SOLABS QM10: DOCUMENT Section Privileges

CONTENTS

Introduction

The intent of this document is to address the setup and maintenance of privileges in the **DOCUMENT** section of **SOLABS QM10**. Assigning permissions/privileges allows the ability to have different levels of document access for users within the system.

The four available permission levels in the **DOCUMENT** section are **Read Only**, **Review/Approve**, **Modify** and **Administer.**

Note: The terms **privileges** and **permissions** are used interchangeable in this document. Privileges build cumulatively on one another, granting all lower-level privileges automatically upon assignment of a higher-level privilege.

Upon initial installation, some privileges are set by default but can be changed as needed:

- **SOLABS General User** is a generic role assigned to all users that is set up with the minimum permission level of **Read Only**.   It is provided as a "start-up" role on the Root folder and will therefore be inherited by any new folders you create. As you create folders, it should ideally be replaced with appropriate Security or Function Roles for your organization that will grant Read Only permissions, and then removed.

- **SOLABS System Administrator** and **SOLABS Document Administrator** are system roles available to assign to users at your organization who will administer users and documents. These roles are provided on the Root folder and set to grant the maximum permission level of **Administer**. They too will be inherited by any new folders you create, but can also be removed or replaced by other appropriate roles as needed.

November 2021

DOCUMENT Section Privileges

As mentioned above, Privileges build cumulatively on one another, granting all lower-level privileges automatically upon assignment of a higher-level privilege.

DOCUMENT Section Privileges | Table

PRIVILEGE LEVEL	ACTIONS POSSIBLE WITH THIS PRIVILEGE/PERMISSION LEVEL	APPLICABLE TO
READ ONLY	Can open and view documents in the **Approved and Effective** status. Can also open and view documents in the **Approved, Not Effective** status when assigned to them for training purposes.	Automatically assigned to users with an account type of **Train ID**. Can be assigned to any **General User** who needs to simply view approved documents.
REVIEW/APPROVE	Can view all **In Process** documents. Can act on **Review Cycles** and/or **Approval Cycles** for documents.	Must be assigned to users who will be document **Reviewers** or **Approvers**.
MODIFY	Can **Create** or **Modify** documents, change Referenced/Linked Documents, change Document Workflows. Has full access to the Review, Approval and Retire cycles.	Must be assigned to users who will be document **Authors**.
ADMINISTER	Can define **Privileges** on documents and folders.	Assigned by default to anyone with the system role assignments of **SOLABS System Administrator** or **SOLABS Document Administrator** but can be assigned to others as necessary.

DOCUMENT Section Privileges | Graphic

	READ ONLY	REVIEW/APPROVE	MODIFY	ADMINISTER
Can view APPROVED & EFFECTIVE documents. Can view APPROVED, NOT EFFECTIVE documents only when assigned to them for training purposes.	YES	YES	YES	YES
Can view all IN PROCESS documents. Can REVIEW or APPROVE documents	NO	YES	YES	YES
Can CREATE and MODIFY documents	NO	NO	YES	YES
Can manage document PRIVILEGES	NO	NO	NO	YES

DOCUMENT Section Privileges | Basic Concepts & Best Practices

Basic Concepts

- Privileges in **SOLABS QM10 DOCUMENT Section** are assigned from the top down (inherited from /Root or, for sub-folders, from the parent folders above them).

- The privileges in the **SOLABS QM10 DOCUMENT section** are completely configurable. When you do not want inheritance to apply, you break it by using the "Remove Inheritance" option, and create a **Custom** permissions scheme using the "Modify Privileges" option that then becomes available. Those Custom permissions are then in effect from that folder downwards, until such time as **Inheritance** is re-established.

- Any privileges that are **not Inherited** must be manually changed or assigned (i.e., **Custom**) by removing inheritance then making custom changes.

- **Inheritance** is *always* set by default; **Custom** has to be *always* manually set.

- Folders with inherited privileges that are moved **inherit the privileges of their new parent(s).**

- If **Inherited** permissions are used (that are passed down the Treeview structure), you will take advantage of the uniformity being passed down, and work with differences and exceptions to define each level in its differences

- If **Custom** privileges are used (that are assigned on a per folder basis, when **Inheritance** is broken), you will treat each folder as an 'island', building a scenario that works for that folder

Best Practices

- As mentioned at the beginning of this User Guide, the SOLABS General User role automatically provides Ready Only permissions to all users.   It is a best practice to replace the SOLABS General User role with appropriate Security Roles. If you want all of your users to be able to see all documents, replace it with an Organizational Security Role – one that is assigned to everyone at your company.   If certain departments need to see certain documents and not others, replace it with the appropriate Departmental Security Roles.
  - If you need to be more specific regarding Read Only permissions, you can also consider using Function Roles.
- Even if you are fine with all users having Ready Only permissions to all of your documents, it is a good idea to replace the SOLABS General User role especially if you will ever have the need to provide access to external parties. That will allow you to save the SOLABS General User role for that purpose if you'd like.
- It is also a best practice not to set fixed, custom privileges on more than two levels down from Root. This is simply because it can become confusing to efficiently manage your permission levels if they differ for every sub-folder level.   This should be considered when you are first setting up your Treeview folder structure.
- Although permissions can also be set on a specific document, it is better to set them at the folder level so that again, they can be more efficiently managed. This also should be considered when you are first setting up your Treeview folder structure.
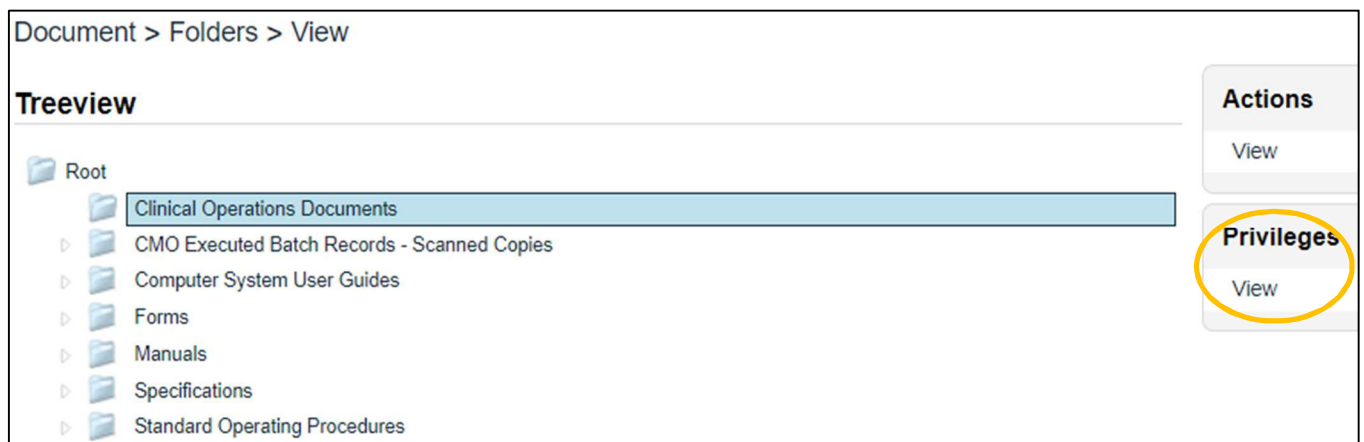
- Lastly, it is a very good practice to conduct periodic reviews of the privileges you have established for your folders.

For more thoughts on considering best practices on permission levels while setting up your Document Treeview folder structure, refer to **SOLABS QM10 Guide for Document Treeview Folder Structure**. This document is provided during initial configuration workshops but can be useful if you later find the original structure is not meeting your needs.

Assigning DOCUMENT Permissions & Privileges

The **Privileges** settings define the type of access the Users have to the different folders.   This access is granted by **Roles**.   When those Roles are assigned to a User, they then have the related Privileges.

To View and Modify Privileges for a Folder, highlight it within the Treeview and then choose **Privileges > View**.
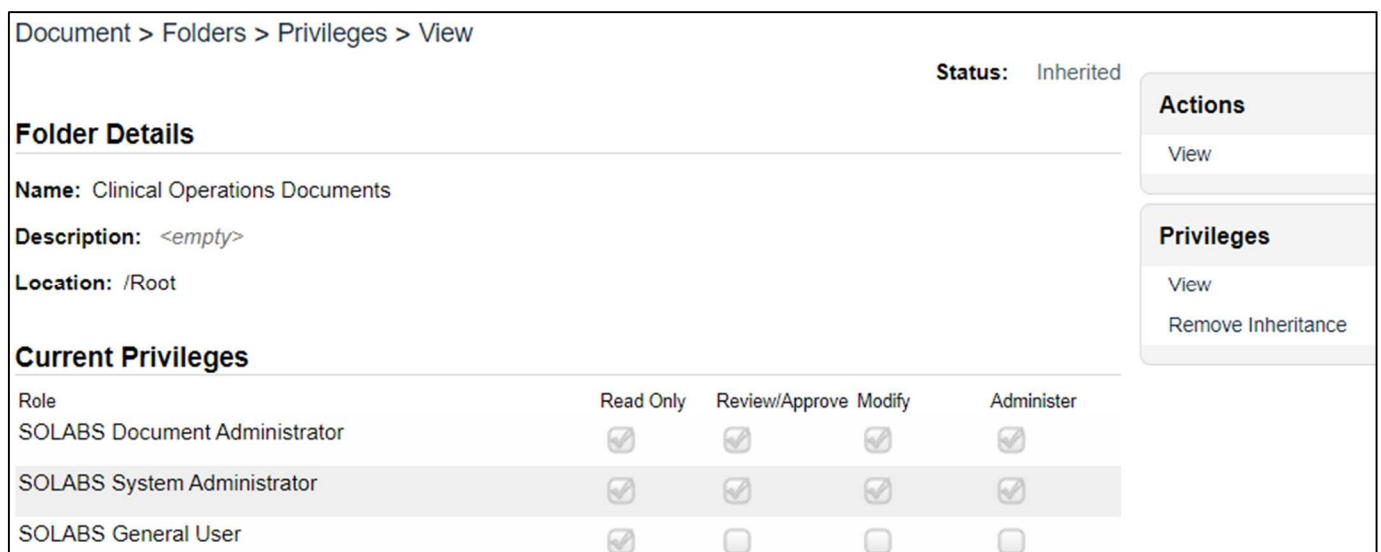
The **Document > Folders > Privileges > View** screen will be displayed. The settings displayed below in the **Current Privileges** section are the default settings applied to the **Root** folder, and therefore any other folders, unless they are modified by using the **Remove Inheritance** option.

Privileges on folders are either **Inherited** from the parent folder or are individually set by choosing to **Remove Inheritance**, which will then open the **Modifying Privileges** option.

To add additional privileges, first choose **Privileges > Remove Inheritance**. After Confirming that choice, the Privileges menu will include the options for **Modify Privileges**.

Clicking on the Modify Privileges option brings up the **Document > Folders > Privileges > Modify** screen.

This screen is used to Remove or Add privileges. All SOLABS QM Users have the **SOLABS General User** role by default so have **Summary View** privileges.

To add Review/Approve, Modify or Administer privileges to another Role, scroll through the list and select it. The list contains all active FCT, SEC, PR and SOLABS Roles. After selecting the Role, select the privileges you would like to add to that Role by choosing them at the bottom of the screen and then clicking on **Update**. When you have made changes, click on **Submit**.

Any privileges you have Added, Removed or Modified will be listed for review.

When you have verified the updates, click on **Confirm** to save the changes.

Current Privileges

Role	Read Only	Review/Approve	Modify	Administer
SOLABS Document Administrator	☑	☑	☑	☑
SOLABS System Administrator	☑	☑	☑	☑
FCT_Clinical Operations	☑	☑	☑	☐
FCT_Associate Director Quality Assurance	☑	☑	☐	☐
SOLABS General User	☑	☐	☐	☐

The **Privileges > Set Inheritance** option can be used to set **privileges back to those of the parent folder if/when needed.**

Privileges

View

Modify Privileges

Set Inheritance