

# Skroot Benchtop App Advanced Settings

Version: v1.1.16; Updated: 4/29/2025

Upon pressing the hamburger icon (☰) in the top left corner of the screen, a sidebar with appear with more advanced options. This is always available during the operation of the application.

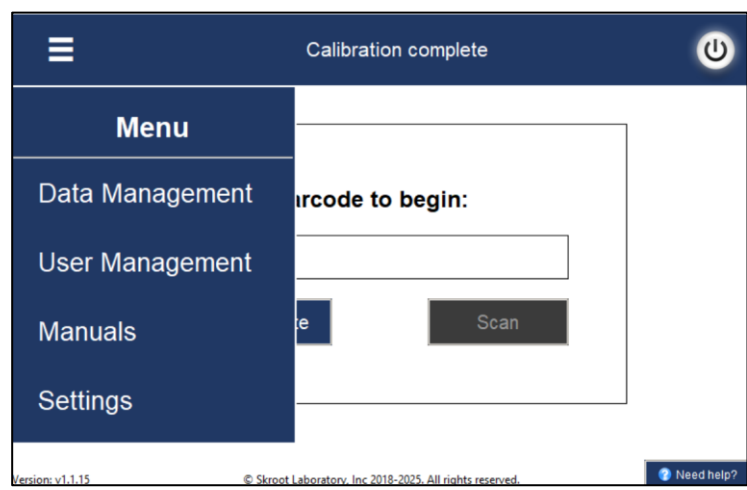


Figure 1: Sidebar menu options listed within the application. These are not needed in normal operation, but to access advanced settings.

## Data Management

The Data Management tab contains all functionalities related to data handling. It allows the user to export batch logs of individual experiments and administrators to export audit trails for the device.

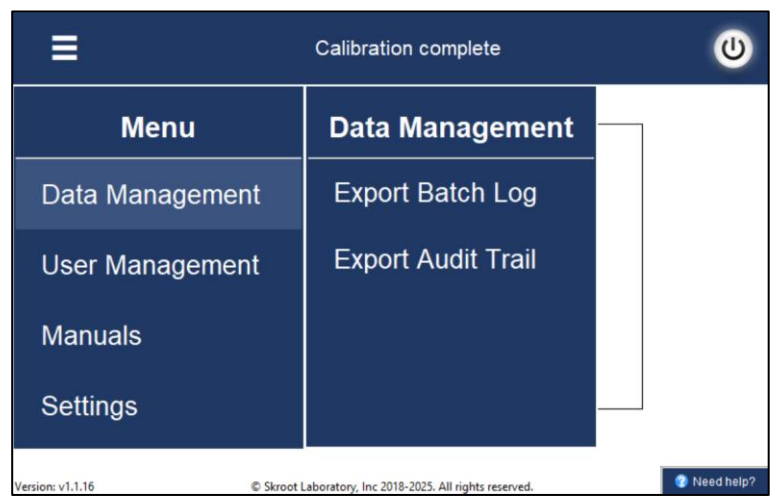


Figure 2: The data management submenu used to perform data exports. Requires a USB drive to be plugged in.

## Export Batch Log

The batch log for any vessel can be downloaded when it is scanned. As an alternative to this, users can download any vessel from the sidebar using this option and authenticating.

After authenticating as a system user, the user can type in the vessel ID for a batch record they would like to export. The exported PDF contains information about all scans performed, and the user who authorized them. It also contains information about when it was exported and who authorized the export.

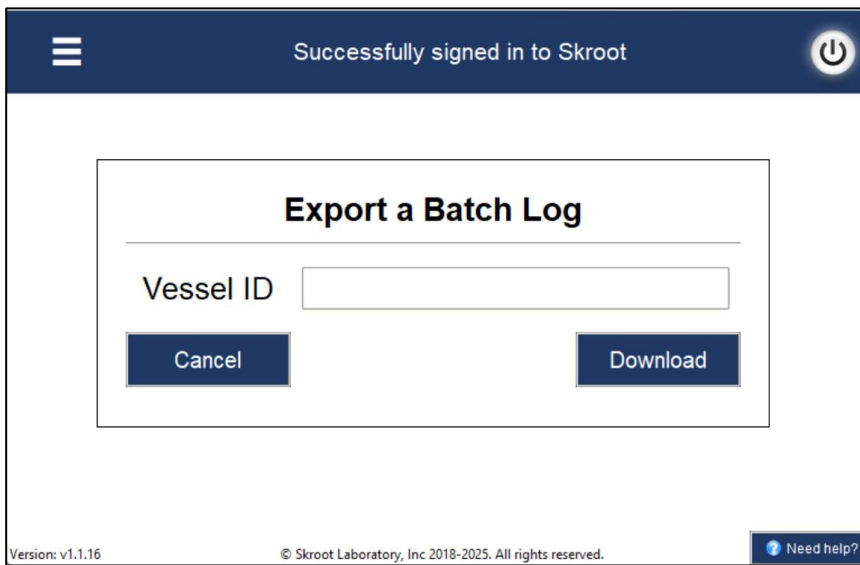


Figure 3: Batch Log Export Screen - Can be used to export a PDF batch log that records all entries for a given run. The PDF generated will be exported directly to the connected flash drive.

## Export Audit Trail

To assist in auditing the system, the Export Audit Trail option is available to the system admin. Upon authenticating, the system will create an “Audit” folder in the connected flash drive and export two types of files to the folder. One CSV file is created – “Auth Trail.csv” that contains all information regarding authentication attempts, failures and successes. It also contains information about the attempt, whether they were deleting a user, performing a scan, resetting a password etc.

In addition to the authentication trail, it will export data integrity logs. These logs are aggregated every week and will be exported as aide-weekly-summary-25W28.log (indicated the 28<sup>th</sup> week of 2025). This file contains logs of any modifications made to files during that week.

## User Management

The user management tab contains all options related to creating, modifying or removing users from the system. Only administrators and system administrators have access to change these settings.



Figure 4: User management options, to assist in controlling access to the system.

## Register a User

This option allows an administrator to register new administrators or users to the system. First it will prompt the user to sign in with a valid administrator, as shown in Figure 2. Once the system verifies the user is an admin, it opens the “User Registration” page to create a new user or administrator.

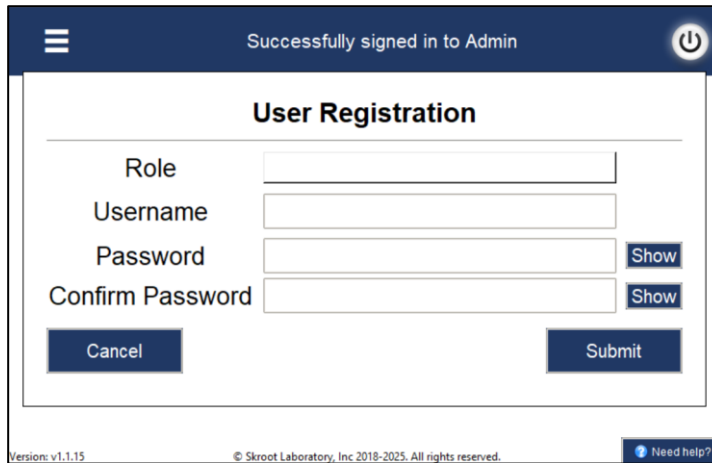
The image shows a web application interface for user registration. At the top, a dark blue header bar contains a hamburger menu icon on the left, the text "Successfully signed in to Admin" in the center, and a power icon on the right. Below the header, the main content area has a title "User Registration" centered. The form contains four input fields: "Role", "Username", "Password", and "Confirm Password". The "Password" and "Confirm Password" fields have "Show" buttons to the right. At the bottom of the form are "Cancel" and "Submit" buttons. The footer of the page includes "Version: v1.1.15", "© Skroot Laboratory, Inc 2018-2025. All rights reserved.", and a "Need help?" link with a question mark icon.

Figure 5: User registration page for administrators to create more users or administrators.

## Reset Password

In the case where a user or administrator forgets their password, there is a password reset available. Since the system is not connected to the internet, this must be done by the system administrator. After authenticating, they can enter a user and their new password into the system. Ensure to record this password somewhere because it will not be output anywhere.

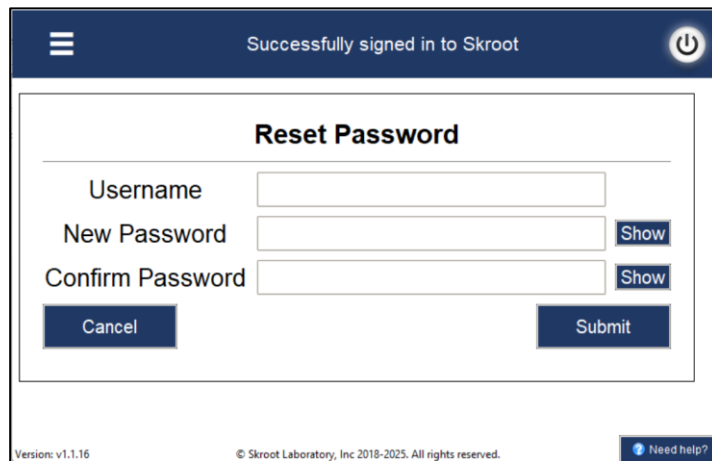
The image shows a web application interface for resetting a password. At the top, a dark blue header bar contains a hamburger menu icon on the left, the text "Successfully signed in to Skroot" in the center, and a power icon on the right. Below the header, the main content area has a title "Reset Password" centered. The form contains three input fields: "Username", "New Password", and "Confirm Password". The "New Password" and "Confirm Password" fields have "Show" buttons to the right. At the bottom of the form are "Cancel" and "Submit" buttons. The footer of the page includes "Version: v1.1.16", "© Skroot Laboratory, Inc 2018-2025. All rights reserved.", and a "Need help?" link with a question mark icon.

Figure 6: Reset Password Screen - The system admin can reset the password of any user.

## Delete User

To revoke access to the system, the system administrator can remove a user or administrator from the system using this option. This cannot be undone, so before deleting the user, ensure that the username was entered correctly.



Figure 7: Delete User Screen - The system admin can delete any user from the system, revoking all access to the system.

## Password Rotation

To assist in maintaining a secure system, System Administrators can configure password rotation. By default, a password reset is required every 90 days. The user is warned when they sign in within 7 days of expiration and users are removed from the system if they are inactive for 30 days after expiration. Users are also only allowed to change the password once per day. All of these settings can be configured to fit the systems specific use case.

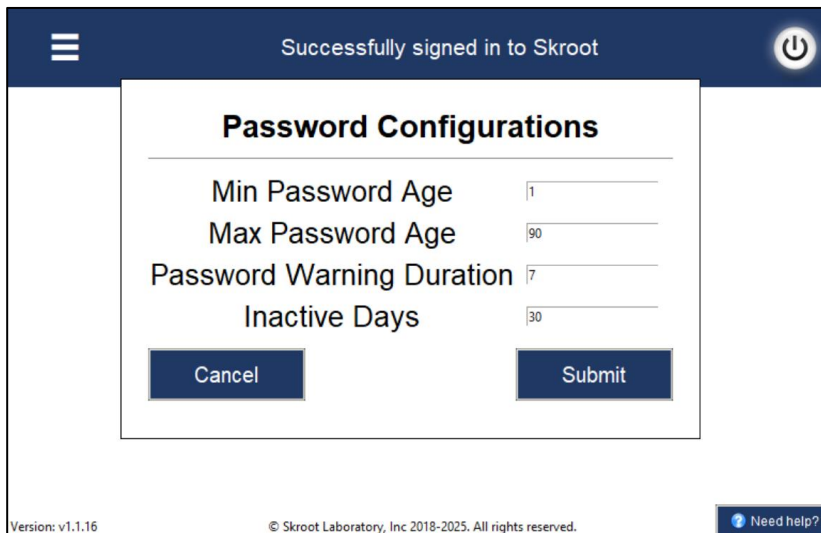


Figure 8: The Password Rotation Configuration can be used to configure password rotation settings to assist in maintaining a secure system.

## Manuals

All user manuals are available for view within the application. The guides are separated into three options – A “User Guide”, which contains information about setup and use of the Reader, intended to help in the operation of the system; A “Troubleshooting Guide” which has common problems and suggested fixes for a variety of issues, and an “Advanced Settings” guide, which is this document.

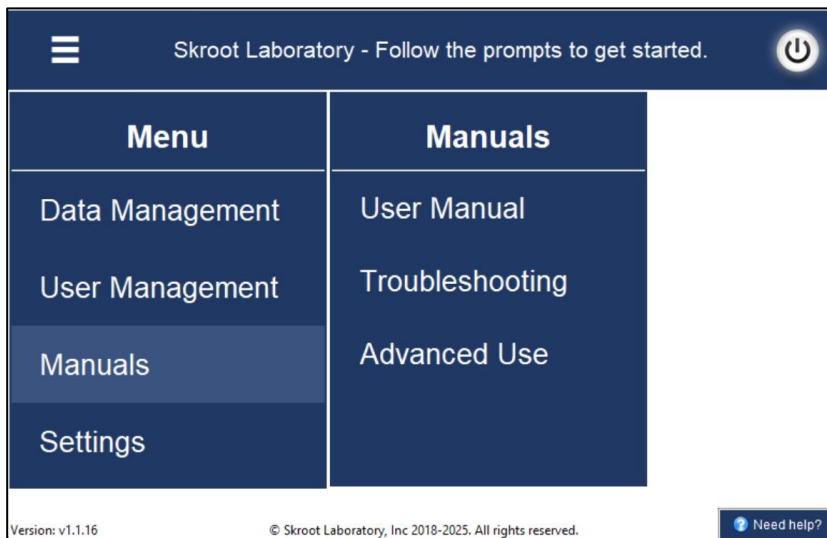


Figure 9: Multiple manuals are available to the user to view during operation.

## User Manual

Brings up this guide along with all troubleshooting steps to assist the user in correct operation of the Reader.

## Troubleshooting

Brings up a troubleshooting document to assist in diagnosing problems. It contains a list of common problems and fixes for them.

## Advanced Use

Brings up this guide, to assist in understanding the sidebar and its functionality.

## Settings

All functionality present in this option is available to the System Administrator only. It is intended to be used primarily during the initial setup to configure the system based on its intended use case.

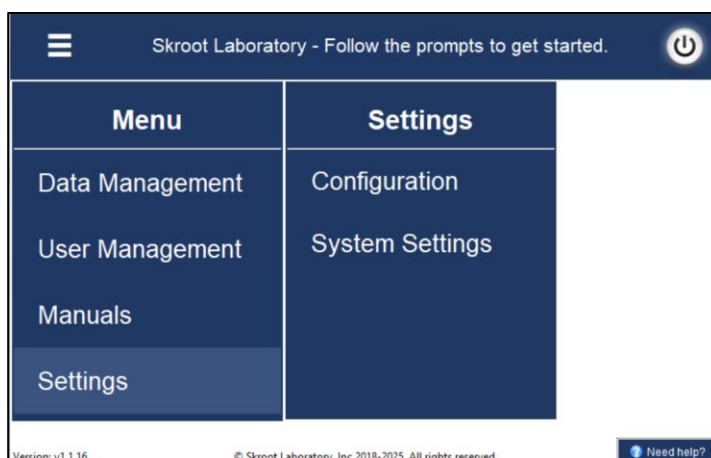


Figure 10: Settings available to the system administrator.

## Configuration

The configurations tab allows the system administrator to change the way the system operates. Some caution should be carried out here to ensure that the system operates securely and meets any compliance requirements necessary. Currently the only configuration is to disable the user sign in requirement.

**Authentication Enabled:** This setting enabled or disables user sign ins. By default, it is enabled but can be disabled for simpler operation.

*\* Disabling user authentication will result in a less secure system that is not CFR compliant.*

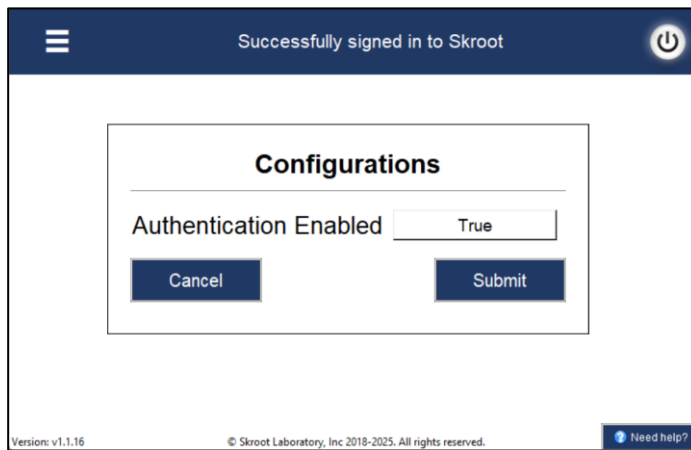


Figure 11: Configurations available to the system administrator that change the way the system operates.

## System Settings

Every Reader will have exactly one System Administrator. This option allows them to bypass the kiosk application and sign in to the desktop. It should only be used when advised by a representative as it has the potential to break the system if the wrong changes are made.