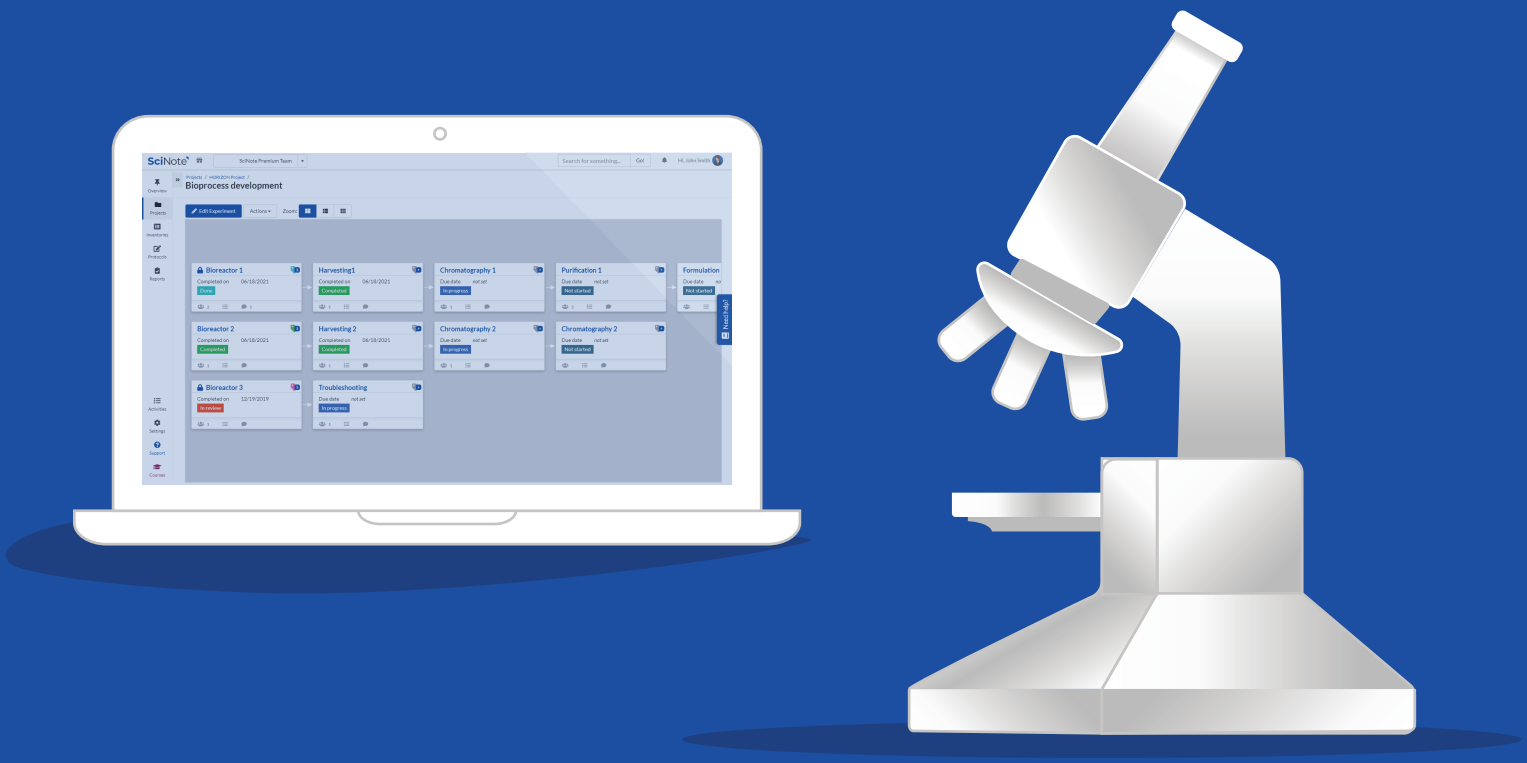
SciNote

FDA 21 CFR Part 11 Compliance

SciNote is proud to be chosen as the solution used at the FDA, one of the leading United States federal executive departments.

Researchers at the FDA are at the forefront of today's scientific progress, responsible for protecting and promoting public health. We are honored to support their work.



Introduction

SciNote Premium plans include a **21 CFR Part 11 add-on** that provides a toolset for compliance with the 21 CFR Part 11 regulations, while still keeping SciNote flexible and easy to use.

The 21 CFR Part 11 add-on includes the following features: electronic signatures, electronic witnessing, audit trails and system log records. According to the FDA guidelines, electronic signatures are considered to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures.

This document provides a short overview of SciNote's 21 CFR Part 11 add-on features and their use.

21 CFR Part 11 permissions

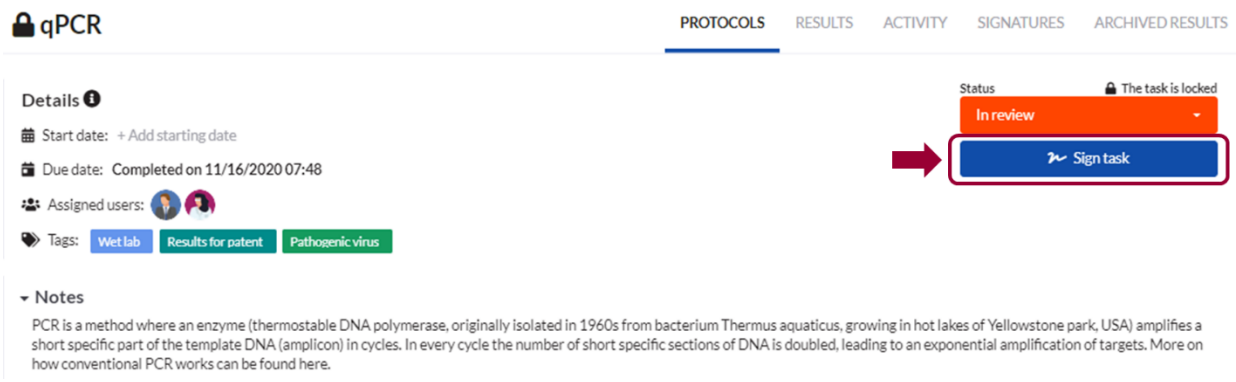
21 CFR Part 11 permissions are accredited to the users with the following Project roles: Owner, User and Technician. This means they have a full authority of signing specific tasks that were completed within projects.

It is possible to co-sign a task or reject a signature, if there are two levels of supervision within an organization. Once signed, the task cannot be co-signed by the same user. Every signee can also revoke his/her own signature and only the Organization administrator has the permission to revoke other peoples' signatures, if necessary.

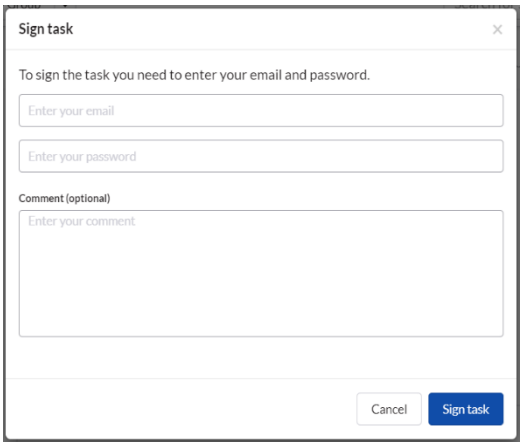
Electronic signatures and witnessing

You are able to sign tasks in SciNote. Tasks are parts of the experiments you are working on, and you can change a status of the task according to the progress of your work.

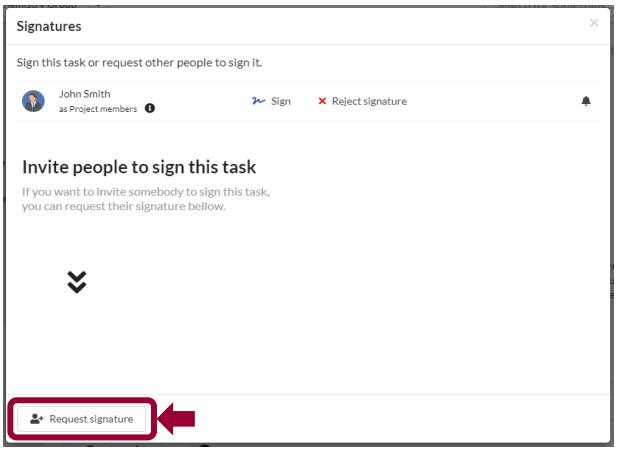
Once you've completed the task you can move it to the *In review* state for review and approval. In the *In review* status the task gets locked for editing and it requires at least one signature, before it can be moved to the final *Done* state. The *Sign task* button appears below the task status and is visible to users with the permission to sign the task.



Each electronic signature is unique to one individual person. It is based on a combination of the individual's e-mail and password, and cannot be reused or reassigned to anyone else. Electronic signature record provides the date and time when the signature was executed.

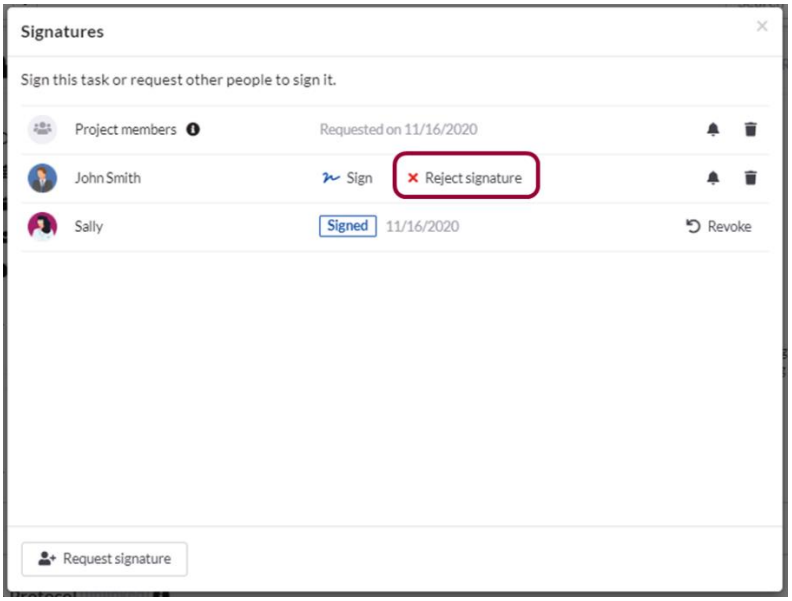


If there are two or more levels of supervision within an organization, additional signature(s) can be requested from specific people or user groups.



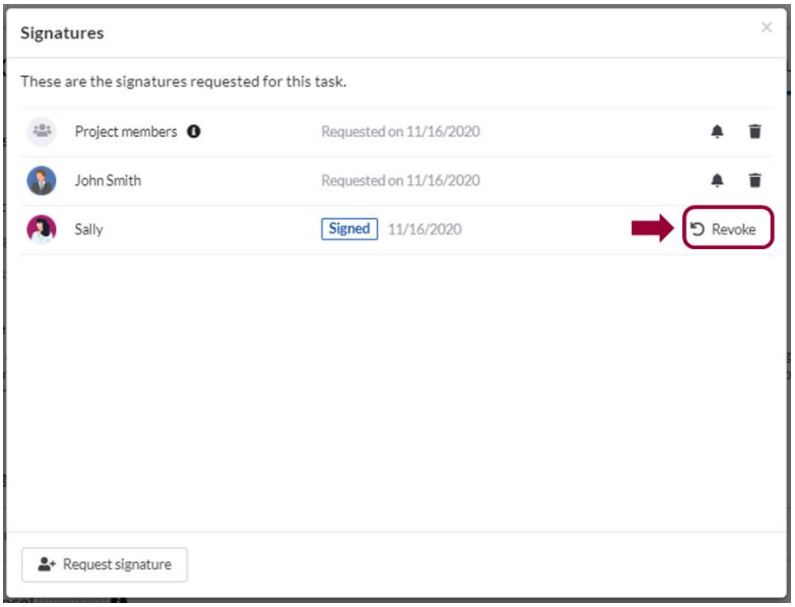
When the signature request is added, the reviewer gets the notification of the request on the dashboard and the option to sign the task.

Everyone who has the permission to sign the task also has an option to reject signing it, if he/she considers that the task needs to be improved.

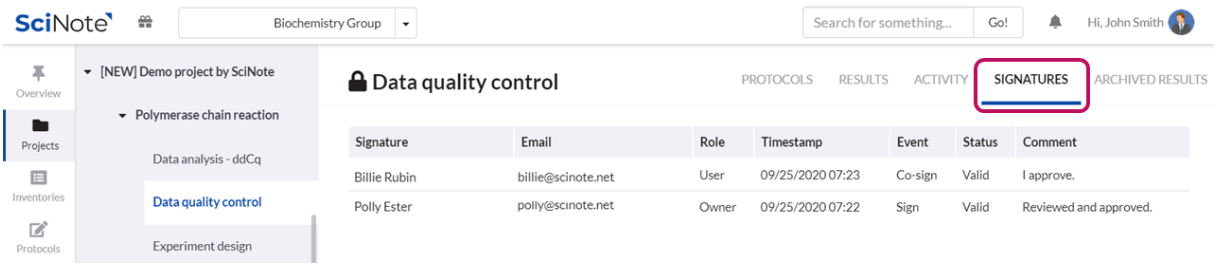


Rejecting a signature invalidates all the existing signatures on the task. Task should then be moved back to the unlocked state to be edited. When the task is moved back to the *In review* state, the signing and reviewing process restarts from the beginning.

Every signee can also revoke his/her own signature, if he/she would like to withdraw his/her signature from the task.



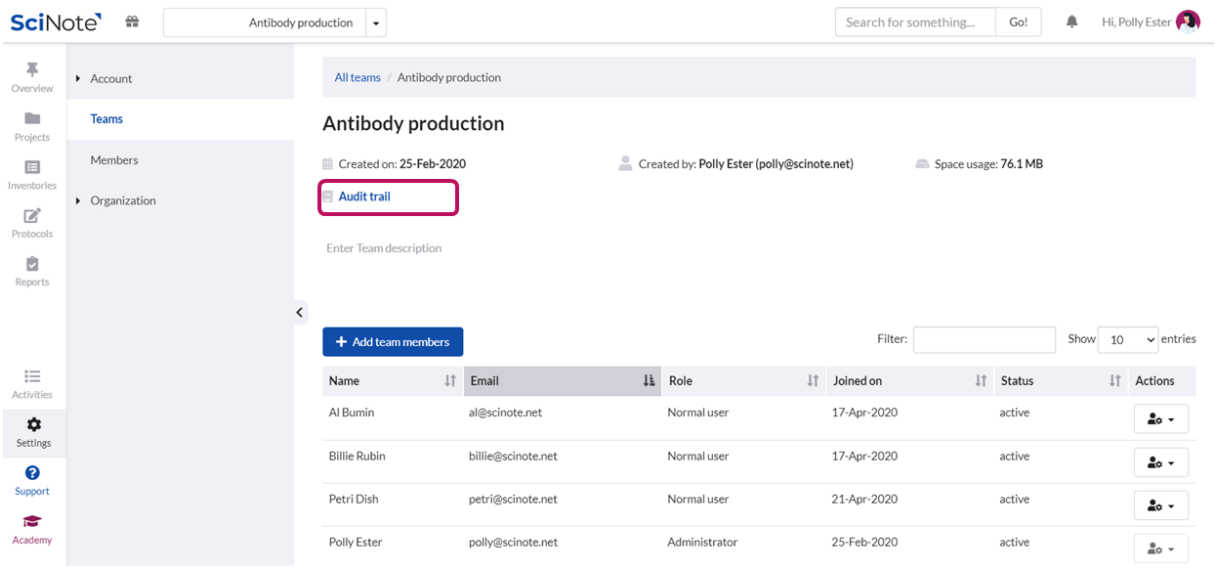
All electronic signatures are automatically recorded under the *SIGNATURES* tab within a task.



Audit trail

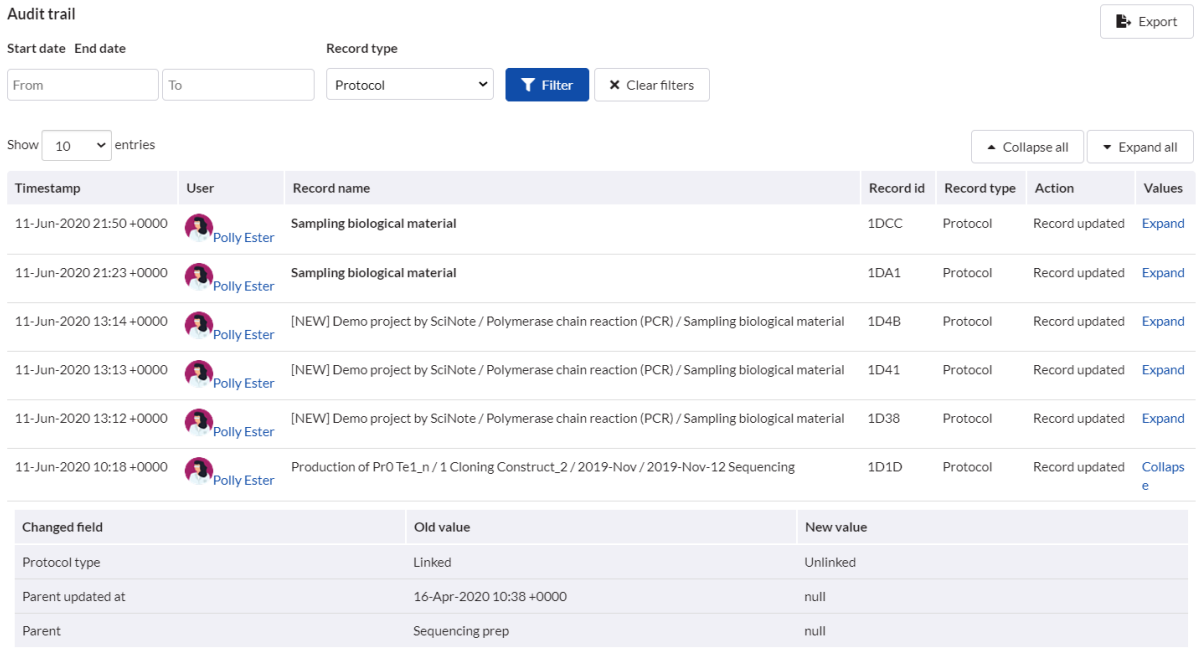
SciNote also maintains an audit trail i.e. a recorded history of all changes made in the system.

You can find the Audit trail for each individual team, by selecting *Teams* in the Settings and choosing the team of interest.

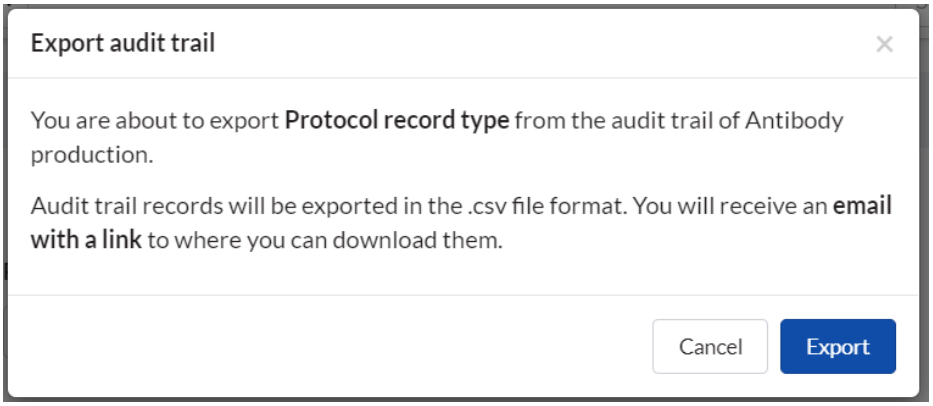


In the Audit trail records you can select which record type you want to see: projects, experiments, tasks, samples, results, files, signatures, etc. and in which time period.

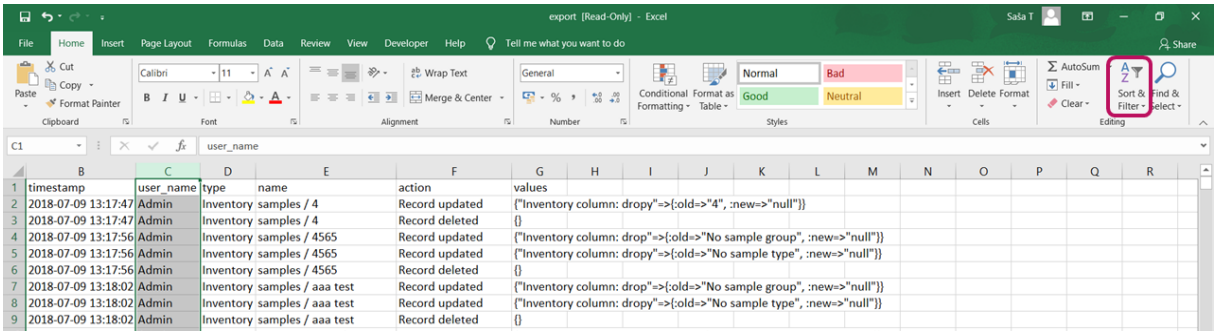
You will see the detailed overview of all changes made in the system: date and time, user who made a change, what was the change, etc. If you expand individual records you can also see what the values were before and after the change.



You can easily export the audit trail as a comma-separated values (.csv) file.



After you download the .csv file, you can reopen it in Excel as a spreadsheet table and use *Sort & Filter* option to filter the audit trail records, for example, by a user name.



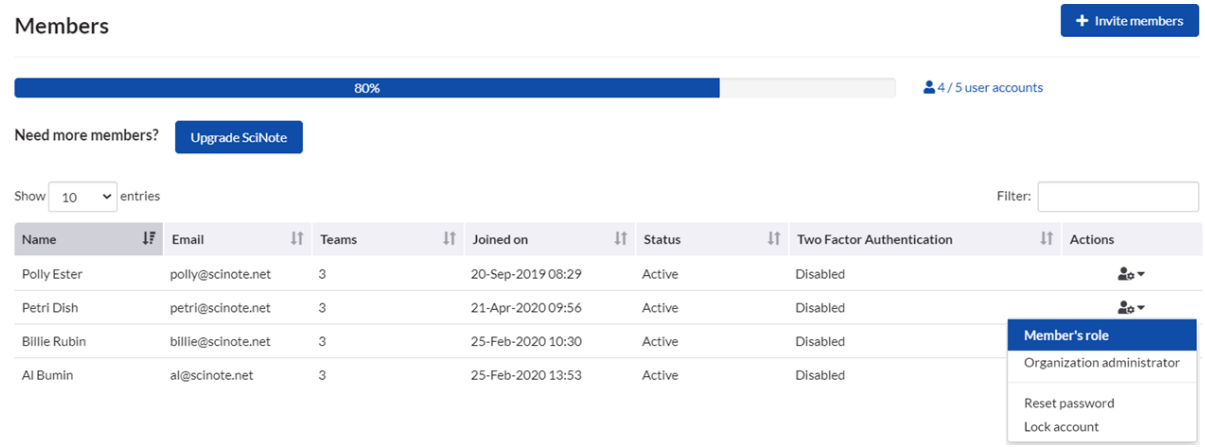
	timestamp	user_name	type	name	action	values
2	2018-07-09 13:17:47	Admin	Inventory	samples / 4	Record updated	{"Inventory column: dropy"=>{:old=>"4", :new=>"null"}}
3	2018-07-09 13:17:47	Admin	Inventory	samples / 4	Record deleted	{}
4	2018-07-09 13:17:56	Admin	Inventory	samples / 4565	Record updated	{"Inventory column: drop"=>{:old=>"No sample group", :new=>"null"}}
5	2018-07-09 13:17:56	Admin	Inventory	samples / 4565	Record updated	{"Inventory column: dropy"=>{:old=>"No sample type", :new=>"null"}}
6	2018-07-09 13:17:56	Admin	Inventory	samples / 4565	Record deleted	{}
7	2018-07-09 13:18:02	Admin	Inventory	samples / aaa test	Record updated	{"Inventory column: drop"=>{:old=>"No sample group", :new=>"null"}}
8	2018-07-09 13:18:02	Admin	Inventory	samples / aaa test	Record updated	{"Inventory column: dropy"=>{:old=>"No sample type", :new=>"null"}}
9	2018-07-09 13:18:02	Admin	Inventory	samples / aaa test	Record deleted	{}

Advanced team management - Organization administrator

Organization administrators can see all teams within the organization and have full access to manage individual teams and their members.

All team members are alphabetically organized in a list under the *Members* in the Settings.

New users can be invited only by the Organization administrator, either in *Members* or directly within the individual team in *Teams* in the Settings. Team administrators, on the other hand, can add only existing users to a team.

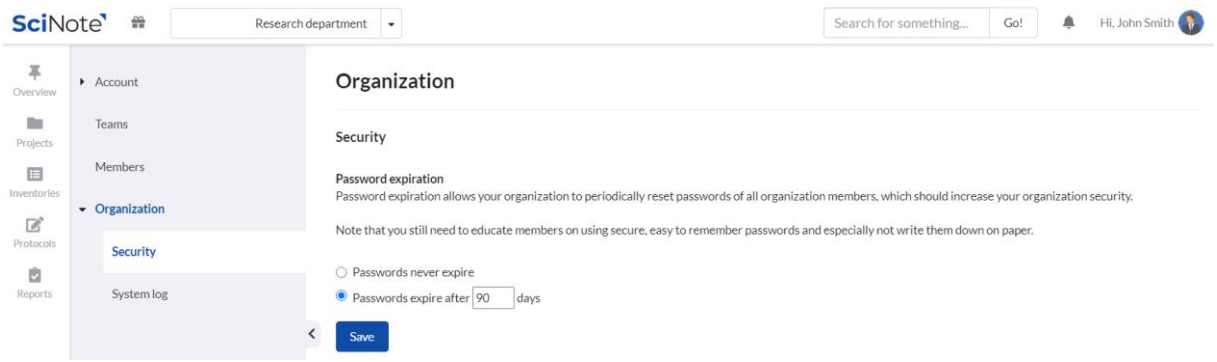


Security

1. Password expiration

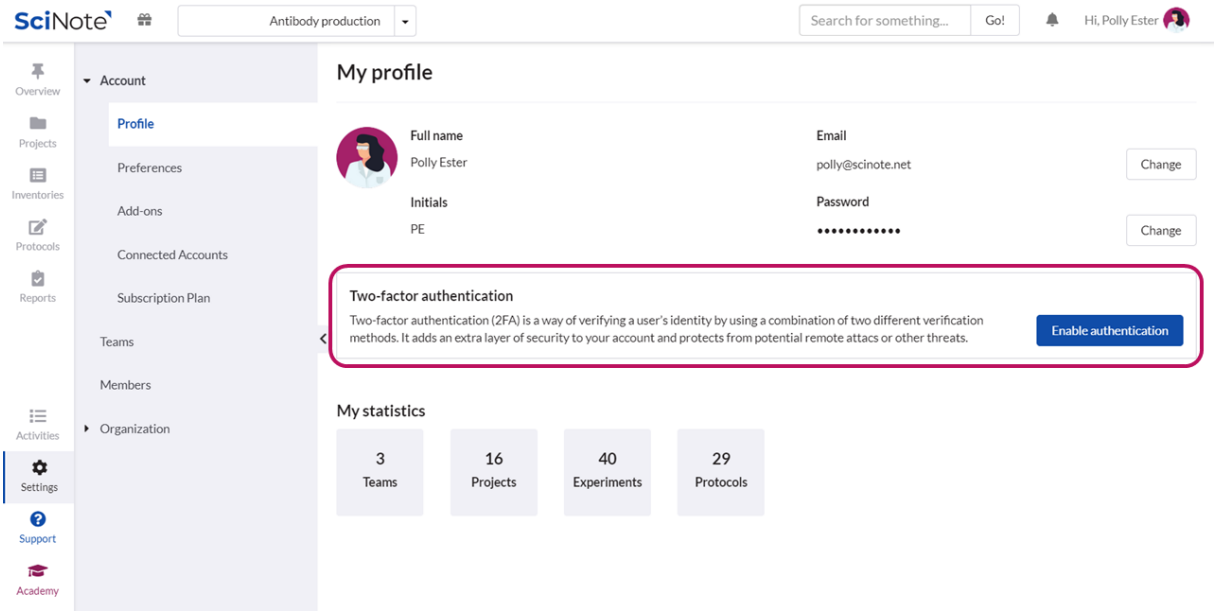
Password expiration is also a part of 21 CFR Part 11 requirements. Password expiration allows your organization to periodically reset passwords of all members, which will increase your organization's security if used properly.

Passwords can be reset on demand for individual users in *Members* (see the image above) or in *Organization* under the *Security* in the Settings (see the image below).



2. Two-factor authentication

You can enable two-factor authentication (2FA) for your account to have an extra layer of security by using a combination of two different verification methods. By enabling 2FA you will have to install the preferred Authenticator App on your mobile device.

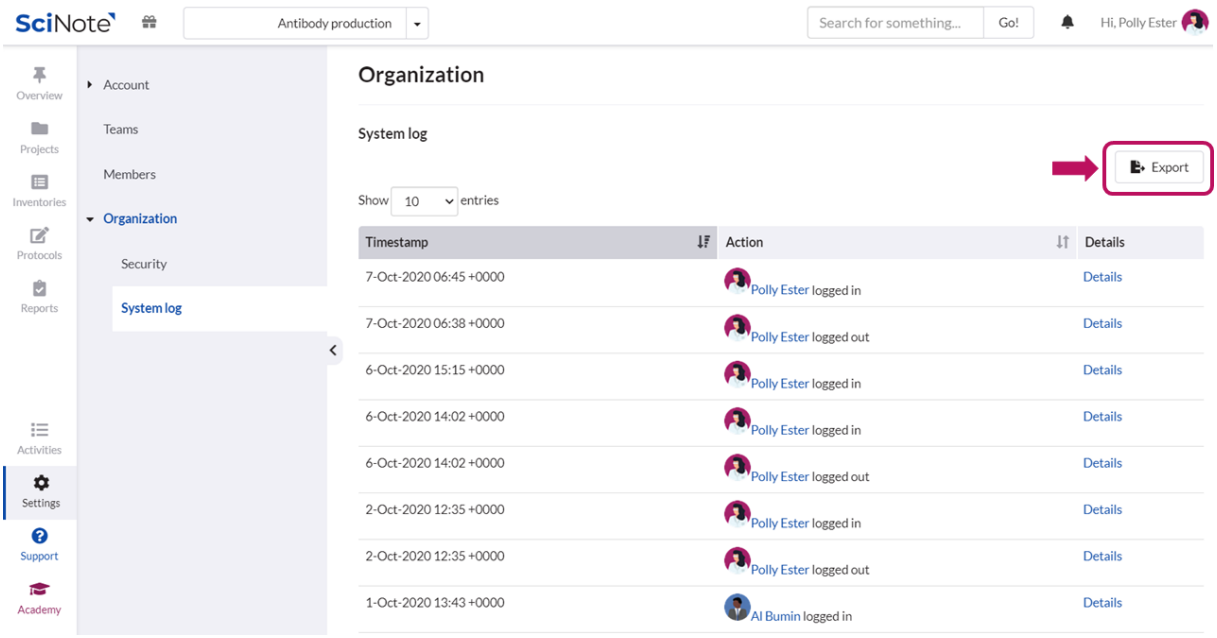


3. System log records

This functionality automatically records system activities and detects potential unauthorized access to SciNote. It gives you a detailed overview over invalid and valid user logins, user logouts and system errors.

System log records can be viewed only by Organization administrators. They can access system logs on a separate page, located under *Settings*, within the *Organization*.

System log records can be exported as a comma-separated values (.csv) file that can be re-opened in Excel as a spreadsheet table.



If you need more information about CFR 21 Part 11 in SciNote, schedule a Q&A session below:

Schedule a demo