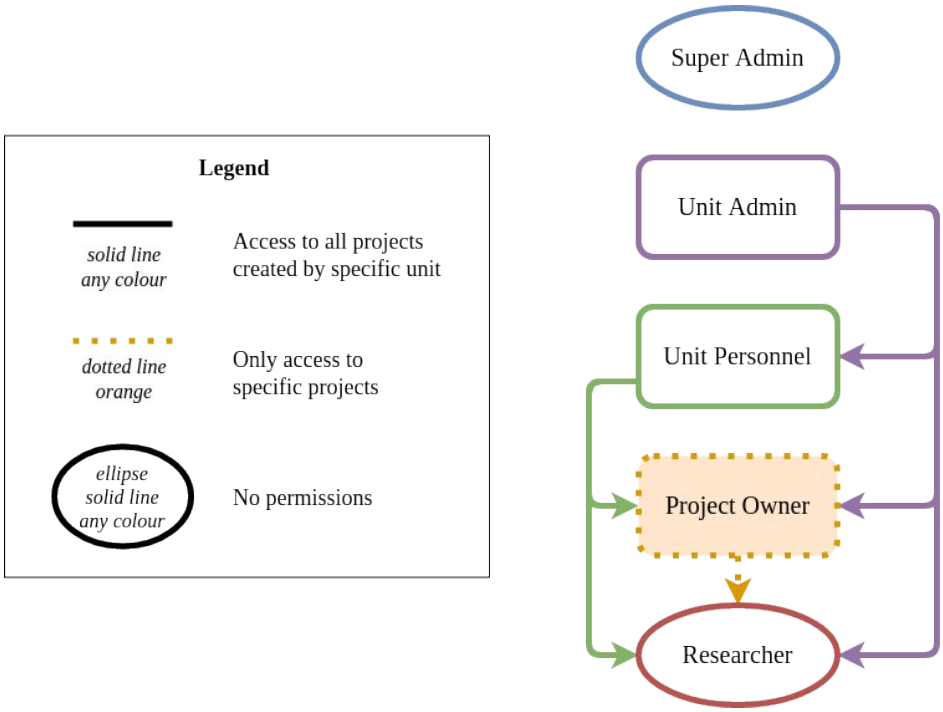

Figure 4. Permissions to renew users project access.
Project Owner is a sub-role of the Researcher.