Image Studio™ Software 21 CFR Part 11

System Management Tool Guide

The latest version of these instructions is available here https://www.licor.com/bio/help/21cfr11mgmt/.

System Management Overview

The System Management Tool is used to administer Image Studio 21 CFR Part 11 Software.

The System Management Tool is housed on the server and controls the Server Host. The System Management Tool is accessed through a browser, and access is password protected. Only designated **System Managers** should be allowed access to the System Management Tool.

System Manager Setup

The **System Manager** is a role within the customer organization responsible for the administration of Image Studio 21 CFR Part 11. LI-COR recommends the following policies for your organization's **System Managers**.

- Assign more than one **System Manager**.

  System Managers should be the organizational representatives responsible for maintaining the PostgreSQL® System Master Password for the Image Studio PostgreSQL database. Having multiple **System Managers** reduces the likelihood that the master password will be lost and provides redundancy in case one **System Manager** forgets his/her account password.

  Important: LI-COR is not responsible for maintaining the PostgreSQL System Master Password. However, LI-COR does provide a service to reset **System Managers'** account passwords if all **System Managers** have been locked out of the system. Contact technical support for details.

- Configure **System Manager** roles so that they cannot save changes in the client.

System Manager Responsibilities

System Manager responsibilities include:

- Maintaining the master password to the PostgreSQL database where Image Studio 21 CFR Part 11 data are stored.

  See "Data Management" on page 10.

- Configuring system security settings.

See "Security Settings" on page 16.

- Configuring which **Actions** are allowed and settings for allowed **Actions**.

  Each **Action** may require a comment, password, and/or an electronic signature. See "About Actions" on page 26.

- Defining **Actions** allowed for each user group (called **Roles**).

  See "About User Roles" on page 23.

- Adding or deactivating users.

  See "Add User" on page 20 or "Deactivate User".

Introduction

System Controls Overview for Image Studio 21 CFR Part 11

If a system administrator has set up Image Studio 21 CFR Part 11 for your group, access to Image Studio will be restricted to users with a valid user name and password.

User access to software functionality and data is controlled through roles and groups assigned to the user. The **System Manager** controls **Actions**, **Roles**, and **Groups** as well as system settings.

- **Actions** - Actions are operations performed by users within the system.
- **Roles** - A role is a set of allowed actions. Roles are assigned to users to control which actions a user can perform. Users may have multiple assigned roles, and roles may have overlapping assigned actions.
- **Groups** - A group is a set of users. Groups are assigned to users to control which **Work Areas** users can access.
- **Work Areas** - Work Areas contain data and allow access to customized software settings and analysis presets.

Notice and Trademarks

The information contained in this document is subject to change without notice.

LI-COR BIOSCIENCES MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. LI-COR Biosciences shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Image Studio software contains third-party open software. The licenses for the third-party software can be found at: http://opensource.licor.com/licenses/bio/index.html.

Doc #: 977-19945

2022-03-25

System Configuration

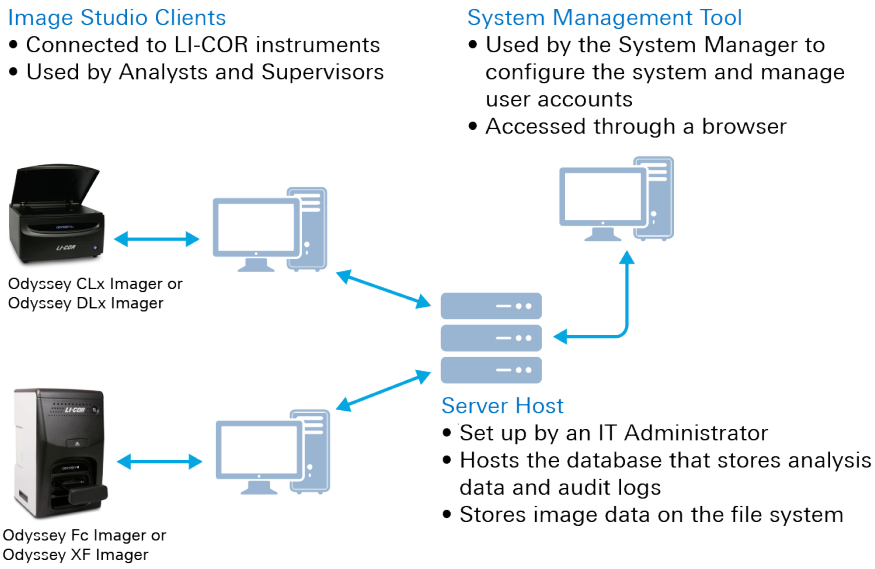
System Overview

System Description

The LI-COR® Odyssey® CLx Imager, Odyssey DLx Imager, Odyssey Fc Imager, and Odyssey XF Imager connect directly to the Image Studio 21 CFR Part 11 client. The Image Studio client connects to a network with access to the Server Host. Data are stored on the server and clients must request data from the Server Host through an authenticated connection. The Server Host passes requested data to the client once the request has been verified against the user's credentials and configured data access.

The System Management Tool is housed on the server and is used to manage the Server Host. The System Management Tool is accessed through a browser and access is password protected.

System Diagram



Server Description

- Maintains images
- Maintains image metadata
- Maintains analysis data

- Maintains user access information including passwords
- Maintains user and sample logs
- Notifies system manager about alerts

System Manager Tool Description

The System Management Tool is run through a browser connected to the server.

The System Management Tool:

- Adds and deactivates user accounts
- Sets actions and roles
- Sets user access
- Sets password requirements and other configurations
- Sets temporary passwords and resets passwords
- Reviews user logs

Image Studio Client

The client connects to the server for all data access. The server restricts access based on the configuration set in the System Management Tool.

- Used by Analysts and Supervisors
- Collects images from the instrument
- Analyzes images
- Submit/Approve changes

Server 1.3.7.30

Server Configuration

Image Studio 21 CFR 11 System Management Tool (Version 1.3.7.x) Server Requirements

The Image Studio 21 CFR 11 System Management Tool requires server class hardware with built-in redundancy.

- Modern server class CPU
- Minimum 8 GB RAM (16 GB recommended)
- 2 TB disk space
- Windows Server 2019 (English language)
- The following table lists which client and server versions are compatible. Other combinations of server and client versions are not compatible.

Image Studio 21 CFR 11 Client	Server
5.3.23	1.2.6.24
5.4.x	1.3.7.x

- Backup software - Utilize corporate backup system. For more information, see "Data Management".

Server Software Information

The following are installed on the server with Image Studio 21 CFR 11 System Management Tool version 1.3.7.x.

- Java 17
- PostgreSQL 9.6.23

Server 1.2.6.24

Server Configuration

Image Studio 21 CFR 11 System Management Tool (Version 1.2.6.24) Server Requirements

The Image Studio 21 CFR 11 System Management Tool requires server class hardware with built-in redundancy.

- Modern server class CPU
- Minimum 8 GB RAM (16 GB recommended)
- 2 TB disk space

- Windows Server 2012, 2012 R2, or 2019 (English language)
- The System Management Tool version 1.2.6.24 works with version 5.3.23 of the Image Studio 21 CFR 11 Client.
- Backup software - Utilize corporate backup system. For more information, see "Data Management".

Server Software Information

The following are installed on the server with Image Studio 21 CFR 11 System Management Tool version 1.2.6.24.

- Java 1.8.X
- PostgreSQL 9.3.4

Client 5.4.4

Client Configuration

Image Studio 21 CFR Part 11 Client (Version 5.4.x) System Requirements

The Image Studio 21 CFR Part 11 client requires the same minimum hardware configuration as the full version of Image Studio Software.

- Minimum 4 GB RAM
- Minimum display resolution of 1920 x 1080
- Windows 10
- Must have IPv6 enabled for instrument communications
- Network Interface Card
- A second Network Interface Card is required for optimal instrument communication when the instrument is not located on the local network.
- A configuration file exists on the client that will configure the client to communicate with the server's IP address/port. These configuration files must be present in the following locations for the Image Studio 21 CFR Part 11 client to function properly.

C:\Program Files\Licor\Image Studio	• 21cfr11.config • IS_keystore_client.p12
C:\Program Files\Licor\Image Studio\Keys	LICOR-21-CFR-11.lke

Client Setup Information

- Image Studio 5.4.x includes private Java installation version 17.
- The client saves event logs, error logs, and some temporary files at `C:\users\<windows login name>\.licor\Image Studio\temporary`. No image data, analysis data, user logs, or sample log data are stored on client drives.
- Image Studio Lab Books, Excel spreadsheets, and publication images can be exported to local or other network drives. Exported files are outside of Image Studio 21 CFR Part 11 control.

Network Configuration

- Client Server Communication TCP: HTTPS, typically on Port 8443
- Required for instrument communications between client and instrument:
  - SSH on TCP port 50000 for the Odyssey® CLx Imager, Odyssey DLx Imager, Odyssey Fc Imager, and Odyssey XF Imager.
  - Instruments are auto-discovered using UDP 5353.
- Firewalls on client must allow IPv6 and all protocols/ports stated above to allow communications to instruments and server.

Client 5.3.23

Client Configuration

Image Studio 21 CFR Part 11 Client (Version 5.3.23) System Requirements

The Image Studio 21 CFR Part 11 client requires the same minimum hardware configuration as the full version of Image Studio Software.

- Minimum 4 GB RAM
- Minimum display resolution of 1920 x 1080
- Windows 7, Windows 8, or Windows 10
- Must have IPv6 enabled for instrument communications
- Network Interface Card
- A second Network Interface Card is required for optimal instrument communication when the instrument is not located on the local network.
- Must have Bonjour for most instrument auto-connection (mDNSResponder installed with Image Studio Client)
- A configuration file exists on the client that will configure the client to communicate with the server's IP address/port. These configuration files must be present in the following locations for the Image Studio 21 CFR Part 11 client to function properly.

C:\Program Files\Licor\Image Studio	21cfr11.config IS_keystore_client.p12
C:\Program Files\Licor\Image Studio\Keys	LICOR-21-CFR-11.lke

Client Setup Information

- Image Studio 5.3.x includes private Java installation version 1.8.x. Image Studio 5.3.x also installs mDNSResponder and USB drivers.

- The client saves event logs, error logs, and some temporary files at C:\users\<windows login name>\.licor\Image Studio\temporary. No image data, analysis data, user logs, or sample log data are stored on client drives.

- Image Studio Lab Books, Excel spreadsheets, and publication images can be exported to local or other network drives. Exported files are outside of Image Studio 21 CFR Part 11 control.

Network Configuration

- Client Server Communication TCP: HTTPS, typically on Port 8443

- Required for instrument communications between client and instrument:

    - SSH on TCP port 50000 for the Odyssey® CLx Imager, C-DiGit® Blot Scanner, and Odyssey Fc Imager.

    - Some instruments can optionally use USB. USB drivers install with Image Studio installation.

- Firewalls on client must allow IPv6 and all protocols/ports stated above to allow communications to instruments and server.

Data Management

Image Studio 21 CFR Part 11 data are stored on the server.

- Images and server log files are saved in the **Server** folder.
  `C:\users\<windows login name>\.licor\ImageStudio\Server`

- All other data, including analysis data and metadata, are stored in a PostgreSQL database.

  Important: The PostgreSQL System Master password is required to back up the database. LI-COR is not responsible for maintaining the password.

Data Backup

Each customer organization is responsible for backing up data according to their own policy. LI-COR recommends the following guidelines for backing up your data:

- Back up the PostgreSQL database and image data in the **Server** folder on a routine basis.
- Keep the database backup and **Server** folder backup in sync by backing both up at the same time.

Contents of the **Server** folder can be backed up using appropriate file management procedures, and the database can be backed up using the methods described below.

Back up Database Using the pgAdmin 4 Interface

Please see the following third-party guide for more information about using the pgAdmin 4 database management system to back up and restore your database https://www.pgadmin.org/docs/pgadmin4/latest/backup_and_restore.html.

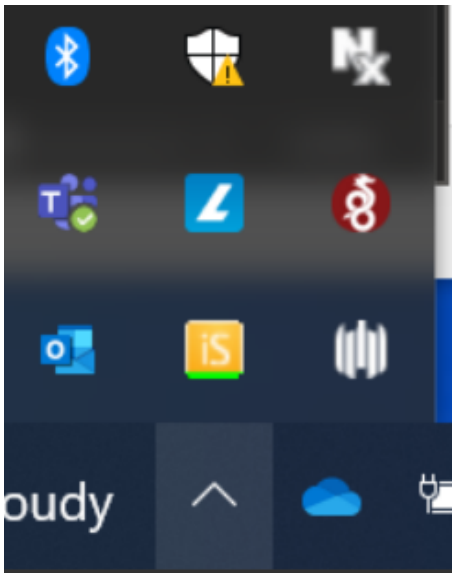
Back up Database Using a Batch Script

A batch script `backup.bat` is provided in the Image Studio 21CFR11 server installation folder to assist with automated backups. This script calls `pg_dump.exe` to create a plain text backup. Use or modify the script as necessary for use in your backup procedure. Ensure that the backup procedure you use meets your needs and complies with your organization's policies.

The following example procedure shows how `backup.bat` can be used.

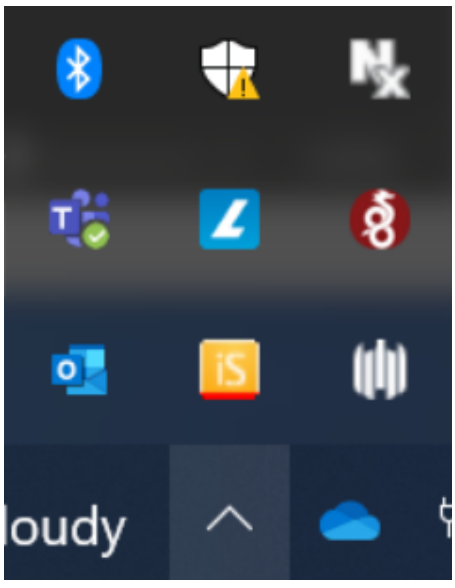
Important: For this procedure, you will need to stop the Image Studio Service on the server. Ensure there are no active Image Studio Client sessions and no active System Management Tool sessions active. Stopping the Image Studio Service will cause clients to disconnect.

1. On the server, open the Windows System Tray and locate the Image Studio Service icon.



If the Image Studio service is running, there will be a green bar underneath the Image Studio Service icon.

2. Right click the Image Studio Service icon, and then click **Stop service**.



A red bar underneath the Image Studio Service icon indicates that the Image Studio Service has stopped.

3. Open the Windows Command Prompt.

4. In the Command Prompt Window, navigate to this folder: `C:\IsServerApp\sample backups files`.

   In this folder, you will find a script called `backup.bat`.

5. To backup the database, run the script by entering the following command:

   `.\backup.bat`

6. As the script runs, output from the `pg_dump` command will be displayed.

   The script will back up the database to a file named in the following format: `MyBackup_<current date>.backup`.

Additional backup and restore information can be found on the PostgreSQL wiki https://wiki.postgresql.org/wiki/Automated_Backup_on_Windows.

Restore a Plain Text Backup

A batch script `restore_with_psql.bat` is provided in the Image Studio 21CFR11 server installation folder to assist with restoring backups.

The following example procedure shows how `restore_with_psql.bat` can be used.

1. In pgAdmin 4, ensure the `licor_image_studio` database is empty and has the owner `image_studio`.

2. Open the file `C:\IsServerApp\sample backups files\restore_with_psql.bat` in a text editor like Windows Notepad.

3. Copy the command in this file.

   This is the command in `restore_with_psql.bat`:

   `"C:\Program Files\Postgresql\9.6\bin\psql.exe" -d "licor_image_studio" -f "MyBackup_10_29_2015.backup" –U “postgres"`

4. Open the Windows Command Prompt.

5. Paste the command you copied from `restore_with_psql.bat` into the Command Prompt.

6. Change `"MyBackup_10_29_2015.backup"` to the name of your backup file.

7. Press **Enter** to run the command.

Data Management (Version 1.2.6.24)

Image Studio 21 CFR Part 11 data are stored on the server.

- Images and server log files are saved in the **Server** folder.
  `C:\users\<windows login name>\.licor\ImageStudio\Server`

- All other data, including analysis data and metadata, are stored in a PostgreSQL database.

  Important: The PostgreSQL System Master password is required to back up the database. LI-COR is not responsible for maintaining the password.

Data Backup

Each customer organization is responsible for backing up data according to their own policy. LI-COR recommends the following guidelines for backing up your data:

- Back up the PostgreSQL database and image data in the **Server** folder on a routine basis.
- Keep the database backup and **Server** folder backup in sync by backing both up at the same time.

Contents of the **Server** folder can be backed up using appropriate file management procedures, and the database can be backed up using the methods described below.

Back up Database Using the pgAdmin III Interface

Please see the following third-party guide for more information about using the pgAdmin III database management system to back up and restore your database http://-get.enterprisedb.com/docs/Tutorial_All_PP_pgAdmin_Backup_Restore.pdf.

Note: Plain text backup files generated from the backup with pgAdmin III **cannot** be restored in pgAdmin III.

Back up Database Using a Batch Script

A batch script `backup.bat` is provided on the Image Studio 21 CFR Part 11 installation CD to assist with automated backups. This script calls `pg_dump.exe` to create a plain text backup.

Copy the batch script from the installation CD to the server, and modify the script as necessary for use in your backup procedure.

Additional backup and restore information can be found on the PostgreSQL wiki https://wiki.-postgresql.org/wiki/Automated_Backup_on_Windows.

Restore a Plain Text Backup

Use the following command (as the PostgreSQL administrative user) to restore a plain text backup from pgAdmin III (where the backup file is `MyBackup_10_29_2015.backup`).

```
"C:\Program Files\Postgresql\9.3\bin\psql.exe" -d "licor_image_studio" -f "MyBackup_10_29_2015.backup" –U “<user name>"
```

Security Settings

Security Settings

The system settings (password requirements, password settings, and security settings) apply to all users, including **System Managers**. The "Default Settings" topic (see page 17) includes system settings defaults for reference.

Changes to the system configuration are recorded in the **User Log**. See "User Log" on page 33.

Modify the system configuration

1. Click Setup on the top navigation bar.
2. Click to the right of the system settings.
3. Make changes and click **Save**.

Password Requirements

Password requirement options are provided to ensure passwords in Image Studio 21 CFR Part 11 comply with your organization's policy. The password requirements do not apply to temporary passwords.

Password Settings

- **Valid for X day(s):** This setting specifies the length of time a password is valid. Users will be locked out of the system if they do not change their passwords within this time frame. To be readmitted to the system, users must receive a temporary password from the **System Manager**. See "Set Temporary Password" on page 21 for how to grant a user a temporary password.
- **Reuse old password after X day(s):** This setting specifies the length of time users must wait before reusing an old password. The time is measured from when the old password was created.
- **Start expiration warning at X hour(s):** Users will be warned to reset their passwords at each login to the system within this time frame. The time is measured from when the password expires.

- **Temporary password valid for X hour(s):** When a user is granted a temporary password, the user must reset the password within this time frame.

Security Settings

- **Lock out user after X failed login attempts.** Once a user is locked out, you will have to provide the user with a temporary password that can be used to login to the system. The user will have to set a new password immediately after logging in with the temporary password. See "Set Temporary Password" on page 21.

- **Post notification after more than X attempts to login with an invalid username occur in Y hour(s).** The notification will be posted on the Home page until it has been marked as read on the Logs page. This notification is available to alert **System Managers** to possible attacks on the system.
- **Time out session after X minute(s).** Users will automatically be logged out after this time and will be required to log back in.

Assigned Actions Table

Actions are software operations performed in Image Studio 21 CFR Part 11. Use the **Assigned Actions** table to select which **Actions** will be allowed in the system and what response (comment, password, signature) will be required when an **Action** is performed. Click  at the right of the table to configure an **Action**.

- See "Manage Actions" on page 27 for details about allowing **Actions** in the system.
- See "Manage Roles" on page 24 for how to assign **Actions** to a **Role**.

Default Settings

The default system configuration is listed below for reference.

Password requirements

- Minimum length: **5**
- Requires mixed case: **Yes**

- Requires numeric: **Yes**
- Requires special characters: **Yes**

Password settings

- Valid for **90** days.
- Reuse old password after **365** day(s).
- Start expiration warning at **168** hour(s).
- Temporary password valid for **24** hour(s).

Security settings

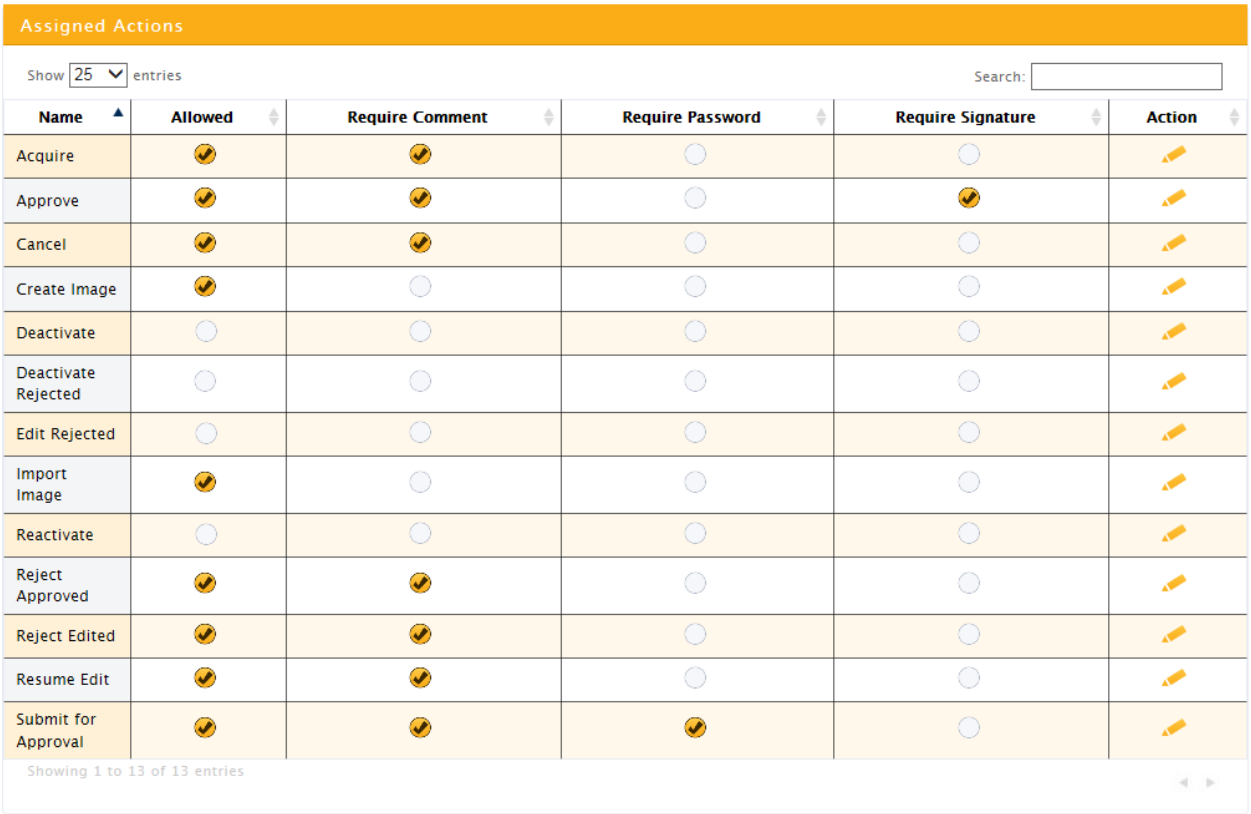
- Lockout user after **5** failed login attempts.
- Post notification after more than **5** attempts to login with an invalid user name occur in **24** hour(s).
- Time out session after **30** minute(s).

Roles and allowed actions

Role Name	Role Description	Actions
Analyst	Acquires images, edits an image's analysis data and associated data, then submits the image and data for approval.	• Acquire • Cancel • Create Image • Edit • Edit Rejected • Import Image • Submit for Approval • Edit Tem-plates

Supervisor	Controls user access to Work Areas containing images and data. Decides if submitted images and data meet organizational standards.	• Approve • Reject Approved • Reject Edited • Create Work Area • Edit Templates
System Manager	Defines user roles and groups of users, modifies users' account settings, and controls system security settings.	Edit System Configuration

Allowed action settings



User Controls

Users

About Users

User access to data and **Actions** in the software is controlled using the System Management Tool.

- Access to **Actions** (software operations) is controlled by assigning a user to a **Role**. Each **Role** has allowed actions. Users are restricted to **Actions** that are allowed for the **Roles** they have been assigned.
- Access to data is controlled by assigning groups to a user. **Groups** are given access to **Work Areas** that contain images, data, and software settings. Users are limited to the **Work Areas** given to the groups they are a part of.

Add User

When adding a user, you must assign the user the correct **Roles** and **Groups**.

- **Roles** specify which **Actions** the user will be allowed to perform.
- **Groups** specify which data the user will be allowed to access.

Add a user:

1. On the Home page, click Users .
2. On the Users page, click Add New .
3. Fill in the required fields.
4. Specify which **Role** or **Roles** should be assigned to the user. Multiple **Roles** can be assigned to a user.
5. Specify which **Group** or **Groups** should be assigned to the user. Multiple **Groups** can be assigned to a user.
6. Click **Save**.

Set Temporary Password

Set a temporary password for users who have forgotten their passwords or have been locked out of Image Studio 21 CFR Part 11 for too many incorrect login attempts. The user will have to reset the password immediately after login with the temporary password you provided.

Important: A **System Manager** who logs in to the System Management Tool with a temporary password should reset the password immediately.

Set a temporary password

1. On the Home page, click Users .
2. On the Users page, find the row in the table for the user whose password needs to be reset and click .
3. Click Reset Password.
4. Set a temporary password for the user.

   Note: The temporary password is not required to conform to the password requirements specified on the Setup page.

5. Give the temporary password to the user in accordance with your organization's policy.

Deactivate User

Deactivate a user to revoke the user's access to Image Studio 21 CFR Part 11. User accounts cannot be deleted, only deactivated. The deactivation will be recorded in the **User Log**.

Deactivate a user:

1. On the Home page, click Users .
2. On the Users page, find the row in the table corresponding to the user who must be deactivated and click .
3. Click **Deactivate User**.

Groups

About Groups

Groups are used to control which data users are able to access. **Work Areas** (containing images, analysis data, software settings, and analysis presets) are assigned to groups to allow users in the group access to the **Work Area**.

The **System Manager** controls **Group** and **Work Area** assignments.

- **Work Areas** can be assigned to multiple **Groups**.
- Users can be assigned multiple **Groups**.

Manage Groups

Create a new **Group** when you need to give a unique set of users access to a unique set of **Work Areas**.

Note: Users must be assigned to **Groups** on the Users page.

Create a group

1. On the Home page, click **Groups** .
2. On the **Groups** page, click create new .
3. Assign the **Group** a name and description that other **System Managers** will easily understand.
4. Click **Save**.

Modify an existing group name or description

1. On the Home page, click **Groups** .
2. On the **Groups** page, find the row in the table for the **Group** you need to modify and click .
3. Click to the right of the **Group** name and description fields.

4. Modify the name or description.
5. Click **Save**.

Roles

About User Roles

A **Role** is a set of allowed actions. **Actions** are operations performed by a user within Image Studio 21 CFR Part 11. **Roles** are assigned to users to control which **Actions** a user can perform.

Only the **System Manager** can add or modify **Roles**.

- The allowed actions for default **Roles** can be adjusted and custom roles can be added.
- Roles can be assigned overlapping allowed actions.
- Users can be assigned multiple roles.

  Note: As long as an action is allowed for one of a user's multiple roles, the user may perform that action.

- Users cannot approve their own work, even if a user is assigned a **Role** with the allowed actions to submit and approve.

Default roles and allowed actions

Role	Description	Actions Allowed By Default

Analyst	Acquires images, edits an image's analysis data and associated data, then submits the image and data for approval.	• Acquire • Cancel • Create Image • Edit • Edit Rejected • Import Image • Submit for Approval • Edit Templates
Supervisor	Controls user access to Work Areas containing images and data. Decides if submitted images and data meet organizational standards.	• Approve • Reject Approved • Reject Edited • Create Work Area • Edit Templates
System Manager	Defines user roles and groups of users, modifies users' account settings, and controls system security settings.	Edit System Configuration

Manage Roles

Default **Roles** can be modified, or new **Roles** can be added. Add a new **Role** if you need to assign users a specific set of allowed actions and you are already using the default **Roles**.

To assign an **Action** to a **Role**, first ensure the **Action** is allowed in the system and ensure the action is configured to require the appropriate response (comment, password, and/or signature).

Check if action is allowed and configured correctly

1. Click Setup on the top navigation bar.

2. Scroll to the **Assigned Actions** table and find the row for the **Action** you need to check.

- If the check box in the Allowed column for the **Action** is selected, the **Action** is allowed in the system and can be added to **Roles**. The selected responses will be required whenever the action is performed.
- If the settings for the **Action** need to be modified, click and then select or clear options that need to be added or removed.

3. Click **Save** if you have made any changes.

Add and configure a new role

1. On the Home page, click **Roles** .
2. On the **Roles** page, click add new .
3. Add a name and description for the role that will be easy to understand for other **System Managers**.
4. Select from among the **Actions** allowed in the system.
5. Click **Save**.

Modify an existing role

1. On the Home page, click **Roles** .
2. In the table, find the row for the **Role** that needs to be modified and click .
   - To change the **Actions** allowed for that **Role**, click to the right of the **Actions** group. Select from among the **Actions** allowed in the system.
   - To change the **Role** name or description, click to the right of the **Role** name and description fields. Make your changes to the fields.
3. Click **Save**.

Actions

About Actions

Actions are software operations performed by users within the system. **Actions** are assigned to **Roles** by the **System Manager**. **Roles** are assigned to users to control which actions users may perform. Many actions are used to change the status of an image (see "Image Status" on page 29).

Note: All **Actions** are recorded in the **Image Log** no matter how the system is configured.

Depending on the system configuration (set up by the **System Manager**), users may need to do the following to complete an action:

- Enter password
- Enter comment
- Provide electronic signature

Complete list of actions and descriptions

Action Name	Action Description
Acquire	Use Image Studio to obtain an image from a LI-COR instrument.
Cancel	Terminate the Acquire process. The partially acquired image will have a Canceled status and cannot be analyzed or edited.
Create Image	Rotate, adjust contrast, or otherwise transform image data. Some options may affect quantification results.
Import Image	Add an image from outside Image Studio to the current Work Area.
Edit	Analyze an image or modify its descriptive text.
Submit for Approval	Stop the editing process and offer an image with its associated data for review. The image will be in the Waiting for Approval status until approved or rejected by a Supervisor.
Resume Edit	Continue editing an image's analysis data or descriptive text for an image with the Waiting for Approval status.

Approve	Designate that an image and its associated data meet organizational standards. Users may never approve their own submissions.
Reject Edited	Designate that an image and/or its associated data do not meet organizational standards.
Edit Rejected	Change an image's status from Rejected to Editing and resume editing an image's analysis data or descriptive text.
Deactivate	Remove image from normal display.
Deactivate Rejected	Remove a rejected image from normal display and prevent further edits to the image.
Reactivate	Transition an image and its associated data from inactive to available for display and edit.
Reject Approved	Designate the image and its information which is Approved as Rejected.
Create Work Area	Name a space in which to store images, analysis data, software settings, and log records.
Edit Templates	Modify certain settings and the layout of shapes or wells that can be used as a template to start an image analysis.
Edit System Configuration	Modify security settings (e.g. password length), modify which actions are allowed (e.g. Acquire), and control Users' access to the system.

Manage Actions

Actions must first be allowed in the system before they are assigned to a **Role**. Assign a **Role** to a user to control which **Actions** the user may perform. **Actions** must be assigned to **Roles** on the **Roles** page.

Actions can be configured so that a password, comment, and/or electronic signature is required to perform the action. If an **Action** is configured to require a response, users will be prompted for the response each time they perform the action.

Note: The **Edit**, **Create Work Area**, and **Edit Template** actions are always allowed in the system. They can still be added and removed from **Roles**.

Allow an action in the system and configure the required responses

1. Click Setup on the top navigation bar.
2. On the Setup page, scroll to the **Assigned Actions** table , and find the row with the **Action** you would like to allow.
3. Click on the right side of the row.
4. Select the check box in the Allowed column, and select the responses you would like to require each time the action is performed.
5. Click **Save**.

Work Areas

A **Work Area** is a grouping of images and data. Software settings and analysis settings can be saved for each **Work Area**.

In the Image Studio 21 CFR Part 11 client, **Groups** have access to **Work Areas**. **Groups** are then assigned to users to allow users in the **Group** access to the images, data, and software presets in the **Work Area**. A **Work Area** can be assigned to multiple **Groups**.

A **Work Area** can be created in one of two ways:

- A **System Manager** can create a **Work Area** through the System Management Tool.
- A user with a **Role** that has the **Create Work Area** action allowed can create a **Work Area** in the client.

Create a work area in the system management tool

1. On the Home page, click **Work Areas** .
2. On the Work Areas page, click create new .
3. Give the **Work Area** a name and description other **System Managers** will easily understand.
4. Choose which **Group** or **Groups** will have access to the **Work Area**.

5. Choose whether to use default settings or import settings from another **Work Area**.
6. Click **Save**.

List of settings that will be imported to a new work area

When creating a **Work Area**, you have the option to import settings from another **Work Area**. Most settings will be included in the import, such as the following:

- Custom added protein markers (*i.e.* ones that have been entered manually)
- **Work Area** preferences located in the **Preferences** dialog
- Show shape options in the **Show** group
- Image display options
- Table settings for all tables including which columns are displayed and how the table is sorted
- Instrument settings including scan presets (such as scan resolution, scan quality, and focus offset) and other options on the **Acquire** tab
- Custom grid, grid array, plate, and plate array templates
- Custom **Lab Book** templates
- Custom chart templates

Image Status

The Image Status is the current state of an image in the Image Studio 21 CFR Part 11 client (see "Workflow"), and it determines which **Actions** may be performed on an image. An **Action** must be performed to change the Image Status. To change an image's status, you must have the correct **Action** allowed for your **Role**.

Note: When an **Action** is performed on an image, the Image Status changes and the change is recorded in the "Image Log".

Image statuses and descriptions

Status Name	Status Description	Associated Actions

Acquiring	An image in the process of being acquired by a LI-COR instrument has the **Acquiring** status. After an image is acquired, the status is automatically changed to **Editing**. If you are assigned a role that is allowed the **Acquire** action but not the **Edit** action, you will be allowed to acquire images but not edit or analyze them.	**Acquire**: Allows you to perform an image acquisition using Image Studio Software and a LI-COR instrument.
Canceled	When the process of acquiring an image on a LI-COR instrument is canceled, the image has the **Canceled** status. A partially acquired image with the **Canceled** status cannot be analyzed or edited. Images cannot be removed from the **Canceled** status. The acquire process must be restarted.	**Cancel**: The **Cancel** action must be allowed for your role to cancel an image acquisition that has already started.
Editing	The **Editing** status allows changes to an image analysis to be saved. A user must have a role with the **Edit** action allowed to save changes to an image analysis.	**Submit for Approval**: Moves the image to the **Waiting for Approval** status. **Resume Edit**: Moves the image from the **Waiting for Approval** status back to the **Editing** status. **Edit Rejected**: Moves the image from the **Rejected** status back to the **Editing** status.
Waiting for Approval	The **Waiting for Approval** status designates that the image needs to be approved or rejected.	**Approve**: Moves the image to the **Approved** status. Reject Edited: Moves the image to the **Rejected** status. **Resume Edit**: Moves the image from the **Waiting for Approval** status back to the **Editing** status.

Rejected	The **Rejected** status designates that an image analysis does not meet organizational standards. Images cannot be edited or analyzed while in the **Rejected** status.	Reject Edited: Moves an image from the **Waiting for Approval** status to the **Rejected** status. **Edit Rejected**: Moves an image from the **Rejected** status back to the **Editing** status.
Approved	The **Approved** status designates that an image analysis meets organizational standards. Images cannot be edited or analyzed while in the **Approved** status.	**Approve**: Moves an image from the **Waiting for Approval** status to the **Approved** status. **Reject Approved**: Moves an image from the **Approved** status back to the **Editing** status.
Inactive	Inactive images are removed from normal view.	**Deactivate**: Moves the image to the **Inactive** status. **Reactivate**: Moves the image from the **Inactive** status to the **Editing** status.

Workflow

The basic Image Studio 21 CFR Part 11 workflow consists of:

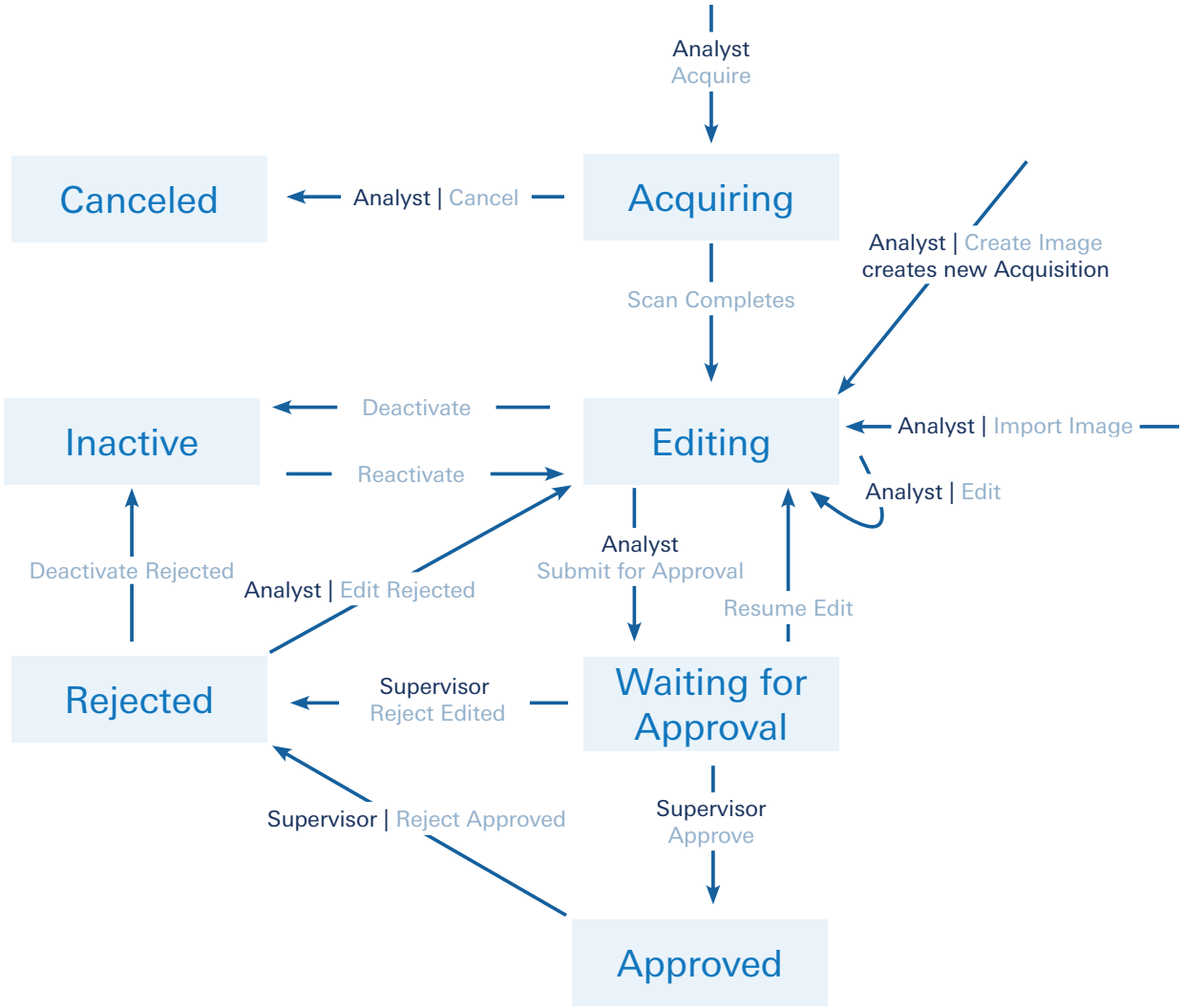
1. User scans or imports an image.
2. User analyzes the image, and then submits the image analysis for approval.
3. A different user will review the image analysis to approve or reject it.

Note: All **Actions** are recorded in the **Image Log**, including which user performed the **Action** and the date and time the action was performed.

The diagram below details the workflow in the Image Studio 21 CFR Part 11 client.

- Image statuses are shown in boxes.
- The **Action** necessary to move between statuses is shown with an arrow.
- If a **Role** is allowed to perform the **Action** by default, that **Role** is shown along with the **Action**.

The default configuration is shown below. **Roles** and **Actions** may be configured differently for your system.



Logs and Notifications

Log Types

Image Studio 21 CFR Part 11 keeps two different log files:

- **User Log**: The **User Log** records user activity in the client and System Management Tool. Notifications are also recorded in the **User Log**. The **User Log** can only be accessed through the System Management Tool.

  See "User Log" on page 33 for more information.

- **Image Log**: The **Image Log** records **Actions** performed on images, image metadata and analysis data, and must be accessed through the client.

  See "Image Log" on page 35 for more information.

User Log

The **User Log**, accessible only through the System Management Tool, contains the following records:

- **User activity:** Includes activity in the client and the System Management Tool. The log keeps the time stamp, full name of the user, and description of the activity performed.
- **Notifications:** Notifications will be posted on the Home page and recorded in the **User Log** when a configurable number of login attempts with an invalid user name occur within a specified time limit. This notification is configurable, see "Security Settings" on page 16.

View and download the user log

1. Click Logs on the top navigation bar.
2. User activity records are in the table, including time stamp, full name, and description of the activity.
3. To find the entries you need, use the search box above the table or the filters to the right of the table.

4. Click download to get a pdf of records in the user log for the date range specified in the Filters group.

   If other filters are applied, the pdf will contain only the entries that meet the filter requirements.

Unassociated Entries

Two conditions will cause the entry in the Full name column to be recorded as `<Unassociated>` instead of a user's full name:

- **Incorrect user name:** If a login attempt is made with an incorrect user name, the login attempt will be recorded as `<Unassociated>` because the login attempt cannot be linked to a known user.
- **Notifications:** System notifications are recorded as `<Unassociated>`.

User Activity Entries

- Login attempts to the client and System Management Tool
  - Successful user logins
  - Failed user logins (a known user name failed to login due to an incorrect password)
  - Attempted logins with an incorrect user name (listed with `<Unassociated>` in the Full name column)
- Logouts

System Manager Activity Entries

- User account created
- User deactivated
- User reactivated
- Password reset
- User **Group** or **Role** assignment changed
- System configuration changed (changes made on the Setup page)

Notifications

Notifications are recorded in the **User Log** and occur when:

- A user attempts to login with a deactivated account
- A threshold of login attempts with invalid user names occur in a specified time period

  This notification is configurable. See "Security Settings" on page 16.

Once a notification is recorded in the **User Log**, a warning is posted on the Home page.

Dismiss the unread notifications warning

1. On the Home page, click unread notifications.

   The Logs page will open, and the Unread Notifications filter will be applied to the table automatically.

2. Click Mark All as Read above the table.

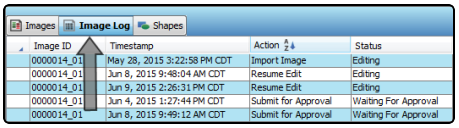
Once the notifications have been marked as read, the warning will no longer appear on the Home page, and other **System Managers** will not see the warning.

You can always view notifications, even after they are marked as read, by filtering the table on the Logs page by Notifications.

Image Log

Note: The **Image Log** can only be accessed through the Image Studio 21 CFR Part 11 client interface.

The **Image Log** contains the record of all **Actions** performed on an image and is located directly to the right of the **Images** table.



Add columns to the Image Log

The **Columns** option allows you to add additional columns to the **Image Log**.

1. Click **Columns** above and to the right of the **Image Log** table.
2. Select the **Column** you would like to include in the **Image Log**.
3. Click **Save**.

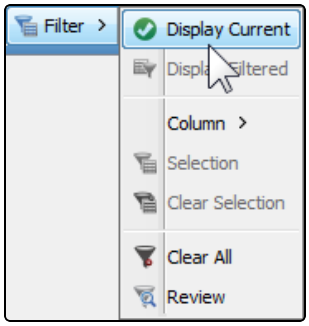
The selected **Column** will be added to the **Image Log**.

View Image Log for all images

By default, the **Current Image** filter is in place to only show entries for the current image in the **Image Log**. The **Current Image** is the image selected in the **Images** table.

To include entries for all images in the current **Work Area** in the **Image Log**, clear the **Current Image** filter.

1. Click **Filter** above and to the right of the **Image Log**.
2. Click **Display Current** to clear the filter.



Export Image Log

The following are options for exporting **Image Log** data.

- **Copy and Paste**: Right click selected data in the **Image Log** and then click copy (or press **CTRL+C**). Paste the data into a spreadsheet.

- **Export table data to a spreadsheet**: Click **Report** above and to the right of the table view and then choose whether to launch the data in an external spreadsheet program or save the data.

  Use **Options** at the bottom of the **Report** menu to:

  - Change whether data are saved as a .xls file or a tab-separated text document.
  - Change whether the entire table is exported or just selected rows.

- **Add to Lab Book Report**:

  1. On the **Lab Book** tab, click **Edit**.
  2. Select **Image Log Table** in the **Available Layout Items** column.
  3. Click **Add Item**.
  4. Once you are finished modifying the layout, click **OK**.